DETECTION OF TRANSIENT IN RADIO FREQUENCY FINGERPRINTING USING SIGNAL PHASE

Jeyanthi Hall Michel Barbeau Evangelos Kranakis
Carleton University, School of Computer Science
1125 Colonel By Drive, Ottawa, Canada

ABSTRACT

Radio Frequency Fingerprinting (RFF) is a technique, which has been used to identify wireless devices. It essentially involves the detection of the transient signal and the extraction of the fingerprint. The detection phase, in our opinion, is the most challenging yet crucial part of the RFF process. Current approaches, namely Threshold and Bayesian Step Change Detector, which use amplitude characteristics of signals for transient detection, perform poorly with certain types of signals. This paper presents a new algorithm that exploits the phase characteristics for detection purposes. Validation using Bluetooth signals has resulted in a success rate of approximately 85-90 percent. We anticipate that the higher detection rate will result in a higher classification rate and thus support various device authetication schemes in the wireless domain.

KEY WORDS

Radio Frequency Fingerprint, transient detection, signal phase, wireless devices, identification, Blue Tooth.

1 Introduction

RFF is a technology initially designed to capture the unique characteristics of the radio frequency energy of the transceiver, for the purpose of identifying cell phones and other devices. Nevertheless, the underlying principle applies equally to all wireless devices.

The extended RFF process, including the identification of devices, consists of four key phases. The first phase involves the extraction of features (e.g. amplitude, phase or frequency information) from the digital signal. These features are subsequently used to detect the start of the transient (see Fig. 1, 2^{nd} plot) in the second phase. Once the end of the transient has been estimated, typically in an experimental manner, the fingerprint (features representing the transient) is obtained. Finally, the transceiver of the device is identified based on the classification of the fingerprint.

Of the four key phases in the RFF process, the detection phase, which is primarily concerned with the start of the transient, is perhaps the most significant. Inaccurate detection will adversely affect the fingerprinting phase and thus will result in a possible misclassification. Therefore, this paper primarily focuses on the detection of the start of the transient. Two key approaches, which exploit the time-domain characteristics of the signal (e.g. amplitude) in order to accomplish this task, are the Threshold [1] and Bayesian Step Change Detector [2] [3]. Both approaches are based on the premise that the amplitude characteristics of the channel noise and transient differ. Furthermore, it is assumed that there is an abrupt change at the start of the transient. Although, this holds true for most signals, it does not work well with signals where the transition between noise and transient occurs more gradually. As a result, the detection of the transient can be delayed. In addition, the performance of the Bayesian Step Change Detector may not be adequate for certain applications.

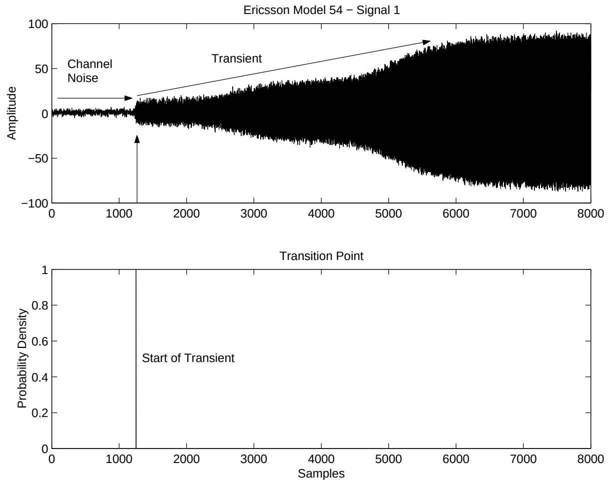

Figure 1. Bluetooth Signal-Ericsson ROK101008/21.

In order to accommodate a vast majority of signals with varying transitional characteristics and to do so as efficiently as possible, a new detection algorithm has been developed. It makes use of the phase characteristics of the signal (features) and the fact that the slope of the phase, associated with the transient, is linear. Since it does not depend on the amplitude characteristics of the signal, which are more susceptible to noise and interference, it represents a more robust solution.

Results of experimentation using Bluetooth (open specification which enables short-range wireless voice and data communications) [4] signals indicate a success rate (estimated start of transient is within 100-200 samples of the actual starting point) of approximately 85-90 percent.

The remaining sections of the paper will provide a brief overview of the two key approaches, the new detection algorithm and the results of the experiments. Section 2 will present a brief summary of the two key approaches within the context of the extended RFF process, while the new detection algorithm will be presented in Section 3. The validation of the algorithm will be described in Section 4 followed by the conclusion in Section 5.

