ZigBee Device Verification for Securing Industrial Control and Building Automation Systems

Clay Dubendorfer, Benjamin Ramsey, Michael Temple

Chapter 4

ZIGBEE DEVICE VERIFICATION FOR SECURING INDUSTRIAL CONTROL AND BUILDING AUTOMATION SYSTEMS

Clay Dubendorfer, Benjamin Ramsey and Michael Temple

Abstract Improved wireless ZigBee network security provides a means to mitigate malicious network activity due to unauthorized devices. Security enhancement using RF-based features can augment conventional bit-level security approaches that are solely based on the MAC addresses of ZigBee devices. This paper presents a device identity verification process using RF fingerprints from like-model CC2420 2.4 GHz ZigBee device transmissions in operational indoor scenarios involving line-of-sight and through-wall propagation channels, as well as an anechoic chamber representing near-ideal conditions. A trained multiple discriminant analysis model was generated using normalized multivariate Gaussian test statistics from authorized network devices. Authorized device classification and ID verification were assessed using pre-classification Kolmogorov-Smirnov (KS) feature ranking and post-classification generalized relevance learning vector quantization improved (GRLVQI) relevance ranking. A true verification rate greater than 90% and a false verification rate less than 10% were obtained when assessing authorized device IDs. When additional rogue devices were introduced that attempted to gain unauthorized network access by spoofing the bit-level credentials of authorized devices, the KS-test feature set achieved a true verification rate greater than 90% and a rogue reject rate greater than 90% in 29 of 36 rogue scenarios while the GRLVQI feature set was successful in 28 of 36 scenarios.

Keywords: ZigBee devices, RF fingerprinting, ID verification, rogue rejection

1. Introduction

The deployment of wireless personal area networks in industrial control and monitoring applications is increasing due to their energy efficiency, low complexity and low cost. Standards-based protocols such as ZigBee and IEEE 802.15.4

commonly provide connectivity in wireless sensor network applications that support energy management and industrial control automation. ZigBee solutions are also implemented with radio frequency identification tags in hospital environments to track expensive medical equipment and patient stay, and to continuously monitor patient vital signs. High levels of security are essential in ZigBee networks used in critical infrastructure applications, including public health and the smart grid, where sensitive personal information is handled or physical systems are controlled.

Improved security and authentication measures must be developed to counter open source hacking tools such as KillerBee [11] that can undermine ZigBee networks. Rogue devices can spoof bit-level credentials such as MAC addresses and network encryption keys. This has motivated research in physical layer (PHY) features that can uniquely identify network nodes. PHY features are inherently difficult to replicate, especially when derived from unintentional waveform modulation effects. Recent work has shown that, once they are identified and extracted, PHY-based features (e.g., RF fingerprints) can achieve human-like device discrimination even when using a relatively simple multiple discriminate analysis (MDA), maximum likelihood (ML) classification technique [4, 5, 8, 10].

This paper expands the use of radio frequency distinct native attribute (RF-DNA) fingerprints for device classification and verification using 2.4 GHz ZigBee devices in a typical indoor office environment. Line-of-sight and through-wall propagation channels are considered with dynamic multi-path and signal attenuation factors such as interior walls and human foot traffic. Time-domain exploitation of the entire 40-bit IEEE 802.15.4 synchronization header response (SHR), a mandatory element of every ZigBee transmission, is considered. The experimental results demonstrate the feasibility of ZigBee device ID verification using collected responses in operational and near-ideal environments.

Device ID verification is characterized using a test statistic based on normalized multivariate Gaussian distributions of MDA-projected fingerprints and receiver operating characteristics (ROC) curve analysis. The MDA-based device ID verification process is demonstrated using RF fingerprints comprising dimensionally-reduced feature sets – minimal features translate to minimal computational complexity. Dimensional reduction analysis (DRA) is used to select reduced feature sets based on pre-classification Kolmogorov-Smirnov (KS) feature ranking and post-classification generalized relevance learning vector quantization-improved (GRLVQI) relevance ranking. A classification performance benchmark of $\%C = 90\%$ is used for comparative assessment and for verification assessment. The device ID verification process is assessed based on the true verification rate (TVR) for authorized devices and the rogue reject rate (RRR) for unauthorized rogue devices.

