

Various Detection Techniques and Platforms for Monitoring Interference Condition in a Wireless Testbed

Wei Liu¹*, Stratos Keranidis², Michael Mehari¹, Jono Vanhie-Van Gerwen¹, Stefan Bouckaert¹, Opher Yaron¹, and Ingrid Moerman¹

Ghent University - IBBT
Gaston Crommenlaan 8 Bus 201, B-9050 Gent, Belgium
{wei.liu,michael.mihari,jono.vanhie,stefan.bouckaert,opher.yaron,ingrid.moerman}@intec.ugent.be
Department of Computer and Communication Engineering,
University of Thessaly, Greece
Centre for Research and Technology Hellas, CERTH, Greece
{efkerani}@uth.gr

Abstract. Recently the constant growth of the wireless communication technology has caused a huge demand for experimental facilities. Hence many research institutes setup public accessible experimental facilities, known as testbeds. Compared to the facilities developed by individual researchers, a testbed typically offers more resources, more flexibilities. However, due to the fact that equipments are located remotely and experiments involve more complex scenarios, the required complexity for analysis is also higher. A deep insight on the underlying wireless environment of the testbed becomes necessary for comprehensive analysis. In this paper, we present a framework and associated techniques for monitoring the wireless environment in an OMF enabled testbed. The framework utilizes most common resources in the testbed, such as WI-FI nodes, as well as some high-end software-defined radio platforms. Information from both physical layer and network layer are taken into account. Further more we explored the added value of distributed sensing system. The performance is mainly analyzed experimentally.

Keywords: Interference detection, testbed, spectrum sensing

1 Introduction

Over the past few years, wireless technology has evolved dramatically [1],[2]. The demand for wireless experimentation infrastructure rises accordingly. It is typically time consuming and inefficient to build experimental setups each time for individual researchers. Therefore, many research institutes adopt testbeds —

* The research leading to these results has received funding from the European Union's Seventh Framework Programme FP7 under grant agreements number 258301 (CREW project) and number 287581 (OpenLab project).

a group of fixed and public accessible infrastructures for experimentation. Such a testbed not only shortens experiment's setup time, it also offers more resources, hence enables more sophisticated experiments.

In a wired-network testbed, the link configuration between network entities is part of the resources that can be reserved by users. Compared to the wired-network testbed, the wireless medium is shared by all the facilities inside the wireless testbed, therefore also shared by different devices reserved by different users. Consequently, simultaneous network experiments performed by independent users on a wireless testbed may interfere each other. Such kind of interference cannot be solved by resource reservation as long as parallel experimentations are allowed. In addition to interference among users, nearby wireless devices, which are not part of the testbed, can also cause interference.

Repeatability and stability are prerequisites for drawing conclusions from any type of experiment. However, in the wireless environment this is usually not the case [3]. Even simple repetition can result in fairly large variations in measurements. The question is what is causing those variations? Sometimes, it is obvious that the variations are due to external interference. But for more complex scenarios, involving tuning of certain parameter sets in the experiment setup, such variations can be extremely confusing and eventually lead to wrong conclusions.

Consequently, we need a good view in the testbed to tell what is really going on in the air. Hence we propose to have a monitor running in the background to detect undesired interference. For this purpose, network layer monitoring tools as well as spectrum sensing techniques can be utilized. In this paper we focus on monitoring techniques for interference detection in WI-FI experiments. The remaining part of the paper is organized as follows: Part 2 outlines related work, including existing monitoring techniques and their usage in various testbeds; Part 3 highlights the feature offered by our framework; Part 4 gives a high-level overview of the w-iLab.t testbed and its monitoring platforms. In Part 5 we verify the performance of the tools in w-iLab.t with various interference models. Finally, we conclude this paper and describe the direction for future work in Part 6.

2 Related Work

Monitoring of the wireless environment can be achieved at different levels. At the network level, many MAC and routing protocols utilize certain types of channel assessment mechanisms. For instance, the IEEE 802.11 standard employs a rate adaptation algorithm ARF (Automatic Rate Fallback) [20] for bit rate adjustment at the physical layer. In ARF, each sender attempts to increase transmission rate after a fixed number of successful transmissions at a given rate, and falls back to a lower bit rate after 1 or 2 consecutive failures. ARF estimates the channel condition via the packet error rate feedback from receivers, more sophisticated protocols involve other statistics to achieve better estimation, [21],[8]. In General, channel assessment at network layer is limited to the links

between the relevant transmitters and receivers, thus commonly referred to as link quality estimation.

The view of channel condition at the physical layer is much broader. Physical layer monitoring tools in essence perform spectrum sensing, which can be either technology dependent (feature detection), or technology independent (general detection). A thorough list of sensing algorithms is presented in [6].

Technology dependent detection mostly requires a certain amount of a-priori knowledge of the transmitter. Some detection techniques involve decoding of the received signal. Many popular feature detection techniques exist, such as matched filtering or waveform based detection. These techniques are only able to detect specific types of traffic.

Energy detection is the most common way of technology independent detection. The major advantage is that no a-priori knowledge of the transmitter is required. There are two common approaches to implement energy detection. One is to perform Fast Fourier Transform and calculate the power spectrum density in the frequency domain; another is to derive the received signal strength directly from samples in the time domain.

In the context of a wireless testbed, there are typically many network devices which can perform some level of link estimation, however, resources capable of general energy detection are scarce.

Various channel estimation mechanisms are custom developed for individual testbeds. The solution proposed in [17] utilizes software-defined radio for channel assessment in the NITOS testbed [5]. The estimation is based on energy detection with time domain RSSI measurement. The framework proposed in [19] is used to inspect link quality between wireless testbed nodes and appropriately map them to user required network topology. The link quality estimation framework proposed in [9] predicts link quality based on packet statistics for pure sensor network environments. We focus on applying sensing and monitoring techniques systematically in a wireless testbed for detecting unwanted interference.

