PHY Foundation for Multi-Factor ZigBee Node Authentication

Benjamin W. Ramsey, Michael A. Temple, and Barry E. Mullins
Department of Electrical and Computer Engineering
Air Force Institute of Technology
Wright-Patterson AFB, OH 45433 USA
Email: [benjamin.ramsey, michael.temple, barry.mullins]@afit.edu

***Abstract*—The ZigBee specification builds upon IEEE 802.15.4 low-rate wireless personal area standards by adding security and mesh networking functionality. ZigBee networks may be secured through 128-bit encryption keys and by MAC address access control lists, yet these credentials are vulnerable to interception and spoofing via free software tools available over the Internet. This work proposes a multi-factor PHY-MAC-NWK security framework for ZigBee that augments bit-level security using radio frequency (RF) PHY features. These features, or RF fingerprints, can be used to differentiate between dissimilar or like-model wireless devices. Previous PHY-based works on mesh network device differentiation predominantly exploited the signal turn-on region, measured in nanoseconds. For an arbitrary benchmark of 90% or better classification accuracy, this work shows that reliable PHY-based ZigBee device discrimination can be achieved at $SNR \geq 8$ dB. This is done using the entire transmission preamble, which is less technically challenging to detect and is over 1000 times longer than the signal turn-on region. This work also introduces a statistical, pre-classification feature ranking technique for identifying relevant features that dramatically reduces the number of RF fingerprint features without sacrificing classification performance.**

I. Introduction

Wireless Personal Area Networks (WPANs) are undergoing rapid deployment in distributed sensing and control applications where extended node battery life and low data rate are key design features. The IEEE 802.15.4 media access control (MAC) and physical-layer (PHY) standards provide a low-data-rate WPAN foundation on which network (NWK) and application (APL) layers are built, such as the ZigBee specification [1]. Backed by an alliance of over 250 companies, ZigBee technology emphasizes low-complexity and low implementation cost. The entire ZigBee protocol stack requires only 120 KB of nonvolatile memory. The radio transceiver and microprocessor are often combined on a single integrated circuit in ZigBee devices. Millions of utility meters utilize bi-directional ZigBee communication in Advanced Metering Infrastructures (AMI) [2]. AMI solutions often include Home Area Network components as well [3]. ZigBee solutions are available for such varied applications as patient vital sign monitoring [4], security systems [5], and industrial control [6].

The Python-based killerbee tool set [7], released in January 2010, is the first of a growing number of tools that expose ZigBee and other IEEE 802.15.4-based WPANs to attack methods originally developed against IEEE 802.11 Wi-Fi and IEEE 802.15.1 Bluetooth. Recent work [8]-[11] demonstrates that tight resource constraints on ZigBee nodes make them particularly vulnerable to attack. Replayed ZigBee packets could open doors, turn valves, shut off fans, etc., depending on WPAN implementation. ZigBee allows for plain-text network key distribution in "standard security mode" and plain-text master and link key distribution under "high security mode." Other ZigBee concerns include access control list vulnerabilities to MAC address spoofing, denial of service through associate request flooding, malicious network impersonation (PAN ID), and a new class of packet-in-packet injection attacks first demonstrated in [12]. PHY layer security using radio frequency (RF) fingerprints is a viable alternative for verifying MAC and NWK credentials, since RF signal characteristics are substantially more difficult to mimic.

Previous work on RF fingerprinting for wireless sensor networks has exploited features within the signal turn-on transient region (~125 ns) [13]-[15], with 70% classification accuracy using five relative amplitude features from ten 433 MHz CC1000 radios [12]. Work in [14] provides improved accuracy of 97% using ten different CC1000 radios at distances of 15 cm [14]. The use of three transient features is promising for classifying 2.4 GHz ZigBee node radios at distances of 40 meters [14]. RF fingerprinting based on differences in Automatic Gain Control circuitry have been less successful; limited feature differences are observed between six ZigBee devices at distances of 10 cm [15].

The IEEE 802.15.4 specification [16] mandates use of a preamble based on 30 to 40 bits, depending on frequency band and modulation scheme. The 32-bit preamble for 2.4 GHz ZigBee nodes is 128 μs long; or 1024 times longer than previously exploited signal transient responses [13]-[15]. Preamble RF features have been effectively used in related work to reliably differentiate IEEE 802.11a radios [17]-[18]. The work here demonstrates reliable differentiation between ZigBee transceivers of the same model (CC2420) at varying signal-to-noise ratios (SNRs) using preamble RF fingerprints. The RF fingerprint techniques used incorporate summary statistics of multiple instantaneous transmission waveform measurements that are resilient against intentional spoofing. Results presented herein are foundational to development of an envisioned PHY-MAC-NWK framework aimed at augmenting current ZigBee security mechanisms with RF fingerprint authentication while achieving backward compatibility with current battery-powered ZigBee end devices.

