

# Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance

R.W. Klein, M.A. Temple, M.J. Mendenhall and D.R. Reising

Air Force Institute of Technology  
Wright-Patterson AFB, Ohio 45433 USA  
Email: michael.temple@afit.edu

**Abstract**—There has been a recent shift toward improving wireless access security within the OSI PHY layer by exploiting RF features that are inherently device specific and difficult to replicate by an unintended party. This work addresses the extraction and exploitation of RF “fingerprints” to classify emissions and provide device-specific identification. Burst transient detection precedes RF fingerprint extraction and is generally the most critical step in the overall process. This work provides a much needed sensitivity analysis of burst detection capability. The analysis is conducted using instantaneous amplitude responses with both Fractal-Bayesian Step Change Detection (Fractal-BSCD) and Variance Trajectory (VT) processes. The performance of each method is evaluated under varying SNR conditions using experimentally collected 802.11a OFDM signals. The impact of transient detection error on signal classification performance is then demonstrated using RF fingerprints and Multiple Discriminant Analysis (MDA) with Maximum Likelihood (ML) classification. The VT technique emerges as the better alternative for all SNRs considered and yields MDA-ML classification accuracy that is consistent with “perfect” transient estimation performance.

## I. INTRODUCTION

Considerable research has been conducted on detecting and/or mitigating spoofing within the Medium Access Control (MAC) layer of the Open Systems Interconnection (OSI) stack [1], [2]. There has been a recent shift toward providing added security at the OSI Physical (PHY) layer by exploiting RF features that are inherently unique to a specific device and that are difficult to replicate by an unintended party. For example, some efforts have investigated Received Signal Strength (RSS) (a power-based metric) for detecting and/or locating a spoofing node [1], [2]. Both of these efforts demonstrated some success at detecting spoofing using experiments conducted with different hardware and in different physical environments.

RF fingerprinting work provides an alternative PHY layer approach but is dismissed in [2] for “scale” reasons. For applications where size constraints may not be a dominant factor, RF fingerprinting remains a viable alternative and is considered in this work. Collectively, related works in RF fingerprinting, electromagnetic signatures, intrapulse modulation, and unintentional modulation [3]–[11], form a solid basis for developing techniques that may be applicable to commercial communication devices.

If the inherent RF fingerprints are repeatedly extractable and unique, they may be used to identify the specific make, model, or serial number of a device. Previous work suggests that this

uniqueness exists and is attributable to various manufacturing, aging, and environmental factors [3]. While several processing steps are required to effectively exploit RF fingerprints, transient detection is perhaps the most important [6], [8]. In this context, transient detection includes both the transient start time and signal duration over which fingerprints are extracted. Both of these factors are important given that improper selection of either can bias the processing to favor channel noise effects or steady-state signal effects [3]. Burst transients can be estimated using various emission features. However, instantaneous amplitude and instantaneous phase features are perhaps the most extensively investigated [3], [6]–[8]. With the exception of more recent work in [12] and [13], these previous efforts lack a detailed sensitivity analysis of burst detection and fingerprint classification performance under varying channel noise conditions.

This type of analysis is imperative for determining the minimum acceptable collected SNR that will provide consistent and accurate results. Establishing the minimum acceptable SNR also allows determination of the maximum transmitter-receiver separation distance which would aid in laying out the physical hardware for network security. Noise sensitivity performance can also provide a good discriminator for comparing various detection and classification techniques. For the work presented here, noise sensitivity analysis for transient detection performance is conducted for three noise-signal conditions, including: 1) noise only effects using a single collected 802.11a burst and multiple noise realizations, 2) signal only effects incorporating burst-to-burst signal variability with a single noise realization, and 3) combined noise-signal effects using multiple burst and noise realizations. The impact of transient detection error on signal classification performance is then demonstrated using Multiple Discriminant Analysis with Maximum Likelihood classification (MDA-ML).

## II. BACKGROUND

### A. Fractal-Bayesian Step Change Detector

It has been demonstrated that transient detection can be accomplished using the fractal dimension measure followed by a Bayesian Step Change Detector [7]. This process is denoted here as Fractal-BSCD. The fractal derivation can be found in [14] and can be calculated using the following Higuchi method.