2. Experimental Methodology

An Agilent E3238S receiver (Rx) was used to collect emissions from ten CC2420 2.4 GHz IEEE 802.15.4 ZigBee devices (denoted as Dev1, Dev2, ..., Dev10). For each transmitting (Tx) device, a total of $N_{SHR} = 1,000$ SHRs

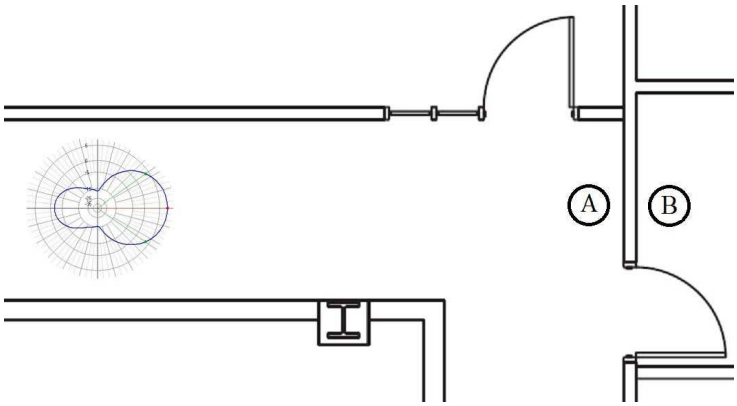


Figure 1. Operational indoor collection geometry.

were collected under three operating conditions: (i) Tx and Rx inside a Ramsey STE3000 RF shielded anechoic chamber (CAGE); (ii) Tx and Rx with a clear line-of-sight (LOS) along a hallway – Location A in Figure 1; and (iii) Tx and Rx on opposite sides of a wall (WALL) – Location B in Figure 1. A 6 dB gain Ramsey LPY2 log periodic antenna was placed in the hallway with the main beam directed at the collection devices.

The collected signals were down-converted, digitized using a 12-bit analog-to-digital converter and stored as complex in-phase and quadrature components for subsequent post-collection processing. Amplitude-based burst detection and baseband processing were performed as described in [1, 6] using a sample frequency $f_s = 11.875$ Msps and an eighth-order Butterworth filter with bandwidth $W_{BB} = 1$ MHz.

2.1 RF Fingerprint Generation

RF fingerprints were extracted from SHR emissions using instantaneous amplitude (a), phase (ϕ) and frequency (f) responses. Characteristics sequences ($a[n]$, $\phi[n]$ and $f[n]$) were generated using collected complex in-phase and quadrature signal samples from the SHR region, centered (i.e., mean removal) and then normalized (i.e., division by maximum value) [5, 9]. Statistical RF fingerprint features of variance (σ^2), skewness (γ) and kurtosis (κ) were calculated to create regional fingerprint markers generated by: (i) dividing each selected characteristic sequence $\{a[n]\}$,$\{\phi[n]\}$ and $\{f[n]\}$ into N_R contiguous equal-length subsequences; (ii) calculating N_S metrics for each subsequence, plus the entire fingerprinted region as a whole ($N_R + 1$ total regions); and (iii) arranging the metrics in vector form as:

$$F_{R_i} = [\sigma^2_{R_i}\ \gamma_{R_i}\ \kappa_{R_i}]_{1 \times N_S} \tag{1}$$

where $i = 1, 2, \ldots, N_R + 1$. Marker vectors from Equation (1) are concatenated to form the composite characteristic vector given by:

$$\mathbf{F} = [F_{R_1} \vdots F_{R_2} \vdots F_{R_3} \ldots F_{R_{N_R+1}}]_{1\times[N_S\times(N_R+1)]}. \quad (2)$$

When all $N_C = 3$ signal characteristics are used, the final RF fingerprint is generated by concatenating vectors from Equation (2) according to:

$$\mathbf{F} = [\mathbf{F}^a \vdots \mathbf{F}^\phi \vdots \mathbf{F}^f]_{1\times[N_S\times(N_R+1)\times N_C]} \ . \quad (3)$$

Full-dimensional RF-DNA fingerprints are based on a total of $N_R = 80$ SHR subsequences using $N_C = 3$ signal characteristics (a, ϕ, f) and $N_S = 3$ statistics (σ^2, γ, κ), for a total of $N_{Full} = N_S \times (N_R + 1) \times N_C = 729$ features per RF fingerprint.

2.2 Device Discrimination

Statistical RF fingerprints for ZigBee SHR responses were generated according to Equation (3) and input to a device discrimination process shown in Figure 2. The device discrimination process supports both classification and verification using selected measures of similarity and test statistics. The process involves separating collected RF-DNA fingerprints into training and testing sets for $N_D = 4$ ZigBee devices (Dev1, Dev2, Dev3 and Dev4). The training emissions were used for device-specific model development for both device classification and device ID verification. Device classification and verification assessments were accomplished by projecting the testing RF fingerprints into a mapped feature space derived through MDA model development and generating measures of similarity using probability-based test statistics.

Multiple Discriminate Analysis Model Development. MDA is an extension of the Fisher linear discriminant process for discriminating more than two device classes ($N_D > 2$). MDA reduces feature dimensionality by projecting RF fingerprints into an $N_D - 1$ dimensional subspace. The MDA projection matrix $\mathbf{W}$ was developed using an iterative K-fold training process with the goal of projecting higher-dimensional input fingerprint $\mathbf{F}$ data into a lower dimensional mapped feature space such that the out-of-class separation is maximized and the within-class spread is minimized [2]. The best performing projection matrix $\mathbf{W}_B$ in the K-fold training process was retained and used to project training fingerprints into the mapped feature space, where projected means and covariances were measured for each of the N_D devices. The means and covariances were used to develop an assumed multivariate Gaussian distributed device specific model. The developed model shown as $\mathbf{M}$ in Figure 2 comprises a projection matrix $\mathbf{W}_B(SNR)$, device projected means $\mu_i(SNR)$, and a pooled covariance matrix $\Sigma_P(SNR)$ where the parenthetical signal-to-noise ratio (SNR) denotes that the model generally varies with SNR and $i = 1, 2, \ldots, N_D$.

