WiSpot: Fast and Reliable Detection of Wi-Fi Networks using IEEE 802.15.4 Radios

Junaid Ansari, Tobias Ang and Petri Mähönen
Institute for Networked Systems, RWTH Aachen University, Kackertstrasse 9, D-52072, Aachen, Germany {jan, tan, pma}@inets.rwth-aachen.de

ABSTRACT

One of the key challenges for the deployment of IEEE 802.15.4 based networks is the interference from more powerful IEEE 802.11 based Wi-Fi networks operating in the same 2.4 GHz ISM frequency band. In order to avoid interference and ensure reliable communication, IEEE 802.15.4 networks are first required to identify potentially interfering channels. In this context, we have designed WiSpot, which uses pair-wise synchronized channel sensing algorithm on a platform with two IEEE 802.15.4 compliant radios. It is able to detect IEEE 802.11b/g signal signatures with ca. 96% accuracy within a maximum required duration of 310 ms. Our experiments confirm its reliable operation within a range of 25 m indoors. WiSpot is also able to detect multiple collocated Wi-Fi transmitters. The algorithm is robust against the IEEE 802.11b/g signal leakages on commercially available NICs and has been tested on five different Wi-Fi transmitters from different vendors. Performance comparison against other state-of-the-art solutions indicates that WiSpot is superior in terms of the detection accuracy and the required detection duration.

Categories and Subject Descriptors
C.2.1 [Network Architecture and Design]: Wireless communication

General Terms
Algorithms, Design, Experimentation, Performance

Keywords
Wi-Fi detection, signal classification, IEEE 802.15.4 radio

1. INTRODUCTION

In recent years, numerous networks and devices using the popular IEEE 802.15.4 compliant radios at 2.4 GHz have emerged for home automation, building monitoring and IEEE 802.15.4 networks already exist in the same frequency band, it results in mutual interference.

Wi-Fi networks typically use approximately 100 times higher transmit power, therefore, they tend to inflict heavy packet losses on IEEE 802.15.4 communication as have been reported by other research studies [1–3]. It has also been observed that in close proximity, IEEE 802.15.4 networks cause interference to IEEE 802.11b/g networks leading to significant performance degradation [4]. Both IEEE 802.11b/g and IEEE 802.15.4 networks have been designed without provision for symbiotic coexistence with each other [5–7], yet they are actively deployed in the same environments. A possibility of pre-assigning dedicated non-interfering channels to each network is not only tedious and expensive in terms of human effort, it is also a waste of spectral resource and is becoming unpractical due to increasing spectrum scarcity [8]. Furthermore, a centralized infrastructure for spectrum management and cooperative spectrum access as in IEEE 802.22 [9] is impractical for heterogeneous networks and devices operating in ad hoc environments in the ISM frequency bands with varying and unpredictable spectral needs.

Reliable detection of potential interferers is a fundamental requirement for applying an interference mitigation scheme and enabling spectral coexistence. The faster a system is able to identify interfering channels, the more energy efficient it is. In this context, we have designed a low cost platform named WiSpot, which is able to reliably identify Wi-Fi channels with an accuracy of ca. 96% and requires a maximum detection duration of 310 ms. WiSpot consists of two IEEE 802.15.4 radios interfaced to a microcontroller. It uses a synchronized channel sensing algorithm to detect IEEE 802.11b and IEEE 802.11g transmitters. One of the key features of the algorithm is its ability to identify a wide-band Wi-Fi transmission channel using a combination of narrow-band IEEE 802.15.4 radios. The algorithm is computationally simple and is implemented on the host microcontroller. We think that WiSpot can be used as 1) a usual single radio node in IEEE 802.15.4 networks while the secondary radio when required allows the possibility of detecting Wi-Fi networks, 2) a dual radio platform such as [10–13] in a Wireless Sensor Network (WSN) with a provision of additional sensing radio and capability of detecting IEEE 802.11b/g networks and 3) a platform for discovering WLAN setups such as ZiFi [14].

The rest of the paper is structured as follows: Section 2 provides the related work. Section 3 describes the prototype implementation while Section 4 describes the design rationale of WiSpot and the algorithmic details. In Section 5 we present extensive empirical performance evaluation studies and the comparison to ZiFi. Finally, Section 6 concludes the paper.

2. RELATED WORK

Spectrum sharing and symbiotic coexistence among different networks and devices are becoming inevitable due to the ever increasing number of wireless network applications in our daily life. The
2.4 GHz ISM band is a popular choice for many consumer networks owing to the available bandwidth, current radio technology, transmission range and energy consumption aspects. Uncoordinated spectrum access and lack of spectrum sharing features in this frequency band cause mutual interference among different networks which eventually leads to performance degradation [1]. Compared to Wi-Fi, low-power IEEE 802.15.4 networks suffer significantly higher performance losses [2, 3]. Infrastructure based coordinated spectrum access such as in IEEE 802.22 networks [9] is not a viable option for heterogeneous networks with often user-deployed consumer devices operating in ISM frequency bands.

