UNIVERSITÀ DEGLI STUDI
DI GENOVA

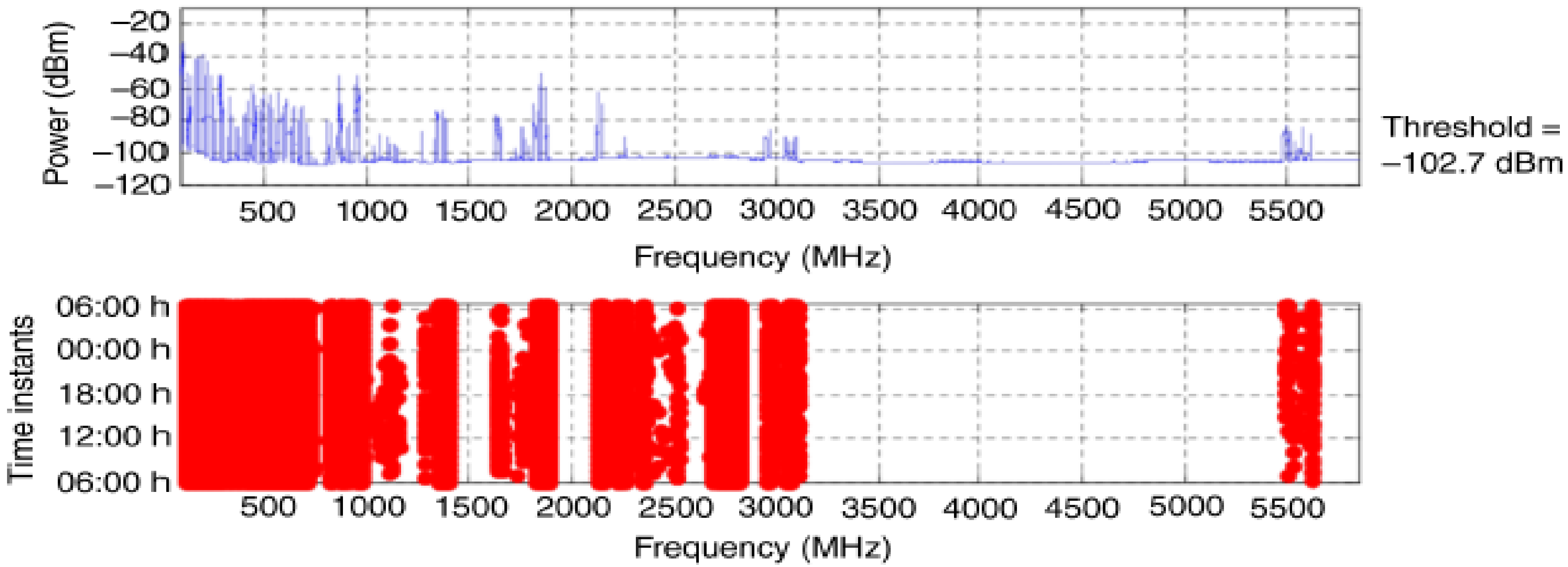
Defense against Stealthy Jamming Attacks in Wide-band Radios- A Physical Layer Approach

T. Nawaz*, L. Marcenaro and C. S. Regazzoni

Department of Electrical, Electronic, Telecommunications Engineering and Naval Architecture – DITEN
University of Genova, Italy.

Email: tassadaq.nawaz@ginevra.dibe.unige.it

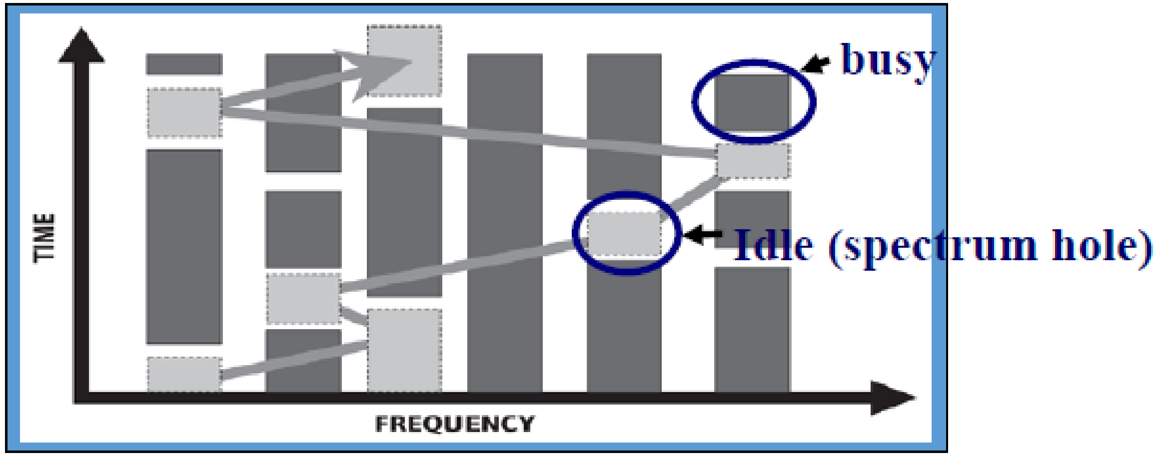
Why Cognitive Radio?



