1-2021

Extending Critical Infrastructure Element Longevity using Constellation-based ID Verification

Christopher M. Rondeau
Air Force Institute of Technology

Michael A. Temple
Air Force Institute of Technology

J. Addison Betances
Air Force Institute of Technology

Christine M. Schubert Kabban
Air Force Institute of Technology

Recommended Citation

Rondeau, C. M., Temple, M. A., Betances, J. A., & Schubert Kabban, C. M. (2021). Extending critical infrastructure element longevity using constellation-based ID verification. Computers & Security, 100, 102073. https://doi.org/10.1016/j.cose.2020.102073

Version of Record: https://www.sciencedirect.com/science/article/pii/S0167404820303461
Manuscript_483c1345454bc867b04526a5c6f1fb24

Title: Extending Critical Infrastructure Element Longevity Using Constellation-Based ID Verification

Christopher M. Rondeau, Michael A. Temple, J. Addison Betances, and Christine M. Schubert Kabban
School of Engineering and Management
Air Force Institute of Technology
Wright-Patterson AFB, USA
[christopher.rondeau; michael.temple*; joan.betancesjorge; christine.schubertkabban]@afit.edu
*Corresponding Author

Abstract: This work supports a technical cradle-to-grave protection strategy aimed at extending the useful lifespan of Critical Infrastructure (CI) elements. This is done by improving mid-life operational protection measures through integration of reliable physical (PHY) layer security mechanisms. The goal is to improve existing protection that is heavily reliant on higher-layer mechanisms that are commonly targeted by cyberattack. Relative to prior device ID discrimination works, results herein reinforce the exploitability of constellation-based PHY layer features and the ability for those features to be practically implemented to enhance CI security. Prior work is extended by formalizing a device ID verification process that enables rogue device detection demonstration under physical access attack conditions that include unauthorized devices mimicking bit-level credentials of authorized network devices. The work transitions from distance-based to probability-based measures of similarity derived from empirical Multivariate Normal Probability Density Function (MVNPDF) statistics of multiple discriminant analysis radio frequency fingerprint projections. Demonstration results for Constellation-Based Distinct Native Attribute (CB-DNA) fingerprinting of WirelessHART adapters from two manufacturers includes 1) average cross-class percent correct classification of $\%C > 90\%$ across 28 different networks comprised of six authorized devices, and 2) average rogue rejection rate of $83.4\% \leq \text{RRR} \leq 99.9\%$ based on two held-out devices serving as attacking rogue devices for each network (a total of 120 individual rogue attacks). Using the MVNPDF measure proved most effective and yielded nearly 12% RRR improvement over a Euclidean distance measure.

Keywords: classification, verification, rogue detection, critical infrastructure, CI, distinct native attribute, DNA, multiple discriminant analysis, MDA, WirelessHART

1.0 Introduction

Systems supporting Critical Infrastructure (CI) elements are becoming increasingly valuable targets for cyberattack. Coincident with the rise of the Industrial Internet of Things (IIoT), physical and cyberattacks on CI elements over the past 20 years have grown to include 1) attacks having merely incidental CI impact – such as occurred with the Maroochy Shire sewage spill (Sayfayn et al., 2017) and Slammer Worm disruption of nuclear monitoring at the Davis-Besse plant (Keefe, 2012), and 2) attacks against vulnerable CI elements – such as occurred with Stuxnet (Zetter, 2015; U.S. DHS, 2010), Shamoon (U.S. DHS, 2012), and CrashOverride (U.S. DHS, 2017). The CI threat space can be categorized relative to 1) the agent(s) perpetuating the attack, e.g., natural, technological, or human and 2) the threat category, e.g., natural, accidental, malicious (Nakamura et al., 2018). While threats in all categories can ultimately have catastrophic effects, protection architectures designed to address malicious threats generally include mechanisms that inherently protect against some accidental and natural threats as well. Thus, the approaches used to address the rise of CI-centric attacks are perhaps less motivated by the agent or threat category and more driven by an apparent divide between providing protection in higher open systems interconnection model layers (Rondeau et al., 2019) (e.g., data link layer and above) or the lowest physical (PHY) layer.

Regardless of where protection is implemented, the ultimate goal is to extend the longevity and useful lifespan of CI element electronics by increasing survivability amidst cyberattack. Apart from the cyber protection aspects, decades of development and demonstration activity have been completed (Bhatt et al., 2015) with a common goal of minimizing the potential for premature service termination and end-to-end lifecycle costs. As conceptually depicted in Fig. 1, the lifecycle of typical electronic items spans component manufacturing, component integration into end products, end product insertion into operations, operational service maintenance, and disposal at life's end. Although the figure depicts a "full" lifecycle spanning all stages, an item's useful life may actually never begin or it may be prematurely terminated for various reasons at any stage (indicated by the dashed bypass lines). Putting the reasons aside for a moment, 1) not all manufactured components pass final quality assurance and/or acceptance testing for end product integration; 2) not all end products meet requirements for a given operational application; and 3) not all operational items remain maintainable. Wilt various factors can contribute to a prematurely terminated useful life span, of most interest here are factors

resulting from adverse cyber activity. This nefarious activity can occur along the entire lifecycle chain and include 1) bug implantation (alterations, defects, etc.) early on, 2) real-time injection of bad (misdirecting, disruptive, etc.) information during operation, and/or 3) system alterations (hardware, firmware, etc.) made during routine or unscheduled maintenance.

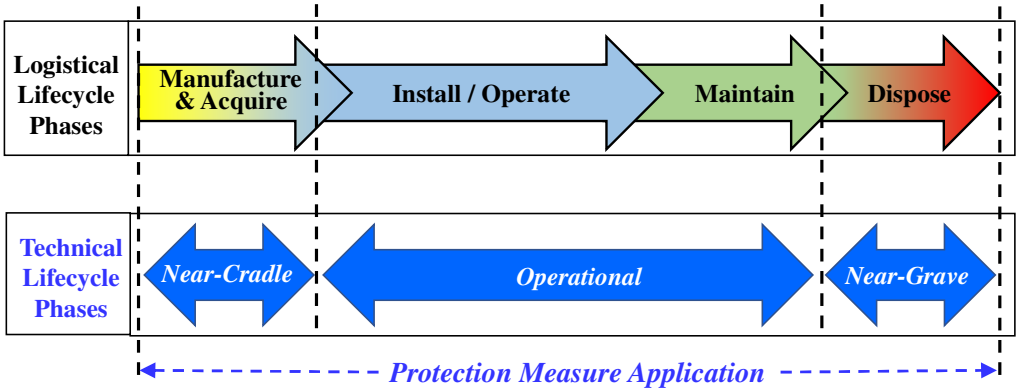


Fig. 1 – Representative logistical cradle-to-grave lifecycle concept derived from the Asset Management Model (IAM, 2015) aligned with the technical lifecycle phases that include near-cradle, operational and near-grave regions where protective measures are applied.

As with the *logistical* cradle-to-grave lifecycle management of elements depicted in Fig. 1 (IAM, 2015), there is a complementary *technical* cradle-to-grave protection approach supporting a common goal of extending element longevity and achieving "full" life expectancy. This includes minimizing the potential for premature termination (removal from service) resulting from adverse cyber activity. Radio Frequency (RF) based discrimination methods are among the capabilities supporting a technical cradle-to-grave protection strategy whereby security is addressed in 1) near-cradle activities of initial development, manufacture, and insertion activity (counterfeit component, device, etc., detection); 2) operational activities that include real-time monitoring (rogue, intrusion, etc., detection) and life sustaining maintenance (hardware, firmware, etc., upgrades), and 3) near-grave activities to identify and remove elements (defective, compromised, etc.) from service at life's end.

While there are many RF-based development and demonstration activities supporting a technical cradle-to-grave protection strategy, highlighting a few is sufficient for illustrating end-to-end community buy-in and the placement of this work among previous activities. At one lifecycle extreme are *near-cradle protection measures* that include using Radio Frequency ID (RFID) methods with onboard functionality embedded at the time of manufacture to 1) detect counterfeit ICs (recycled, cloned, etc.) prior to IIoT supply chain insertion (Yang et al., 2017), and 2) enable real-time encryption-based checking of host component status (normal, compromised, etc.) throughout the component's life (Leef, 2018). At the other lifecycle extreme are *near-grave protection measures* which are equally important for mitigating the inadvertent disclosure of sensitive information, technology, etc., that could be exploited by cyber criminals (Peng et al., 2019). Such exploitation may be achieved by scavenging through e-waste (an estimated 50 million tons worldwide (DSPO, 2016) that includes discarded items that have not been properly sanitized by 1) deleting, wiping, overwriting, etc., data stores, 2) resetting devices to factory defaults, and/or 3) destroying media, removable components, etc.– destroying the entire hardware device is arguably the best protective measure for avoiding compromise.

The heart of a cradle-to-grave protection strategy for ensuring that "full" life expectancy is achieved ultimately rests within the effectiveness of mid-life *operational protection measures* given the operational period represents a majority a device's lifecycle. This assumes the useful life hasn't been prematurely terminated due to hardware failure or adverse cyber activity causing protection mechanisms to become ineffective. While activity continues in operational life sustaining maintenance areas (firmware upgrade validation, etc.), the emphasis of work here is on security improvement in the real-time monitoring area. This protective monitoring collectively embodies higher-layer (bit-level) intrusion detection methods (Rondeau et al., 2019) and lowest PHY layer (waveform-level) methods. For CI cybersecurity in general, development of higher-layer methods have dominated with considerably less activity involving the lowest PHY layer. This imbalance is most evident by the wealth of "cross-layer" security works that emerge from a simple internet search – these works are perhaps be better categorized as "higher-cross-layer" works given the disproportionate number of PHY layer security works. Relative to CI applications, the noted lack of PHY layer feature exploitation is attributable in part to the inconsistent association between PHY layer vulnerabilities (Weiss, 2018; Wang et al., 2010) and observable abnormalities within higher-layer CI elements.

The emphasis here is on a PHY-based Radio Frequency Fingerprinting (RFF) approach for augmenting higher-layer protection mechanisms. This includes using unique, device dependent Distinct Native Attribute (DNA) features to provide reliable device identification (ID), with demonstrations addressing PHY layer vulnerability in the form of a physical access attack (Lopez et al., 2018). Such attacks may include supply chain tampering (counterfeiting, cloning, etc.), operational insider threat (authorized bad actor), and hardware/firmware manipulation that enables *rogue* devices to form unauthorized access points (Hua et al., 2018). These rogue devices mimic authorized device bit-level IDs to conduct so-called evil twin attacks (Shrivastava et al., 2020; Zhang et al., 2019). Detecting mimicked bit-level IDs is an important first step for defending against wireless rogue attacks and motivates the need for continued development and demonstration of reliable device discrimination methods – the objective of work presented here.

Of equal importance, it is desirable for the rogue detection method to be readily insertable as an operational protection measure with minimal complexity, costs, etc. Thus, the choice here for considering a Constellation-Based DNA (CB-DNA) device ID verification approach based on In-phase/Quadrature-phase (I/Q) signaling in the PHY layer. Wired and wireless I/Q signaling is among the communication methods used in CI applications Thus, successful demonstration here supports efficient (minimized cost, complexity, etc.) insertion of CB-DNA Fingerprinting into CI elements hosting *typical* I/Q-based communication processing and increases the potential for near-term community adoption. Applicability to other CI elements not using I/Q-based communication is addressed in Section 1.2.2. The generalized nature of the I/Q development herein also supports broader applicability to all other *M*-ary Quadrature Amplitude Modulation (*M*-QAM) and *M*-ary Quadrature Phase Shift Keyed (*M*-PSK) communication signaling schemes commonly used in other applications. The use of *M*-ary notation is common in communications and denotes the use of *M* available communication symbols (waveform shapes). One of the *M* symbols is transmitted in a given symbol time interval, with determination of which symbol based on the current information (bit values) to be transmitted. The projection of all *M* possible symbols into the two-dimensional I/Q space forms the communication signaling constellation.

1.1 Relationship to Prior Works

Two device discrimination categories are used to denote separate (yet related) functional processing actions, including: 1) *device classification* which involves a "looks most like" determination that is made relative to one of a given number of possible candidates, and 2) *device ID verification* which involves a "looks how much like" determination that is made relative to a specific claimed ID. The suitability of RFF-based device classification in common wireless applications (Bluetooth, WiFi, ZigBee, etc.) is duly noted in (Peng et al., 2019) which aptly compares related ZigBee RFF classification activity therein and works by numerous other researchers over the past decade. Given the thoroughness of (Peng et al., 2019) in presenting their Table II ZigBee summary, a compilation of historically related activities is not re-presented here for brevity.

For completeness, a comparative summary of this work and the two most related prior works (Peng et al., 2019; Rondeau et al., 2018a) is provided in Table 1. This includes selected technical elements that are either addressed (X) or not unaddressed (N/A). Relative to the other noted works, the table shows that this work represents 1) a transition from common ZigBee to CI-centric WirelessHART signals, while 2) addressing much needed development activity to improve rogue detection capability. To the best of the authors' knowledge, this work represents the first consideration of constellation-based feature extraction and RFF exploitation of CI-centric WirelessHART signals for the purpose of detecting rogue devices.

Table 1 – Comparison of selected technical elements that are addressed (X) or not addressed (N/A) in this work and the two most related prior works.

	Signal Type		**Measure of Similarity**		**Device Discrimination**		
	ZigBee	**Wireless HART**	**Distance Based**	**Probability Based**	**Device Classification**	**Device ID Verification**	**Rogue Detection**
This Work	N/A	X	X	X	X	X	X
(Rondeau et al., 2018a)	X	N/A	X	N/A	X	X	X
(Peng et al., 2019)	X	N/A	X	N/A	X	N/A	N/A

The work in (Peng et al., 2019) highlights the importance of user ID authentication which 1) is appropriately deemed as being essential in wireless applications for establishing user legitimacy, and 2) commonly implemented in higher non-PHY layers (e.g., IP, MAC, etc.) using bit-level credentials that are vulnerable to attack (Hua et al., 2018; Shrivastava et al., 2020; Zhang et al., 2014; Zhang et al., 2019). This inherent bit-level vulnerability provided the primary motivation for adopting PHY layer device ID verification principles from (Rondeau et al., 2018a) and extending the development for ZigBee-like WirelessHART demonstration. Device ID verification remains an important next step for achieving robust user authentication. Reliable authentication enables robust detection of *rogue* devices attempting to form unauthorized access points (Hua et al., 2018) by mimicking authorized bit-level identities (Rondeau et al., 2018a; Shrivastava et al., 2020).

