WiMAX Mobile Subscriber Verification Using Gabor-Based RF-DNA Fingerprints

Donald R. Reising and Michael A. Temple
Department of Electrical & Computer Engineering
US Air Force Institute of Technology
Wright-Patterson AFB, OH 45433 USA
Email: [Donald.Reising Michael.Temple]@afit.edu

***Abstract*—Considerable effort has been put forth to exploit physical layer attributes to augment network bit-level security mechanisms. RF-DNA fingerprints possess such attributes and can be used to uniquely identify authorized users and mitigate unauthorized network activity. These attributes are unique to a given electronic device and difficult to replicate for cloning, spoofing, etc. Device discrimination (*identification*) of WiMAX devices has been successfully demonstrated using a one-to-many comparison against a pool of unknown device fingerprints. The work here now addresses device *authentication* using a one-to-one comparison against the specific fingerprint associated with a claimed bit-level identity (MAC, SIM, IMEI, etc). The concept is demonstrated using Gabor-based RF-DNA extracted from near-transient burst responses of 802.16e WiMAX mobile subscriber devices–device *identification* of better than 96% is achieved with *verification* EER ≤ 1.6% for $SNR \geq -3$ dB.**

I. Introduction

Security enhancement via exploitation of Physical (PHY) layer attributes within the Open System Interconnection (OSI) model remains of interest. Such attributes can be used to uniquely identify authorized network devices while mitigating unauthorized activity [1]–[9]. The work in [4]–[9], successfully exploited imitation-resistant Radio Frequency "Distinct Native Attributes" (RF-DNA) from selected modulated signal regions to demonstrate device discrimination. The RF-DNA attributes are 1) sufficiently "distinct" to facilitate persistent cross-device discrimination and 2) "native" in that variations due to hardware implementation, component type, manufacturing processes, etc., impart unintentional "coloration" within intentionally modulated signal responses. RF-DNA has also enabled discrimination of non-radiating devices, or components contained therein such as Integrated Circuits (IC), using unintentional emissions [10].

A majority of related RF-DNA fingerprinting work has been focused on device *identification* [4]–[9]. In this case, the network recognition system performs a "one-to-many" comparison to determine the identity of an *unknown* device. This is done by comparing the *unknown* device's current RF-DNA ("challenge" fingerprint) to each RF-DNA reference stored for known (authorized) network devices. For networks supporting many devices, the "one-to-many" comparison may not be practical when timely and accurate authentication is required to support users who enter/leave frequently or randomly (e.g., cellular-based networks, public WiFi hotspots, etc).

RF-DNA fingerprints have been successfully used for "one-to-one" comparison and device *verification* to authenticate the identity of ICs [10]. In this case, the network recognition system performs a comparison to determine the authenticity of a current *unknown* device fingerprint using its claimed bit-level identity, e.g., Medium Access Control (MAC) address, Subscriber Identity Module (SIM) number, International Mobile Equipment Identity (IMEI) number, etc. This is done by comparing the *unknown* device's current RF-DNA ("challenge" fingerprint) with the stored RF-DNA reference associated with the claimed bit-level identity. Based upon [10]–[12], device *verification* is demonstrated here using RF-DNA fingerprints extracted from IEEE 802.16e Worldwide Interoperability for Microwave Access (WiMAX) Mobile Subscriber (MS) signals.

WiMAX signals are considered here for demonstration given 1) commercial equipment is readily available (Alvarion BreezeMAX Extreme 5000 equipment used here), 2) the anticipated proliferation of IEEE 802.16e compliant equipment, or variants thereof such as Long Term Evolution (LTE), and 3) the potential adoption of a WiMAX variant for next generation airport communications by the FAA, Eurocontrol and International Civilian Aviation Organization (ICAO) [13], [14]. Furthermore, WiMAX systems use a Wireless Access Point (WAP) architecture which remains among the top 10 Information Technology (IT) security threats [15]. The WAP security threat (unauthorized access, device spoofing, cloning, etc.) is of even greater concern when considering WiMAX implementations involving public safety [14].

Work in [4], [6], [9], [16] was based on RF-DNA extracted from 1-D signal features (amplitude, phase, frequency, power spectral density, etc.) from both near-transient (802.11a preamble) and non-transient (GSM midamble) signal regions, with subsequent device *identification* performed using Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification. These 1-D signal features are associated with pre-defined "standard" signal responses typically incorporated by-design and used for channel estimation, device synchronization, network timing and control, etc. In theory, these standard responses would be *identical* for all standard-compliant devices. In practice, they actually contain unintentional coloration that provides RF-DNA uniqueness. While pre-defined "standard" responses have not been observed in Alvarion BreezeMAX 5000 MS transmissions [17], this earlier work has

identified a burst "power-up" bias in the near-transient region that has been successfully exploited using RF-DNA based on 2-D Gabor Transform (GT) signal features.