2 Related Work

This section provides a brief overview of the extended RFF process and discusses the detection algorithms, used by the Threshold and Bayesian Step Change Detector approaches, at the appropriate phases.

Before proceeding to the discussion of the four phases, it may prove beneficial to establish some background details regarding the representation of signals in RFF.

Although signals with only real components have been used in RFF in the past, the use of complex signals provides one key advantage. Since the amplitude and phase information of the digital signal is adequately preserved, the use of such information could enhance both the detection and classification phase of the RFF process) [5]. The instantaneous amplitude and phase can be calculated as follows:

$$a(t) = [i^2(t) + q^2(t)]^{\frac{1}{2}} \tag{1}$$

$$\theta(t) = tan^{-1}[\frac{q(t)}{i(t)}] \tag{2}$$

where $i(t)$ and $q(t)$ represent the in-phase and quadrature components of the complex signal).

Step 1: Extract Features from Signal

The objective of the first phase is to extract the features from the signal using information from the time (amplitude) or frequency domain (frequency or phase). These features will be used to detect the start of the transient.

In order to address the non-stationary property (signal characteristics are a function of time) of the signal, a sliding rectangular window is used to extract the features from successive portions of the signal. These features are stored in a vector of length (L). Thus, given the total number of samples in the signal (N), window size (w), and sliding factor (no. of samples to advance the window) (s), the length of the resulting vector is defined as follows:

$$L = \lfloor \frac{N-w}{s} \rfloor + 1 \tag{3}$$

An indirect benefit of using a smaller vector with length L, instead of the total number (N) of samples in the signal, is the reduction in processing time associated with the detection phase.

Threshold Detection Approach

It is well known that the Euclidean dimensions of a point, line and plane can be represented by integer values of 0, 1 and 2. However, fractional quantities can also be used to accommodate such objects as signals. Whereas fractals refer to objects that are similar to each other, the fractal dimension can be regarded as the *irregularity* of a fractal) [6].

In this approach, the feature to be extracted is the variance dimension (variance of the amplitude), which is calculated as follows for successive portions of the signal:

$$D(t) = E + 1 - H \tag{4}$$

where E represents the Euclidean dimension and has been assigned a value of one for this application. This forces the value of the variance dimension $(D(t))$ to fall between 1 (highly correlated portion of the signal) and 2 (uncorrelated white noise). It also implies that the value of H, referred to as the Hurst exponent, will be within the range of [0-1]. H is in turn obtained from

$$H = \lim_{\Delta t \to 0} \frac{1}{2} \frac{log[Var(\Delta X_{\Delta t})]}{log(\Delta t)} \tag{5}$$

where Δt is the time increment and $\Delta X_{\Delta t}$ represents the difference between two samples that are separated by the value of the time increment. As the variance is a function of the time increment and is related to it according to

$$Var[\Delta X_{\Delta t}] \approx |\Delta t|^{2H} \tag{6}$$

the log function is used to determine the value of H.

Since it is given that the variance of the noise and the transient portion of the signal differ sufficiently, the start of the transient should be located at the transition point. Hence, the variance dimensions should mirror the corresponding transition point.

Bayesian Step Change Detector

Unlike the Threshold process, the fractal dimension is calculated for successive portions of the signal using Higuchi's method) [7]. First, subsets of samples e.g. $X(1), X(2), \ldots, X(N))$ of the original signal are created according to :

$$X(m,k); X(m), X(m+k), ..., X(m+[\frac{N-m}{k}]\times k) \tag{7}$$

where m and k are integers indicating the initial time (sample) and the interval time (number of samples), respectively.

Thus, for example, setting $k = 3$, $N = 100$ and $m = 1, 2, 3$ will result in the following 3 subsets:

X(1,3); X(1), X(4), ..., X(100),
X(2,3); X(2), X(5), ..., X(98),
X(3,3); X(3), X(6), ..., X(99).

Second, the length of the curve for each of the subset ($X(m, k)$) is calculated using the following :

$$L_m(k) = \left\{ \left(\sum_{I=1}^{\frac{N-m}{k}} |x(m+ik) - x(m+(i-1)k)| \right) \frac{N-1}{[\frac{N-m}{k}]k} \right\} /k \tag{8}$$

The term, $N - 1/[(N-m)/k] \times k$ represents the normalisation factor of the curve length.

