Signal Classifiers using Self-Organizing Maps "Performance & Robustness"

Awais Khawar, Charles Clancy

Electrical and Computer Engineering

University of Maryland

Spectrum Sensing & PUE

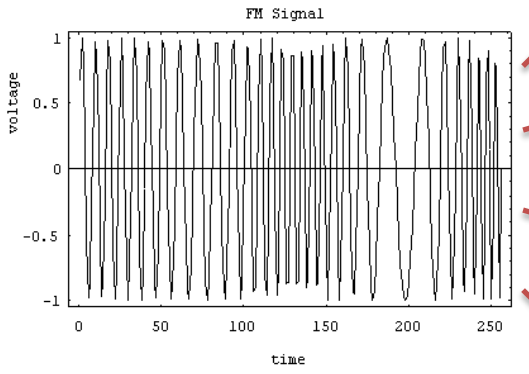
- Major driver: dynamic spectrum access
- Seeks to answer:
  - Which bands are occupied?
  - Are the occupants primary or secondary users?
- Greedy secondary devices seek to cause misclassification
  - Detected as primary rather than secondary
  - Other secondary users vacate the band; more resources to greedy secondary user
  - *Primary User Emulation* (PUE) attack

Techniques for Spectrum Sensing

- Power Statistic (energy detection)
- Time-domain
  - Matched filter
  - Temporal statistics
  - High-order moments and cumulants
- Frequency-domain
  - Spectral mask (frequency-domain matched filter)
  - Cyclostationary statistics

Generalized Approach

- Extract features from signal, and perform template matching on them using classification engine