Given data time series  $\{X(1), X(2), \dots, X(N_X)\}$ , the curve length is defined as:

$$L_m(k) = \frac{\bar{X}(N_X - 1)}{k^2 N_L}, \quad (1)$$

$$\bar{X} = \sum_{i=1}^{N_L} |X(m + ik) - X(m + (i-1)k)|,$$

where  $N_L = \lfloor (N_X - m)/k \rfloor$ ,  $\lfloor \bullet \rfloor$  is the floor operator,  $k$  is the interval index number, and  $m \in [1, k]$  is the start time index number. For this work, the signal of interest was divided into windowed regions containing  $N_X = 20$  samples.

The average of  $L_m(k)$  over  $m$  is denoted here as  $\langle L(k) \rangle$  and defines the curve length for time interval  $k$ . By varying  $k$  over  $[1, k_{max}]$  and plotting  $\langle L(k) \rangle$  versus  $k$  on a log-log scale, the data ideally forms a straight line, with a proper selection of  $k_{max}$ . The fractal dimension  $d$  is defined as the negative of the line slope, which can be calculated using a least squares method.  $k_{max}$  is empirically chosen. If it is too large, the data plotted on the log-log scale will not be linear. If it is too small, there will not be enough data points for an accurate linear fit. For this work, a value of  $k_{max} = 10$  is chosen for all fractal calculations.

Using the fractal dimension vector  $\mathbf{d}$  formed across all data windows, BSCD is applied to determine the *a-posteriori* probability that a given fractal dimension  $d_m \in \mathbf{d}$  represents the data change point corresponding to the transient start. The *a-posteriori* Probability Distribution Function (PDF) for  $m$  given  $\mathbf{d}$  is [15]

$$p(\{m\} | \mathbf{d}, I) \propto \left[ \sqrt{m(N_F - m)} \times \bar{d} \left( \frac{N_F - 2}{2} \right) \right]^{-1}, \quad (2)$$

$$\bar{d} = \sum_{i=1}^{N_F} d_i^2 - \frac{1}{m} \left( \sum_{i=1}^m d_i \right)^2 - \frac{1}{N_F - m} \left( \sum_{i=m+1}^{N_F} d_i \right)^2,$$

where  $N_F$  is the length of  $\mathbf{d}$ ,  $I$  denotes prior information, and  $m$  is the potential change point being evaluated. The value of  $m$  corresponding to  $\max[p(\{m\} | \mathbf{d}, I)]$  establishes the transient start sample number. The work in [3], [6] shows that abrupt, non-gradual feature changes are important for the BSCD to work successfully. Signals that possess more gradually changing amplitude responses require a different technique for transient location. A representative signal, fractal dimension, and *a-posteriori* PDF is shown in Fig. 1.

### B. Variance Trajectory (VT)

The work in [6] analyzed Bluetooth signals using Fractal-BSCD with instantaneous amplitude and showed some improvement over BSCD using a VT process with instantaneous phase. The work presented here generates VT sequence  $\{VT_a(i)\}$  using instantaneous amplitude sequence  $\{a(k)\}$ ,  $k = 1, 2, \dots, N_a$ , to estimate the burst transient start. The  $i^{th}$  element of sequence  $\{VT_a(i)\}$  is given by [12]

$$VT_a(i) = |W_a(i) - W_a(i+1)|, \quad (3)$$

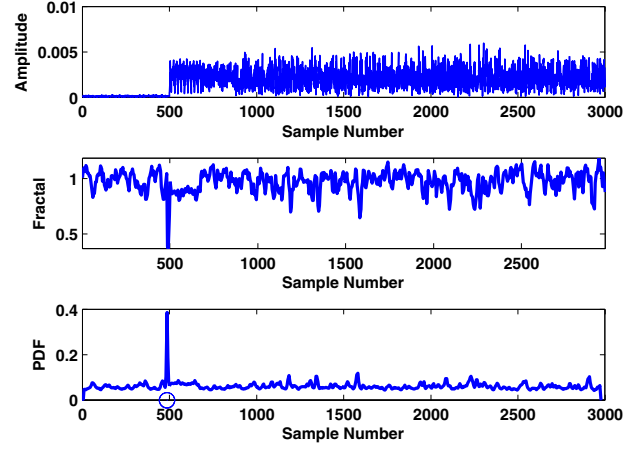


Fig. 1. Instantaneous Signal Amplitude (Top), Fractal  $d$  (Middle), and *A-Posteriori* PDF (Bottom).