Spectrum utilization from 30 MHz to 6 GHz in Singapore.

Cognitive Radio [1, 2]

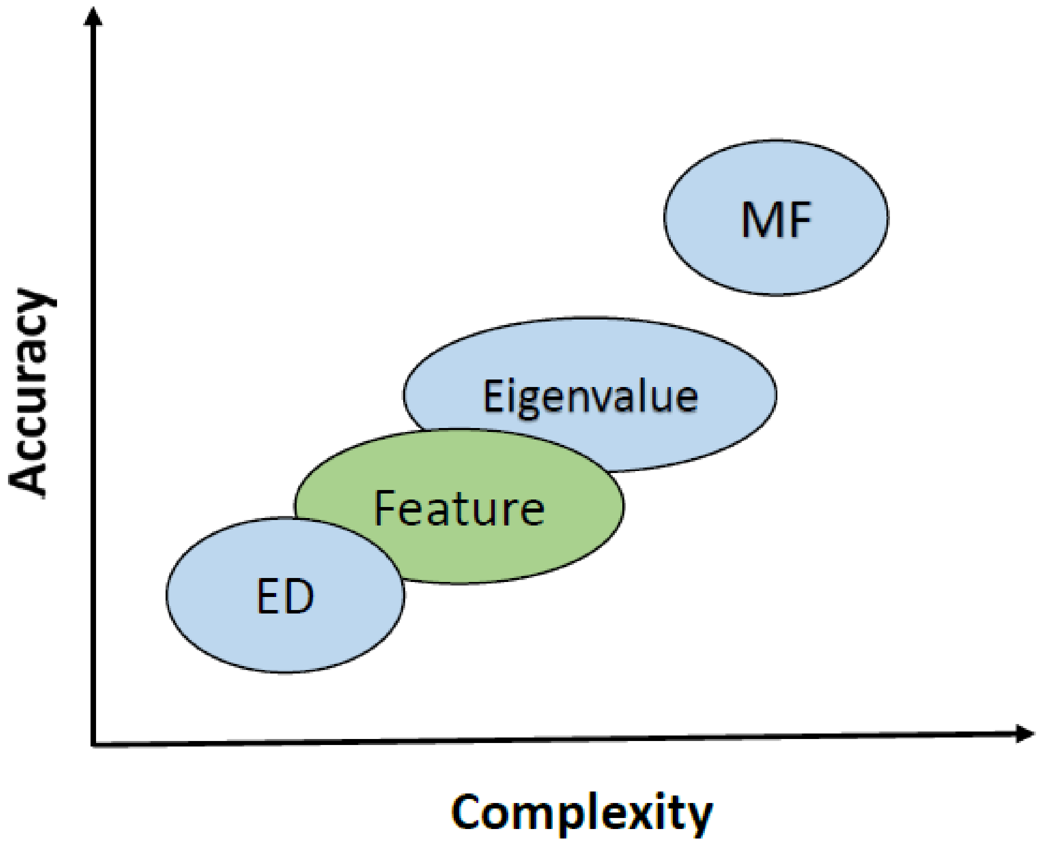
- Spectrum scarcity



- Cognitive radio
  - Environment awareness and spectrum intelligence
- Applications
  - Dynamic spectrum access
  - Communication electronic warfare solutions

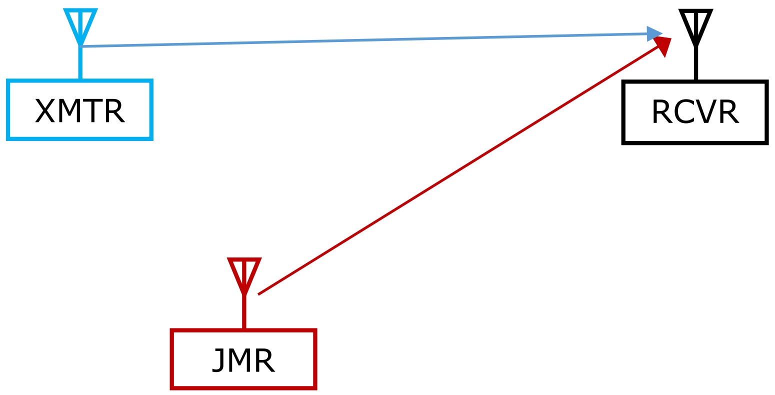
Spectrum Sensing Techniques [3, 4]

