Securing ZigBee Commercial Communications Using Constellation Based Distinct Native Attribute Fingerprinting

Christopher M. Rondeau

J. Addison Betances
Air Force Institute of Technology

Michael A. Temple
Air Force Institute of Technology

Follow this and additional works at: https://scholar.afit.edu/facpub

Part of the Computer Sciences Commons

Recommended Citation
Rondeau, Christopher M.; Betances, J. Addison; and Temple, Michael A., "Securing ZigBee Commercial Communications Using Constellation Based Distinct Native Attribute Fingerprinting" (2018). Faculty Publications. 172.
https://scholar.afit.edu/facpub/172

This Article is brought to you for free and open access by AFIT Scholar. It has been accepted for inclusion in Faculty Publications by an authorized administrator of AFIT Scholar. For more information, please contact richard.mansfield@afit.edu.
Research Article

Securing ZigBee Commercial Communications Using Constellation Based Distinct Native Attribute Fingerprinting

Christopher M. Rondeau, J. Addison Betances, and Michael A. Temple

Department of Electrical and Computer Engineering, US Air Force Institute of Technology, Wright-Patterson AFB, Dayton, OH 45433, USA

Correspondence should be addressed to Michael A. Temple; michael.temple@afit.edu

Received 19 April 2018; Revised 8 June 2018; Accepted 20 June 2018; Published 11 July 2018

Academic Editor: Bela Genge

Copyright © 2018 Christopher M. Rondeau et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This work provides development of Constellation Based DNA (CB-DNA) Fingerprinting for use in systems employing quadrature modulations and includes network protection demonstrations for ZigBee offset quadrature phase shift keying modulation. Results are based on 120 unique networks comprised of seven authorized ZigBee RZSUBSTICK devices, with three additional like-model devices serving as unauthorized rogue devices. Authorized network device fingerprints are used to train a Multiple Discriminant Analysis (MDA) classifier and Rogue Rejection Rate (RRR) estimated for 2520 attacks involving rogue devices presenting themselves as authorized devices. With MDA training thresholds set to achieve a True Verification Rate (TVR) of TVR = 95% for authorized network devices, the collective rogue device detection results for SNR \( \geq 12 \text{dB} \) include average burst-by-burst RRR \( \approx 94\% \) across all 2520 attack scenarios with individual rogue device attack performance spanning \( 83.32\% < \text{RRR} < 99.81\% \).

1. Introduction

The need to establish reliable and secure communications remains a challenge across commercial Industrial Internet of Things (IIoT) applications that support Critical Infrastructure (CI) elements (water treatment, petroleum product distribution, transportation, etc.) that are commonly operated through Industrial Control System (ICS) architectures. ZigBee networks are common within the IIoT and CI/ICS domains and remain a mainstay for implementing wireless sensor and automation networks supporting medical, smart home and building automation, and consumer electronics [1–3]. The degree of required ZigBee antihacking security varies with application criticality and will increase as the number of deployed ZigBee devices under 802.15.4 market expansion grows to 1 billion units being shipped annually by 2022 and the next generation multiprotocol 802.15.4/Bluetooth/WiFi hardware becomes available [4]. As device makers strive to take advantage of market opportunity and satisfy consumer wants for the next “greatest” interface device, it remains unclear that they have taken necessary prudent steps to address legacy security concerns.

In light of vital asset vulnerability, protection of IIoT CI and ICS elements has become a national-level priority for both the public and private sectors [5–7]. Mitigation strategies against cyberattacks have traditionally focused on bit-level solutions targeting the higher communication protocol layers and until recently there has been minimal emphasis on physical (PHY) layer development [8–10]. This work addresses hardware device identity (ID) verification as a means to enhance network security by preventing unauthorized access through the PHY doorway through which a preponderance of malicious cyberattacks occur. The focus on ZigBee device security is motivated by two factors, including the following: (1) ZigBee and related 802.15.4 communication systems are deployed world-wide and (2) ZigBee serves as a representative protocol for broader IIoT applications [11, 12]. This work expands previous wireless device ID discrimination activity that has successfully exploited various Distinct Native Attribute (DNA) features extracted from selected signal responses to reliably discriminate transmitting hardware devices.

The Constellation Based DNA (CB-DNA) development here is motivated by concepts introduced in [13] used to
discriminate Ethernet cards with features extracted from a contrived (nonconventional) binary constellation. The extension to this earlier work includes (1) formal analytic development of CB-DNA Fingerprinting for systems using conventional M-ary Quadrature Amplitude Modulation (M-QAM) signaling, (2) demonstration of CB-DNA Fingerprinting applicability to ZigBee and related 802.15.4 communication protocols, and (3) proposition of a network device ID process that incorporates mechanisms of localised RF air monitors that have been vetted for other wireless networks [14–17] while achieving security benefits of verification-based Multifactor Authentication (MFA). This proposition includes use of wireless MFA processing with success of the first “something you have” (network compliant device) and second “something you know” (authorized device bit-level ID) checks followed by a final “something you are” (biometric-based) check to boost overall security [18, 19]. While comparison of the proposed verification-based rogue detection process with fielded and/or emerging commercial approaches is certainly of interest, a meaningful comparison is not viable given that (1) implementation details of commercial methods are generally proprietary and (2) the statistical effectiveness of such methods is generally unpublished. Regardless, the computational efficiency and speed of biometric-based MFA [18] make it a top-ranked choice for communication device discrimination [19] and it is reasonable to expect similar advantages in MFA-based CB-DNA security applications.