3 The Proposed framework

In order to obtain optimal observation of the experimental environment, we argue that the relevant channels should be monitored not only during the experiment but also before and after it. More specifically for a given experiment, the relevant channel should be monitored in three phases : before the experiment, during the experiment and also after the experiment.

- Monitoring before the experiment provides an overview of the channel condition. If interference is detected, the system will postpone the experiment until the channel is clean, or consider to switch to another channel. The purpose of this phase is to avoid invalid experiments. Since any signal present during this phase is interference, a general energy detection is sufficient.
- The monitoring system required during the experiment should be able to distinguish interference from the ongoing experiment. In this case energy

detection might be not enough. It is necessary to combine feature detection with network layer information.

- Post-experiment monitoring is similar to pre-experiment monitoring, which requires only simple energy detection. The logic here is, if there is interference detected immediately after the experiment, then most likely the interference was also present during the experiment. The experimenter should be informed that the validity of this experiment needs to be double checked.

Since pre-experiment and post-experiment monitoring only require simple energy detection, the main challenge is to derive optimal techniques to detect interference during the experiment. Our proposed solution is to construct a hybrid system, which employs general energy detection and feature detection, as well as network layer information.

In addition to the three-phase observation and hybrid detection technique, we also extend our framework with spatially distributed measurement tools. In comparison to monitoring based on a single device, a distributed system formed by multiple devices provides more insights of the wireless environment. The added value of distributed monitoring is further explored in Part 5.

4 The w-ilab.t testbed

The w-iLab.t testbed is a generic and heterogeneous wireless testbed. It consists of two sub testbeds: the w-iLab.t office and w-iLab.t Zwijnaarde. The w-iLab.t office is deployed in a real office environment while the testbed Zwijnaarde is located at a utility room. There is little external interference at the Zwijnaarde testbed as no regular human activity is present and most of its walls and ceiling are covered with metal as shown in Figure 1. The majority of devices in w-iLab.t are embedded PCs equipped with Wi-Fi interfaces and sensor nodes. Since the Zwijnaarde testbed was deployed more recently, the devices in this testbed are more powerful in terms of processing power, memory and storage. In this paper, our experiments are performed at the Zwijnaarde testbed, therefore we mainly focus on the introduction of this testbed.

There are several types of wireless devices deployed : Zigbee sensors, blue-tooth dongles, Wi-Fi based devices, sensing platforms and some software-defined radio (SDR) platforms. All devices are reachable over a wired interface for management purposes. Each device can be fully configured by the experimenters. When the wireless devices are configured via the same control interface, they are said to be attached to one “node”.

A typical node in w-iLab.t Zwijnaarde is shown in Figure 2. It consists an embedded PC with two WI-FI interfaces and one Zigbee sensor. The location of the nodes are indicated with circles in Figure 1. One of the deployed SDR platforms is the USRP N210 [4], abbreviated as USRP throughout this paper. The USRP’s are attached to powerful quad-core servers instead of embedded PC’s. There are 60 nodes installed in the Zwijnaarde testbed, among which 6 are USRP’s. The topology of the testbed is shown in Figure 3, the locations of



Fig. 1. The w-iLab.t Zwijnaarde testbed

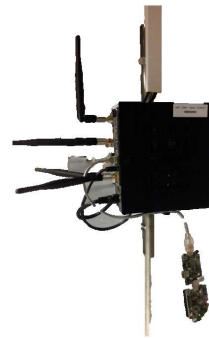


Fig. 2. The w-iLab.t node

the USRP's are marked with hexagons while regular nodes are indicated with circles.

The w-iLab.t Zwijnaarde has adopted OMF as its testbed control and management framework[14]. OMF allows experimenters to describe their experiments systematically. It provides easy data logging services and the ability to configure multiple devices.

There are two main advantages of using OMF framework in the aspect of the interference detection framework — its central control capability and data collection service. Both features are essential for monitoring based on distributed and heterogeneous devices. As an experimenter, the monitoring tools are no more than regular experimental facilities that can be configured via OMF. The data generated by the monitoring system can be logged into the database just like regular measurements as well. For an experienced OMF testbed user, the extra effort of using such a monitoring system is trivial.

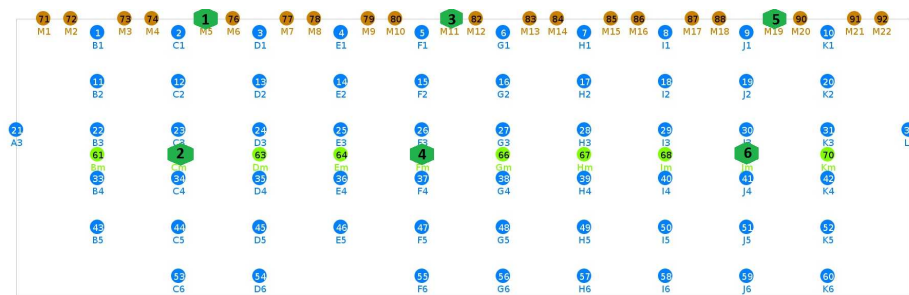


Fig. 3. The Zwijnaarde testbed topology

4.1 The Interference Detection Tools offered by w-iLab.t

WI-FI Interface in Monitor Mode As described above, a typical node in the Zwijnaarde testbed has two WI-FI interfaces. Since most experiments do not utilize the second WI-FI interface, it is possible to configure it into monitor mode on selected channel. When configured into this mode, the interface is not associated with any access point (AP). It will capture packets in promiscuous mode. Received WI-FI packets may include a Radiotap header [15], which contains the received signal strength indication (RSSI) of the incoming packet. Therefore, the physical layer information can be extracted directly from WI-FI packets, thus a regular WI-FI card combined with a simple packet sniffer software can serve as a physical layer measurement tool. This is referred as WI-FI monitor throughout this paper.

