ENHANCING INTRUSION DETECTION IN WIRELESS NETWORKS USING RADIO FREQUENCY FINGERPRINTING (EXTENDED ABSTRACT)

Jeyanthi Hall
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario, Canada
email: jeyanthihall@rogers.com

Michel Barbeau and Evangelos Kranakis
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario, Canada
email: barbeau,kranakis@scs.carleton.ca

ABSTRACT

Media access control (MAC) address spoofing can result in the unauthorized use of network resources. This paper demonstrates a novel approach, which incorporates radio frequency fingerprinting (RFF) into a wireless intrusion detection system (IDS), for detecting this attack. RFF is a technique that is used to uniquely identify a transceiver based on the transient portion of the signal it generates. Moreover, the success rate of a wireless IDS is also improved by correlating several observations in time, using a Bayesian filter. Simulation results, with an average success rate of (94-100%), support the feasibility of employing RFF and Bayesian filtering techniques to successfully address the aforementioned problem.

KEY WORDS

Intrusion Detection, Media Access Control, Radio Frequency Fingerprinting, Wireless Networks, Network Security, Bayesian Filter.

1 Introduction

Unlike wired IDSs, wireless IDSs for 802.11 [1] networks must also defend against attacks including rogue access points, media access control (MAC) address spoofing and password-guessing for 802.1x [2] (authentication standard [3] used by the 802.11i security infrastructure [4]), according to Potter [5].

While commercial IDS products such as AirDefense, Netstumbler and Airtraf are currently available, they tend to focus primarily on the detection of rogue access points, as indicated by Potter in [5]. Although AirDefense does address the issue of MAC address spoofing, it can only make a distinction between transceivers from different manufacturers. In terms of solutions that are open source, Kismet and Snort-wireless are used to counter war driving (driving in a vehicle and searching for the presence of wireless networks) and to detect rogue access points in ad hoc networks respectively. Finally, the use of an agent framework for detecting rogue access points and unauthorized clients (nodes) is explored by Chirumamilla and Ramamurthy in [6]. The main disadvantage with this approach is the use of a list of MAC addresses, which can be spoofed, for identifying authorized access points and nodes.

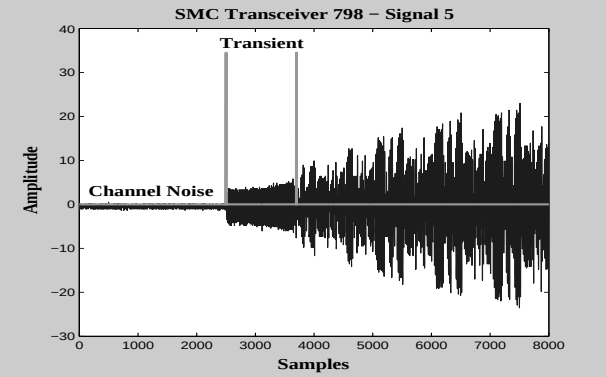

Figure 1. Signal from a 802.11b Transceiver

The problem that is addressed in this paper is the malleability of the identifier used for access control. In the case of MAC address spoofing, the address itself (used as an identifier) is acquired over the air by an intruder and subsequently used to gain unauthorized access to the network.

What is required is a form of identification that is non-malleable (cannot be spoofed easily). Pioneered by the military to track the movement of enemy troops and subsequently implemented by some cellular carriers (e.g. Bell Nynex) to combat cloning fraud [7], radio frequency fingerprinting (RFF) has been used to uniquely identify a given transceiver, based on its transceiverprint. A transceiverprint consists of features, which have been extracted from the turn-on transient portion of a signal [8]. Figure 1 illustrates the location of the transient from the SMC 802.11b transceiver (ID:798). The key benefit of this technique is that a transient reflects the unique hardware characteristics of a transceiver and thus cannot be easily forged, unless the entire circuitry of a transceiver can be accurately replicated (e.g. theft of an authorized device).

In this paper, a novel approach is presented whereby a profile of a transceiver (created using RFF) is used for anomaly-based intrusion detection. By associating a MAC address with the corresponding transceiver profile, the capabilities of a wireless IDS is further enhanced.

It is generally known that current IDSs render a decision, as to whether an observed behavior/event is normal or anomalous, based on a *single* observation. By delaying this decision until *multiple* observations have been analyzed, the level of uncertainty is reduced, resulting in a higher success rate. Thus, the Bayesian filter, presented by Russell and Norvig in [9], has been used to achieve this goal.

