# Security Assessment of Wideband Spectrum Sensors

Rabia Tugce Yazicigil, Deepak Gopalan, and David Starobinski
Electrical and Computer Engineering Department, Boston University, Boston, MA, USA 02215
{rty, staro}@bu.edu

***Abstract*—We investigate security vulnerabilities of wideband spectrum sensors to denial of service (DoS) attacks, launched by an adversary with limited power budget. We survey traditional spectrum analysis methods and compressed-sensing (CS) spectrum sensors in terms of their operation principles and system performance metrics. We develop and simulate end-to-end system models of the wideband spectrum sensors to evaluate their detection probabilities and false alarm probabilities in both non-adversarial and adversarial environments. We show that sweeping spectrum scanners are inherently secure against DoS attacks due to their high dynamic range and small instantaneous bandwidth (BW) equal to their resolution bandwidth. Next, we evaluate Nyquist-rate FFT-based spectrum sensors and show that they are only vulnerable to high-power DoS attacks due to their wide instantaneous BW equal to their Span. These traditional spectrum sensors, however, have high energy consumption for wideband RF spectrum sensing either due to their long scan time or high power. Thus, CS spectrum sensors have recently been proposed as an alternative for RF spectrum sensing thanks to their low energy consumption and fast scan time. A major contribution of this paper is to show that CS spectrum sensors are vulnerable to stealthy DoS attacks (i.e., the attacks are hard to detect). For the same attacker power budget, we further show that the attacks become more potent if the adversary uses multiple attack signals with low power rather than a single attack signal with high power. Finally, we discuss possible countermeasures against the attacks.**

***Index Terms*—spectrum scanner, cognitive radio, compressed sensing, security**

## I. Introduction

The next-generation of radio receivers require spectrum agility and content awareness to facilitate accessing a shared pool of spectrum in the sub-6 GHz frequency band [1], [2]. Fast and energy-efficient signal monitoring over a wideband spectrum (e.g., 1GHz and beyond) is necessary to support short dynamic links. Thus, spectrum sensors must be employed to detect incumbent (primary user) signals and interferers (e.g., other secondary users and external sources of interference). Detecting strong interference signals is also important to prevent the compression or desensitization of receivers [3].

Traditional architectures for spectrum analysis are typically organized into two main categories: (1) sweeping spectrum scanners with high sensitivity and low power but slow scan time (proportional to the number of bins) and (2) Nyquist-rate FFT-based spectrum sensors with short scan times but high power consumption (to a first order, energy consumption remains the same for the traditional spectrum monitoring systems resulting in a fixed trade-off between scan time and power consumption).

Compressed-sensing (CS) [4], [5] techniques have recently been proposed to break the traditional RF spectrum scanning trade-offs between energy consumption, scan time, and hardware complexity [6], [7]. CS analog-to-information converters (AICs) have been demonstrated with very short scan times (i.e., in the order of a few $\mu$s) and significant energy savings (two orders of magnitude lower than for traditional spectrum sensors).

To our knowledge, all of the existing spectrum sensor hardware introduced in the literature have been designed under the assumption of a non-adversarial environment. Yet, to ensure their viability in future dynamic shared spectrum access (DSSA) applications, it is crucial to understand the behavior of traditional and CS spectrum systems when they are facing adversarial conditions. Indeed, under such circumstances, the performance of spectrum sensors should gracefully degrade rather than completely break down.

While there exists a large literature on attacks on spectrum sensing, these attacks focus on sensing functionalities above the hardware level. Examples include attacks on cooperative spectrum sensing [8]–[10], primary user emulation (PUE) attacks [11], [12], and attacks on components of cognitive radios (e.g., learning components) [13], [14]. We refer to [12] for a survey of security issues in spectrum sensing and sharing.

In this paper, we conduct a thorough security assessment of the aforementioned three types of sensors (i.e., sweeping spectrum scanners, Nyquist-rate FFT-based spectrum sensors, and CS spectrum sensors). For the case of CS spectrum sensors, we further consider two different AIC architectures (i.e., Modulated Wideband Converter (MWC) [6] and Quadrature Analog-to-Information Converter (QAIC) [15]), which we review in the sequel. We develop detailed simulation models of these systems and benchmark their behavior in non-adversarial environments. Next, for each of these sensing systems, we evaluate if it is possible for an adversary to mount a DoS attack (i.e., make the system effectively unusable) and furthermore make the attack stealthy (i.e., avoid being detected).

Our main contributions are as follows: (1) We show that sweeping spectrum scanners are inherently secure against DoS attacks; (2) Nyquist-rate FFT-based spectrum sensors are only vulnerable to high-power DoS attacks (i.e.. the attacker's power is about 45dB higher than that of legitimate signals). Furthermore, the attacks can be detected. (3) CS spectrum sensors are vulnerable to stealthy, DoS attacks. Interestingly, the attacks become more potent if the adversary uses multiple low-power signals rather than a single high-power signal. We discuss possible countermeasures to attacks on CS systems, which come at the expense of higher energy consumption or longer scan times. Hence, these results indicate that there is no "free lunch."

The rest of this paper is organized as follows. Section II

D. Gopalan is also with IIT Bombay, Mumbai, India. This research was supported in part by NSF under grant CNS-1409053.

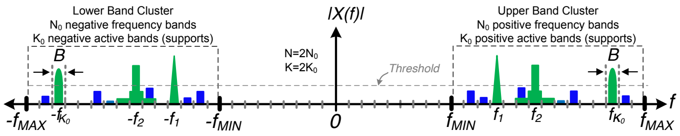

**Fig. 1:** *Sparse multi-band signal model of an RF spectrum ranging from $f_{MIN}$ to $f_{MAX}$. Active supports (i.e. active spectrum bins) above the signal-level detection threshold are shown in green, while the inactive ones are in blue. Image courtesy with permission [7].*

reviews the different types of spectrum sensors and introduces our notation, performance metrics, and sensing scenarios. In Section III, we introduce simulation models for each sensor type and evaluate the performance of the sensors in non-adversarial environments. Then, in Section IV, we conduct a security assessment of the sensors to DoS attacks, and discuss possible countermeasures. We conclude the paper in Section V.

## II. Background

### A. RF Signal Model and Spectrum Scenario

We review terminology and metrics related to spectrum scanning, with an emphasis on compressed sensing [6], [7], [15]–[17].

- *Multi-Band Signal Model:* We consider multi-band signals [16], [19] that are real-valued, square-integrable signals $x(t)$ satisfying two properties: the signal of interest $x$ is sparse in the frequency domain and the fourier transform, $X(f)$ is only valid in the frequency range of $\mathcal{F}$ = $(-f_{MAX}, -f_{MIN}] \bigcup [f_{MIN}, f_{MAX})$.
  As shown in Figure 1, for a real-valued signal $x(t)$, $\mathcal{F}$ has been partitioned into $N = 2N_0$ disjoint spectrum bands with a resolution bandwidth of $RBW$ [7]. The sparse Fourier transform $X(f)$ is supported on only $K = 2K_0 < N = 2N_0$ of these bands. These $2K_0$ bands are referred to as the *active bins* or *supports* when their power level is above a signal-level detection threshold.
- *Sparsity:* The key underlying assumption of CS systems is that of *sparsity*. Sparsity makes it possible to uniquely determine the original spectrum of a band-limited signal without requiring Nyquist rate sampling of the instantaneous bandwidth [4]. Signals of interest are sparse if they can be represented by a sparse vector in a well-chosen basis. Specifically, a sparse vector of dimension $N_0$ has $K_0$ nonzero coefficients where $K_0 \ll N_0$. The sparsity level is defined as $S = K_0/N_0$ [17], [18]. Note that if the *spectral occupancy* $S_0 = K_0/N_0$ is small, then the support of $X(f)$ has a Lebesgue measure which is much smaller than the Nyquist rate of the instantaneous bandwidth, that is $K_0 RBW \ll f_{Nyq} = 2f_{MAX}$ [7], [16].
- *Spectrum Scenario:* In this paper, we consider a case study of RF spectrum sensing under non-adversarial and adversarial spectrum conditions in a 1.26GHz of interest spectrum band ranging from 2.57GHz to 3.83GHz with a 20MHz RBW resulting in $N_0 = 63$ spectrum bins [15], [17]. In this scenario, there are 3 non-adversarial signals, i.e. desired signals, that are above the signal-level detection threshold, $K_0 = 3$. The sparsity level for this scenario is $S = 3/63$ which indicates a spectrum occupancy of $4.8\%$. The $K_0 = 3$ signals can be located in *any* of the $N_0 = 63$ spectrum bins. The goal is to efficiently locate those $K_0$ signals while satisfying a reliable detection performance, e.g. high detection and low false alarm probabilities.
- *Adversary:* Adversarial signals are introduced with varying number of attack signals under a constant power budget. The goal is to analyze the impact of the attacker power budget and power allocation on the detection of the desired signals as well as the detection of the attacker.

