Wireless security through RF fingerprinting

Sécurité sans fil par une empreinte digitale RF

Oktay Ureten and Nur Serinken*

The process of identifying radio transmitters by examining their unique transient characteristics at the beginning of transmission is called RF fingerprinting. The security of wireless networks can be enhanced by challenging a user to prove its identity if the fingerprint of a network device is unidentified or deemed to be a threat. This paper addresses the problem of identifying an individual node in a wireless network by means of its RF fingerprint. A complete identification system is presented, including data acquisition, transient detection, RF fingerprint extraction, and classification subsystems. The classification performance of the proposed system has been evaluated from experimental data. It is demonstrated that the RF fingerprinting technique can be used as an additional tool to enhance the security of wireless networks.

Le processus d'identification des radios émetteurs par l'examen de leurs caractéristiques uniques transitoires au début d'une transmission est désigné par la prise d'empreinte digitale RF. La sécurité des réseaux sans fil peut être améliorée par la requête envers un usager de prouver son identité, si l'empreinte d'un élément du réseau n'est pas identifiée ou si elle est considérée comme une menace. Cet article considère le problème d'identification d'un noeud individuel dans un réseau sans fil au moyen de son empreinte RF. Un système d'identification complet est présenté, incluant l'acquisition d'information, la détection des caractéristiques uniques transitoires, l'extraction de l'empreinte RF, ainsi que la classification. La performance de la classification du système proposé a été évaluée au moyen de données expérimentales. Il a été démontré que la technique d'empreinte RF peut être utilisée en tant qu'outil additionnel pour l'amélioration de la sécurité de réseaux sans fil.

Keywords: RF fingerprinting; transient classification; transmitter identification; wireless security

I. Introduction

In recent years, ad hoc networks have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research efforts assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multi-hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wireline networks, the unique characteristics of ad hoc networks pose a number of non-trivial challenges to security design. Consequently, the existing security solutions for wired networks do not directly apply to the ad hoc network domain. Novel approaches and additional tools are required in order to increase security.

In this paper, RF fingerprinting is proposed as a means of enhancing the security of wireless networks. When a radio transmitter is activated, the RF signal emitted from the transmitter shows a transient behaviour with respect to instantaneous frequency and amplitude. Transient signal behaviour is attributable to a variety of sources, such as the acquisition characteristics of frequency synthesis systems, modulator subsystems, and RF amplifiers. The duration of the transient behaviour may change, depending on the type and model of the transmitter. Typically, differences are observable even for transmitters of the same type, mainly because of the manufacturing tolerances and the aging of the devices. The unique turn-on transient signal behaviour is called the RF fingerprint of a radio and can be used to identify the transmitter.

In military and civilian spectrum-management operations, identification of a specific RF transmitter is often used in traffic analysis or in the determination of the source of interference. To improve the safety and security of mobile VHF radio networks, transmitter identification systems relying on the unique turn-on characteristics of the radios have been reported [1]–[9]. Similarly, RF fingerprinting is used by cellular operators in order to prevent fraud and phone cloning [10]–[11].

*Oktay Ureten and Nur Serinken are with the Communications Research Centre, 3701 Carling Avenue, P.O. Box 11490, Stn H, Ottawa, Ontario K2H 8S2. E-mail: {oktay.ureten, nur.serinken}@crc.ca

RF fingerprinting can also be applied to ad hoc networks. The security of a network can be enhanced by challenging a user to prove its identity if the fingerprint of a network device is unidentified or deemed to be a threat. In this paper, the problem of identifying an individual node in a wireless network by means of its RF fingerprint is addressed. The task involves capturing the signal of interest, detection of the start of the transient in the signal data, extraction of the RF fingerprint, and classification of the unknown transient. A complete classification system, including data acquisition, transient detection, RF fingerprint extraction, and classification subsystems, is presented in this paper. In this study, IEEE 802.11b devices have been analyzed because of their widespread availability.

In Section II, certain physical-layer specifications of IEEE 802.11b devices are given, as the specifications are essential for understanding the RF signal characteristics, the construction of the data acquisition system, and the transient detection process. In Section III, the experimental data acquisition setup is illustrated. Differences among the fingerprints of various IEEE 802.11b devices are presented in Section IV. Transient detection, RF fingerprint extraction, and classification subsystems are detailed in Section V. Classification tests and their results are summarized in Section VI. Conclusions and directions for future work are discussed in Section VII.

II. WiFi signal characteristics

The IEEE 802.11b standard defines the physical layer of WiFi devices. WiFi is the popular name for wireless local area networks based on the IEEE 802.11b standard. A detailed explanation of the WiFi physical layer is given in [12]. A brief summary of some spectral and time-domain characteristics of WiFi signals is given here.