II. Envisioned Multi-factor Framework for ZigBee

The concept of an "air monitor" that observes wireless network transmission characteristics to augment bit-layer security mechanisms is not new [20]-[21]. However, many of the challenges associated with practical network integration have not been adequately addressed. The work here builds upon the air monitor concept and describes the envisioned integration into ZigBee WPANs to improve security.

A. ZigBee Nodes and Topologies

IEEE 802.15.4 specifies two node classes, including: Full Function Devices (FFDs) and Reduced Function Devices (RFDs). FFDs are always actively listening on the network and are typically powered by a constant external power supply. RFDs are battery-powered and primarily operate in sleep mode, waking only to check for pending messages or periodic updates.

Building upon this foundation, ZigBee defines three node classes: ZigBee Coordinator (ZC), ZigBee Router (ZR) and ZigBee End Device (ZED). The ZC and ZRs must be FFDs, while ZEDs can be either FFDs or RFDs. There can only be one ZC per WPAN and it is responsible for establishing the network, allocating NWK addresses, and routing traffic. The WPAN fails without its ZC. ZRs extend the WPAN physical range by routing messages between their child RFD ZEDs using multi-hop topologies, such as the *Cluster Tree* and *Mesh* topologies illustrated in Fig. 1. The Star Topology is shown for completeness and does not support multi-hop communication. In a cluster tree topology, ZEDs have no children and can only communicate with the ZC and other ZEDs through their parent ZR. ZigBee Stack Profile `0x01` limits the number of children for each ZR to $N_c = 20$, 6 of which can be ZRs. The ZigBee PRO specification (Stack Profile `0x02`) increases this limit to $N_c = 254$ children per ZR. Mesh topologies are only allowed using ZigBee PRO, and permit FFD ZEDs to communicate directly with one another.

B. Air Monitor Placement

The envisioned air monitors would be electronic devices, separate from, but connected to FFD ZigBee hardware by a short cable for sharing fingerprint assessment feedback. A single air monitor co-located with the ZC would be sufficient to observe all traffic within the Star WPAN topology. On cluster tree WPANs, communication with each ZED is concentrated through its parent ZR. Therefore, an air monitor co-located with every ZR would be the maximum number required to observe all traffic on the WPAN. Mesh topologies pose significantly greater challenges to security. For example, memory overhead required for link key storage (confidentiality for every hop) can grow exponentially larger than for cluster tree topologies. Air monitoring of large mesh topologies will be challenging for similar reasons. Nodes are largely stationary in ZigBee profiles such as Smart Energy, Building Automation, and Home Automation, simplifying air monitor coverage. Profiles that feature mobile ZEDs, such as Health Care, pose significant challenges to air monitor coverage. Mobile ZEDs are also inherently more vulnerable to physical attacks such as key extraction, theft, and tampering.

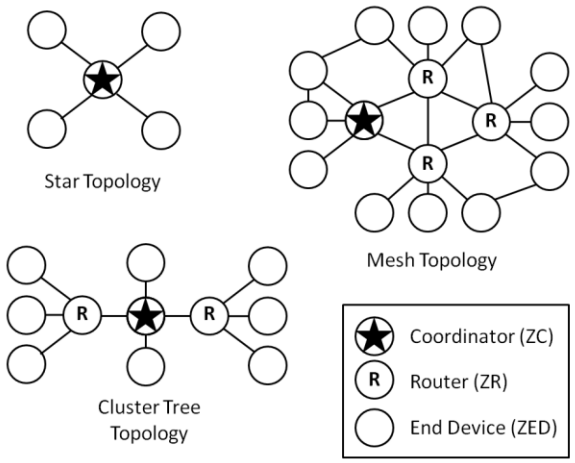

Figure 1. ZigBee WPAN Topologies.

C. Air Monitor and Trust Center Integration

ZigBee WPANs under either security mode (standard or high) must appoint an FFD (usually the ZC) to serve as the Trust Center, recognized and trusted by all nodes on the WPAN. The Trust Center is responsible for security and key management. A new node *n** can only join the WPAN if it receives permission from the Trust Center. Permission to join can be restricted by an access control list of valid MAC addresses. If *n** presents a valid MAC address but does not know the network key, the Trust Center can transmit the key in plain text. ZigBee advocates assume that this window of vulnerability is "quite small and acceptable" [22], but tools such as *zbdsniff* can endlessly sniff a WPAN until such keys are intercepted [7]. An air monitor framework for ZigBee WPANs would defend against active attacks such as fuzzing, associate request flooding, and packet injection by establishing three-factor authentication:

1. "Something you know" (NWK – encryption keys)
2. "Something you have" (MAC – MAC address)
3. "Something you are" (PHY – RF fingerprint)

While keys and MAC addresses are vulnerable to current attacks, RF fingerprints from physical radio emissions are unique and technically infeasible to mimic.