### B. RF Spectrum Sensing Performance Metrics

We next detail key system performance metrics of traditional and CS RF spectrum scanners and sensors that are designed to detect up to $K_0$ desired signals located in any of $N_0$ spectrum bins. These metrics include the scan time and energy consumption required to capture information in a certain instantaneous bandwidth and dynamic range [7]. A reliable detector satisfies target detection and false alarm probabilities which are statistical in nature.

- *Detection and False Alarm Probabilities:* The detection probability $P_D$ is the probability that a spectrum sensor correctly reports a signal in the RF spectrum as being active [15]. The false alarm probability $P_{FA}$ is the probability that a spectrum sensor incorrectly reports a spectrum bin as being occupied while there is no signal present [15].
  For the rest of the paper, the $P_D$ and $P_{FA}$ simulation results are reported based on the correct detections and the false alarms from 125 iterations (number of experiments, $N_E$). Consider that experiment $i$ produces $(CD_i)$ correct detections and $(FA_i)$ false alarms, then [15]:
  $$P_D = \frac{1}{N_E}\sum_{i=1}^{N_E}\frac{CD_i}{K_0} \text{ and } P_{FA} = \frac{1}{N_E}\sum_{i=1}^{N_E}\frac{FA_i}{N_0 - K_0} \quad (1)$$
  The threshold choice for the signal detection impacts the reliability and performance of the detector [20]. For instance, if the threshold value is close to the noise floor, $P_D$ will be maximized at the expense of increase in $P_{FA}$ [7]. In this paper, we assume a signal-detection threshold that is 10dB above the noise floor.
- *Scan Time:* The scan time $T_{scan}$ is defined as the sum of the detector response time $T_{resp}$ and the digital signal processing (DSP) time $T_{rec}$ [15]. The DSP time is proportional to $N_s/f_s$, where $f_s$ is the analog-to-digital converter (ADC) sampling rate and $N_s$ is the number of samples collected from the ADCs [15]. The detector response time is proportional to the settling time of the low-pass anti-aliasing filters connected to the ADCs [15].
- *Energy Consumption:* Energy consumption for a scan $E$ is defined as the product of the power consumption $Power$ with the scan time $T_{scan}$ [15]:
  $$E = Power \cdot T_{scan} = Power \cdot [T_{resp} + T_{rec}]. \quad (2)$$
- *Instantaneous Bandwidth:* The instantaneous bandwidth (or *Span*) represents the bandwidth of which signals can be successfully and rapidly detected, while meeting target detection and false alarm probabilities [7].
- *Dynamic Range:* The dynamic range (DR) of a spectrum sensor is defined as its ability to successfully detect a weak signal in the presence of strong signals over the instantaneous bandwidth [15], [16]. The dynamic range is typically limited by the resolution of ADCs employed by the spectrum sensors.

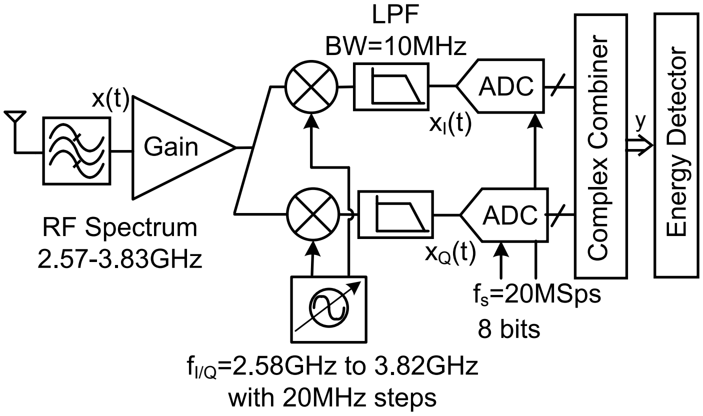

**Fig. 2:** *Sweeping Spectrum Scanner*

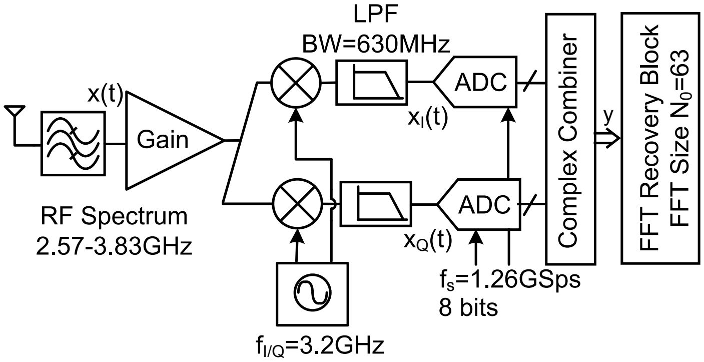

**Fig. 3:** *Nyquist-rate FFT-based Spectrum Sensor*

In the next two subsections, we review traditional and CS spectrum sensing techniques in terms of their hardware architectures and design choices.

### C. Traditional Spectrum Analysis Techniques

- *Sweeping Spectrum Scanner:* A traditional sweeping spectrum scanner shown in Fig. 2 captures the spectrum information in a time-multiplexed fashion by sweeping the local oscillator frequency of the quadrature downconverter mixers in a single-branch hardware [7]. Sweeping spectrum scanners offer a high sensitivity and high dynamic range across small instantaneous BW equal to its RBW [21]–[23]. However, this approach requires a long scan time especially for fine resolutions. Therefore, the tradeoff between the scan time and resolution bandwidth make them incompatible for DSSA scenarios with short dynamic links [16].
- *Nyquist-rate FFT-based Spectrum Sensor:* To reduce the scan time, a Nyquist-rate ADC or multi-branch spectrum sensors can be used at the expense of increased power consumption and hardware complexity [7]. We only consider the Nyquist-rate FFT-based spectrum sensors in this paper. The architecture of such spectrum sensors is shown in Fig. 3.

  Note that this approach does not scale well to high frequencies and becomes power hungry for capturing a large instantaneous BW. Nyquist-rate approach captures the interest spectrum band very rapidly by reducing $T_{resp}$ through high filter bandwidth and $T_{rec}$ through high sampling rate. In the digital back end, the detector performs an FFT with a dimension of $N_0$ to recover the signals above the signal-detection threshold in each individual bin with a bandwidth equal to $RBW$ [23].

### D. Compressed-Sensing Spectrum Sensors

Compressed sensing [4], [5], [24] offers a very fast signal detection with scan times in the order of $\mu s$ over $GHz$-wide spectrum by sampling the spectrum at sub-Nyquist rate. Existing CS spectrum sensors have been demonstrated with two orders-of-magnitude lower energy consumption compared to the traditional spectrum sensors [7].

A key design parameter for CS spectrum sensors is the number of incoherent measurements (m) required for the successful detection of $K_0$ signals while satisfying the target $P_D$ and $P_{FA}$. The number of incoherent measurements required in a CS AIC, $m$, is given by:

$$m \approx \lceil C \cdot K_0 \cdot \log\left(\frac{N_0}{K_0}\right)/q\rceil \tag{3}$$

where $K_0$ is the number of active signals above the threshold, $N_0$ is the number of spectrum bins, and $C$ is a constant in the range of 2 to 4 [15], [16]. CS theory [4], [5], [24] demonstrates the successful recovery and reconstruction of a sparse signal, i.e. $K_0$ active signals in $N_0$ spectrum bins, from only few incoherent measurements, where $K_0 < m << N_0$. Each incoherent measurement is traditionally collected from a single unique hardware branch. Therefore, the total number of incoherent measurements corresponds to the number of hardware branches in a CS AIC. The number of branches $m$ may be traded for the increased sampling rate in each branch by an odd integer factor of $q$, where $q = 1, 3, 5, ...$ [6], [16].