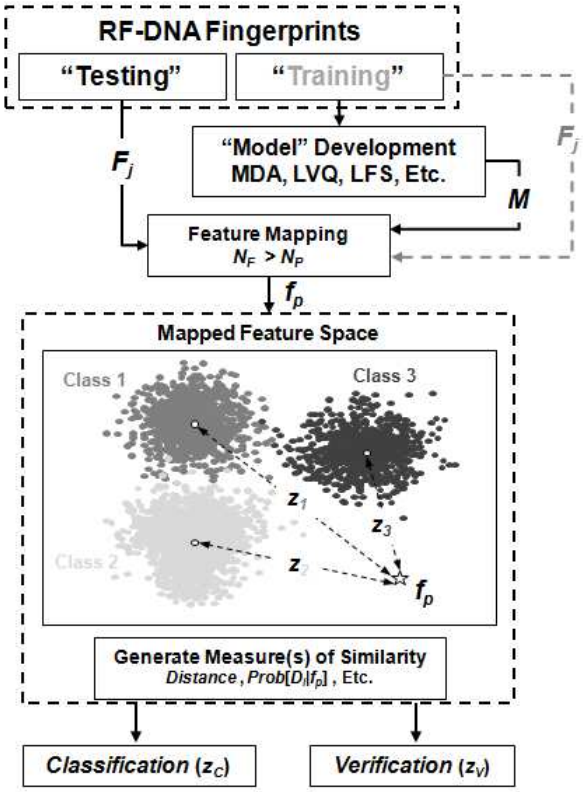


Figure 2. Block diagram of device discrimination.

Maximum Likelihood Classification. Device classification was performed using an ML classifier derived from Bayesian decision theory with the testing RF fingerprints classified as affiliated with one of the N_D possible devices. For ML classification, the prior probabilities were assumed to be equal, the costs uniform and the device likelihoods to have a multivariate Gaussian distribution generated during MDA model development. The ML classification process involved: (i) inputting a testing RF fingerprint $\mathbf{F}_j$ generated according to Equation (3) for a collected emission from an unknown device D_j; (ii) projecting $\mathbf{F}_j$ into the mapped feature space using $\mathbf{f}_j = \mathbf{F}_j \mathbf{W}_B$; and (iii) associating $\mathbf{f}_j$ with the device yielding the maximum conditional likelihood probability:

$$D_i \; : \; \arg\max_i \left[\; p(\mathbf{f}_j | D_i) \; \right] \tag{4}$$

where $i = 1, 2, \ldots, N_D$ and $p(\mathbf{f}_j|D_i)$ is the conditional likelihood probability that fingerprint $\mathbf{f}_j$ belongs to device D_i. This was done for all testing RF fingerprints in order to assess the device classification performance.

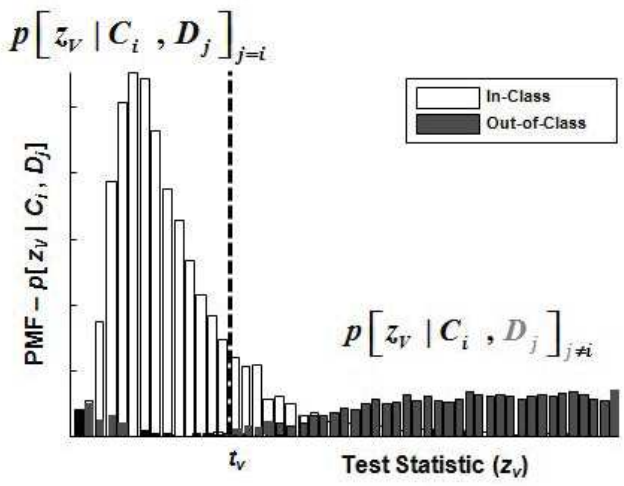


Figure 3. Representative in-class and out-of-class probability mass functions.

Device ID Verification. The RF fingerprinting methodology used for device ID verification is consistent with the process used in [1, 7]. RF fingerprints can authenticate the claimed bit-level identity of a device (e.g., the device wants to access a network and has presented a MAC address, SIM number or IMEI number to gain access). Since bit-level credentials can be replicated by rogue devices, RF fingerprint verification provides a means to mitigate unauthorized access attempts. Device ID verification was accomplished using a one-to-one comparison of current versus claimed RF signatures. The similarity measure or verification test statistic z_V reflects how well the current and claimed RF fingerprint identities match and is compared with a threshold t_V to verify the ID claimed by the device and grant or deny network access to the device.

