ANOVA-BASED RF DNA ANALYSIS
Identifying Significant Parameters for Device Classification

Kevin S. Kuciapinski, Michael A. Temple and Randall W. Klein
Department of Electrical and Computer Engineering, US Air Force Institute of Technology, Dayton, OH, U.S.A.

Keywords: RF Fingerprinting, Network security, Anti-spoofing, Analysis of variance, ANOVA.

Abstract: Analysis of variance (ANOVA) is applied to RF DNA fingerprinting techniques to ascertain the most significant signal characteristics that can be used to form robust statistical fingerprint features. The goal is to find features that enable reliable identification of like-model communication devices having different serial numbers. Once achieved, these unique physical layer identities can be used to augment existing bit-level protection mechanisms and overall network security is improved. ANOVA experimentation is generated using a subset of collected signal characteristics (amplitude, phase, frequency, signal-to-noise ratio, etc.) and post-collection processing parameters (bandwidth, fingerprint regions, statistical features, etc.). The ANOVA input is percent correct device classification as obtained from MDA/ML discrimination using three like-model devices from a given manufacturer. Full factorial design experiments and ANOVA are used to determine the significance of individual parameters, and interactions thereof, in achieving higher percentages of correct classification. ANOVA is shown to be well-suited for the task and reveals parametric interactions that are otherwise unobservable using conventional graphical and tabular data representations.

1 INTRODUCTION

The proliferation of 4G wireless Radio Frequency (RF) devices will provide unlimited world-wide access for millions of global communication and internet users. However, greater access does come at a cost as users will experience greater exposure and increased security risk, i.e., there is greater opportunity for unauthorized users to monitor their RF emissions (intended and unintended) and intercept, identify, geolocate, and/or track them using bit-level processes. To counter bit-level attacks, research emphasis has begun to shift toward techniques using RF signatures (fingerprints) that are unique to specific hardware devices.

Previous proof-of-concept demonstrations using 802.11 (Klein et al., 2009a, 2009b) and GSM signals (Reising et al., 2010a, 2010b) with RF "Distinct Native Attribute" (RF DNA) fingerprinting has provided some promise for improving access authentication and enhancing overall network security. The goal of these earlier works and the work presented here is to use RF physical layer attributes to augment bit-level security mechanisms that have been routinely "hacked" and which remain under attack (Blau, 2009; Kassner, 2009). It is believed that this augmentation will help mitigate bit-level impersonation attacks such as spoofing given that replication of device dependent, unique RF fingerprint characteristics is very difficult.

Earlier works used statistical Time Domain (TD) features (Reising et al., 2010a, 2010b) and Wavelet Domain (WD) features (Klein et al., 2009a, 2009b) that were generated from specific regions of collected RF signals. These works demonstrated reliable device discrimination (80% or better) at reasonable signal-to-noise ratios (SNR). Unsurprisingly, the device classification performance was directly impacted by typical signal collection and post-collection processing parameters such as Signal-to-Noise Ratio (SNR), sample frequency (f_s), filter bandwidth (BW), etc. The basic goal of these earlier works (proof-of-concept demonstration) mitigated the need for optimization and parameter selection was based on empirical practices.

When considering SNR, f_s, BW, and other parameters in the RF fingerprinting process, e.g., the number of fingerprints used for training and classification, the number of signal fingerprint regions, the number of statistical features per fingerprint region, etc., the number of parametric combinations grows quickly. In this case, assessing

S. Kuciapinski K., A. Temple M. and W. Klein R. (2010).
ANOVA-BASED RF DNA ANALYSIS - Identifying Significant Parameters for Device Classification.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 47-52
DOI: 10.5220/0002994100470052

the impact of given parameters or parameter combinations on device classification performance presents a problem that is well-suited for an Analysis of Variance (ANOVA) experiments.