The remaining sections of the paper are organized as follows. The details of using RFF for anomaly-based detection is presented in Section 2, followed by the results of the simulation in Section 3. Section 4 briefly summarizes other related work in the area of RFF. Finally, the conclusions drawn are reported in Section 5.

2 Novel Approach: RFF for Anomaly-based Detection

This section describes the framework and the key activities that are undertaken to fulfill two primary objectives: the creation of a profile for each transceiver and the specification of the classification system.

2.1 Intrusion Detection Framework

The intrusion detection framework is illustrated in Figure 2. The overall objective is to classify an observed transceiverprint as normal (belongs to the transceiver of a device with a given MAC address) or anomalous (belongs to another transceiver).

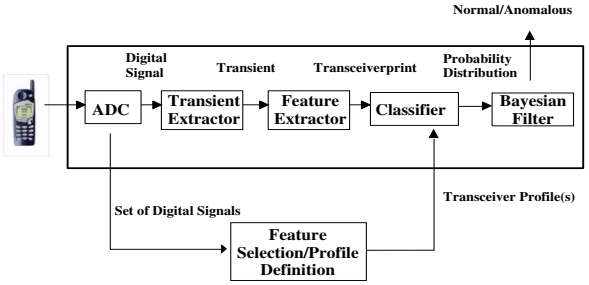

Figure 2. Anomaly-based Intrusion Detection

The flow of information begins with the conversion of an analog signal to a digital signal using an analog to digital converter (will not be covered in detail). Once in a digital form, the transient portion of the signal is extracted by the transient extractor. Upon isolating the transient, the amplitude, phase and frequency components of the transient are subsequently extracted by the feature extractor. In turn, these components are used for the extraction of specific features that define a transceiverprint. The classifier is then used to determine the probability of a match between a transceiverprint and each of the transceiver profiles in the IDS. Finally, the Bayesian filter is applied to render a final decision regarding the status (normal/anomalous) of a transceiverprint.

A transceiver profile is created by extracting the transceiverprints from a set of digital signals and storing the corresponding centroid and the covariance matrix (discussed in section 2.4) in a profile. This exercise is undertaken prior to the detection process. Due to factors, such as transceiver aging, there is a need to periodically update the profiles. One possible strategy would be to continuously recalculate the centroid and the covariance matrix (after successful transceiver identification) using one or more recent transceiverprints and pre-established thresholds (e.g. classification error rate).

2.2 Transient Extractor

As the unique characteristics of transceivers are manifested in the transient portion of a signal, the key objective is to extract the transient using the phase characteristics of the signal, as proposed by Hall, Barbeau and Kranakis [8]. In brief, the successful detection of the start of the transient is based on the fact that the variance of the phase remains constant until the start of the transient. The end of the transient is identified in an experimental manner.

2.3 Feature Extractor

Once the transient has been isolated, the next requirement is to extract the three primary components from the transient. The amplitude and phase [10] components are obtained using Eq.1 and Eq.2 respectively.

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

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

The preferred approach for obtaining the frequency component of a non-stationary signal (e.g. transient) is the application of the Discrete Wavelet Transform (DWT) [11]. Due to its lower computational complexity, as stated by Choe et al. [12] and Hippenstiel and Payal [13], the Daubechies filter is used to obtain the DWT coefficients.

While other research teams have focused primarily on the use of a single component (e.g. amplitude or frequency) for feature extraction, we have opted to make use of all three components, namely amplitude, phase and frequency. This strategy increases the number of components from which a set of features (feature vector) are derived, thus enhancing the characterization of the transceivers.

Figure 3 displays a signal from the SMC transceiver 798 as well as the frequency component (DWT coefficients) of the transient (between vertical lines in the first plot).

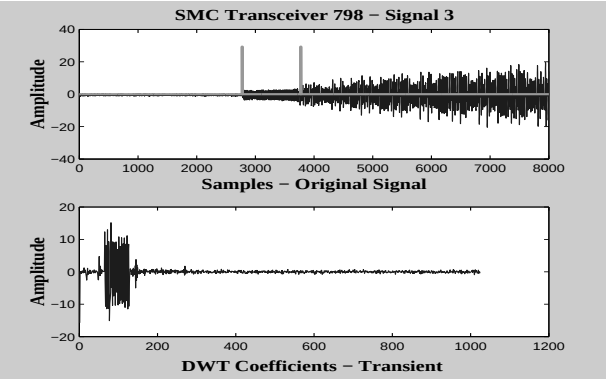

Figure 3. Frequency component of Transceiver 798

Once these components have been extracted, a feature vector, defined by the feature selection/profile definition process (discussed in Section 2.6), is created to represent a transceiverprint. Please note that the term transceiverprint and feature vector will be used interchangeably in the following sections.