Each incoherent measurement is obtained by mixing the signal of interest with unique, low cross-correlation pseudorandom binary sequences (PRBSs) [6]. PRBS mixing aliases the signal spectrum information in each bin to other bins widely known as a spread spectrum technique [30]. By using a single copy of this aliased spectrum around baseband and sampling at the sub-Nyquist rate of the instantaneous bandwidth, e.g., Span, the sparse signal processing algorithm can still disentangle this folding and recover the signal supports from fewer measurements than in the Nyquist case [15]. Widely-used sparse signal processing algorithms in the CS digital back end [7] are Orthogonal Matching Pursuit (OMP) [25], [26], convex relaxations based on $l1$ minimization [27], and other greedy methods such as CoSamp [28]. In this paper, we use a simple greedy algorithm, namely OMP, for signal support recovery.

CS architectures can broadly be organized into two main categories.

- *Modulated Wideband Converter:* A Modulated Wideband Converter (MWC) [6], [29], shown in Fig. 4, is a multi-branch low-pass CS architecture that senses the spectrum from DC to a maximum frequency of interest $f_{MAX}$ [6]. Since the MWC operates on a real signal x(t), it will detect $2K_0$ active signal supports out of $2N_0$ spectrum bins. Each branch of the MWC consists of a low-noise amplifier, a mixer driven by a unique PRBS at its local oscillator port, a low-pass anti-aliasing filter,

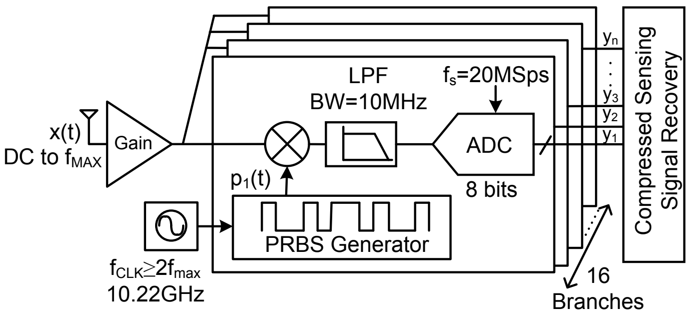

**Fig. 4:** *Low-Pass CS Architecture: Modulated Wideband Converter [6]*

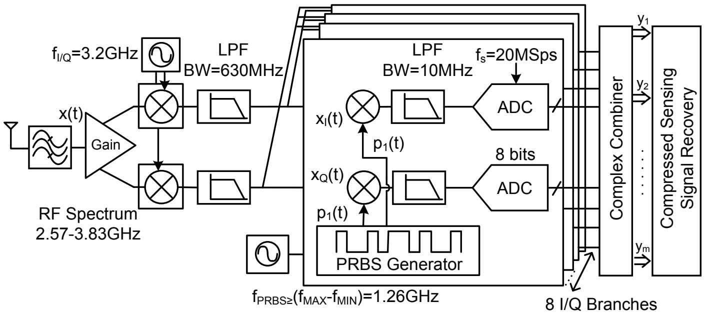

**Fig. 5:** *Band-Pass CS Architecture: Quadrature Analog-to-Information Converter [15]*

and an analog-to-digital converters (ADCs) sampling at a sub-Nyquist rate of the instantaneous bandwidth.

Unique PRBSs with low cross-correlation are preferred since they satisfy the restricted isometry property and incoherency for the successful CS measurements [15]. Even though the ADC samples at a sub-Nyquist rate equal to the resolution bandwidth $RBW$, the PRBS generator with a clock frequency of $f_{CLK}$ operates at the Nyquist-rate of the maximum frequency of interest, i.e., $f_{CLK} \geq 2 \cdot f_{MAX}$. Capturing the entire spectrum from DC to $f_{MAX}$ makes the PRBS generator the most power-hungry block of this architecture. The generation and distribution of the high-frequency PRBSs further increase the hardware complexity [7]. Therefore, such low-pass CS architectures do not scale well to high frequencies for RF spectrum sensing applications.

- *Quadrature Analog-to-Information Converter:* A Quadrature Analog-to-Information Converter (QAIC), shown in Fig. 5, is a multi-branch band-pass CS architecture designed for energy-efficient sensing of an RF spectrum [15]. It only senses the active signals in a band-pass frequency range with a minimum frequency $f_{MIN} > 0$ by limiting the RF bandwidth with a quadrature downconverter. In contrast to the MWC, the QAIC samples a complex signal, i.e. $I(t) \pm j \cdot Q(t)$. It will detect $K_0$ active signal supports out of $N_0$ spectrum bins. Due to the RF bandwidth limiter, the clock frequency of the PRBS generator is now reduced to $f_{CLK} \geq Span = f_{MAX} - f_{MIN}$ [15]. Therefore the QAIC architecture scales well to higher frequencies in contrast to low-pass CS architectures [15], [16].

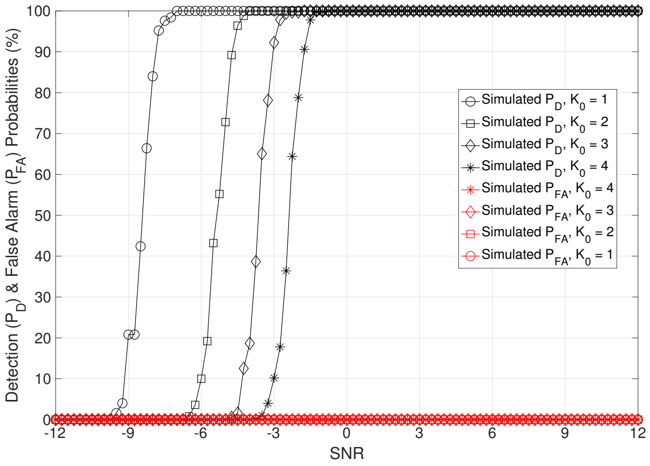

**Fig. 6:** ***Nyquist-rate FFT-based spectrum sensor** detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) vs SNR for varying number of signals from $K_0$ 1 to 4 with a signal-detection threshold 10dB above the noise floor.*

## III. Spectrum Sensor Models

In this section, we develop a behavioral hardware model in MATLAB for each spectrum sensor architecture shown in Fig. 2-5 and benchmark their performance in non-adversarial environments. In the next section, we use these models to evaluate the performance of the spectrum sensors under attacks.

We next detail our simulation model. A noise generator is used to model thermal noise in wireless communication channels as an Additive White Gaussian Noise (AWGN). ADC quantization noise is also considered for an 8-bit ADC. The noise power level relative to the signal power level is set with the signal-to-noise ratio (SNR) parameter by changing the total integrated noise power over the $N_0$ bins in the interest Span. The threshold value is set above the noise floor with a margin of 10dB.

The input signal spectrum is modeled as $K_0$ signals in the RF frequency band of interest ranging from 2.57GHz to 3.83GHz. These signals are generated in baseband as a band-limited noise signal and upconverted to $K_0$ RF center frequencies randomly chosen out of 63 bins. The total integrated signal power is kept constant for the non-adversarial experiments in which we vary the number of signals $K_0$ from 1 to 4.

- *Nyquist-rate FFT-based Spectrum Sensor:* The Nyquist-rate FFT-based spectrum sensor model captures the entire 1.26GHz instantaneous bandwidth ranging from 2.57GHz to 3.83GHz with a wideband I/Q downconverter operating at 3.2GHz and ADCs operating at 1.26GSps in each I and Q branch. To detect $K_0$ signal, this 1.26GHz-wide spectrum is subdivided into 63 RBW-wide bins by performing an FFT with a size of 63 in the digital back end. Design parameters for the Nyquist-rate FFT-based spectrum sensors associated with the use case are listed in Table I.

