Wireless Guard for Trustworthy Spectrum Management

Mukaram Shahid, Sarath Babu, Hongwei Zhang, Daji Qiao, Yong Guan,
Joshua Ofori Boateng, Taimoor Ul Islam, Guoying Zu, Ahmed Kamal, Mai Zheng
Department of Electrical and Computer Engineering, Iowa State University
Ames, Iowa, USA
{mukaram,sarath4,hongwei,daji,guan,jboateng,tislam,gyzu,kamal,mai}@iastate.edu

ABSTRACT

ARA is a first-of-its-kind wireless living lab for advanced wireless in rural regions. In ARA, users can reserve programmable wireless resources, for instance, Software Defined Radios (SDRs), and wireless spectrum to perform a wide range of of experiments. Given ARA-enabled open access to programmable wireless resources , it is important to enforce proper usage of the available spectrum, thereby ensuring no user (benign or malicious) creates any harmful interference to other experimenters or any incumbent. Therefore, we develop Wireless Guard (WG), a mechanism for wireless spectrum usage monitoring. For WG, we use two approaches for enforcing the spectrum policy: (*i*) reactive approach and (*ii*) proactive approach. In this paper, we present the hardware and software architectures of the ARA WG along with the end-to-end pipeline for managing experiments in case of deviation from the spectrum usage policy. Initial evaluations show the effectiveness of WG in enforcing spectrum usage policies in ARA.

CCS CONCEPTS

• **Network Experimentation**; • **5G Networks**; • **Dynamic Spectrum Sharing**;

KEYWORDS

ARA, Wireless Guard, Spectrum Use Policy Enforcement, Spectrum Sensing

1 INTRODUCTION

Rural broadband is essential to societal progress in developed, developing, and least-developed countries worldwide. In the USA alone, around 46 million people live in rural areas that are deprived of sufficient Internet/broadband access [5, 7]. To unleash the entrepreneurial potential of the rural communities and to improve the prosperity of the people, it is essential to provide broadband Internet access and making them connected to the rest of the world. Applications such as plant phenotyping, smart agriculture, rural education, and augmented/virtual reality-based applications require wireless communications with different throughput and latency requirements. There exists no single architecture which meets such a diverse set of requirements. Moreover, the wireless channel characteristics and spatial distribution densities of households and enterprises in rural environments are very different from those of suburban or urban environments [9, 14]. Therefore, ARA [14] wireless living lab focuses on rural settings and is being deployed in Central Iowa, USA. The living lab is expected to cover ∼250 square miles area across Iowa State University, the City of Ames, and surrounding agriculture farms and rural communities, with 12 Base-Station (BS) sites and more than 100 mobile and stationary User Equipment (UE) sites deployed.

The ARA wireless living lab consists of Radio Access Networks (RAN) employing technologies ranging from NI (National Instruments) SDR (Software Defined Radios), Skylark commercial massive MIMO (mMIMO) platforms, to Ericsson mMIMO and millimeter wave (mmWave) Stand-Alone solutions. In addition, ARA employs Microwave, mmWave, and Free Space Optical (FSO) links for backhaul connectivity [14]. The devices that employ such technologies operate at different frequencies, for instance, with the radio access networks operating from 460–776 MHz in TV Whitespace (TVWS), 3.4–3.6 GHz in mid-Band, to the 26–28 GHz 5G FR2 band, and with the long-distance, high-capacity wireless mesh backhaul using 11 GHz point-to-point Micro-Wave links, 71–76 GHz and 80–86GHz mmWave links, and 194 THz FSO links. With the use of diverse wireless technologies and frequency bands, ARA is envisioned to provide an innovative research platform for various measurement and network design studies.

With the use of diverse wireless devices, it is important to ensure isolation between users in terms of the spectrum usage, i.e., the experiments of one user should not create any harmful interference to other ARA user experiments nor to the users of existing service providers or networks of Department of Defense (DoD) and other incumbents. In scenarios where devices and applications become spectrum and bandwidth-hungry, we need to monitor the spectrum and enforce spectrum policies to protect incumbents from harmful interference beside utilizing this scarce natural resource in optimal ways [10, 13, 15]. Therefore, we design a mechanism called *Wireless Guard (WG)* to continuously monitor the spectrum used by the experimenters and enforce the spectrum policies so that no user causes any intentional or unintentional interference to other users. The WG also monitors the transmission power users are operating at, to ensure compliance with the regulations of Federal Communications Commission (FCC). To enable other spectrum management functions, the WG also provides an open API for collecting information about the RF spectrum usage at the individual ARA sites.

The rest of the paper is organized as follows. Section 2 presents the related work, and Section 3 describes the WG system design including its hardware and software architectures. In Section 4,

WiNTECH '22, October 17, 2022, Sydney, NSW, Australia

ACM ISBN 978-1-4503-9527-4/22/10…$15.00
https://doi.org/10.1145/3556564.3558241

we discuss the spectrum enforcement and interference mitigation techniques used in WG. The evaluation results are provided in Section 5. Finally, we make concluding remarks in Section 6.