Feature Extraction

Feature Vector

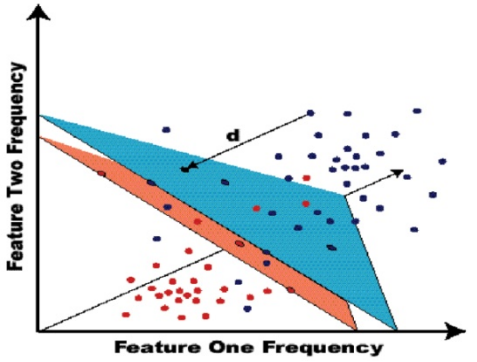
Classification

Var(Amplitude) → 1.2

Var(Phase) → 0.5

Kurtosis(Amplitude) → 2.1

Kurtosis(Phase) → 0.2



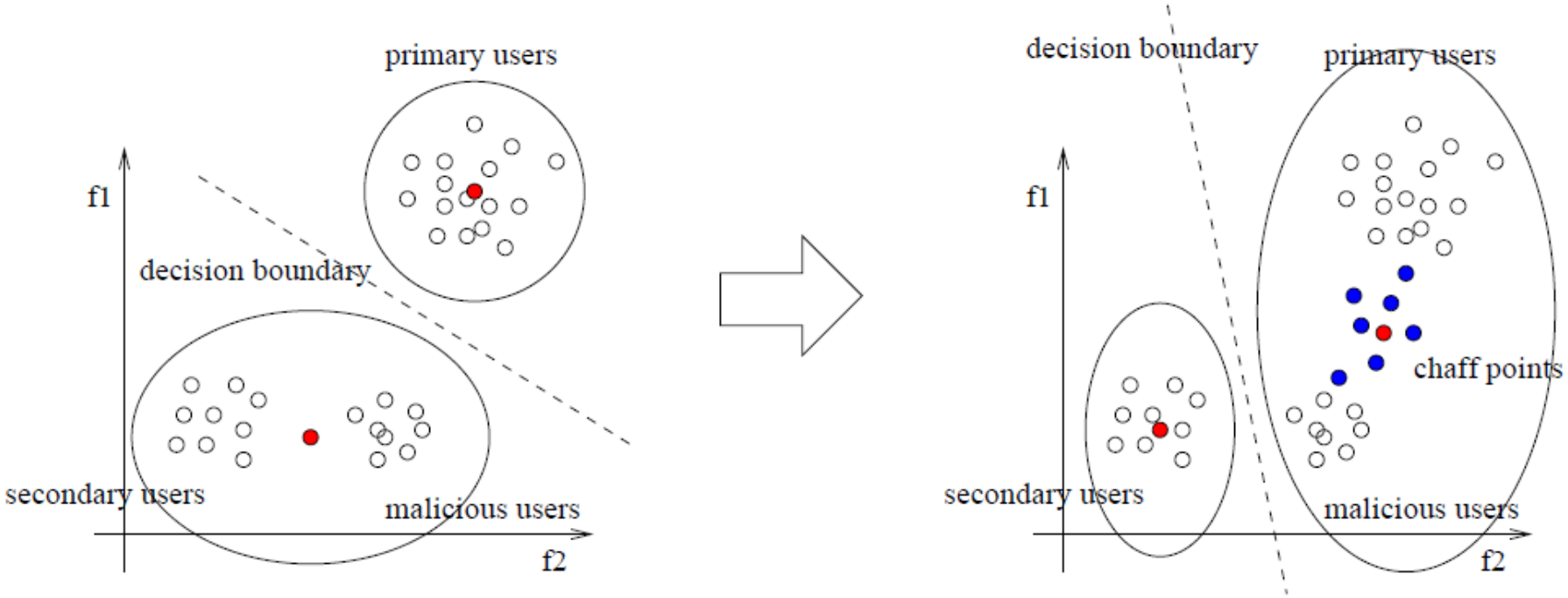
Neural Nets,
SVMs, HMMs, etc

Unsupervised Learning

- In radio environment, want to be able to evolve and adapt classifier for unique and previously-unencountered signals
- Continuously update statistics given new exemplar data
- Basic approach: K-Means Clustering
  - Requires storing significant state information (all previous feature vectors)
- Modern approach: Self-Organizing Maps

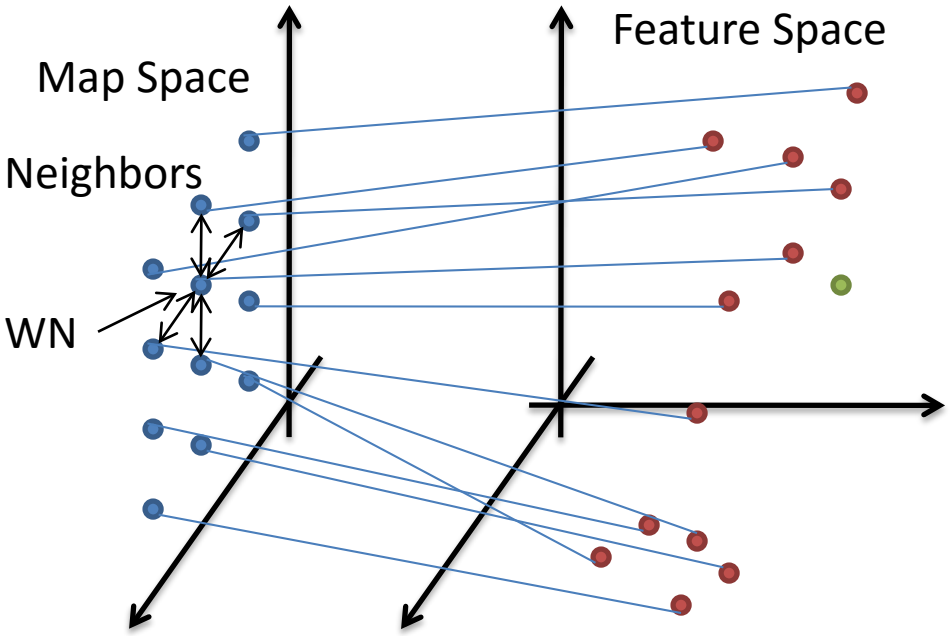
Dangers of Unsupervised Learning

- Attacker has ability to redraw decision boundary in its favor using chaff points
- Example using K-Means Clustering:



Self-Organizing Maps

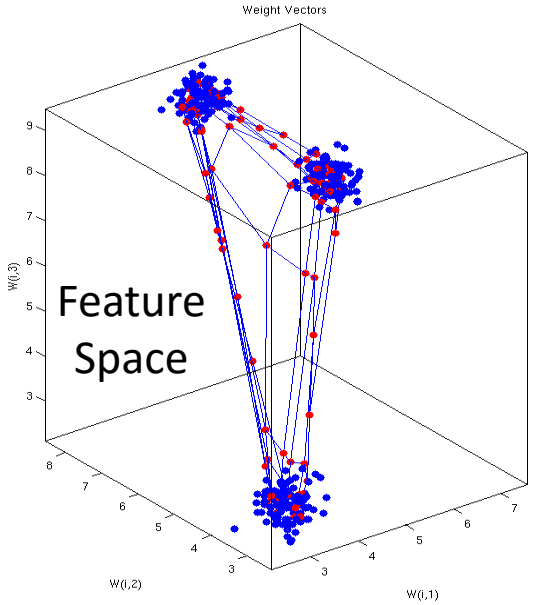
- Neurons map “feature” space to “map” space
  - Have fixed position in 1-D or 2-D map space
  - Positions in feature space converge to fit input data
  - Projection of feature space into fewer dimensions