In the star topology in Fig. 1, the combined ZC/Trust Center receives feedback from its air monitor as to how well the current RF fingerprint from every incoming transmission matches the stored fingerprint profile established for the claimed sender. Thresholds for packet rejection must be tailored based on operational conditions to prevent undue denial of service. In cluster tree topologies, the routers only forward transmissions "cleared" as sufficiently well-matched by their respective air monitors. Air monitors maintain an evolving RF fingerprint profile of the devices assigned to its ZR to account for variations in environment and device operating characteristics. Sufficiently complex mesh networks

require larger and more flexible RF fingerprint databases and air monitor placement.

An air monitor framework would be most valuable if every transmission is validated by the current RF fingerprint. This is because many exploits, such as replay attacks and packet injection, may be effective if a single malicious transmission is accepted as valid by the WPAN. However, even fractional air monitor protection may mitigate active denial of service attacks such as associate request flooding.

Despite the challenges that must still be addressed before the envisioned air monitor framework is successfully implemented, the relatively infrequent transmission rate of ZigBee WPANs, short transmission range, and limitation of N_c = 254 child devices per ZR makes them an ideal early candidate for upcoming air monitor experimental research.

III. Background

A. Signal Collection Methodology

An Agilent E3238S-based system [23] serves as the RF Signal Intercept Collection System (RFSICS). All Signal collections are down converted to near-baseband, digitized using 12-bit analog-to-digital conversion and stored as complex in-phase and quadrature (I-Q) components for subsequent post-collection processing. Collection parameters include sample frequency f_s = 11.875 Msps and baseband filter bandwidth W_{BB} = 1 MHz using a 4th-order Butterworth filter. Signal collections included a total of N_P = 1000 transmission preambles from N_D = 7 CC2420 2.4 GHz IEEE 802.15.4 devices. Transceiver positioning is consistent between collections in a Ramsey STE3000 RF test enclosure with RF absorbent foam lining, 20 cm from a dipole antenna connected to the RFSICS input by a shielded cable.

Amplitude-based threshold detection with a leading edge value of T_D = -6.0 dB is used to identify and extract individual burst transmissions from the multi-second RF collections. The approximate duration of experimentally collected preamble responses is 1536 samples (129 µs), which closely matches the 128 µs specification [16]. The collection SNR for all bursts was SNR_C > 50 dB.

B. Statistical Fingerprint Generation

The statistical fingerprint (**F**) for a signal derives from its instantaneous amplitude (a), phase (ϕ) and/or frequency (f) characteristics. More specifically, the sequences $\{a[n]\}$, $\{\phi[n]\}$, and/or $\{f[n]\}$ are generated from complex samples of the signal region of interest, centered (mean removal) and then normalized (division by maximum value) [17]-[18]. Statistical fingerprint features are generated as variance (σ^2), skewness (γ), and/or kurtosis (k) within specific signal regions. The *regional fingerprint markers* are generated by: 1) dividing each characteristic sequence into N_R contiguous, equal length sub-sequences, 2) calculating N_S statistical metrics for each sub-sequence, plus the entire fingerprinted region as a whole (N_R + 1 total regions), and 3) arranging the metrics in a vector of the form:

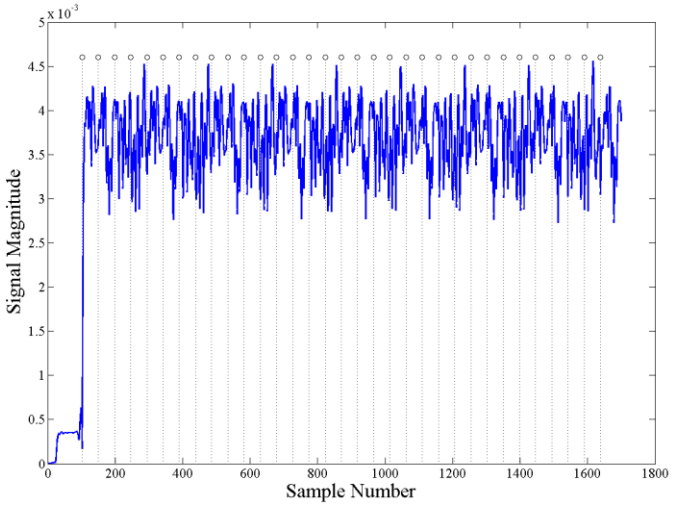

Figure 2. Provision of Collected Burst Preamble into N_R = 32 Sub-regions.