$$W_a(m) = \frac{1}{N_w} \sum_{k=1+(m-1)N_s}^{1+(m-1)N_s+N_w} [a(k) - \mu_w]^2, \quad (4)$$

where  $i = 1, 2, \dots, L_w - 1$ ,  $m = 1, 2, \dots, L_w$ ,  $L_w = \lfloor (N_a - N_w)/N_s \rfloor + 1$ ,  $N_w$  is the window extent, and  $N_s$  is the number of samples the window advances between calculations. The  $\mu_w$  factor in (4) is the sample mean of  $\{a_w(k)\}$  which is the subsequence of consecutive elements from  $\{a(k)\}$  contained in the window.

Fig. 2 shows a representative amplitude response and corresponding  $\{VT_a(i)\}$  sequences for two different SNRs. As shown, there is a distinct VT peak response corresponding to the burst transient start which becomes less discernable as SNR decreases. Given optimization is not addressed under this work, a simple sliding window average and thresholding technique is used to automatically estimate the transient start based on locating the initial peak response in  $\{VT_a(i)\}$ .

### C. MDA-ML Classification

MDA is an extension of Fisher's Linear Discriminant (FLD) process for more than two classes [16]. Classification is demonstrated here using an MDA-ML process [17]. For the 3-class problem, the MDA process projects higher-dimensional data onto a 2-dimensional "Fisher plane" that maximizes interclass distances while simultaneously minimizing intraclass distances. In principle, this method cannot improve classification potential. However, it provides good class separation and visualization of data having dimensionality greater than three. Using lower-dimensional data, ML decision boundaries are determined assuming normally distributed input data, equal costs or risk and uniform prior probabilities. To discriminate  $c$  classes using  $d$ -dimensional input data, the input vector  $\mathbf{x}$  is linearly projected onto a  $(c-1)$ -dimensional space using

$$\mathbf{y} = \mathbf{W}^t \mathbf{x}, \quad (5)$$

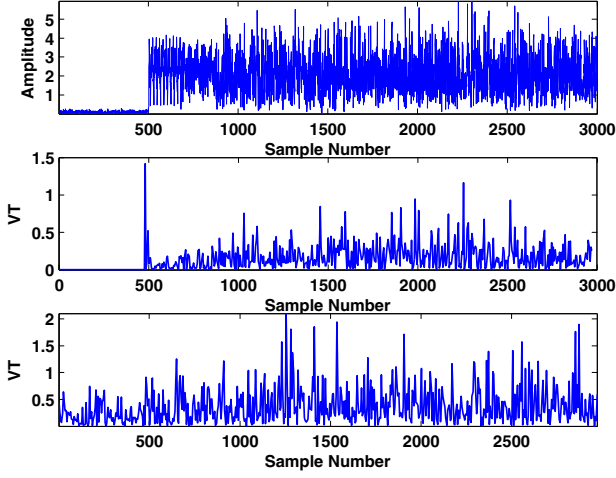


Fig. 2. Instantaneous signal amplitude (Top) and corresponding  $VT_a$  for: (Middle)  $SNR = 30$  dB (Middle) and (Bottom)  $SNR = 3$  dB.

where  $\mathbf{y}$  is the vector of projected values and  $\mathbf{W}$  is a  $d \times (c-1)$  projection matrix. Classification is performed using unknown data and the 2-dimensional trained decision boundaries. The process classifies each unknown input data set by projecting it onto the trained “Fisher plane” using (5). Projected points falling within the correct region are correctly classified while those falling outside the correct region are misclassified. The percentage of correct classification is determined based on the total number of unknown trials.