The results presented here are based on applying ANOVA methods to device classification results obtained from RF fingerprinting. As a first step, the overall process is developed and verified using a previously developed TD fingerprinting process (Klein et al., 2009b). Output TD classification results are used with a 3-way ANOVA that is initially implemented using three factors: Device, SNR and BW. Initial ANOVA results are consistent with behavior previously observed in single parameter variation plots (e.g., percent correct device classification versus SNR and BW). More importantly, the ANOVA analysis reveals the effects of parametric interaction that were not previously observable. Given these early favorable results, work continues to extend the ANOVA analysis to include 1) more than three factors simultaneously, and 2) the use of Spectral Domain (SD) fingerprinting. These extensions are important to the overall success and subsequent implementation of RF fingerprinting to augment bit-level security mechanisms.

2 SYSTEM AND EXPERIMENT

The focus here is on applying ANOVA to device RF fingerprinting classification results as shown in Figure 1. As input to the ANOVA process, intra-manufacturer classification results were generated for three like-model Cisco Aironet 802.11a/b/g wireless adapters operating in 802.11a mode. The devices were identical except for serial number (last four digits of N4U9, N4UD, N4UW). These specific serial numbered devices were chosen for initial ANOVA experimentation because previous research showed that this particular combination of devices presented the most challenging classification problem (Klein et al., 2009a).

Signals were collected using an RF Signal Intercept and Collection System (RFSICS). The RFSICS is an Agilent E3238S-based system and collects signals spanning 20 MHz to 6 GHz (Agilent, 2004). The overall collection and processing method is shown in Figure 2, where the dashed boundaries delineate between hardware and software processes.

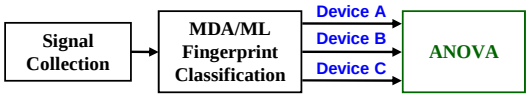

Figure 1: ANOVA experimentation process with signal collection and MDA/ML RF fingerprint classification results provided per the process in Figure 2.

The 802.11a adapter to be tested was placed in a laptop and signals from the device were collected by the RFSICS (Klein et al., 2009a, 2009b). The RFSICS has a W_{RF} = 36 MHz RF bandwidth that is down-converted to a f_{IF} = 70.0 MHz IF, digitized using a 12-bit ADC at f_s = 95 Msps, digitally filtered, sub-sampled (Nyquist maintained), and resultant samples stored as complex In-Phase and Quadrature (I-Q) components. The 802.11 wireless adapters and RFSICS were collocated in an anechoic chamber for all signal collections.

As shown in Figure 2, the collected signals were post-processed using MATLAB. Following burst detection using a t_d = – 3 dB amplitude threshold, the collected signal was digitally filtered using a base-band filter (bandwidth W_{BB}) and combined with like-filtered noise that is scaled to achieve the desired analysis SNR. For initial concept validation, W_{BB} and SNR were the ANOVA factors that were incrementally varied and statistical fingerprints were used to generate classification results.

Bandwidth variation was simulated using a 3rd-order Butterworth digital filter having a – 3 dB bandwidth of BW = 5.5, 6.5, 7.5 and 8.5 MHz. Given the selected filter, SNR variation was simulated using randomly generated AWGN that was like-filtered (same filter used for the signal) and scaled to achieve the desired analysis SNR (Klein et al., 2009a, 2009b). The range of SNRs considered was based on previous works and included 1) lower values where SNR was suspected to dominate correct classification performance, and 2) higher values where SNR changes produced minimal impact. This range enabled both validation of the ANOVA process as applied to RF Fingerprinting and investigation of lesser dominant parameters in higher SNR regions.

Device classification is accomplished using a Fisher-based MDA/ML process with statistical fingerprint features extracted from physical wave-form characteristics of instantaneous amplitude, phase, and/or frequency. The features are generated using common statistics of standard deviation, variance, skewness, and/or kurtosis (Klein et al., 2009a, 2009b). As parameters (factors) are altered during simulation and processing, classification errors occur when the analysis signal in Figure 2 is classified as the wrong device signal.