2 RELATED WORK

One primary objective of spectrum policy enforcement systems in a resource-shared environment is to ensure that the resources are efficiently utilized. Radio frequency spectrum is considered to be a scarce resource that needs efficient and mutual planning among different entities under the roof of a central regulatory body. Significant efforts have been made among research communities and industry in developing spectrum allocation and policy enforcement solutions. In [8], Park et al. discussed the security and spectrum enforcement techniques, and how ex-ante and ex-post techniques are required for spectrum sharing models when multiple stakeholders share the same resource. On the other hand, an interference detection and mitigation technique was proposed in [2] where the Primary User (PU) employed forced-silence to identify the set of cognitive radios that cause interference to the PU.

Weiss et al. [12] provided the use-case of spectrum enforcement techniques with a case-study of Dynamic Spectrum Sharing (DSS) between LTE users and the incumbents in the 1696–1710 MHz band. Further, they discussed the systems and opportunity costs for different ex-ante, ex-post, and protection zone schema that can be utilized to enforce the spectrum policy. Similarly, Galott et al. [4] shared the policy enforcement strategy based on misbehavior detection, penalty function, and resource allocation.

The detection of malicious user behavior forms the primary essence of the spectrum enforcement policy. Spectrum sensing can be used to detect potential policy violations. In wireless testbeds such as ARA, there exists a need to efficiently monitor the spectrum in a timely fashion, mitigate the impact of malicious users, and stop their operations at the earliest so that no incumbent faces any harmful interference caused by the testbed users. In this context, Terry et al. [11] described spectrum sensing and source separation techniques where the prototype employs a bi-directional coupler in the RF chain right before the antenna. A source separation algorithm separates the signal source, i.e., the signal from the Power Amplifier (PA), and the RF signal from the antenna. One of the challenges in such an implementation is the complexity and accuracy of source separation algorithms so that the exact operations of the SDR users are identified correctly and the number of false alarms is minimized.

In [3], Dutta et al. devised a crowd-source spectrum sensing and enforcement technique where multiple mobile nodes are utilized as eye witnesses of policy breach for spectrum usage in dynamic spectrum access. A data fusion algorithm was proposed to leverage the outcome from different nodes to reduce the error probability.

Kumar et al. [6] proposed transmitter identification mechanisms based on waveform authentication where the enforcement entity blindly identifies the misbehaving users based on the authentication signals. The framework uses crowd-sourcing blind authentication techniques for transmitter authentication under low SNR conditions as well as in scenarios where multiple transmitters operate in the same frequency band. In [16], Zubow et al. discussed the development of a deep-learning based module DeepTxFinder that uses multiple RF sensors to monitor and localize multiple transmitters with different environmental uncertainties such as unknown SNR, number of transmitters, the transmission power, and channel conditions.

In view of the aforementioned challenges of user identification and spectrum policy enforcement in ARA, we design and develop a novel spectrum policy enforcement and interference mitigation technique that utilizes multi-fold mechanisms to detect and localize the misbehaving users and stop their operations. More importantly, Wireless Guard is a real-world implementation in the ARA platform to provide trustworthy spectrum management. Apart from protecting the incumbents from harmful interference caused by ARA Users, WG also provides the means to monitor the near real-time spectrum utilization at all ARA Base-Station sites.

3 SYSTEM DESIGN

In the overall ARA architecture, the radio access network, i.e., AraRAN [14], plays a very significant role. AraRAN comprises NI SDRs and COTS (commercial off-the-shelf) radios deployed at each base-station site with an operational frequency in the 3.4–3.6 GHz band. One of the main goals of building the ARA platform is to give experimenters this access to run their experiments and test 5G algorithms in a real-world rural environment.

Given the above use-case, the ARA experimenters have access to the SDRs using the SDR-Host computer so that users can run a kind of application within the spectrum that ARA is allowed to operate in. To ensure the ARA platform's smooth operations, we need to ensure that no ARA user is causing any harmful interference. Nevertheless, achieving this goal is challenging since manipulating the SDRs' transmission behavior is much easier compared to the legacy COTS radios. To enforce the spectrum use policy and monitor user behavior, ARA needs a mechanism to monitor the selected frequencies on all the SDRs. Unlike conventional spectrum monitoring where the objective is to identify spectrum availability at certain locations, here we need a one-to-one mapping between each user experiment and the frequencies and the SDR it is operating at to enforce the spectrum policies. This objective cannot be achieved by simply sensing the RF environment. Instead, it requires a more sophisticated mechanism that can monitor each RF chain without causing any hurdles to the normal transmission operations of the users.

Given the above scenario that requires a spectrum policy enforcement infrastructure for the ARA platform, we have devised a spectrum sensing and policy enforcement module named *Wireless Guard (WG)*. Wireless guard has four different modes of operations as follows that provide multiple folds of security for spectrum enforcement:

- Proactive Approach
- Reactive Approach based on COTS RF Sensor
- Reactive Approach based on B205 mini-i Monitor SDR
- Over the Air Spectrum Sensing and Monitoring

Based on the mode of access, i.e., bare metal or container, of the specific computer to which SDRs are attached to, the wireless guard ensures that no experiment uses an illegitimate frequency band or transmission power level which is harmful to other user experiments or incumbents. The proactive approach of WG is a

software-based solution to monitor the configuration parameters of the radios to ensure the users select the valid set of parameters. On the other hand, the reactive approach uses spectrum sensing to monitor the frequencies being transmitted from a specific SDR so that the spectrum policy can be enforced and necessary steps can be taken to prevent users from creating interference. Based on the method of implementation, the pros and cons of the proactive and reactive approaches are summarized in Table 1.