$$F_{Ri} = \left[\sigma^2_{Ri}\ \gamma_{Ri}\ k_{Ri}\right]_{1\times 3}, \quad (1)$$

where i = 1, 2, …, N_R + 1. The marker vectors from (1) are concatenated to form the *composite characteristic vector* for each characteristic and are given by

$$\mathbf{F}^C = \left[F_{R1} \vdots F_{R2} \vdots F_{R3} \ldots F_{R(NR+1)}\right]_{1\times NS(NR+1)}. \quad (2)$$

If only one signal characteristic (a, ϕ, or f), is used the expression in (2) represents the final fingerprint used for classification. When all N_C = 3 signal characteristics are used, the final *RF fingerprint* is generated by concatenating vectors from (2) according to

$$\mathbf{F} = \left[\mathbf{F}^a \vdots \mathbf{F}^\phi \vdots \mathbf{F}^f\right]_{1\times NS(NR+1)\times NC}. \quad (3)$$

Exploratory data analysis revealed that N_R = 32 preamble sub-regions, or four regions per each of the eight repeated symbols comprising the preamble (Fig. 2), serves as a successful baseline for this proof-of-concept demonstration.

C. MDA/ML Device Classification Methodology

Statistical RF fingerprints are generated using (3) for collected preamble transmissions from N_D = 7 IEEE 802.15.4 radios. The resultant RF fingerprints are input into a Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) process for device classification. MDA is an extension to Fisher's Linear Discriminant when more than two classes (devices) are considered. MDA reduces the higher-dimensional input feature space with the goal of maximizing inter-class separation while reducing intra-class spread [24]. For the N_C = 3 class problems considered here, MDA projects the multidimensional RF fingerprints into a 2-dimentional space. RF fingerprints are classified as being affiliated with one of N_C = 3 possible classes based on Bayesian decision criteria using prior known probabilities, probability densities, and relevant costs associated with making a decision [25]. For all results presented herein the associate costs are assumed equal for all classes.

The MDA/ML process implementation uses K-fold cross-validation with $K = 5$ to improve classification reliability. The best-performing model generated from examining a *training* set of preamble features from each device is then used to classify a second collection previously unseen preamble features using its MDA/ML algorithm. Only classification accuracies resulting from this "day-after" *testing* are reported in Section IV.

D. Pre-Classification Feature Dimentionality Reduction

In the aggregate, assembled RF fingerprints are effective for inter-device classification; however, individual RF fingerprint components do not generally contribute uniformly to classification performance. The MDA/ML classification process inherently provides no insight into feature relevance. Intuitively, however, RF fingerprint components that exhibit maximal inter-device dissimilarity and minimal intra-device dissimilarity are generally advantageous for MDA/ML classification. It may be beneficial to statistically examine RF fingerprints *prior* to MDA/ML classification to identify features (RF fingerprint components) that exhibit statistical properties that may be most advantageous for classification; the process for identifying and removing less relevant features is called Dimensional Reduction Analysis (DRA). The goal of DRA is to reduce RF fingerprint size (minimize N_F) while having minimal or tolerable impact on classification accuracy. Given the RF fingerprints assembled from collected preambles are non-normally distributed, nonparametric statistical analysis is appropriate. The Kolmogorov-Smirnov goodness-of-fit test (KS-test) is a suitable option that quantifies differences in cumulative distribution functions (CDF) between two datasets, with lower *p*-values indicating greater CDF differences.

For the $N_D = 7$ device case considered here, there were $N_p = 21$ unique pairwise devices comparisons made. Fig. 3 presents summed *p*-values for the corresponding $N_p = 21$ KS-tests ($\alpha = 0.1$) conducted at $SNR = 8$ dB using full dimensional fingerprints, i.e., $N_F = (N_R + 1 = 33)$ x $(N_S = 3)$ x $(N_C = 3) = 297$ features. The robustness of phase features has been previously noted [19] and is evident here in Fig. 3. The mean *p*-values and qualitative visual analysis of Fig. 3 further suggests that frequency-based features are less relevant than phase-based features and amplitude-based features are least relevant. Classification results presented in Section IV are consistent with this assessment and validate the KS-test approach as a viable means for discovering the *relative relevance* of instantaneous amplitude (a), phase (ϕ) and frequency (f) features prior to MDA/ML classification.