While there are many similarity measures that can be used to characterize likeness, a Euclidean-based distance measure was used for device ID verification in (Rondeau et al., 2018a) as a matter of convenience. Variability can likewise be captured using a probabilistic approach whereby a histogram of measurements (test statistics) is used to form an empirical Probability Density Function (PDF) estimate for the measurements (López-Rubio, 2014). Considering probabilistic versus geometric distance measures to characterize similarity is certainly not new, with probability-based measures benefiting image retrieval (Aksoy et al., 2000), electron density pattern retrieval (Gopal et al., 2004), and network intrusion/anomaly detection (Weller-Fahy et al., 2015) applications. Results in (Gopal et al., 2004) highlight probabilistic measure superiority while (Weller-Fahy et al., 2015) addresses benefits of probability distance measures. The favorable Euclidean-based device ID verification results in (Rondeau et al., 2018a) are consistent with network intrusion detection performance in (Weller-Fahy et al., 2015) where a geometric-based distance measure reveals "clear differences between normal and attack conditions" – an objective of the rogue detection assessments being considered here. In light of the probabilistic measure benefits in (Aksoy et al., 2000; Gopal et al., 2004; Weller-Fahy et al., 2015), it was reasonable for the next development and demonstration steps here to consider a probabilistic Multivariate Normal Probability Density Function (MVNPDF) measure of similarity for both device classification and device ID verification.

The direct relevance of (Peng et al., 2019) is also evident in the authors' consideration of constellation-based features and presentation of independent (non-hybrid) classification performance along with best-case hybrid classification performance – the main contribution of (Peng et al., 2019). Presentation of non-hybrid results in (Peng et al., 2019) is most providential and highlights the information-bearing nature of constellation features, as done previously in (Rondeau et al., 2018a) and again here using constellation-based Distinct Native Attribute (DNA) features. Despite the dissimilarity in constellation-based feature generation methods, which generally prohibit a direct comparison of classification performance, the results presented in (Peng et al., 2019) and herein collectively reinforce the exploitability of constellation-based features for providing reliable discrimination. These works are complementary with no technical barriers that preclude 1) a probability-based measure of similarity (e.g., the MVNPDF used here) from being incorporated into classification processing of (Peng et al., 2019), or 2) the specific constellation-based features in (Peng et al., 2019) from being adopted into the device ID verification process demonstrated herein. The final decisions related to which measure of similarity, which constellation features, which discrimination processing, etc., to implement in the operational system will be driven by the system architecture to be augmented with protection.

Prior DNA fingerprinting developments have supported both pre-attack defense and post-attack forensic objectives, with a vision toward bolstering the cross-layer security paradigm. The previously investigated DNA techniques for protecting wireless sensor networks have included Time Domain DNA (TD-DNA) for WiFi (Reising et al., 2015) and home automation signals (Talbot et al., 2017), Wired Signal DNA (WS-DNA) for wired Highway Addressable Remote Transducer (HART) signals (Lopez et al., 2018) and Constellation-Based DNA (CB-DNA) for ZigBee signals (Rondeau et al., 2018a). All of these works have addressed device classification in their respective domains and rogue device detection using some form of device ID verification process with a distance-based measure of similarity.

1.2 Implications and Limitations

1.2.1 Network Protection Perspective

From a network protection perspective, demonstrations herein motivate further development of an envisioned DNA-based digital passport credentialing method supporting cross-layer security augmentation concepts in (Rondeau et al., 2019). The digital passport concept emerged from cybersecurity community member discussions at (Rondeau et al., 2018b). The DNA-based digital passport is symbolically denoted as $\mathbf{F}_P$ and would enable device ID verification when 1) initially requesting system access at a given node (similar to crossing country borders), and 2) throughout the course of operations on an as-requested basis (similar to the challenge posed when accessing

banking assets). The real-time generation and device ID verification would also enable fingerprint tracking and provide the ability to assess detected passport changes that may be normal (e.g., as may occur due to aging) or abnormal (e.g., as may occur due to cyberattack).

Relative to digital passport integrity during cyberattack and sustaining network connectivity, channel propagation (communication symbol reception) and information extraction (symbol-to-bit demodulation) must remain intact. A network becomes unreliable when the extracted information (user ID, synchronization, payload, etc.) becomes unavailable and/or unreliable. This can occur with 1) channel propagation degradation/failure (PHY-level), 2) parity check failure (bit-level), and/or 3) user ID credential compromise (bit-level). Of these factors, only channel propagation degradation/failure impacts DNA Fingerprinting performance which remains robust despite the increased bit-level degradation—the exploited DNA features are largely independent of the actual bit-level information being conveyed in the symbols. Degraded channel conditions yield lower processed Signal-to-Noise (SNR) for symbol demodulation and increase bit-level degradation (bit error rate, packet error rate, etc.). For these same degraded conditions, CB-DNA fingerprinting results in (Rondeau et al., 2018a) and Section 4.0 here show that $\%C > 90\%$ discrimination is maintained when SNR degrades by up to 30%. That is, the integrity of digital passport CB-DNA features is sufficiently maintained to provide desired discriminability and device ID verification.

DNA-based digital "passport" credentialing may be employed as illustrated in Fig. 2 to counter adverse operations activity resulting from 1) Remote Access Attacks (RAA) that include system processing and control elements acting upon an altered sensor state (i.e., a state different than the actual state being reported by the sensor) and causing the system to take inappropriate action, and 2) Physical Access Attacks (PAA) whereby the physical sensor device hardware, firmware, and/or software are altered and cause an errant sensor state to be reported (Rondeau et al., 2019). The related RAA and PAA operating spaces are shown in Fig. 2 along with potential the locations for digital $\mathbf{F}_P$ passport generation, augmentation, and usage (registration, verification, and tracking).

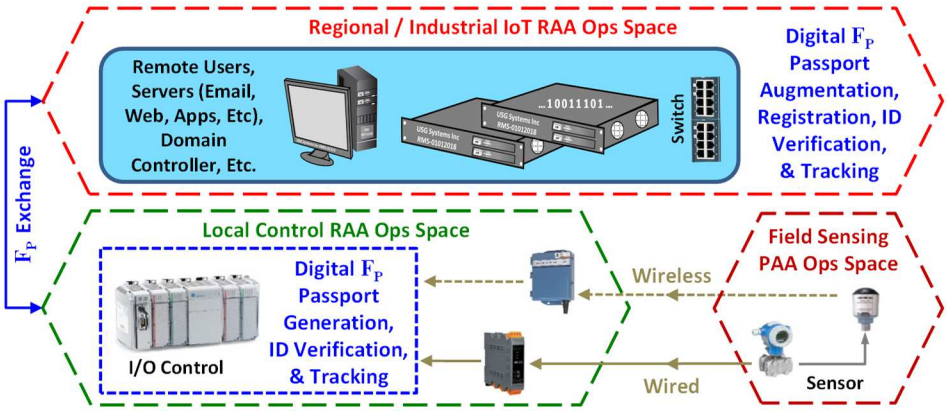


Fig. 2 – Illustration of digital DNA-based device passport $\mathbf{F}_P$ generation and employment within remote (RAA) and physical (PAA) attack spaces of a representative IIOT system using supervisory control and data acquisition components.

1.2.2 Technical Demonstration Perspective

From a technical demonstration perspective, any communication element in Fig. 2 (wired or wireless) that hosts *typical* I/Q-based processing is a target for efficient (minimized cost, complexity, etc.) insertion of the proposed CB-DNA fingerprinting. In addition, the CB-DNA development for the general two-dimensional (2D) I/Q signal constellation in Section 2.2.4 is 1) directly applicable to *all* M-QAM and M-PSK communication signaling, and 2) readily extendable to other M-ary signaling schemes where M communication symbols and/or their effects can be mapped 1:1 into a 2D space (so-called unconventional constellation). One proof-of-concept demonstration using an unconventional constellation has been completed and included the mapping of Manchester encoded binary symbols in unintentional 10BASE-T Ethernet cable emissions to reliably discriminate Ethernet cards (Carbino et al., 2015).

As with all similar emerging cybersecurity capabilities, and particularly the PHY-based approaches that have been greatly overshadowed by a myriad of higher layer activity, the proposed CB-DNA device ID verification method demonstrated herein is not without limitation(s). Historically, some DNA-based fingerprinting performance has been sensitive to varying propagation channel conditions in certain applications. This variation may be induced by relative transmitter-receiver motion (Doppler frequency shift), adverse atmospheric factors (amplitude fading), and alter constellation projection statistics. Results herein are most applicable under static (non-mobile) network

conditions which exist in some, but not all, IIoT architectures. The impact of mobile elements being present and resultant DNA fingerprinting performance remains to be determined.

Perhaps the most evident technical limitation is not based on wired versus wireless interconnectivity differences but rather on the specific communication modulation type(s) employed within the PHY layer. One specific modulation that remains to be addressed in the CB-DNA arena is Orthogonal Frequency Division Multiplexing (OFDM). OFDM is among the pool of modulations supporting 4G communications and is a fundamental technique in emerging 5G communications that are destined to become prevalent in IIoT applications. In 4G/5G OFDM systems, a selected number of individual sub-subcarriers (tens to hundreds of Fourier coefficients) are independently data modulated using complex I/Q values commonly obtained through *M*-QAM and/or *M*-PSK signaling. The data modulated coefficients are then inverse Fourier transformed to generate the transmitted time domain signal. Upon reception and Fourier transformation (inherently present in all OFDM-based receivers), the complex OFDM sub-carrier modulations are available in I/Q constellation space and are likely candidates for considering the same CB-DNA feature extraction method demonstrated herein for time-based modulations. Thus, the degree of hardware and/or software modifications required for implementing post-MODEM monitoring capability in emerging OFDM-based systems is conjectured as being consistent with modification requirements for the I/Q-based systems targeted here. Assessing the effectiveness of CB-DNA fingerprinting for OFDM-based systems remains of interest for future research activity.

1.2.3 Monitor Processing Perspective

From a processing requirement perspective, demonstrations here are sufficiently promising to warrant additional investigation into monitor integration aspects with a goal of realizing the efficient insertion objective noted in Section 1.2.2. This includes consideration for required processing capability and real-time ("in time") monitor response requirements that can vary widely across the CI arena. The extreme "in time" responses can range from what is required for personal safety and preserving human life applications (sub-second reaction) to preserving national economic security (reaction over days, months, etc.). This wide range of reaction times motivates the need for considering multiple system applications and required functionality that ranges from "monitor and act" when sub-second timing counts to "monitor and alert" when time permits. As with all developmental work, the applicability of methods demonstrated herein across the spectrum of monitor functional requirements remains to be determined. However, two related actions have been completed that provide preliminary insight at processing requirements and satisfying various "in time" requirements.

The first action included consideration of overall CB-DNA authentication algorithm complexity. The required monitor operations were quantified by analyzing three main components of the algorithm: 1) communication symbol cluster generation, 2) fingerprint generation, and 3) device classification. Once again, near-term insertion is aimed at hosting monitor capability in CI elements that have embedded functionality that includes communication symbol modulation/demodulation (MODEM) processing. The computational complexity is addressed in each of the algorithm component areas using Big-$O(N_q)$ notation (Kleinberg and Tardos, 2014).

1) Generation of the communication symbol clusters list can be accomplished in real-time as the different constellation points are estimated within the host system MODEM process and subsequently ingested by the monitor. Consequently, the monitor cluster generation process adds minimum complexity to symbol demodulation occurring within the host system MODEM. Thus, the CB-DNA algorithm is implemented through post-MODEM processing with communication symbol clusters generated by traversing the list once. This yields an overall complexity of $O(N_q)$ where N_q is the number of constellation points within the cluster.

2) The CB-DNA fingerprints used for demonstration are generated by computing statistics of variance, skewness, kurtosis, co-variance, co-skewness, and co-kurtosis for each communication symbol cluster. The computational complexity of fingerprint generation is bounded by $O(M*N_q)$ where M is the number of communication symbol clusters used. For the WirelessHART MODEM being considered here, with a) one cluster formed within each of the $M = 4$ constellation signaling quadrants, and b) the longest observed burst duration being $T_{Brst} \approx 2.57$ *m*Sec (approximately 2556 communication symbols), the number of constellation points per cluster is $N_q \approx 2556/4 = 639$ and the CB-DNA fingerprint generation algorithm is considered low complexity. Of all CB-DNA fingerprint features, calculation of co-kurtosis is the most computationally intense and contributes most to overall complexity. Thus, the complexity analysis for calculating co-kurtosis statistics is provided for illustration. Considering two random feature variables X and Y, the three non-trivial co-kurtosis ($\kappa\kappa$) statistics are obtained using (Miller, 2014),

$$\kappa\kappa_{X,X,X,Y} = \mathrm{E}[(X-\mu_X)^3(Y-\mu_Y)]/\left(\sigma_X^3\sigma_Y\right), \quad (1)$$

$$\kappa\kappa_{X,X,Y,Y} = \mathrm{E}[(X-\mu_X)^2(Y-\mu_Y)^2]/(\sigma_X^2\sigma_Y^2), \quad (2)$$

$$\kappa\kappa_{X,Y,Y,Y} = \mathrm{E}[(X-\mu_X)(Y-\mu_Y)^3]/\left(\sigma_X\,\sigma_Y^3\right), \quad (3)$$

where E[•] denotes the expected value operation, $\mu_X = \mathrm{E}[X]$ is the mean of X, $\mu_Y = \mathrm{E}[Y]$ is the mean of Y, $\sigma_X = \sqrt{\mathrm{E}[(X-\mu_X)^2]}$ is the standard deviation of X, and $\sigma_Y = \sqrt{\mathrm{E}[(Y-\mu_Y)^2]}$ is the standard deviation of Y. Thus, each of the co-kurtosis statistics in (1)-(3) requires mean value and standard deviation computations that are bounded by $O(N_q)$ operations. Accounting for M symbol clusters, the calculation of co-kurtosis fingerprint features yields an overall complexity of $O(M*N_q)$.

3) The major contributor to complexity in device ID verification is the projection of input fingerprint vector $\mathbf{F}_{1xN_F}$ (N_F total features) into an N_D-1 dimensional decision space where N_D is the number of devices represented in the model. This projection is done through multiplication of fingerprint vector $\mathbf{F}$ with classification projection matrix $\mathbf{W}_{N_F x N_{D-1}}$ and has complexity bounded by $O(N_F*N_{D-1})$. The projection operation is followed by measure of similarity calculation and comparative one-vs-N_{Cls} classification estimation which contributes minimally to overall projection complexity.

The second related action included a demonstration using ZigBee communication hardware and implementation of the three CB-DNA algorithm components in a C++ development environment (Matsui, 2020). Processing was performed on a workstation equipped with an Intel Xeon E5-2687W v3 processor having a 25 MB cache and operating a speed of 3.10 GHz. The end-to-end timing demonstration included 1) typical MODEM functional processing (burst reception, synchronization, symbol constellation point generation), and 2) post-MODEM CB-DNA fingerprinting functional processing (constellation point ingestion, cluster formation, fingerprint generation, fingerprint projection, and device classification). Post-MODEM process timing calculations for representative $T_{Brst} \approx 3.4$ *m*Sec ZigBee bursts (3392 communication symbols) included completion of all CB-DNA algorithm processing with a final classification decision being output an average of $T_{Cls} \approx 65$ μSec from the start of constellation point ingestion.