  We first model and analyze the performance of Nyquist-rate FFT-based spectrum sensors under varying noise conditions. When there are equal-power strong or weak signals present over the instantaneous bandwidth, the effect of the quantization noise is negligible under the assumption of an automatic gain control block adjusting

**TABLE I:** *System Parameters - Traditional and CS Spectrum Sensors*

| System Parameters | QAIC | MWC | Nyquist FFT | Sweeping Scanner |
|---|---|---|---|---|
| I/Q Downconverter | 3.2GHz | N/A | 3.2GHz | 2.58GHz-3.82GHz |
| I/Q Filter BW | 630MHz | N/A | 630MHz | 10MHz |
| fPRBS | 1.26GHz | 10.22GHz | N/A | N/A |
| Anti-Aliasing LPF BW | 10MHz | 10MHz | N/A | N/A |
| Sampling Rate (fs) | 20MSps | 20MSps | 1.26GSps | 20MSps |
| N0 (PRBS Length for CS) | 63 | 511 | 63 | 63 |
| Hardware Branches | 8I/Q (16) | 16 | I/Q (2) | I/Q (2) |
| N/A: Not Applicable | | | | |

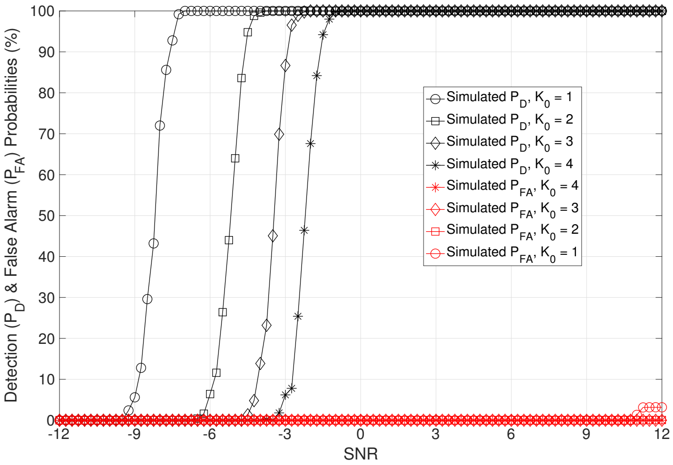

**Fig. 7:** ***Sweeping spectrum scanner*** *detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) vs SNR for varying number of signals from $K_0$ 1 to 4 with a signal-detection threshold 10dB above the noise floor.*

the signals to fit into the full scale of the ADC.

For the results presented in Fig. 6, we vary the SNR from -12dB to 12dB for $K_0$=1,2,3, and 4. Each $P_D$ and $P_{FA}$ value is reported from 125 iterations ($N_E = 125$). Simulated $P_D$ results in Fig. 6 demonstrate that $P_D$ is $\geq 90$ for SNR of -4.75dB for $K_0 = 2$, while the same $P_D$ is obtained for SNR of -1.75dB for $K_0 = 4$.

The signal power per active bin is halved in the $K_0 = 4$ case compared to the $K_0 = 2$ case, and this explains the 3dB drop in $P_D$. Simulated $P_{FA}$ results in Fig. 6 illustrates that $P_{FA}$ only depends on the threshold value and when the threshold is 10dB higher than the noise floor, there is almost no false alarm.

- *Sweeping Spectrum Scanner:* The sweeping spectrum scanner model consists of an I/Q mixer driven by a tunable LO signal with an initial frequency at $2.57GHz + RBW/2$. This LO frequency is increased by $RBW$ until it reaches to $3.83GHz - RBW/2$ to scan each bin sequentially. For the sweeping spectrum scanner model, ADCs only operate at the rate of 20MSps (RBW) for each I and Q branch. We perform a simple energy detection by calculating the power of a complex signal in each RBW and compare it to the signal-detection threshold. Design parameters for the sweeping spectrum scanner associated with the use case are listed in Table I.

  We also analyze the sweeping spectrum scanner performance in the presence of noise only. In this scenario, it does not matter for the $P_D$ performance if the signals are equal power or not since there is an AGC block before the digitization of the signal to fit the signal into the full scale of ADC in each RBW. However, we keep the total integrated signal power constant with equal power $K_0$ signals for the consistency of different models. For the results presented in Fig. 7, we vary the SNR from -12dB to 12dB for $K_0$=1,2,3, and 4. Each $P_D$ and $P_{FA}$ value is reported from 125 iterations ($N_E = 125$). Simulated $P_D$ results in Fig. 7 demonstrate that $P_D$ is $\geq 90$ for SNR of -4.75dB for $K_0 = 2$, while the same $P_D$ is obtained for SNR of -1.75dB for $K_0 = 4$. The signal power per active bin is halved in the $K_0 = 4$ case compared to the $K_0 = 2$ case, and this explains the 3dB drop in $P_D$. Since the detection threshold is 10dB above the noise floor, $P_{FA}$ is low.

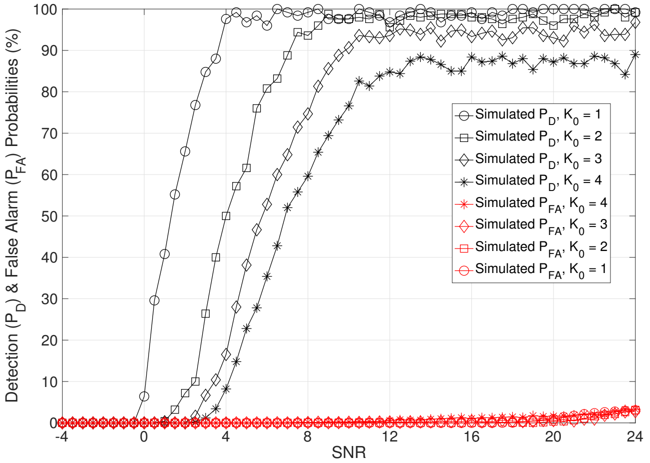

**Fig. 8:** ***CS QAIC*** *detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) vs SNR for varying number of signals from $K_0$ 1 to 4 with a signal-detection threshold 10dB above the noise floor and 40 samples ($N_s = 40$).*

- *CS QAIC:* The CS QAIC model employs a RF band limiter consisting of a wideband RF I/Q downconverter to downconvert the spectrum ranging from 2.57GHz to 3.83GHz to complex baseband spectrum from -630MHz to +630MHz. The complex baseband signal is mixed with 8 unique PRBSs with a length of 63 and a chipping frequency ($f_{PRBS}$) of 1.26GHz in each I and Q hardware branches. Since PRBS mixing aliases and spreads the signal information in each RBW, we used low-pass filters with a 3-dB bandwidth of 10MHz and ADCs operating at 20MSps in each I and Q branch to digitize the aliased spectrum information in only one of the spectrum bins centered around DC. CS support recovery disentangles this aliased information to find the signal support locations by using the OMP algorithm [25].

  The OMP is an iterative algorithm that finds the largest signal support that is above the signal-detection threshold by checking the correlations with the measurement residual and updates the residual as each signal support is recovered [25]. The CS system-measurement-matrix row dimension and the recovery threshold are the two design parameters for setting the number of OMP iterations [7]. In our model, we assume the OMP iterations are equal to the CS system-measurement-matrix row dimension which is the number of incoherent measurements $m$. Design parameters for the CS QAIC associated with the use case are listed in Table I.