Table 1: Pros and Cons for Different Policy Enforcement Approaches

	Proactive	Reactive
Container support	Yes	Yes
Bare-metal support	No	Yes
Dedicated hardware required	No	Yes
Computational overhead	Low	High
Use in dynamic spectrum sharing	No	Yes

3.1 ARA Resource Reservation

The software architecture of ARA platform is designed in a way that users can reserve containers or bare metal computers deployed at the ARA sites. The block diagram representing the overall resource reservation through the ARA controller is shown in Figure 1.

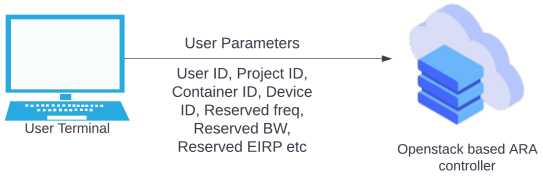

Figure 1: Resource Reservation in ARA

As shown in the figure, users can access the ARA controller (more specifically, its web portal) and create an experiment profile that will be associated with a specific project and experimenter ID. The user can then move forward to reserve the ARA resources (e.g., computers, SDRs, and spectrum) through the ARA controller portal and specify the reservation of the specific resources. The resources that users need to identify include the node location, resource type, reserved frequency, reserved bandwidth, and reserved maximum transmission power (i.e., EIRP). The ARA controller receives this information and schedules the experiment for the specific location according to a scheduled time frame.

3.2 Software Architecture for Wireless Guard

The wireless guard module has been designed as a distributed application running at the Management Computer of each Base Station (BS) and User Equipment (UE) site. All these management computers are connected, and the ARA controller uses an extensive fiber network and wireless backhaul/access network to orchestrate

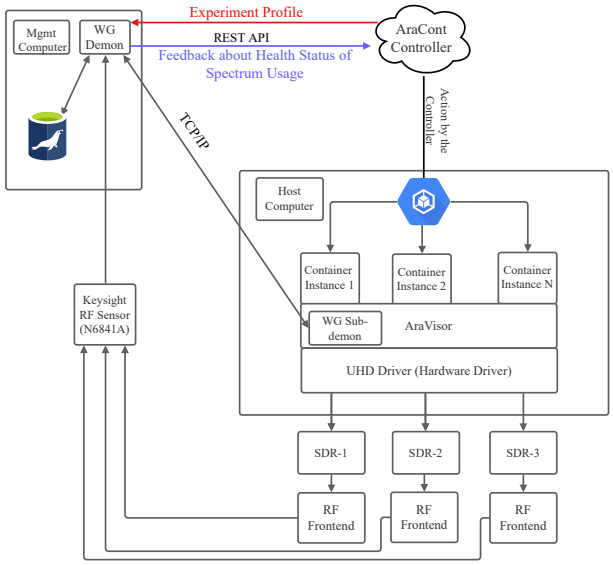

Figure 2: Software Architecture of Wireless Guard at BS Site

their operations. The overall software architecture of the Wireless Guard module at BS site is shown in Figure 2.

As soon as an experiment profile is created on the ARA Portal, the controller pushes the experiment profile to the Wireless Guard Daemon running on the management computer of that specific site. Once the profile is received, the WG daemon saves that information in the local MariaDB database tables (i.e., experimenter_profile, resource_reservation, and resource_type).

Once the profile has been registered at the WG daemon, it starts communicating and taking feedback from the WG sub-daemon running at the SDR-Host Computer. The WG sub-daemon is a module that helps enable the proactive approach and monitors the user frequency by intercepting the frequency commands selected by the user. More details about the proactive approach will be presented in Section 4.1. The WG daemon also takes the input from the spectrum monitoring hardware, and it saves the feedback from the WG sub-daemon and RF spectrum sensing hardware to a user-behavior table. After collecting the data, the WG Daemon compares the observed user behavior and what has been specified in the experiment profiles to identify the users who are misbehaving, and, based on the overall behavior score, a feedback is sent to the ARA Controller to stop the operations of the misbehaving users.