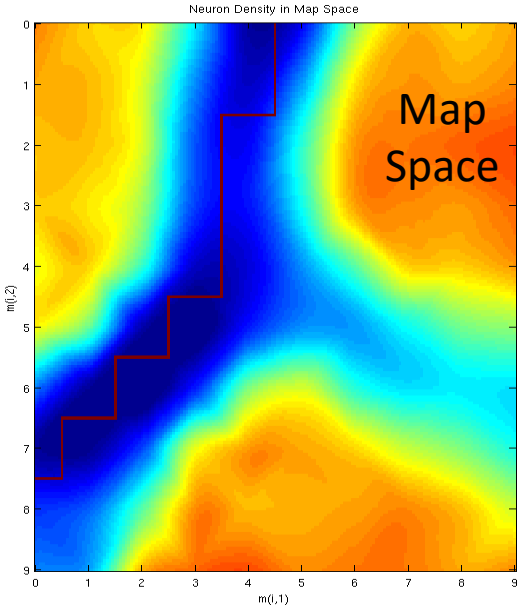


- For each input data sample:
  - Find closest neuron in feature space
  - Move it toward data point
  - Move neuron map-space neighbors closer in feature space to input point
  - System parameters control magnitude of changes, damp behavior

Decision Boundaries

- Example: self-organizing map trained with data from 3 probability distributions