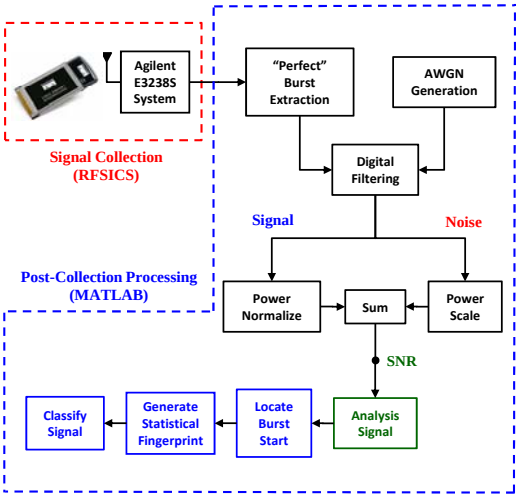

Figure 2: Signal collection and MDA/ML fingerprint classification (Klein et al., 2009a).

The results of MDA/ML device classification generally indicate some predictable performance trends for parametric (factor) variation. These trends were used to verify and validate results from the ANOVA process. As obtained from the MDA/ML classification process, these performance trends are illustrated in Figure 3 which shows that average percent correct classification (average across all three devices) is dependent upon both SNR and BW.

2.1 3-Way ANOVA

The statistical model uses a 3-Way ANOVA with input data generated using a full factorial experimental design approach with three factors, including: specific device, BW, and SNR. The ANOVA Fixed Effects Model was used to complete the analysis and is given by (Montgomery 2009):

$$y_{ijk} = u + \alpha_i + \beta_j + \tau_k + (\alpha\beta)_{ij} + (\alpha\tau)_{ik} + (\beta\tau)_{jk} + (\alpha\beta\tau)_{ijk} + \varepsilon_{ijk} \quad (1)$$

where μ is the overall mean, α is the specific device effect, β is the Bandwidth (BW) effect, τ is the SNR effect, $\alpha\beta$ is the Device-BW interaction effect, $\alpha\tau$ is the Device-SNR interaction effect, $\beta\tau$ is the BW-SNR interaction effect, $\alpha\beta\tau$ is the Device-BW-SNR interaction effect, and ε is the random error.

The Fixed Effects Model compares each parameter and parameter combination to the mean correct classification value. If varying a given parameter or parameter combination does not result in a divergence from the mean, that parameter or parameter combination *does not have* a significant effect on correct classification.

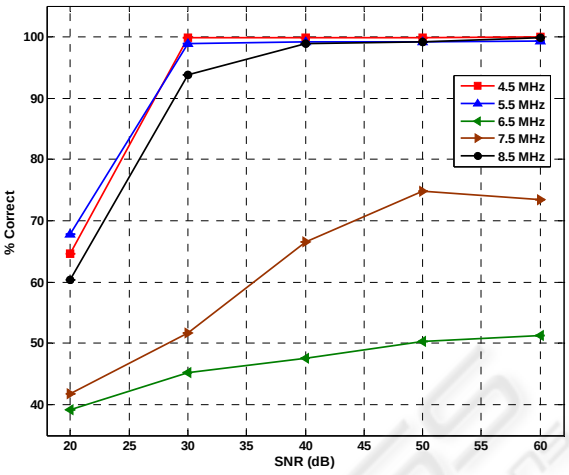

Figure 3: Average Percent Correct Classification (Across All Devices) for various SNR and BW values.

Otherwise, if varying a given parameter or parameter combination results in a deviation from the mean, that parameter or parameter combination *does have* a statistically significant effect on correct classification results. This can be expressed using hypothesis notation:

$$H_o : \alpha_1 = \alpha_2 = \ldots = \alpha_i = 0 \quad (2)$$

$$H_A : \exists \text{ some } i : \alpha_i \neq 0 \quad (3)$$

$$H_o : \beta_1 = \beta_2 = \ldots = \beta_j = 0 \quad (4)$$

$$H_A : \exists \text{ some } j : \beta_j \neq 0 \quad (5)$$

$$H_o : \tau_1 = \tau_2 = \ldots = \tau_k = 0 \quad (6)$$

$$H_A : \exists \text{ some } k : \tau_k \neq 0 \quad (7)$$

$$H_o : (\alpha\beta)_{1,1} = (\alpha\beta)_{1,2} = \ldots = (\alpha\beta)_{ij} = 0 \quad (8)$$

$$H_A : \exists \text{ some } i, j : (\alpha\beta)_{ij} \neq 0 \quad (9)$$

$$H_o : (\beta\tau)_{1,1} = (\beta\tau)_{1,2} = \ldots = (\beta\tau)_{jk} = 0 \quad (10)$$