3.3 Hardware Architecture for BS Node

The hardware for the spectrum monitoring on each base-station node is being integrated with the RF Front-end. As shown in Figure 3, the Downlink and Uplink channels of the N320 BS SDR ports are coupled using a 10 dB coupler. For the prototyping of Wireless Guard, the directional couplers have been procured from Keysight with the model number 87300 B. The coupler has the directivity of 10 dB with an insertion loss less than 1.9 dB. The Directional Coupler (DC) is being used to divide the transmitted signal from the SDR into a proportion of 90:10, where 90% of the power is being

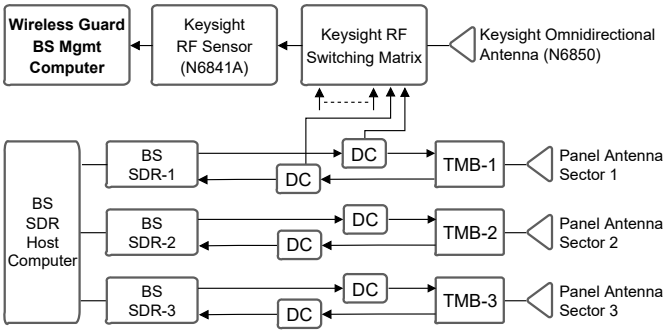

Figure 3: Wireless Guard Hardware Architecture for BS Node

transmitted to the Tower Mounted Boosters or TMBs, which amplifies the signal to get it transmitted over the air. The remaining 10 percent SDR power is coupled to the Keysight RF Switching Matrix. A 10 dB DC was chosen because of the easy off-the-shelf availability and reliable signal sampling for spectrum sensing and signal decoding, and to ensure that the RF operations are not disturbed. Using the network analyzer, we observe that the introduction of DC causes an attenuation of 1.45 dB at 3.5 GHz in the main RF chain. The RF design of ARA is in such a way that even with the DC-induced power loss in the RF chain, the maximum feasible transmission signal power at the panel antennas remains higher than the maximum transmission power allowed by the FCC regulations. Therefore, the introduction of DC does not reduce the coverage area of ARA RANs. As seen in the Figure 4, the introduction of DC in the transmission does not cause any distortion in the transmitted signal, however, results in an attenuation of 1 dB in the overall transmitted signal.

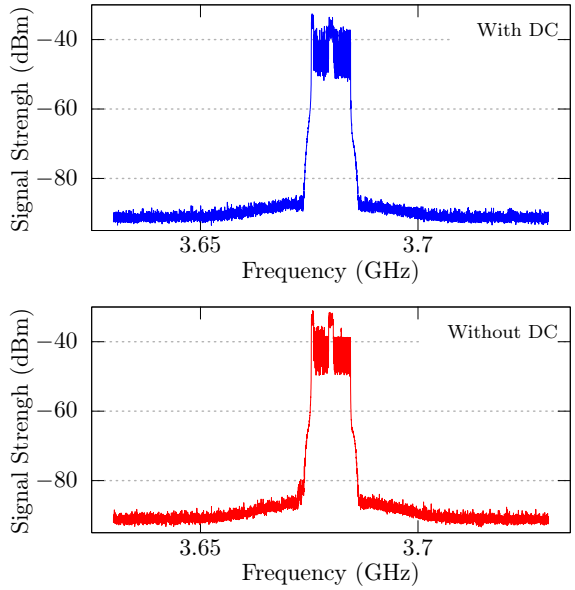

Figure 4: Wide-band Spectrum Detection using NI SDR

The output of the RF Switching Matrix is being fed to the Keysight RF Sensor (N6841A) for spectrum monitoring purposes. In Figure 4, the overall attenuation in the main RF chain due to the coupled signal is close to 1 dB at the frequency of 3.5 GHz. In addition, the copy of signal received at the RF sensor is around 11 dB lower than the main transmission line. Such a very low attenuation introduced by the couplers does not disrupt the RF operations of our users. The RF sensor can operate at a frequency range of 20 MHz to 6 GHz and can be configured to monitor the higher spectrum bands using an up-down converter. The sensor has multiple trigger methods, including frequency, amplitude, time, and spectral shape-based triggers. The sensor can be configured to various resolution bandwidths starting from 5 Hz to up to 1.67 MHz. Further, the RF sensor can monitor the spectrum from 20 Mhz to 6 GHz, with the minimum display average noise level at -140 dBm at 10 Hz of the resolution bandwidth.

The omnidirectional antenna (N6850) is a wide band antenna with an isotropic gain of 0 dBi and is being used to monitor the overall spectrum used at a given time slot. The operational frequency of the antenna varies from 20 MHz to 6 GHz and can be used to monitor the signals as well as geolocate the transmitter operating at a particular frequency. The RF Sensor is further configured with different Keysight Software modules named the Surveyor 4D that allows us to capture the signals based on the alarms that can be set based on the signal under consideration and are predefined in the software. The software module helps to save all the signal parameters and signal logs in an SQL-based database that the WG daemon can use to take continuous feedback and monitor multiple RF Chains one at a time.

3.4 Hardware Architecture for UE Node

Like the base-station node, the UE also has the Wireless Guard spectrum monitoring hardware for accomplishing the reactive approach. The hardware architecture for the UE nodes is slightly different from the BS nodes, and it is shown in Figure 5.

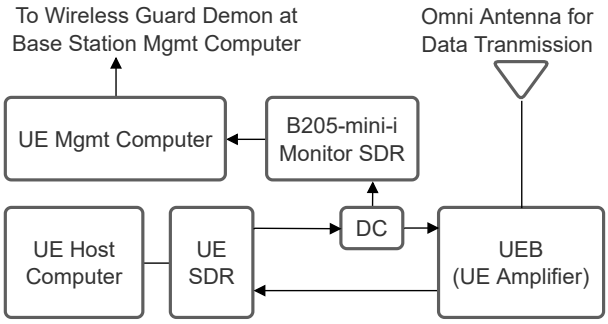

Figure 5: Wireless Guard Hardware Architecture for UE Node

A 10 dB direction coupler is used to monitor the user signals and spectrum compliance. The coupled port is fed into the Ettus Research B205mini-i SDR for spectrum monitoring purposes. The B205mini-i is responsible for the IQ sample collection and spectrum stitching over the complete span at which we want to monitor the signals. The next sections will share details about the software architecture for spectrum monitoring and stitching.