WiFi devices operate in the 2.4 GHz industrial, scientific, and medical (ISM) band. The number of operating channels and the centre frequency of each channel, as allocated by regulatory bodies in North America, Europe, and Japan, are listed in the standard. The transmit-

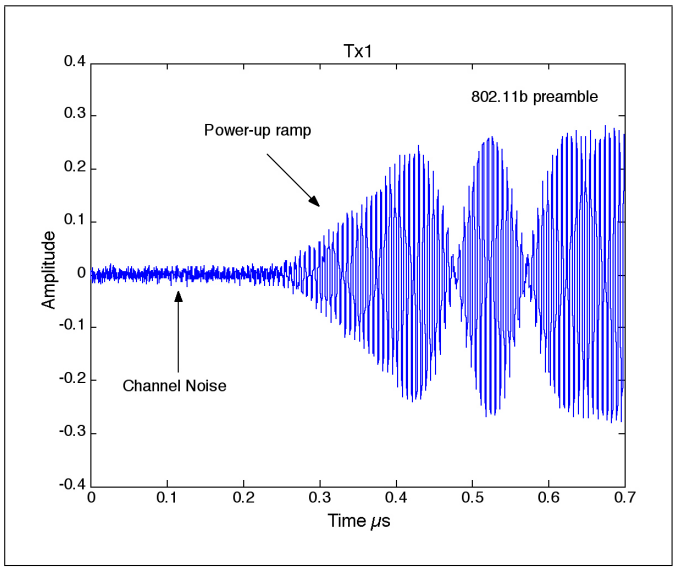


Figure 1: *Typical waveform captured from a WiFi device.*

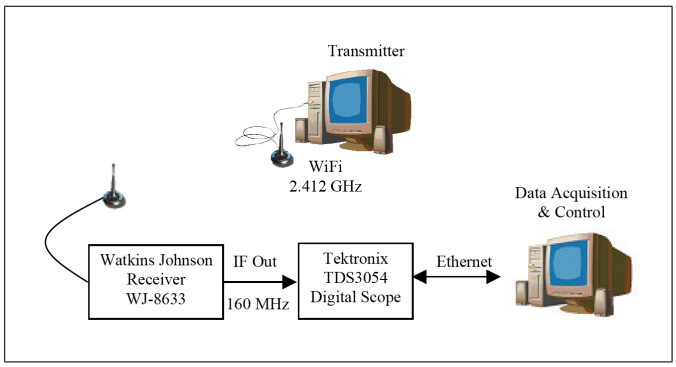


Figure 2: *Data capture system.*

ted centre-frequency tolerance specified in the standard is a maximum of ± 25 parts per million (ppm).

Four modulation formats and data rates (1, 2, 5.5, and 11 Mbits/s) are specified in the high-rate physical layer. For 11 Mbits/s, 8-chip complementary code keying (CCK) is used with a chip rate of 11 Mchips/s. At this data rate, 8 bits are transmitted per symbol.

According to the standard, transmitted spectral products of WiFi signals shall be less than -30 dBr (decibels relative to the $\sin(x)/x$ peak) for frequencies between 11 and 22 MHz from the centre frequency and shall be less than -50 dBr for frequencies more than 22 MHz from the centre frequency, yielding an effective bandwidth of 22 MHz. The standard also specifies a gradual transmit power-up and power-down scheme in order to ensure that power is not spread to adjacent channels during device turn-on and turn-off.

Fig. 1 shows a typical waveform captured from a WiFi device operating at a data rate of 11 Mbits/s. Pre-trigger channel noise samples and post-trigger IEEE 802.11b preamble data are shown together with the actual transient signal.

III. Experimental setup and data acquisition

A data acquisition system was designed to capture IEEE 802.11b WiFi signals in the 2.4 GHz ISM band. The system is shown in Fig. 2. The IEEE 802.11b WiFi cards were installed in computers and set to ad hoc networking mode on radio channel 1 at 2.412 GHz. WiFi radios transmit packets at regular intervals to announce their presence to other devices that are listening on the same radio frequency. A Watkins-Johnson model WJ-8633 receiver was tuned to WiFi channel 1 and connected to an omnidirectional antenna for reception of burst transmissions. The WJ-8633 is a VMEbus eXtensions for Instrumentation (VXI) bus receiver controlled by a personal computer. The intermediate frequency (IF) bandwidth was set to 80 MHz. The IF output of the WJ-8633 at 160 MHz was connected to a digital oscilloscope. The oscilloscope has an Ethernet interface for control and data acquisition/transfer functions. An oscilloscope control program was written for a personal computer to collect transients from WiFi transmitters. Signals were sampled at a rate of 5 GSamples/s with 9-bit resolution. One hundred transmissions were collected from eight different WiFi radios.

IV. RF fingerprint characteristics

Waveforms captured from four different WiFi radios are represented in Fig. 3, exposing differences among the waveforms of different radios. Differences are observed even among the waveforms of radios of the same make and model, such as Tx1 and Tx2.

More distinctive features are observed from the instantaneous attributes (complex amplitude and phase angle) of the signals, the calculation of which is explained in Section V. Instantaneous amplitudes of the waveforms shown in Fig. 3 are plotted in Fig. 4. A gradual increase in power level is seen explicitly from the amplitude profiles. Different ramp-up characteristics observed during the power-up interval can be used to discriminate among the wireless devices, as the differences are significant.

Instantaneous phase angles of the waveforms shown in Fig. 3 are plotted in Fig. 5. In these plots, vertical axes are shifted relative to each other to display the profiles on the same scale. The curvature and slope variations in the phase profiles are the result of frequency shifts from the carrier. The phase plots have a shorter transient duration prior to settling to a steady state.