2.4 Classifier

With regards to classification, the guiding factor is the need to determine the probability of a match between a given transceiverprint and each of the transceiver profiles.

Although the Probabilistic Neural Network (PNN) [14] has been used by many research teams including Shaw and Kinsner [15] and Hunter [16], the issue of scalability (memory requirement per profile (MPP)) prohibits its use in real time systems. In contrast, the MPP of a statistical classifier is very modest and is defined by Eq.3

$$MPP(m,n) = mn + m(n^2) \tag{3}$$

where n is the number of features, m is the size in bytes, and mn and mn^2 represent the memory requirement for the centroid and covariance matrix respectively. Setting n to ten and m to four, results in a MPP of 440 bytes in comparison to 61,440 bytes (2048 bytes per training pattern multiplied by 30 patterns) required for PNN.

A statistical classifier uses a set of variables, in this case a set of features, to represent a vector that is to be classified. The probability of a match is calculated using a Kalman filter from Bar-Shalom [17] that has been modified:

$$P(\bar{u}) = \exp\left[-\frac{1}{2}(\bar{u}-\mu)^T V^{-1}(\bar{u}-\mu)\right] \tag{4}$$

where $\bar{u}$ represents the feature vector to be classified, μ corresponds to the centroid (vector with elements representing the average of each of the features) and V is the covariance matrix, which characterizes the dispersion or variability of each feature with respect to one another. Eq.4 returns a probability based on the relationship between an observed feature vector and the profile of a transceiver.

2.5 Bayesian Filter

In a wireless environment, characterized by noise and interference, there is a potential for increased variability between signals from a given transceiver. The Bayesian filter probabilistically estimates the state of a system from noisy observations. We will use Figure 4 to illustrate the application of the Bayesian filter to 10 transceiverprints from transceiver SMC 798.

In RFF, the state is defined as a transceiver (from the transceiver space: x-axis) to which a transceiverprint from SMC 798 could potentially belong to. At each point in time t, a probability distribution, called *belief*, over the state (x_t) space, represents the uncertainty and is denoted as $Bel(x_t)$. Initially, the $Bel(x_0)$ or probability is uniformly distributed at $t = 0$. This is demonstrated by the similar height of the vertical bars (y-axis) along the x-axis for transceiverprint number one. Actual classification of the 10 transceiverprints begins with transceiverprint number two on the z-axis.

Therefore, at $t = 1$, the probability distribution associated with the first transceiverprint (z=2) is obtained from the classifier. The filter sequentially estimates such beliefs using Eq.5 for $(t = 1, 2, \ldots, 10)$. At each iteration, the belief at time t represents the current probability that has been influenced by the probability of the previous observation (transceiverprint) o_t at $t-1$.

$$Bel(x_t) = p(x_t|o_t)Bel(x_{t-1}) \tag{5}$$

Based on the normalized distribution at $t = 10$, it is clearly evident that there is a high probability of a match, between the transceiverprints and transceiver SMC 798.

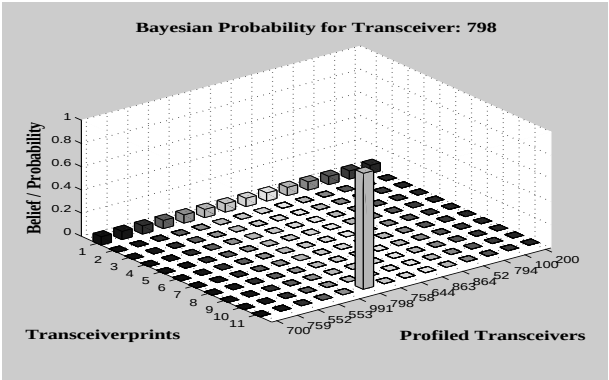

Figure 4. Bayesian Probability: Transceiver 798

2.6 Feature Selection/Profile Definition

In order to define a profile (for each transceiver), one must first define the composition of a transceiverprint. The key

objective is to select a set of features that have low intra-transceiver variability (within a transceiver) and high inter-transceiver variability (between transceivers).

In order to determine the two classes of variability, the use of euclidian distance (ED) and clustering techniques of Multivariate Analysis (MVA) are employed [18]. The features (variables), to be analyzed using MVA, are extracted from the three components of the signal.