In order to minimize wireless interference, many approaches enabling dynamic spectrum access have been proposed by the research community during the past few years. Simulation results show that graph coloring schemes such as [15] [16] help in mitigating interference. Interference aware medium access procedures such as [6] [7] [5] [4] have been designed to ensure communication reliability by selecting interference minimal channels. In [17], the authors have devised a Pareto model to characterize white spaces in Wi-Fi networks based on the statistical analysis of white space empirical data. They have proposed a new ZigBee control protocol to exploit the expected frame collision probability and the channel utilization ratio. While most of the IEEE 802.15.4 and IEEE 802.11 network deployments are carried out indoors in unstructured and ad hoc topologies, due to fast fading and multi-path effects, the resulting channel propagation conditions are complicated and hard to predict. These lead to complex time-varying distributions for the expected channel occupancies in contrast to rather simple channel occupancy distributions as studied in [17]. In [18], the authors proposed a model to allow co-existence between IEEE 802.15.4 and IEEE 802.11b/g networks in different operating ranges. However, this scheme requires timing modification of the two protocols and does not completely solve the problem of mutual interference. Authors in [19] claim that IEEE 802.15.4 compliant CC2420 [20] radio has good properties for alternate and adjacent channel rejection thereby allowing it to coexist with WLAN, Bluetooth and other ZigBee interfering networks. However, their measurements do not take into account out-of-band leakages and MAC behaviours. Therefore, in real deployments other researchers have noted a performance loss [2, 3, 18]. Liang et al. [4] have analyzed interference patterns between IEEE 802.15.4 and Wi-Fi networks at a bit-level granularity. They have noticed that a significantly high packet loss ratio in IEEE 802.15.4 transmission is due to the corruption of header bytes while the rest of the packet remains uncorrupted. Based on this observation, they have devised a scheme of repeating headers back to back in the frame and using Reed-Solomon encoding based Forward-Error-Correction (FEC) scheme to mitigate Wi-Fi interference. While an FEC based approach can certainly reduce the packet losses in the case of wireless interference, dynamic selection of less interfering channels can lead to higher performance gains without imparting extra channel coding overhead [21] [22]. Accurate and reliable detection of interfering channels is rudimentary to any Wi-Fi interference mitigation strategy. In [23], authors survey the various techniques used for spectrum sensing and classification of signals. With the current low-power radio technology, energy detection is the most practical and viable option. Other methods such as spectrum cyclostationarity detection and matched filter based detection [23] are too complex to be implemented on low-power radios. In [24], authors apply spectral mask fitting of the signal strength measurements to WLAN transmissions. This scheme has limitations in the case of out of band signal leakages and in the case of overlapped transmissions. Zhou et al. have developed ZiFi [14], which utilizes an IEEE 802.15.4 radio to ascertain the existence of IEEE 802.11b/g Access Points (APs) generating periodic beacons. It uses a Common Multiple Folding (CMF) algorithm for detecting the Received Signal Strength Indicator (RSSI) of the periodic interfering signal. The basic idea of CMF is to search for a periodic signal (with a period $P$) within a series of RSSI samples. The series is divided into smaller sequences of length $P$ at different starting points (phases). If the phase of the folding happens to align with that of the periodic signal, the magnitude of the sum is amplified at a period of $P$ while the aggregate value of the noisy samples in the series remains low. In order to determine the correct phase, CMF requires systematically calculating the result for all the different phases. ZiFi has been implemented on an Asus Linux notebook connected to a TelosB sensor node and on a Nokia N73 smart-phone connected to a ZigBee module over the miniSD interface. ZiFi claims to have an average accuracy of 95% reliable detection with a spectrum sensing overhead of 786.4 ms. We have observed that WiSpot outperforms ZiFi in the same experimental settings as described in Section 5.7.

3. PROTOTYPE IMPLEMENTATION

In this section we describe the hardware design and algorithmic aspects of WiSpot prototype.

3.1 Hardware Design

WiSpot consists of two IEEE 802.15.4 compliant radios interfaced to a low-power microcontroller as shown in a simplified block diagram in Figure 1. We have selected CC2420 radio transceivers interfaced with an MSP430 [25] series microcontroller for our design. The Serial Peripheral Interface (SPI) bus is used for reading/writing the configuration registers as well as the RX/TX FIFOs on the two radios. The RSSI value from the CC2420 radio is mapped to an internal register and is also read over the SPI bus. The CCA (Clear Channel Assessment) pin interrupts the microcontroller with the status of the channel assessment while the SFD (Start-of-Frame-Delimiter) pin triggers an interrupt when an IEEE 802.15.4 header is detected.