V. Fingerprint classification system

The RF fingerprinting system consists of preprocessing, detection, feature extraction, and classification stages. During the preprocessing stage, the Hilbert transform of the captured signals is taken to obtain the instantaneous attributes of the signals. The signals are then down-converted to baseband in software. The turn-on instant of the transmitters is estimated for the captured signals. Features are then calculated from the instantaneous attributes of the signals, and a neural network classifier is trained with the computed features.

A. Preprocessing

Hilbert transformation is a technique for generating complex-valued analytic functions from real-valued data [13]. The resulting waveform has a single-sided spectrum and is useful in calculating the instantaneous attributes of a signal. The instantaneous amplitude and phase are computed using the real and imaginary parts of the complex-valued signal.

The IF output of the receiver used for data collection is at 160 MHz. Because of reference oscillator inaccuracies, there is always an offset from the carrier frequency. As the amount of frequency offset may vary, the offset is estimated for every received signal by calculating the peak location of the power spectral density. The received signal at the IF output is then down-converted to baseband using the estimated frequency value.

B. Detection

The objective of the detection stage is to determine the exact time instant at which the transmitter is turned on. Performance of the detection stage is significant because inaccurate detection adversely affects

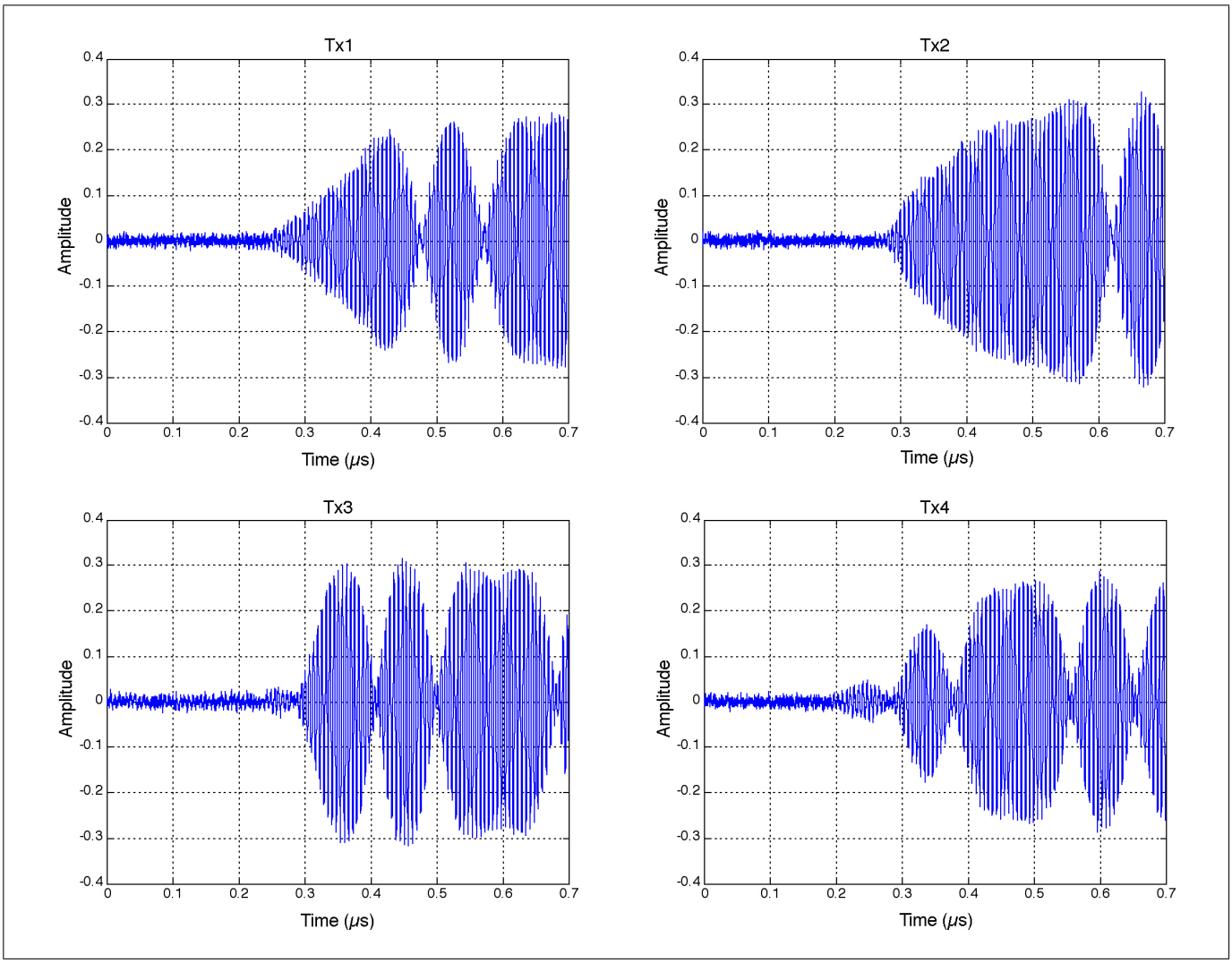


Figure 3: *Instances of waveforms captured from four different WiFi radios.*

the fingerprinting stage, and thus the classification performance of the overall system is reduced.