2. Background

2.1. Quadrature Amplitude Modulation (QAM). The general development for the class of complex M-ary QAM modulated signals having in-phase/quadrature-phase (I/Q) components includes the \( m \)th complex data modulated symbol given by

\[
S_m(t) = I_{S_m} + jQ_{S_m},
\]

for \( 0 < t < T_{Sym} \) where \( T_{Sym} \) is the total symbol duration, \( m = 1, 2, \ldots, M \), and \( I_{S_m} \) and \( Q_{S_m} \) are real-valued modulation components in the I/Q constellation space with \( I_{S_m} \in \{I_S, I_{S_2}, \ldots, I_{S_M}\} \) and \( Q_{S_m} \in \{Q_S, Q_{S_2}, \ldots, Q_{S_M}\} \). For complex symbols given by (1), a transmitted \((Tx)\) burst of \( N_{Sym} \) QAM modulated symbols is given by

\[
S_{Tx}(t) = \sum_{m=1}^{N_{Sym}} S_m(t - kT_{Sym}) \exp(2\pi f_c t + \phi_{Tx}),
\]

\[
S_{Rx}(t) = \sum_{m=1}^{N_{Sym}} S_m(t - kT_{Sym}) \cos(2\pi f_c t + \phi_{Tx}) + j \sum_{m=1}^{N_{Sym}} S_m(t - kT_{Sym}) \sin(2\pi f_c t + \phi_{Tx}),
\]

for \( 0 < t < N_{Sym} XT_{Sym} \) with \( f_c \) being the transmitted carrier frequency and \( \phi_{Tx} = \phi/2 \) accounting for quadrature-phase error induced by hardware components [21]. The sequence of ideal transmitted QAM symbols in \( S_{Tx}(t) \) is denoted by vector \( S_m = (S_1, S_2, \ldots, S_m, \ldots, S_{N_{Sym} - 1}, S_{N_{Sym}}) \) where \( S_m \in [S_1, S_2, \ldots, S_M] \). For the case of \( M = 4 \)-ary signaling, the QAM \( S_{Tx}(t) \) expression in (2) can be used to effectively represent the 4-ary Offset Quadrature-Phase Shift Keyed (O-QPSK) used here for ZigBee demonstration.

Considering channel amplitude \( A_{Ch} \) and transmitter-to-receiver propagation delay \( \tau_{Ch} \) factors, the received \((Rx)\) burst corresponding to \( S_{Tx}(t) \) in (2) is given by

\[
S_{Rx}(t) = A_{Ch} S_{Tx}(t - \tau_{Ch}),
\]

which has baseband received \( I_{Rx}(t) \) and \( Q_{Rx}(t) \) components that can be expressed as

\[
I_{Rx}(t) = G_{I/Q} \sum_{k=1}^{N_{Sym}} I_{S_k} \left( t - kT_{Sym} - \tau_D \right) + O_I(t),
\]

\[
Q_{Rx}(t) = G_{I/Q} \sum_{k=1}^{N_{Sym}} Q_{S_k} \left( t - kT_{Sym} - \tau_D \right) + O_Q(t),
\]

where \( G_{I/Q} \) is the I/Q gain imbalance, \( \tau_D \) accounts for \( \tau_{Ch} \) and relative time delay between receiver I/Q channels, and \( O_I(t) \) and \( O_Q(t) \) represent I/Q offset factors [21]. The \( G_{I/Q}, \tau_D, O_I(t), \) and \( O_Q(t) \) factors in (4) and (5) collectively account for transmitter \( \phi_{Tx} \) error in (2) and additional receiver imperfections. The sequence of corrupted received QAM symbols in \( S_{Rx}(t) \) is denoted by vector \( S_k = (S_1, S_2, \ldots, S_k, \ldots, S_{N_{Sym} - 1}, S_{N_{Sym}}) \).

The cumulative effect of transmitter-receiver imperfections and channel errors captured in \( I_{Rx}(t) \) and \( Q_{Rx}(t) \) components is a degradation in received QAM symbol estimates, denoted here as \( \hat{S}_k = (\hat{S}_1, \hat{S}_2, \ldots, \hat{S}_k, \ldots, \hat{S}_{N_{Sym} - 1}, \hat{S}_{N_{Sym}}) \) for a given \( S_k \), induced by a location shift of received \( C^\phi = I_{S_k} + jQ_{S_k} \) QAM constellation points relative to the corresponding ideal transmitted \( C^\phi = I_{S_k} + jQ_{S_k} \) constellation points. In addition to potential QAM symbol estimation error induced by received \( C^\phi \) deviation, there are two other receiver processes that are key for achieving reliable QAM symbol estimation, including (1) received carrier frequency offset \( f_{Rx} \) estimation and (2) phase recovery for symbol constellation derotation.

2.1.1. Received Carrier Estimation. Following downconversion by \( f_c \) and baseband filtering, samples of the received M-QAM signal at the receiver’s Matched Filter (MF) output can be modeled as [22]

\[
S_{MF}(n) = K_{R} S_k(n) \exp(j 2 \pi f_{Rx} T) + N_{B}(n),
\]

where \( n = 1, 2, \ldots, N_{MF} \), \( K_R \) is a real-valued scalar, \( S_k \) are the transmitted QAM symbols in (2), \( f_{Rx} \) is relative received carrier frequency offset, and \( N_B \) is communication channel background noise [22]. The residual \( f_{Rx} \) in \( S_{Rx}(t) \) can be estimated by raising \( S_{RF}(n) \) in (6) to the \( M \)th power to remove the modulation effects. This effectively creates a multitone spectral response with a dominant (highest power) tone
algorithm that rotates the received constellation derotation was implemented here using an
phase errors [24]. While generally beneficial, this within-
2.1.2. Constellation Phase Recovery. Receivers commonly use
the discrete Fourier transform.

occuring at M×f_{Rx} [23]. This is illustrated for 4-QAM where
S_{MF}^4(n) can be expanded as

\[ S_{MF}^4(n) = \left[K_RS_m(n)\right]^4 \exp\left(j8\pi f_{Rx}t\right) \]
\[ + 4 \left[K_RS_m(n)\right]^3 \exp\left(j6\pi f_{Rx}t\right) N_B(n) \]
\[ + 4 \left[K_RS_m(n)\right]^2 \exp\left(j2\pi f_{Rx}t\right) N_B^2(n) \]
\[ + 6 \left[K_RS_m(n)\right] \exp\left(j4\pi f_{Rx}t\right) N_B^3(n) \]
\[ + N_B^4(n) \]

which includes a dominant 8πf_{Rx} = 2π(4f_{Rx}) frequency component. The estimated received carrier frequency offset is
given by f_{Rx} = 4[\arg\max_{\theta}(\mathcal{F}[S_{MF}^4(n)])] where \mathcal{F}(\cdot) denotes the discrete Fourier transform.