In the prototype implementation (c.f. Figure 2a), we have interfaced two TelosB nodes [26] from Crossbow Technology Inc. in a Master-Slave configuration as shown in Figure 2b. A TelosB platform has a CC2420 radio transceiver and an MSP430 series microcontroller operating at 4 MHz. The microcontroller supports commonly used serial bus interfaces and provides multiple General Purpose Input/Output (GPIO) lines. The Universal Asynchronous Receiver/Transmitter (UART) interface is used for communicating with the slave TelosB. In particular, RSSI values and the status for different operations are read over UART. The UART interface is also used for communicating information such as the CCA detection threshold value, the channel to be scanned and the channel scanning duration to the slave node. The CCA interrupt from both

![Figure 1: A simplified block diagram of WiSpot consisting of a microcontroller and two radios.](image)
the radios is processed at the master microcontroller. Besides the radio interfacing, a GPIO line (shown as INT in Figure 2b) is used for coordinating the synchronized sensing operation on the two radios.

3.2 Embedded Software Implementation

We have implemented the drivers and the algorithm on TinyOS 2.x [27]. MSP430 assembly language and low-level TinyOS 2.x abstractions are used to minimize the signaling overhead of TinyOS 2.x in handling the interrupts and GPIO callback functions. The native MSP430 clock drivers are modified to allow higher SPI and UART bus speeds. Most notably, in the driver implementation, we have separated the commands necessary for switching a frequency channel from the sequence of commands required only at boot-up. Furthermore, while switching a frequency channel, the voltage regulator is kept running instead of completely switching off the radio. This implementation has improved the frequency channel switching speeds to approximately 60 % faster as compared to our previous implementation [5]. Table 1 lists the average time required for different operations on the prototype hardware platform.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Required time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading an RSSI sample</td>
<td>70 (\mu)s</td>
</tr>
<tr>
<td>Checking the CCA status</td>
<td>22 (\mu)s</td>
</tr>
<tr>
<td>Radio boot-up duration (once only)</td>
<td>2.41 ms</td>
</tr>
<tr>
<td>Frequency channel switching</td>
<td>740 (\mu)s</td>
</tr>
<tr>
<td>Timeout for SFD interrupt after channel busy</td>
<td>160 (\mu)s</td>
</tr>
<tr>
<td>Maximum channel sensing duration</td>
<td>100 ms</td>
</tr>
</tbody>
</table>

The algorithm is computationally lightweight and is implemented on the host microcontroller. The executable code for TinyOS 2.x is in the form of a single binary file. The memory footprint in terms of the RAM and ROM usage on the master microcontroller is 17308 B and 9184 B, respectively. The RAM and ROM usage of the executable binary file on the slave microcontroller are 12156 B and 4470 B, respectively. The code size accounts for approximately 35 % of the available flash memory.

4. ALGORITHMIC DETAILS

Our algorithm uses pair-wise sensing of the IEEE 802.15.4 channels. The pair-wise channel sensing is performed to cover the whole 2.4 GHz frequency spectrum. During the spectrum scanning process, samples for signal strength levels are gathered, which are later analyzed at the master microcontroller for Wi-Fi transmitter detection. The algorithm consists of multiple parts and will be explained in detail in this section.

Before going into the algorithmic details, first we give an overview of the key characteristics of IEEE 802.11/b/g networks that directly influence the different parameters of our algorithm. Then we describe a radio array platform, which enabled us to empirically analyze the signal strength measurements and the latencies associated with different operations on the CC2420 radio. Finally, we describe a scheme which minimizes the required channel switching combinations for detecting Wi-Fi transmission channels.

4.1 IEEE 802.11/b/g Signal Characteristics

As shown in Figure 3a, there are 13 overlapping IEEE 802.11/b/g channels with a bandwidth of 22 MHz. The separation between the center frequencies of adjacent channels is 5 MHz. On the contrary, 2 MHz IEEE 802.15.4 channels with adjacent channel separation of 5 MHz are non-overlapping as shown in Figure 3b. Sensing adjacent channels is necessary in order to uniquely identify a particular IEEE 802.11/b/g channel using a narrow band IEEE 802.15.4 radio. In reality, this is more challenging since an IEEE 802.11/b/g signal can be ephemeral and intermittent. IEEE 802.11/b/g protocol standard specifies the frame formats and the timing characteristics. A sender-receiver pair exchanges Request-To-Send (RTS), Clear-To-Send (CTS), Data and acknowledgement (ACK) frames with fixed intervals of SIFS and DIFS in between. The channel sensing duration must be longer than a DIFS interval in order to detect an ongoing transmission.