The information obtained via the WI-FI monitor contains more details on packet level, and requires less post processing effort. More importantly, there are no special requirements on either hardware or software, hence all nodes with WI-FI interfaces in the w-iLab.t can be configured as WI-FI monitors. However the monitoring functionality is restricted by the capability of the WI-FI card, no information can be provided if the interference can not be decoded. Hence in terms of detection type, WI-FI monitor belongs to the class of feature detection.

To illustrate the capability of the WI-FI monitor, one node in the Zwijnaarde testbed was configured to scan all 13 WI-FI channels in the 2.4 GHz ISM band. The result shown in Figure4 tells us there are three access points active in the neighborhood, located on channel 1, 6, and 13. The beacon from the access point with essid “robotcontrol” on channel 1 has highest RSSI, which corresponds with the fact that the “robotcontrol” AP is active at the time of the experiment. The graph also shows that the beacon sent on channel 1 can be measured even up till channel 5. The other two access points’ beacons are received with considerably weaker RSSI due to the fact that they are located outside the testbed. The WI-FI monitor can be used find out which access point is active on what channel, and how their transmit power is distributed over the neighboring channels. This observation can certainly be applied to the pre-experiment monitoring phase.

USRP Based Spectrum Sensing Engine The Universal Software Radio Peripheral (USRP) developed by Ettus Research [4], consists of two parts, a fixed mother board and a plug-in daughter board. The daughter board provides basic RF front-end functionality. In the Zwijnaarde testbed, all USRP’s are by default equipped with XCVR2450 daughter boards which covers the 2.4 and 5 GHz ISM bands and has a configurable analog front-end filter with maximum bandwidth of 30 MHz.

GNU Radio is by far the most well-known 3rd party application to work with USRP [13]. The platform selected here is Iris — a software platform developed by Trinity College Dublin [10]. It has similar component structure as GNU Radio, but is more suitable for reconfigurability on the fly. Both GNU Radio and Iris utilize UHD [12] driver and firmware to communicate with USRP and C++ to realize the underlying signal processing block. But the glue logic between signal

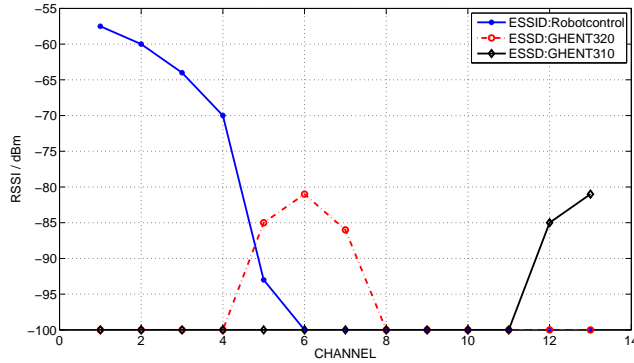


Fig. 4. RSSI Measurement of WI-FI card

processing blocks is realized differently. Compared to GNU Radio, Iris is more transparent due to its simple structure, and hence easier to get access to low level parameters on the hardware. This high transparency and reconfigurability are more desired in our context, hence we selected this platform.

We have implemented a customized solution within the Iris platform to use USRP for spectrum analysis. The spectrum analysis task is performed by several Iris components. The first component collects complex samples from the USRP device. The received samples are used to calculate power spectrum density (PSD) via the periodogram algorithm. By default, USRP's are configured to sample at 25MHz on a fixed frequency, which is wide enough to cover one WI-FI channel. It is also possible to use the USRP sensing engine in a wide-band mode. In this mode, the front end of USRP is configured to perform fast sweeping across the selected channels. The spectra obtained at multiple channels are assembled into one complete spectrum trace when the sweep is complete. The wide-band mode is suitable for obtaining an overview of multiple channels at the same time, however, the probability of interception on each channel decreases with the increase of the covered bandwidth.

There is an option to add a component for power integration over a certain band based on the PSD. Sometimes, the frequency resolution provided by power spectrum density can overskill if only the received power on the entire channel is interesting. In this case a single RSSI value can be used instead of the PSD trace. More details about the implementation of the USRP sensing engine are provided in [11]. A dedicated OMF wrapper is created for logging the spectrum information into the central database.

The USRP sensing engine belongs to the energy detection category. It is technology independent, however, it can only provide information at the physical layer.

5 Experimental Evaluation

In this section, we evaluate several experimental scenarios that aim at presenting the abilities offered by the different interference detection tools and techniques in w-iLab.t.

More specifically, each experiment is designed to demonstrate a representative interference scenario that can occur during an ongoing experiment. The considered scenarios are listed below:

- Interference may come from devices located in close proximity and operating on the same channel. The performance decrease observed in this case is caused due to the sharing of the medium among devices. This situation is referred as *Channel Contention*.
- When the testing devices are located far away, two transmitters may not be able to detect the existence of each other even when they are on the same channel. This is termed as the “hidden terminal” scenario, where the CSMA MAC protocol would fail and as a result transmitters can start transmitting simultaneously. We refer this type of interference as *Co-channel Interference*.
- IEEE 802.11 set of standards make use of the ISM (Industrial Scientific Medical) bands. The popular 2.4 GHz band, used by 802.11b and 802.11g standards, offers 11 consecutive channels, spaced 5 MHz apart and occupying 22 MHz of bandwidth. As a result, most channels partially overlap with consecutive channels, limiting the number of theoretically non-overlapping channels to three (e.g. 1, 6, 11). As a result, transmissions on a specific channel may interfere with simultaneous transmissions on overlapping channels. This is referred as *Overlapping Channels Interference*.
- Finally within a wireless testbed, interference may also come from non-IEEE802.11 compatible devices. We refer to this situation as *Interference from Heterogeneous Technology*.