$$H_A : \exists \text{ some } j, k : (\beta\tau)_{jk} \neq 0 \quad (11)$$

$$H_o : (\alpha\tau)_{1,1} = (\alpha\tau)_{1,2} = \ldots = (\alpha\tau)_{ik} = 0 \quad (12)$$

$$H_A : \exists \text{ some } i, k : (\alpha\tau)_{ik} \neq 0 \quad (13)$$

$$H_o : (\alpha\beta\tau)_{1,1,1} = (\alpha\beta\tau)_{1,1,2} = \ldots = (\alpha\beta\tau)_{ijk} = 0 \quad (14)$$

$$H_A : \exists \text{ some } i, j, k : (\alpha\beta\tau)_{ijk} \neq 0 \quad (15)$$

The hypothesis tests in (2)–(15) are designed to show whether or not a given parameter or parameter combination has an effect on percent correct classification. For example, the null hypothesis H_O in (2) states that for any given device among the three being considered, the effect on the mean correct classification will be zero. The alternative hypothesis H_A in (3) states that for at least one of the

devices being used, there is a statistically significant effect on percent correct classification.

For final experimental results presented in this paper, the 3-factor interaction term $\alpha\beta\tau$ in (1) was not considered. Preliminary results indicated that the 2-factor interactions were more significant for correct classification than three factor interaction. Thus, all combinations of 2-factor interaction effects ($\alpha\beta$, $\alpha\tau$, $\beta\tau$) for the three parameters (Device, SNR, BW) were the focus of this work.

3 RESULTS

The device classification process in Figure 2 allows variation of any given number of parameters. To enable validation of the ANOVA RF fingerprinting experimentation process, the parameters that were varied included Device, BW, and SNR. In addition, performance analysis was limited to using only the 802.11a preamble signal region, with classification accomplished using three statistical fingerprint regions as shown in Figure 4 (Klein et al., 2009a).

Signals were collected, RF statistical fingerprints extracted, MDA/ML classification performed and resultant classification data analyzed for three devices using selected BW and SNR values. The specific device, BW and SNR parametric combinations are shown in Table 1 along with corresponding classification results that were used for generating ANOVA results in Section 3.1.

3.1 ANOVA Results

To determine the statistical significance of a given parameter or parameter combination, an *F-Test* was applied and a *P-Value* calculated. The *P-Value* is the probability that the test statistic will have a value that is at least as extreme as the observed value when the null hypothesis is true (Montgomery 2009). Thus, if a *P-Value* (Prob > F) is at or near zero, the null hypothesis is rejected in favour of the alternative. Alternately stated, if the *P-Value* for a given parameter or parameter combination is at or near zero, that parameter or parameter combination has a statistically significant effect on correct classification. Results of the ANOVA analysis using data in Table 1 is presented in Table 2.

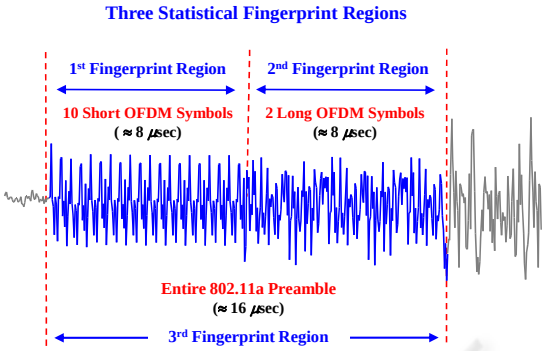

Figure 4: Preamble structure showing modulated signal response and fingerprint regions for the 802.11a signals (Klein et al., 2009a).

Table 1: MDA/ML percent correct classification for each device and specific combination of BW and SNR factors.