Finally, the average value $< L(k) >$, of the k sets of $L_m(k)$, is plotted against k on a log-log scale followed by the application of the least-square procedure. This produces a straight line, of which the slope represents the fractal dimension. The use of the fractal dimension serves the same purpose as the variance fractal dimension used in the Threshold approach.

Step 2: Detect Start of Transient

As previously discussed, detecting the start of the transient is based on the assumption, that the characteristics of the channel noise and the transient are adequately different. Detection is typically carried out by considering each element in the feature vector (obtained from phase 1) in sequence and attempting to locate the point where there is an abrupt change between two consecutive elements. This point should theoretically correspond to the section of the original signal where the start of the transient is located, see Fig. 1, 2^{nd} plot.

Threshold Detection Approach

Once the variance fractal dimensions have been determined and stored in the feature vector (referred to as the fractal trajectory), the start of the transient is detected according to

$$|D(t) - \mu| > (\tau \times \mu) + \sigma \tag{9}$$

where $D(t)$ is the variance dimension and τ is the threshold that has been established experimentally. In addition, μ and σ represent the mean and standard deviation of the noise portion ($t = 1, 2, \ldots, T/4$) of the original signal.

The algorithm calculates the difference between each fractal dimension (element in the fractal trajectory) and the mean value until the condition in Equation 9 is met. Given that the mean value has been calculated based on a representative portion of the noise samples, the absolute difference between the variance dimension and the mean would not satisfy Equation 9, if the variance dimensions represent the noise portion of the signal. However, at the start of the transient, where the variance dimension is expected to be significantly lower or higher than the noise portion, the absolute difference would be greater than the sum of the standard deviation and a percentage of the mean. Once the detection has been triggered, the corresponding location within the signal can be determined based on the parameters of the window and sliding factor.

In terms of performance, this detection algorithm of order n, works well for signals with an abrupt change at the start of the transient. However, establishing an appropriate threshold can prove challenging. Moreover, the algorithm does not take into account any abrupt spikes after the first ($T/4$) samples, but within the channel noise portion of the signal. This results in an inaccurate detection of the start of the transient.

A variation of this approach, which makes use of the amplitude (Equation 1) from complex signal, for detecting the start of the transient can be found in) [8].

Bayesian Step Change Detector

Unlike the previous approach, the detection of the start of the transient is accomplished using the following posteriori probability density function of a Bayesian Step Change Detector.

$$p(\{m\}|d)\alpha$$

$$\frac{\frac{1}{\sqrt{m(N-m)}}}{[\sum_{i=1}^{N} d_i^2 - \frac{1}{m}(\sum_{i=1}^{m} d_i)^2 - (\frac{1}{N-m})(\sum_{i=m+1}^{N} d_i)^2]^{\frac{N-2}{2}}} \tag{10}$$

The parameters of the function have the following definition: d represents the fractal dimension, N is the number of elements in the fractal trajectory and m represents a potential change point (start of transient). In addition, while the term -(N-2)/2 is used to accentuate the difference in variance, the numerator $1/\sqrt{m(N-m)}$ provides a weighting function in order to place more emphasis on the middle elements of the fractal trajectory.

For each fractal dimension at point m in the fractal trajectory, this function calculates the variance of the fractal dimensions for the sequence $[1, \ldots, m]$ and $[m+1, \ldots, N]$. The larger the difference in variance between these two sequences, the larger the value of the probabilistic density function. Since the fractal dimensions are typically higher for the noise portion of the signal than the transient, we expect that the difference in variance between two sequences would be the highest at the start of the transient.

The 3^{rd} plot in Fig. 2 illustrates the use of the fractal trajectory (sliding factor set to one sample) in detecting the start of the transient (highest value of the probability density function). With this particular signal, the difference in variance is more gradual at the start of the transient. Consequently, the detection is delayed by 500 samples (from 3500 to 4000), see Fig. 2, 2^{nd} plot.

In comparison to the Threshold detection algorithm, the Bayesian Step Change Detector is less efficient with an order of n^2. Although, it could be considered more effective than the threshold mechanism, it does not perform as well with signals, which exhibit similar characteristics as the waveform depicted in Fig. 2, 1^{st} plot. The key advantage, nevertheless, is that it could be applied to various types of signals without having prior knowledge of their specific characteristics.