The detection of the turn-on transients of VHF radios is based on the change-point detection principle, in which the detector determines the instant at which the received power level exhibits a sudden increase. The abrupt-change detector system was successfully used for VHF radios, where there is a sudden change in the power level at the transition from channel noise to turn-on of the radio [14]–[15]. However, as indicated in Section II, the WiFi standard specifies that the output power level must be ramped up smoothly. Following the channel noise, the received power level increases gradually after the transmitter is turned on. If the change detector lags behind the actual starting point, characteristics important for classification may be lost. In this study, transient detection is achieved using a Bayesian ramp change detector, which estimates the time instant at which the signal power starts its gradual increase. In this approach, amplitude data is modelled as a piecewise continuous signal, and the model assumes a linear increase in the power level of the radio during startup [16].

C. Feature extraction

Feature extraction is the process of generating characteristic attributes from the raw signal. Extracted features can either be obtained from a hypothetical or pure mathematical concept that will reduce the dimension of the input space efficiently, or they can be selected based on the physical nature of the problem. An efficient feature extraction algorithm should minimize the length of the feature vector without losing the necessary components for classification [17].

In Section IV, it is shown that there are distinctive features in the amplitude characteristics of the RF waveforms. Amplitude profiles of 100 signals from eight WiFi transmitters are shown in Fig. 6(a), where the amplitude levels are coded with different gray levels. It is seen from the figure that amplitude profiles are visually distinctive for most of the transmitters. Even though the transients from Tx4 and Tx6 look similar to the transients from Tx5 and Tx8, respectively, a neural network classifier can distinguish minor differences among them. Another feature of the collected transients is that the 100 transient signals collected from each radio are consistent within each class, i.e., the same features are produced in different realizations. These attributes make the amplitude profile a good candidate as the feature vector for classification.

Phase profiles of the RF waveforms from the WiFi transmitters are illustrated in Fig. 6(b). As shown, there is no definite pattern that will help to discriminate among the transmitters. The reason for the irregular nature of the pattern is that the phase variations have a very small dynamic range, as seen from Fig. 5. The duration in which the phase variations settle is much shorter than that of the carrier's amplitude stabilization. This means that features extracted from the phase profiles will be more prone to detection errors. As a result, the phase profiles are not included as part of the feature vectors.

To reduce the dimensionality of the feature space, principal component analysis (PCA) can be used [18]. PCA is a multivariate procedure that rotates the data such that maximum variability is projected onto the axes. Essentially, a set of correlated variables is transformed into