- Matched Filter
  - Perfect knowledge
  - Dedicated receiver architecture
- Eigenvalue Detection
  - Max-Min eigenvalues
  - Computational complexity
  - Difficulty to threshold selection
- Feature Detection
  - Cyclostationary property
  - Complex processing algorithm
- Energy Detection
  - Simple implementation
  - Poor performance



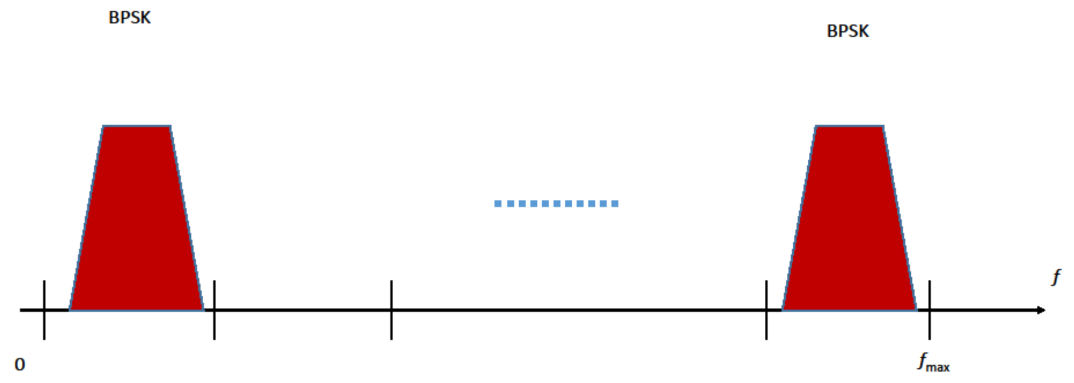
RF Jamming [13, 14]

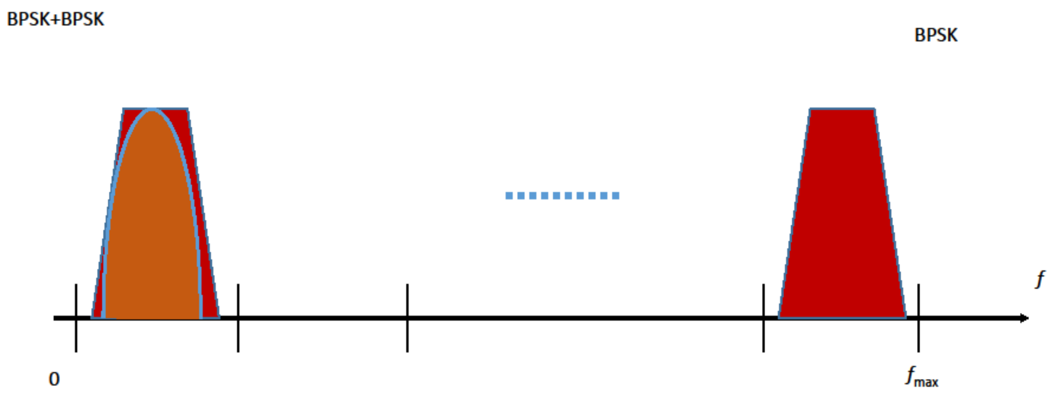
- Illegitimate RF transmission with the objective of causing maximum distortion to the communication of the targeted system.
- CR technology has enabled devising and deploying of more advanced, self-reconfigurable jamming and anti-jamming solutions.