Given successful device *identification* in [17], as well as successful demonstration of device *verification* using IC emissions in [10], the work here expands upon this previous activity using 2-D GT RF-DNA fingerprints for *verification* of 802.16e WiMAX MS devices. Results presented in Sect. IV using Receiver Operating Characteristic (ROC) curves and Equal Error Rate (EER) analysis demonstrate effectiveness of the proposed approach–device *identification* of better than 96% is achieved with *verification* EER $\leq 1.6\%$ for $SNR \geq -3$ dB.

The remainder of this paper is organized as follows. Section II provides an overview of the 802.16e WiMAX network used for demonstration. Section III-A describes the experimental signal collection procedure. As in [17], this work utilizes Gabor Transform (GT) based RF-DNA fingerprints. GT RF-DNA fingerprint feature generation is described in Sect. III-B. Section III-C and Section III-D describe the device *identification* and *verification* techniques, respectively. Section IV provides demonstration results for device *identification* and *verification*, followed by a summary and conclusion in Sect. V.

II. WiMAX Demonstration System

An 802.16e WiMAX network, comprised of Alvarion BreezeMAX Extreme 5000 equipment, using 60/40 Time Division Duplexing (TDD) was used for experimental demonstration. The first 60% of the $T_F = 5\ mSec$ TDD frame was allocated for BTS Down-Link (DL) transmission and the remaining 40% allocated for MS Up-Link (UL) transmission [18]. The RF channel occupied a bandwidth of $W_{ch} = 5$ MHz centered at $f_c = 5475$ MHz. Previous work in [17] identified three distinct UL sub-frame responses for the Alvarion network, including what are called *Data-Only*, *Range-Plus-Data*, and *Range-Only* modes. All subsequent discussion as well as results presented in Sect. IV are based exclusively on the network operating in the *Range-Only* mode.

Collected mobile WiMAX MS signals lack a distinct response region where a "standard" response is included for synchronization, timing, control, etc. [17]. This is quite different from previously investigated signals such as GSM and 802.11 signals [4]–[6], [16]. However, the three signal responses from all three of the previously noted operating modes do contain a "power-up" bias that spans the UL sub-frame. The typical bias response can be seen in Fig. 1 as the "step" occurring during the first 2.0 μSec of the 16 μSec UL sub-frame response (the remaining 14.0 μSec is not of interest here and intentionally omitted for graphic clarity). It is believed that the bias is incorporated by design to stabilize electronic component response and mitigate adverse peak-to-average power ratio effects that frequently occur in OFDM. The "near-transient" response in Fig. 1 has thus far yielded the best results for generating RF-DNA [17] and is used here for all results presented in Sect. IV.

III. Demonstration Methodology

A. Signal Collection & Detection

The signal detection and collection process used in this work was adopted from [6]. An Agilent E3238S-based RF Signal Intercept and Collection System (RFSICS) was used for all signal collections and is tunable from 20.0 MHz to 6.0 GHz with a $W_{RF} = 36.0$ MHz RF filter [19]. The selected frequency band is down-converted to a $f_{IF} = 70$ MHz Intermediate Frequency (IF) and digitized by a $b = 12$ bit analog-to-digital converter (ADC) at a maximum rate of $f_s = 95$ mega-samples-per-second (Msps). During analog-to-digital conversion, the IF signal is down-converted to baseband, digitally filtered at a bandwidth $W_b = 9.28$ MHz, sub-sampled in accordance with Nyquist criteria, and subsequently stored as complex in-phase (I) and quadrature (Q) data. The collected 802.16e WiMAX MS devices and the RFSICS were co-located in an office building environment during collection, with emissions from $N_{MS} = 6$ Alvarion BreezeMAX Extreme MS devices used for demonstration. Collections were made when the MS under test transmitted in the *Range-Only* mode. Detection of the *Range-Only* bursts was performed using amplitude-based variance trajectory (VT) as implemented in [4]. Following detection of a *Range-Only* burst, the complex samples associated with the near-transient response were removed from the collection and stored for subsequent RF-DNA fingerprint generation.