Thus, the initial set of ten features (transceiverprint) is comprised of the following:

Standard deviation of normalized amplitude, Standard deviation of normalized phase, Standard deviation of normalized frequency, Variance of change in amplitude, Standard deviation of normalized in-phase data, Standard deviation of normalized quadrature data, Standard deviation of normalized amplitude (mean centered), Power per section, Standard deviation of phase (normalized using mean) and the Average change in DWT coefficients.

In order to refrain from a detailed treatment of each feature, a brief overview of the first four features is provided next:

Standard deviation of normalized amplitude is defined as

$$\sigma_{An} = \sqrt{(A_n - M_{an})^2} \tag{6}$$

where A_n represents the normalized instantaneous amplitude (Eq.1) and is denoted as $\frac{Ai}{Ma}$. While A_i represents the amplitude at time instant t $(i = 1, 2, \ldots, N)$, $M_a = max\{A_i\}$ and it is the maximum of the instantaneous amplitudes. Finally, the mean of the normalized amplitudes M_{an} is defined as $\frac{1}{N}\sum_{i=1}^{n} A_n$.

The Standard deviation of normalized phase and the Standard deviation of normalized frequency are similarly defined by substituting A_i with the phase and frequency data (DWT coefficients) respectively.

Variance of change in amplitude is defined as

$$V = \sum \left((D_{A_i}) - (\frac{1}{n} \sum_{i=1}^{N-1} (\vec{D_{A_i}}) \right)^2 \tag{7}$$

where D_{A_i} is the difference in the amplitude $A_i - A_{i+1}$ and N is the size of the transient.

The extraction of the 10 features from each transient results in a set of feature vectors referred to as a cluster. In order to assess the intertransceiver variability of two or more transceivers (clusters), a centroid (composed of the average value of each of the features in the vectors) is created for each cluster. The centroids as well as the variability between the SMC transceivers are illustrated in Figure 5.

Intratransceiver variability, on the other hand, is depicted in Figure 6. The individual data curves represent the ED of each of the 31 transceiverprints from the corresponding centroids. The transceiverprints have been sorted based on the ED in order to determine the range of the dispersion.

Once the composition of a transceiverprint has been established, through an iterative process of profiling and classification, a subset of these transceiverprints is used to create the profile (centroid and the covariance matrix).

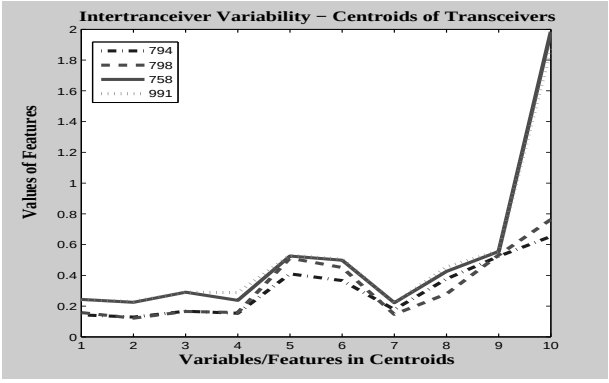

Figure 5. Intertransceiver Variability for SMC Transceivers

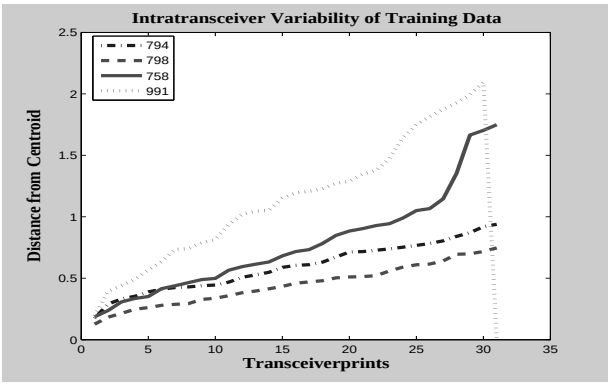

Figure 6. Intratransceiver Variability for SMC Transceivers

3 Simulation

The purpose of the simulation was to primarily assess the composition of the transceiverprint based on the classification success rate (metric). In order to fulfill this objective, the following steps were carried out using a set of signals from each transceiver:

For each transceiver being profiled, the predefined features were extracted from the transients. A subset (approximately 31) of the transceiverprints was selected (based on the ED) and subsequently used to create a centroid and covariance matrix. The remaining transceiverprints (approximately 60) were used for testing purposes.