  We model and analyze the CS QAIC performance in

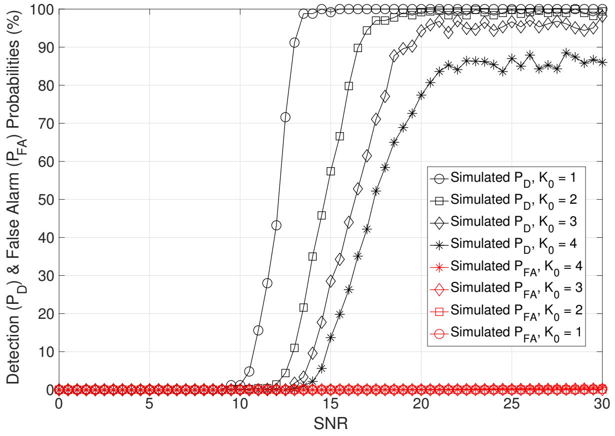

**Fig. 9:** ***CS MWC*** *detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) vs SNR for varying number of signals from $K_0$ 1 to 4 with a signal-detection threshold 10dB above the noise floor and 40 samples ($N_s = 40$). Both $P_D$ and $P_{FA}$ curves are shifted to right on the SNR axis by 9.1dB or $10\log(511/63)$ in contrast to the CS QAIC due to the additional noise folding in low-pass CS architectures.*

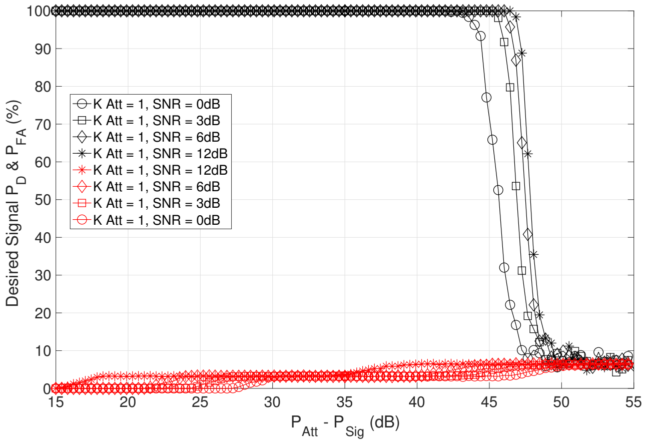

**Fig. 10:** ***Nyquist-rate FFT-based spectrum sensor*** *performance under an adversarial environment with a high-power attacker. Desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) are shown for varying attacker power ($P_{Att}$) for $K_{Att} = 1$ relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for SNR= 0, 3, 6, and 12dB.*

the presence of noise only with a varying number of signals, hence different sparsity conditions. For the results presented in Fig. 8, we vary the SNR from -4dB to 24dB for $K_0$=1,2,3, and 4. Each $P_D$ and $P_{FA}$ value is reported from 125 iterations ($N_E = 125$) and 40 samples are used for the sparse signal processing ($N_s = 40$). Simulated $P_D$ results in Fig. 8 demonstrate that $P_D$ is $\geq 90$ for SNR of roughly 3.5dB for $K_0 = 1$, while the same $P_D$ is obtained for SNR of 9.5dB for $K_0 = 3$. We note that the detection probability and false alarm plots are shifted to right on the SNR axis in contrast to the traditional spectrum sensors due to the noise folding of PRBS mixers. $P_D$ does not reach above 90% for $K_0 = 4$ signals since the number of incoherent measurements (m = 8I/Q) is designed for successful detection of $K_0 = 3$ signals. The signal-level detection threshold is 10dB above the noise floor and it limits the false alarm significantly below 10%.

- *CS MWC:* The CS MWC model is a low-pass architecture that senses the spectrum from DC to $f_{MAX}$. The clock frequency of the PRBS generator must be $\geq 2 \cdot f_{MAX}$. We assume a linear feedback shift register implementation in our model resulting in a length of 511 for 20MHz RBW with a clock frequency of 10.22GHz. The CS MWC model operates on a real signal with $K = 2K_0$ active bins in the 2.57GHz to 3.83GHz interest band. Input signal spectrum mixed with 16 unique PRBSs in each hardware branch. Since PRBS mixing aliases and spreads the signal information in each RBW, we used low-pass filters with a 3-dB bandwidth of 10MHz and ADCs operating at 20MSps in each branch to digitize the aliased spectrum information in only one of the spectrum bins centered around DC. CS support recovery disentangles this aliased information to find the signal support locations by using the OMP algorithm [25]. Design parameters for the CS MWC associated with the use case are listed in Table I.

  For the RF spectrum sensing application where there are no signals of interest below $f_{MIN} = 2.57GHz$, the MWC has degraded sensitivity due to the extra noise folding in from DC to 2.57GHz range in contrast to the CS QAIC. For the results presented in Fig. 9 where we vary the SNR from 0dB to 30dB for $K_0$=1,2,3, and 4, $P_D$ and $P_{FA}$ curves have a 9.1dB SNR shift or $10\log(511/63)$ in contrast to the CS QAIC that is proportional to the ratio of the length of the PRBSs.

## IV. Security of Spectrum Sensors

### A. Threat Model

Clearly, no protection is possible against an adversary with unlimited resources. Hence, we assume that the adversary has a limited transmission power $P_{Att}$. We assume that the adversary can split its power into $K_{Att} \geq 1$ different signals. Under such constraints, the goal of an adversary is to reach a certain objective, where the specific objective depends on the adversary's type.

We consider two types of adversaries:

- *Type-I adversary:* This adversary aims to make the spectrum sensing system effectively unusable to its users. Thus, the Type-I adversary aims to lower the probability of detection of legitimate signals $P_D$ to an unacceptably low value or maximize the probability of false alarm $P_{FA}$ to an undesirable high value.
- *Type-II adversary:* This adversary aims to transmit without being detected by the legitimate users (i.e., low Attacker $P_D$). For instance, transmitting outside the dynamic range or below the sensitivity level of the legitimate spectrum sensor may allow an adversary to maintain deniability.

In the rest of this section we first investigate the security of spectrum sensors and scanners to Type-I adversaries (i.e., DoS attacks). We then consider the combination of Type-I and Type-II adversaries (i.e., stealthy DoS attacks). We evaluate the impact of different settings of the parameters $P_{Att}$ and $K_{Att}$ on the effectiveness of the attacks.

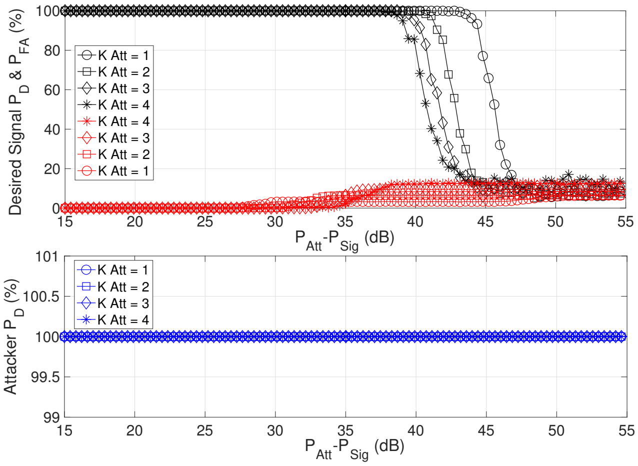

**Fig. 11:** ***Nyquist-rate FFT-based spectrum sensor*** *performance under an adversarial environment with varying number of attacker signals for a constant adversary power budget. Top plot shows the desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) and bottom plot shows the attacker $P_D$ (blue curves) for varying attacker power ($P_{Att}$) for $K_{Att}$=1, 2, 3, and 4 relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for SNR= 0dB.*

### *B. Denial of Service Attack against Spectrum Sensors (Type-I Adversary)*

We first consider the case of a Type-I adversary that aims to launch a denial of service (DoS) attack against spectrum sensors.

- *Traditional Spectrum Sensors:* Nyquist-rate FFT-based spectrum sensors and sweeping spectrum scanners are analyzed and simulated under varying number of adversarial signals with a constant total integrated power for the attacker. For these simulations, we keep the number of desired signals $K_0 = 3$ and use SNR of 0, 3, 6, and 12dB. For these SNR values, the simulated $P_D$ is at 100% in a non-adversarial environment. We illustrate the impact of the attacker's total power budget relative to the total power of the desired signals and the effect of changing the number of adversarial signals (by reducing the power of each adversarial signal proportionally).

  A key finding is that Nyquist-rate FFT-based spectrum sensors are vulnerable against denial of service attacks only when the attacker signal power is significantly higher than the desired signal power since the AGC block prior to the ADC will scale the signals across the entire Span and fit the amplitude of the large adversarial signals into the full scale of the ADC. Since there are large adversarial signals and relatively smaller desired signals present simultaneously over the same instantaneous BW (or Span), the detection of desired signals is limited by the quantization noise. Fig. 10 shows the Nyquist-rate FFT-based spectrum sensor performance with a single attacking signal. In this case, the attacker can only degrade the desired signal $P_D$ to 65% when their power is 45dB higher than the desired total signal power for 3 signals when the SNR is 0dB and this power has to be increased by roughly 2.5dB for SNR 12dB. Fig. 11 demonstrates the Nyquist-rate FFT-based spectrum sensor performance when the attacker varies the number of adversarial signals for $K_{Att} = 1$ to 4 with a constant total power budget. The top plot illustrates the desired $P_D$ (black curves) with respect to the total attacker power budget. When there are 4 moderate-power adversarial signals rather than 1 large-power adversarial signal, the desired signal $P_D$ degrades by 6dB due to the possibility of higher peak amplitudes when they are in phase, hence elevated quantization noise impact for the desired signals.