2.1.2. Constellation Phase Recovery. Receivers commonly use
a Phase Locked Loop (PLL) to reconstruct the suppressed carrier via dynamic feedback that autocompensates for phase errors [24]. While generally beneficial, this within-burst autocompensation can potentially obscure subtle DNA feature differences that may help discriminate transmitters. Therefore, burst-by-burst discrete phase estimation and constellation derotation was implemented here using an algorithm that rotates the received C^S_m constellation points for each burst from 0 to \pi/2 radians in N_A = 100 increments and selects the phase rotation angle yielding the minimum variance between the incrementally rotated pool of received C^S_m and the ideal C^S_m constellation points. The pseudocode for implementing this algorithm is presented in Table 1.

There are four different phase ambiguity that can exist after derotating the constellation using the algorithm in Table 1. These are resolved using estimated rotation angles of known preamble (training) symbols. The rotated constellation projections can also be normalized by scaling (dividing) each Rot(C^S_m) point by the mean (\langle Rot(C^S_m)\rangle) which locates the center of all constellation clusters on the unit circle.

2.2. ZigBee Communications. The ZigBee Communication protocol includes a Medium Access Control (MAC) layer, where device IDs are verified using bit-level credentials, that
interfaces with the RF communications channel through the PHY layer using RF hardware and firmware [25]. The PHY layer is implemented according to the IEEE 802.15.4 standard for low data-rate, low-power, and short range RF communications [20]. It is estimated that more than one billion 802.15.14 compliant components will be sold by the end of this decade with a majority of them supporting localised smart home networks [4]. One such component is the Atmel AT86RF230 radio transceiver that is hosted on RZUSBSTICK devices [26]. These are small low-power devices that support ZigBee operation at 2.4 GHz through an integrated folded dipole antenna with a net peak gain of G_A = 0 dB. Accounting for G_A = 0 dB and maximum AT86RF230 output power of P_{Out} = +3.0 dBm [27], the effective transmit power of the RZUSBSTICK is P_{Tx} = +3.0 dBm which make it a viable alternative for not only smart home networks but other wireless sensor networks, industrial control system, and building automation [27]. Details for the specific RZUSBSTICK devices used for demonstration are provided in Table 2 which shows the unique ZigBee Communication (ZC) device IDs assigned for experimentation.

The use of PHY layer O-QPSK modulation is mandatory for ZigBee operation at 2.4 GHz, with the O-QPSK modulator preceded by a 4-to-32 (information bit-to-spread chip) Pseudorandom Noise (PN) mapping such that the information bits are transmitted at an effective rate of (2M Chips/Sec) \times (4/32 Bits/Chip) = 250K Bits/Sec [20, 25]. Accounting for I/Q channel offset processing in the modulator, the corresponding output O-QPSK communication symbol rate for a transmitted S_{Sym}(t) burst given by (2) is R_{Sym} = 1/T_{Sym} = (250K Bits/Sec)/(2 Bits/Sym) = 125K Sym/Sec.

The required 4-to-32 PN mapping for 2.4 GHz ZigBee operation is shown in Table 3 [20]. Given this mapping, there are specific transmitted O-QPSK S_{m} symbol sequences that occur with varying probability. For example, the bold highlighted \{1 0 0 1 0 0\} 6-bit pattern in the output chip sequences in Table 3 is among the most frequently occurring ones (appears in 13 of 16 chip sequences) and produces the O-QPSK transmitted symbol sequence S_m = (S_2, S_3, S_4, S_5). This 5-symbol S_{m} vector is denoted in Table 4 by an * and

<table>
<thead>
<tr>
<th>ID</th>
<th>MAC</th>
<th>Mark 1</th>
<th>Mark 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZC1</td>
<td>A0:F6:9F:E7</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
<tr>
<td>ZC2</td>
<td>A0:01:43:70</td>
<td>0923 PH</td>
<td>8P0772</td>
</tr>
<tr>
<td>ZC3</td>
<td>A0:01:5D:34</td>
<td>0936 PH</td>
<td>9P0187-2</td>
</tr>
<tr>
<td>ZC4</td>
<td>A0:F6:A0:68</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
<tr>
<td>ZC5</td>
<td>A0:F6:A0:4E</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
<tr>
<td>ZC6</td>
<td>A0:F6:9F:FF</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
<tr>
<td>ZC7</td>
<td>A0:F6:A0:0C</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
<tr>
<td>ZC8</td>
<td>A0:F6:A0:04</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
<tr>
<td>ZC9</td>
<td>A0:F6:9F:EA</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
<tr>
<td>ZC10</td>
<td>A0:F6:9F:E0</td>
<td>1442 PH</td>
<td>IR8338-7</td>
</tr>
</tbody>
</table>

Table 1: Constellation phase derotation algorithm.