IV. Device Classification Results

The IEEE 802.15.4 specification mandates the use of a synchronization header (SHR) containing a Preamble and Start-of-Frame Delimiter (SFD) sequence for all transmission bursts. Although the entire SHR *can* be used for generating RF fingerprints, exploratory data analysis revealed that inclusion of the SFD response did not significantly improve MDA/ML classification accuracy. Additional analysis revealed that features based on power-spectral-density underperformed relative to features based on the instantaneous a, ϕ, and f time-domain responses considered herein.

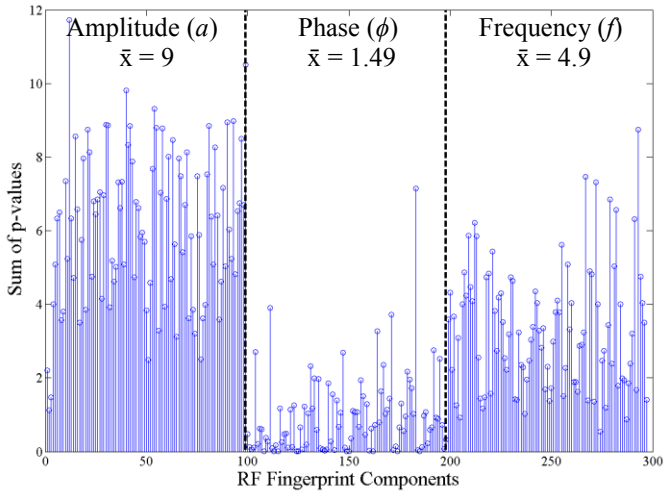

Figure 3. Sum of $N_p = 21$ Pairwise KS-test P-values for Each Fingerprint Feature Using a Full Dimensional ($N_F = 297$) Feature Set at SNR = 8dB.

MDA/ML inter-device classification results were generated for all $N_{Prm} = 35$ possible permutations of 3-class problems using $N_D = 7$ ZigBee devices. Classification experiments used $N_P = 1000$ independent preamble responses (500 each for training and classification) and $N_N = 5$ Monte Carlo noise realizations per preamble response at each SNR; a total of N_{Tst} = (500 Preambles) x $(N_N = 5) = 2500$ independent classification decisions per device in each 3-device trial. This large number of trials reduced the mean error bars to within the vertical extent of the plotted markers. Therefore, trial mean error bars are not presented in plots to enhance visual clarity.

A. Full Dimensional RF Fingerprinting Accuracy

Full dimensional RF fingerprints include features based on $N_C = 3$ signal characteristics (a, ϕ, and f), $N_s = 3$ statistical fingerprint features (σ^2, γ, and k), and $N_R + 1 = 33$ regions, for a total fingerprint $\mathbf{F}$ comprised of $N_F = 297$ RF features as given by (3). Fig. 4 presents the aggregate full dimensional classification accuracies for $N_{Prm} = 35$ device permutations at $SNR \in [0\ 20]$ dB. The cross-perm average is shown as filled circle markers. As indicated, the mean classification accuracy exceeds an arbitrary benchmark of 90% for $SNR \geq 8$ dB.

B. Reduced Dimensional RF Fingerprinting Accuracy

While full dimensional RF fingerprinting is effective, the DRA process in Section III.D revealed significant differences (range of p-values) among RF fingerprint components derived from the instantaneous $\{a[n]\}$, $\{\phi[n]\}$, and $\{f[n]\}$ sequences. Classification results are presented here for RF fingerprinting with a 66.7% reduced feature set ($N_F = 99$ of 297 retained). This is done by evaluating classification performance using only amplitude (*Amp-Only*), phase (*Phz-Only*) and frequency (*Frq-Only*) feature subsets of the full dimensional feature set.

Fig. 5 presents the aggregate *Amp-Only* classification accuracies for all $N_{Prm} = 35$ permutations, with the cross-perm average shown with filled circle markers. The resulting decline in classification performance is readily apparent by visual comparison with full dimensional RF fingerprint performance