4 SPECTRUM ENFORCEMENT TECHNIQUES

In what follows, we propose different spectrum enforcement techniques for the wireless guard (WG) to ensure that users do not create interference (malicious or unintentional) between each other or with users of any incumbent service provider.

4.1 Proactive Approach

The proactive approach employed in WG is a software-based monitoring scheme for spectrum usage to track the user behavior. At each BS location, three NI N320 SDRs are made available for ARA users for their experiments where each SDR covers 120 degrees azimuth of a single sector. The USRP devices are managed by Universal Hardware Driver (UHD), a software component written in C and C++. Besides carrying the baseband data packets from user applications to the SDR's FPGA for transmitting them over the air, UHD manages the hardware parameters of SDR as per the user requirements.

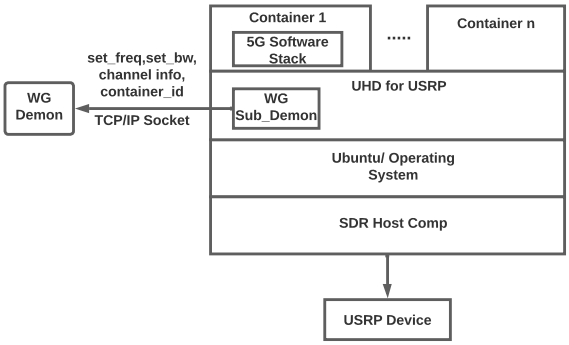

Figure 6: Architecture for Proactive Approach

Once the experiment profile is created and scheduled for execution, the information is sent to the WG daemon running at the management computer residing at the resource site. In proactive approach, we leverage UHD to monitor the parameters that are sent by the users to configure on the USRP's FPGA. The WG sub-daemon receives a feedback when a user tries to set a new operational parameter. The configuration parameters along with the container identifier are sent to the WG daemon of the management computer. The WG daemon saves the operational parameters provided by the user in the user behavior table of the database. Further, the WG daemon compares the received hardware parameters with the experiment profile. The experiment continues in cases where the users are well-behaving and the parameters provided by the users are consistent with the corresponding experiment profile. In case of a mismatch between the user behavior and the experiment profile (e.g., user setting a transmission frequency outside the reserved bandwidth), the WG daemon reports the event to the controller, and the controller stops the experiment; in this case, the USRP device gets detached from the experiment, thereby preventing potential interference to other users. Since the USRP devices can only be configured using UHD, the proactive approach can be generalized for the use by other testbeds that are using the USRP devices as well as law enforcing agencies to ensure the appropriate usage of the spectrum. The feasibility of realizing proactive approach using FPGA can be considered as a future work.

4.2 Reactive Approach Using COTS RF Sensor

Based on the different application requirements, the users might need to access the platform under different types of leases (e.g., bare-metal or containerized applications) to perform the experiments. Unlike a containerized application, in the case of bare-metal access, the WG daemon do not have any access to the WG agents residing in the SDR-Host computer, so to enforce the spectrum policy in the case of Bare-Metal access, a reactive approach is proposed so that we ensure that spectrum is utilized most efficiently without causing interference to other users or primary users of a certain band.

As shown in Figure 3, the RF chains of base-station SDRs are connected to the switching matrix that enables the RF sensor to monitor multiple RF chains, one at a time. The switching matrix is customized depending on the needs of each site and the matrix incorporates directional couplers, RF switches, and a 10 dBm limiter to protect SDRs and RF sensor from any RF surge from multiple sources, lightening, DC transients, and electro-static discharge. Figure 7 shows the switching matrix module built for one of the ARA sites.

Figure 7: RF Switching Matrix

The output of the switching matrix is passed to one of the ports of the RF sensor. Using the Keysight APIs and custom scripts, we select one of the RF chains at random and monitor the signals transmitted by the user. The sweep time for the RF sensor as well as the time to record the data in the database are in the order of a few milliseconds based on the Resolution Bandwidth (RBW) and frequency span we monitor. Once the RF chain has been selected, the RF sensor sweeps through the signals of the corresponding RF chain, and the operational parameters of the users operating on that RF chain, e.g., the Center Frequency, Occupied BW, Modulation Schemes, are stored in the database from where the WG daemon accesses these operational parameters to make a comparison with the reserved spectrum resources. The selection of the RF chain is done randomly with the help of the Keysight RF Switching Matrix.