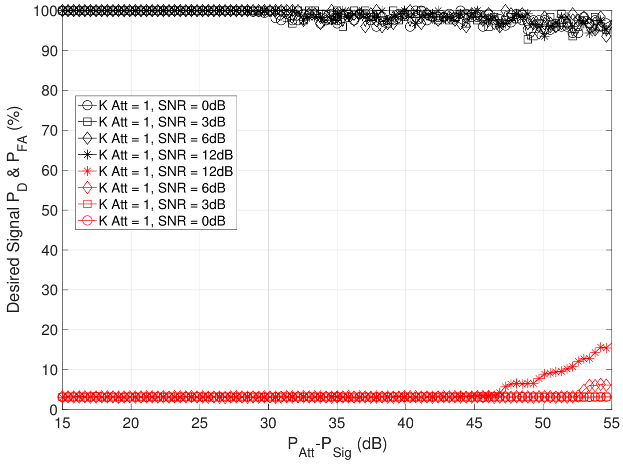

**Fig. 12:** ***Sweeping spectrum scanner*** *performance under an adversarial environment with a high-power attacker. Desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) are shown for varying attacker power ($P_{Att}$) for $K_{Att} = 1$ relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for SNR= 0, 3, 6, and 12dB.*

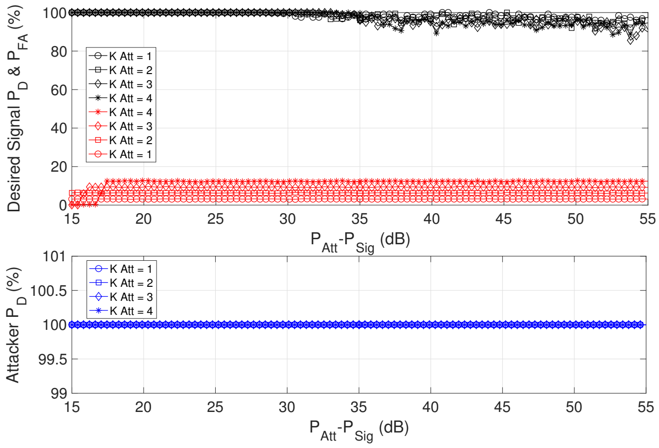

**Fig. 13:** ***Sweeping spectrum scanner*** *performance under an adversarial environment with varying number of attacker signals for a constant adversary power budget. Top plot shows the desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) and bottom plot shows the attacker $P_D$ (blue curves) for varying attacker power ($P_{Att}$) for $K_{Att}$=1, 2, 3, and 4 relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for SNR= 0dB.*

  Sweeping spectrum scanners are inherently secure against denial of service attacks under a stationary spectrum scenario. The sweeping spectrum scanner senses signals in each frequency bin individually, so an attack signal in one bin does not affect signal detection in another bin. Since the AGC block adjusts and maximizes the gain for each RBW in a time-multiplexed fashion, both weak desired and large adversarial signals enjoy the maximum gain and fit into the full scale of the ADC while sweeping through each RBW sequentially. This results in minimized degradation

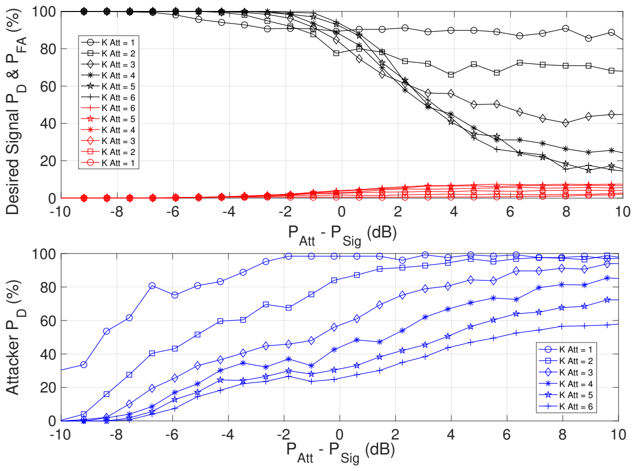

**Fig. 14:** ***CS QAIC*** *performance under an adversarial environment with varying number of attacker signals for a constant adversary power budget. Top plot shows the desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) and bottom plot shows the attacker $P_D$ (blue curves) for varying attacker power ($P_{Att}$) for $K_{Att}$=1 to 6 relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for* ***SNR= 12dB****.*

due to quantization noise. Hence, the small instantaneous bandwidth of the sweeping scanner makes it more secure compared to the Nyquist-rate FFT based spectrum sensor. Fig. 12 demonstrates the sweeping spectrum scanner performance when there is only a single attacker under a varying SNR from 0 to 12dB. The simulated $P_D$ (black curves) illustrates that the attacker can not harm the detection performance of the sweeping spectrum scanner even with a large power budget. Further, $P_D$ of the desired $K_0 = 3$ signals does not degrade under varying number of adversarial signals as shown in Fig. 13.

- *CS Spectrum Sensors:* CS sensors are designed to operate under an assumption of a maximum sparsity level. When the number of signals exceeds the expected sparsity level, i.e., under signal support overload [17], traditional CS detectors perform poorly and yield a low $P_D$. For example, if a CS AIC is designed to detect maximum $K_0 = 3$ signals with $P_D \geq 90\%$ but deployed in a spectrum with $K_0 = 6$ signals, the measured $P_D$ degrades drastically from $\geq 90\%$ and stays around a maximum value of 50% for 6 signals with unreliable detection results since the number of hardware branches, i.e., the number of measurements, are lower than the theoretical limit for the required branches given in (3) for successful detection of signals by satisfying a target $P_D$ of $\geq 90\%$ [7], [17].
  An attacker can leverage this robustness vulnerability to launch a denial of service attack on existing CS spectrum sensors such as the MWC and the QAIC. This DoS attack, which we refer to as a *signal-overload attack* results in a catastrophic breakdown of existing CS monitoring systems when the spectrum becomes nonsparse.
  Under the assumption of an adversary with a limited power budget, we analyze the most effective denial of service attacks against the CS spectrum sensors to lower their $P_D$ or maximize their $P_{FA}$. Specifically, is it more advantageous for an adversary to transmit few signals at high power or a larger number of signals at lower power?

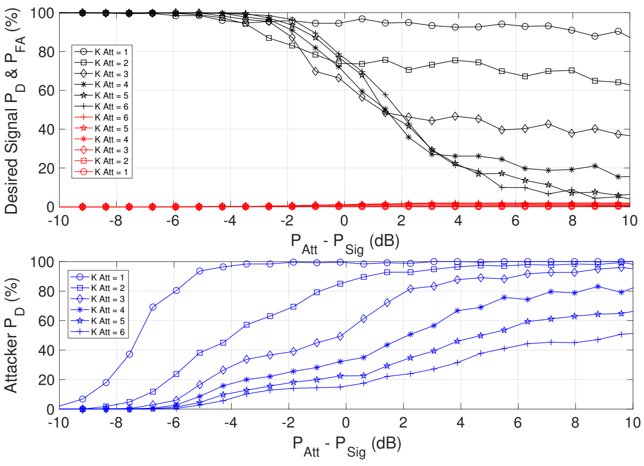

**Fig. 15:** ***CS MWC*** *performance under an adversarial environment with varying number of attacker signals for a constant adversary power budget. Top plot shows the desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) and bottom plot shows the attacker $P_D$ (blue curves) for varying attacker power ($P_{Att}$) for $K_{Att}$=1 to 6 relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for* ***SNR= 21dB****.*