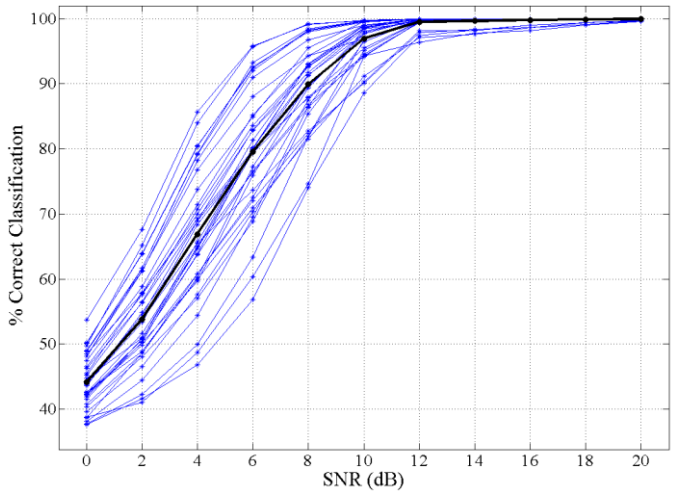

Figure 4. Full Dimensional ($N_F = 297$) Classification Accuracy for $N_{Prm} = 35$ Permutations. Perm Average Shown as Filled Circle Markers.

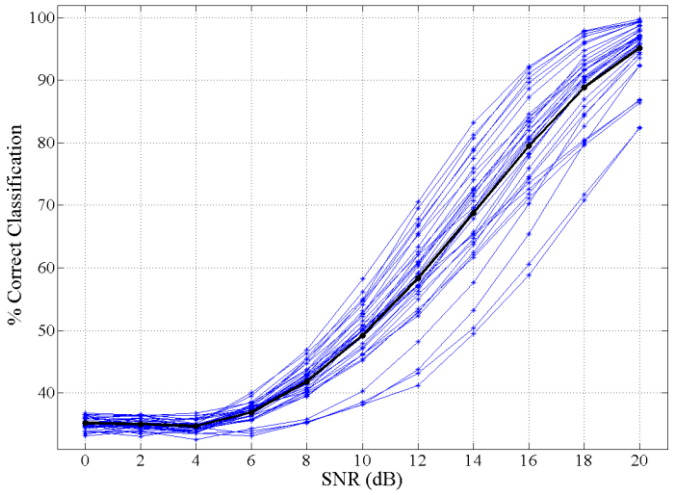

Figure 5. Reduced Dimensional ($N_F = 99$) Classification for $N_{Prm} = 35$ Permutations Using the *Amp-Only* Subset of the Full Dimensional Feature Set.

in Fig. 4. Relative to the arbitrary benchmark of 90%, *Amp-Only* RF fingerprinting requires $SNR > 18$ dB.

Fig. 6 presents the aggregate classification accuracies for all $N_{Prm} = 35$ permutations for *Phz-Only* RF fingerprinting, with the cross-perm average shown with filled circle markers. These results mirror those of full dimensional fingerprinting in Fig.. 5, with average *Phz-Only* fingerprinting 1) exceeding the arbitrary benchmark of 90% for $SNR \geq 8$ dB, 2) matching full dimensional performance for $SNR \geq 16$ dB, and 3) achieving approximately 2% better performance than full dimensional for $SNR < 16$ dB. This represents a successful demonstration of the potential for pre-classification dimensionality reduction using the KS-test *p*-value analysis described in Sect. III.D.

Fig. 7 presents the aggregate classification accuracies for all $N_{Prm} = 35$ permutations for *Frq-Only* RF fingerprinting, with the cross-perm average shown with filled circle markers. As predicted by KS-test *p*-value results in Fig. 3, the average perm classification accuracy in Fig. 7 falls between that of *Amp-Only* and *Phz-Only* RF fingerprinting, with the arbitrary benchmark of 90% achieved for $SNR \geq 14$ dB.

Conclusions relative to results in Fig. 4 through Fig. 7 are best drawn using the overlay plot presented in Fig. 8 which shows full dimensional and reduced dimensional MDA/ML classification performance for $SNR \in [0\ 20]$ dB. Considering an arbitrary classification accuracy of 90% as a reasonable benchmark for assessing the potential contribution of RF PHY features to an overall multi-factor authentication solution, both the full dimensional ($N_F = 297$) and *Phz-Only* ($N_F = 99$) feature sets would perform reliably for $SNR \geq 8$ dB. However, the reduced dimensional *Phz-Only* feature set has the added advantage of only requiring calculation and processing of one-third the number of features. The methodology and classification accuracies presented herein are promising and demonstrate the technical feasibility for reliably differentiating between IEEE 802.15.4 transceivers using RF fingerprints extracted from preamble transmissions–a solid foundation for continued development of the envisioned multi-factor PHY-MAC-NWK authentication framework.