Figure 3 shows representative in-class (unfilled) and out-of-class (filled) probability mass functions (PMFs) generated from test statistic z_V and a fixed threshold t_V. The in-class probability is defined as $p[z_V|C_i, D_j]$ where $j = i$, C_i is the claimed device ID and D_j is the actual device. The out-of-class distribution was generated using z_V for the case when an unknown device falsely claims to be an authorized device, where the unknown device is: (i) a rogue device ($j \neq 1, 2, \ldots, N_D$); or (ii) an authorized device claiming the identity of a different authorized device ($j = 1, 2, \ldots, N_D$). The out-of-class probability is denoted as $p[z_V|C_i, D_j]$ where $i \neq j$ and $i = 1, 2, \ldots, N_D$.

Device ID verification was assessed using conventional ROC curve analysis [3]. Varying the threshold t_V and measuring the area under the curve for each PMF enabled the determination of the true and false device ID verification rates. The TVR is a measure of how well current RF fingerprints match the true claimed ID and is the area under the in-class PMF when $z_V < t_V$. The corresponding false verification rate (FVR) provides a measure of how

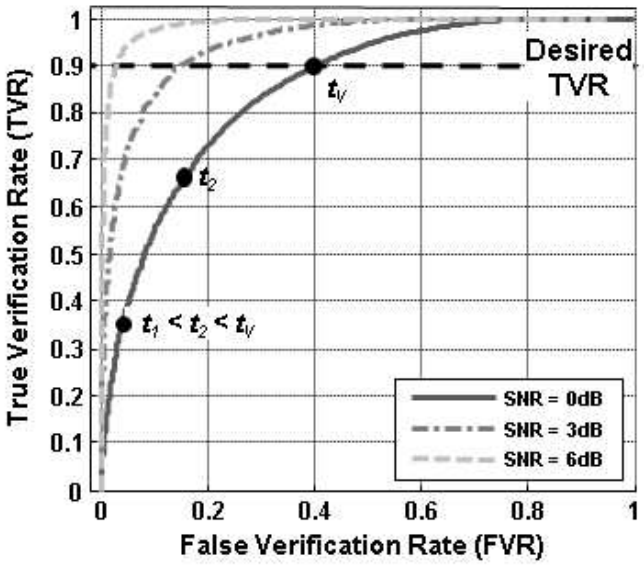


Figure 4. Device ID verification ROC curves.

well current RF fingerprints match a false claimed ID and is the area under the out-of-class PMF when $z_V < t_V$.

The threshold t_V was varied and the corresponding device TVRs and FVRs were used to generate ROC performance curves for 6 dB > 3 dB > 0 dB. Figure 4 shows the variation in ROC curve performance as a function of three arbitrarily selected SNR values. Representative performance points for various thresholds ($t_1 < t_2 < t_V$) are shown to emphasize that the verification threshold value dictates TVR and FVR performance.

2.3 Dimensional Reduction Analysis

The Fisher-based MDA process inherently masks the feature contribution to the resulting discrimination performance, inhibiting the ability to determine the features that have the greatest impact. The goal of DRA is to minimize the number of RF fingerprint features while achieving the desired classification accuracy. Identifying the features that provide the most significant contribution to classification while removing less relevant features may be accomplished using two techniques: (i) a pre-classification KS goodness-of-fit test [6]; and (ii) a feature relevance ranking provided by GRLVQI processing [7].

The quantitative pre-classification feature reduction process was used to identify and select the l most relevant features from the full-dimensional RF feature set $\mathbf{F}$ prior to MDA/ML classification. The KS-test is a suitable option for analyzing statistical feature differences and was used to quantify differences in cumulative distribution functions between full-dimensional RF feature sets from two devices. The KS-test results are presented as summed p-values from

all pairwise combinations of the N_D devices considered, where lower p-values indicate a more significant difference between the data sets.

The second alternative to feature selection considered was GRLVQI processing, which inherently provides an indication of feature relevance following model development. The process was adopted entirely from previous research that shows that GRLVQI is a powerful tool for performing device classification and DRA [7, 8]. The GRLVQI process provided a relevance ranking for each feature comprising the RF fingerprint at a specified SNR. The relevance ranking value is the contribution of a particular feature to device separation within the GRLVQI classification process. The higher the relevance value, the greater the impact on class separation. Feature dimensional reduction was achieved by selecting the top l features from the feature relevance ranking of the GRLVQI classifier. This GRLVQI DRA selected subset of features was used in the MDA/ML device classification and ID verification processes.