Require: Received Constellation Projection C^S_m
RotationVariances \leftarrow \co
for N_A = 1 \to 100 \textbf{do}
\theta \leftarrow (N_A \cdot \pi)/(2 \times 100)
Rot(C^S_m) \leftarrow C^S_m \cdot e^{j\theta}
Temp \leftarrow |Re[Rot(C^S_m)]| + jIm[Rot(C^S_m)]
RotationVariances (N_A) \leftarrow Variance(Temp)
end for
N_A \leftarrow \arg\min_{N_A}[RotationVariances]
return C^S_m \cdot e^{j(N_A \pi)/(2 \times 100)}
training means ($\mu$) and covariances ($\Sigma$). MDA models are generated using a pool of 4400 total fingerprints per class that are equally divided into $N_{TNG} = 2200$ Training (even indexed fingerprints) and $N_{TST} = 2200$ Testing (odd indexed fingerprints) subsets. The even-odd indexing assignment ensures the models account for temporal channel variation, collection bias, etc., effects occurring during the course of emission collection.

The TNG fingerprints at a given SNR are used for MDA model training that includes $K = 5$-fold cross-validation [Dud1] with the best projection matrix $W_{\text{Best}}$ selected as the fold $W$ producing the highest cross-validation accuracy. The TST fingerprints are then input to the model and a 1 versus $N_{ClS}$ best match ML classification decision is made based on a selected classification test statistic ($Z_{ClS}$). The trained class yielding highest conditional probability $P(Z_{Gi} \mid Z_{ClS})$ for all $i = 1, 2, \ldots, N_{ClS}$ is the called class (right or wrong) assigned to the unknown input fingerprint $\mathbf{F}$. Classification performance at a given SNR is presented in an $N_{ClS} \times N_{TST}$ (input versus called) classification confusion matrix, with (1) average cross-class percent correct classification ($\%C$) calculated as the sum of diagonal (correct) matrix entries divided by the total number of classification trials ($N_{ClS} \times N_{TST}$) and (2) individual class $\%C$ for each class $C_i$ calculated as the sum of $i$th row entries divided by $N_{TST}$. Alternately, classification performance is presented in $\%C$ versus SNR plots.

The device ID verification process uses the selected MDA model components ($W$, $\alpha$, $\mu$, and $\Sigma$) and device TST fingerprints to estimate both (1) authorized network device True Verification Rate (TVR) (true positive) and (2) unauthorized device Rogue Rejection Rate (RRR) (true negative). For a given claimed (unknown) authorized device ID to be verified, the process includes the following: (1) projecting TST $\mathbf{F}$ fingerprints for the device under test into the $N_{ClS}$-1 discrimination space using $\mathbf{P}_F = \alpha \otimes \mathbf{W}$ where $\otimes$ denotes element-by-element vector multiplication, (2) calculating the selected verification test statistic ($Z_{Fv}$) for $N_{TST}$ total fingerprints using training $\mu$ and/or $\Sigma$, (3) forming a normalized (unit area) Probability Mass Function (PMF) using $N_{TST}$ total $Z_{Fv}$, (4) overlaying a desired training verification threshold ($t_{Fv}$), and (5) calculating the PMF area above/below $t_{Fv}$ to estimate the desired verification rate. Common $Z_{Fv}$ measures of similarity include (1) distance-based metrics such as the Euclidean distance between projected $\mathbf{P}_F$ and the claimed training class mean $\mu$ and (2) probability-based metrics that map the calculated $\mathbf{P}_F$ Euclidean distance to a normalized multivariate Gaussian probability distribution having mean $\mu$ and covariance $\Sigma$. Euclidean distance is perhaps the most easily conceptualised and was chosen here for proof-of-concept demonstration.

The PMFs in Figure 1 are used to illustrate Device ID verification for Euclidean distance “lower-is-better” measure of similarity [11]. Given these PMFs, the ID verification process includes (1) using network ZC TNG fingerprint $Z_{Fv}$ to set the training verification threshold $t_{Fv}$ shown in Figure 1(a) to achieve the desired TVR (blue PMF1 area) where PMF1 is for ZC TNG and PMF2 is based on accumulated TNG $Z_{Fv}$ for

### Table 3: Input-output sequences for ZigBee 4-to-32 premodulation PN mapping [20].

<table>
<thead>
<tr>
<th>Input [$b_0, b_1, b_2, b_4$]</th>
<th>Output Chip Sequence [$c_0, c_1, c_2, \ldots, c_{31}$]</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>1010010011000011001010001010110</td>
</tr>
<tr>
<td>1000</td>
<td>11010010101010011010010101000010</td>
</tr>
<tr>
<td>0100</td>
<td>00101101101001110001100101001010</td>
</tr>
<tr>
<td>1100</td>
<td>00100010110011001010010101000011</td>
</tr>
<tr>
<td>0010</td>
<td>01000100101010100110010101000001</td>
</tr>
<tr>
<td>1010</td>
<td>01100010011010011001101100110100</td>
</tr>
<tr>
<td>1110</td>
<td>0110100000011011101000001</td>
</tr>
<tr>
<td>0011</td>
<td>00101110000111011101000001</td>
</tr>
<tr>
<td>1011</td>
<td>01100000011110000111011001000010</td>
</tr>
<tr>
<td>1111</td>
<td>1010010001011011010010100000101</td>
</tr>
</tbody>
</table>

* is among the 30 highest probability transmitted O-QPSK $S_m$ used for conditional CB-DNA demonstration.
all “other” network ZCk (k = 1, 2, , N_C, and k ≠ i) and (2) calculating the corresponding RRR (true negative, blue PMF2 area) in Figure 1(b) where PMF1 is the same and PMF2 is based on TST fingerprint ZV for the rogue ZRj device. ID verification performance can be based on TNG tV(i) set for either (1) equal error rate conditions with False Verification Rate (FVR) given by FVR = 1 - TVR or (2) a specific desired authorized TVR.

The authorized TVR (true positive) versus FVR (false positive) trade-off is effectively captured in a Receiver Operator Characteristic (ROC) curve [Faw1] as shown in Figure 2 using Figure 1 PMFs with varying the TNG verification threshold tV varied from Min[ZV] to Max[ZV]. Figure 2(a) shows TVR versus FVR with the indicated operating point (■) corresponding to desired TVR = 90% and yielding FVR ≈ 1.2%. Figure 2(b) shows TVR versus RAR where Rogue Accept Rate (false positive) is used to estimate the RRR ≈ 1-RAR shown along the x-axis for three arbitrary ZR devices (▼, ▲, and ▼) and the TVR = 90% operating point.