4.3 Reactive Approach Using B205mini-i SDR

The high cost and bulkiness of RF sensors are two challenges in realizing the reactive approach at the user equipment (UE) side. Therefore, we use NI B205mini-i SDRs for spectrum monitoring

at UEs. The real-time bandwidth for B205-mini is 56 MHz and the operational frequency ranges from 70 MHz to 6 GHz. To realize spectrum monitoring using B205mini-i, we use energy-based spectrum detection algorithms that take the FFT (Fast Fourier Transform) of the input signal, calculate the energy, and compare the energy with a set of thresholds to determine the user's operations at a particular frequency and bandwidth. The system model for the energy-based spectrum sensing can be represented in Eqn. (1), where $w(n)$ and $x(n)$ represent the noise and user signal, respectively. The user's presence is determined by comparing the energy with the predefined threshold. H_0 indicates the case where the SDR is idle, and H_1 indicates the case where the user is using the SDR and transmitting at a certain frequency and bandwidth.

$$\begin{cases} H_0 : y(n) = w(n) \\ H_1 : y(n) = s(n) + w(n) \end{cases} \tag{1}$$

We use a spectrum stitching technique with the B205mini-i SDR to monitor a large spectrum span since the instantaneous bandwidth of 56 MHz is insufficient to monitor the complete span of the spectrum under consideration. The procedure for spectrum stitching and energy-based detection is described in Algorithm 1 and runs on top of the UHD. The Multi-USRP API provided by UHD is used for executing different functionalities ranging from setting up the center frequency, bandwidth, the RF chain of the SDR, the gain of SDR, and the configurations to set the sampling rate. As shown in Figure 5, B205mini-i captures the IQ samples at a center frequency. The IQ samples are stored in a buffer and we collect n IQ samples at a particular center frequency. The recorded IQ samples in the time-domain are first passed through the Blackman Harris window to reduce the spectral leakage. For a better interpretation of the recorded data, the resolution bandwidth of the filter is set to 15 KHz since the sub-carrier spacing in LTE signals remains the same. Once the signal is passed through the window, we use 1024-points FFT to find the spectral density and compare the energy with a certain threshold. Once the signal is found in a frequency frame, we take three more measurements of the same frame to increase the confidence level and then report the frequency and bandwidth value to the wireless guard daemon for further analysis of the user behavior.

5 EXPERIMENTAL EVALUATION

We have implemented the Wireless Guard in an ARA sandbox environment as shown in Figure 8. The ARA sandbox includes a BS SDR (NI N320) and a UE (NI B210), in addition to the associated SDR host computers and ARA Controller. The BS and UE host computers execute the srsRAN software stack to establish the link between the BS and UE. For the evaluation purpose, the BS SDR was hosted on a Dell PowerEdge T340 with Intel(R) Xeon(R) CPU@3.40 GHz, with 12 cores, 64 GHz Memory and 1 TB of Hard Drive. For the UE host computer and the management computer, we selected the Intel NUC 10 BXNUC10I7FNHN1 with Core-i7 processor and up to 4.7 GHz clock speed.

To test the performance of Algorithm 1, the Downlink port of the BS USRP device is connected to the Directional Coupler with the coupling ratio of 10 dB, and the output of the coupler is connected to the antenna for the data signal transmissions. The coupling port

Algorithm 1: Wide-band Spectrum Monitoring Using NI SDR

Input: Start_Freq, Stop_Freq, Resolution Bandwidth (RBW), Intermediate Frequency Bandwidth (IFBW), RF Chain, Scan Interval
Output: Occupied Spectrum Bands (OSB)

$OSB \leftarrow \emptyset$;
$F_C \leftarrow Start\_Freq$;
while *current time % Scan Interval == 0* **do**
  while $F_C + \frac{IFBW}{2} \leq Stop\_Freq$ **do**
    Capture IQ Samples;
    forall *Subband j of bandwidth RBW in* $[F_C - \frac{IFBW}{2}, F_C + \frac{IFBW}{2}]$ **do**
      Multiply the IQ samples with a windowing function to filter the IQ samples through subband j;
      Take N-point FFT of the filtered signal, and calculate its Energy E;
      if $E \geq$ *signal detection threshold* τ **then**
        Repeat steps 5, 7, and 8 and take three more measurements to remove uncertainties in the signal detection;
      end
      if *Signal presence in subband j is confirmed* **then**
        $OSB \leftarrow OSB \cup \{subband\ j\}$;
      end
    end
    $F_C \leftarrow F_C + IFBW$
  end
  Report the Occupied Spectrum Bands (OSB) back to WG Daemon running in management computer;
end

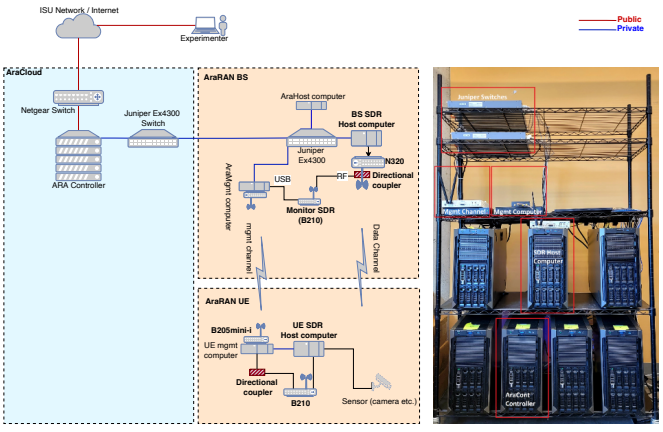

Figure 8: ARA Sandbox Evaluation Network

of the WG Monitoring SDR is connected to the AraMgmt computer and talks to the WG daemon sitting inside the AraMgmt computer.