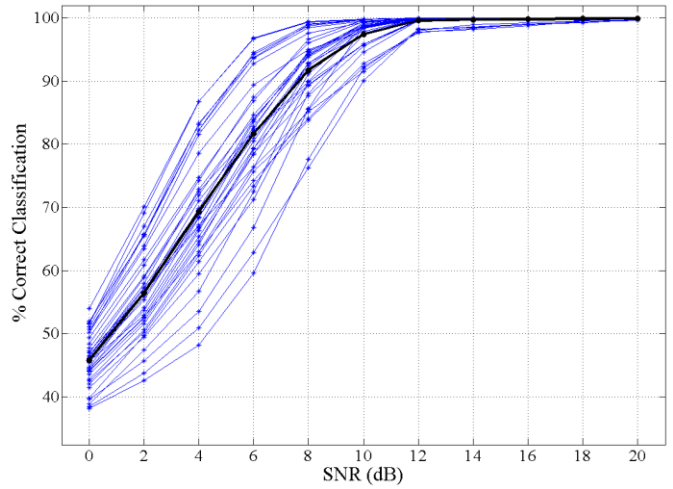

Figure 6. Reduced Dimensional ($N_F = 99$) Classification for $N_{Prm} = 35$ Permutations Using the *Phz-Only* Subset of the Full Dimensional Feature Set.

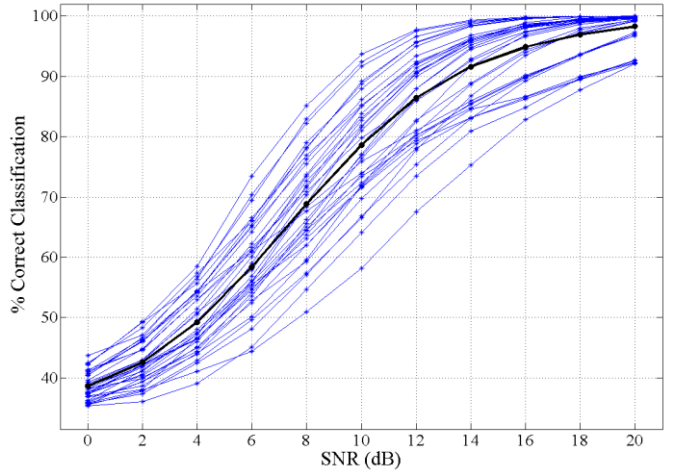

Figure 7. Reduced Dimensional ($N_F = 99$) Classification for $N_{Prm} = 35$ Permutations Using the *Frq-Only* Subset of the Full Dimensional Feature Set.

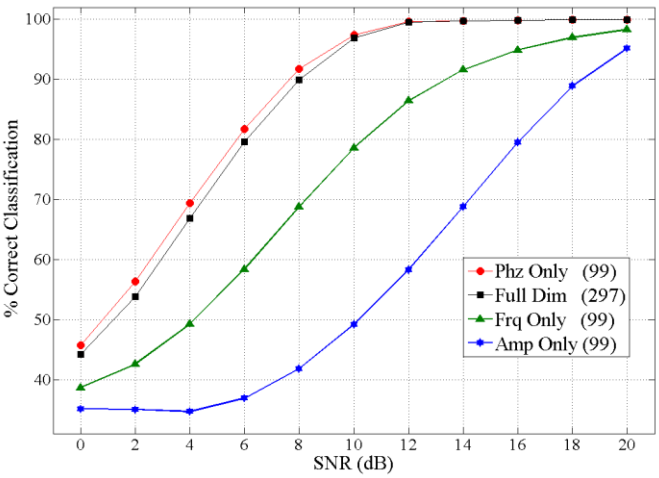

Figure 8. Overlay of Previous Perm Averages for Full Dimensional and Reduced Dimensional MDA/ML Classification.

V. Conclusion

The low-cost, low complexity, and low power consumption benefits of ZigBee WPANs make them competitive solutions in many wireless sensor and control applications. As with all wireless networks, a defense-in-depth approach to mitigating security vulnerabilities is paramount. Results here demonstrate that ZigBee devices can be accurately and reliably identified solely by using time-domain RF statistical features extracted from their transmission preambles; an arbitrary benchmark of 90% classification accuracy is demonstrated for $SNR \geq 8$ dB using like-model ZigBee devices. This PHY "something you are" addition to current ZigBee two-factor authentication (MAC address + NWK encryption keys) is analogous to the addition of human biometrics where computer network security is critical. The work here is foundational to future work aimed at achieving additional RF fingerprint dimensionality reduction and maturing the proposed cross-layer PHY-MAC-NWK multi-factor authentication framework. As consumers become increasingly reliant on ZigBee, they must be confident and trust that the operational integrity of their appliances, home infrastructure, personal medical data, etc., can be maintained–multi-factor authentication can mitigate ZigBee WPAN security vulnerability and bolster this trust.