B. Gabor-Based RF-DNA Fingerprinting

In previous work, RF-DNA fingerprints have been independently extracted from either time or spectral domain responses [4]–[7]. The work in [20], suggests the use of momentary and/or time localized energy as a function of frequency to describe a signal. The use of Time-Frequency (T-F) localization, shown across the T-F plane, captures this momentary and localized signal behavior. One method of T-F localization is the Discrete Gabor Transform (DGT) and is calculated as follows [20],

$$G_{mk} = \sum_{n=1}^{MN_\Delta} s(n) W^*(n - mN_\Delta) \exp^{-j2\pi kn/K_G}, \quad (1)$$

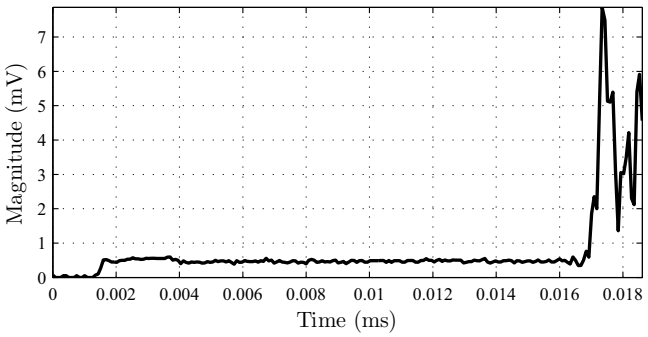
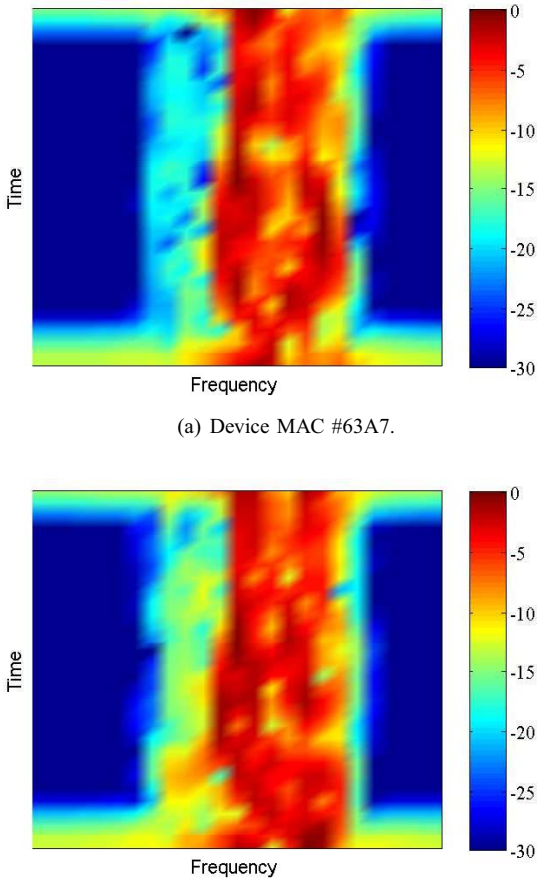


Fig. 1. WiMAX "near-transient" region of *Range-Only* magnitude response with constant bias present at the beginning of each UL sub-frame [17].

where G_{mk} are the Gabor coefficients, $s(n) = s(n + lMN_\Delta)$ is the periodic input signal, $W(n) = W(n+lMN_\Delta)$ is the periodic analysis window, N_Δ is the number of samples shifted, $m = 1, 2, \ldots, M$ for M total shifts, and $k = 0, 1, \ldots, K_G - 1$ for $K_G \geq N_\Delta$ and $mod(MN_\Delta, K_G) = 0$ satisfied [17]. In the case where $K_G = N_\Delta$, the Gabor transformation represents *critical sampling*. *Oversampling* occurs when $K_G > N_\Delta$ and is desirable when processing noisy data [20]–[23]. Therefore, oversampling is appropriate here since the near-transient responses of the *Range-Only* bursts are noisy; thus, enabling a more reliable analysis with varying SNR.

The T-F magnitude response is computed from the complex I-Q components of the Gabor coefficients G_{mk} in (1). Representative Gabor magnitude responses for two MS devices (identified by the last four digits of their MAC address) at $SNR = 0$ dB are shown in Fig. 2. Feature uniqueness captured during RF-DNA fingerprint generation is attributed to the observable localized differences as well as inconspicuous differences that may not be apparent in Fig. 2.