3. Experimental Results

MDA training was accomplished using $N_{SHR} = 500$ independent ZigBee SHR responses collected from each location (CAGE, LOS and WALL) for each device (Dev1, Dev2, Dev3 and Dev4). In addition, $N_z = 5$ independent, like-filtered Monte Carlo noise realizations were added to the SHR responses for each analysis SNR considered. Thus, for MDA training with $N_D = 4$ devices, K-fold generation of the best $\mathbf{W}_B(SNR)$, $\mu_i(SNR)$, $\Sigma_P(SNR)$ and multivariate Gaussian statistics of projected training fingerprints involved a total of $N_{TNG} =$ 500 (SHR) $\times$ 3 (locations) $\times$ 5 (N_z) = 7,500 independent realizations per device. The classification and verification results were likewise based on $N_{SHR} = 500$ testing fingerprints per location for each device and $N_z = 5$ noise realizations per SNR, resulting in $N_{TST} = 7,500$ test realizations.

3.1 Device Classification (Full-Dimensional)

Full-dimensional RF fingerprints included features based on $N_C = 3$ signal characteristics (a, ϕ and f), $N_S = 3$ statistical fingerprint features (σ^2, γ and κ), and $N_R + 1 = 81$ regions, for a total fingerprint $\mathbf{F}$ comprising $N_F = 729$ features as specified by Equation (3). Figure 5 shows the full-dimensional testing classification performance for the hybrid location scenario (i.e., responses from CAGE, LOS and WALL) at SNRs ranging from 0 to 24 dB. Note that a performance benchmark of $\%C = 90\%$ is achieved at SNR $\approx$ 10 dB, with all the devices achieving $\%C = 80\%$ or better classification.

3.2 DRA Feature Selection

Feature dimensional reduction analysis was subsequently performed to determine the minimum number of features required to achieve the $\%C = 90\%$ benchmark. Feature relevance was determined by fixing the RF fingerprints at SNR = 10 dB and performing a quantitative assessment on the $N_F = 729$

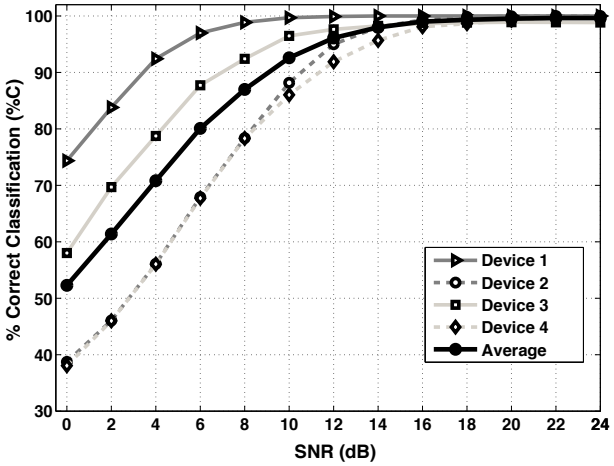


Figure 5. MDA/ML device classification performance.

full-dimensional features using the pre-classification KS-test feature selection and the feature relevance ranking from the GRLVQI classifier.

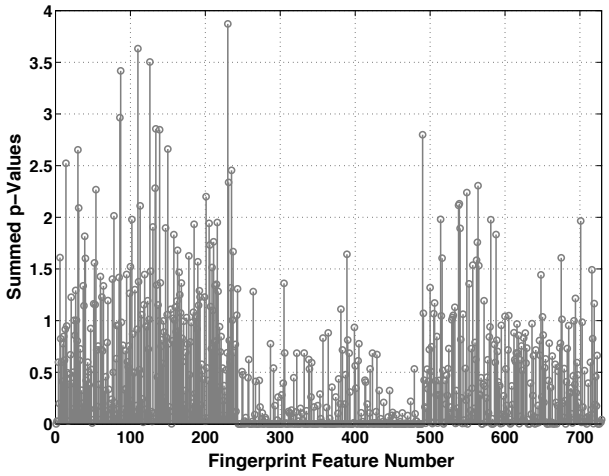
Quantitative feature assessment enabled the identification and selection of the most relevant subset of full-dimensional features. Figure 6 shows the $N_F = 729$ full-dimensional feature indices and relevance indicators for SNR = 10 dB based on the pre-classification KS-test and the GRLVQI feature relevance ranking. Note that lower KS-test p-values and higher GRLVQI λ-values indicate greater relevance. The results at SNR = 10 dB correspond to the cross-device average $\%C \approx 90\%$ shown in Figure 5.