Problem Formulation

- Wideband spectrum
- Occupied by various narrowband waveforms
- Narrowband jammer





Stealthy Jammer [17, 18]

- Equiped with sensing capability
- Adaptive

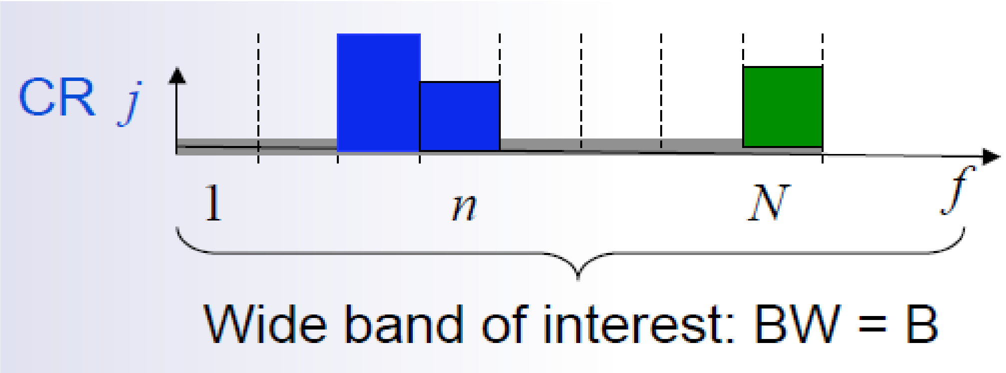
OPTIMAL JAMMING SIGNALS IN A COHERENT SCENARIO

Victim Signal	Modulation scheme of pulsed jamming signal
BPSK	BPSK
QPSK	QPSK
4-PAM	BPSK
16-QAM	QPSK

Compressed Sensing [8,10]

- Conventional spectral estimation methods require to operate at or above Nyquist rate
- Requires high rate A/D or bank of low rate A/D for wideband signals
- Compressed Sampling: sub-Nyquist rate sampling and reliable signal recovery via computationally feasible algos
- Applicable to sparse signals

Limits on Sampling Rates [9,11]

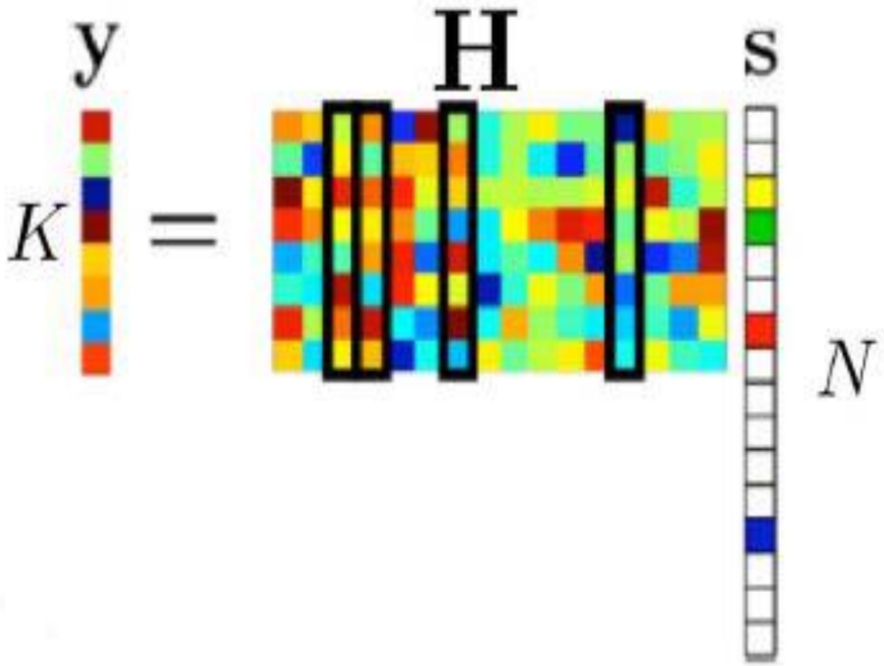


Spectrum occupancy ratio
$$r_{nz} = N_{nz}/N \ll 1$$

- Lower bounds on sampling rates f_s
  - Lowest f_s for reconstruction without aliasing
    - Nyquist Rate = 2B
- Lowest f_s for reconstruction of CR signals
  - Motivating factor for CR is low spectrum utilization
  - Landau rate = $2B_{eff} = 2r_{nz}B < Nyquist\ Rate$