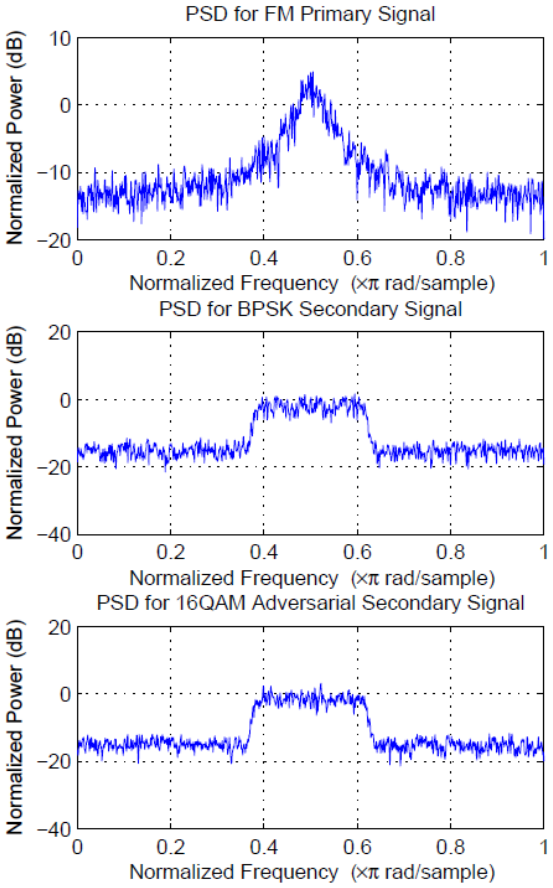


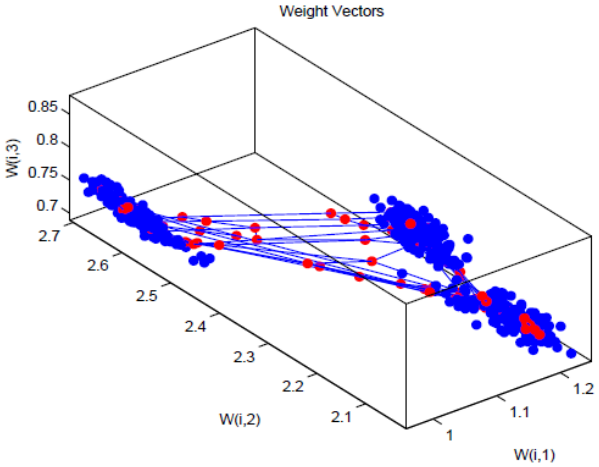


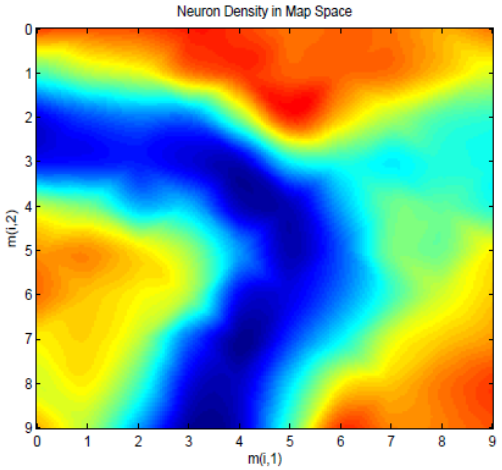
Neuron Density Plot
- log(average neighbor distance in weight space)

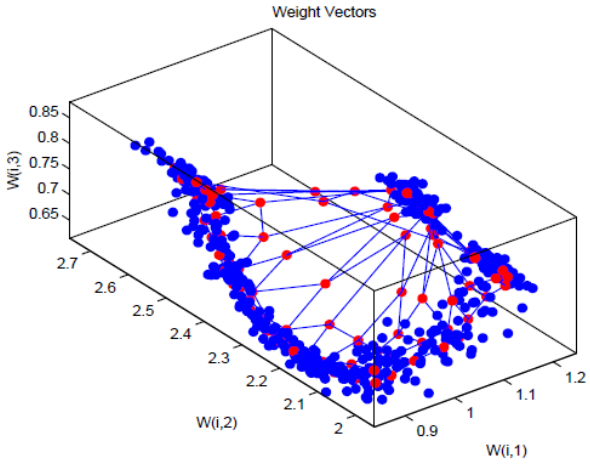
- Decision boundary drawn in map space using neuron densities: K-Means clustering and hierarchical clustering tested