### III. RESULTS: TRANSIENT DETECTION

1) *Channel Noise Variability*: These results illustrate the effect of channel noise variation for a given RF burst using 200 AWGN realizations scaled and added to achieve the desired analysis SNR. Fractal-BSCD and VT estimation results are shown in Fig. 3 and Fig. 4, respectively.

At higher SNRs the two methods perform similarly as the noise power varies, with primary differences beginning at  $SNR \approx 9$  dB. Fractal-BSCD degradation is directly attributed to the a-posteriori PDF degradation, as calculated per (2) and shown in Fig. 1. The PDF loses the strong peak response and becomes more uniformly distributed as noise power increases. VT degradation is attributed to, and affected by, threshold selection criterion. For the non-optimum method implemented here, the threshold criterion is not always satisfied and a default transient start value is assigned – a *missed* detection. The number of missed detections at lower SNRs can be reduced by changing the threshold. However, this also reduces estimation accuracy and precision at higher SNRs.

2) *Burst-to-Burst Variability*: These results illustrate the effect of burst-to-burst variation using a given AWGN realization scaled to achieve the desired analysis SNR. Results for Fractal-BSCD and VT estimation using 200 collected bursts are shown in Fig. 5 and Fig. 6, respectively. As with the channel noise

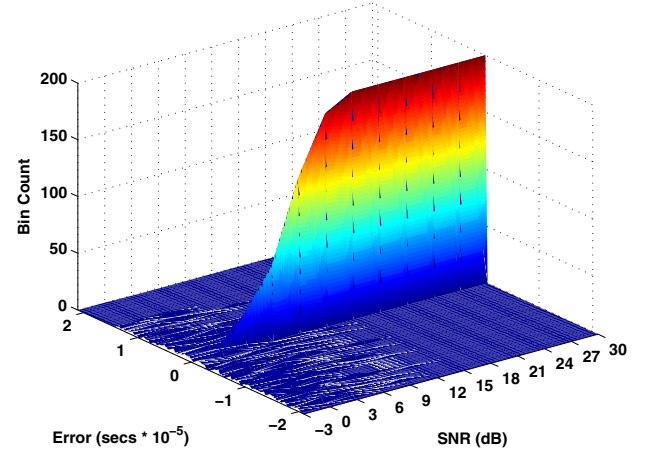


Fig. 3. Impact of *Channel Noise* variation: *Fractal-BSCD* transient estimation using 200 noise realizations and a given 802.11a RF Burst.

impact, the two methods perform similarly at higher SNRs. Differences arise at lower SNRs, with the VT method degrading as before and producing missed detections. The Fractal-BSCD response degrades differently than before, becoming multi-modal at lower SNRs and producing a significant number of detections in the noise-only portion of the signal. The modes are attributable to anomalous spikes in a specific noise realization. This is consistent with results in [6] and [3] given that BSCD processing is most effective when non-gradual parameter changes occur. At lower SNRs the amplitude change is too gradual in some bursts for the BSCD method to reliably detect them.

3) *Combined Noise-Signal Variability*: These results illustrate the combined effects of noise and burst-to-burst signal variability. In this case, 200 AWGN realizations are scaled for each SNR and added to each of the 200 collected bursts – a

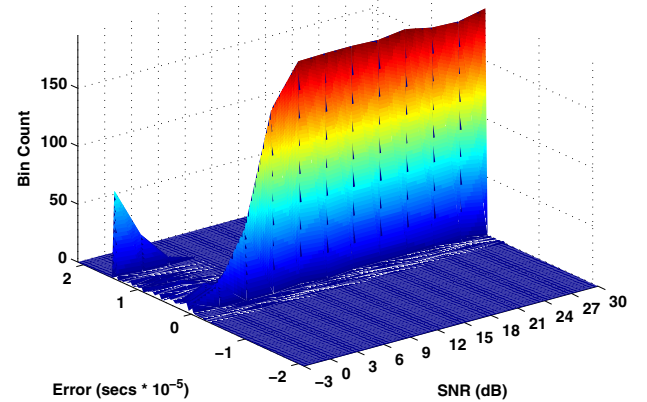


Fig. 4. Impact of *Channel Noise* variation: *VT* transient estimation using 200 noise realizations and a given 802.11a RF Burst.