3. CB-DNA Fingerprinting Development

Time domain RF-DNA Fingerprinting has historically exploited statistical features extracted from partial-burst responses where invariant (data independent) synchronisation and channel estimation (preamble, midamble, etc.) symbols are transmitted [15, 28–30]. The CB-DNA Fingerprinting method developed here differs considerably and exploits features extracted from full-burst responses, including regions where variant (data dependent) symbols are transmitted. The CB-DNA Fingerprinting development here is motivated by concepts first used in [13] to discriminate
Ethernet cards but it fundamentally differs in that work in [13] is based on features extracted from a contrived (nonconventional) binary constellation while the development here is for any application using conventional M-QAM signaling as introduced in Section 2.1. The development for unconditional and conditional fingerprinting is supported by the process depicted in Figure 3.

For ideal transmitted symbols having constellation projections $C_{S_m}^n$ such as those shown in Figure 3(a), the $k$th received QAM symbol in burst $S_{R_k}(t)$ of (3) is denoted as $S_k$ for $t_k < t < t_k + T_{Sym}$ where $t_k$ is the symbol start time, $T_{Sym}$ is the symbol duration, and $k = 1, 2, \ldots, N_{Sym}$ where $N_{Sym}$ is the total number of symbols in a received burst. Following synchronisation to the $k$th symbol interval, the QAM receiver extracts symbol $S_k$ and projects it to a single point $C_{S_k}^n$ in the QAM constellation space (Figure 3(b)). The corresponding estimated transmitted symbol is determined as $\hat{S}_k = S_m : \arg \min_m [C_{S_k}^n - C_{S_m}^n]$, for $m \in \{S_1, S_2, \ldots, S_M\}$ (Figure 3(c)). For generating unconditional CB-DNA statistical fingerprint features, the $N_{Sym}$ received $C_{S_k}^n$ in each $S_{R_k}(t)$ burst are grouped based on their corresponding $\hat{S}_k = S_m$ estimate with the group of $C_{S_k}^n$ yielding the $m$th QAM symbol estimate denoted by the sequence $\{C_{S_m}^n\}$ for $m = 1, 2, \ldots, M$.

While some prior works have investigated constellation error differences as a means for device discrimination [31], e.g., mean and variance, of Euclidean distances between received $C_{S_k}^n$ and ideal $C_{S_{m0}}^n$, the approach here exploits constellation spatial statistical differences in $[C_{S_m}^n]$ groups which are induced by channel propagation and hardware variability (e.g., I/Q imbalance) resulting from component differences (oscillator phase noise, spurious mixer tones, manufacturing processes, etc.) [21]. The exploitation of these differences was first demonstrated for the contrived binary constellation work in [13] which showed that the statistical distribution of $[C_{S_m}^n]$ elements around the corresponding ideal $C_{S_m}^n$ point is conditional, i.e., the location of a given $C_{S_k}^n$ for $S_k$ in the received QAM constellation space is dependent upon symbols received just prior to and immediately following $S_k$; these two symbols are denoted as $S_{k-1}$ and $S_{k+1}$, respectively.

The device discrimination improvement in [13] using conditional fingerprint features from the contrived binary constellation motivated formal development of the multisymbol constellation conditioning (subgrouping) method for M-QAM signaling. For the $S_k$ dependent $[C_{S_m}^n]$ group sequences, the basic process includes considering multiple consecutive received QAM symbols in a $S_{R_k}(t)$ burst which are denoted here by vector $S_k = (\ldots, S_{k-2}, S_{k-1}, S_k, S_{k+1}, S_{k+2}, \ldots)$ where $S_k$ is the central reference symbol. These received symbols have corresponding estimates that are used to form vector $\hat{S}_k = (\ldots, \hat{S}_{k-2}, \hat{S}_{k-1}, \hat{S}_k, \hat{S}_{k+1}, \hat{S}_{k+2}, \ldots)$ where $\hat{S}_k$ is the estimate for reference symbol $S_k$. Multisymbol constellation conditioning involves parsing each of the unconditional $[C_{S_m}^n]$ groups into conditional $[C_{S_m}^{n(m)}]$ subgroups for $n = 1, 2, \ldots, N_{SG}$ total subgroups with $S_{k(m)}$ denoting the $n$th subgroup. The parsing of unconditional $[C_{S_m}^n]$ sequences and selection of $N_{SG}$ subgroups is somewhat arbitrary but performed with a goal of maximising cross-subgroup distribution differences that will be captured in statistical fingerprint features.
The subgrouping of \( \{C_m^n\} \) is illustrated (as shown in Figure 3(d)) by considering three received symbols of \( S_k = (S_{k-1}, S_k, S_{k+1}) \) and a set of \( N_{SG} \) desired subgroup conditioning vectors \( G^k \) of equivalent dimension and denoted by \( G^k = (G^k_1, G^k_2, G^k_3) \) where \( G^k_i \in \{S_1, S_2, \ldots, S_M\} \). The process for assigning each element of the \( m \)-th \( \{C_m^n\} \) group to one of \( N_{SG} \) subgroups based on \( G^k \) conditions includes (1) taking each received \( S_k \) producing \( C_m^n \), (3) estimating received \( S_{k-1} \) and \( S_{k+1} \) and forming \( S_k = (S_{k-1}, S_k, S_{k+1}) \), and (4) comparing the resultant \( S_k \) with each desired \( G^k \). If \(|S_k - G|^n \neq 0\) for some \( n = 1, 2, \ldots, N_{SG} \) the \( C_m^n \) symbol under evaluation is assigned to the \( n \)-th conditional \( \{C_{m(n)}^n\} \) subgroup. If \(|S_k - G|^n = 0\) for all \( n \) the \( C_m^n \) symbol under evaluation is assigned to an “other” conditional subgroup. Formation of the \( N_{SG} + 1 \) “other” subgroup is required when all possible combinations of estimated \( S_k \) symbols are not included as desired \( G^k \) conditions and ensures that all elements of \( \{C_m^n\} \) are accounted for. Accounting for all possible M-QAM symbol vectors, the total number of conditional subgroups formed for fingerprint generation is either \( M \times N_{SG} \) or \( M \times N_{SG} + 1 \) if an “other” subgroup is required.