BW	Dev#	SNR (dB)				
MHz		20	30	40	50	60
4.5	1	67.00	99.92	99.86	99.92	99.96
	2	82.30	99.96	100	100	100
	3	44.36	99.78	99.76	99.78	99.80
5.5	1	72.78	97.24	98.38	98.00	98.24
	2	88.48	99.66	99.84	100	100
	3	42.24	99.64	99.28	99.64	99.56
6.5	1	22.84	17.60	19.04	25.42	28.36
	2	63.00	74.94	80.78	82.76	83.86
	3	31.72	43.22	42.74	42.68	41.76
7.5	1	37.42	70.78	86.06	81.50	81.56
	2	44.94	71.62	67.82	80.28	79.84
	3	42.92	12.56	45.78	62.68	58.96
8.5	1	73.96	88.52	96.94	99.74	99.78
	2	89.42	100	100	100	100
	3	17.76	92.86	99.64	97.66	99.60

Table 2: Analysis of Variance Results.

Source	Sum^2	D.F.	Mean^2	*F*	*P-Value*
Dev	0.47044	2	0.23522	18.45	0.0000
SNR	0.95996	4	0.24149	18.94	0.0000
BW	2.75173	4	0.68793	53.95	0.0000
Dev-SNR	0.12833	8	0.01604	1.26	0.2994
Dev-BW	0.62613	8	0.07827	6.14	0.0001
SNR-BW	0.19087	16	0.01193	0.94	0.5411
Error	0.40806	32	0.01275		
Total	5.54152	74			

3.2 Application of ANOVA

According to the ANOVA results in Table 2, the Device, BW, and SNR factors *all* have a statistically significant effect on overall correct classification for parameter values considered. This is indicated by the *P-Values* approaching zero for each parameter. This conclusion is consistent with previous empirical assessment based on varying a single parameter (Klein et al., 2009a, 2009b) and serves as proof-of-concept validation for the ANOVA experimentation process.

3.2.1 2-Factor Interactions

Also of significance and not directly represented in previous research are the Device-BW interaction effects. As shown in Table 2, the *P-Value* for this interaction is very near zero which indicates that Device-BW interaction is statistically significant to correct classification. This result was investigated further and qualitatively assessed using results in Figure 5. It is clear that classification performance varies considerably as a function of BW (30-80% degradation across devices) with Device 2 being least sensitive and Device 1 being most sensitive for the BWs considered.

The classification performance "dip" in Figure 5 was observed between BW = 6.5 and 7.5 MHz for all SNR values considered, i.e., SNR = [20dB to 60dB]. The cause of this was analyzed by considering MDA/ML classification confusion matrix data. A representative confusion matrix for BW = 7.5 MHz and SNR = 40 dB is shown in Table 3. The diagonal entries represent percent of correct classification for each device. The off-diagonal entries represent percent of misclassification (confusion) between devices. As evident in the highlighted (red text) off-diagonal entries in Table 3, Device 1 and Device 3 are the most often confused. With one exception, similar behaviour was reflected in confusion matrices for all SNRs as well as BW = 4.5, 5.5 and 8.5 MHz. The one difference occurred for BW = 6.5 MHz which produced the confusion matrix results shown in Table 4. In this case, Device 1 and Device 2 are the most often confused and both Device 1 and Device 3 are misclassified as Device 2 most often.

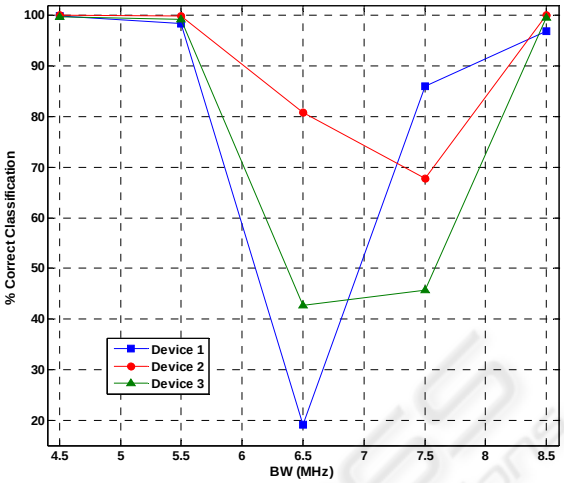

Figure 5: Percent correct classification vs. BW for each device and the average across devices for SNR = 40 dB.

Table 3: MDA/ML classification confusion matrix for BW = 7.5 MHz and SNR = 40 dB.