The actual simulation was carried out by: selecting a transceiver to be tested (from a list); obtaining a set of 10 consecutive transceiverprints (for that transceiver) from a given starting point (changed between each iteration) in the test data set; classifying each of the 10 transceiverprints and thus obtaining the corresponding probability distributions; and finally determining the transceiver with the highest probability using the Bayesian filter.

3.1 Details of Simulation

In order to ensure statistical significance, 100 signals from each of the 14 802.11b transceivers (3COM-2, DLink-2, SMC-4, Spectrum-2, Breezenet-3, Lucent-1) were captured for the purpose of RFF. All subsequent processing and simulations were carried out using Matlab software and associated tools. As far as the simulation platform is concerned, a notebook (HP Pavilion N5445), with 256 Mbs of memory and running XP and Matlab software, was used.

3.2 Simulation Results - RFF and Bayesian Filter

After running the simulation for 50 iterations, the following classification success rates (no.of correct classification / number of iterations) (Table 1) were obtained.

Based on the simulation results, there are some observations that are noteworthy. First, the high success rates for most of the transceivers, especially those from the same manufacturer, attest to the quality of the characterization of the transceivers.

Spectrum	%	Dlink	%	SMC	%
700	100	552	100	991	100
759	88	553	98	798	100
				758	96
				794	100
3Com	%	Breezenet	%	Lucent	%
644	100	864	100	200	100
863	100	52	100		
		100	100		

Table 1. Classification Success Rate

Second, an improvement in the success rates achieved by the classifer (e.g. from 92% to 100% and from 95% to 100% for transceivers SMC 794 and 3Com 863) provides evidence to support the use of the Bayesian filter.

Finally, as expected, the success rates for transceivers SMC 758, Spectrum 759 and Dlink 553 reflect the lower intertransceiver variability between transceivers from the same manufacturer.

As current classifiers for RFF are typically based on some variant of neural networks e.g. PNN and Artificial Neural Network (ANN) used by Zuidweg and Zuidweg [19], and Self Organizing Maps by Kayacik et al. [20], a direct comparison of the simulation results is rather difficult.

Nevertheless, the type of research carried out by Choe [12] is similar to some degree. However, the number of profiled transceivers was limited to three (2-Motorola HT-220, 1-Motorola MX-330) in comparison to the 14 802.11b transceivers used in this project. Despite the increased complexity, the average success rate of (94-100%), achieved using RFF and Bayesian filter, is consistent with their results of (94%).

4 Related Work

This section provides a brief overview of the various research initiatives that have been undertaken to address the requirements of the RFF process.

Radio Transmitter Fingerprints

In the paper by Ellis and Serinken [21], the authors examine the amplitude and phase components of signals and arrive at the conclusion that all transceivers do possess some consistent features.

Detection of Transients

The detection of transients, based on the variance of the amplitude, is proposed by Shaw and Kinsner [15] and Ureten and Serinken [22].

Feature Selection

As far as the selection of features is concerned, the use of the Probabilistic Neural Network (PNN) by Specht [23] is explored by Hunter in [16].

Classification of Transceiverprint

In terms of classification, different approaches have been proposed. In the paper by Somervuo and Kohonen [24], the authors make use of the Self-Organizing Map and a Learning Vector Quantization (LVQ) algorithm to support variable-length feature sequences used for classification. While the use DWT coefficients is explored by Hippenstiel and Payal in [13], Toonstra and Kinsner [25] exploit the properties of genetic algorithms for classification purposes.

5 Conclusion

Based on the simulation results (average classification success rate of 94-100%), the use of RFF and Bayesian filter for anomaly-based intrusion detection is technically feasible.

More specifically, the characterization of transceivers using multiple features has proven to be effective (high classification rate). In addition, the use of a statistical classifier that is memory conscious (440 bytes per transceiver profile) could achieve sufficient performance for supporting real-time applications. Furthermore, delaying the final decision until a sufficient number of transceiverprints have been classified, increases the confidence level and classification success rate.

Nevertheless, there are some issues, which warrant further attention. First and foremost, the success rates should be improved by optimizing the composition of the transceiverprints and validating them using additional transceivers from the same manufacturer. Second, it would prove beneficial to repeat the profiling exercise periodically in order to determine the impact of various factors, e.g. transceiver aging, on the classification success rate. Finally, as far as scalability is concerned, the comparison of a single

transceiverprint to multiple transceiver profiles should only be carried out during the profiling phase. During the execution phase of the IDS, the classifier and the Bayesian filter will be applied to the target profile only, along with appropriate thresholds (e.g. level of correlation). This will permit us to determine, whether or not, an observed transceiverprint belongs to the target transceiver, which is associated with a given MAC address.