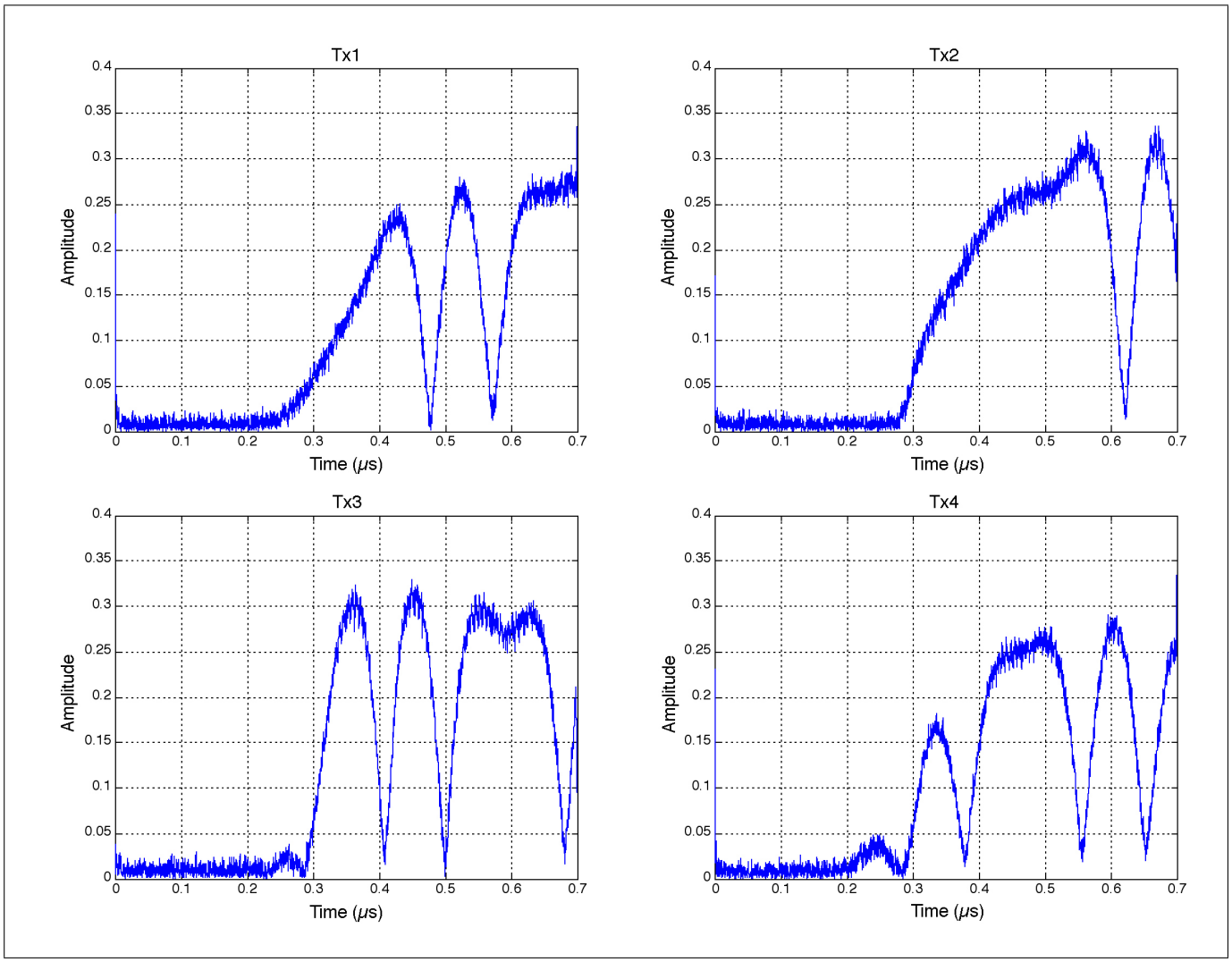


Figure 4: *Instantaneous amplitudes of the waveforms shown in Fig. 3.*

a set of uncorrelated variables, which are ordered by decreasing variability. By ordering the eigenvectors in descending order (largest first), one can create an ordered orthogonal basis, with the first eigenvector having the direction of largest variance of the data. In this way, one can find directions in which the data set has the most significant amounts of energy.

D. Classification

Classification is the task performed by a network trained to respond when an input vector resembling a learned vector is presented. The network recognizes the input as one of the original target vectors. In this study, a probabilistic neural network (PNN) is used as a classifier. The PNN provides a general solution to pattern classification problems by following an approach developed in statistics called Bayesian classification. Bayes theory takes into account the relative likelihood of events and uses *a priori* information to improve prediction. The Bayesian network paradigm also uses Parzen estimators, which were developed to construct the probability density functions required by Bayes theory. Detailed information about the PNN can be found in [19].

VI. Classification tests

In order to evaluate the performance of the system, classification tests were performed. A set of 800 signals was created by capturing 100 transient signals from eight WiFi radios. For each radio, 20 of the 100 transients were chosen randomly to create a training set. The remaining 80 transients were used as a test set. A PNN was created using the training set, and its performance was evaluated using the test set. The classification error was calculated by dividing the number of misclassified signals into the number of total test signals. This process was called a classification test. In each classification test, 640 unknown transient signals were classified.

The following classification tests were performed.

A. Benchmark test

This test aimed to measure the performance of the basic system. In the basic system, amplitude profiles were used as the feature vector. The length of the feature vector was chosen to be 1024 samples, which corresponds approximately to 200 ns.

One hundred classification tests were run for the benchmark test. The results of the classification tests are shown as a histogram in Fig. 7(a). The average value of the classification error was found to be 2%.

B. Transient duration test

The purpose of this test was to investigate the effect of feature-vector length on the classification rate. In the test, feature vectors of length 256, 512, 1024, 2048, and 4096 samples were tested. For each window length, 100 classification experiments were run. The average values of the classification error were found to be 35%, 4%, 2%, 3%, and