Compressed Sensing Basics

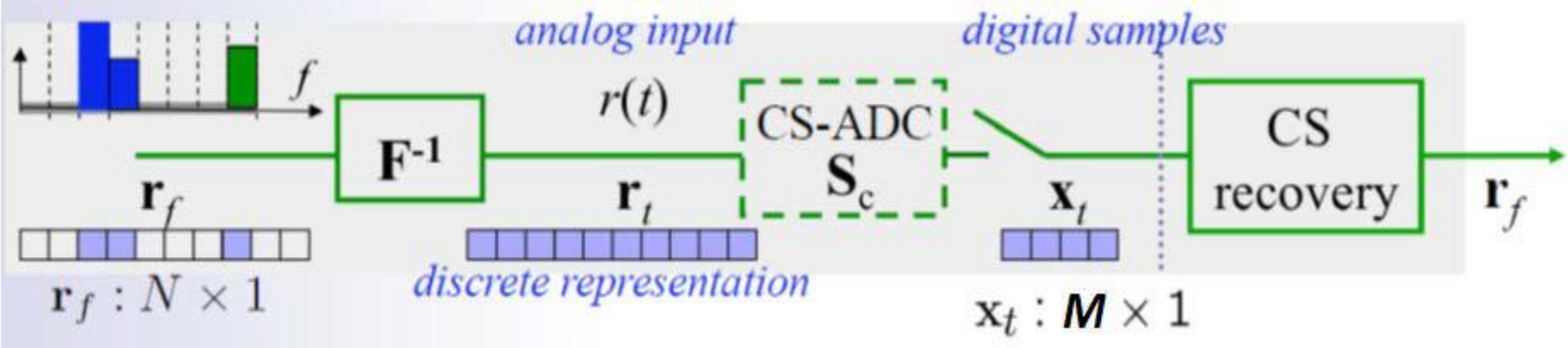
- Y=$\boldsymbol{H}_{K\times N}\boldsymbol{S}$



- **S** should be sparse
- **H** can be fat ($K \leq N$)

- Compressed Sensing
  - Given Y and H, unknown S can be found with high probability!

Sub-Nyquist rate Sampling [10, 22]



- Received signal: $r(t): t \in [0, NT_s]$
  - Discrete representation: $\boldsymbol{r}_t \leftrightarrow \boldsymbol{r}_f = \mathbf{F}\boldsymbol{r}_t$
- Linear Sampling: $\mathbf{X}_t = \mathbf{S}_c\mathbf{r}_t = \mathbf{S}_c\mathbf{F}^{-1}\mathbf{r}_f$
  - Compression: $S_c : K \times N$

Sub-Nyquist rate Sampling [20]

- Estimation is achieved by solving the following convex optimization problem:

$$\arg\min_{\boldsymbol{r}_f} \| \boldsymbol{r}_f \|_1, \qquad s.t. \quad \mathbf{X}_t = \mathbf{S}_c \mathbf{F}^{-1} \mathbf{r}_f$$

- Techniques to solve the above problem:
  - Linear Programming: Basis Pursuit
  - Iterative greedy algorithms: Maching Pursuit and orthognal Maching Pursuit

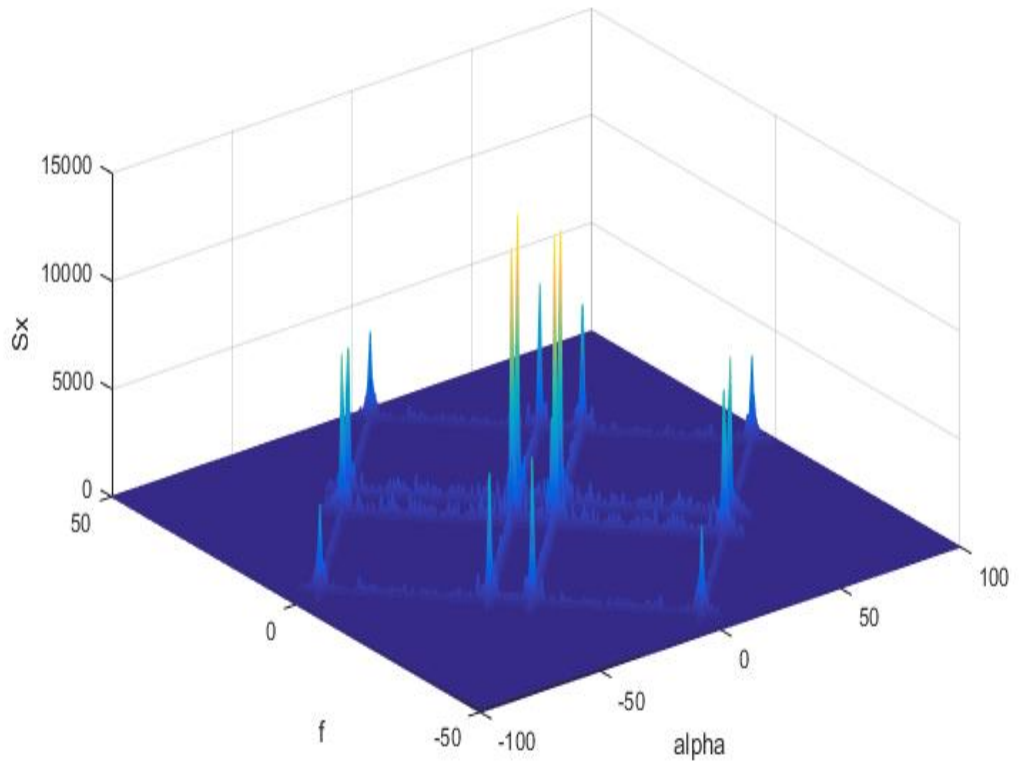
The I_n-norm of x is defined as:

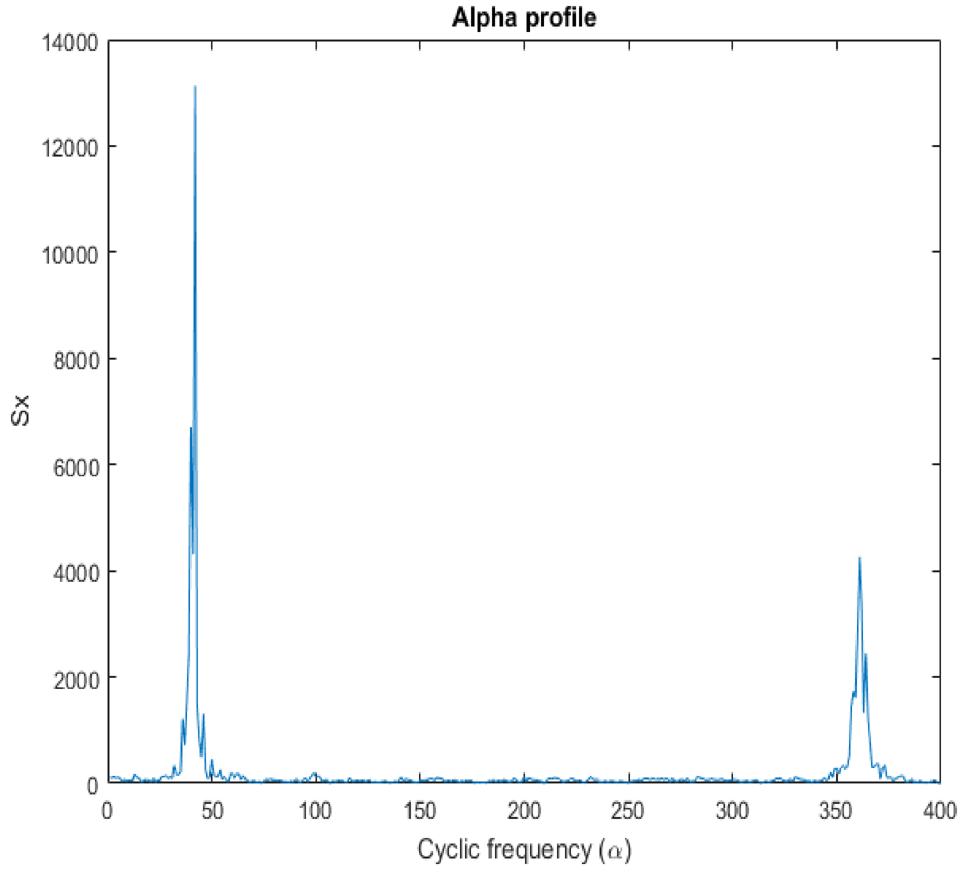
$$\| x \|_n = \sqrt[n]{\sum_i |x_i|^n}$$

Cyclostationary Spectral Analysis [4]-[7]

- Good performance at medium-to-low SNRs
- Higher implementation complexity than EDs
- Cyclostationarity of the modulated signals
- The Fourier Transform of the cyclic autocorrelation function is known as spectral correlation function (SCF)
- Furthermore, different types of modulated signals (BPSK, AM, FSK, MSK, QAM, PAM) with overlapping power spectral densities have highly distinct SCFs.
- AWGN is WSS and has no cyclic correlations