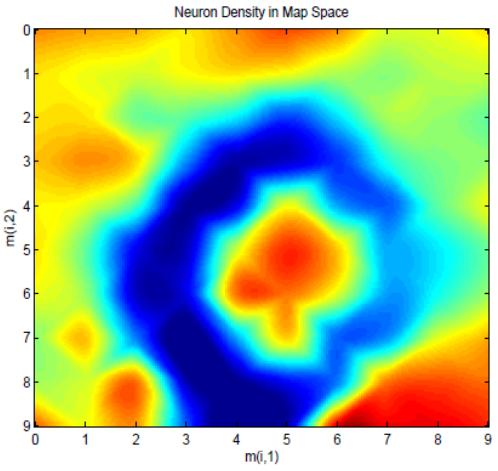
Attack Using Simulated Signals





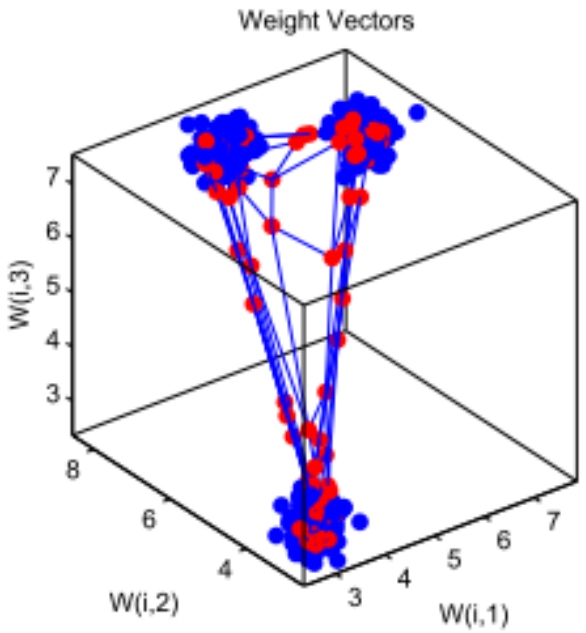


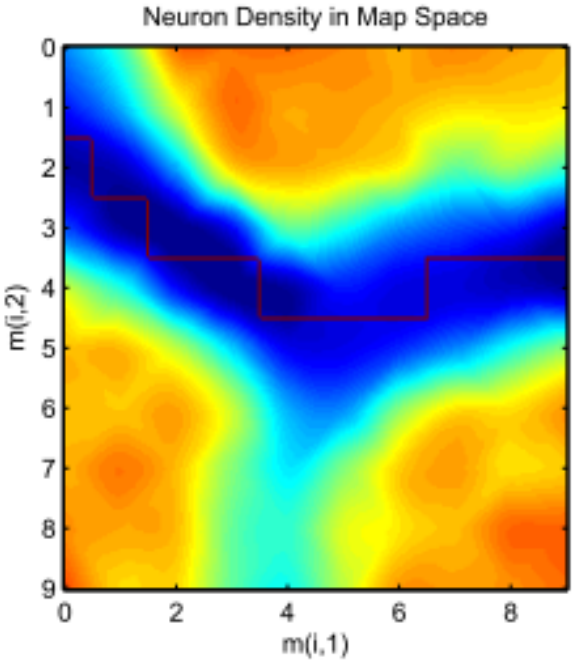




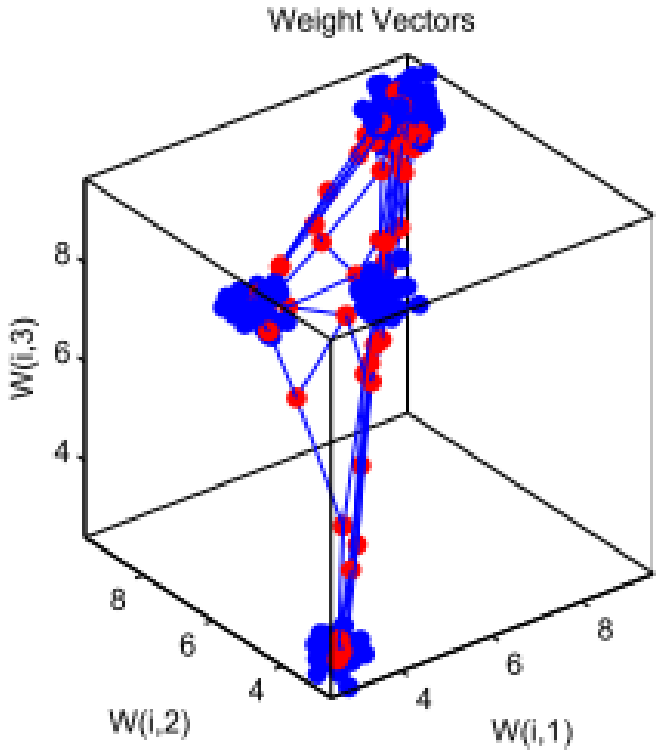
Features: std(x(t)), std(lpf(x(t))), std(x(t+1)-x(t))

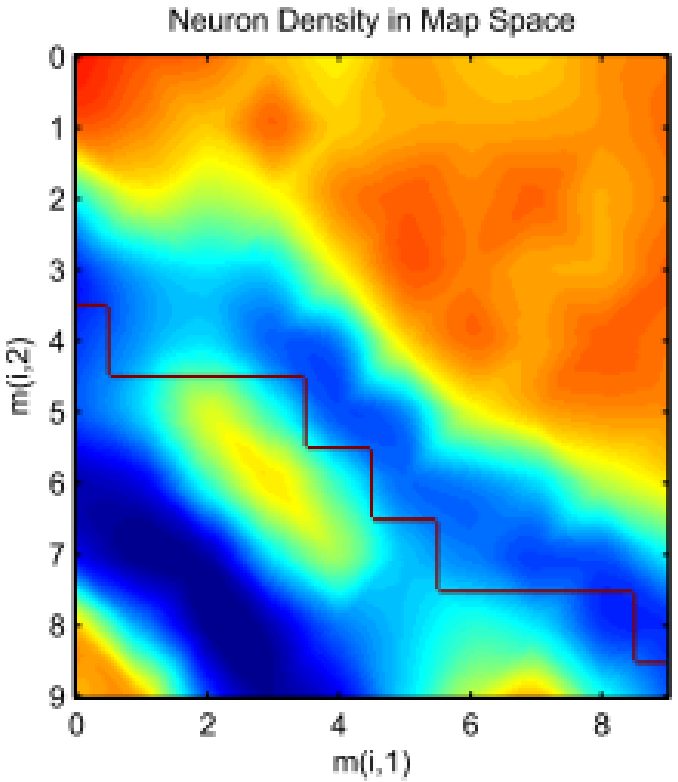
Weight vectors and neuron densities for adjacent adversaries without an attack present