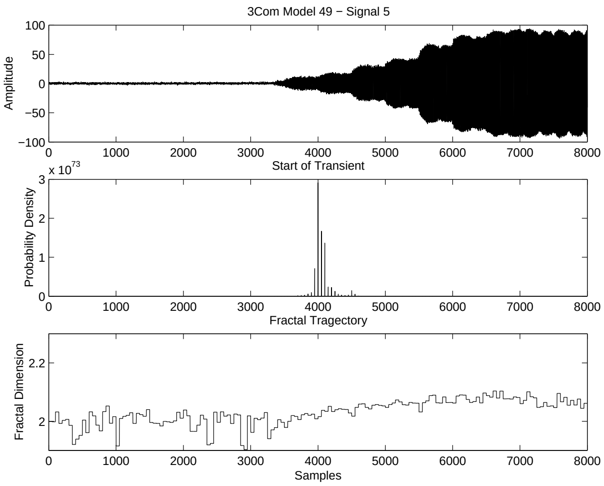

Figure 2. Bluetooth Signal-3Com 3CRWB6096.

The use of other dimensions, such as information and correlation for transient detection, is explored in) [9].

Step 3: Extract Fingerprint

After having isolated the transient (using the start and end points) from the signal, the fractal dimension is obtained once again (possibly using different parameters e.g. window size) for each segment of the transient. The resulting vector is then used as a fingerprint.

While in most cases, the method of extraction is based on the concept of fractal dimension, wavelet-based extraction has also been explored by [[10] [11] [12]].

Step 4: Classify Fingerprint

Although various techniques such as the parallel analog network are available for pattern classification (e.g. fingerprint), the use of probabilistic neural network (PNN) is by far the preferred approach) [13]. In general, the fingerprints from a subset of the signals are used to train the PNN, while the remaining signals are subsequently fingerprinted and classified as having originated from a given transceiver.

3 Transient Detection Using Phase Characteristics

After having implemented and analyzed both approaches, the need to enhance the detection process became apparent. Thus, a decision was made to explore the feasibility of using phase and/or frequency characteristics of the signal in order to develop an algorithm, which is both effective and efficient.

Step 1: Extract Features from Signal

Unlike the previous approaches, whereby the features were derived from the amplitude characteristics of the signal, this approach makes use of phase characteristics to represent the features of the signal.

Using the characteristics of the signal phase has a number of advantages over those associated with the amplitude. First, as the phase of a signal is less susceptible to noise and interference, it does not exhibit the same degree of fluctuations. Second, the slope of the phase becomes linear at the start of the transient. This should render the task of establishing a threshold more manageable and thus permit us to leverage on the principle of threshold detection. Finally, the linearity of the slope should also render the detection algorithm more effective, especially, when processing signals with a less abrupt change at the start of the transient, see Fig. 3, 1^{st} plot.

The fractal trajectory is created as follows:

The instantaneous phase of the signal, calculated using Equation 2, is unwrapped in order to remove the discontinuities that result at multiples of 2π radians. The resulting vector, referred to as *unwrapped*, has the same length N as that of the original signal.

The absolute value of each element in the unwrapped vector, absUnwrapped or (AV), is then obtained in order to simplify the detection process.

In order to magnify the variation between the noise and transient portion of the signal, the variance of the phase (features) is calculated for each successive portion of the AV. A non-overlapping window of size s is used for this purpose. The features are then stored in a temporary vector (TV) of length N/s.

$$TV(i) = Var(AV(d+1), AV(d+2), \ldots, AV(g)) \quad (11)$$

where, $i = 1, 2, \ldots, N/s$, $g = i \times s$, $d = g - s$ and Var represents the variance of the phase.

Finally, using the TV, the difference between the phase variance is obtained in order to create the fractal trajectory (FT), see Fig. 3, 3^{rd} plot.

Step 2: Detect Start of Transient

The successful detection of the transient is based on the fact that the slope of the phase becomes and remains linear from the start of the transient. Therefore, the corresponding difference in phase variance (in the fractal trajectory) should have a value of zero, at the start of the transient, see Fig. 3, 3^{rd} plot, value of 68.

The detection of the transient is carried out using a 2-step process as follows: Each element in the FT is compared to a threshold until the value of the element, as well as the values of the next 4 elements, meet the following condition:

$$FT(i), FT(i+1), ..., FT(i+4) \leq 5 \quad (12)$$

At this point, the start of the transient can usually be identified within 100 samples of the actual starting point.