	Estimated Device		
Actual Device	1	2	3
1	**86.06%**	1.26%	**12.68%**
2	22.84%	**67.82%**	9.34%
3	**53.70%**	0.48%	**45.78%**

Table 4: MDA/ML classification confusion matrix for factor combination of BW = 6.5 MHz and SNR = 40 dB.

	Estimated Device		
Actual Device	1	2	3
1	**19.04%**	**65.06%**	15.90%
2	15.04%	**80.78%**	4.18%
3	19.40%	**37.86%**	**42.74%**

4 CONCLUSIONS

As 4G wireless communication technology continues to proliferate and users become increasingly exposed to bit-level attacks, RF DNA fingerprinting may emerge as the preferred physical layer method for improving network security. As introduced in previous work and adopted here, RF fingerprinting performance is driven by a myriad of signal collection, post-collection processing, and device classification parameters. Thus, the end-to-end process is well-suited for ANOVA experimentation and parametric analysis aimed at

identifying key factors, or combinations thereof, for predicting and implementing efficient and robust fingerprinting.

Initial results validate applicability of ANOVA for enhancing RF fingerprinting development. This was done using three factors (Device, SNR and BW) and corresponding 2-factor interaction effects which provide additional insight into fingerprint process design. The range of ANOVA factors included three like-model 802.11a/b/g Cisco wireless devices operated in the 802.11a configuration, SNR = [20 60] dB in 10 dB steps, and BW = 4.5, 5.5, 6.5, 7.5 and 8.5 MHz. The Device-BW interaction provided the greatest insight into discriminating information and showed that greatest device confusion (poorest overall classification accuracy) occurs within the BW = 6.5 to 7.5 MHz region. While the exact cause of this remains under investigation, this result is consistent with previous comparisons made using time domain (TD) and wavelet domain (WD) techniques (Klein et al., 2009a).

The ANOVA also revealed that specific serial-numbered devices were more susceptible to BW variation, i.e., classification performance varied considerably as a function of BW and 30-80% degradation was observed across devices. The ANOVA process also revealed some semi-significant effects based on Dev-SNR interaction. Although not as strong as the Device-BW interaction, specific like-model devices were shown to be more susceptible to SNR variation.

Given preliminary favorable results, research activity continues and work has begun to extend the ANOVA analysis process by 1) considering more than three ANOVA factors simultaneously, 2) extending applicability to Spectral Domain (SD) fingerprinting, and 3) identifying significant parameters from among those not considered in this initial proof-of-concept demonstration. These extensions are important to the overall success and subsequent implementation of RF fingerprinting to augment bit-level security mechanisms.

REFERENCES

Agilent (2004). *Agilent E3238 Signal Intercept and Collection Solutions: Family Overview.* Publication #5989-1274EN, Agilent Technologies Inc., USA.

Blau, J. (2009). Open-source effort to hack GSM. spectrum.ieee.org/Telecom/Wireless/Open-Source-Effort-to-Hack-GSM.

Kassner, M. (2009). Cracking GSM encryption just got easier. blogs.techrepublic.com.com/wireless.

Klein, R., Temple, M., and Mendenhall, M. (2009a). Application of wavelet-based RF fingerprinting to enhance wireless network security. *Jour of Communications and Networks*. Vol. 11, No. 6, 544-555, Dec.

Klein, R., Temple, M., Mendenhall, M., and Reising, D., (2009b). Sensitivity analysis of burst detection and RF fingerprinting classification performance. IEEE Int. Conf on Communications (ICC09), Germany, Jun.

Montgomery, D., (2009). *Design and Analysis of Experiments*, John Wiley & Sons Inc. Hoboken, 7th Edition.

Reising, D., Temple, M., and Mendenhall, M. (2010a). Improved wireless security for GMSK-based devices using RF fingerprinting. *Int. J. Electronic Security and Digital Forensics.* Vol. 3, No. 1, 41-59, Mar.

Reising, D., Temple, M., and Mendenhall, M. (2010b). Improving intra-cellular security using air monitoring with RF fingerprints. IEEE Wireless Comm and Networking Conf (WCNC10), Australia, Apr.

"The views expressed in this paper 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."