There are many possible symbol combinations that could be used for conditioning \( G^k \) vectors and formation of conditional subgroups. In light of noted M-QAM I/Q phase imbalance effects, there are some specific \( G^k \) that may accentuate cross-subgroup differences based on how the phase in consecutive \( S_{R_x}(t) \) symbols changes during QAM signaling. The two extreme phase changes are captured using (1) \( G^k = (S_k, S_k, S_k) \) which represents the case of no symbol-to-symbol phase change across \( S_k \) symbols and (2) \( G^k = (S_k, -S_k, -S_k) \) which represents the case of maximum \( \pm 180 \) degrees’ symbol-to-symbol phase change across \( S_k \) symbols. Considering 4-QAM and accounting for all possible symbol combinations in the \( 1 \times 3 \)-dimensional \( G^k \) vectors, there are a total of \( N_{SG} = 16 \) conditional \( \{C_{m(n)}^n\} \) subgroup sequences for \( m = 1, 2, 3, 4 \) with no “other” subgroup formed. The effect of conditional subgrouping is illustrated with the aid of Figure 4 which shows an unconditional QAM received constellation for an \( S_{R_x}(t) \)

\[
F^X = \begin{bmatrix} \sigma^2_{Mag(X)} & \kappa_{Mag(X)} & \sigma^2_{Ang(X)} & \gamma_{Ang(X)} & \kappa_{Ang(X)} \end{bmatrix} \sqrt{\sigma^2_{X(1:3)} \gamma^2_{X(1:2)} \kappa_{X(1:3)}}_{1 \times N_{Stat}},
\]

where \( N_{Stat} = 14 \) if all indicated statistics are included.

For unconditional CB-DNA Fingerprinting \( F^X \) in (8) is calculated for all \( m = 1, 2, \ldots, M \) constellation symbols with \( |X| = |C_m| \) and the resultant \( F_m \) concatenated to form the final composite unconditional CB-DNA Fingerprint vector \( F_{CB}^{UNC} \) given by

\[
F_{CB}^{UNC} = \left[ F_1^X; F_2^X; \cdots; F_M^X \right]_{1 \times N_{UNC}},
\]

where \( N_{UNC} = N_{Stat} \times M \) is the total number of unconditional CB-DNA features.

For conditional CB-DNA Fingerprinting \( F^X \) in (8) is calculated for all \( m = 1, 2, \ldots, N_{SG} \) subgroups of each \( m = 1, 2, \ldots, M \) constellation symbol using \( |X| = |C_{m(n)}| \). The resultant \( F_{CB}^{COND} \) vectors are used form the \( m \)-th Conditional CB-DNA Fingerprint vector \( F_m^{COND} \) given by

\[
F_{m}^{COND} = \left[ F_{SG(m,1)}^{COND}; F_{SG(m,2)}^{COND}; \cdots; F_{SG(m,N_{SG})}^{COND} \right]_{1 \times (N_{Stat} \times N_{SG})},
\]
Figure 4: Received unconditioned QAM constellation at SNR = 12 dB for a burst of $N_{sym} \approx 3400$ symbols producing approximately 850 total projections in the indicated $C_1^{Sk}$, $C_2^{Sk}$, $C_3^{Sk}$, and $C_4^{Sk}$ quadrant groups.

Figure 5: Received conditional QAM constellation points for $S_1$ quadrant projections in Figure 4 showing pairwise relationship of five conditioned $\{C_1^{Sk}\}$ subgroups with elements assigned using the indicated $G^n$ conditions.
which are concatenated for all \( m = 1, 2, \ldots, M \) to form the composite conditional CB-DNA Fingerprint vector

\[
\mathbf{F}_{\text{CND}}^{\text{CB}} = \left[ \mathbf{F}_1^{\text{CND}} ; \mathbf{F}_2^{\text{CND}} ; \ldots ; \mathbf{F}_M^{\text{CND}} \right]_{1 \times N_{\text{CND}}^{\text{CB}}},
\]

where \( N_{\text{CND}}^{\text{CB}} = N_{\text{Stag}} \times N_{\text{SG}} \times M \) is the total number of conditional CB-DNA features. In general, unconditional and conditional CB-DNA fingerprint features can be generated using all or a subset of noted statistics, calculated for all or a subset of available projected \( \{ C_{\text{Stag}}^k \} \) groups or \( \{ C_{\text{Stag}}^m \} \) subgroups. The choice of which statistics and which groups to use may vary with the specific communication application (fixed, mobile, urban, city, etc.) and determines the final number of \( N_{\text{CND}}^{\text{UCB}} \) and \( N_{\text{CND}}^{\text{CCB}} \) features generated.