3.3 Device Classification (DRA Performance)

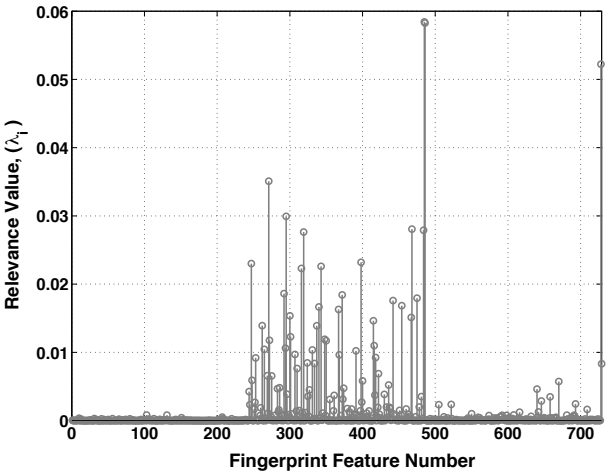
Figure 7 shows the results of reducing the RF fingerprint features using the pre-classification KS-test feature selection and the feature relevance ranking from the GRLVQI classifier. For the KS-test, the top $N_F = 243$ features to the top $N_F = 50$ features require SNR $\approx$ 10 to 17 dB to achieve the $\%C = 90\%$ classification benchmark. Note that the top $N_F = 25$ features never reach the $\%C = 90\%$ benchmark. For the GRLVQI classifier, a range of SNR $\approx$ 10 to 29 dB is necessary to achieve 90% classification accuracy for the top $N_F = 243$ features to the top $N_F = 25$ features.

3.4 Device ID Verification (Authorized Devices)

Device ID verification was performed using a one-to-one comparison of the current RF fingerprint versus claimed ID RF fingerprints. The current RF fingerprint was compared with the stored reference fingerprint template associated with the claimed bit-level identity. The stored reference fingerprint template was created in the MDA training process using $N_{TNG} = 7,500$ independent



(a) KS-test (lower p-value implies greater relevance).

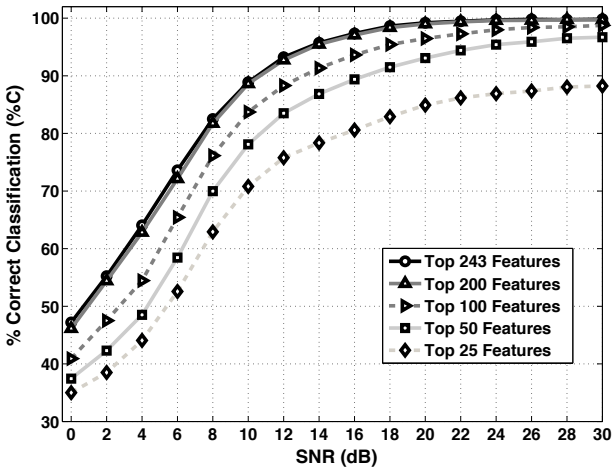


(b) GRLVQI (higher λ-value implies greater relevance).

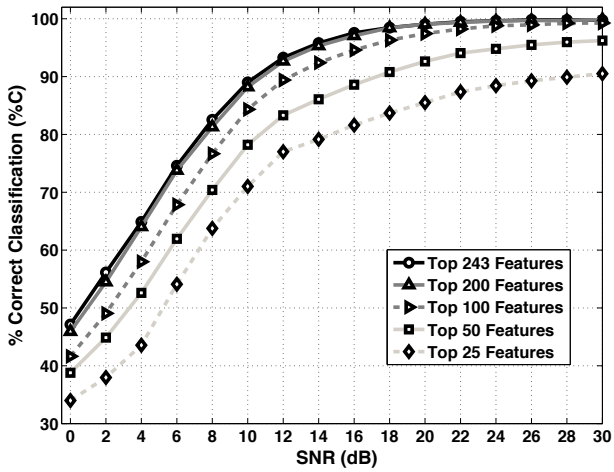
Figure 6. DRA feature relevance indicators at SNR = 10 dB.

realizations for the $N_D = 4$ authorized devices. The projected training fingerprints were used to generate the in-class PMF constructed from the verification test statistic z_V. This test statistic z_V was derived from the inherent MATLAB classify function, which outputs a normalized conditional multivariate Gaussian posterior probability given by:

$$z_V = \frac{p(\mathbf{f}_j|D_i)}{\sum_{k=1}^{N_D} p(\mathbf{f}_j|D_k)} \tag{5}$$



(a) KS-test feature selection.

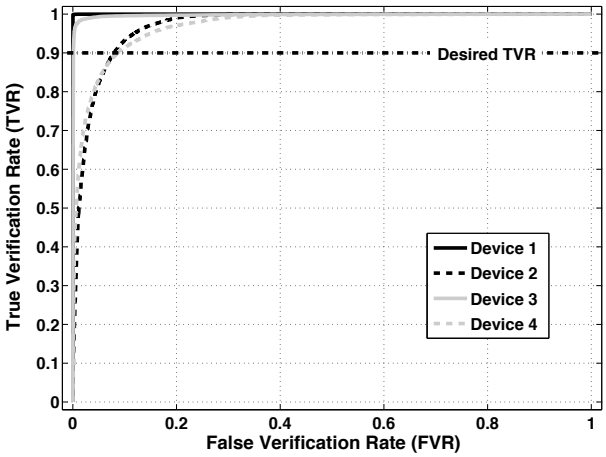


(b) GRLVQI feature selection.