Given the experimental $T_{Cls} \approx 65$ μSec CB-DNA fingerprint generation and classification processing time, the motivation for CB-DNA-based monitoring is bolstered when considering additional ZigBee transmission constraints. For example, each burst transmission must be followed by a mandatory off-time that is dictated by the inter-frame spacing (IFS) (IEEE, 2011). The minimum standard IFS (transmission gap) for ZigBee corresponds to $T_{SIFS} = 192$ μSec (12 symbols) for short bursts and $T_{LIFS} = 640$ μSec (40 symbols) for long bursts (Neuhaeusler, 2016). Thus, the experimental $T_{Cls} \approx 65$ μSec is sufficiently fast regardless of the IFS employed to complete post-MODEM CB-DNA fingerprint processing during the IFS transmission gap. Alternately, the maximum supportable burst transmission update rate can be considered using $1/T_{Tot}$ where $T_{Tot} = T_{Brst} + T_{IFS}$. Considering $T_{Brst} \approx 3.4$ *m*Sec and the two possible IFS times, rates of 1/(3.4 *m*Sec + 192 μSec) ≈ 278 and 1/(3.4 *m*Sec + 640 μSec) ≈ 248 bursts-per-second are supportable. These clearly exceed the much lower update rate requirements for the ZigBee-like WirelessHART devices considered here. For example, when used in Supervisory Control And Data Acquisition applications the WirelessHART devices support controller directed query-sense-report cycles that at the fastest occur in 1 second intervals (Siemens, 2012, Pepperl+Fuchs, 2015). Collectively, the derived update rates based on experimental demonstration are sufficient to support some (perhaps all) envisioned functional requirements for both "monitor and act" and "monitor and alert" operations.

1.3 Paper Contributions

The motivation for adopting CB-DNA methods to discriminate WirelessHART devices includes 1) the complementary ZigBee device classification work in (Peng et al., 2019) that likewise exploits constellation-based features, and 2) the successful proof-of-concept ZigBee device ID verification (rogue detection) work in (Rondeau et al., 2018a). The concepts introduced in (Rondeau et al., 2018a) are formalized herein to address WirelessHART device discriminability. This includes demonstration activity using eight WirelessHART adapters (four like-model adapters from each of two different manufacturer sources) and supports the following paper contributions:

1) WirelessHART *device classification* using CB-DNA fingerprint features as an extension to prior ZigBee works given a) the successful use of constellation-based features in (Peng et al., 2019; Rondeau et al., 2018a) and b) the ZigBee-like nature of experimentally collected WirelessHART signals observed herein. Device classification results herein serve to reinforce exploitability and highlight the

information-bearing nature of constellation-based features while demonstrating the general extensibility of (Peng et al., 2019; Rondeau et al., 2018a) using an alternate CI-centric protocol.

2) WirelessHART *device ID verification* using CB-DNA fingerprint features as new development and demonstration activity. This includes *rogue* device assessments under conditions consistent with a physical access attack whereby an unauthorized device mimics authorized network device bit-level credentials (Hua et al., 2018; Shrivastava et al., 2020; Zhang et al., 2014; Zhang et al., 2019). Such assessments and conditions were not previously considered in (Peng et al., 2019) and the ZigBee rogue device detection work in (Rondeau et al., 2018a) was limited to a) concept introduction without formal development, and b) use of a Euclidean distance measure of similarity as a matter of convenience.

3) Introduction and use of a probability-based MVNPDF measure of similarity for *both* the device classification and device ID verification processes. This includes transitioning from distance-based measures as used in (Peng et al., 2019; Rondeau et al., 2018a) and adapting the MVNPDF measure to realize benefits noted in (Aksoy et al., 2000; Gopal et al., 2004; Weller-Fahy et al., 2015). Introducing the MVNPDF measure proved to be most effective for device ID verification, with nearly 12% improvement in rogue detection capability achieved relative using to a Euclidean distance measure.

1.4 Paper Organization

Following presentation of the Table 2 Summary of Acronyms and the Table 3 Summary of Notations in Table 3, the remainder of the paper includes Process Development in Section 2.0, Experimental Demonstration Methodology in Section 3.0, Discrimination Assessment Results in Section 4.0, and the Summary and Conclusions in Section 5.0.

Table 2 – Summary of Acronyms.

CB-DNA	Constellation Based DNA	PDF	Probability Density Function
CI	Critical Infrastructure	PHY	Physical
DNA	Distinct Native Attribute	PN	Pseudo-random Noise
FN	False Negative	PSD	Power Spectral Density
FP	False Positive	QAM	Quadrature Amplitude Modulation
HART	Highway Addressable Remote Transducer	QPSK	Quadrature Phase Shift Keyed
ID	Identification	OFDM	Orthogonal Frequency Division Multiplexing
IFS	*Inter*-frame spacing	RAA	Remote Access Attack
I/Q	In-Phase/Quadrature	RFF	Radio Frequency Fingerprinting
IIoT	Industrial Internet of Things	RRR	Rogue Rejection Rate
ISM	Industrial, Scientific, Medical	TP	True Positive
MDA	Multiple Discriminant Analysis	TD-DNA	Time Domain DNA
ML	Maximum Likelihood	TNG	Training
MVNPDF	Multivariate Normal PDF	TST	Testing
O-QPSK	Offset Quadrature Phase Shift Keyed	TVR	True Verification Rate
PAA	Physical Access Attack	WS-DNA	Wired Signal DNA

Table 3 – Summary of Notations.

A_{Ch}	Channel amplitude factor	N_{TNG}	Number of training fingerprints
β	Shaping window roll-off factor	N_{TST}	Number of testing fingerprints
$\mathbf{C}^{Sk}$	Constellation projection of $S_k(t)$	Q_{Sm}	Quadrature component of m^{th} symbol
Dj	j^{th} experimental device	ϕ_{Tx}	Transmitter hardware phase error
Dj:D$_k$	Device Dj claiming device D$_k$ ID	$\boldsymbol{O_I}(t)$	Complex in-phase offset factor
f_c	Carrier frequency	$\boldsymbol{O_Q}(t)$	Complex quadrature offset factor
f_S	Collection receiver I/Q sample frequency	$Q_{Rx}(t)$	Quadrature baseband signal
$\mathbf{F}^{Rgn}$	Regional fingerprint vector	$Q_{S_k}^{W}$	Windowed Q component of $S_k(t)$
$\mathbf{F}^{Stat}$	Statistic fingerprint vector	$S_{Rx}(t)$	Received communication signal
$\mathbf{F}_{\text{TD}}$	Composite TD-DNA fingerprint vector	τ_{Ch}	Channel propagation delay
$G_{I/Q}$	Constellation I/Q gain imbalance	T_{Brst}	Communication burst duration
I/Q	In-Phase/Quadrature-Phase	T_{Cls}	Experimental classification time
$I_{Rx}(t)$	In-phase baseband signal	T_{IFS}	Inter-frame spacing time
$I_{S_k}^{W}$	Windowed I component of $S_k(t)$	T_{LIFS}	Long burst inter-frame spacing time

I_{Sm}	In-phase component of m^{th} symbol
M	Number of communication symbols
N_{Cls}	Number of MDA classes
N_F	Number of fingerprint features
N_F^{CB}	Number of CB-DNA fingerprint features
N_F^{TD}	Number of TD-DNA fingerprint features
N_q	Number of quadrant constellation points
N_R	Number of fingerprinting sub-regions
N_{Rg}	Number of non-model rogue devices
N_S	Number of communication symbols

T_{SIFS}	Short burst inter-frame spacing time
T_{Sym}	Communication symbol duration
$S_k(t)$	k^{th} communication symbol
$S_{Rx}(t)$	Received communication signal
$S_{Tx}(t)$	Transmitted communication signal
$\mathbf{W}_{\text{Best}}$	Best MDA Projection Matrix
$W_{RC}(t)$	Raised cosine pulse shaping window
$W_{Rect}(t)$	Rectangular pulse shaping window
W_{RF}	Collection receiver RF bandwidth
$W_{HS}(t)$	Half sine pulse shaping window

2.0 Process Development

2.1 WirelessHART PHY Layer Signaling

The WirelessHART protocol supports a maximum data rate of 250 Kbits/Sec using (32,4) pre-modulation encoding that includes mapping of four process variable information bits to 1-of-16 32-bit orthogonal Pseudo-random Noise (PN) sequences (IEEE, 2011). Successive PN sequences are concatenated and modulated using O-QPSK signaling – a form of complex In-phase and Quadrature-phase (I/Q) signal modulation.

For completeness, a general development of I/Q signal modulation is presented. Considering M total communication symbols, the m^{th} I/Q symbol for $m = 1, 2, \ldots, M$ is given by,

$$S_m(t) = I_{S_m} + jQ_{S_m}, \qquad (4)$$

for $0 < t < T_{Sym}$ where T_{Sym} is symbol duration, I_{S_m} and Q_{S_m} are real-valued constants (I/Q constellation coordinates) over T_{Sym} with $I_{S_m} \in [I_{S_1}, I_{S_2}, \ldots, I_{S_M}]$ and $Q_{S_m} \in [Q_{S_1}, Q_{S_2}, \ldots, Q_{S_M}]$. Consecutive symbols from (4) form the transmitted signal given by,

$$S_{Tx}(t) = \left[\sum_{k=-\infty}^{\infty} S_m\left(t - kT_{Sym}\right)\right] e^{j(2\pi f_c t + \phi_{Tx})} \qquad (5)$$

where f_c is the carrier frequency and ϕ_{Tx} is transmitter hardware phase error (Zhuo et al, 2017). Accounting for channel A_{Ch} amplitude and τ_{Ch} propagation delay, the corresponding received signal $S_{Rx}(t)$ is given by,

$$S_{Rx}(t) = A_{Ch} S_{Tx}(t - \tau_{Ch}), \qquad (6)$$

which has baseband $I_{Rx}(t)$ and $Q_{Rx}(t)$ components of,

$$I_{Rx}(t) = G_{I/Q}\left[\sum_{k=-\infty}^{\infty} I_{S_k}(t - mT_S - \tau_{Ch})\right] + O_I(t), \qquad (7)$$

$$Q_{Rx}(t) = G_{I/Q}\left[\sum_{k=-\infty}^{\infty} Q_{S_k}(t - mT_S - \tau_{Ch})\right] + O_Q(t), \qquad (8)$$

where $\boldsymbol{G_{I/Q}}$ is I/Q gain imbalance, and $\boldsymbol{O_I(t)}$ and $\boldsymbol{O_Q(t)}$ represent I/Q offset factors (Zhuo et al, 2017).

The WirelessHART signal structure is illustrated in Fig. 3 which shows a representative collected burst amplitude response (top) and corresponding Power Spectral Density (PSD) (bottom). The illustrated ZigBee burst spans $T_{Brst} \approx 1.57$ *m*Sec and contains a total of $N_S \approx 1556$ modulated O-QPSK symbols ($N_q \approx 389$ symbols per I-Q quadrant). Experimentally observed bursts for both the Siemens and Pepperl+Fuchs devices included both 1) the shorter $T_{Brst} \approx 1.57$ *m*Sec duration shown in Fig. 3, and 2) a longer $T_{Brst} \approx 2.57$ *m*Sec duration containing $N_S \approx 2556$ modulated O-QPSK symbols ($N_q \approx 639$ symbols per I-Q quadrant). This variability is indicative of a variable PHY layer payload being employed by both manufacturers. The bottom PSD plot in Fig. 3 shows spectral characteristics that are consistent with a Channel #18 Industrial, Scientific, and Medical (ISM) band signal (IEEE, 2011) transmitted at a center frequency of $f_c = 2440$ MHz and occupying $W_{CH} \approx 2$ MHz of bandwidth (approximately 1 MHz of bandwidth on either side of f_c). The post-collection filter impulse response is shown overlaid on the PSD for reference. All WirelessHART SNR referred to in this paper were calculated at the output of this filter, i.e., in the $W_{CH} \approx 2$ MHz bandwidth.

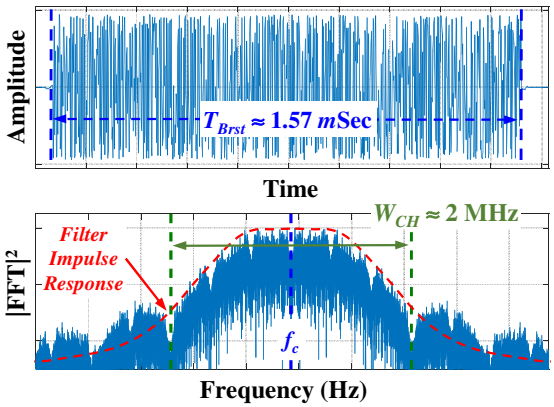


Fig. 3 – Representative WirelessHART burst amplitude response (top) and corresponding power spectral density (PSD) response (bottom) response for ISM Channel #18 burst. The post-collection filter impulse response is shown overlaid on the PSD for reference.

The historical DNA-based approaches to realize PHY layer benefit and boost cross-layer security potential have included TD-DNA (Reising et al., 2015; Talbot et al., 2017), WS-DNA (Lopez et al., 2018), and CB-DNA (Rondeau et al., 2018a) features. All of these works have performed device classification in their respective domains and addressed rogue detection using some form of device ID verification with distance-based measures of similarity. Relative to the noted TD-DNA works, benefits for adopting CB-DNA device ID verification concepts in (Rondeau et al., 2018a) and extending them here include decreased complexity for integrating required CB-DNA fingerprinting functionality into CI elements hosting *typical* communication signal processing, i.e., signal synchronization, constellation symbol mapping, demodulation, decoding, etc. A formal development of CB-DNA fingerprinting is presented in Section 2.2 that 1) provides generalization of CB-DNA fingerprinting from the specific O-QPSK modulation considered in (Rondeau et al., 2018a) to arbitrary I/Q signaling applications, while 2) highlighting the increased potential for near-term adoption and efficient integration into CI elements hosting *typical* communication signal I/Q processing.

2.2 Constellation-Based DNA Fingerprinting

2.2.1 Post-Collection Signal Processing

The CB-DNA fingerprinting concepts in (Rondeau et al., 2018a) are adopted here and generalized from the specific ZigBee O-QPSK modulation used therein to 1) support arbitrary I/Q signaling applications, 2) effectively exploit features extracted across the *full* WirelessHART burst duration, including the *variant* (data dependent) symbol regions, and 3) increase the potential for constellation-based fingerprinting methods to be efficiently integrated into operational CI elements hosting *typical* communication signal processing.