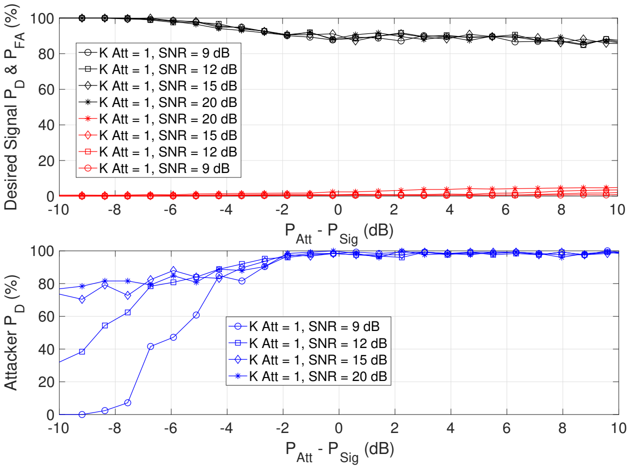

**Fig. 16:** ***CS QAIC*** *performance under an adversarial environment with varying number of attacker signals for a constant adversary power budget. Top plot shows the desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) and bottom plot shows the attacker $P_D$ (blue curves) for varying attacker power ($P_{Att}$) for $K_{Att}$=1 relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for SNR= 9, 12, 15, and 20dB.*

Since the adversary has a limited power budget, we assume that the adversary keeps the total integrated power the same across the two possible scenarios.

- *High-power few signals:* Fig. 14 for $K_{Att} = 1$, 2 and Fig. 16 demonstrate the impact of a high-power attacker with only a single or a few adversarial signals on the QAIC performance. When the total attacker power for $K_{Att} = 1$ is equal to the total signal power for $K_0 = 3$ desired signals, $P_D$ starts to degrade and flattens around 90% due to the increased number of signals from 3 to 4 to recover with $8I/Q$ incoherent measurements. $P_D$ of the desired signals remain at practically usable levels. Fig. 15 for $K_{Att} = 1$ and 2 illustrates the impact of the same high-power attacker with only a few signals on the MWC performance.

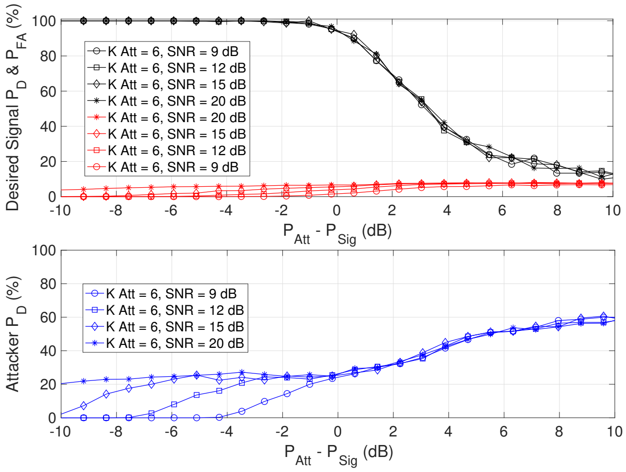

**Fig. 17:** ***CS QAIC*** *performance under an adversarial environment with varying number of attacker signals for a constant adversary power budget. Top plot shows the desired signal detection probability $P_D$ (black curves) and false alarm probability $P_{FA}$ (red curves) and bottom plot shows the attacker $P_D$ (blue curves) for varying attacker power ($P_{Att}$) for $K_{Att}$=6 relative to desired signal power ($P_{Sig}$) for $K_0 = 3$ for SNR= 9, 12, 15, and 20dB.*

The main difference between the CS QAIC and MWC performance in an adversarial condition is the additional 9.1dB SNR degradation of the MWC. As shown in Fig. 15, the CS MWC requires a 21dB SNR to provide the same performance under an attack in contrast to the CS QAIC requiring a 12dB SNR shown in Fig. 14.

- *Low-power large number of signals:* Fig. 14 for $K_{Att} = 3$ to 6 and Fig. 17 illustrate a more dangerous attack when a large number of low-power adversarial signals exist. For example, if we consider the $K_{Att} = 3$ case for the QAIC, when the total attacker power is only a few dB above the signal power, $P_D$ drastically degrades and stays around $50\%$ since there are only 8I/Q measurements and that is the theoretical limit for the required number of branches as given in (3) for the successful detection of 3 signals. As shown in Fig. 17, if the attacker has 6 signals that utilizes the same attacker power budget as the single attacker, 6 lower power adversarial signals harm the spectrum sensor performance significantly. Under a malicious attack with a large number of low-power signals such as $K_{Att} = 6$, the QAIC and the MWC performance do not degrade gracefully anymore resulting in a complete break down as shown in Fig. 14 and Fig. 15 respectively. In addition to the unacceptable $P_D$ performance for the desired signals, both CS spectrum sensors also fail at detecting the attack which satisfies the Type-II adversary threat model. We discuss this attack scenario in detail next in Section IV-C.

### *C. Stealthy Interferer (Type-II Adversary)*

The second type of adversary is a stealthy interferer. This adversary aims to transmit without being detected by the spectrum sensors. For the attack scenarios discussed in Section IV-B, we also simulate and report the attacker detection probability (Attacker $P_D$) shown as bottom plots with blue curves for traditional spectrum sensors in Fig. 11, Fig. 13, and CS spectrum sensors in Fig 14 - Fig. 17. Each of the traditional spectrum sensors can locate the attacker with a $100\%$ detection probability when the attacker aims to harm the desired signal detection. However, for CS spectrum sensors such as MWC and QAIC, attackers can maintain their deniability while drastically degrading the desired signal $P_D$. As shown in Fig. 17, if the adversary generates six signals in the spectrum band of interest, CS spectrum sensors completely break down and provide unreliable results when the total attacker power is only a few dB above the signal power, e.g., $P_{Att} - P_{Sig} \geq 2dB$, regardless of how high the SNR is. Further, the adversary can transmit without being detected by a CS spectrum sensor (with a maximum $60\%$ detection probability) even when the total power budget for those six adversarial signals is significantly higher than the total power budget for the three desired signals, e.g., $P_{Att} - P_{Sig} \geq 8dB$ for the QAIC. Even at a high SNR of 21dB, MWC is vulnerable to a Type-II adversary with a large number of adversary signals, $K_{Att} > 4$, as shown in Fig. 15 bottom plot.

### *D. Countermeasures for CS Spectrum Sensors*

Traditional spectrum sensors are much more robust against attacks compared to the CS-based spectrum sensors. As demonstrated, the attack signals introduced had little effect on the performance of the sweeping spectrum scanner. The Nyquist-rate FFT-based spectrum sensor can be attacked due to the limit in its dynamic range over a wide instantaneous bandwidth, by introducing high-power attack signals along with the low-power signals. If a higher resolution ADC is employed, the adversary would have to invest a larger amount of power to cause similar levels of performance degradation.

CS spectrum sensors on the other hand present more serious security issues. A possible adaptive action in response to a Type-I DoS attack for CS spectrum sensors is to relax the threshold of recovery algorithms in the DSP. Hence, the CS AIC becomes blind to lower power signals and detects signals above the new threshold reliably with a high $P_D$ [17]. Another successful mitigation technique against this type DoS attack on the monitoring system might be to employ sparsity estimation with adaptive thresholding in DSP and hardware virtualization through time segmentation to avoid system failure [17]. Sparsity estimation technique takes advantage of the residual information provided by the OMP algorithm in DSP. Monitoring the residual allows the CS spectrum sensor to lower the detection threshold adaptively. If the residual is high, the CS spectrum sensor increases the time-segmented measurements through hardware virtualization for successful detection of the additional signals below the threshold level at the expense of increased scan time [17]. Further, sparsity estimation through the OMP residual monitoring [17] might be a useful technique for attacker detection against Type-II adversary.

## V. Conclusions

The paper presents a security evaluation platform for wideband spectrum sensors. We discuss the trade-offs between security and sensor performance in terms of energy efficiency and scan time for traditional spectrum sensors and compressed-sensing architectures. Models for end-to-end system evaluation are developed for traditional spectrum analysis methods such as sweeping spectrum scanners and

Nyquist-rate FFT-based spectrum sensors and also for CS spectrum sensors such as the MWC [6] and the QAIC [15]. These models are first analyzed in order to demonstrate their operation and performance in terms of detection ($P_D$) and false alarm ($P_{FA}$) probabilities under a non-adversarial environment with varying wireless channel noise conditions.