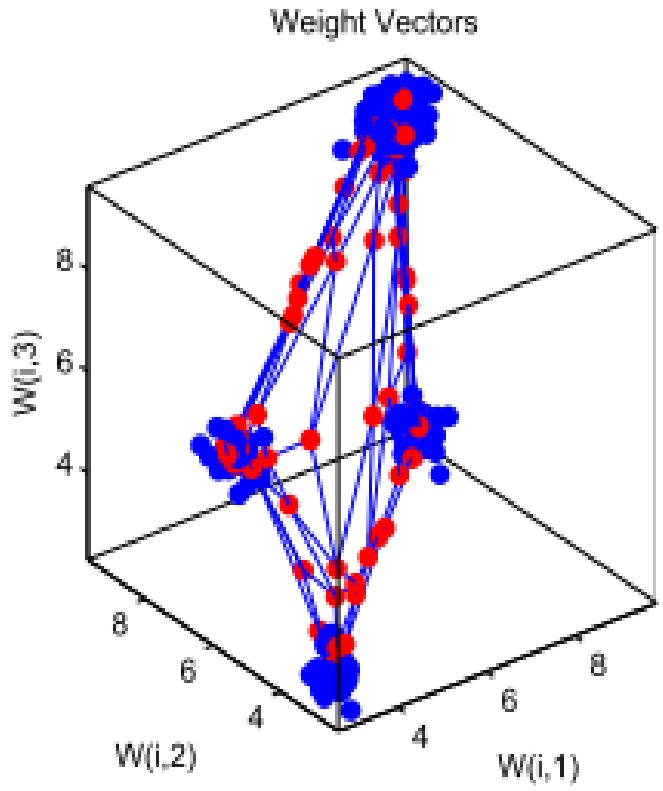


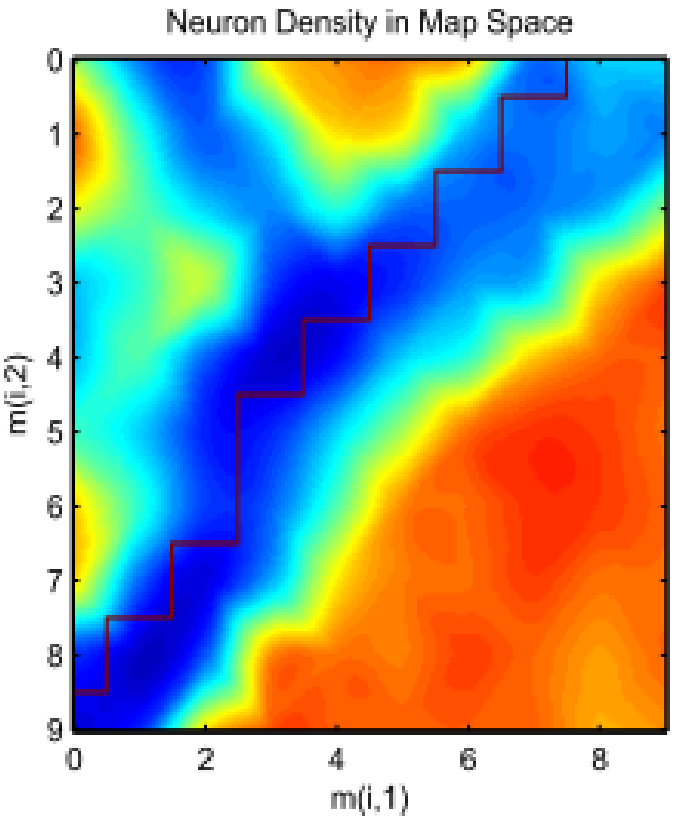
Weight vectors and neuron densities for adjacent adversaries under point cluster attack