Spectral Correlation Function and Alpha Profile

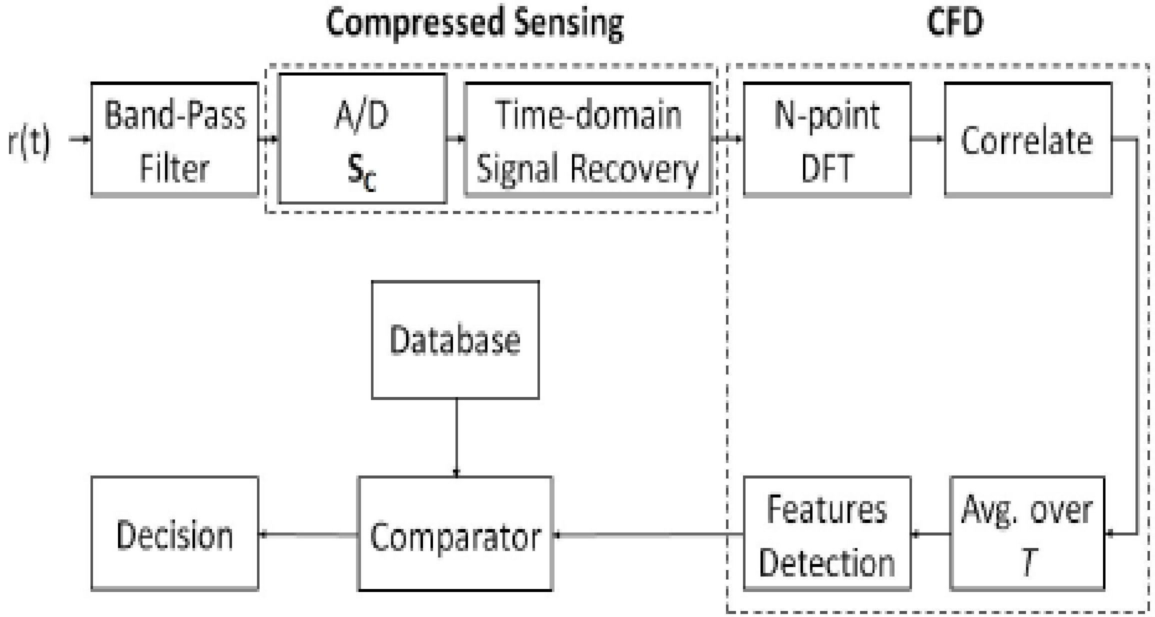




Proposed Algorithm

Algorithm 1 Pseudo-code for proposed algorithm

```
function JAMMER DETECTOR
    Initialise all SB states to "free"
    Receive the WB signal
    Set compression rate  K/N
    Construct the measurement matrix  Sc
    Estimate the WB from compressed samples using BP
    Compute the SCF of estimated WB signal
    Extract the α profile from SCF
    Divide WB into i SBs
    for i = 1 to I, do
        Access the database
        Compare parameters with the database waveforms
        Decision ← Licit or Jammer
    end for
end function
```