The DGT was implemented here using a Gaussian synthesis window $W(n)$ [20]. RF-DNA fingerprints are generated from the *normalized* (subtraction of the minimum value followed by division by the maximum value) magnitude-squared Gabor coefficients ($|G_{mk}|^2$). The resultant T-F surface (representative surface plot shown in Fig. 3) is subsequently divided into $N_T \times N_F$ 2-dimensional subregions (patches), vectorized to a length of N_{TF}, and statistics calculated(standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (κ)). The dimensions of each $N_T \times N_F$ patch were selected to ensure a minimum of $N_{TF} = 15$ entries for statistical calculation. For the results presented in Sect. IV, $M = 30$, $K_G = 25$, and $N_\Delta = 5$ which results in an oversampling factor of $N_{OS} = {}^{K_G}/_{N_\Delta} = 5$ [17]. Each RF-DNA fingerprint used for subsequent device *identification* and *verification* was comprised of $N_{feat} = 660$ elements.



(a) Device MAC #63A7.

(b) Device MAC #6373.

Fig. 2. Representative Gabor T-F magnitude responses for two 802.16e WiMAX MS devices. Responses based on near-transient responses of bursts collected during *Range Only* Mode at $SNR = 0$ dB.

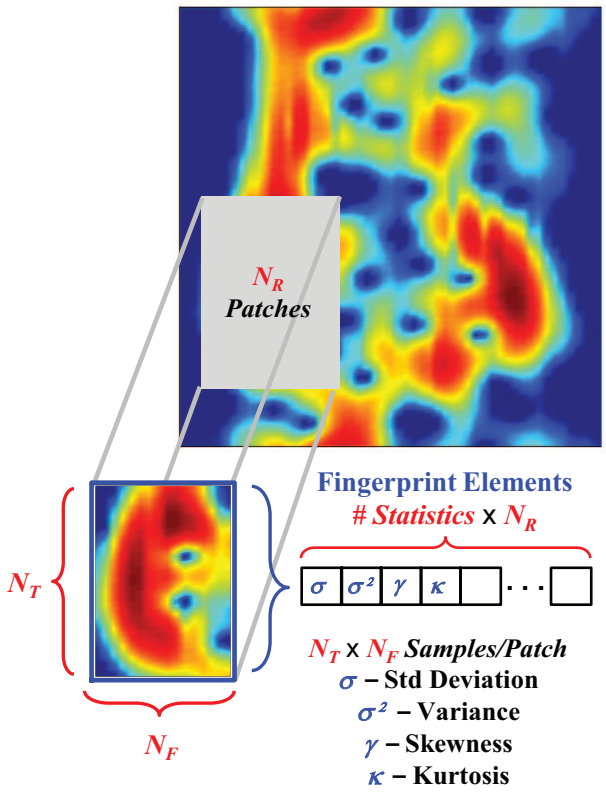


Fig. 3. Gabor-based RF-DNA fingerprint generation using $N_T \times N_F$ 2D patches taken from the centered and normalized magnitude-squared Gabor coefficients ($|G_{mk}|^2$) [17].

C. Device Identification

As in [6]–[10], [17], MDA/ML is used to perform feature selection and device *identification*. The goal of MDA is to reduce feature dimensionality while improving class separability. MDA extends Fisher's linear discriminant analysis (LDA) from a two-class case to the C-class case, where C is the total number of classes/devices. MDA is a linear operation that projects the samples (i.e., the RF-DNA fingerprints) to a $(C-1)$-dimensional subspace without reducing the power of class separability [24]. The MDA projection maximizes inter-class distances while minimizing intra-class spread. All of the results presented herein are projected into a $(C-1) = 5$-dimensional subspace.

In MDA, the between (inter-) ($\mathbb{S}_b$) and within (intra-) ($\mathbb{S}_\omega$) class scatter matrices are computed [24]:

$$\mathbb{S}_b = \sum_{i=1}^{C} P_i \Sigma_i, \tag{2}$$

$$\mathbb{S}_\omega = \sum_{i=1}^{C} P_i (\mu_i - \mu_0)(\mu_i - \mu_0)^T, \tag{3}$$

where Σ_i and P_i are the covariance matrix and prior probability of class c_i, respectively. Individual RF-DNA fingerprints are projected into the lower $(C-1)$-dimensional subspace by:

$$\mathbf{F}_i^{\mathbb{W}} = \mathbb{W}^T \mathbf{F}, \tag{4}$$

where $\mathbb{W}$ is the projection matrix formed from the $(C-1)$ eigenvectors of $\mathbb{S}_\omega^{-1}\mathbb{S}_b$. It is through the formation of the projection matrix $\mathbb{W}$ that results in the optimal ratio between the inter-class distances and intra-class variances [24]. For each class, a total of $N_t = 800$ samples are projected (noted by the superscript $\mathbb{W}$) during the MDA training process to form the projected training matrix $\mathbb{F}^{\mathbb{W}}$ as follows:

$$\mathbb{F}^{\mathbb{W}} = \left[\mathbf{F}_1^{\mathbb{W}}, \mathbf{F}_2^{\mathbb{W}}, \cdots, \mathbf{F}_{N_t}^{\mathbb{W}}\right]_{N_t \times 2}^T. \tag{5}$$