The timing characteristics of the IEEE 802.11/b/g frames dictate the minimum required sensing duration and the number of samples in performing signal strength measurements for the detection of Wi-Fi transmitters using our platform. Currently, IEEE 802.11b and IEEE 802.11g are the most widely deployed Wi-Fi networks. Here we note that although IEEE 802.11n is getting popular but has still a low penetration. IEEE 802.11b and IEEE 802.11g support raw data rates of 11 Mbps and 54 Mbps, respectively. These data rates result in different timing characteristics for the two standards. Table 2 lists the frame transmission durations and the inter-frame intervals for IEEE 802.11b and IEEE 802.11g networks. A unique characteristic of IEEE 802.11 networks is the periodic transmission

![Figure 3: Frequency channels of (a) IEEE 802.11b/g and (b) IEEE 802.15.4.](image-url)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>IEEE 802.11b</th>
<th>IEEE 802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIFS</td>
<td>30 (\mu)s</td>
<td>10 (\mu)s</td>
</tr>
<tr>
<td>DIFS</td>
<td>50 (\mu)s</td>
<td>28 (\mu)s</td>
</tr>
<tr>
<td>Slot time</td>
<td>20 (\mu)s</td>
<td>9 (\mu)s</td>
</tr>
<tr>
<td>Min. length packet</td>
<td>202 (\mu)s</td>
<td>194 (\mu)s</td>
</tr>
<tr>
<td>Max. length packet</td>
<td>1906 (\mu)s</td>
<td>542 (\mu)s</td>
</tr>
</tbody>
</table>
of a beacon frame. A beacon frame is transmitted every 100 ms to 200 ms. A default value of 100 ms is used in most of the deployed networks. A beacon frame is transmitted at the lowest possible raw data rate of the radio. Based on the frame structure and the transmission rates, the minimum in-air time of a beacon frame for IEEE 802.11b/g turns out to be 224 $\mu$s.

### 4.2 Spectrum Sensing on IEEE 802.15.4 Radio

Within the minimum in-air frame duration of 194 $\mu$s and the minimum in-air beacon interval of 224 $\mu$s, our enhanced driver implementation (c.f. Table 1) allows obtaining at least two RSSI samples. If a measured RSSI value is found to be higher than the estimated noise floor in a channel, it may indicate the presence of a Wi-Fi transmitter. However, sensing a 2 MHz wide channel cannot guarantee the presence of a Wi-Fi transmitter and its center frequency unless the adjacent channels are also sensed. Considering typical transmitters in the 2.4 GHz spectrum, a high energy level sensed in one of the IEEE 802.15.4 channels can possibly also be due to another IEEE 802.15.4 transmitter or a Bluetooth device. The channel switching duration of 740 $\mu$s (c.f. Table 1) is so long that it does not guarantee a correct Wi-Fi detection while the in-air time of a Wi-Fi transmission can possibly be shorter. Therefore, unless a signal is periodic and/or the Wi-Fi transmission intervals are continuous and long, reliable detection of a Wi-Fi transmitter is not possible using a single IEEE 802.15.4 radio.

### 4.3 Spectrum Sensing using IEEE 802.15.4 Radio Array

In order to study the simultaneous channel sensing characteristics and the effects of different RSSI sample sizes for reliable detection of a Wi-Fi transmitter, we have designed a radio array platform by concatenating eight TelosB nodes. One of the nodes acts as the master node while the rest are slaves. A GPIO interrupt link from the master node to all the slave nodes is used in a similar configuration as on the WiSpot prototype (c.f. Figure 2b) for synchronized channel sensing. The RSSI samples from all the nodes were gathered on a PC over the USB interface for post-processing and analysis. Two important parameters were studied during the measurements on the radio array platform, namely the CCA threshold (or detection threshold) and the RSSI sample size. Since the received power also depends on the distance from the transmitter, a very high CCA threshold value suppresses the weak/distant transmitters while a very low threshold can lead to higher false positives. We have studied the effects of different detection thresholds and chose a default value of -77 dBm. We will discuss the implications of different values for CCA threshold in Section 5.4. The simultaneous channel occupation scheme gives an average Wi-Fi detection accuracy of over 98%. Furthermore, we have noted that using the bandwidth of the detected signal, Wi-Fi and IEEE 802.15.4 transmissions can be distinguished. We have to also consider a situation where adjacent IEEE 802.15.4 channels are used by different IEEE 802.15.4 networks. Though the probability of simultaneous usage of adjacent channels is extremely low, yet such a case can potentially lead to false detection decision of a Wi-Fi transmitter. This problem is overcome in WiSpot using the Start-of-Frame (SFD) interrupt provided by the CC2420 radio transceiver, which is triggered only upon detecting an IEEE 802.15.4 frame header. Figure 4 shows the RSSI sample set required for detecting a Wi-Fi AP beacon.