Since the goal of this work is to assess the security vulnerabilities of these spectrum sensors, we secondly introduce two threat models for denial of service (DoS) attacks and stealthy interferers who aim to maintain deniability. These adversary types are modeled with varying number of attacker signals and power budgets to illustrate the effectiveness of the attacks on the detection and false alarm probabilities performance of the wideband spectrum sensors.

Sweeping spectrum scanners are inherently secure against these adversary models due to their small instantaneous BW equal to their RBW and high dynamic range. On the other hand, Nyquist-rate FFT-based spectrum sensors are only vulnerable against the high-power DoS attacks due to their wide instantaneous bandwidth and limited dynamic range. However, both of the traditional spectrum sensors typically have a high energy consumption due to their long scan time or high power consumption.

CS spectrum sensors have been proposed as fast and low energy-consuming alternatives for wideband spectrum sensing. The CS spectrum sensors rely on the sparsity of the spectrum. In this paper, we show that existing architectures, such as MWC and QAIC which are architected with a fixed sparsity assumption, are vulnerable to DoS attacks and stealthy interferers. Recent compressed-sensing techniques proposed in [17], such as sparsity estimation by monitoring the residual of the CS OMP algorithm and increasing the number of incoherent measurements through time segmentation, might be useful for attacker detection and providing physical-layer security against the DoS attacks considered in this paper, albeit at the expense of increased scan time and energy consumption. The evaluation of these new CS spectrum sensing techniques in various adversarial contexts represents an interesting area for future work.

## References

[1] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," 1999 IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99), San Diego, CA, USA, 1999, pp. 3-10.

[2] L. Falconetti et al., "Design and evaluation of licensed assisted access LTE in unlicensed spectrum," IEEE Wireless Communications, vol. 23, no. 6, pp. 24-30, Dec. 2016.

[3] K. Entesari and P. Sepidband, "Spectrum Sensing: Analog (or Partially Analog) CMOS Real-Time Spectrum Sensing Techniques," IEEE Microwave Magazine, vol. 20, no. 6, pp. 51-73, June 2019.

[4] E. J. Candés and M. B. Wakin, "An Introduction To Compressive Sampling," in IEEE Signal Processing Magazine, vol. 25, no. 2, pp. 21-30, March 2008.

[5] D. Donoho, "Compressive sensing," IEEE Transactions on Information Theory, vol. 52, no. 4, pp. 1289-1306, 2006.

[6] M. Mishali and Y. C. Eldar, "From Theory to Practice: Sub-Nyquist Sampling of Sparse Wideband Analog Signals," IEEE Journal of Selected Topics in Signal Processing, vol. 4, no. 2, pp. 375-391, April 2010.

[7] R. T. Yazicigil, T. Haque, P. R. Kinget and J. Wright, "Taking Compressive Sensing to the Hardware Level: Breaking Fundamental Radio-Frequency Hardware Performance Tradeoffs," IEEE Signal Processing Magazine, vol. 36, no. 2, pp. 81-100, March 2019.

[8] R. Chen, J. Park and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, Phoenix, AZ, 2008, pp. 1876-1884.

[9] A. S. Rawat, P. Anand, H. Chen and P. K. Varshney, "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks," in IEEE Transactions on Signal Processing, vol. 59, no. 2, pp. 774-786, Feb. 2011.

[10] G. Ding et al., "Robust Spectrum Sensing With Crowd Sensors," in IEEE Transactions on Communications, vol. 62, no. 9, pp. 3129-3143, Sept. 2014.

[11] R. Chen, J. Park and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," in IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 25-37, Jan. 2008.

[12] J. Park, J. H. Reed, A. A. Beex, T. C. Clancy, V. Kumar and B. Bahrak, "Security and Enforcement in Spectrum Sharing," in Proceedings of the IEEE, vol. 102, no. 3, pp. 270-281, March 2014.

[13] T. C. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), Singapore, 2008, pp. 1-8.

[14] G. Jakimoski and K. P. Subbalakshmi, "Denial-of-Service Attacks on Dynamic Spectrum Access Networks," ICC Workshops - 2008 IEEE International Conference on Communications Workshops, Beijing, 2008, pp. 524-528.

[15] R. T. Yazicigil, T. Haque, M. R. Whalen, J. Yuan, J. Wright and P. R. Kinget, "Wideband Rapid Interferer Detector Exploiting Compressed Sampling With a Quadrature Analog-to-Information Converter," IEEE Journal of Solid-State Circuits, vol. 50, no. 12, pp. 3047-3064, Dec. 2015.

[16] T. Haque, R. T. Yazicigil, K. J. Pan, J. Wright and P. R. Kinget, "Theory and Design of a Quadrature Analog-to-Information Converter for Energy-Efficient Wideband Spectrum Sensing," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 62, no. 2, pp. 527-535, Feb. 2015.

[17] R. T. Yazicigil, T. Haque, M. Kumar, J. Yuan, J. Wright and P. R. Kinget, "How to Make Analog-to-Information Converters Work in Dynamic Spectrum Environments With Changing Sparsity Conditions," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 65, no. 6, pp. 1775-1784, June 2018.

[18] Z. Qin, J. Fan, Y. Liu, Y. Gao, and G. Y. Li, "Sparse representation for wireless communications: A compressive sensing approach," IEEE Signal Processing Magazine, vol. 35, no. 3, pp. 40-58, 2018.

[19] M. Mishali and Y. C. Eldar, "Blind multiband signal reconstruction: Compressed sensing for analog signals," IEEE Transactions on Signal Processing, vol. 57, no. 3, pp. 993-1009, 2009.

[20] J. E. Salt and H. H. Nguyen, "Performance Prediction for Energy Detection of Unknown Signals," in IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3900-3904, Nov. 2008.

[21] M. S. Oude Alink, E. A. M. Klumperink, M. C. M. Soer, A. B. J. Kokkeler and B. Nauta, "A 50Mhz-To-1.5Ghz Cross-Correlation CMOS Spectrum Analyzer for Cognitive Radio with 89dB SFDR in 1Mhz RBW," 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN), Singapore, 2010, pp. 1-6.

[22] A. Goel, B. Analui and H. Hashemi, "A 130-nm CMOS 100-Hz-6-GHz Reconfigurable Vector Signal Analyzer and Software-Defined Receiver," in IEEE Transactions on Microwave Theory and Techniques, vol. 60, no. 5, pp. 1375-1389, May 2012.

[23] S. Pollin et al., "Digital and Analog Solution for Low-Power Multi-Band Sensing," 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN), Singapore, 2010, pp. 1-2.

[24] E. Candés and T. Tao, "Robust uncertainty principles: Signal reconstruction from highly incomplete frequency information," IEEE Transactions on Information Theory, vol. 52, no. 2, pp. 489-509, 2006.

[25] T. Zhang, "Sparse Recovery With Orthogonal Matching Pursuit Under RIP," in IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 6215-6221, Sept. 2011.

[26] J. A. Tropp and A. C. Gilbert, "Signal Recovery From Random Measurements Via Orthogonal Matching Pursuit," in IEEE Transactions on Information Theory, vol. 53, no. 12, pp. 4655-4666, Dec. 2007.

[27] D. Donoho, "For most large underdetermined systems of equations, the minimal $l_1$ norm near solution approximates the sparsest solution," Communications on Pure and Applied Mathematics, vol. 59, no. 7, pp. 907-934, 2006.

[28] Deanna Needell and Joel A. Tropp, "CoSaMP: iterative signal recovery from incomplete and inaccurate samples," Communications of the ACM, vol. 53, no. 12, pp. 93-100, Dec. 2010.

[29] D. Adams, Y. C. Eldar, and B. Murmann, "A mixer front end for a four-channel modulated wideband converter with 62-dB blocker rejection," IEEE Journal of Solid-State Circuits, vol. 52, no. 5, pp. 1286-1294, May 2017.

[30] R. L. Pickholtz, D. Shilling, and L. B. Milstein, "Theory of spread-spectrum communications - A tutorial," IEEE Transactions Communications, vol. 30, no. 5, pp. 855-884, 1982.