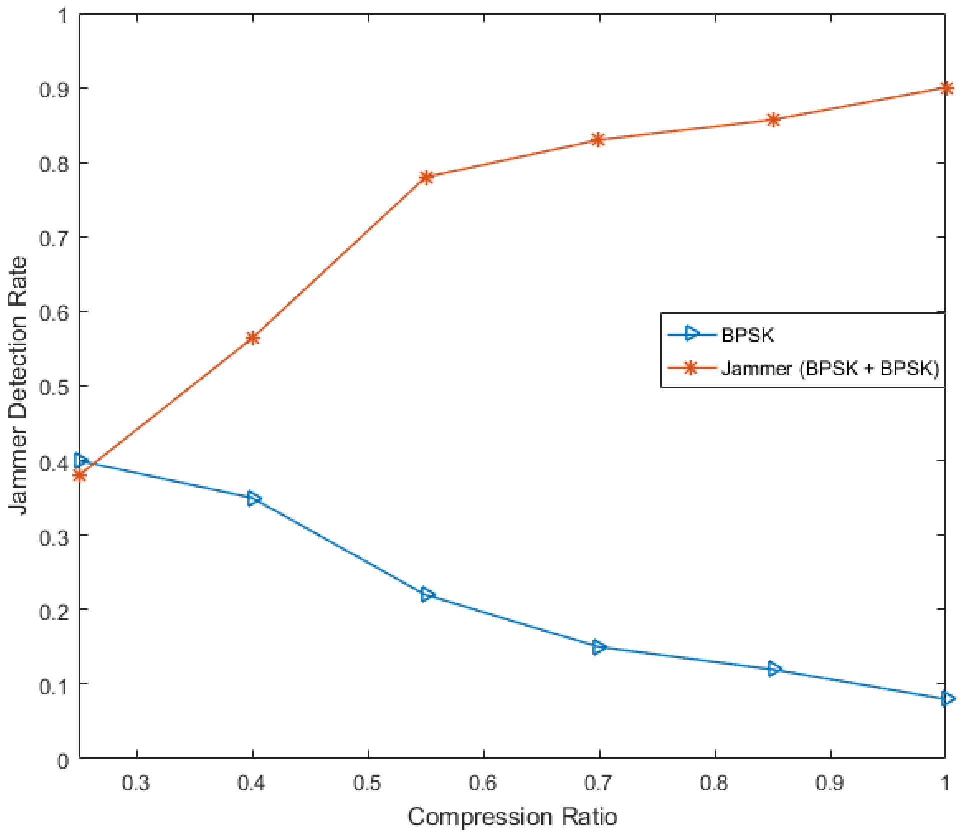


Experimental Setup

- Wideband spectrum of 500 ΔHz
- 5 sub-bands of 100 ΔHz
- Legit waveform = BPSK / QPSK
- Jamming signal = BPSK / QPSK
- SNR = 0 dB
- 1000 Monte-Carlo runs
- Test scenarios
  - Sub-band 1 and sub-band 5 has legit signal
  - Sub-band 5 has legit signal
    - Sub-band 1 has legit + stealthy jamming signal
  - Sub-band 1 has legit signal
    - Sub-band 5 has legit + stealthy jamming signal

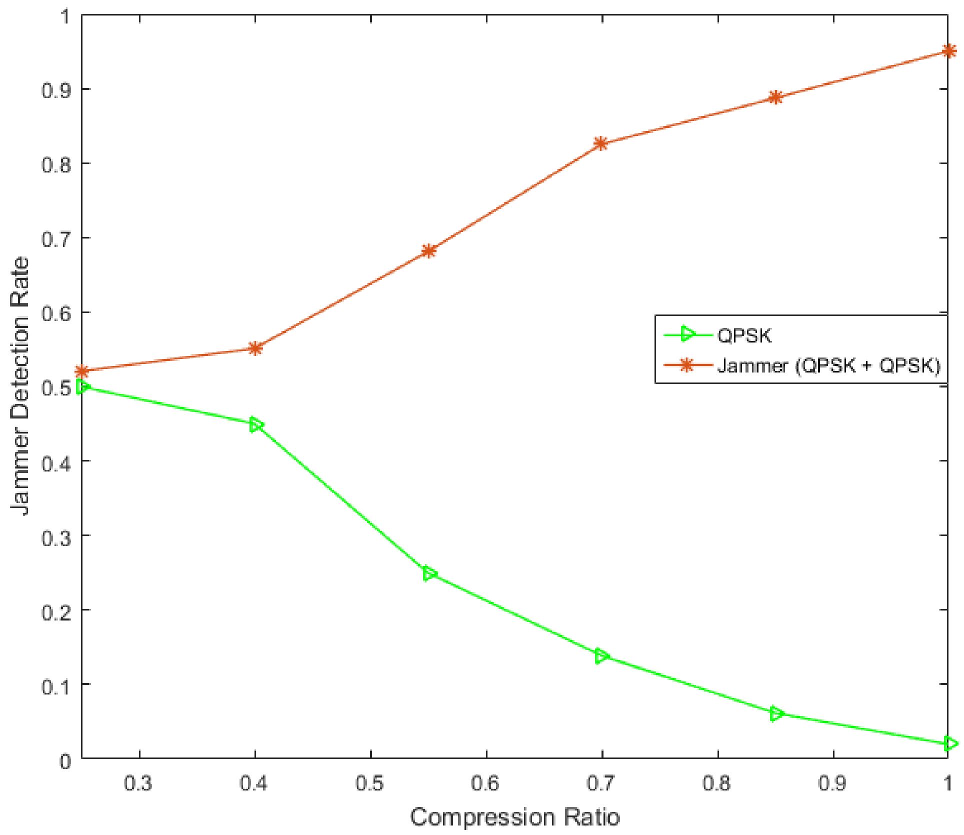
Experimental Results

Test Case 1:
SB-1 and SB-5 are used by BPSK signals and jammer target licit signal in SB-1 .



Experimental Results

Test Case 2:
The licit users changed modulation scheme to QPSK in SB-1 and SB-5 and jammer target licit signal in SB-1 .



Conclusion and Future Work

- A stealthy jammer detection algorithm was proposed for wide-band cognitive radios using compressed sensing.
- Performance gain compare to common methods of signal classification, which needs 10 dB to 20 dB for comparable classification rate [23].
- Proposed algorithm performs good within some limitations:
  - Plain database comparison.
  - Requirement to maintain databases.
- Future works may include:
  - Artificial Neural network classifiers
  - Dataset for PHY-Layer security.
  - Jammer with different capabilities.

Thanks for your Attention

Suggestions / Questions