4. CB-DNA Fingerprinting Demonstration

ZigBee transmissions were collected for all RZUSBSTICK devices in Table 2 using an X310 Software Defined Radio (SDR) having an RF bandwidth of \( W_{\text{RF}} = 10 \text{ MHz} \) and operating at a sampling rate of \( f_s = 10 \text{ MSPs} \) in both the I/Q channels. Subsequent postcollection signal processing was performed using MATLAB and included burst-by-burst (1) center frequency estimation, (2) baseband (BB) downconversion and filtering using a 16th-order Butterworth filter having a -3 dB bandwidth of \( W_{\text{BB}} = 2 \text{ MHz} \), (3) constellation phase de-rotation, and (4) unconditional and conditional CB-DNA fingerprint generation per Section 3. The CB-DNA fingerprints were used to generate demonstration results for a total of \( N_{\text{NC}} = 10 - \text{choose-3} = 120 \) unique network configurations with the \( N_{\text{ZR}} = 3 \) chosen devices serving as unauthorized attacking ZigBee Rogue (ZR) devices and the remaining \( N_{\text{ZC}} = 7 \) devices serving as authorized ZC network devices.

For each network configuration, the RRR was estimated for the \( N_{\text{ZR}} = 3 \) rogue devices using the device ID verification process detailed in Section 2.3. For each network configuration, each of the \( N_{\text{ZR}} = 3 \) ZR devices presents false ID credentials for all \( N_{\text{CBS}} = 7 \) authorized ZC network devices for a total of \( 7 \times 3 = 21 \) ZRj/ZCi assessments per network configuration. Considering all networks, a total of \( 120 \times 21 = 2520 \) ZRj/ZCi device ID verification (rogue detection) assessments were completed. Alternately, each ZC device in Table 2 served as an attacking ZR device 36 times for a total of \( 36 \times 7 = 252 \) ZRj/ZCi device ID verification assessments per RZUSBSTICK device. The RRR estimates are based on a total of 4400 fingerprints per ZR device that are presented on a fingerprint-by-fingerprint basis for ID verification; the assessments here do not include nor account for envisioned benefits to be realised by averaging fingerprints, features, etc., prior to making a final authorized versus rogue verification decision. For presentation brevity, limited results are presented herein that are representative of the poorest (lowest RRR) and best (highest RRR) results obtained across all \( N_{\text{NC}} = 120 \) network configurations and are sufficient for supporting proof-of-concept demonstration conclusions.

4.1. Authorized Network Device Classification. Device classification is first required to generate the MDA/ML models \( (\mathbf{W}, \alpha, \mu, \text{ and } \Sigma) \) required for device ID verification. The CB-DNA Fingerprinting results in Figure 6 were generated using unconditional and conditional features for all \( N_{\text{NC}} = 120 \) networks. Results show \%C versus SNR for all 120 networks along with cross-network average \%C (solid lines) and extreme bounds (dashed lines with \( \circ \) markers) for highest and lowest \%C. The benefit of constellation conditioning is evident by comparing cross-network averages which show that the \( \%C = 90\% \) benchmark is achieved for conditional features (\( \bullet \)) at SNR = 11 dB and unconditional features (\( \blacktriangle \)) at SNR = 14 dB. For presentation brevity, additional results in this section are presented for conditional CB-DNA Fingerprinting only given its superiority.

For conditional CB-DNA Fingerprinting at SNR = 12 dB in Figure 6(b), the extreme results include (1) lowest \%C = 86.78% performance for Model #1 (excludes ZC1, ZC2, and ZC3 devices) and (2) highest \%C = 98.75% performance for Model #90 (excludes ZC4, ZC5, and ZC10 devices). The classification confusion matrices for these extreme cases are provided in Tables 5 and 6 and suggest that the inclusion of ZC4, ZC5, ZC6, and ZC10 devices in Model #1 is most detrimental (italic entries in Table 5). Of note from Table 2 is that package markings for the ZC2, ZC3 pair differs from all other package markings. Thus, Model #1 versus Model #90 performance is consistent with historical DNA discrimination given that the ZC2, ZC3 pair is (1) excluded in the poorest Table 5 results (model includes all like-model, similarly marked devices) and (2) included in the highest Table 6 results (model includes a higher number of like-model dissimilarly marked devices).

4.2. Authorized Network Device ID Verification. SNR dependent MDA/ML model components \( (\mathbf{W}, \alpha, \mu, \text{ and } \Sigma) \) from Section 4.1 are used to assess authorized network ZC device ID verification at selected verification SNR\(_{V}\). Results are presented for conditional CB-DNA fingerprints at SNR\(_{V}\) = 12 dB where average MDA/ML performance in Figure 6(b) achieves the \%C = 90\% benchmark. For each network, device TNG fingerprints are used to set device dependent \( t_{V}(i) \) for all authorized devices to achieve TVR \( \approx 95\% \). \( t_{V}(i) \) for the worst and best performing MDA/ML models in Figure 6(b) are shown in Figure 7(a) (Model #1) and Figure 7(b) (Model #90). \( t_{V}(i) \) are overlaid with Euclidean distance TNG statistics \( (Z_{V}) \) and ID verification identified as either accept (\( \circ \)) or reject (\( \times \)) decisions. The accept/reject decisions and final performance are based on \( Z_{V} \) for TVR\(_{TNG} = 2200 \) fingerprints per authorized device with \( Z_{V} < t_{V}(i) \) (\( \circ \) markers) representing correct ID verification (proper access granted) and \( Z_{V} > t_{V}(i) \) (\( \times \) markers) representing incorrect ID verification (improper access denial). The resultant TVR for individual ZC devices is shown along the x-axis and yields an overall cross-ZC average TVR = 94.84% for both models.