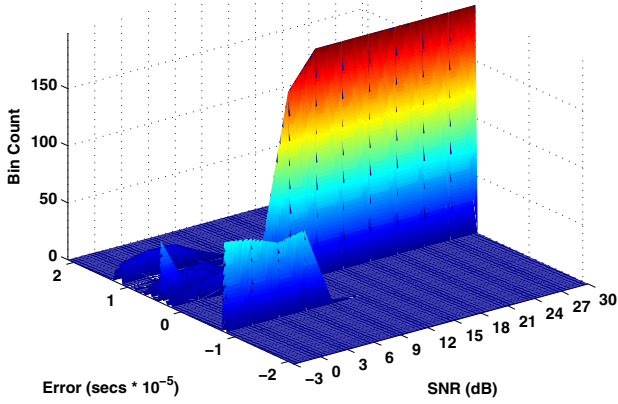


Fig. 5. Impact of *RF Burst* variation: *Fractal-BSCD* transient estimation using 200 802.11a bursts and fixed noise realization.

total of 40,000 unique AWGN realizations per SNR. Results for the Fractal-BSCD and VT method are shown in Figs. 7 and Fig. 8, respectively. In this combined channel noise and burst-to-burst variability effect, the channel noise is dominant. This is evident in that channel noise effect results in Fig. 3 and Fig. 4 are almost identical to the combined effects results Fig. 7 and Fig. 8.

#### IV. RESULTS: SIGNAL CLASSIFICATION IMPACT

A total of 200 802.11a bursts were collected from three different devices and used to demonstrate the impact of transient estimation on MDA-ML classification performance. After locating the transient start, statistical waveform feature data is extracted from the next 16  $\mu$ Sec of the burst (802.11a preamble region [18]) and MDA-ML classification performed in accordance with Section II.C. The multi-dimensional input

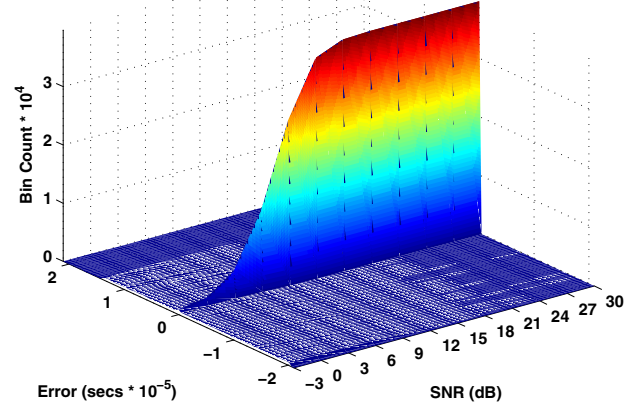


Fig. 7. Impact of *Combined* variation: *Fractal-BSCD* transient estimation using 200 noise realizations per 200 802.11a bursts.

data represents the signal “fingerprint” used by the MDA-ML process and includes variance, kurtosis and skewness statistics calculated over the preamble instantaneous amplitude, frequency and phase responses.

A five-fold cross validation and Monte Carlo process was used to ensure statistical significance. The overall process included: 1) generate AWGN, scale to achieve desired SNR, and add independent realizations to each burst, 2) estimate transient start using the method being evaluated, 3) generate  $\mathbf{W}$  per Section II.C using the first 160 bursts from each device for MDA training, 4) use remaining 40 bursts from each device as “unknown” input data, transform/project them using  $\mathbf{W}$ , and classify each per ML criteria, 5) store/accumulate classification results, 6) circularly shift (re-order) the collected bursts by 40 and repeat Step 2 through Step 6 four times, 7) repeat Step 1 through Step 6 200 times using different independent realizations of AWGN for each iteration, 8) average