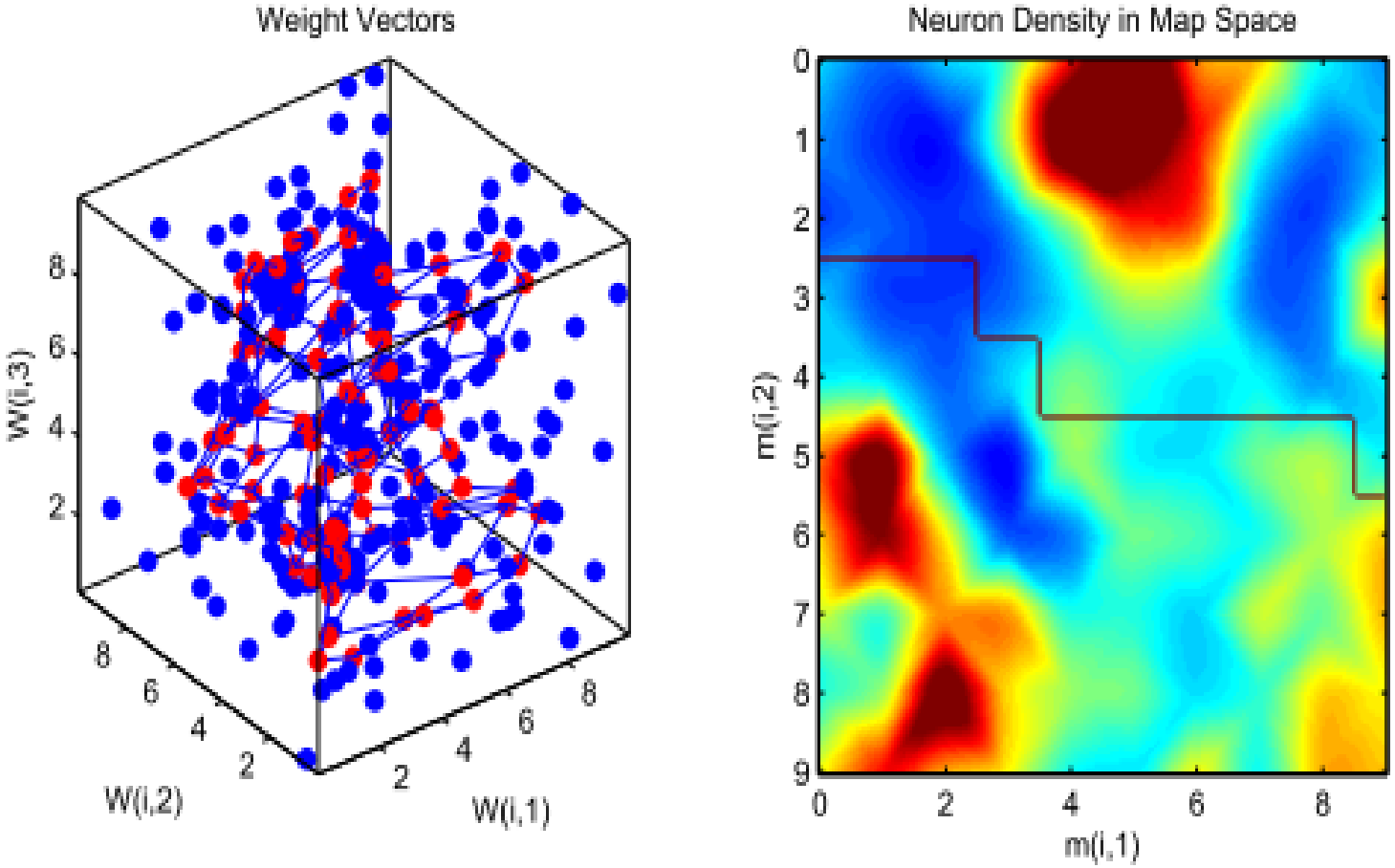


Weight vectors and neuron densities for equilateral adversaries under point cluster attack