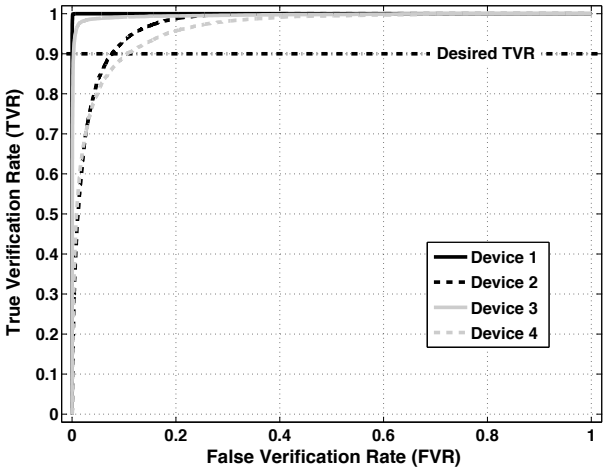
Figure 7. MDA/ML device classification using DRA subsets.

where $i = 1, 2, \ldots, N_D$ and $\mathbf{f}_j$ is the current projected RF fingerprint claiming to have an ID from device D_i. The test statistic z_V from Equation (5) was stored when the projected fingerprint $\mathbf{f}_j$ was actually from the claimed ID device.

Each designated authorized device has a stored RF signature template to use when a testing input RF fingerprint is received and claims the ID of an authorized device. In authorized device ID verification, the current testing RF fingerprints were selected from a pool of N_D authorized devices and claimed IDs of authorized devices. The test statistic from Equation (5) for current testing



(a) KS-test feature selection.



(b) GRLVQI feature selection.

Figure 8. Authorized device ID verification for $N_D = 4$ authorized devices.

fingerprints was used to create the out-of-class PMF. The resulting in-class and out-of-class PMFs were used to produce device ID verification ROC curves.

Figure 8 shows the device ID verification performance for each of the $N_D = 4$ authorized devices using a reduced feature set ($N_F = 50$) selected with pre-classification KS values and post-classification GRLVQI relevance rankings. The resulting ID verification ROC curves were evaluated at SNR =18 dB based on the classification performance benchmark ($\%C = 90\%$) for the reduced feature set ($N_F = 50$). As seen in each plot, there is a device-dependent

verification threshold t_V such that all authorized device IDs can be verified at TVR $> 90\%$ and FVR $< 10\%$ for both the methods considered.

3.5 Device ID Verification (Rogue Devices)

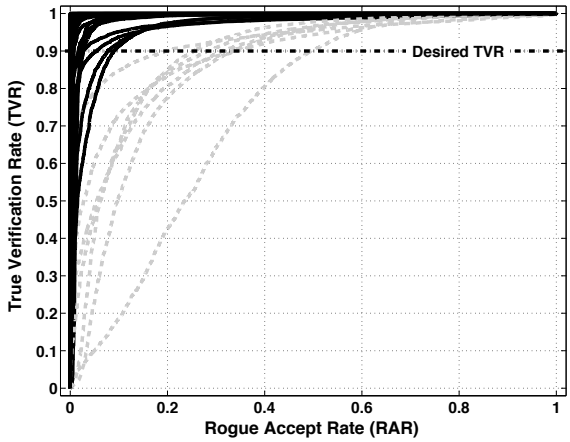
The use of RF fingerprints to reject rogue devices is demonstrated using the same device ID verification process implemented for authorized devices. In this case, the out-of-class PMFs were constructed from $N_U = 6$ (Dev5, Dev6, ..., Dev10) unauthorized rogue device RF fingerprints collected from the three locations (CAGE, LOS and WALL). A total of N_{TST}= 1,000 (SHR) $\times$ 1 (location) $\times$ 5 (N_z) = 5,000 previously unseen RF fingerprint realizations were used for each N_U device.

Rogue device rejection is an assessment of how well current RF fingerprints selected from a pool of rogue (previously unseen and unauthorized) devices match the claimed authorized device ID. The authorized device reference template created in MDA training was used when a rogue testing input RF fingerprint was received and claimed the ID of an authorized device. The test statistic from Equation (5) for current rogue testing fingerprints was used to create the out-of-class PMFs. The in-class PMF of each of the $N_D = 4$ authorized device stored templates was compared with the newly-generated rogue scenario out-of-class PMF, producing four ROC curves (one for each claimed authorized device ID). $N_U = 6$ rogue devices were used in nine different rogue device placements (three each located at CAGE, LOS and WALL) where each rogue device claimed the identity of each of the $N_D = 4$ authorized devices, producing a total of 36 rogue scenarios.