6 Acknowledgments

The authors graciously acknowledge the financial support received from the following organizations: Natural Sciences and Engineering Research Council of Canada (NSERC) and Mathematics of Information Technology and Complex Systems (MITACS). In addition, the authors also acknowledge the support received from Lucent, SMC, Spectrum, D-Link, BreezeNet and 3COM.

References

[1] Working Group for Wireless Local Area Networks. IEEE Standard for Wireless LAN MAC and PHY Specifications. http://standards.ieee.org/wireless, 1997.

[2] Frank Robinson. 802.11i and WPA Up Close. *Network Computing*, pages 79–82, 2004.

[3] Working Group for Wireless Local Area Networks. Port Based Network Access Control. http://standards.ieee.org/wireless, August 2003.

[4] Working Group for Wireless Local Area Networks. MAC Security Enhancements. http://standards.ieee.org/wireless, June 2004.

[5] Bruce Potter. Wireless Intrusion Detection. *Wireless Security*, pages 4–5, 2004.

[6] Mohan K. Chirumamilla and Byrav Ramamurthy. Agent based intrusion detection and response system for wireless LANs. In *Communications*, pages 492–496. IEEE, May 2003.

[7] Michael J. Riezenman. Cellular security: better, but foes still lurk. *IEEE Spectrum*, pages 39–42, June 2000.

[8] Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis. Detection of transient in radio frequency fingerprinting using signal phase. In *Wireless and Optical Communications*, pages 13–18. ACTA Press, July 2003.

[9] S.J. Russell and P. Norvig. *Artificial Intelligence: A Modern Approach*. Prentice Hall, 2002.

[10] John G. Proakis and Dimitris G. Manolakis. *Digital Signal Processing*. Prentice Hall PTR, 1996.

[11] Stephane Mallat. *A Wavelet Tour of Signal Processing*. Academic Press, 1999.

[12] H. Choe, C.E. Poole, A.M. Yu, and H.H. Szu. Novel identification of intercepted signals from unknown radio transmitters. *SPIE*, 2491:504–516, 1995.

[13] Ralph D. Hippenstiel and Yalcin Payal. Wavelet based transmitter identification. In *International Symposium on Signal Processing and its Applications*, Gold Coast Australia, August 1996.

[14] Laurene Fausett. *Fundamentals of Neural Networks Architectures, Algorithms and Applications*. Prentice Hall, 1994.

[15] D. Shaw and W. Kinsner. Multifractal modelling of radio transmitter transients for classification. In *Communications Power and Computing*, pages 306–312, Winnipeg Manitoba, May 1997. IEEE.

[16] Andrew Hunter. Feature selection using probabilistic neural networks. *Neural Computing and Applications*, 9:124–132, 2000.

[17] X.-R. Li Y. Bar-Shalom and T. Kirubarajan. *Estimation with Applications to Tracking and Navigation*. John Wiley, 2001.

[18] Jr. Joseph F. Hair, Rolph E. Anderson, and William C. Black Ronald L. Tatham. *Multivariate Data Analysis*. Prentice Hall, 1998.

[19] Johan Zuidweg and Han Zuidweg. *Next Generation Intelligent Networks*. Artech House, 2002.

[20] H. Gunes Kayacik, A. Nur Zincir-Heywood, and Malcolm I. Heywood. On the Capability of an SOM based Intrusion Detection System. In *Neural Networks*, pages 1808–1813. IEEE, July 2003.

[21] K.J. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. *Radio Science*, 36:585–597, 2001.

[22] Oktay Ureten and Nur Serinken. Detection of radio transmitter turn-on transients. *Electronic Letters*, 35:1996–1997, 1999.

[23] D.F. Specht. Probabilistic neural networks for classification mapping or associative memory. In *IEEE International Conference on Neural Networks*, pages 525–532. IEEE, 1988.

[24] Panu Somervuo and Teuvo Kohonen. Self-Organizing Maps and Learning Vector Quantization for Feature Sequences. *Neural Processing Letters*, 10:151–159, 1999.

[25] J. Toonstra and W. Kinsner. Transient analysis and genetic algorithms for classification. In *WESCAN*. IEEE, 1995.