The adopted CB-DNA feature generation concepts are introduced in (Rondeau et al., 2018a) and based on an $S_{Rx}(t)$ structured similarly to that shown in (6)-(8). While (Rondeau et al., 2018a) specifically addresses O-QPSK modulation, the CB-DNA development herein is extended to include general applicability for arbitrary I/Q signaling applications. Consistent with communication system I/Q demodulation methods, the $S_{Rx}(t)$ receiver processing for CB-DNA generation includes burst-to-burst 1) carrier frequency estimation, 2) phase recovery and constellation derotation, and 3) timing synchronization via preamble correlation. This is followed by symbol-to-symbol processing that includes 1) locating the k^{th} symbol interval, i.e., $S_k(t) = I_{S_k}(t) + \mathrm{j}Q_{S_k}(t)$ in (6)-(8), 2) applying a given window $W(t)$ across $S_k(t)$, and 3) projecting the windowed $S_k^W(t)$ response into the I/Q constellation space as $\mathrm{C}^{S_k} = I_{S_k}^W + jQ_{S_k}^W$. At this point, the windowed $I_{S_k}^W$ and $Q_{S_k}^W$ constants include contributions from the non-ideal transmitter ($G_{I/Q}$, O_I, O_Q) and channel (A_{Ch}, τ_{Ch}) factors included in (6)-(8).

Consideration of pulse-shaping windows is motivated by common communication processing that uses pulse-shaping to minimize inter-symbol interference effects and improve symbol estimation. Reliable symbol estimation is not essential for effective fingerprinting but the effect of windowing on DNA discriminability is of interest. This includes assessing the potential for integrating CB-DNA fingerprinting into existing system architectures where constellation-space I/Q projection points ($\mathbf{C}^{S_k}$) are readily accessible.

2.2.2 Communication Signal Windowing

The three window types considered for demonstration are analytically expressed by (9)-(11) and include rectangular (W_{Rect}), half-sine (W_{HS}), and raised cosine (W_{RC}) shapes.

$$W_{Rect}(t) = \begin{cases} 1 & -T_{Sym}/2 < t < T_{Sym}/2 \\ 0 & Elsewhere \end{cases} \quad (9)$$

$$W_{HS}(t) = \begin{cases} sin\left(\frac{\pi}{T_{Sym}}t\right) & -T_{Sym}/2 < t < T_{Sym}/2 \\ 0 & Elsewhere \end{cases} \quad (10)$$

$$W_{RC}(t) = \begin{cases} \frac{cos[\beta\theta(t)]}{1-[2\beta\theta(t)/\pi]^2} \times \frac{sin[\theta(t)]}{\theta(t)} \\ \beta = 0.25\,, \theta(t) = \pi t/T_{Sym} \\ -5T_{Sym}/2 < t < 5T_{Sym}/2 \end{cases} \quad (11)$$

As indicated, the W_{Rect} of (9) and W_{HS} of (10) each span one T_{Sym} interval while W_{RC} of (11) spans a 5xT_{Sym} interval. The consideration of a raised cosine window spanning multiple T_{Sym} is consistent with requirements of the IEEE 802.15.4 standard governing WirelessHART operation (IEEE, 2011). The 5xT_{Sym} span and $\beta = 0.25$ roll-off factor for W_{RC} were empirically determined through qualitative visual comparison of an ideal preamble response with experimentally collected, windowed WirelessHART preamble responses.

Considering the ideal W_{Rect} in (9) (effectively no weighting) is consistent with a majority of prior related TD-DNA fingerprinting works that applied no windowing prior to feature extraction (Reising et al., 2015; Talbot et al., 2017). Thus, W_{Rect} is included here to enable a baseline comparison of TD-DNA and CB-DNA fingerprinting performances using a common window type. Considering the half-sine W_{HS} window type for ZigBee-like WirelessHART signals is motivated by prior ZigBee CB-DNA work (Rondeau et al., 2018a) that did include W_{HS} weighting based on operating standards (IEEE, 2011). Additional consideration of the raised cosine W_{RC} in (11) type is included here given its broad common usage in digital communications (Zoltowski, 2019) and expectations that some existing network elements to be augmented with PHY-based CB-DNA fingerprinting will include it.

2.2.3 TD-DNA Fingerprint Generation

As in (Lopez et al., 2018; Reising et al., 2015; Talbot et al., 2017), the centered-normalized (ctrd-nrm) instantaneous amplitude (AMP), phase (PHZ), and frequency (FRQ) responses of WirelessHART bursts were used for TD-DNA fingerprint generation. The plot in Fig. 4 shows overlaid instantaneous FRQ responses for the first $T_{Pre} \approx 160$ μSec preamble responses of 600 detected bursts from each of the eight adapters (four Siemens and four Pepperl+Fuchs). This includes 600x8 = 4,800 overlaid FRQ responses and clearly highlights the invariant *PreAmbRgn* response that is present in all bursts collected from all devices. TD-DNA fingerprints from this invariant region have been successfully used to discriminate various communication devices (Lopez et al., 2018; Reising et al., 2015; Talbot et al., 2017).

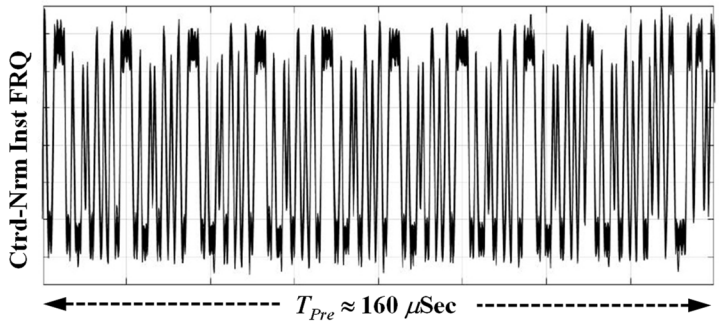


Fig. 4 – Overlay of 4,800 instantaneous frequency (FRQ) *PreAmbRgn* responses for 600 detected bursts from four each Siemens and Pepperl+Fuchs WirelessHART devices. The plot shows a $T_{Pre} \approx 160$ μSec span and clearly highlights the *invariant* cross-device *PreAmbRgn* response.

Time domain fingerprint features are extracted from instantaneous AMP, PHZ, and FRQ responses with three statistics of variance (σ^2), skewness (γ), and kurtosis (κ) calculated over the *PreAmbRgn* samples. The statistics are used to form statistic vector $\mathbf{F}^{Stat} = [\sigma^2\ \gamma\ \kappa]_{1\times 3}$ which is calculated over N_R contiguous, equal duration sub-regions spanning the *PreAmbRgn* ROI. All ROI samples are used for calculating additional features as well,

resulting in $\mathbf{F}^{Stat}$ vectors being formed for a total of $N_R + 1$ fingerprinting regions. The *Regional Statistic Vector* for each of the instantaneous AMP, PHZ, or FRQ responses is formed as,

$$\mathbf{F}^{Rgn} = \left[\mathbf{F}_{R_1}^{Stat} \vdots \mathbf{F}_{R_2}^{Stat} \vdots \cdots \vdots \mathbf{F}_{N_{R+1}}^{Stat}\right]_{1\times[3\times(N_R+1)]}. \qquad (12)$$

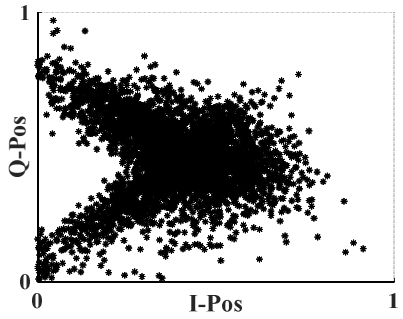
where the vertical ellipse ⋮ symbol is used herein to denote vector concatenation. Considering the selected *PreAmbRgn* ROI and formation of three $\mathbf{F}^{Rgn}$ vectors per (12) for each of the AMP, PHZ, and FRQ responses, the final *Composite TD-DNA Fingerprint Vector* $\mathbf{F}_{\text{TD}}$ is formed as,

$$\mathbf{F}_{\text{TD}} = \left[\mathbf{F}_{\text{AMP}}^{Rgn} \vdots \mathbf{F}_{\text{PHZ}}^{Rgn} \vdots \mathbf{F}_{\text{FRQ}}^{Rgn}\right]_{1\times N_F}. \qquad (13)$$

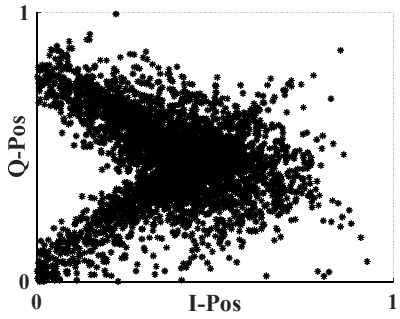
The N_F vector dimension in (13) is the total number of time domain fingerprint features and is calculated as $N_F = 3\text{x}3\text{x}(N_R + 1)$. A value of $N_R = 26$ was empirically determined to yield consistent classification performance using the indicated *PreAmbRgn* ROI in Fig. 4. Thus, the TD fingerprinting results in Section 4.1.1 are based on $\mathbf{F}_{\text{TD}}$ from (13) having $N_F^{TD} = 3\text{x}3\text{x}(26 + 1) = 243$ total features.

2.2.4 CB-DNA Fingerprint Generation

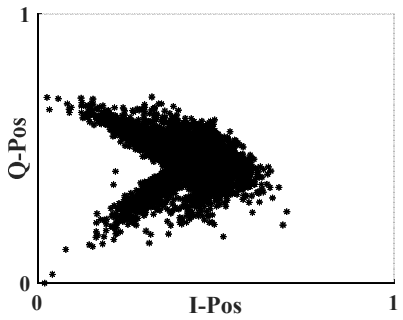
For each fingerprinted burst, the projected $\mathbf{C}^{S_k}$ are placed in a given quadrant sequence Q_q: $\{\mathbf{C}_q^{S_k}\}$ (q = 1, 2, 3, 4) based on the sign of $I_{S_k}^W$ and $Q_{S_k}^W$ components, yielding Q_1: $[+I_{S_k}^W, +Q_{S_k}^W]$, Q_2: $[-I_{S_k}^W, +Q_{S_k}^W]$, Q_3: $[-I_{S_k}^W, -Q_{S_k}^W]$, and Q_4: $[+I_{S_k}^W, -Q_{S_k}^W]$ quadrant designations. Variation of $\mathbf{C}_q^{S_k}$ projections within the quadrant sequences is illustrated in Fig. 5 which shows Q_1: $\{\mathbf{C}_1^{S_k}\}$ sequence elements for 20 collected bursts ($N_S \approx 2556$ total symbols) from selected Siemens AW210 and Pepperl+Fuchs Bullet adapters and the windows given in (9)-(11). These Q_1 quadrant responses are representative of other quadrant responses so plots showing Q_2, Q_3 and Q_4 variation are omitted for brevity. Of note is that the two specific devices represented in Fig. 5 projections were selected for illustration given they yielded the greatest cross-device visual dissimilarity of all device pairs. Despite this, the visual discriminability is minimal and poses a considerable discrimination challenge if using the $\{\mathbf{C}_1^{S_k}\}$ directly for classification and verification. Thus, statistical characteristics of $\{\mathbf{C}_1^{S_k}\}$ are used to form the CB-DNA fingerprints used for device discrimination assessments.



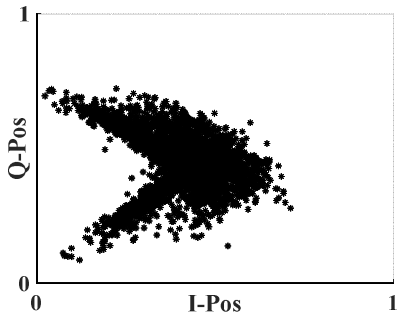
(a) AW210: W_{Rect}



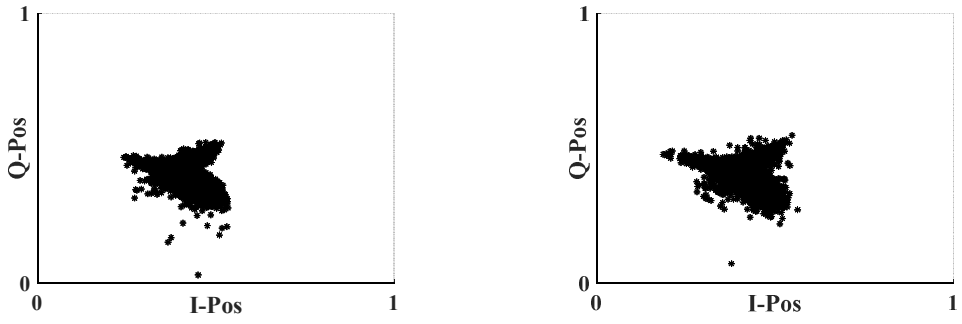
(d) Bullet: W_{Rect}



(b) AW210: W_{HS}



(e) Bullet: W_{HS}



(c) AW210: W_{RC} (f) Bullet: W_{RC}

Fig. 5 – Effect of ideal rectangular (W_{Rect}), half-sine (W_{HS}) and raised cosine (W_{RC}) windowing on quadrant $\mathbf{Q_1}$ projected $\{\mathbf{C_1^{S_k}}\}$ constellation points. Plots include symbol projections from 20 bursts for selected Siemens AW210 (a-c) and Pepperl+Fuchs Bullet (d-f) adapters under identical SNR conditions.

The CB-DNA fingerprint vectors $\mathbf{F}_{\mathrm{CB}}$ were generated using each of the Q_q: $\{\mathbf{C}_q^{S_k}\}$ sequences and processing methods adopted from (Rondeau et al., 2018a). Some development is provided here for completeness using an arbitrary Q_q sequence having N_q total elements. Fingerprint statistics were calculated for 1) *polar* magnitude $\left(\text{denoted as } |Q_q|\right)$ and angle $\left(\text{denoted as } \overline{Q_q}\right)$, and 2) *rectangular* real ($Re\{\mathrm{Q}_q\}$) and imaginary ($Im\{\mathrm{Q}_q\}$) components of complex Q_q elements. The statistical CB-DNA features extracted from *polar* components included variance (σ^2), skewness (γ) and kurtosis (κ) of both the magnitude $\{|Q_q|\}$ and angle $\{\overline{Q_q}\}$ sequences (a total of four polar statistics). Twelve additional features were calculated by forming the $1\text{x}N_q$ matrix $[Re\{\mathrm{Q}_q\}: Im\{\mathrm{Q}_q\}]$ and calculating statistics of co-variance $\sigma^2\sigma^2$ (three unique statistics), co-skewness moments $\gamma\gamma$ (four non-trivial statistics) and co-kurtosis moments $\kappa\kappa$ (five non-trivial statistics) (Miller, 2014).