The spectrum sensing results from Algorithm 1 are shown in Figure 9. The user in our experiment operates at a center frequency of 3.68 GHz with an operational BW of 10 MHz. The monitoring frequency span under consideration is of 150 MHz from 3.6 GHz to 3.75 GHz. .

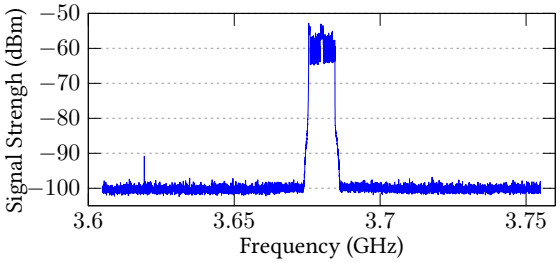

Figure 9: Wide-band Spectrum Detection using NI SDR

For the overall performance analysis of the Wireless Guard prototype, we create multiple tests that mimic the real use-case in the ARA platform. We have created a set of experiment profiles and tried to generate the scenario where the user initially started the operations and was being honest, i.e., was operating at the reserved frequency. Afterward, the user tries to misbehave and starts an out-of-band emission. The mean time delay to stop the operations of a misbehaving user using the proctive and reactive approaches is shown in Table 2.

Table 2: Average Detection and Response Delay

	Proactive Approach	Reactive Approach
Mean Delay	0.97 s	5.89 s

The values in the table represent the time delay to detect the RF activity as the overall time required by the controller in stopping the container of the misbehaving user when it tries to start the RF operations in frequencies outside its reservation. The reason for relatively higher time delays in the case of the reactive approach is the computational complexity that comes with the FFT. Also, based on Algorithm 1, once the energy is detected, we take three more measurements to increase the confidence levels for reporting the accurate BW and F_C (Center Frequency).

Besides the time delays, the proactive approach performs better in terms of the accuracy of the RF operation detections. Since the parameters are retrieved directly from the software stack, the proactive approach provides very accurate results in case of low SNR values which is a concern in all conventional cognitive radios.

The overall system performance of the reactive approach depends on several factors and we test the overall system performance using different parameters. As seen in Figure 8, we monitor the time delay required to take the FFT and compare with the threshold during a single cycle. As seen in the above Figure 10, the computational overhead increases linearly as we increase the frequency span that needs to be measured. For every 100 MHz increase in the frequency span, we can observe an increase in delay of 1 s. The overall computational overhead/CPU usage was computed by considering different number of FFT points for the same monitoring span. As shown in Figure 10, the computational overhead increases as we increase the FFT points.

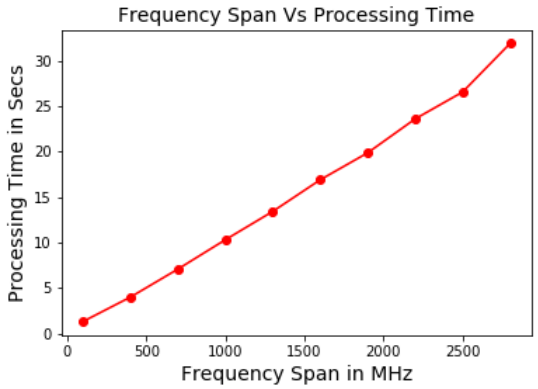

Figure 10: Span vs. End-to-End Processing Time

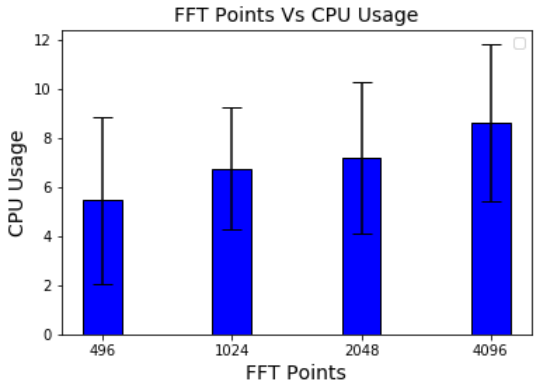

Figure 11: No. of FFT Points vs. CPU Usage

The CPU usage for the initial scan of the whole span was relatively very high, i.e., up to 108% (i.e., 1.08 cores of the system). In the initial scan, the hardware gets configured and, once the SDR has been configured with the firmware, the subsequent processes include read/write from/to the SDR and FFT for the captured signals. Further, as shown in Figure 10, the CPU usage also increases as we increase the number of FFT points. Since the optimal results can be obtained using 1024 FFT points, i.e., the error to monitor the correct bandwidth is very low as compared to FFT with lower number of points, we keep the value for WG to reduce the computational overhead.