In the following experiments, we consider a typical scenario of two IEEE 802.11 standard compliant nodes, operating in infrastructure mode with 802.11g standard on channel 11 (2462 MHz) and generating traffic on Uplink.

We refer to these two nodes as the System Under Test (SUT) and also consider the measured application layer UDP throughput of the SUT, as the overall performance metric.

The first three experiments consider channel contention, overlapping channels and co-channel interference respectively. Interference is generated by a collocated pair of IEEE802.11 compliant nodes under various settings. We refer to these two nodes as the interference generating group, abbreviated as INT. In the fourth experiment, we use a narrow band signal generated by a zigbee sensor node in order to examine interference generated by heterogeneous technology.

For all the aforementioned scenarios, we configure the second IEEE802.11 interface on the receiver of the SUT to monitor mode and continuously monitor RSSI of all the packets that are successfully decoded.

In each scenario we configure a different number of USRP devices to perform spectrum sensing on the operating frequency of the SUT. The PSD is recorded

with 25 MHz span on the selected channel at the speed of 10 sweeps per second. Alternatively, one single value representing the RSSI of the selected band is recorded instead of PSD trace.

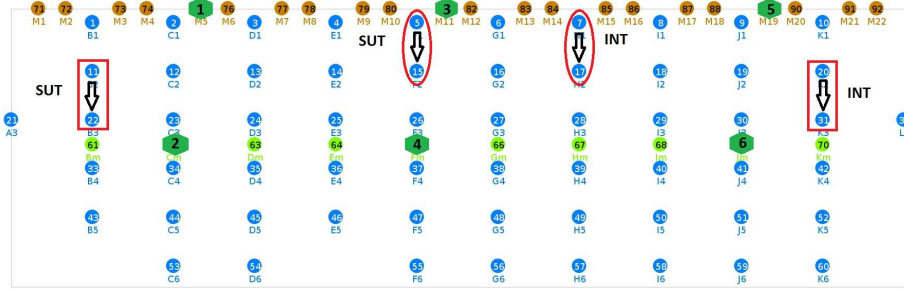


Fig. 5. Experiment topology

5.1 Channel Contention Detection

In the first experiment, we place the INT group close to the SUT and configure it to operate on the same channel as the SUT. These two pairs of nodes are indicated with ovals in Figure 5. We use Iperf to generate traffic on the application layer and set the bandwidth requirement of both the SUT and INT to 30 Mbit/s. The Iperf of the SUT group is active throughout the duration of the experiment, while the Iperf application of the INT group is activated just for a short period, in order to explore how the performance of the SUT is affected. We select 30 Mbit/s as it is slightly above the maximum bandwidth the SUT can achieve without interference, ensuring that contention will happen during the experiment.

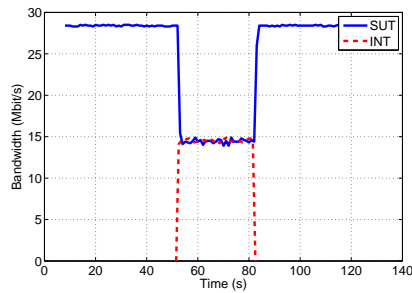


Fig. 6. Throughput performance

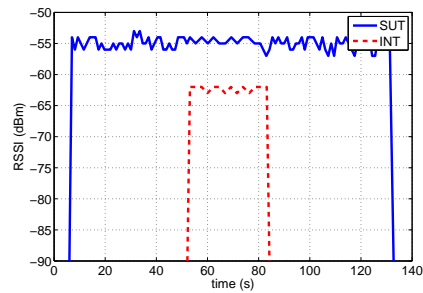


Fig. 7. RSSI trace of WI-FI monitor

The throughput performance of both the SUT and the INT groups are illustrated in Figure 6. Upon the activation of the INT group, the throughput performance of the SUT drops to 15 Mbit/s, which is half of its original throughput and equal to the throughput of the INT. This clearly shows that the available channel capacity is equally divided through the CSMA protocol between the two contending pairs of nodes.

Having examined the bandwidth performance of the SUT, the next step is to check the performance of the monitoring tools. The RSSI trace obtained from the WI-FI monitor contains records from both senders. We apply a source MAC address filter on the entire record, and separate the RSSI trace for each group, as illustrated in Figure 7. We conclude that for this scenario, a WI-FI monitor combined with MAC layer information is able to clearly identify which IEEE802.11 compatible device appeared and when exactly the contention happened.

However, the USRP device, not being aware of MAC layer information, is not able to distinguish between different Wi-Fi sources that transmit on the same channel. We notice in Figure 8 that the PSD measurements gathered from USRP4 do not provide any valuable input that can aid the identification of the different traffic sources. The only valid observation is that the channel under consideration is occupied during the entire experiment and the density of the spectrogram becomes slightly higher, while the INT group is active. However, such observations are not sufficient to detect interference activity and therefore, energy detection is not the preferred detection technique in this scenario.