Accounting for all the noted statistics, the Q_q: $\{\mathbf{C}_q^{S_k}\}$ *Quadrant Fingerprint Vector* is formed as,

$$\mathbf{F}^{Q_q} = \left[\mathbf{F}_{Polar}^{Q_q} \vdots \mathbf{F}_{Rect}^{Q_q}\right]_{1\times 18}, \tag{14}$$

$$\mathbf{F}_{Polar}^{Q_q} = \left[\sigma^2_{|Q_q|}\ \gamma_{|Q_q|}\ \kappa_{|Q_q|}\ \sigma^2_{\overline{Q_q}}\ \gamma_{\overline{Q_q}}\ \kappa_{\overline{Q_q}}\right], \tag{15}$$

$$\mathbf{F}_{Rect}^{Q_q} = \left[\sigma\sigma^2_{Q_q}\ \gamma\gamma_{Q_q}\ \kappa\kappa_{Q_q}\right]. \tag{16}$$

Considering all four Q_q: $\{\mathbf{C}_q^{S_k}\}$ sequences (q = 1, 2, 3, 4), the quadrant vectors from (14)-(16) are used to form the final *Composite CB-DNA Fingerprint Vector* $\mathbf{F}_{\mathrm{CB}}$ as,

$$\mathbf{F}_{\mathrm{CB}} = [\mathbf{F}^{Q_1} \vdots \mathbf{F}^{Q_2} \vdots \mathbf{F}^{Q_3} \vdots \mathbf{F}^{Q_4}]_{1\times 72}, \tag{17}$$

which shows that full-dimensional CB-DNA fingerprints contain $N_F^{CB} = 72$ features.

2.3 Device Discrimination

Device discrimination includes both 1) *device classification* as a "looks most like" determination that is made relative to one of a given number of possible candidates, and 2) *device ID verification* as a "looks how much like" determination that is made relative to a single claimed ID. These two are related in that a single Multiple Discriminant Analysis (MDA) model is first trained and its performance validated using Maximum Likelihood (ML) device classification. The validated MDA model is then used to perform device ID verification of both authorized (modelled) devices claiming their legitimate IDs, and rogue (non-modelled) devices mimicking the ID for one of the authorized devices. Device classification and device ID verification assessments are made using independent *training* (N_{TNG} per class) and *testing* (N_{TST} per class) fingerprints. These are selected from the pool of 1) TD-DNA $\mathbf{F}_{\mathrm{TD}}$ fingerprints generated per (13) in Section 2.2.3 using the W_{Rect} window in (9), and 2) CB-DNA $\mathbf{F}_{\mathrm{CB}}$ fingerprints generated per (17) in Section 2.2.4 using all three window types in (9)-(11). Of particular importance in making the fingerprinting performance comparison in Section 4.1.1 is that the pools of $\mathbf{F}_{\mathrm{TD}}$ and $\mathbf{F}_{\mathrm{CB}}$ fingerprints are generated from the *same* experimentally collected signals.

2.3.1 Device Classification

MDA performs multi-class (N_{Cls} > 2) linear discrimination using N_{TNG} input training fingerprints per class, i.e., the $1\text{x}N_F$ dimensional time domain $\mathbf{F}_{\mathrm{TD}}$ from (13) and constellation-based $\mathbf{F}_{\mathrm{CB}}$ from (17). For the development here,

each class is associated one-to-one with a modeled authorized device D_k (k =1, 2, …, N_D) where N_D is the number of authorized network devices. MDA training yields an N_FxN_D-1 dimensional matrix $\mathbf{W}$ that projects the N_{TNG} fingerprints into an N_D-1 decision space while maximizing cross-class (cross-device) projected mean separation distance and minimizing within-class (cross-device) projected spread (Duda et al., 2001). A cross-validation process is implemented using K = 5-folds to improve model training rigor (Hastie et al., 2001), with $\mathbf{W}_{\text{Best}}$ selected based on the "best" performing fold validation results.

Additional MDA training outputs that are required for subsequent device classification and device ID verification include input fingerprint mean $\boldsymbol{\mu}_{\mathbf{F}}$ (1xN_F) and standard deviation $\boldsymbol{\sigma}_{\mathbf{F}}$ (1xN_F) normalization factors, projected training class means $\boldsymbol{\mu}_k$ (1xN_D-1), and projected training class covariance $\boldsymbol{\Sigma}_k$ (N_D-1xN_D-1). The ($\mathbf{W}_{\text{Best}}$, $\boldsymbol{\mu}_{\mathbf{F}}$, $\boldsymbol{\sigma}_{\mathbf{F}}$, $\boldsymbol{\mu}_k$, $\boldsymbol{\Sigma}_k$) notation is used herein to denote a trained MDA model for k = 1, 2, …, N_D model classes.
The trained MDA model is validated using a ML classification process and N_{TST} fingerprints per class/device. Classification decisions are based on assuming that 1) input fingerprints are normally distributed such that their projection by $\mathbf{W}_{\text{Best}}$ is likewise normally distributed, and 2) Bayesian conditions of equal *a priori* probabilities for all classes and equal costs in making classification errors. Under the first assumption, the *a posteriori* likelihood for projection vector $\mathbf{p}_j = \left[\left(\mathbf{F}_j - \boldsymbol{\mu}_{\mathbf{F}}\right) \odot \boldsymbol{\sigma}_{\mathbf{F}}^{-\mathbf{1}}\right]\mathbf{W}_{\text{Best}}$ (1xN_D-1) of all training fingerprints $\mathbf{F}_j$ (j = 1, 2, …, N_{TNG}) from the k^{th} class (k = 1, 2, …, N_D), where $\odot$ denotes Hadamard product, can be represented as a MVNPDF given by,

$$f_{\mathbf{P}_k}(p_1, \ldots, p_{N_D-1}) = \exp\left[\mathrm{g}\left(\mathbf{p}_j, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k\right)\right] / \mathrm{h}(\boldsymbol{\Sigma}_k), \qquad (18)$$

$$\mathrm{g}\left(\mathbf{p}_j, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k\right) = -\frac{1}{2}\left(\mathbf{p}_j - \boldsymbol{\mu}_k\right)^{\mathrm{T}} \boldsymbol{\Sigma}_{\boldsymbol{k}}^{-\mathbf{1}} \left(\mathbf{p}_j - \boldsymbol{\mu}_k\right), \qquad (19)$$

$$\mathrm{h}(\boldsymbol{\Sigma}_k) = \sqrt{(2\pi)^{N_D-1}|\boldsymbol{\Sigma}_k|}, \qquad (20)$$

where $\boldsymbol{\mu}_k$ and $\boldsymbol{\Sigma}_k$ are the k^{th} class training mean and covariance. For each *unknown* testing fingerprint ($\mathbf{F}_{\mathrm{U}}$) to be classified, the classification process includes calculating projection $\mathbf{p}_{\mathrm{U}} = \left[\left(\mathbf{F}_{\mathrm{U}} - \boldsymbol{\mu}_k\right) \odot \boldsymbol{\sigma}_k^{-\mathbf{1}}\right]\mathbf{W}_{\text{Best}}$, inputting $\mathbf{p}_{\mathrm{U}}$ into (18)-(20), and calculating $f_{\mathbf{P}_k}(\mathbf{p}_{\mathrm{U}})$ for all k = 1, 2, …, N_D. The unknown $\mathbf{F}_{\mathrm{U}}$ is then estimated (rightly or wrongly) as coming from device D_k according to,

$$\widehat{\mathrm{D}}_k : \underset{k}{\arg\max}\left[f_{\mathbf{P}_k}(\mathbf{p}_{\mathrm{U}})\right] \qquad (21)$$

where the estimated $\widehat{\mathrm{D}}_k$ corresponds to the training class producing $\mathbf{p}_{\mathrm{U}}$ with higher likelihood.

For MDA/ML classification, the held-out N_{TST} testing fingerprints for each model class D_k are input and class (device) estimates made using (21). The multi-class classification results are presented in an input-vs-estimated (true-vs-predicted) multi-class confusion matrix (Tharwat, 2020). The particular row-column format of confusion matrices presented herein include 1) each row representing one of the true class D_k inputs for k = 1, 2, …, N_{Cls}, and 2) columns in each row corresponding to estimates (predictions) $\widehat{\mathrm{D}}_j$ of D_k for j = 1, 2, …, N_{Cls}. Thus, correct decisions ($\widehat{\mathrm{D}}_k = \mathrm{D}_k$) fall along the matrix diagonal and incorrect decisions ($\widehat{\mathrm{D}}_l = \mathrm{D}_k, l \neq k$) are in off-diagonal locations. Overall *cross-class percent correct classification* (*%C*) is calculated as the sum of diagonal matrix elements divided by $N_{TST} \times N_{Cls}$ and multiplied by 100. Given that the classification decisions represent independent Monte Carlo trials, 95% Confidence Interval ($CI_{95\%}$) analysis (Park et al., 2019) is used for comparative (best, same, different, etc.) assessments.

Using the generally less rigorous *%C* metric is consistent with previous DNA works (Lopez et al., 2018; Reising et al., 2015; Talbot et al., 2017) and is motivated by a desire to enhance broader, cross-discipline appreciation for the work. The *%C* assessments are augmented here using a generally more rigorous approach based on True Positive (TP), False Positive (FP) (also called a Type I error), and False Negative (FN) (also called a Type II error) metrics commonly used in hypothesis testing (Tharwat, 2020). Hypothesis testing here includes a given device (authorized or rogue) presenting an ID (actual or mimicked) for a given authorized network device. Thus, a *true positive* test includes an authorized device presenting its own ID and being *correctly* verified as authorized and *granted* network access. A *false positive* Type I error includes a presented rogue device ID being *errantly* verified as authorized and the device being *granted* network access. A *false negative* Type II error includes an authorized device presenting its own ID and being *errantly* verified and *denied* network access.

The hypothesis testing metrics are generated from confusion matrix results and used to calculate the *Precision* and *Recall* measures given in (22) and (23), respectively (James et al., 2017; Tharwat, 2020). Of particular note is that the confusion matrix *%C* equals the average of all individual per-class recall measurements.

$$Precision = \frac{TP}{TP + FP} \qquad (22)$$

$$Recall = \frac{TP}{TP + FN} \quad (23)$$

2.3.2 Device ID Verification

Device ID verification is performed with the trained MDA model ($\mathbf{W}_{\text{Best}}$, $\boldsymbol{\mu}_{\mathbf{F}}$, $\boldsymbol{\sigma}_{\mathbf{F}}$, $\boldsymbol{\mu}_k$, $\boldsymbol{\Sigma}_k$) from Section 2.3.1 using 1) testing fingerprints from an "unknown" device (D_j), and 2) a claimed ID (D_k for $k = 1, 2, \ldots, N_D$) for one of the authorized model devices. The verification process enables assessment of both 1) *authorized device ID verification* when D_j is one the trained model devices, and 2) *rogue device ID verification* when D_j is not a trained model device. Verification assessments involving actual:claimed device IDs are denoted as D_j:D_k. As with device classification in Section 2.3.1, testing fingerprint $\mathbf{F}_j$ from device D_j is projected as $\mathbf{p}_j = \left[\left(\mathbf{F}_j - \boldsymbol{\mu}_{\mathbf{F}}\right) \odot \boldsymbol{\sigma}_{\mathbf{F}}^{-1}\right] \mathbf{W}_{\text{Best}}$ into the decision space and a verification test statistic Z_{V}^{j} (measure of similarity) generated to reflect how much $\mathbf{p}_j$ "looks like" training fingerprint projections of the claimed D_k device.

While various distance-based and probability-based measures of similarity may be used for the verification test statistic Z_{V}, in light of the benefits detailed in (Aksoy et al., 2000; Gopal et al., 2004; Weller-Fahy et al., 2015) a multivariate normal distribution is assumed here for the pool of $\mathbf{p}_m$ ($m = 1, 2, \ldots, N_{TNG}$) projections from claimed device D_k training fingerprints. Assuming this is the case for all N_D devices represented in the model, the MVNPDF in (18)-(20) may be used to represent all modeled D_k projections ($k = 1, 2, \ldots, N_D$) using $\boldsymbol{\mu}_k$ (1xN_D-1) and $\boldsymbol{\Sigma}_k$ (N_D-1xN_D-1) as the k^{th} class MDA training mean and covariance. Therefore, the desired verification test statistic Z_{V}^{m} for the m^{th} testing fingerprint $\mathbf{F}_j^m$ from "unknown" device D_j is calculated using $\mathbf{p}_j = \left[\left(\mathbf{F}_j - \boldsymbol{\mu}_{\mathbf{F}}\right) \odot \boldsymbol{\sigma}_{\mathbf{F}}^{-1}\right] \mathbf{W}_{\text{Best}}$ in (18)-(20) and setting $Z_{\text{V}}^{m} = f_{\mathbf{P}_k}\left(\mathbf{p}_j^m\right)$ for the k^{th} claimed D_k device.

This device ID verification process is used here for three specific assessments, including estimation of 1) *True Verification Rate* (TVR) for authorized device ID *training*, 2) TVR for authorized device ID *testing*, and 3) *Rogue Rejection Rate* (RRR) for rogue device ID *testing* verification. As a first required step, authorized device ID *training* verification is performed to establish the device dependent thresholds, denoted as $t_V(k)$ for $k = 1, 2, \ldots, N_D$, required for subsequent verification assessments. Each $t_V(k)$ threshold is established using the pool of Z_{V}^{m} values ($m = 1, 2, \ldots, N_{TNG}$) obtained from $\mathbf{p}_m$ projections of the k^{th} modeled class *training* fingerprints. The value of $t_V(k)$ is set to achieve a desired TVR which is calculated as the number of $Z_{\text{V}}^{m} > t_{\text{V}}(k)$ divided by N_{TNG} for a higher-is-better metric (e.g. MVNPDF) or as the number of $Z_{\text{V}}^{m} < t_{\text{V}}(k)$ divided by N_{TNG} for a lower-is-better metric (e.g., Euclidean distance).

The threshold setting process is illustrated in Fig. 6 for a representative ($\mathbf{W}_{\text{Best}}$, $\boldsymbol{\mu}_{\mathbf{F}}$, $\boldsymbol{\sigma}_{\mathbf{F}}$, $\boldsymbol{\mu}_k$, $\boldsymbol{\Sigma}_k$) model and higher-is-better metric. The plot shows all Z_{V}^{m} plotted for authorized device ID training verification (D_A-TNG) and the corresponding Device A threshold value of $t_V = 0.326$ required to obtain training TVR ≈ 90% (the percentage indicated below the D_A-TNG label). The colored marker convention used in Fig. 6 and results presented in Section 4.0 includes blue **O** and red **X** markers denoting desired (positive) and undesired (negative) outcomes, respectively. The remaining device ID verification results illustrated in Fig. 6 (D_A-TST, R1:D_A, R2:D_A) are obtained using the *same* training $t_V = 0.326$ threshold value. Authorized device ID *testing* verification (D_A-TST) is performed using the pool of Z_{V}^{m} values ($m = 1, 2, \ldots, N_{TST}$) obtained from $\mathbf{p}_m$ projections of the k^{th} modeled class *testing* fingerprints. The resultant D_A-TST Z_{V}^{m} values are plotted in Fig. 6, with application of $Z_{\text{V}}^{m} > t_{\text{V}} = 0.326$ accept criteria (accept that the claimed ID is the actual ID) yielding authorized D_A-TST TVR ≈ 88.5%.