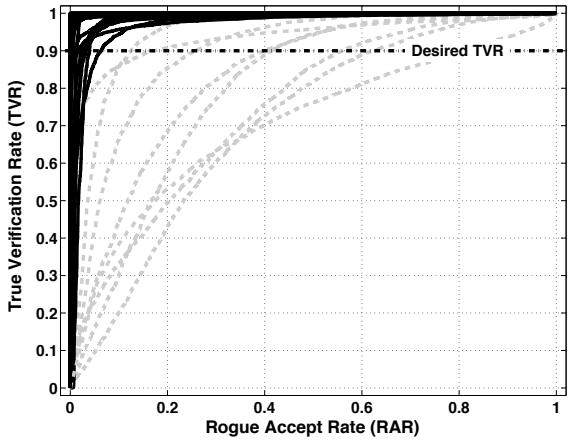
Figure 9 presents the rogue rejection results for the device ID verification process. Specifically, the figure shows the rogue device rejection for $N_U = 6$ unauthorized devices spoofing the bit-level IDs of the $N_D = 4$ authorized devices (36 total scenarios). The assessment is based on the top ranked $N_F = 50$ features with the KS-test and GRLVQI selected features. The grey ROC curves correspond to scenarios where RAR $< 10\%$ is not achieved. Each case includes 36 rogue scenarios corresponding to the feature dimensional reduction method where the top $N_F = 50$ feature sets selected were evaluated at SNR = 18 dB. The results are plotted as the rogue accept rate (RAR) versus TVR, where the rogue reject rate (RRR) is defined as RRR = 1 − RAR (higher RAR reflects poorer security performance). As shown in Figure 9, KS-test selected features perform similar to GRLVQI selected features in the case of rogue rejection. When selecting a threshold such that TVR $> 90\%$, the KS-test feature set achieves an RRR $> 90\%$ in 29 of 36 rogue scenarios considered while the GRLVQI selected features are successful in 28 of 36 scenarios (shown as solid black ROC curves).

4. Conclusions

Unauthorized ZigBee network access is a serious concern in industrial control and building automation systems. RF fingerprinting techniques have the



(a) KS-test feature selection.



(b) GRLVQI feature selection.

Figure 9. Rogue device rejection for $N_U = 6$ unauthorized devices.

potential to identify rogue devices that spoof the bit-level credentials of authorized devices. The experimental results demonstrate that ID verification with dimensionally-efficient RF fingerprints can detect and reject unauthorized rogue devices very effectively. The RF fingerprints were obtained using a dimensional reduction analysis process with relevant features identified by a pre-classification KS-test process and a post-classification GRLVQI process.

The MDA-based device ID verification process was demonstrated using $N_D = 4$ authorized devices. Using RF fingerprints comprising DRA $\approx 93\%$ of the feature subset, the classification performance benchmark of $\%C = 90\%$ was achieved at SNR ≈ 18 dB for the KS-test and GRLVQI selected features, and each method yielded a TVR greater than 90% and an FVR less than 10%

for all authorized devices. The KS-test feature set achieved a rogue reject rate exceeding 90% in 29 of 36 rogue scenarios considered while the GRLVQI selected features were successful in 28 of 36 scenarios.

Note that the views expressed in this paper are those of the authors and do not reflect the official policy or position of the U.S. Air Force, U.S. Department of Defense or the U.S. Government.

References

[1] C. Dubendorfer, B. Ramsey and M. Temple, An RF-DNA verification process for ZigBee networks, *Proceedings of the Military Communications Conference*, pp. 1–6, 2012.

[2] R. Duda, P. Hart and D. Stork, *Pattern Classification*, Wiley, New York, 2001.

[3] T. Fawcett, *ROC Graphs: Notes and Practical Considerations for Researchers*, Kluwer Academic, Dordrecht, The Netherlands, 2004.

[4] R. Klein, M. Temple and M. Mendenhall, Application of wavelet-based RF fingerprinting to enhance wireless network security, *Journal of Communications and Networks*, vol. 11(6), pp. 544–555, 2009.

[5] R. Klein, M. Temple, M. Mendenhall and D. Reising, Sensitivity analysis of burst detection and RF fingerprinting classification performance, *Proceedings of the IEEE International Conference on Communications*, 2009.

[6] B. Ramsey, M. Temple and B. Mullins, PHY foundation for multi-factor ZigBee node authentication, *Proceedings of the IEEE Global Telecommunications Conference*, pp. 795–800, 2012.

[7] D. Reising, Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing, Ph.D. Dissertation, Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2012.

[8] D. Reising, M. Temple and M. Oxley, Gabor-based RF-DNA fingerprinting for classifying 802.16e WiMAX mobile subscribers, *Proceedings of the International Conference on Computing, Networking and Communications*, pp. 7–13, 2012.

[9] W. Suski, M. Temple, M. Mendenhall and R. Mills, Using spectral fingerprints to improve wireless network security, *Proceedings of the IEEE Global Telecommunications Conference*, 2008.

[10] M. Williams, M. Temple and D. Reising, Augmenting bit-level network security using physical layer RF-DNA fingerprinting, *Proceedings of the IEEE Global Telecommunications Conference*, 2010.

[11] J. Wright, KillerBee: Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks, version 1.0 (`code.google.com/p/killerbee`).