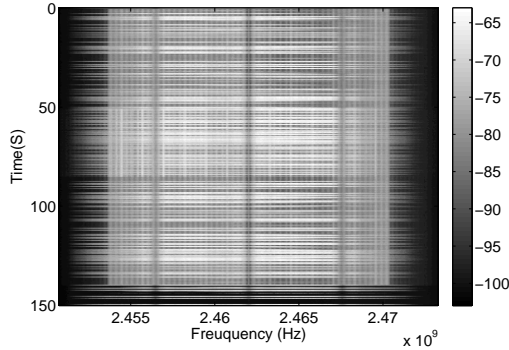


Fig. 8. Spectrogram of USRP4 on channel 11

5.2 Overlapping Channels Interference Detection

The second experiment is designed to evaluate the effect of interference generated by IEEE802.11 compliant devices operating on overlapping channels. For this purpose, we use the same network topology as in the previous experiment.

However, instead of configuring the INT group to operate on the same channel as the SUT, we now set it to transmit on the adjacent channels of the SUT group. More specifically the channel index of INT group is varied from 7 to 10 while the SUT is always operating on channel 11.

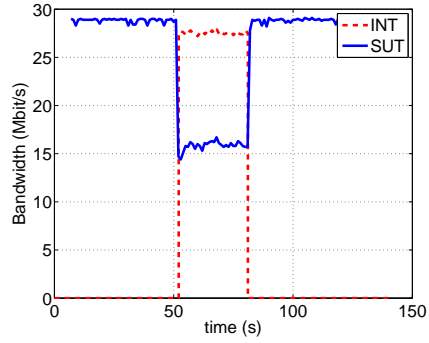


Fig. 9. BW when INT at channel 7

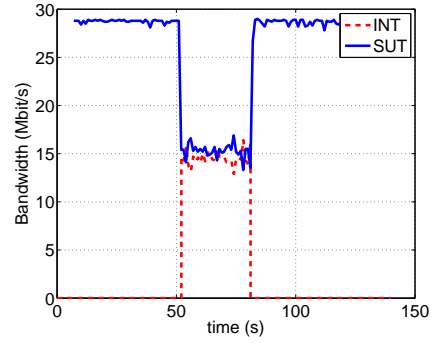


Fig. 10. BW when INT at channel 8

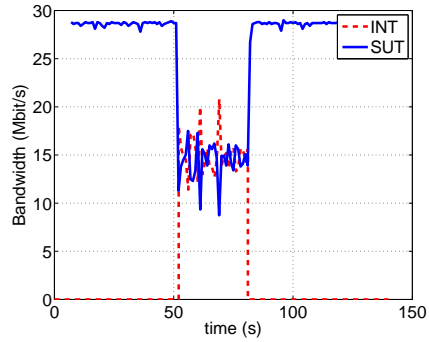


Fig. 11. BW when INT at channel 9

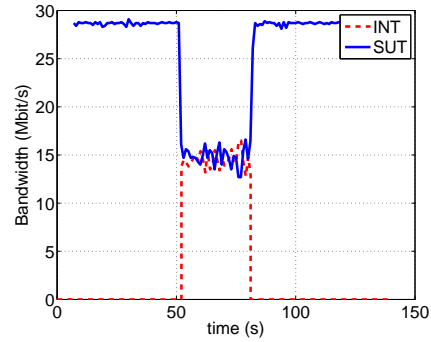


Fig. 12. BW when INT at channel 10

Figures 9, 10, 11, 12 illustrate the throughput performance when the INT group is active on Ch. 7, Ch. 8, Ch. 9, Ch. 10 respectively. We notice that the activation of the INT traffic results in significant reduction of the SUT performance, in all the cases under consideration. Among channels that are closely spaced, such as Ch. 8, Ch. 9, Ch. 10, the bandwidth performance of both groups is around 15 Mbit/s when INT is active, which is close to half of the maximum bandwidth achieved by a single pair of nodes with no interference. This is due to the contention of shared medium as in the previous experiment. Hence the per-

formance of both groups under Overlapping-Channel interference resembles the performance in Channel Contention scenario when selected operating channels are closely spaced.

This observation is clearly violated when the interference is present on Ch. 7, where an overall bandwidth of approximately 45 Mbit/s is achieved and the bandwidth of INT group is significantly higher than SUT. This comes from the fact that when the amount of channel overlapping falls below a certain threshold, the carrier sense mechanism may fail to detect ongoing transmissions and thus results in collisions. In wireless networks, a frame collision does not necessarily result in all the simultaneously transmitted frames being lost. The survival of the collision depends on the relative signal power and the arrival timing of the involved frames. This phenomenon is related to the Capture Effect [16].

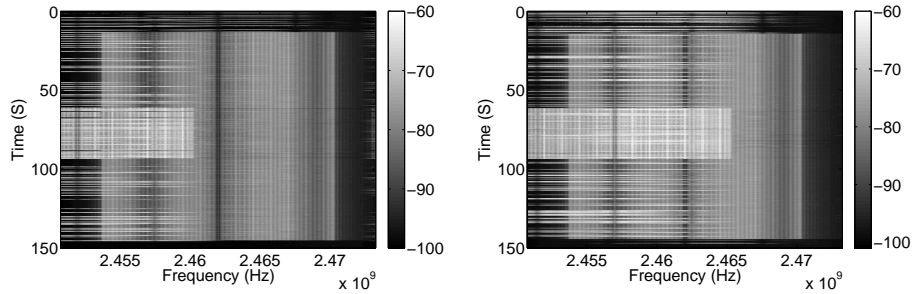


Fig. 13. Spectrogram with INT on Ch. 9 **Fig. 14.** Spectrogram with INT on Ch. 10

According to our experiments, certain topology and channel configurations lead the Capture Effect to either favor the SUT or the INT link. These observations yield interesting insights regarding the impact of the Capture Effect on interference and motivate further investigation.