The remaining two illustrations in Fig. 6 are for rogue ID *testing* verification (R1:D_A, R2:D_A) and are indicative of two non-modeled rogue devices (R1 and R2) presenting a false claimed ID matching the modeled authorized Device A. For these assessments the $t_V = 0.326$ training threshold is once again maintained and $Z_{\text{V}}^{m} > t_{\text{V}}$ accept criteria applied to yield the indicated R1:D_A and R2:D_A performances of RRR ≈ 97.5% and RRR ≈ 99.7%, respectively. Note that the colored marking of R1:D_A and R2:D_A test statistics in Fig. 6 have been changed to maintain the blue **O** (desired) and red **X** (undesired) outcome convention.

3.0 Experimental Demonstration Methodology

3.1 WirelessHART Hardware Devices

As shown in Table 4 and denoted as D_1-D_8 for experimentation, there were a total of eight WirelessHART adapters used for demonstration, including three Siemens Sitrans AW210 (Siemens, 2012) and three Pepperl+Fuchs Bullet (Pepperl+Fuchs, 2015) devices. Apart from having different serial numbers and some firmware differences, these are functionally equivalent, 802.15.4 standard compliant devices (IEEE, 2011) that are one-to-one interchangeable. These devices transmit operating status payload information that includes 1) the 4-20 mA current loop *primary variable* value for the process being monitored and controlled, 2) the input power source voltage *secondary variable* value, and 3) the internal device temperature *tertiary variable* value.

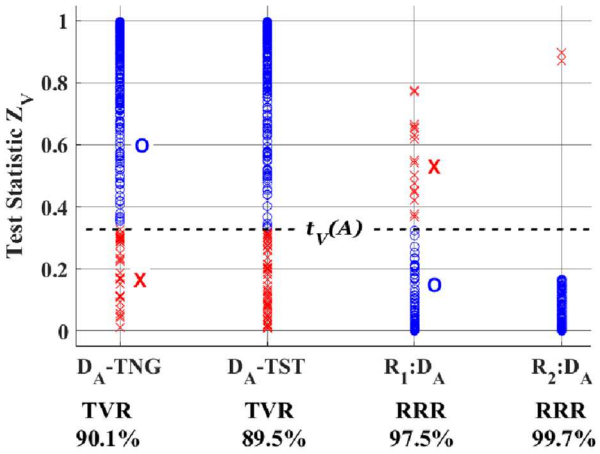


Fig. 6 – Device ID verification illustration showing test statistics for (a) authorized Device A ID training (D_A-TNG), (b) authorized Device A ID testing (D_A-TST), and (c) rogue device ID verification for two rogue devices (R1:D_A, R2:D_A). The indicated t_V verification threshold is set for authorized Device A to achieve TVR ≈ 90% for D_A-TNG, and remains *fixed* for other verification assessments that yield the indicated TVR (D_A-TST) and RRR (R1:D_A, R2:D_A) percentages along the x-axis.

Table 4 – Details for WirlessHART Hardware Adapters.

Device ID	Manu	Model	Serial No.	Manu Date	Firmware ID
D_1	Siemens	Sitrans AW210	003095	1/1/2009	198
D_2			003159	1/1/2009	200
D_3			003097	1/1/2009	198
D_4			003150	1/1/2009	200
D_5	Pepperl+ Fuchs	Bullet	1A32DA	10/16/2018	200
D_6			1A32B3	10/16/2018	200
D_7			1A3226	10/16/2018	200
D_8			1A32A4	10/16/2018	200

3.2 WirelessHART Signal Collection

The experimental signal collection setup in Fig. 7 was used to collect signals from all WirelessHART devices listed in Table 4. As shown, the main experimental demonstration components included the WirelessHART adapters under evaluation, a National Instruments 2952R Software Defined Radio (SDR) (NI, 2016) used for signal collection, and a networked Emerson 1410 WirelessHART gateway. The WirelessHART adapters were powered by an external 5.0 volt power source, with separation distances between the WirelessHART adapters, SDR collection receiver, and Emerson gateway set to ensure network communication connectivity and achieve collected SNR conditions of SNR ≈ 30 dB. Component gains and attenuation in the SDR collection receiver were set to ensure there was no amplitude clipping of collected burst responses. The electromagnetic background was consistent with a typical office environment and included other industrial, scientific, and medical (ISM) band devices operating.

The primary process variable input to the WirelessHART devices was held constant, i.e., the 4-20 mA input current level was set using a test fixture to simulate a "0" value state. Thus, the transmitted burst payloads were controlled such that any variation occurring during signal collection could be directly attributed to change in the secondary supply voltage variable and/or the tertiary internal temperature variable. Emerson 475 Communicator and Emerson 1410 gateway monitoring allowed for real-time confirmation that the WirelessHART adapters were operating properly.

3.2.1 Collection Receiver Configuration.

The National Instruments 2952R SDR was used for making all WirelessHART collections. It was configured with an Ettus SBX 5.1 daughter card (Ettus, 2019) and controlled by a laptop computer running Ubuntu 16.04 and the open-source GNU Radio Companion. The SDR was set to operate at an I/Q sample rate of f_S = 10 MSps in both the I and Q channels using an RF input collection bandwidth of W_{RF} = 10 MHz. The complex I/Q samples were recorded and stored for subsequent post-collection processing and DNA fingerprinting.

3.2.2 WirelessHART Network Configuration.

The experimental collection setup embodies typical elements of a feedback control network that may include 1) a process to be monitored and/or controlled (i.e., real-world physical phenomenon), 2) a process measurement or sensing device, 3) element-to-element communications (WirelessHART here), and 4) a network gateway for receiving and displaying information to facilitate operational monitoring. WirelessHART network operation, adapter functionality, and reported adapter values were monitored via an Emerson 1410 gateway controlled through a laptop computer.

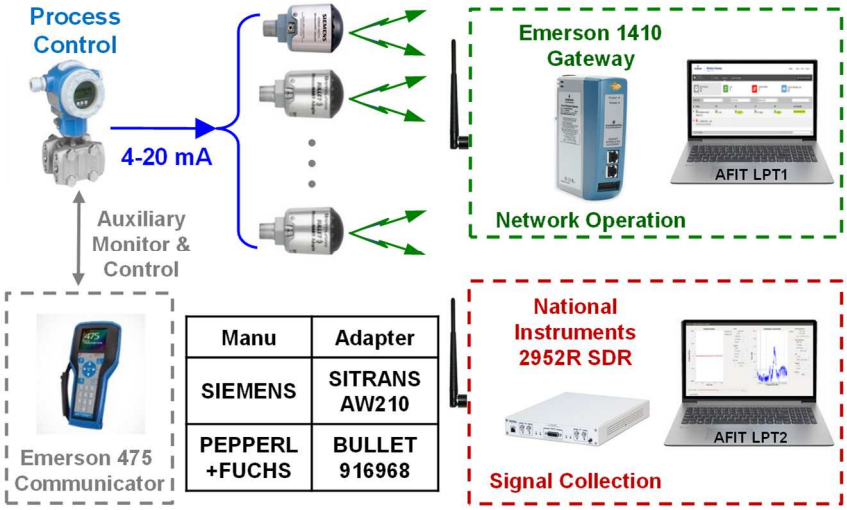


Fig. 7 – Experimental collection setup for WirelessHART signal collection showing the adapters, Emerson 1410 network gateway interface, and NI 5952R SDR collection receiver.

The experimental design included making collections using a random ordering of devices listed in Table 4. This randomization was incorporated to reduce the effects of unknown or unrealized experimental biases. Initial signal collections were accomplished over a continuous period of 110 minutes per device. A sufficient number of supplemental 30 minute collections were performed to ensure a minimum of 1000 independent bursts per device were available for subsequent DNA fingerprinting assessments. Additional randomization was inherently present in that *only* the WirelessHART signals being transmitted in Channel #18 of the ISM band (see Fig. 3 for PSD spectral characteristics) were collected and processed. Single channel fingerprinting was motivated by the desire to maintain experimental repeatability and Emerson 1410 gateway firmware constraints that require a minimum of nine ISM channels be used. Thus, the network was configured to use ISM Channels #14–#22 with the WirelessHART devices transmitting pseudo-randomly across all nine channels on a burst-by-burst basis.

3.3 WirelessHART Device Discrimination

MDA-based device discrimination was performed for 1) an $N_{Cls} = 8$ class model (all D_1-D_8 devices listed in Table 4 serving as authorized devices), and 2) a total of N_M = 8-choose-6 = 28 distinct $N_{Cls} = 6$ network models with devices assigned authorized (A) and held-out rogue (R) roles according to Table 5. Of necessity for completing the desired rogue rejection assessments, the MDA models were first generated and ML device classification performance validated using a MVNPDF measure of similarity per details provided in Section 2.3.1. Results for multi-model device classification performance are presented in Section 4.2.

Table 5 – Device assignments used for $N_M = 28$ models showing Authorized (A) and held-out Rogue (R) devices.

Model ID	D1	D2	D3	D4	D5	D6	D7	D8
M1	A	A	A	A	A	A	R	R
M2	A	A	A	A	A	R	A	R
M3	A	A	A	A	A	R	R	A
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
M26	R	A	A	R	A	A	A	A
M27	R	A	R	A	A	A	A	A
M28	R	R	A	A	A	A	A	A

The $N_M = 28$ validated MDA models were used to perform device ID verification and assess rogue detection performance as detailed in Section 4.3. During device ID verification, each of the individual WirelessHART devices was held-out of seven different models to serve in a rogue device role. For a given network model, both of the held-out devices are presented as rogue devices attacking each of the six authorized devices in that model. Thus, there were a total of twelve D_j:D_k (actual:claimed) rogue ID verification assessments performed per model. For example, as shown in Table 5 the M1 model D_j:D_k rogue assessments included authorized j = 1, 2, 3, 4, 5, 6 and held-out rogue k = 7, 8 combinations. Accounting for all M1−M28 models, a total of 12x28 = 336 rogue assessments were completed. These device ID verification results were generated using both the MVNPDF and Euclidean distance measures of similarity and are presented in Section 4.3, respectively.

4.0 Discrimination Assessment Results

WirelessHART adapter discrimination assessments were completed for both device classification and device ID verification, with emphasis on assessing rogue detection capability. For the following results, the burst region of interest used for CB-DNA fingerprint generation included a $T_{Brst} = 1.57$ *m*Sec interval (minimum burst duration noted in Section 2.1) regardless of collected burst type.

Results are presented to support CB-DNA Fingerprinting contributions noted in Section 1.3 and include: 1) device classification in Section 4.1 for $N_{Cls} = 8$ class models to establish baseline windowing effects, 2) device classification in Section 4.2 for the $N_M = 28$ distinct $N_{Cls} = 6$ class models detailed in Table 5 and required for device ID verification (rogue rejection) assessments, and 3) device ID verification and rogue rejection assessments in Section 4.3 using a MVNPDF measure of similarity and highlighting benefits relative to performance using a Euclidean-based measure.

4.1 WirelessHART Device Classification: $N_{Cls} = 8$ Class Model

4.1.1 TD-DNA vs. CB-DNA Fingerprinting

Performance of TD-DNA and CB-DNA fingerprinting are quantitatively compared using the MDA/ML classification methodology in Section 2.3.1 with 1) TD-DNA $\mathbf{F}_{\mathrm{TD}}$ fingerprints from (13) comprised of $N_F^{TD} = 243$ features extracted from the burst *PreAmbRgn* ROI, and 2) CB-DNA $\mathbf{F}_{\mathrm{CB}}$ fingerprints from (17) comprised of $N_F^{CB} = 72$ features extracted from the full-burst ROI. The classification matrices are provided in Table 6 (TD-DNA) and Table 7 (CB-DNA) and show near-perfect average $\%C = 99.96\%$ for TD-DNA and marginally lower $\%C = 95.63\%$ for CB-DNA. The poorer CB-DNA performance is predominantly attributed to confusion with the D8 device being errantly being called the D1.

Table 6 – MDA/ML confusion matrix for $N_{Cls} = 8$ class *TD-DNA Fingerprinting* using W_{Rect} windowing at collected SNR ≈ 30 dB. Device D2 was the only confused class (three instances).

Ave %C 99.96%		Predicted Class							
		D1	**D2**	**D3**	**D4**	**D5**	**D6**	**D7**	**D8**
True Class	**D1**	**945**	0	0	0	0	0	0	0
	D2	0	**942**		0	3	0	0	0
	D3	0	0	**945**	0	0	0	0	0
	D4	0	0	0	**945**	0	0	0	0
	D5	0	0	0	0	**945**	0	0	0
	D6	0	0	0	0	0	**945**	0	0
	D7	0	0	0	0	0	0	**945**	0
	D8	0	0	0	0	0	0	0	**945**

Table 8 provides a comparison of statistical precision and recall measures calculated using (22) and (23), respectively, with Table 6 (TD-DNA) and Table 7 (CD-DNA) W_{Rect} confusion matrix results. These results show 1) better than 90% average precision and precision for both TD-DNA and CB-DNA fingerprinting, with 2) the average cross-device recall measures being consistent with $\%C \approx 99.96\%$ reported in Table 6 and $\%C \approx 95.63\%$ reported in Table 7. Collectively, the results show that TD-DNA fingerprinting performs best ($\%C_\Delta \approx 4.33\%$ higher) when compared to CB-DNA fingerprinting. Of note, however, is that 1) this modest $\%C_\Delta = 4.33\%$ improvement is realized using $N_F^{TD} = 243$ vs. $N_F^{CB} = 72$ features, 2) generation and processing of more than three times the number of features (171 additional TD-DNA features) requires more computing

resources (processing power, storage, etc.), and 3) a $\%C_{\Delta} = 4.33\%$ trade-off in performance is considered reasonable when considering the objective of efficiently integrating (minimizing cost, complexity, etc.) CB-DNA Fingerprinting into CI elements hosting *typical* I/Q-based communication processing.

Table 7 – MDA/ML confusion matrix for $N_{Cls} = 8$ class *CB-DNA Fingerprinting* using W_{Rect} windowing at collected SNR ≈ 30 dB. The table shows that device D8 was the most confused class.