The mean vector $\widehat{\mu}_i^{\mathbb{W}}$ and covariance matrix $\widehat{\mathbf{\Sigma}}_i^{\mathbb{W}}$ are estimated and stored for each class' projected training samples. The pooled covariance matrix $\widehat{\mathbf{\Sigma}}_P^{\mathbb{W}}$, used in subsequent generation of each class' reference templates, is then calculated from the individual estimated class covariances $\widehat{\mathbf{\Sigma}}_i^{\mathbb{W}}$ as follows,

$$\widehat{\mathbf{\Sigma}}_P^{\mathbb{W}} = \frac{1}{N_f - N_{MS}} \sum_{i=1}^{N_{MS}} \widehat{\mathbf{\Sigma}}_i^{\mathbb{W}}, \tag{6}$$

where $N_f = 4800$ and $N_{MS} = 6$ are the total number of training samples and devices/classes, respectively.

A device's identity is determined through the comparison of its ***unknown*** RF-DNA fingerprint with each reference template that has been fit to each of the C training sets following feature selection. A classification decision is made by computing a similarity measure between the unknown RF-DNA fingerprint and each of the C known reference templates and assigning it to the class that results in the best match. As in [10], this work uses the Bayesian posterior probability, under the assumptions of uniform costs and equal priors, as the similarity measure. This approach optimally minimizes the classification error probability [24]. In the case of C devices, an ***unknown*** device's RF-DNA fingerprint $\hat{\mathbf{F}}$ is assigned to class c_i using:

$$P(c_i|\hat{\mathbf{F}}) > P(c_j|\hat{\mathbf{F}}) \ \forall j \neq i, \tag{7}$$

where $i \in \{1, 2, \ldots, C\}$ and $P(c_i|\hat{\mathbf{F}})$ is the conditional posterior probability that $\hat{\mathbf{F}}$ belongs to class c_i. Applying Bayes' Rule, the conditional probability is computed as [25]:

$$P(c_i|\hat{\mathbf{F}}) = \frac{P(\hat{\mathbf{F}}|c_i)P(c_i)}{P(\hat{\mathbf{F}})}. \tag{8}$$

Due to the assumption of equal prior probabilities ($P(c_i) = 1/C$) for all classes, $P(c_i)$ can be neglected when evaluating (8). Since the conditional probability is being calculated for a given fingerprint $\hat{\mathbf{F}}$, the denominator remains constant across all c_i and can be neglected as well. This reduces the decision criteria in (8) to maximizing the likelihood for $P(\hat{\mathbf{F}}|c_i)$ for all c_i. A multi-variate Gaussian distribution, computed using the pooled covariance matrix $\widehat{\mathbf{\Sigma}}_P^{\mathbb{W}}$ and appropriate estimated mean vector $\widehat{\mu}_i^{\mathbb{W}}$, is fitted to each class' training samples to form the reference templates. These reference templates are used to estimate the likelihood values of the given fingerprint $\hat{\mathbf{F}}$ [24]:

$$P(\hat{\mathbf{F}}|c_i) = \frac{1}{(2\pi)^{(C-1)/2} \left|\widehat{\mathbf{\Sigma}}_P^{\mathbb{W}}\right|^{1/2}} \cdot \exp\left(\mathcal{F}_e\right), \tag{9}$$

where,

$$\mathcal{F}_e = -\frac{1}{2}(\hat{\mathbf{F}} - \widehat{\mu}_i)^T (\widehat{\mathbf{\Sigma}}_P^{\mathbb{W}})^{-1} (\hat{\mathbf{F}} - \widehat{\mu}_i). \tag{10}$$

Average percent correct device classification is calculated as the percentage of the time the classifier correctly assigns an observed RF-DNA fingerprint to its true class over all trials. *K-fold cross-validation*, with $K = 5$, was implemented during the MDA/ML identification process to improve the reliability of the results. While the value selected for K can be data dependent, a value of $K = 5$ remains consistent with common practice which suggests values of $K = 5$ and $K = 10$ [26].