Unlike the previous experiment and in contradiction to the results shown in Figure 4, the WI-FI monitor does not succeed to decode any packets transmitted on the INT link and as a result, all the recorded RSSI measurements in this case belong to the SUT transmitter. Hence, the Wi-Fi monitor fails to detect any interfering activity in this scenario. Considering the measurements plotted in Figure 4, we notice that WI-FI card is able to decode Beacon frames even when it is on channels that are not adjacent to the Beacon's sender. This can be explained by the fact that Beacon frames are transmitted at the basic rate of 1 Mbit/s, while the data from application layer is transmitted at much higher rates, typically 48 Mbit/s or above. Hence it is much easier to successfully decode Beacon frames than regular data frames.

According to the above observations, we conclude that standard compliant devices that operate in monitor mode, are not able to provide valuable monitoring information for the detection of Overlapping-Channel interference.

Fortunately, we can overcome such situations by using another “eye” in the air — the USRP sensing engine. Figure 13 and Figure 14 represent the recorded spectrogram when interference is present on Ch. 9 and Ch. 10 respectively. Based on the spectrogram, it is clear that the activity in adjacent channels is the reason for the SUT throughput reduction.

5.3 Co-channel Interference Detection

This scenario focuses on how distributed sensing can contribute to the detection of co-channel interference. As previously mentioned, co-channel interference may occur when two transmitters are located far away. In this case, the transmitters may fail to detect each other’s ongoing transmissions and thus transmit simultaneously, resulting in packet collisions. For this experiment, we setup a distributed spectrum sensing system, using the 6 USRP’s that are currently distributed over half of the testbed.

Similar to the setup used in the previous scenario, the experiment here also involves two pairs of IEEE802.11 compliant nodes, however instead of choosing two groups next to each other, the groups are now located at different sides of the testbed. The selected nodes for this experiment are marked with rectangles in Figure 5, while the USRP sensing engines are indicated with hexagons, labeled from 1 to 6.

We configured the SUT group on the left side of the testbed to generate continuous traffic at 20 dBm. The INT group on the right side of the testbed follows an ON-OFF traffic pattern, so that each time the client starts a data stream for 15 seconds, OMF will wait for another 15 seconds before the client is turned on again. The transmit power of the INT group is reduced from 20 dBm to 0 dBm in the step of 2 dBm. Both the INT and SUT are operating on the same channel.

The ON-OFF traffic pattern of the INT group makes it possible to distinguish between signals that are generated by the SUT and the INT groups, solely based on RSSI measurements. Ideally the duty cycle should be 50%, in reality it is also influenced by the control lag introduced within OMF.

Unfortunately USRP 1 was not available during the conduction of this experiment, we hence only configured the remaining 5 USRP’s to collect spectrum data. Each USRP sensing engine produces an RSSI value every two seconds over the selected WI-FI channel.

The average bandwidth performance when INT is active is plotted against the transmit power of the INT group (Figure 15). The graph shows a clear trend that the impact of INT on the performance of SUT increases with its transmit power. Once the transmit power rises above 6 dBm, the INT group’s impact on the SUT becomes visible.

When examining the RSSI records from the WI-FI monitor, the RSSI from the SUT sender is more or less constant, since there is no variation of transmit power at the SUT group. The RSSI recorded from the INT group is also very stable within each experiment. Therefore, the actual value of the RSSI is no longer important, what matters is the length of the packet trace from each

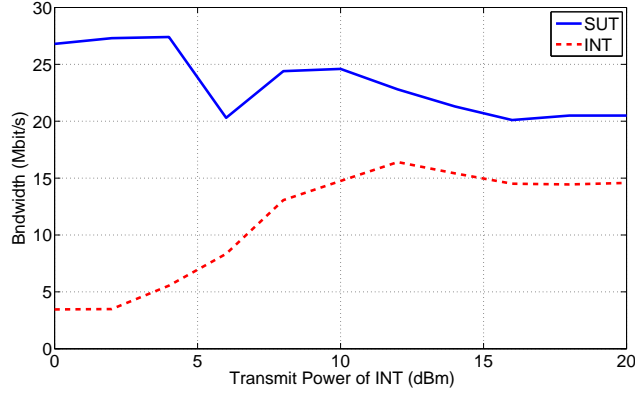


Fig. 15. Bandwidth performance of SUT and INT with various INT transmit power

sender, since this is the number of packet that can be detected by the WI-FI monitor. Based on this idea, Figure 16 and Figure 17 are generated. The first remark is that the number of detection of SUT is significantly higher than INT. More over, when the transmit power of INT is below 14 dBm, there is no detection of INT based on the packet trace at all. When the INT transmit power lies between the interval of 6 dBm and 14 dBm, we do observe the reduction of SUT throughput performance, however, the WI-FI monitor at SUT side does not detect any interference. In this situation, the INT transmitter becomes a “hidden terminal” for the WI-FI monitor and the SUT transmitter

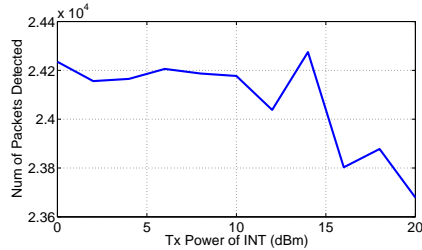


Fig. 16. WI-FI detection of SUT

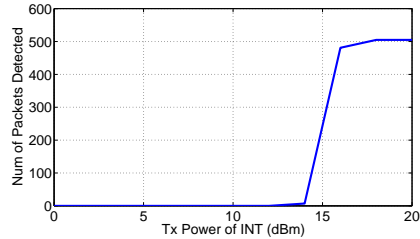


Fig. 17. WI-FI detection of INT

When the WI-FI detector is incapable of interference detection, how is the performance of USRP sensing engines? We select the RSSI traces of USRP sensing engine when INT transmit power is at 0 dBm, 6 dBm, 14 dBm and 20 dBm to present (Figure 18). At the first glance, USRP 5 and 6 are able to follow the ON-OFF traffic pattern produced by the INT group, while the rest of USRP’s are dominated by the SUT group’s transmission, since their measurements appear