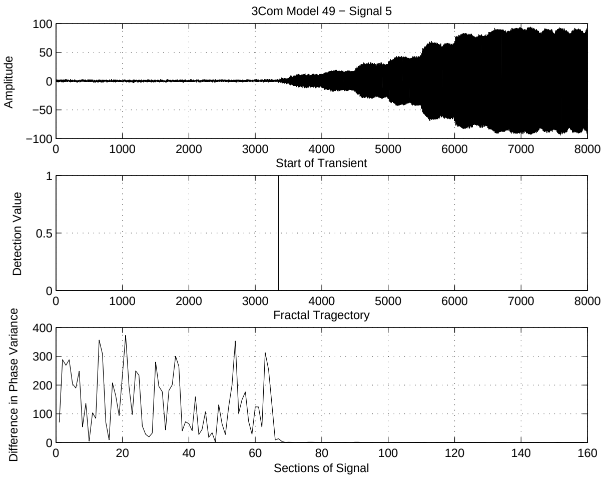

Figure 3. Bluetooth Signal-3Com 3CRWB6096.

In addition, the starting point of the transient can be rendered more accurate (compensation for phase transition). A temporary vector, which holds the sum of the amplitudes (SV) for each successive portion of the signal, is used for this purpose. If the following condition

$$|SV(i) - SV(i-1)| \leq 0.25 \times FT(i) \qquad (13)$$

is met, then the start point, denoted by $FT(i)$, is decreased by 1. It is also feasible to test more than one element in order to achieve greater accuracy. However, it may prove challenging with signals that are characterised by amplitude, which increases slowly at the transition point.

Figure 3, 2nd plot illustrates the application of the detection algorithm to a Bluetooth signal from an Ericsson transceiver. This signal is identical to the one depicted in Fig. 2, 1st plot.

4 Validation

This section provides details of the infrastructure used to capture signals from Bluetooth wireless PC cards, Bluetooth test radios and 802.11) [14] wireless LAN adapters.

Infrastructure

The baseband signals (2400-2483.5 MHz) were captured using an Omni (3 dBi) antenna. Using the Rohde & Schwarz RF generator with the output level set to +3dB and the Watkins Johnson MIG mixer, an IF signal (5-105 MHz) was produced. This signal was then filtered using MiniCircuits BBLP-156 LPF with $F_c \sim$ (90 MHz. The filtered signal, in turn, was sampled at 500 MHz using the LeCroy 9354L digital oscilloscope (8 bit ADC - analog to digital converter). Resulting samples were converted from binary to ascii format and stored on compact discs for future analysis.

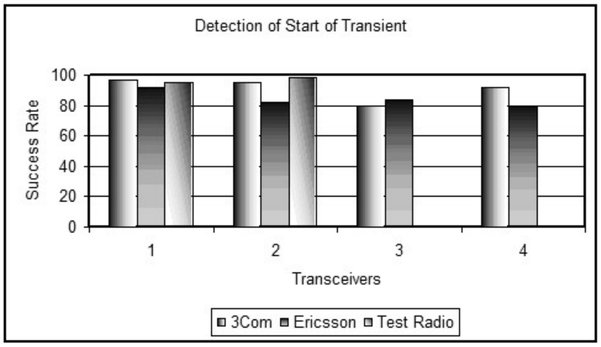

Figure 4. Success Rate of Transient Detection.

In terms of Bluetooth transceivers, three different models were used: 3Com Model 3CRWB6096 (4 units), Ericsson Model ROK101008/21 (4 units), Test Radios Model 3CW1057-E (2 units) for a total of (10) transceivers. One hundred signals were captured per transceiver resulting in a test base of 1000 signals. In addition, the same number of signals per transceiver were captured using the Breezenet Pro.11 Series Model SA-PCR (2).

All subsequent processing and experimentation were carried out using Matlab software and associated tools e.g. the Neural Network toolbox. As we are currently in the process of testing signals from 802.11 transceivers, the following results are based on Bluetooth signals only.

Results

With an order of n, the success rate (estimated start of transient is within 100-200 samples of the actual starting point) of the algorithm is approximately 85-90%. In comparison to our implementation of the Bayesian step change detector (approx. 80-85%), the new algorithm seems to be more suited to the characteristics of Bluetooth signals. Although the Threshold detection algorithm was also implemented, testing proved to be very time consuming as the threshold value had to be changed frequently, to accommodate all Bluetooth signals. Hence, the experiments were discontinued.

Figure 4 presents the success rate of the detection algorithm.

While the overall success rate is 89.5%, the success rate for each model is as follows: 3Com (91%), Ericsson (84.5%), Test Radio (96.5%). In comparison, the classification techniques proposed in [10] and [12] have resulted in success rates of 95% and 100% respectively. Furthermore, in the area of cellular security, RFF has been instrumental in reducing cloning fraud [15] by approximately 95%, thus supporting the feasibility of achieving high classification and detection rates.