Acknowledgment

This work is sponsored by the Sensors Directorate, Air Force Research Laboratory, and the Tactical SIGINT Technology (TST) Program Office.

The views expressed in this article are those of the authors and do not reflect official policy of the United States Air Force, Department of Defense or the U.S. Government.

References

[1] ZigBee Alliance, "ZigBee Specification." ZigBee Document 053474r17, Jan 2008.

[2] T. Whittaker, "Final Word," *Control & Automation*, vol. 18, no. 3, pp. 48, Jun-Jul 2007.

[3] Federal Energy Regulatory Commission, "2010 Assessment of Demand Response and Advanced Metering," Feb 2011, http://www.ferc.gov/legal/staff-reports/2010-dr-report.pdf.

[4] S-.K Chen, et al., "A Reliable Transmission Protocol for ZigBee-Based Wireless Patient Monitoring," *IEEE Trans on Information Technology in Biomedicine*, vol. 16, no. 1, pp. 6-16, Jan 2012.

[5] I. Tihon and V. Croitoru, "ZigBee Sensor Networks Telesurveillance," *10th Int'l Symposium on Signals, Circuits and Systems (ISSCS '11)*, pp. 1-4, Jun 2011.

[6] D. Egan, "The emergence of ZigBee in building automation and industrial control," *Computing & Control Engineering Journal*, vol. 16, no. 2, pp. 14-19, Apr-May 2005.

[7] J. Wright, "Killerbee: Framework and Tools for Txploiting ZigBee and IEEE 802.15.4 Networks." Version 1.0, 2010. http://code.google.com/p/killerbee/

[8] G. Dini and M. Tiloca, "Considerations on Security in ZigBee Networks," *IEEE Int'l Conf on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2010)*, pp. 58-65, Jun 2010.

[9] P. Radmand, et al., "ZigBee/ZigBee PRO Security Assessment Based on Compromised Cryptographic Keys," *Int'l Conf on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 465-470, Nov 2010.

[10] R. A. Melgares, "802.15.4/ZigBee Analysis and Security: Tools for Practical Exploration of the Attack Surface." Darthmouth Computer Science Technical Report TR2011-689, Jun 2011.

[11] T. Goodspeed, et al., "Api-do: Tools for Exploring the Wireless Attack Surface in Smart Meters," *Int'l Conf on System Science (HICSS-45)*, pp.2133-2140, Jan 2012.

[12] T. Goodspeed, et al., "Packets in Packets: Orson Welles' In-Band Signaling Attacks for Modern Radios," *5th USENIX Workshop on Offensive Technologies*, Aug 2011.

[13] K. B. Rasmussen and S. Capkun, "Implications of Radio Fingerprinting on the Security of Sensor Networks," *Int'l Conf on the Security and Privacy for Emerging Areas in Communication Networks (SecureComm'07),* Sep 2007.

[14] B. Danev and S. Capkun, "Transient-based Identification of Wireless Sensor Nodes," *ACM/IEEE Int'l Conf on Information Processing in Sensor Networks*, Apr 2009.

[15] D. A. Knox and T. Kunz, "AGC-based RF Fingerprints in Wireless Sensor Networks for Authentication," *1st Int'l Workship on Wireless Sensor, Actuator and Robotic Networks,* Jun 2010.J.

[16] IEEE 802.15.4 Standard, Wireless MAC and PHY Specifications for Low-Rate WPANS, 2006.

[17] W. C. Suski, et al., "Using Spectral Fingerprints to Improve Wireless Network Security," *IEEE Global Telecommunications Conference*, (GLOBECOM'08), Nov 2008.

[18] R. W. Klein, et al., "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance," *IEEE Int'l Conf on Communications* (ICC'09), Jun 2009.

[19] M. D. Williams, et al., "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," *IEEE Global Telecommunications Conference* (GLOBECOM'10), Dec 2010.

[20] Y. Sheng, et al., "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," *27th Conference on Computer Communications* (INFOCOM'08), 2008, pp. 1768-1776.

[21] P. K. Harmer, et al., "Using DE to Optimize 'Learning from Signals' and Enhance Network Security," *13th Annual Conference on Genetic and Evolutionary Computation* (GECCO'11), Jun 2011.

[22] Texas Instruments, "*RemoTI Developer's Guide,"* http://www.ti.com/lit/ml/swru198/swru198.pdf

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

[24] R. Duda, et al., *Pattern Classification*, 2nd ed. New York: John Wiley & Sons, Inc., 2001.

[25] T. Hastie, et al., *The Elements of Statistical Learning; Data Mining, Inference, and Prediction*. Springer-Verlag, New York, New York, USA, 2001.