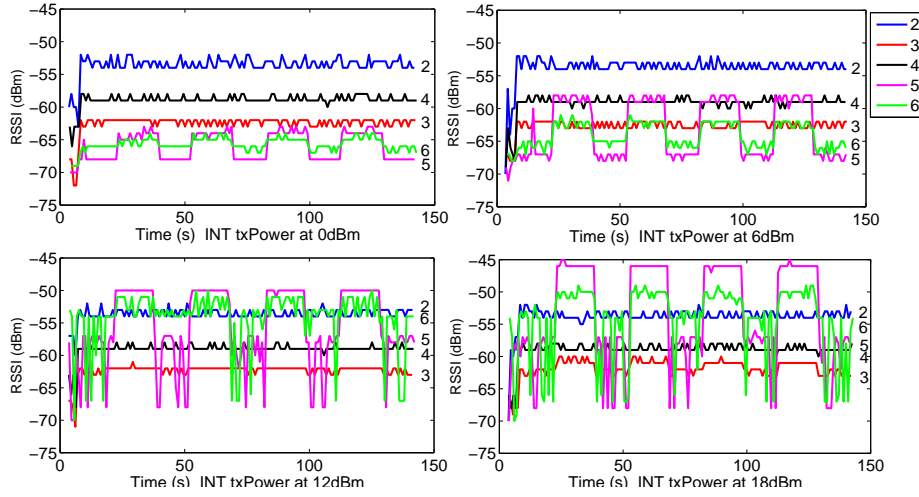


Fig. 18. PSD trace when the transmit power of INT group is at 0 dBm, 6 dBm, 12 dBm, 18 dBm

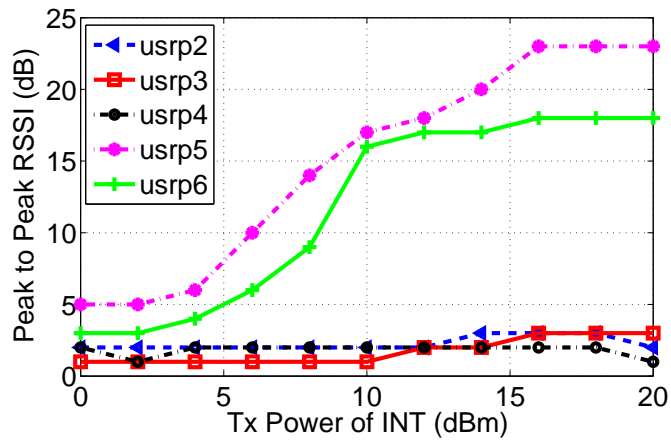


Fig. 19. The peak-to-peak RSSI vs Transmit power of INT group

to be stable. This observation is confirmed by Figure 19, where the peak-to-peak value of RSSI in each trace for each USRP is plotted against the INT's transmit power. We clearly see that USRP 5 and 6's peak-to-peak RSSI values increasing with the transmit power of INT group, while the rest USRP's are almost unaffected. Hence, as a single device, USRP located far away from the INT group also fails to detect the interference. We do see that WI-FI monitor can detect the interference when its transmit power is above 14 dBm. Therefore, when using a single device as a monitoring tool, feature detection is more sensitive than energy detection. However, when combining the view of all the USRP's, we are able to identify the interference with energy detection even when the transmit power of the INT group is at 0 dBm. In this case, the advantage of distributed detection over localized detection is evident.

5.4 Heterogeneous Technology Interference Detection

In the last experiment, we focus on the detection of the interference caused by heterogeneous technology. Hence we do not use IEEE802.11 devices to produce interference but use a narrow band signal generated by a zigbee sensor node. The interfering signal is centered at 2.465 Ghz. This jamming signal is a simplified representation for interference generated by none IEEE802.11 compliant devices.

Based on bandwidth measurements, we observe that due to the activation of the narrow-band jammer, the performance of the SUT almost drops to zero, as indicated in Figure 20. The RSSI trace recorded by WI-FI monitor, illustrated in Figure 21, does not provide any valuable information except that the RSSI record becomes less dense when interference is present.

In the spectrogram obtained via the USRP sensing engine (Figure 22), the presence of the narrow band jammer becomes evident. Upon the activation of the jammer, the SUT's activity is greatly reduced. Based on this fact, we conclude that the IEEE802.11 transmitter is able to detect ongoing transmissions of the jammer through the Carrier Sense mechanism.