D. Device Verification

As in [10], device *verification* is used to authenticate a device's claimed identity (i.e., its MAC address, SIM number, IMEI number, etc.) against the specific reference template for the true class. As in device *identification*, the similarity measure used in device *verification* is the Bayesian posterior probability under the assumption of uniform costs and equal priors. However, for the case of verification, the resultant decision is binary and the device's claimed identity is determined to be authentic when the posterior probability meets or exceeds a predetermined threshold:

$$P(c|\mathbf{F}^{\mathbb{W}}) \geq t, \tag{11}$$

where $\mathbf{F}^{\mathbb{W}}$ is the given RF-DNA fingerprint, c is the class the device has claimed to belong, and t is the verification decision threshold. If the posterior probability fails to meet the verification decision threshold, then the device is deemed to be an impostor/impersonator.

As indicated in Table I, there are two types of errors that can be made during verification [10]–[12]:

1) *False Accept*: An impostor/impersonator is incorrectly identified as authentic

2) *False Reject*: An authentic device is identified as an impostor/impersonator

Through adjustment of the decision threshold t, system security can be increased to reduce false accept errors or decreased to reduce false reject errors. The Receiver Operating Characteristic (ROC) curve and corresponding Equal Error Rate (EER) is used to determine device *verification* performance [10], [11]. The ROC curve is created by plotting the

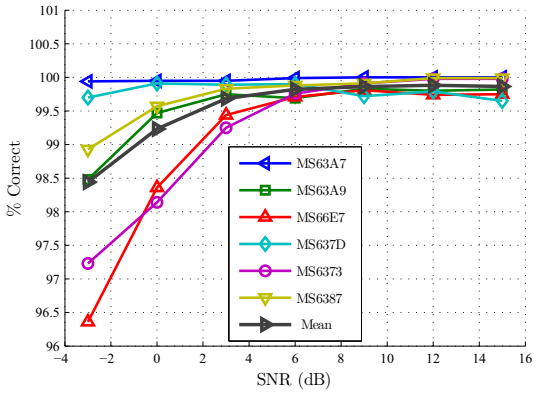


Fig. 4. Gabor-based RF-DNA fingerprinting: MDA/ML classification for individual WiMAX MS device identification with MAC ID as indicated.

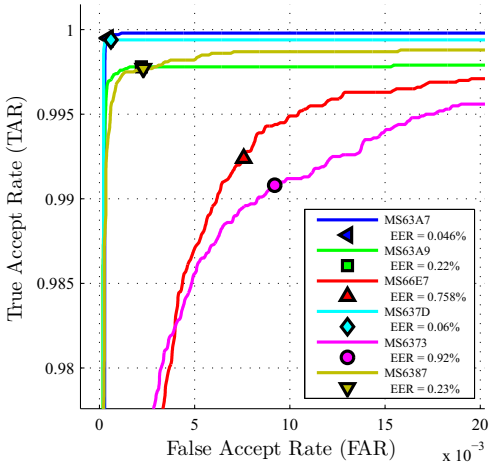


Fig. 5. ROC curves and corresponding EERs for individual WiMAX MS device *verification* performance at $SNR = 0$ dB.

True Accept Rate (TAR) versus False Accept Rate (FAR) as t changes across the interval $[0, 1]$ [11], [12]. The EER is defined as the point on the ROC curve where the False Reject Rate (FRR = 1 - TAR) equals the FAR. The EER is often used as a summary statistic for comparing classification performance across multiple systems. In general, the lower the EER value, the better the classification performance for the chosen system [10], [11]. Device *verification* results and the associated analysis are presented in Section IV.

IV. Results

A. Device Identification

Figure 4 shows MDA/ML device *identification* results for $N_{MS} = 6$ MS devices using Gabor-based RF-DNA fingerprints at $SNR \in [-3, 15]$ dB. The collection of 1000 near-transient responses per device and 10 Monte Carlo noise realization trials per SNR result in a total of 10000 classification decisions for the results presented in Fig. 4. The amount of classification decisions represents adequate statistical significance to facilitate Confidence Interval CI=95% assessment. For the results shown in Fig. 4, each data marker's vertical extent exceeds the CI=95% interval; therefore, error bars have been neglected to increase visual clarity. Figure 4 shows that Gabor-based RF-DNA fingerprints, using $N_{OS} = 5$ oversampling, result in better than 96% individual device *identification* for $SNR \geq -3$ dB.

B. Device Verification

Figure 5 shows individual device *verification* performance for the $N_{MS} = 6$ devices considered (MS63A7, MS63A9, MS66E7, MS637D, MS6373, MS6387) at $SNR = 0$ dB.

TABLE I
Verification Error Types.