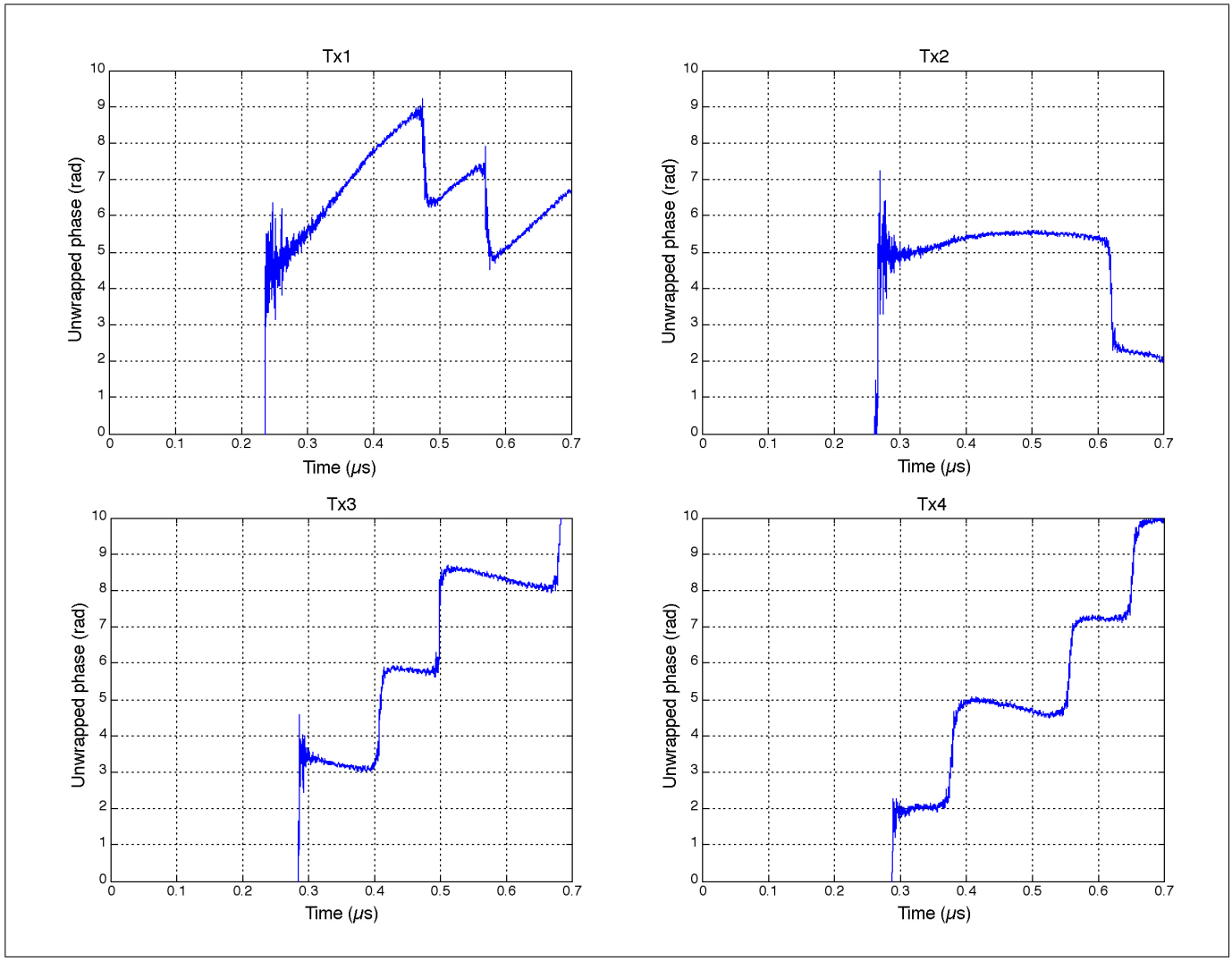


Figure 5: *Instantaneous phase angles of the waveforms shown in Fig. 3.*

4% respectively. The best classification rate was obtained when the window length was set to 1024 samples.

C. Dimension reduction test

In this test, performance of the dimension reduction technique was evaluated. One hundred classification tests were run. In each test, principal components were calculated from the training set. The training set was then projected onto a subset of principal components whose number was determined by the energy concentration of the eigenvalues. The number of principal components was set to 5 because 99% of the energy was concentrated in the first five eigenvectors. The test set was then projected onto the principal components, which were calculated from the training set. Computed feature values were then applied to the trained PNN, and the classification error was calculated. The results of 100 classification tests are shown as a histogram in Fig. 7(b). The average value of the classification error was found to be 2%.

VII. Summary and conclusions

In this work, an experimental system was designed for capturing and identifying RF waveforms from WiFi devices as an authentication tool. It is possible to adapt the developed test bed to simulate various case scenarios and test different threat models, depending on desired application and specific requirements. In this study, an ad hoc network containing eight nodes was considered. It was assumed that RF fingerprints of the nodes, i.e., training samples, were captured and stored before the network was deployed. During testing, RF transmissions were captured while the radios were in operation. The designed system was able to classify the captured signals with an error rate of 2%.

The achieved high classification rate demonstrates that the RF fingerprinting technique can be used as an efficient tool to enhance the security of wireless networks. In operation, transmitter fingerprints that are not known or are deemed to be a threat could be used to initiate protective actions. For example, the suspect device could be challenged to prove its identity or access to services could be restricted.

It was noted that the carrier's amplitude characteristics during startup offer more useful features than its phase characteristics. Although the phase profiles have distinctive features, their dynamic range is smaller. Feature vectors extracted from the phase characteristics can be explored in applications where the amplitude characteristics do not provide enough separation among the radios when the system is scaled to fit networks containing tens of radios, as in [9]. For the scenario considered in this paper, the amplitude characteristics provided sufficient information for successful separation of the transmitters.

As observed from the captured data, the duration of the transient state may vary from one transmitter to another. In the extraction of the feature vector, determination of a suitable signal length is important. As shown in the paper, if the signal length is set shorter than the actual transient-state duration, important characteristic information is