### 4.4 Synchronized Channel Sensing on a Dual Radio Platform

The experiments with the radio array platform have shown that simultaneous occupation of adjacent IEEE 802.15.4 channels is a reliable indication for a Wi-Fi transmitter detection. However, using an 8-radio or a 4-radio platform for detecting Wi-Fi signals on the host platform involves a high communication/coordination overhead for the master microcontroller. This has led us design a platform having a minimum number of required radios and yet providing a high level of accuracy. A dual-radio platform certainly is the most cost effective platform requiring multiple radios and gives a low communication overhead compared to larger radio array platforms and is still able to perform synchronized channel sensing. Furthermore, a dual-radio platform also allows efficient MAC designs [11, 13, 28].

For a fast Wi-Fi detection, the required overhead has to be minimized. The overhead for detecting a Wi-Fi transmitter can be divided into three distinct categories: communication overhead, sensing overhead and processing overhead. While the sensing overhead is attributed to the characteristics of the IEEE 802.11b/g signals (including the frequency channel bandwidth and the minimum in-air frame duration), the communication and processing overhead has been kept to a minimum on the WiSpot prototype as we will describe later with the help of Figure 5. The sensing overhead duration can maximally go to 100 ms, which corresponds to the default beaconing rate of a Wi-Fi AP. The communication overhead on the WiSpot accounts for the master-slave communication and the overhead for sending configuration command messages to the radios. Furthermore, reading RSSI samples and handling interrupts are also attributed to the communication overhead. Finally, the processing overhead is ascribed from the analysis of RSSI samples and the decision logic.

WiSpot has two modes of operation. In the RSSI mode, the RSSI samples are gathered from the two radios in adjacent channels for a duration of 100 ms and post-processed for a simultaneous channel occupancy detection. In the RSSI+CCA mode, besides the RSSI samples, the CCA interrupt signals are also analyzed. Please note that a CC2420 radio transceiver has a built in clear channel assessment algorithm [20]. A CCA threshold is selected through the configuration registers (we use a default value of -77 dBm). If the sensed energy in the medium is detected to be higher than this threshold, the CCA interrupts from the two radios are invoked at the master microcontroller.

Figure 5 shows different steps performed on the master and slave nodes while the simultaneous channel sensing operation is performed in the RSSI+CCA mode. The operations on the master node are indicated through M1-M9 while those performed at the slave node are indicated through S1-S5. These operations are divided into the communication, sensing and processing overhead.

![Figure 4: RSSI sample size and the Wi-Fi beacon detection ratio on IEEE 802.15.4 radio array with a detection threshold of -77 dBm.](image-url)
categories. Compared to the RSSI+CCA mode, the operations in M5 and M6 on the master node and the corresponding operation S3 (as shown in Figure 5) differs in the RSSI mode, where both the master and slave nodes always collect RSSI samples for a fixed duration of 100 ms. Since gathering and simultaneously processing the RSSI samples on-the-fly significantly slows down the processing speed, the gathered RSSI samples are post-processed for simultaneous channel occupancy in the RSSI mode. WiSpot gathers >2800 samples in the RSSI mode, which gives it a high reliability as can be seen from Figure 4.

In the RSSI+CCA mode, only in the case when the CCA interrupts on both the radios are not triggered, channel sensing steps M5 and S3 are performed for the maximum duration of 100 ms. In the case of RSSI+CCA mode, as soon as the CCA interrupts at the master node indicate simultaneous detection, collect RSSI samples at the slave node and collect RSSI samples. This scheme results in much shorter overall detection duration as compared to the RSSI mode as we will describe in Section 5.3. Having a shorter detection duration, RSSI+CCA mode is also more energy efficient.

The algorithm for the scanning sequence of different channels to cover the complete spectrum is described later in Section 4.5. The set of operations shown in Figure 5 are repeated sequentially for each channel step.