	System Decision	
Actual	Authentic	Impostor
Authentic	True Accept	False Reject
Impostor	False Accept	True Reject

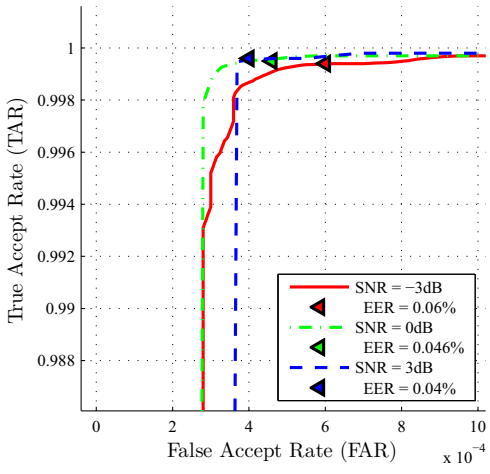
The ROC curves were created by testing the verification performance using the bit-level *claimed* identity (MAC address) of each of the tested device's RF-DNA fingerprints against their known *true* identity (e.g., RF-DNA reference template). The individual curves illustrate the trade-off between system security and accessibility as the decision threshold varies for a selected device [10]. At an $SNR = 0$ dB, devices MS63A7 and MS6373 achieved the best and poorest EERs of 0.046% and 0.92%, respectively. Figure 6 shows the ROC curves and associated EER for the two WiMAX MS devices that resulted in the best case (Fig. 6(a)) and worst case (Fig. 6(b)) device *identification* performance for $SNR \in [-3, 0, 3]$ dB. These figures illustrate that at $SNR = -3$ dB, the poorest EER occurs for MS6373 with a value of 1.61%.

V. Summary and Conclusions

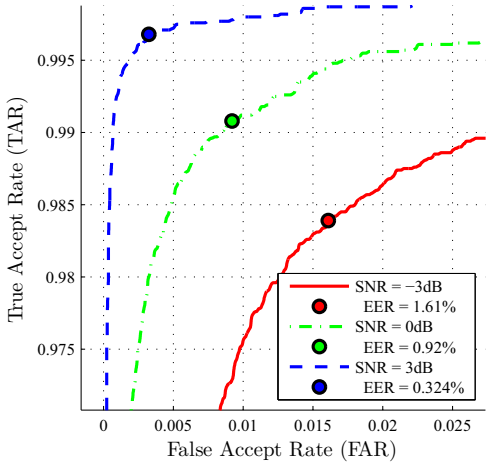
Given existing threats to 802.11a/g WiFi networks, and the anticipated proliferation of other OFDM-based systems such as WiMAX and LTE, it is reasonable to expect that unauthorized network access will continue at WAPs. The need for improved security across all layers of the OSI model remains, with some of the most relevant works emphasizing improvement at the PHY layer [1]–[9]. Some of these earlier works have included the use of RF-DNA fingerprints to augment bit-level security mechanisms at WAPs.

Previous RF-DNA fingerprinting work in [4]–[9] successfully exploited unique signal coloration, present within specific regions of OFDM-based 802.11a and 802.16e signal responses, to demonstrate one-to-many device *identification*–the degree by which an *unknown* device's current RF-DNA ("challenge" fingerprint) statistically matches all stored RF-DNA references for known (authorized) network devices.

The work here expands upon earlier results by adopting the methodology in [10] and demonstrating one-to-one device *verification* performance–the degree by which an *unknown* device's current RF-DNA ("challenge" fingerprint) statistically



(a) Best device *identification*: MS63A7.



(b) Worst device *identification*: MS6373.

Fig. 6. ROC curves and EER for the best and worst case WiMAX MS device *identification* performance at $SNR = [-3, 0, 3]$ dB.

matches the stored RF-DNA associated with the claimed bit-level identity. The assessment is done using Gabor-based RF-DNA fingerprints extracted from 802.16e WiMAX MS near-transient responses. Gabor-based RF-DNA fingerprinting successfully achieves device *identification* of better than 96% and *verification* at EER$\leq$ 1.6% for $SNR \geq -3$ dB.

ACKNOWLEDGMENT

This work sponsored by the Sensors Directorate, Air Force Research Laboratory, Wright-Patterson AFB, OH.

"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] Jana, S. and S.K. Kasera, "Wireless Device Identification with Radiometric Signatures," in *Proc of the ACM 14th Int'l Conf on Mobile Computing and Networking (MOBICOM08)*, Sep 2008.

[2] Tippenhauer, N.O., K.B. Rasmussen, C. Popper, and S. Capkun, "Attacks on Public WLAN-Based Positioning," in *Proc of the ACM 7th Int'l Conf on Mobile Systems, Applications and Serrvices (MOBISYS09)*, Jun 2009.