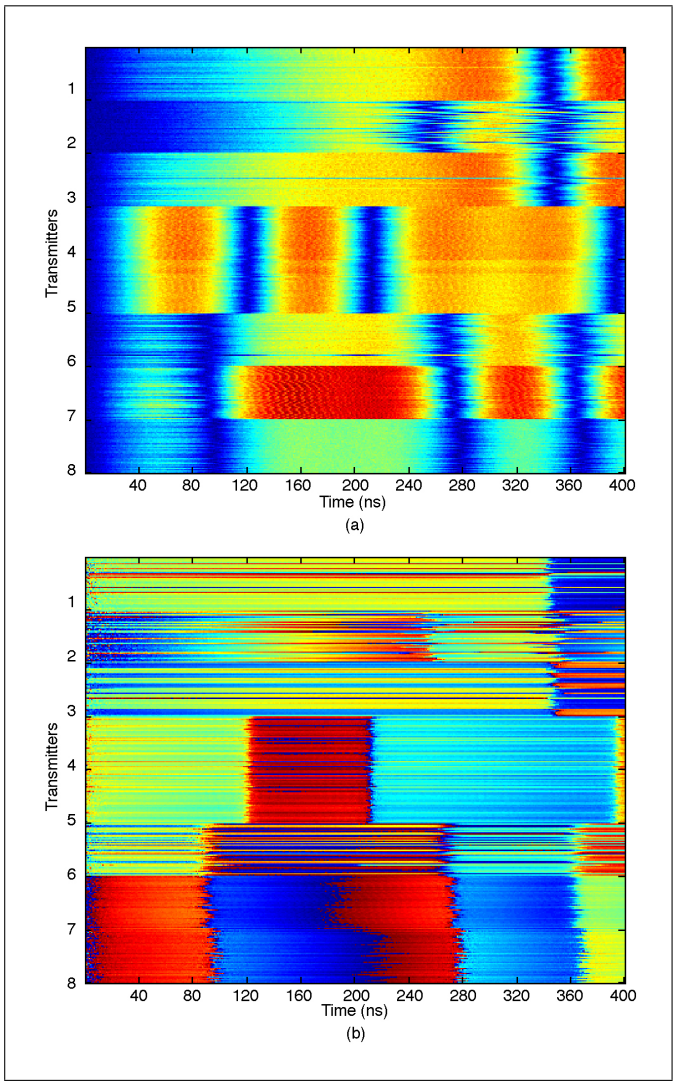


Figure 6: *(a) Amplitude profiles of eight transmitters. (b) Phase profiles of eight transmitters.*

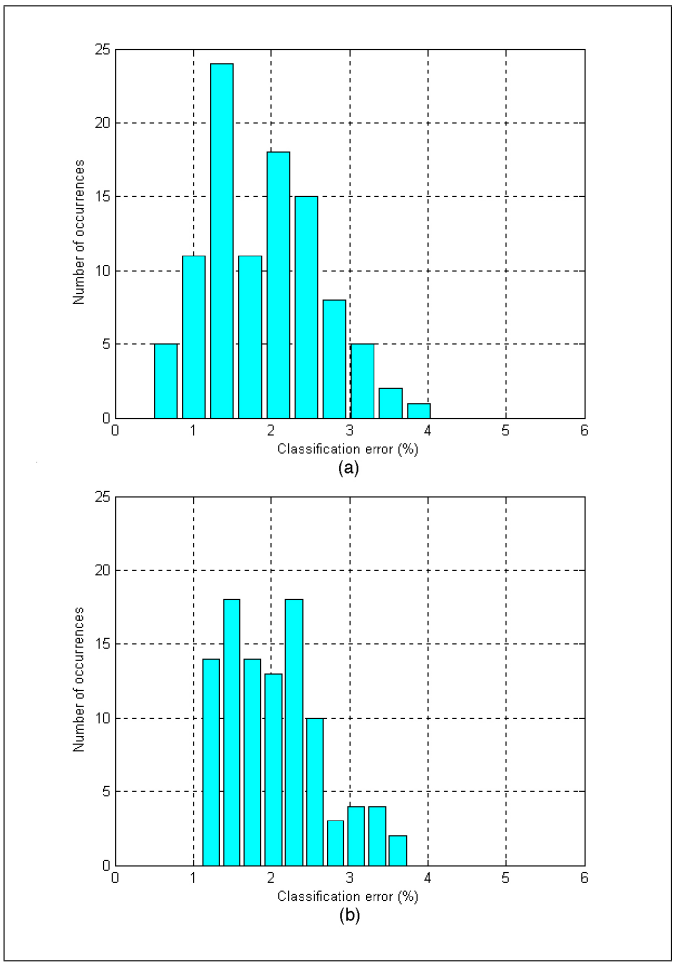


Figure 7: *Histogram of the classification error for (a) the benchmark test; (b) the dimension reduction test.*

lost, and performance of the classification system degrades. If, on the other hand, the signal length is set longer than the transient-state duration, then dominant turn-on characteristics may be obscured, as the signal data after the transient is similar for all transmitters. It was found that a signal duration of around 200 ns results in the best classification performance.

Because the PNN classifier stores all of the training vectors in memory, memory requirement and processing time grow with the number and size of training vectors. In this work, we reduced the dimension of the feature vector by using PCA. Since the energy of the principal components is concentrated in a few eigenvectors, the use of dimension-reduced vectors did not cause any classification performance loss. Moreover, lower memory requirement was achieved, and the PNN testing became faster.

In this work, RF fingerprints were collected in a "controlled" environment, i.e., there were no significant temperature changes or interference sources. Directions for extension currently being pursued include various realistic case scenarios under varying environmental conditions. Environmental changes would certainly degrade the performance of a transmitter identification system because of the minute changes in the characteristics of the transient signals, especially in the plurality of transmitters that have very similar amplitude and/or phase characteristics. In this case, creating a larger training set that contains samples of transients captured at varying temperature levels will improve the classification performance significantly, as reported in [9]. The classification performance of a transmitter identification system in noisy environments can be improved by means of the noise injection technique described in [8]. These two techniques, tested with VHF radio networks, can be directly applied to WiFi networks.

Acknowledgements

This work was supported by Industry Canada's Spectrum Engineering Branch.