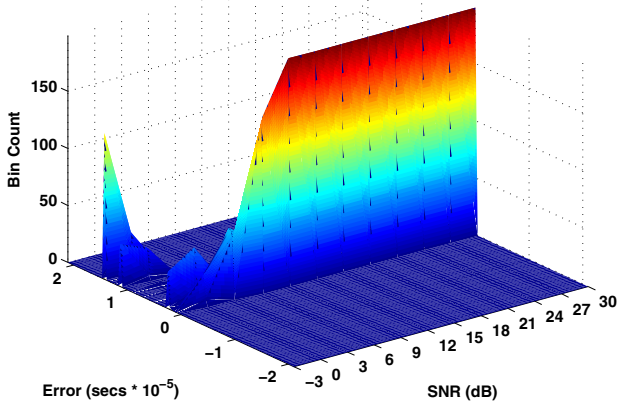


Fig. 6. Impact of *RF Burst* variation: *VT* transient estimation using 200 802.11a bursts and fixed noise realization.

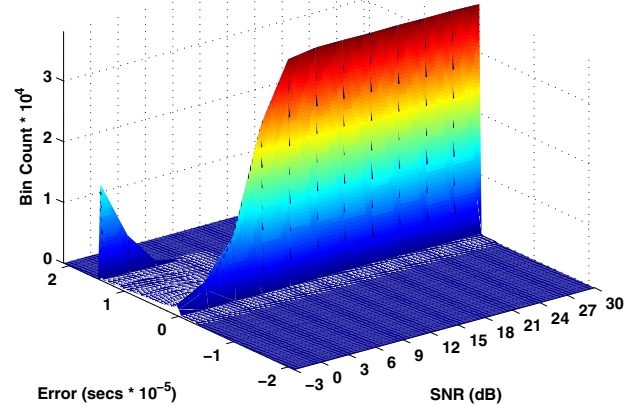


Fig. 8. Impact of *Combined* variation: *VT* transient estimation using 200 noise realizations per 200 802.11a bursts.



accumulated classification results from Step 5 to obtain final classification performance. This process is repeated in 3 dB steps for  $SNR \in [-3, 30]$  dB.

Fig. 9 shows average MDA-ML classification accuracy including burst transient detection error effects for Perfect, Perfect with random error, Fractal-BSCD, and VT transient detection methods. In this case, “perfect” results are obtained using a transient start location based on visual inspection of each collected burst. To determine if “perfect” provides best possible MDA-ML classification accuracy, a uniform randomly distributed error was added to the perfect transient location estimates and results generated for comparison. As shown, the Perfect with Random Error results are consistent with Perfect results and marginally better/poorer for  $SNR$  below/above approximately 14 dB, respectively. The VT technique marginally outperforms Perfect estimation for  $SNR \in [6, 12]$  dB but provides considerable performance improvement when compared to the Fractal-BSCD technique at lower  $SNRs$ .

## V. CONCLUSION

Using experimentally collected emissions from 802.11a OFDM devices, a sensitivity analysis was conducted for burst transient detection and RF fingerprinting classification performance. Transient detection error of Fractal-BSCD and VT processes was characterized and its impact on signal classification evaluated using MDA-ML. Overall, the VT technique provided MDA-ML classification performance that was consistent with “perfect” transient estimation results and provided considerable performance improvement when compared with the Fractal-BSCD technique at lower  $SNRs$ . In addition, the VT method is algorithmically less complex and requires orders-of-magnitude less computation time, making it a viable approach for automatic transient detection and classification applications.

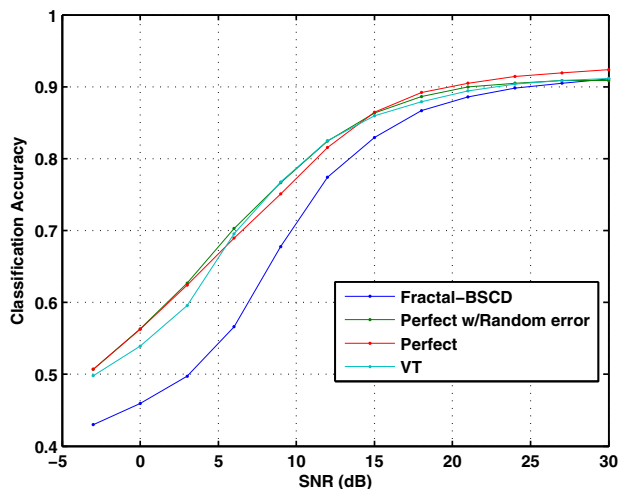


Fig. 9. Average MDA-ML classification accuracy including burst transient detection error effects for various burst detection methods.