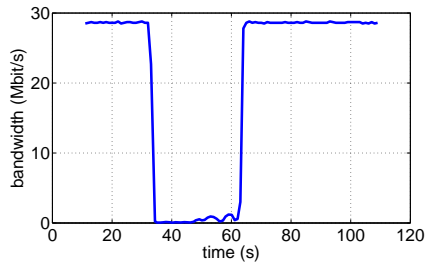


Fig. 20. Throughput performance

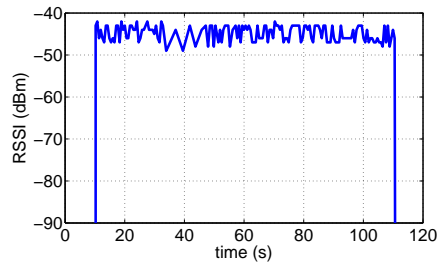


Fig. 21. RSSI trace of WI-FI Monitor

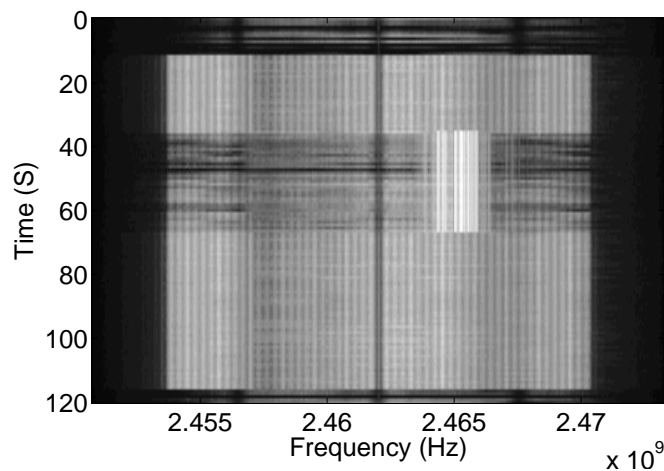


Fig. 22. Spectrogram from USRP

6 Conclusion and Future Work

In this paper, we prove that wireless experiments are very susceptible to unpredictable interference, a monitoring system is hence necessary for validating experiments. Two types of measurement tools are offered by the w-iLab.t testbed: the standard WI-FI card, and the custom-designed sensing engine based on the software-defined radio platform (USRP). A distributed detection system can be easily formed via the OMF control framework.

We considered several common interference scenarios for WI-FI experiments inside the wireless testbed, including the interference caused by WI-FI device on the same channel, the interference caused by WI-FI device from overlapping channel and finally interference caused by none WI-FI technology. For each scenario, the performance of available measurement tools are examined. Within the co-channel WI-FI interference scenario, we are able to demonstrate the advantage of distributed detection over localized detection when the interfering transmitter is located far away.

In the future, the aforementioned interference detection techniques will be integrated into a benchmarking framework, in which the experiment cycle will be fully automated, offering services such as scheduling an experiment with specific parameter sets, and evaluating the gathered results. The validity of experiments will be evaluated based on the input from the interference detection framework proposed in this paper.

References

1. IEEE802.11 standards revised due to fast WI-FI growth, <http://www.telecoms.com/43908/802-11-standards-revised-due-to-growth-of-wifi/>

2. IEEE standards, <http://standards.ieee.org/findstds/standard/>
3. R. Burchfield et al.: "RF in the Jungle: Effect of Environment Assumptions on Wireless Experiment Repeatability" in Communications, 2009. ICC '09. IEEE International Conference on Digital Object Identifier:10.1109/ICC.2009.5199421, pp. 1-6 2009
4. Ettus Research, <http://www.ettus.com/>
5. NITOS wireless testbed, <http://nitlab.inf.uth.gr/NITlab/index.php/testbed>
6. Y. Tevfik, A. Huseyin, "A survey of spectrum sensing algorithms for cognitive radio applications", in *IEEE comm.Survey and Tutorial*, vol. 11, no. 1, pp. 116-130, 2009
7. S. Bouckaert et al. "Federating wired and wireless test facilities through Emulab and OMF: the iLab.t use case" in the proceedings of TridentCom 2012
8. N. Baccour, A. Koubaa, H. Youssef, M. Ben Jamaa, D. do Rosario, , M. Alves, and L. B.Becker: "F-Iqe: A fuzzy link quality estimator for wireless sensor networks" in 7th European Coriference on Wireless Sensor Networks(EWSN 2010), ser. LNCS 5970. Coimbra, Portugal: Springer, February 2010, p. 240255
9. Nouha Baccour et al.: "A testbed for the evaluation of link quality estimators in wireless sensor networks" in Computer Systems and Applications (AICCSA), IEEE/ACS International Conference 2010
10. P. Sutton et al.: "Iris: an architecture for cognitive radio networking testbeds," in *IEEE comm. Mag.*, vol. 48, no.9, pp. 114-122, 2010
11. W. Liu et al.: "Real-time wide-band spectrum sensing for cognitive radio" In Communications and Vehicular Technology in the Benelux (SCVT), 2011 18th IEEE Symposium
12. Universal Hardware Driver(UHD), <http://code.ettus.com/redmine/ettus/projects/uhd/wiki>
13. GNU Radio wiki, <http://gnuradio.org/redmine/projects/gnuradio/wiki>
14. Rakotoarivelo, T. and Ott, M. and Jourjon, G. and Seskar, I.:OMF: A Control and Management Framework for Networking Testbeds. In: SIGOPS Oper. Syst. Rev. pp. 54-59 vol.43 (2010)
15. Radiotap <http://www.radiotap.org/>
16. Jeongkeun Lee et al: "An experimental study on the capture effect in 802.11a networks" in Proceedings of the second ACM international workshop on Wireless network testbeds, experimental evaluation and characterization, pp. 19-26
17. V. Passas, S. Keranidis, T. Korakis, I. Koutsopoulos and L. Tassiulas: "An Experimental Framework for Channel Sensing through USRP/GNU Radios", in Trident-Com 2012
18. Nikoli D, Muresan RC, et al.: "Scaled correlation analysis: a better way to compute a cross-correlogram". *European Journal of Neuroscience*, pp. 121, 2012
19. D. Syrivelis, A. C. Anadiotis, A. Apostolaras, T. Korakis, L. Tassiulas: "TLQAP : A Topology and Link Quality Assessment Protocol For Efcient Node Allocation on Wireless Testbeds", in the proceedings of WiNTECH 2009, Beijing, China, September 2009.
20. A. Kameron and L. Monteban. WaveLAN-II: "A High-performance wireless LAN for the unlicensed band". *Bell Lab Technical Journal*, pages 118133, Summer 1997
21. M. Lamage et al. "IEEE 802.11 rate adaptation: a practical approach " in Proceeding MSWiM '04 Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems, pp 126-134