Ave %C 95.63%		Predicted Class							
		D1	**D2**	**D3**	**D4**	**D5**	**D6**	**D7**	**D8**
True Class	**D1**	**891**	18	0	0	3	0	0	33
	D2	9	**927**		0	0	0	0	9
	D3	0	0	**900**	0	21	0	24	0
	D4	0	0	0	**939**	6	0	0	0
	D5	0	0	0	0	**945**	0	0	0
	D6	0	0	0	0	0	**921**	12	12
	D7	0	0	3	0	0	9	**924**	9
	D8	150	6	3	0	3	0	0	**783**

Table 8 – Individual device *precision* and *recall* measurements calculated from Table 6 (TD-DNA) and Table 7 (CD-DNA) confusion matrix results and using (22) and (23), respectively.

	TD-DNA		**CB-DNA**	
	PRECISION (%)	***RECALL*** (%)	***PRECISION*** (%)	***RECALL*** (%)
D1	100	100	84.86	94.29
D2	100	99.68	97.48	98.10
D3	100	100	99.34	95.24
D4	100	100	100	99.37
D5	99.68	100	96.63	100
D6	100	100	99.03	97.46
D7	100	100	96.25	97.78
D8	100	100	92.55	82.86
Ave	**99.96**	**99.96**	**95.77**	**95.63**

4.1.2 CB-DNA Fingerprinting: Window Type Variation

Device classification was first evaluated for each of the communication windows in Section 2.2.2 using MVNPDF-based MDA/ML classification per Section 2.3.1. This was done for the $N_{Cls} = 8$ class model (all devices) with CB-DNA $\mathbf{F}_{\mathrm{CB}}$ fingerprints from (17) comprised of $N_F^{CB} = 72$ features. The resultant classification confusion matrices are provided for W_{Rect}, W_{HS}, and W_{RC} in Table 9, Table 10 and Table 11, respectively. Based on $\mathrm{CI}_{95\%}$ analysis, statistically equivalent $\%C \approx 96.5\%$ performance is achieved for the W_{HS} and W_{RC} windows with both being superior to the $\%C \approx 93.49\%$ performance of the W_{Rect} window.

Given the favorable W_{HS} and W_{RC} windows results above, the use of multi-symbol W_{RC} windowing in WirelessHART signaling (IEEE, 2011) and increased potential for efficient integration of CB-DNA Fingerprinting into CI systems hosting *typical* communication processing, all subsequent discrimination results presented in this paper are based exclusively on CB-DNA fingerprinting using a raised cosine W_{RC} window. Final analysis for W_{RC} window performance included calculation of the statistical measures given by (22) and (23). These are provided in Table 12 which shows relatively high precision and recall levels, with average cross-device recall matching the $\%C \approx 96.43\%$ reported Table 11 confusion matrix results.

Table 9 – MDA/ML confusion matrix for N_{Cls} = 8 class CB-DNA Fingerprinting using the W_{Reet} **window** of (9) at SNR = 20 dB.

%C: 93.49%		**Predicted Class**							
		D_1	**D_2**	**D_3**	**D_4**	**D_5**	**D_6**	**D_7**	**D_8**
True Class	**D_1**	**819**	45	0	0	0	0	0	81
	D_2	63	**831**	3	0	0	12	0	36
	D_3	0	0	**915**	0	3	6	21	0
	D_4	0	3	0	**942**	0	0	0	0
	D_5	0	0	6	0	**939**	0	0	0
	D_6	0	0	6	0	3	**888**	42	6
	D_7	0	0	21	0	0	9	**915**	0
	D_8	90	27	0	0	0	3	6	**819**

Table 10 – MDA/ML confusion matrix for N_{Cls} = 8 class CB-DNA Fingerprinting using the W_{HS} **window** of (10) at SNR = 20 dB.

%C: 96.51%		**Predicted Class**							
		D_1	**D_2**	**D_3**	**D_4**	**D_5**	**D_6**	**D_7**	**D_8**
True Class	**D_1**	**891**	9	6	3	0	3	0	33
	D_2	33	**885**	0	3	0	3	0	21
	D_3	0	0	**924**	0	0	3	18	0
	D_4	6	0	0	**939**	0	0	0	0
	D_5	0	0	0	0	**945**	0	0	0
	D_6	0	3	6	0	0	**909**	18	9
	D_7	0	0	15	0	0	6	**924**	0
	D_8	48	9	3	0	0	3	3	**879**

Table 11 – MDA/ML confusion matrix for N_{Cls} = 8 class CB-DNA Fingerprinting using the W_{RC} **Window** of (11) at SNR = 20 dB.

%C: 96.43%		**Predicted Class**							
		D_1	**D_2**	**D_3**	**D_4**	**D_5**	**D_6**	**D_7**	**D_8**
True Class	**D_1**	**888**	9	0	0	0	0	0	48
	D_2	21	**921**	0	0	0	0	0	3
	D_3	0	0	**921**	0	15	0	9	0
	D_4	0	0	0	**945**	0	0	0	0
	D_5	0	0	0	0	**945**	0	0	0
	D_6	0	3	0	0	0	**918**	15	9
	D_7	0	3	0	0	0	6	**933**	3
	D_8	105	18	0	0	0	0	3	**819**

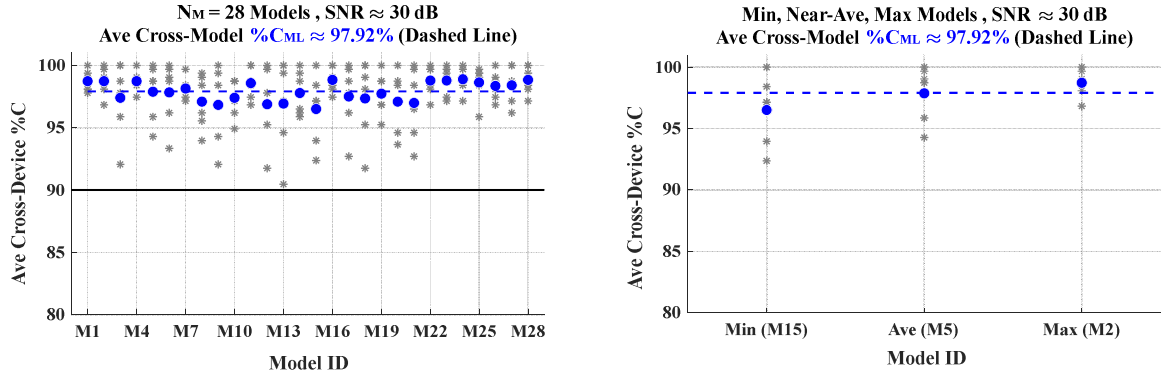
Table 12 – Per-class CB-DNA precision and recall calculated using the W_{RC} confusion matrix in Table 11 with (22) and (23).

	PRECISION (%)	***RECALL*** (%)
D_1	87.57	93.97
D_2	96.54	97.46
D_3	100	97.46
D_4	100	100
D_5	98.44	100
D_6	99.35	97.14
D_7	97.19	98.73
D_8	92.86	86.67
Ave	**96.49**	**96.43**

4.2 WirelessHART Device Classification: N_{Cls} = 6 Class Models

As a necessary first step for rogue rejection assessments, MDA/ML classification was performed to generate the trained MDA models ($\mathbf{W}_{\text{Best}}$, $\boldsymbol{\mu}_F$, $\boldsymbol{\sigma}_F$, $\boldsymbol{\mu}$, $\boldsymbol{\Sigma}$) using authorized device assignments given in Table 5. This includes $N_{Rg} = 2$ devices being held-out and $N_{Cls} = N_D = 6$ MDA models (M1–M28) models generated. Considering $N_{Rg} = 2$ rogues devices per model, with each rogue device serving in an attack role for each of the $N_D = 6$ authorized devices, a total of 2x28 = 56 individual Dj:D$_k$ rogue attack assessments were conducted.

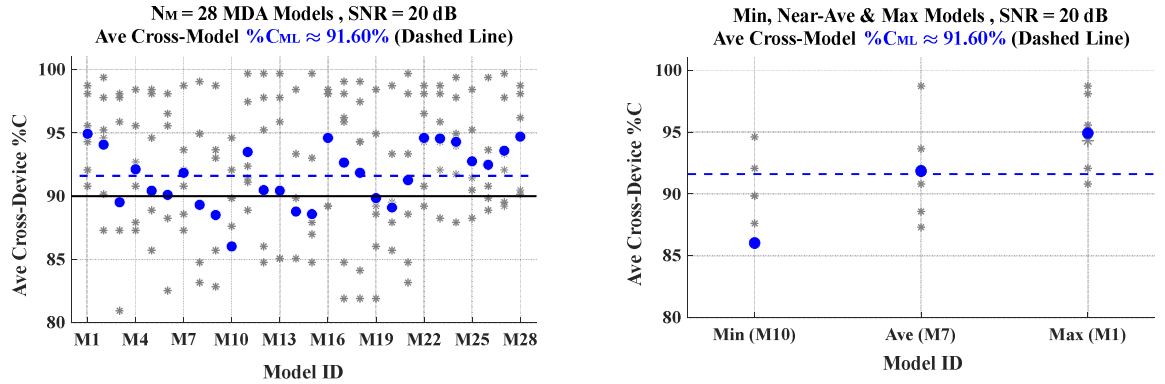
MVNPDF-based MDA/ML classification performance for the $N_M = 28$ models under collected SNR ≈ 30 dB conditions is shown in Fig. 8a, along with results for the minimum, near-average and maximum performing individual model results in Fig. 8b. The asterisk markers (∗) are individual model device results that are averaged to yield the cross-class solid circle marker (•) results. As indicated by the average dashed line in Fig. 8a, overall average cross-model $\%C \approx 97.92\%$ is achieved, with individual $\%C_D$ device results (∗) spanning $90.48\% \le \%C_D \le 100\%$. As indicated in Fig. 8a, all 28 models achieve an arbitrary $\%C = 90$ benchmark.



(a) All $N_{Cls} = 6$ class models (M1, M2, …, M28). (b) Min (M15), Near-Ave (M5), and Max (M2).

Fig. 8 – MVNPDF-based MDA/ML device classification showing average cross-device $\%C$ at the collected SNR ≈ 30 dB**.**

Additional MVNPDF-based MDA/ML classification results were generated for the $N_M = 28$ models under SNR = 20 dB conditions (approximate 33% degradation). These are presented in Fig. 9 using the same $\%C$ vertical scale as in Fig. 8 to enable direct comparison. The lower average cross-model $\%C \approx 91.60\%$ indicated by the dashed line in Fig. 9a is expected given the lower SNR conditions. This includes poorer individual device results (∗) that span $80.95\% \le \%C_D \le 99.68\%$. The minimum, near-average and maximum performing individual models are presented in Fig. 9b. As indicated in Fig. 9a, all but 7 of 28 models achieve the $\%C = 90\%$ benchmark. These seven models (M3, M8, M9, M10, M14, M15, and M20) fall just short by $\%C_\Delta \le 3.57\%$.

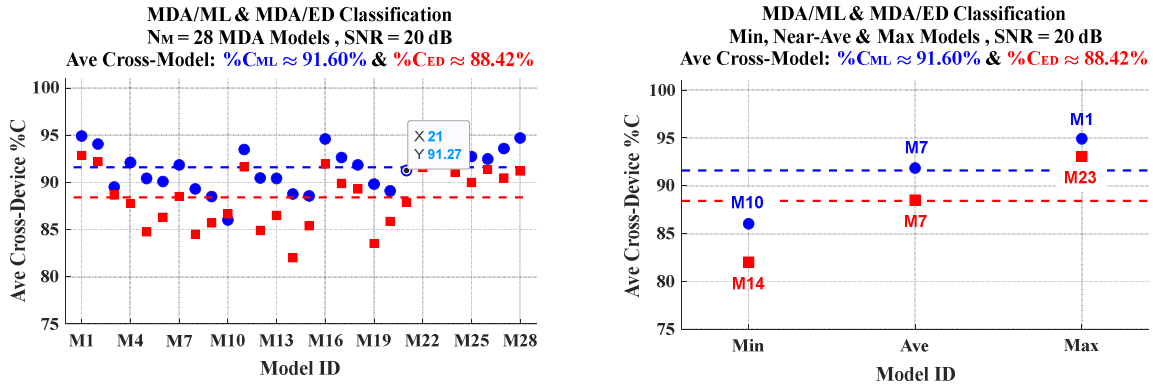


(a) All $N_{Cls} = 6$ class models (M1, M2, … M28). (b) Min (M10), Near-Ave (M7), and Max (M1) Models.

Fig. 9 – MVNPDF-based MDA/ML device classification showing average cross-device $\%C$ at SNR = 20 dB.

For completeness, Euclidean-based MDA/ED classification results were generated using the *same* $N_M = 28$ MDA models used to generate the MVNPDF-based MDA/ML results in Fig. 9. The MDA/ED results (■) are shown in Fig. 10 along with Fig. 9 MDA/ML results (●) overlaid. These results reflect an average cross-model difference of $\%C_{ML} - \%C_{ED} = \%C_\Delta \approx 3.2\%$ between the two classification measures. Considering individual model CI$_{95\%}$ confidence intervals in Fig. 10a (not evident given they are encompassed within the vertical extend

of the data markers) the model-by-model comparison includes MDA/ML (●) being statistically better than MDA/ED (■) in 26 of 28 models. The other two models (M3 and M10) are statistically similar.



(a) All N_{Cls} = 6 class models (M1, M2, …, M28).

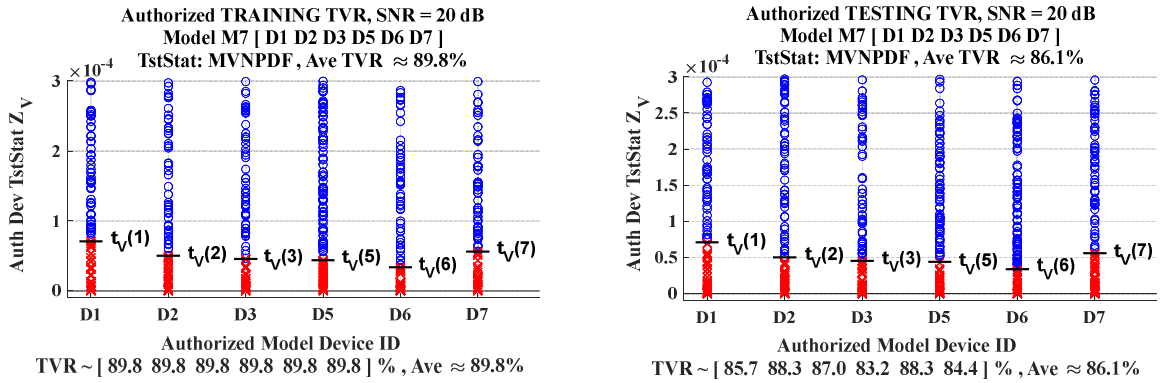
(b) Min, Near-Ave, and Max Models.