4.5 Spectrum Scanning Sequence

In order to uniquely detect a particular Wi-Fi channel, three scanning sequences of adjacent IEEE 802.15.4 channels are required. However, using the scheme described in Figure 6, WiSpot requires only 15 sensing steps to cover the complete 2.4 GHz spectrum. For instance, in the first step (T1), the master node chooses IEEE 802.15.4 channel 11 while the slave is assigned IEEE 802.15.4 channel 12. During a particular sequence step, the set of operations described in Figure 5 are performed at the master and slave nodes. If an IEEE 802.15.4 channel pair is detected to be simultaneously occupied, the mean RSSI values for the channel pair is stored before proceeding to the next channel pair. The IEEE 802.11b/g channels corresponding to the IEEE 802.15.4 channel pair (as shown in Figure 6) with simultaneous channel occupation are marked as shortlisted. At the end of the complete spectrum scanning operation (after step T15), identification of IEEE 802.11 b/g channels is carried out at the master node using the algorithm described in Figure 7. The shortlisted IEEE 802.11 b/g channels are checked for any overlaps. If no overlap is found, the shortlisted channel becomes the final list for IEEE 802.11b/g detected channels. A shortlisted channel list without a conflict indicates that the colocated Wi-Fi channels are non-overlapping, i.e., the central frequencies are more than 25 MHz apart.

In certain cases, a conflict situation may also arise due to the out-of-band channel leakages and overlapping Wi-Fi channels. If an overlap is found, an iterative conflict resolution strategy is applied. The conflict is resolved by sorting all the shortlisted channels in a descending order based on their four channel RSSI total. The four channel RSSI total is the sum of the mean RSSI values (higher than the CCA threshold) of the four IEEE 802.15.4 channels and is a representation of the total energy measured over a bandwidth of 15 MHz. Based on the fact that the total energy is highest around the central frequency of an IEEE 802.11 transmission channel, finding the correct channel from a list of overlapping channels is done by picking the shortlisted channel with the highest RSSI total. It is due to the fact that shortlisted channels have been sorted, the first entry is stored in the final list and all other subsequent channels which overlap with this entry are ignored. Thereafter, when the next non-overlapping channel with the highest RSSI total is found, it is automatically added to the final list and once again all other subsequent channels which overlap with this channel are ignored. Once the search has reached the end of the sorted list, it becomes the final list. The conflict resolution scheme is also robust against considerable amount of Wi-Fi signal leakages as observed within a range of ca. 6 m on most of the commercially avail-
able NICs. Besides using the RSSI samples to detect the presence of an IEEE 802.11 transmitter, the RSSI samples over two sensing durations are also analyzed to characterize the channel utilization ratio as well as the interference levels. This information can be later used for the selection of transmission channel in an IEEE 802.15.4 network [21]. Furthermore, after a separation of 11 MHz and 22 MHz from the center frequency, the radiated energy from an IEEE 802.11b transmitter is 30 dB and 50 dB below the maximum level, respectively. In contrast, IEEE 802.11g transmitter’s radiated energy level after a separation of 11 MHz and 22 MHz from the central frequency is only 20 dB and 30 dB below the maximum, respectively. This unique characteristic is exploited in WiSpot RSSI readings over a short distance (ca. 10 m) to identify the Wi-Fi signal mask.

5. EXPERIMENTAL PERFORMANCE EVALUATION

We have carried out performance evaluation of WiSpot both in the RSSI mode and the RSSI+CCA mode. We have considered the IEEE 802.11b/g AirHORN dual band signal generator, Linksys WRT54GL broadband router and Atheros based mini-PCI-E card on Asus Eee netbooks as signal sources using 20 dBm of transmit power level. The beacon rate for all the APs was fixed to the default value of 100 ms. All the experiments were conducted in an indoor office environment with line-of-sight between the WiSpot and the transmitter(s). We have obtained 500 samples for each measurement point in all the experiments.

5.1 Experimental Setup

Figure 8 shows the experimental setup using a single transmitter as well as multiple transmitters, where the distances of the transmitters were varied from WiSpot platforms operating in the RSSI mode and the RSSI+CCA mode. PCs connected to the WiSpot platforms record the detection characteristics for each experiment. During the experiments, Agilent’s E4440A spectrum analyzer was used to monitor that no astray signal influences the measurements.

5.2 True Positive and False Negative Detections

In this experiment, we used an AirHORN IEEE 802.11b signal generator transmitting with the maximum possible rate, giving a radio duty cycle of approximately 72 % (ATP), an IEEE 802.11b/g beaconsing Linksys AP (BeaconB, BeaconG) and a netbook sending a UDP stream using the iperf tool in both the IEEE 802.11b and IEEE 802.11g modes (UDPB and UDPG). The UDP stream used a datagram size of 1470 B and the observed traffic statistics per second were reported as an average of 7.3 Mbps and 24 Mbps for UDPB and UDPG, respectively. In the rest of the experiments, the traffic settings were kept the same as above and we follow the same notations as above. Figure 9 shows the true positive ratio for different traffic patterns in a single transmitter scenario when the WiSpot distance to the transmitter was fixed to 3 m (to allow a comparison with ZiFi [14]). It can be observed that the RSSI mode shows a detection ratio between 95 % to 99.8 % when the channel utilization is high for the case of ATP, UDPB and UDPG, while it drops to 80 % for the case of just beacon transmissions. On the contrary,
the RSSI+CCA mode shows a detection ratio of 96% except for the case of UDPG where it falls to 82%. The figure also shows the breakdown analysis of the true positive ratio in terms of the detection without the conflict situations for overlapping Wi-Fi channel detections and the detections after successfully resolving the conflict situations. The RSSI+CCA mode shows much higher conflict cases, which are due to a high sensitivity threshold and the leakages at this short distance. However, our algorithm (c.f. Figure 7) is able to successfully resolve the conflicts and is able to provide an overall detection accuracy between 95% to 99.8%. In both the operating modes, we did not encounter any false detections. This is because compared to a single channel sensing scheme, the chances of getting a simultaneous noisy spike in both independently sensed adjacent channels are extremely low.