4.3. Unauthorized Rogue Device Detection. Accounting for all \( N_{\text{NC}} = 120 \) network configurations with each of the \( N_{\text{ZR}} = 3 \) held-out ZRj (\( j = 1, 2, \ldots, 10 \), \( j \neq i \)) devices serving in an attacking ZRj/ZCi role a total of 252 times (including multiple
attacks against a given ZCi device present in multiple networks), the cumulative per ZRj RRR performance averaged across all networks for $8 \leq \text{SNR}_V \leq 20$ dB is shown in Table 7. Of note here is the average cross-ZRj RRR $\approx 89.42\%$ at SNR$_V = 12$ dB which is approximately the same SNR where MDA/ML device classification in Figure 6(b) achieves the %C = 90% benchmark. As shown in Table 7 SNR$_V = 12$ dB results, the lowest RRR occurs for ZR4 and ZR6 devices and the highest RRR occurs for ZR1 and ZR3 devices. Excluding SNR$_V = 8$ dB performance, collective rogue device results for SNR$_V \geq 12$ dB include (1) cumulative cross-ZR RRR $\approx 94\%$ across all ZR:ZC attack scenarios and (2) individual cross-ZR performance across 252 attacks spanning $83.32\% < \text{RRR} < 99.81\%$.
Table 7: Conditional rogue ID verification performance showing cumulative average RRR (%) for indicated ZRj. The highest and lowest RRR per SNRν are denoted by bold text and italic, respectively.

<table>
<thead>
<tr>
<th>SNRν (dB)</th>
<th>ZR Rogue ID</th>
<th>Cross-ZR Ave</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ZR1</td>
<td>ZR2</td>
</tr>
<tr>
<td>8</td>
<td>95.55</td>
<td>65.76</td>
</tr>
<tr>
<td>12</td>
<td>99.24</td>
<td>83.17</td>
</tr>
<tr>
<td>16</td>
<td>99.64</td>
<td>92.78</td>
</tr>
<tr>
<td>20</td>
<td>99.66</td>
<td>98.64</td>
</tr>
</tbody>
</table>

For the overall poorest ZR4 and ZR6 results in Table 7 at SNRν = 12 dB there are eight network models (#1, #45, #66, #86, #91, #92, #93, and #94) that include both ZR4 and ZR6 serving as rogue devices. Considering only these models, the cumulative ZR4 and ZR6 results include RRR ≈ 85.25% and RRR ≈ 82.03%, respectively. The overall poorest ZR4 and ZR6 RRR results for these eight models at SNRν = 12 dB are presented in Figure 8 and occur for Model #45 with ZC1, ZC3, ZC5, ZC7, ZC8, ZC9, and ZC10 authorized devices. As estimated by averaging individual ZRj:ZCi RRR presented along Figure 8 x-axes, the average performance is RRR ≈ 82.94% for ZR4:ZCi and RRR ≈ 77.56% for ZR6:ZCi. These are higher than the cumulative model averages in Table 7 and thus do not represent the overall poorest ZR4 and ZR6 device results.

For completeness, the overall poorest ZR4 and ZR6 RRR results across all 120 models are presented in Figure 9 which shows that the lowest RRR results are obtained for separate models and include average RRR = 76.7% in Figure 9(a) for ZR4 with Model #19 and average RRR = 64.84% in Figure 9(b) for ZR6 with Model #4. While it is not immediately obvious why these are the two poorest cases, these ID verification results are consistent with the increased MDA/ML classification challenge noted in Section 4.1 for models based on similarly marked authorized devices. Specifically, the poorest RRR < 80% results in Figure 9 are all attributable to ZCj:ZCi combinations of similarly marked ZC4, ZC5, ZC6, and ZC10 devices.

For the overall best RRR ZR1 and ZR3 results in Table 7 at SNRν = 12 dB there are eight network models (#1, #9, #10, #11, #12, #13, #14, and #15) that include both ZR1 and ZR3 serving as rogue devices. The overall best rogue ZR1 and ZR3 detection results for these models at SNRν = 12 dB are presented in Figure 10 and include assessments for Model #11 with ZC2, ZC4, ZC5, ZC7, ZC8, ZC9, and ZC10 authorized devices. As estimated by averaging the individual ZRj:ZCi RRR indicated along Figures 10(a) and 10(b) x-axes, the average RRR performance across best case ZR1:ZCi is RRR = 99.31% and across all ZR3:ZCi is RRR = 99.98%; this best case cross-ZRj RRR was observed for a majority of models and ZRj:ZCi considered.

5. Conclusion

An analytic development of CB-DNA Fingerprinting for conventional QAM features is presented as well as its application to verification-based rogue detection demonstrated using ZigBee RZSUBSTICK communication devices. Results are
Figure 8: Rogue ID verification for (a) ZR4 and (b) ZR6 devices attacking Model #45 with ZC1, ZC3, ZC5, ZC7, ZC8, ZC9, and ZC10 network devices and contributing to poorest (minimum) RRR shown in Table 7 at SNR = 12 dB.

Figure 9: Overall poorest Rogue ID verification performance across 120 models for (a) ZR4 and (b) ZR6 with indicated network devices and contributing to poorest (minimum) RRR shown in Table 7 at SNR = 12 dB.

based on experimentally collected signals with postcollection fingerprint generation and authorized versus rogue device ID verification performed for 120 unique networks consisting of seven authorized and three unauthorized attacking rogue devices. Collective authorized device discrimination results for all 120 network configurations using an MDA classifier included (1) average cross-class percent correct classification of %C > 90% achieved for SNR ≥ 12 dB and (2) identification of device dependent verification thresholds yielding True Verification Rates (true positive) of TVR = 95% for all authorized network devices. The MDA network models were used for rogue device ID verification and Rogue Rejection Rate (RRR) (true negative) estimated for all rogues presented to the networks. Collective rogue device detection results for SNR ≥ 12 dB included (1) cumulative average burst-by-burst RRR = 94% across 2520 total rogue attack scenarios and (2)
performance across 252 attacks per individual devices spanning 83.32% < RRR < 99.81%. As a first successful proof-of-concept demonstration using CB-DNA Fingerprinting with conventional communication constellation features, these results are promising and further research is warranted.

Data Availability

The data used to support the findings is generally unavailable due to public releasability constraints. However, please contact the corresponding author for special release consideration.

Disclosure

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the Air Force Institute of Technology, the Department of the Air Force, the Department of Defense, or the US Government. This paper is approved for public release, Case#: 88ABW-2018-2040.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References