During the process of testing, some general observations were made.

Transceivers used by 3Com cards and the Test Radios,were very consistent and so were the phase variance of the noise and transient portion of the signal. On the other hand, those from Ericsson transceivers exhibited much more variation, resulting in a lower success rate. We suspect that the higher degree of variation was caused by the minor imprecision of the infrastructure and may not reflect the true characteristics of the transceivers.

The frequency hopping behaviour of the transceivers was clearly noticeable, although it did not affect the performance of the detection algorithm.

As the accuracy of the detection algorithm is based on the phase characteristics (not amplitude) of the signal, it is logical to assume that the algorithm can be applied to signals from other wireless devices in addition to 802.11 transceivers.

5 Conclusion

The Threshold and Bayesian Step Change Detector approaches, which utilise the amplitude characteristics of the signal, can be employed to detect the start of the transient. However, a detection algorithm that exploits the phase characteristics of the signal, can provide better performance by accommodating signals where the transition, between noise and transient, occurs more gradually. It is particularly beneficial when processing signals associated with some Bluetooth transceivers. The higher success rate of 85-90 is attributable to two key factors. First, the susceptibility of the signal phase to noise and interference is minimal. Second, the slope of the phase becomes and remains linear from the start of the transient portion of the signal.

While preliminary results are promising, the detection algorithm must be enhanced in order to achieve a higher success rate and to accommodate signals from other wireless devices. Benefits accrued from this exercise will no doubt play a vital role in the next phase, the classification of transceivers.

Finally, the success rate of classification (authentication), in turn, will support various types of applications including device to device communication (e.g. hidden computing), access control via access points (802.11) and inventory control.

6 Acknowledgments

The members of the RFF Research Team graciously acknowledge the support received from the following organizations : Ericsson, 3COM, Mitel (for the loan of Bluetooth devices), Communications and Information Technology Ontario and Natural Sciences and Engineering Research Council of Canada (for their financial support), Mathematics of Information Technology and Complex Systems, Communications Research Centre (Dr. Oktay Ureton) and Defense Research Establishment Ottawa (Mr. Larry Ryan).

References

[1] D. Shaw and W. Kinsner, Multifractal Modelling of Radio Transmitter Transients for Classification, *Proc. Conference on Communications, Power and Computing*, 1997, 306-312.

[2] O. Ureten and N. Serinken, Bayesian detection of radio transmitter turn-on transients, *Proc. NSIP99*, 1999, 830-834.

[3] O. Ureten and N. Serinken, Detection of radio transmitter turn-on transients, *Electronics Letters*, volume 35, 1999, 1996-1997.

[4] Bluetooth, Specification of the Bluetooth System, Specification Volume 2, 2001.

[5] K.J. Ellis and N. Serinken, Characteristics of radio transmitter fingerprints, *Radio Science*, Volume 36, Number 4, 2001, 585-597.

[6] W. Kinsner, A unified approach to fractal and multifractal dimensions, Technical Report, Department of Electrical and Computer Engineering, University of Manitoba, 1994, 140.

[7] T. Higuchi, Approach to an irregular time series on the basis of the fractal theory, *Physica D*, 1988, 227-283.

[8] O.H. Tekba, N. Serinken, Transmitter Fingerprinting from Turn-on Transients, Communications Research Centre, 2001.

[9] O. Ureten and N. Serinken, Detection, Characterization and Classification of Radio Transmitter Turn-On Transients, Communications Research Centre, 2001.

[10] H. Choe, C.E. Poole, A.M. Yu and H.H. Szu, Novel identification of intercepted signals from unknown radio transmitters, *SPIE*, volume 2491, 1995, 504-517.

[11] R.D. Hippenstiel and Y. Payal, Wavelet Based Transmitter Identification, *Proc. Information Symposium on Signal Processing and its Applications*, Gold Coast, Australia, 1996.

[12] J. Toonstra and W. Kinsner, Transient Analysis and Genetic Algorithms for Classification, *Proc. IEEE WESCANEX*, 1995.

[13] D.F. Specht, Probabilistic neural networks for classification, mapping, or associative memory, *Proc. IEEE International Conference On Neural Networks*, 1988, 525-532.

[14] B.P. Crow, I. Widujaja, L.G. Kim and P.T. Sakai, IEEE 802.11 Wireless Local Area Networks, *IEEE Communications Magazine*, 1997, 116-126.

[15] M.J. Riezenman, Cellular security: better, but foes still lurk, *IEEE Spectrum*, 2000, 39-42.