5.3 Analysis of the Detection Time

Fast and reliable detection is not only energy efficient but is also desirable in dynamic environments to sense the interfering channels and opportunistically utilize this information. The RSSI mode shows almost the same detection time for different traffic patterns and the average detection duration is $1.99 \pm 0.2s$. The absence of a signal source has almost no effect on the detection duration. On the contrary, as can be observed from Figure 10, the required time for Wi-Fi detection on WiSpot operating in RSSI+CCA mode is much lower. Based on the average detection time of 1.24 s, the longest per IEEE 802.11 channel detection and the overall sensing durations turn out to be 310 ms and 2.33 s, respectively. The average per channel communication and processing overhead is approximately 55 ms, which accounts for 17.74% of the overall timing overhead. The figure also indicates that as the channel utilization ratio increases (from beacon to UDP traffic and ATP), the required detection time decreases.

Figure 10: Average detection duration on WiSpot in the RSSI+CCA mode.

5.4 Effect of the Detection Threshold

The CCA detection threshold has direct influence on the detection capability of the WiSpot platform. In order to observe the influence of the CCA threshold level on the performance of RSSI+CCA mode of the WiSpot, we placed a UDPB transmitter at a distance of 5 cm. We varied the detection threshold from the default -77 dBm value to -35 dBm. It can be observed from Figure 11 that due to very strong signal leakage at this short distance, none of the channels were detected conflict free at the default threshold of -77 dBm. Similarly, at a detection threshold of -55 dBm, a conflict free detection of only 2% could be observed. However, our conflict resolution scheme could result in approximately 75% of true positives in these two extreme cases. For higher detection thresholds of -45 dBm and -37 dBm, no conflicting channel case was observed and over 95% true positive ratio was obtained. However, at a very high detection threshold value of -35 dBm, only 9% cases were detected. On the other extreme, lowering down the detection threshold to -85 dBm has resulted in 4% false positives which rises to 100% at a detection threshold of -98 dBm, which is out of the sensitivity range of the radio transceiver chip.

5.5 Effect of Distances

In order to study the effect of physical distance from the transmitter on the performance of WiSpot platform, we have carried out the above mentioned experiments at different distances. Figure 12 shows that at higher distances from the transmitter, the performance of the RSSI mode for BeaconB has shown to suffer. The WiSpot operating in the RSSI+CCA mode has shown to be more stable over the range of distances. The measured received power at a distance of 21 m was observed to be approximately -78.1 dBm which is very close to the detection threshold of -77 dBm and hence beyond this range WiSpot does not detect a signal. Of course, the detection threshold can be reduced to achieve higher range but it may lead to false detections.

Figure 11: Effects of the detection threshold value.

Figure 12: Average true positives w.r.t. distance from the transmitter. A total of 500 samples were taken for each distance.
5.6 Detection of Multiple Collocated Wi-Fi Transmitters

The existence of multiple collocated Wi-Fi networks is very common in office and home environments. WiSpot is able to detect multiple collocated Wi-Fi networks. In most of the Wi-Fi deployment setups, non-overlapping channels 1, 6 and 13 are used. In order to study the reliability and accuracy of WiSpot, we conducted a series of experiments with 3 collocated Wi-Fi networks in channels 1, 6 and 10 to represent a separation case of 5 and 4 channels, respectively. Furthermore, we used heterogeneous traffic patterns as described above and use different distances of the transmitter from the WiSpot platforms operating in both the modes. Figure 13 shows the mask overlap of two Wi-Fi networks with a separation of 4 channels. In our measurements, the case would become more challenging as we placed the transmitters at different distances resulting in unequal scaling of the mask overlapping. Figure 14 shows the true positives for the case when the transmitters in channel 1 and channel 6 are placed at a distance of 1 m, while the transmitter in channel 10 is at a distance of 15 m. It is worth noting that the RSSI mode performs better the RSSI+CCA mode and is able to give an average successful detection to be over 95%, while for the case of RSSI+CCA mode, in the non-overlapping channels 1 and 6, a true positive ratio of 70% is observed. This shows that the ability of WiSpot in the RSSI+CCA mode to detect IEEE 802.11 transmitters in the correct channel is higher when the transmission channels do not overlap. RSSI mode has the advantage of first gathering all the samples and then perform the analysis while the RSSI+CCA mode, upon getting a CCA interrupt may lose the later samples and can falsely base its decision upon the aggregate signal from the sidebands of two overlapping channels. This has resulted in an overall detection ratio of 75%. One solution to this problem is to gradually decrease the CCA threshold in steps, which will avoid the trigger of simultaneous detections when the threshold is small but it will require more scanning rounds.