## ACKNOWLEDGMENT

This research supported by the Sensors Directorate, Air Force Research Laboratory, and the Tactical SIGINT Technology (TST) Program.

*“The views expressed in this article are those of the author(s) and do not reflect official policy of the United States Air Force, Department of Defense or the U.S. Government.”*

## REFERENCES

- [1] Y. Chen, W. Trappe and R. Martin, “Detecting and localizing wireless spoofing attacks,” IEEE Conf on Sensor, Mesh and AdHoc Comm and Nets (SECON), pp. 193-202, Jun 2007.
- [2] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC layer spoofing using received signal strength,” IEEE 27th Annual Conf on Computer Comm (INFOCOM), Apr 2008.
- [3] O. Ureten and N. Serinken, “Wireless security through RF fingerprinting,” *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27 – 33, Winter 2007.
- [4] L.E. Langlely, “Specific Emitter Identification (SEI) and classical parameter fusion technology, pp. 277-381,” IEEE Western Electronics Show and Conference (WESCON), Sep 1993.
- [5] J. Hall, M. Barbeau and E. Kranakis, “Using transceiverprints for anomaly based intrusion detection,” 3rd IASTED Int’l Conf on Comm, Internet and Info Technology (CIIT), Nov 2004.
- [6] —, “Detection of transient in radio frequency fingerprinting using signal phase,” IASTED Int’l Conf on Wireless and Optical Communications, May 2003.
- [7] O. Ureten and N. Serinken, “Detection of radio transmitter turn-on transients,” *IEE Electronics Letters*, vol. 35, no. 23, pp. 1996 – 1997, Nov 1999.
- [8] —, “Bayesian detection of WiFi transmitter RF fingerprints,” *IEE Electronics Letters*, vol. 41, no. 6, pp. 373 – 374, Mar 2005.
- [9] N. Serinken and O. Ureten, “Generalised dimension characterization of radio transmitter turn-on transients,” *IEE Electronics Letters*, vol. 36, no. 12, pp. 1064 – 1064, Jun 2000.
- [10] J. Dudczyk, J. Matuszewski and M. Wnuk, “Applying the radiated emission to specific emitter identification,” Int’l Conf on Microwaves, Radar and Wireless Comm (MIKON), pp. 431-434, May 2004.
- [11] A. Kawalec, T. Rapacki, S. Wnuczek, J. Dudczyk, and R. Owczarek, “Mixed method based on intrapulse data and radiated emission to emitter sources recognition,” May 2006, pp. 487-490.
- [12] W.C. Suski, M.A. Temple, M.J. Mendenhall and R.F. Mills, “Using spectral fingerprints to improve wireless network security,” in *Proceedings of the 2008 IEEE Global Communications Conference*, Mar 2008.
- [13] —, “Radio Frequency (RF) fingerprinting commercial communication devices to enhance electronic security,” *Int. J. of Electronic Security and Digital Forensics*, Dec 2008.
- [14] T. Higuchi, “Approach to an irregular time series on the basis of the fractal theory,” *Phys. D*, vol. 31, no. 2, pp. 277-283, 1988.
- [15] J. O Ruanaidh and W. Fitzgerald, *Numerical bayesian methods applied to signal processing*. Statistics and Computing Series, New York: Springer, 1996.
- [16] R.A. Fisher, “The use of multiple measurements in taxonomic problems,” *Annals of Eugenics*, vol. 7, pp. 179 – 188, 1936.
- [17] R. Duda, P. Hart, and D. Stork, *Pattern Classification*, 2nd ed. New York: John Wiley & Sons, Inc., 2001.
- [18] 802.11a, *WLAN MAC and PHY layer specs: high speed PHY extension in the 5 GHz band*, IEEE, Piscataway, NJ 08855-1331, USA, Sep 16, 1999, revised 2003.