[3] Danev B. and S. Kapkun, "Transient-Based Identification of Wireless Sensor Nodes," in *Proc of the 8th ACM/IEEE Int'l Conf on Information Processing in Sensor Networks (IPSN09)*, Apr 2009.

[4] Klein R.W., M.A. Temple, M.J. Mendenhall and D.R. Reising, "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance," in *Proc of IEEE Int'l Conf on Communications (ICC09)*, Jun 2009.

[5] Klein, R.W., M.A. Temple and M.J. Mendenhall, "Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security," *Jour of Communications and Networks*, Vol. 11, No. 6, Dec 2009.

[6] Reising D.R., M.A. Temple and M.J. Mendenhall, "Improving Intra-Cellular Security Using Air Monitoring with RF Fingerprints," in *Proc of 2010 IEEE Wireless Communications & Networking Conf (WCNC10)*, Apr 2010.

[7] Williams M.D., S.A. Munns, M.A. Temple and M.J. Mendenhall, "RF-DNA Fingerprinting for Airport WiMax Communications Security," in *Proc of 4th Int'l Conf on Net and Sys Security (NSS10)*, Sep 2010.

[8] Suski W.M. II, M.A. Temple, M.J. Mendenhall and R.F. Mills, "Using Spectral Fingerprints to Improve Wireless Network Security." 2008 IEEE Global Communications Conf (GLOBECOM), Mar 2008.

[9] ——, "RF Fingerprinting Commercial Communication Devices to Enhance Electronic Security," *Int. J. Electronic Security and Digital Forensics*, Vol. 1, No. 3, pp. 301-322, 2008.

[10] Cobb W., E. Laspe, R. Baldwin, M. Temple and Y. Kim, "Intrinsic Physical Layer Authentication of ICs," *IEEE Trans on Information Forensics and Security*, vol. 2, no. 4, pp. 793–808, Dec 2011.

[11] Danev B. H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on Physical-layer Identification," in *Proc of the 3rd ACM Int'l Conf on Wireless Network Security (WiSec10)*, Mar 2010.

[12] Jain A., A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[13] *IEEE 802.16E System Profile Analysis for FCI's Airport Surface Operation*, European Organisation for the Safety of Air Navigation, Edition 1.3, Released Issue, 30 Sep 2009.

[14] Hall E., J. Budinger, R. Diamond and R. Apaza, "Aeronautical Mobile Communications System Development Status," in *Proc of Int Communications, Navigation and Surveillance Conf (ICNS10)*, May 2010.

[15] "Top 10 Network Security Threats, *Government Technology*," Sep 2010. [Online]. Available: http://www.govtech.com/security/Top-10-Network-Security-Threats

[16] Williams M.D., M.A. Temple and D.R. Reising, "Augmenting Bit-Level Network Security Using PHY Layer RF-DNA Fingerprinting," in *Proc of 2010 IEEE Global Communications Conf (GLOBECOM10)*, Dec 2010.

[17] Reising D.R., M.A. Temple and M.E. Oxley, "Gabor-Based RF-DNA Fingerprinting for Classifying 802.16e WiMAX Mobile Subscribers." 2012 IEEE Int'l Conf on Computing, Networking & Communications (ICNC), Jan 2012.

[18] *BreezeMAX Extreme 5000: WiMAX 16e Pioneer for the License-Exempt Market*, Alvarion, Edition 215373 Rev. A, 2009.

[19] *Agilent E3238 Signal Intercept and Collection Solutions: Family Overview*, Agilent Technologies Inc., USA, Publication 5989-1274EN, Jul 2004.

[20] Bastiaans, M. J., "Discrete Gabor Transform and Discrete Zak Transform," in *Proc of IEEE Int'l Conf on Signal and Image Processing Applications (ICSIPA96)*, 1996.

[21] Gabor D., "Theory of Communication," *J. Inst. Elect. Eng. (London)*, Vol. 93, No. III, pp. 429-457,1946.

[22] Wexler J. and S. Raz, "Discrete Gabor Expansions," *IEEE Trans. Signal Processing*, Vol. 21, No. 3, pp. 207-221,1990.

[23] Zibulski M. and Y. Y. Zeevi, "Oversampling in the Gabor Scheme," *IEEE Trans. Signal Processing*, Vol. 41, No. 8, pp. 2679-2687,1993.

[24] Theodoridis S. and K. Koutoumbas, *Pattern Recognition*, 4th ed. Academic Press, 2009.

[25] MacKay D.J.C., *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press, 2003.

[26] Hastie T., R. Tibshirani and J. Friedman, *The Elements of Statistical Learning; Data Mining, Inference, and Prediction*. Springer-Verlag, New York, New York, USA, 2001.