References

[1] J. Toonstra and W. Kinsner, "A radio transmitter fingerprinting system ODO-1," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, Calgary, Alta., 1996, pp. 60–63.

[2] D. Shaw and W. Kinsner, "Multifractal modeling of radio transmitter transients for classification," in *Proc. IEEE Conf. Commun. Power and Computing*, Winnipeg, Man., 1997, pp. 306–312.

[3] N. Serinken and O. Ureten, "Generalised dimension characterization of radio transmitter turn-on transients," *IEE Electron. Lett.*, vol. 36, June 8, 2000, pp. 1064–1066.

[4] O. Ureten and N. Serinken, "Detection, characterisation and classification of radio transmitter turn-on transients," in *Multisensor Fusion*, ed. A.K. Hyder et al., Dordrecht, Netherlands: Kluwer Academic Publishers, 2000, pp. 611–616.

[5] H.C. Choe, C.E. Poole, A.M. Yu, and H.H. Szu, "Novel identification of intercepted signals from unknown radio transmitters," in *Proc. SPIE Wavelet Applications II*, Orlando, Fla., 1995, pp. 504–517.

[6] R.D. Hippenstiel and Y. Payal, "Wavelet based transmitter identification," in *Proc. Int. Symp. Signal Processing and its Applications*, Gold Coast, Australia, 1996, pp. 740–743.

[7] K.J. Ellis and N. Serinken, "Characteristics of radio transmitter fingerprints," *Radio Sci.*, vol. 36, no. 4, 2001, pp. 585–597.

[8] O.H. Tekbas, O. Ureten, and N. Serinken, "Improvement of transmitter identification system for low SNR transients," *IEE Electron. Lett.*, vol. 40, no. 3, Feb. 5, 2004, pp. 182–183.

[9] O.H. Tekbas, N. Serinken, and O. Ureten, "An experimental performance evaluation of a novel transmitter identification system under varying environmental conditions," *Can. J. Elect. Comput. Eng.*, vol. 29, no. 3, July 2004, pp. 203–209.

[10] M.B. Frederick, "Cellular telephone anti-fraud system," U.S. Patent No. 5,448,760, Sept. 5, 1995.

[11] K.D. Hawkes, "Transient analysis system for characterizing RF transmitters by analyzing transmitted RF signals," U.S. Patent No. 5,758,277, May 26, 1998.

[12] IEEE Std 802.11b-1999, Part 11, *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher-speed physical layer extension in the* 2.4 *GHz band*, 2000.

[13] B. Boashash, "Estimating and interpreting the instantaneous frequency of a signal: Part I: Fundamentals," *Proc. IEEE*, vol. 80, no. 4, Apr. 1992, pp. 520–538.

[14] O. Ureten and N. Serinken, "Bayesian detection of radio transmitter turn-on transients," in *Proc. IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing*, 1999, pp. 830–834.

[15] ———, "Detection of radio transmitter turn-on transients," *IEE Electron. Lett.*, vol. 35, Nov. 11, 1999, pp. 1996–1997.

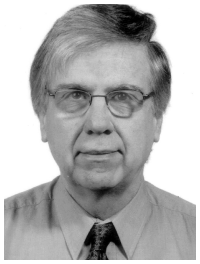
[16] ———, "Bayesian detection of WiFi transmitter RF fingerprints," *IEE Electron. Lett.*, vol. 41, no. 6, 2005, pp. 373–374.

[17] C.M. Bishop, *Neural Networks for Pattern Recognition*, New York: Oxford University Press, 2004, pp. 295–319.

[18] R. Duda, P. Hart, and D. Stork, *Pattern Classification*, 2nd ed., New York: John Wiley & Sons, 2001, pp. 115–117.

[19] D.F. Specht, "Probabilistic neural networks," *Neural Networks*, vol. 3, no. 1, 1990, pp. 109–118.

Oktay Ureten was born in Ankara, Turkey, in 1972. He received his B.S., M.S., and Ph.D. degrees in electronics engineering from the University of Ankara in 1993, 1995, and 2000, respectively. Between 1993 and 2000, he was a research and teaching assistant at the Electronics Engineering Department of Ankara University. He then worked at the National Research Institute of Electronics and Cryptology (UEKAE), Gebze, Turkey. From 2001 to 2005 he was affiliated with the Communications Research Centre in Ottawa, Ontario, Canada, first as an NSERC visiting fellow and then as a research scientist. Since 2005, he has been employed by the University of Ottawa, School of Information Technology and Engineering (SITE), Ottawa, Ontario, Canada. His research interests include signal processing and radio communication systems with special emphasis on synchronization and channel estimation techniques for OFDM systems.



Nur Serinken has a Ph.D. in electrical engineering from Loughborough University, Leicestershire, U.K. After graduation he started working at the Hirst Research Centre in the U.K. in 1974, and then joined Bell-Northern Research from 1977 to 1981 in Ottawa, Ontario, Canada. Since 1981 he has been working in the Terrestrial Wireless Research Group for the Government of Canada in the Communications Research Centre. Some of his research areas are wireless data transmission systems and radio transmitter identification for security applications. He has been participating in standardization activities within ITU-R and NATO committees.