5.7 Comparison with ZiFi Scheme

Unlike ZiFi, WiSpot requires two IEEE 802.15.4 radios. However, WiSpot is able to detect multiple collocated Wi-Fi transmitters and receive IEEE 802.15.4 frames. It is lightweight and is implemented on a sensor node microcontroller. We have evaluated WiSpot under identical experimental settings as described in [14]. Table 3 compares different performance metrics on the two platforms. It can be observed that WiSpot outperforms ZiFi in terms of the detection ratio and the timing characteristics. Additionally, WiSpot does not pose any restriction on the channel utilization ratio and is able to detect multiple collocated Wi-Fi transmitters.

<table>
<thead>
<tr>
<th>Performance metric</th>
<th>ZiFi</th>
<th>WiSpot</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSSI mode</td>
<td>95%</td>
<td>91%</td>
</tr>
<tr>
<td>False Positive Ratio</td>
<td>5%</td>
<td>0%</td>
</tr>
<tr>
<td>Min. detection time per channel</td>
<td>786.4 ms</td>
<td>500 ms</td>
</tr>
<tr>
<td>Max. detection time per channel</td>
<td>786.4 ms</td>
<td>266 ms</td>
</tr>
<tr>
<td>Whole spectrum scanning duration</td>
<td>3.75 s</td>
<td>2.33 s</td>
</tr>
<tr>
<td>Required channel utilization</td>
<td>0-30%</td>
<td>0-100%</td>
</tr>
<tr>
<td>Detects multiple Wi-Fi transmitters</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

6. CONCLUSIONS

In this paper, we have described the design and implementation details of WiSpot – a platform for fast and reliable detection of IEEE 802.11b/g signals. WiSpot is based on two IEEE 802.15.4 radios. It uses a synchronized channel sensing scheme for detecting Wi-Fi transmitters. Using a conflict resolution strategy and the spectral masks of the IEEE 802.11b/g signals, WiSpot algorithm is able to accurately identify Wi-Fi transmissions and is robust to out-of-band signal leakages in commercially available Wi-Fi NICs. The SFD interrupt on WiSpot platform allows distinguishing IEEE 802.15.4 transmissions in adjacent channels from a Wi-Fi transmission. The algorithm is lightweight and is implemented on the host microcontroller. Extensive performance evaluation of WiSpot in the presence of different types of traffic patterns and over different distances have been conducted. Furthermore, the effects of detection threshold has been studied and timing analysis of the algorithm has been carried. We have observed that WiSpot with two radios is able to maintain as high detection reliability as a higher radio array platform. We have devised a scheme that minimizes the number of lookups required for the spectrum scanning operation in order to uniquely identify a Wi-Fi transmission channel. We have also evaluated the performance of WiSpot in the presence of multiple signal
sources with overlapping and non-overlapping frequency channels. Our results confirm a high detection accuracy over a range of operating distances.

We have also conducted comparative performance evaluation studies of WiSpot with ZiFi in identical experimental conditions. The results indicate that WiSpot outperforms ZiFi in terms of detection reliability. Furthermore, WiSpot requires a shorter duration for the detection of a Wi-Fi transmitter. A single IEEE 802.15.4 radio, as is the case in ZiFi, does not permit sampling a larger coordinated sensing bandwidth. Therefore, it has to rely purely on the periodicity of the IEEE 802.11b/g signal, which leads to a longer detection time. Unlike ZiFi, WiSpot also allows detection of multi-collocated Wi-Fi transmitters. The developed WiSpot algorithm works without modification for IEEE 802.11n networks as long as they do not use channel bonding, i.e., use a bandwidth of 22 MHz. However, in the case of channel bonding (40 MHz bandwidth), the algorithm requires minor modifications in the channel lookup table.

Acknowledgment

We would like to thank partial financial support from DFG through UMIC Research Centre, and European Union through FARAMIR and 2PARMA projects.

7. REFERENCES