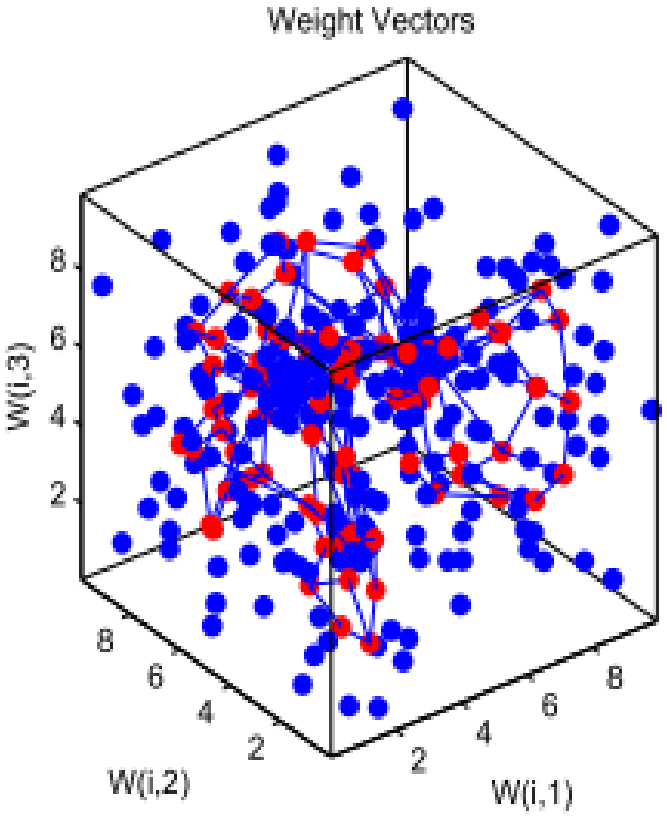


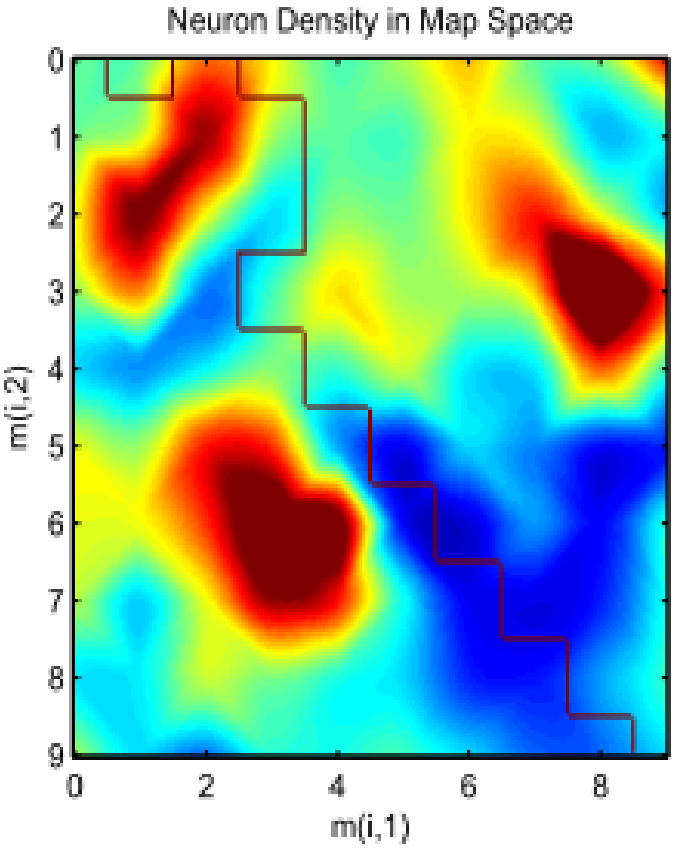


Weight vectors and neuron densities for adjacent adversaries under random noise attack



Weight vectors and neuron densities for equilateral adversaries under random noise attack





Error types and rates for different attack types using K-means clustering with adjacent adversaries

Error Type	None	Connect	Cluster	Noise
Pri→Sec	0	0	0	0
Sec→Pri	0	0	0.35	0
Adv→Pri	0	0	0.38	0

Error types and rates for different attack types using K-means clustering with equilateral adversaries

Error Type	None	Connect	Cluster	Noise
Pri→Sec	0	0	0	0
Sec→Pri	0.38	0.33	1	0.36
Adv→Pri	0.35	0.36	1	0.58

Error types and rates for different attack types using hierarchical clustering with adjacent adversaries

Error Type	None	Connect	Cluster	Noise
Pri→Sec	0	0	0	0
Sec→Pri	0	0	0.10	0.38
Adv→Pri	0	0	0.11	0.39

Error types and rates for different attack types using hierarchical clustering with equilateral adversaries

Error Type	None	Connect	Cluster	Noise
Pri→Sec	0	0	0	0
Sec→Pri	0.30	0.16	0.85	0.40
Adv→Pri	0.42	0.75	0.98	0.55

Adv→Pri error rates for different attack densities using hierarchical clustering with equilateral adversaries

Attack Type	Number of Chaff Points			
	0	**200**	**400**	**600**
Point Cluster	0	.91	.96	.98
Connectivity	.44	.52	.58	.81
Random Noise	.39	.46	.50	.54

Performance of Classification Algorithms under ‘No Attack’ with equilateral adversaries

Classification Algorithms	Pri→Sec	Sec→Pri	Adv→Pri
K-Means	0	0.56	0.30
Weighted	0	0.54	0.44
Average	0	0.84	0.16
Complete	0	0.90	0.10
Single	0	0.68	0.56
Yard	0	0.70	0.30

Future Work

- Exploring other signal classifiers & decision boundary algorithms
- Use of different modulation schemes

Conclusion

- Self-organizing maps can be used for unsupervised learning for spectrum sensing
- Can be manipulated by greedy users by using different attacks
- Need for efficient signal classifiers and decision boundary algorithms