6 CONCLUDING REMARKS

We have designed and implemented the Wireless Guard (WG) for spectrum monitoring and enforcement in the ARA wireless living lab [14]. The proactive approach is a software-based approach

which keeps monitoring the frequencies selected by the users in the software stack. For multi-layer security, WG also uses the reactive approach where the spectrum use from each RF chain is monitored using COTS RF Sensors at the base station sites and B205mini-i SDRs at the user equipment sites. We have evaluated the effectiveness of the WG design and implementation in the ARA sandbox environment, and we will evaluate WG in at-scale field deployment once the first phase of ARA [1] is completed in fall 2022. This study of wireless guard has focused on spectrum enforcement to make sure that no user or incumbent suffers from unexpected interference from ARA experiments. However, the WG software and hardware architectures can be used for studies such as dynamic spectrum sharing between terrestrial and aerial networks. In addition, the over-the-air data collected from the RF sensors can be used to train machine-learning models for wireless network design and to get a better understating of RF environment in rural settings.

ACKNOWLEDGMENTS

We thank Miguel Llanes for his help with the use of Keysight equipment in ARA. This work is supported in part by the NSF awards 2130889 and 1827211, NIFA award 2021-67021-33775, and PAWR Industry Consortium.

REFERENCES

[1] 2022. Phased ARA Deployment. https://arawireless.org/deployment/.
[2] George Atia, Anant Sahai, and Venkatesh Saligrama. 2008. Spectrum Enforcement and Liability Assignment in Cognitive Radio Systems. In *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*. 1–12.
[3] Aveek Dutta and Mung Chiang. 2016. "See Something, Say Something" Crowdsourced Enforcement of Spectrum Policies. *IEEE Transactions on Wireless Communications* 15, 1 (2016), 67–80.
[4] Carlo Galiotto, George K. Papageorgiou, Konstantinos Voulgaris, M. Majid Butt, Nicola Marchetti, and Constantinos B. Papadias. 2018. Unlocking the Deployment of Spectrum Sharing With a Policy Enforcement Framework. *IEEE Access* 6 (2018), 11793–11803.
[5] Abhay Karandikar. 2019. Frugal 5G: Towards Affordable Rural Wireless Broadband. In *2019 URSI Asia-Pacific Radio Science Conference (AP-RASC)*. 1–1.
[6] Vireshwar Kumar, He Li, Jung-Min Jerry Park, and Kaigui Bian. 2018. Enforcement in Spectrum Sharing: Crowd-sourced Blind Authentication of Co-channel Transmitters. In *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. 1–10.
[7] Claire Najjuuko, Georginah K. Ayebare, Ronald Lukanga, Edwin Mugume, and Dorothy Okello. 2021. A Survey of 5G for Rural Broadband Connectivity. In *2021 IST-Africa Conference (IST-Africa)*. 1–10.
[8] Jung-Min Park, Jeffrey H. Reed, A. A. Beex, T. Charles Clancy, Vireshwar Kumar, and Behnam Bahrak. 2014. Security and Enforcement in Spectrum Sharing. *Proc. IEEE* 102, 3 (2014), 270–281.
[9] Matthias Sander-Frigau, Tianyi Zhang, Chen-Ye Lim, Hongwei Zhang, Ahmed E. Kamal, Arun K. Somani, Stefan Hey, and Patrick Schnable. 2021. A Measurement Study of TVWS Wireless Channels in Crop Farms. In *IEEE MASS*.
[10] Roya H. Tehrani, Seiamak Vahid, Dionysia Triantafyllopoulou, Haeyoung Lee, and Klaus Moessner. 2016. Licensed Spectrum Sharing Schemes for Mobile Operators: A Survey and Outlook. *IEEE Communications Surveys Tutorials* 18, 4 (2016), 2591–2623.
[11] Boston C Terry, Alex Orange, Neal Patwari, Sneha Kasera, and Jacobus Van Der Merwe. 2020. Spectrum monitoring and source separation in POWDER. In *Proceedings of the 14th International Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*. 25–32.
[12] Martin B H Weiss, Mohammed Altamimi, and Mark McHenry. 2013. Enforcement and spectrum sharing: A case study of the 1695–1710 MHz band. In *8th International Conference on Cognitive Radio Oriented Wireless Networks*. 7–12.
[13] Jincan Xin, Sen Xu, Hua Zhang, and Shangkun Xiong. 2021. Efficient Dynamic Spectrum Sharing for LTE-NR Networks. In *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*. 538–543.
[14] Hongwei Zhang, Yong Guan, Ahmed Kamal, Daji Qiao, Mai Zheng, Anish Arora, Ozdal Boyraz, Brian Cox, Thomas Daniels, Matthew Darr, et al. 2022. ARA: A Wireless Living Lab Vision for Smart and Connected Rural Communities. In *ACM WiNTECH*.
[15] Qing Zhao and Ananthram Swami. 2007. A Survey of Dynamic Spectrum Access: Signal Processing and Networking Perspectives. In *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*, Vol. 4. IV–1349–IV–1352.
[16] Anatolij Zubow, Suzan Bayhan, Piotr Gawłowicz, and Falko Dressler. 2020. DeepTxFinder: Multiple Transmitter Localization by Deep Learning in Crowdsourced Spectrum Sensing. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. 1–8.