Fig. 10 – MDA/ED (■) and Fig. 9 MDA/ML (●) overlay showing average cross-device *%C* at SNR = 20 dB.

4.3 WirelessHART Device ID Verification

Device ID verification assessments were first conducted using the MVNPDF measure of similarity and the *same* N_M = 28 MDA trained ($\mathbf{W}_{Best}$, $\boldsymbol{\mu}_F$, $\boldsymbol{\sigma}_F$, $\boldsymbol{\mu}_k$, $\boldsymbol{\Sigma}_k$) models used classification results in Section 4.2. Results for rogue ID verification assessments at the collected SNR and under SNR = 20 dB were only marginally different; as such only results for SNR = 20 dB are presented for brevity. Presentation of results is further limited given that there were a total of 336 individual rogue assessments (N_M = 28 models, N_{Rg} = 2 held-out rogue devices per model, with both rogues attacking each of the N_D = 6 authorized model devices) completed at each SNR.

As detailed in Section 2.3.2, the first verification process step following MDA model training is authorized (modeled) device ID *training* verification to establish the device dependent $t_V(k)$ thresholds required for subsequent ID verification assessments. This is illustrated in Fig. 11 for MVNPDF-based statistics using the trained ($\mathbf{W}_{Best}$, $\boldsymbol{\mu}_F$, $\boldsymbol{\sigma}_F$, $\boldsymbol{\mu}_k$, $\boldsymbol{\Sigma}_k$) for model M7 which produced the near-average *%C* classification in Fig. 9b. The indicated $t_V(k)$ in Fig. 11a are device dependent training thresholds set to achieve training TVR ≈ 89.8%. These training $t_V(k)$ are used to validate authorized model ID verification using testing fingerprint Z_V as illustrated in Fig. 11b and yield an average testing TVR ≈ 86.1% across the authorized devices for the TST TVR shown below the device ID label.



(a) *Training* fingerprint Z_V statistics with device-dependent $t_V(k)$ thresholds set to achieving *training* TVR ≈ 90%.

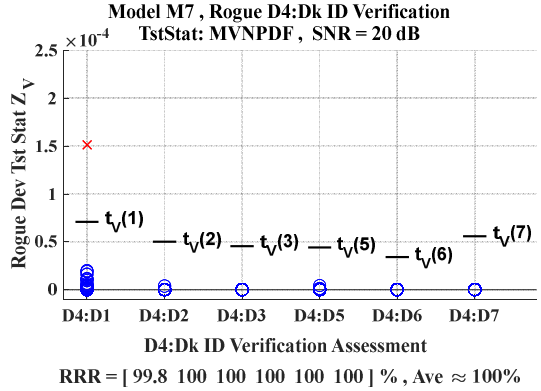
(b) *Testing* fingerprint Z_V statistics with training $t_V(k)$ used to calculate the *testing* TVR shown below the device label.

Fig. 11 – Authorized device ID verification using the MVNPDF-based test statistics for model M7 showing (a) training $t_V(k)$ threshold determination and (b) corresponding testing TVR using training $t_V(k)$.

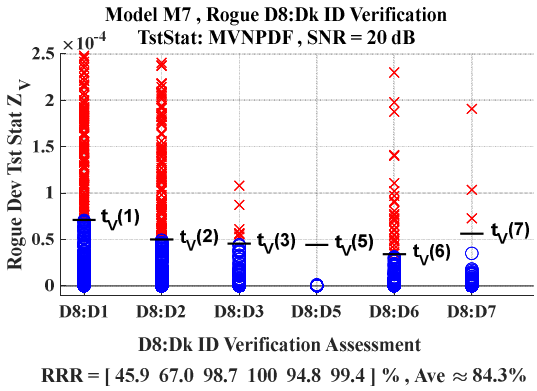
Given the authorized device ID verification consistency reflected in Fig. 11, the next device ID verification step included rogue rejection assessments. As detailed in Section 2.3.2, this is accomplished on a model-by-model basis with the N_{Rg} = 2 held-out devices serving as attacking rogues against each of the authorized model devices. The process is illustrated in Fig. 12 for MVNPDF-based statistics and model M7 which produced near-average classification performance at SNR = 20 dB. The Fig. 12 RRR assessments (12 total) are representative of results

obtained for the remaining 12x27 = 324 assessments using other models. An overall summary of accumulated RRR performance across all $N_M = 28$ models is presented following the discussion of the Fig. 12 results.

The individual rogue ID verification results in Fig. 12 are for MVNPDF-based Z_V generated from rogue testing fingerprints for claimed IDs matching each of the M7 authorized devices (D1, D2, D3, D5, D6, and D7). The training verification thresholds are applied from Fig. 11a, with all Z_V falling above the indicated device dependent $t_V(k)$ threshold representing a desired outcome, i.e., the falsely claimed ID is rejected. The RRR for D_j:D_k assessments of attacking D4 and D8 rogue devices is presented in Fig. 12a and Fig. 12b, respectively. As indicated below the D_j:D_k Verification Assessment labels, average RRR across all assessments included RRR ≈ 100% and RRR ≈ 84.3% for the D4 and D8 rogue devices, respectively.



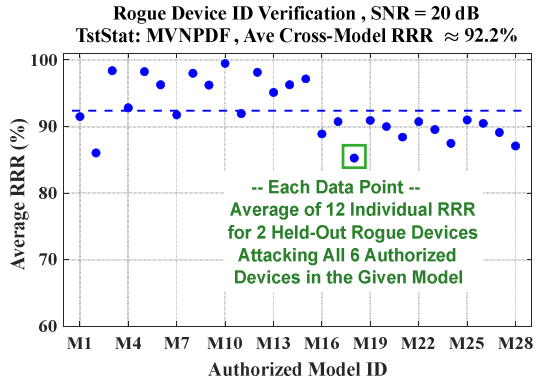
(a) Rogue device D4 claiming all model M7 authorized.



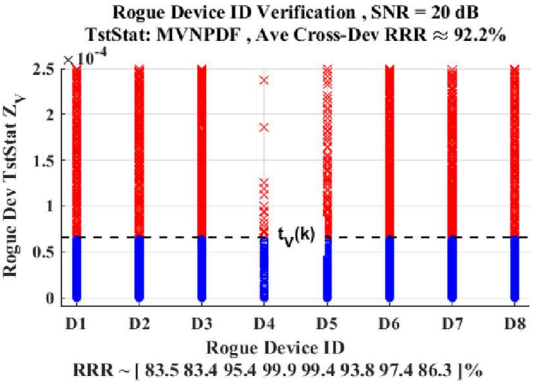
(b) Rogue device D8 claiming all model M7 authorized.

Fig. 12 – Rogue device ID verification using MVNPDF-based test statistics for model M7 (D1, D2, D3, D5, D6 and D7 devices) with training tv(k) from Fig. 11a yielding the indicated individual device and cross-device average RRRs.

A summary of cumulative RRR results for MVNPDF-based statistics and all 336 rogue assessment scenarios are presented in two ways, with each showing that an average RRR ≈ 92.2% is achieved for SNR = 20 dB conditions. As noted previously, results for collected SNR conditions were better and included average RRR ≈ 100% across all 336 rogue scenarios. The first cumulative summary for MVNPDF-based test statistics is provided in Fig. 13a which shows the average RRR performance across all rogue assessments completed on a model-by-model basis. For example, the cumulative average of D4 and D8 rogue assessments in Fig. 12 for model M7 is the average of RRR ≈ 100% and RRR ≈ 84.3% , or RRR ≈ (100% + 84.3%)/2 ≈ 92.2%. This average is appropriately reflected in Fig. 13a for M7 and approximately equals the overall cross-model average (dashed line) for all $N_M = 28$ models.



(a) Individual model average RRR for all rogue attacks.



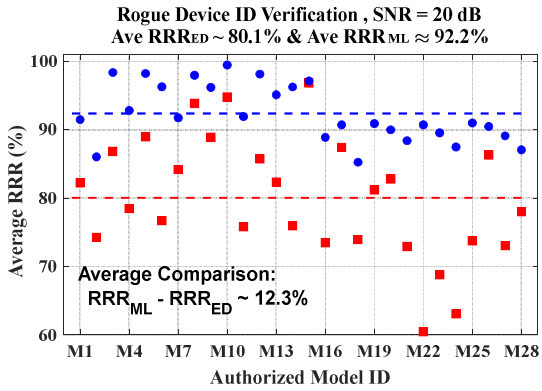
(b) Verification tv(k) aligned/centered as indicated.

Fig. 13 – Cumulative summaries of *MVNPDF-based* rogue rejection performance accounting for all 336 rogue assessment scenarios. Accumulations for (a) all $N_M = 28$ models with average RRR based on ($N_{Rg} = 2$)x($N_D = 6$) = 12 rogue attacks per model, and (b) each of the 8 WirlessHART devices being held-out of 7 models and attacking all $N_D = 6$ authorized devices in the model. Both summary accumulation methods yield an overall average RRR ≈ 92.2%.

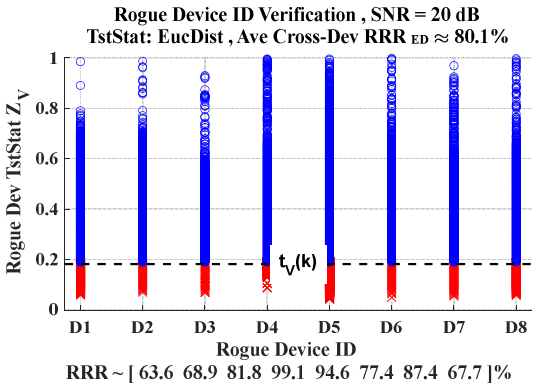
The second cumulative summary method includes considering that each available device has served in a rogue D_j ($j = 1, 2, \ldots, 8$) role when held-out of 7 different models and falsely claiming an authorized D_k device ID a total of 7x6 = 42 times (including replication). The accept/reject rogue Z_V test statistics from these 42 assessments for each D_j are accumulated and plotted as shown in Fig. 13b where individual assessment t_V values have been "centered" at

the indicated $t_V(k)$. Once again, the accumulated average RRR across all 336 scenarios is RRR ≈ 92.2% which is calculated by averaging the per-device RRR shown in Fig. 13b which spans 83.4% ≤ RRR ≤ 99.9%.

Rogue detection results are presented for a Euclidean-based test statistic in support of highlighting noted benefits of the MVNPDF-based test statistic. Rogue device ID verification was performed using the Euclidean-based measure of similarity and the *same* 28 trained ($\mathbf{W}_{Best}$, μ_F, σ_F, μ_k, Σ_k) MDA models used for MVNPDF results presented in Fig. 11 through Fig. 13. The Euclidean-based summary includes 1) the accumulated cross-device average RRR for all models in Fig. 14a and 2) the accumulated cross-model RRR for all devices in Fig. 14b. Note that relative to the MVNPDF-based results in Fig. 13b, the corresponding Euclidean-based results in Fig. 14b include a reversal of undesired (red **X** markers) and desired (blue **O** markers) outcomes and their relationship to the $t_V(k)$ verification thresholds. This reversal is due to 1) the MVNPDF-based Z_V statistic being a higher-is-better metric, with a higher Z_V value reflecting greater likeness ($Z_V > t_V \rightarrow$ errant rogue ID validation and red **X** assignment), and 2) the Euclidean-based Z_V statistic being a lower-is-better metric, with values closer to 0 representing greater likeness ($Z_V < t_V \rightarrow$ errant rogue ID validation and red **X** assignment).



(a) Euclidean-based (■) versus Fig. 13a MVNPDF-based (●)



(b) Verification $t_V(k)$ aligned/centered as indicated.

Fig. 14 – Cumulative summaries of *Euclidean-based* (■) rogue rejection performance for 336 rogue scenarios including (a) all $N_M = 28$ models with average RRR based on ($N_{Rg} = 2$)x($N_D = 6$) = 12 rogue attacks per model, and (b) each of the 8 WirelessHART devices being held-out of 7 models and attacking all $N_D = 6$ authorized devices in the model. Both summary accumulation methods show an overall average $RRR_{ED} \approx 80.1\%$ for the Euclidean-based device ID verification.

Superiority of the MVNPDF-based statistic for rogue ID verification is highlighted in Fig. 14a which shows Euclidean-based results (■) overlaid with MVNPDF-based results (●) from Fig. 13a. The Euclidean-based performance includes average RRR ≈ 80.1% across all 336 rogue assessments which is obtained by averaging the Fig. 14b per-rogue device RRR which spans 63.6% ≤ RRR ≤ 99.1%. The benefits noted in (Aksoy et al., 2000; Gopal et al., 2004; Weller-Fahy et al., 2015) for using probabilistic measures is evident in Fig. 14a which shows nearly 12% improvement when using the MNVPDF-based device ID verification process.

5.0 Summary and Conclusions

This work supports a technical cradle-to-grave protection strategy that enables Critical Infrastructure (CI) elements to reach full life expectancy using mid-life security protection measures to minimize premature service termination resulting from adverse cyber activity. These measures include real-time monitoring which collectively embodies both higher-layer (bit-level) and the lowest PHY layer (waveform-level) methods. Bit-level protection is commonly targeted by *rogue* devices aiming to conduct nefarious activity by mimicking authorized device bit-level identities (Hua et al., 2018; Shrivastava et al., 2020; Zhang et al., 2014; Zhang et al., 2019). Detecting such devices remains an important first step for countering attacks and has been the focus of prior PHY layer ZigBee works (Peng et al., 2019; Rondeau et al., 2018a). These works exploited constellation-based features to achieve reliable authorized and rogue device discrimination. Of significance is that such features can be practically generated and employed within CI elements hosting typical communication signal processing. Given the favorable ZigBee classification results in (Peng et al., 2019; Rondeau et al., 2018a), and the observed ZigBee-like characteristics of the WirelessHART signals considered here, this work expands upon prior works by 1) demonstrating general extensibility using a CI-centric protocol while further reinforcing the exploitability of constellation-based features, 2) assessing both device classification and device ID verification (rogue detection) as functionally separate yet related processes, and 3) demonstrating benefits for using a Multivariate Normal Distribution Probability Density Function (MVNPDF) measure of similarity which yielded nearly 12% improvement in rogue detection capability when transitioning from a Euclidean distance measure.

The device discrimination demonstrations are based on Constellation-Based Distinct Native Attribute (CB-DNA) features extracted from WirelessHART devices for two different manufacturers and include 1) average cross-class (cross-device) percent correct classification of $\%C > 90\%$ being achieved across 28 different networks comprised of six authorized devices each, and 2) average rogue rejection rate in the range of $83.4\% \leq \text{RRR} \leq 99.9\%$ based on two held-out devices serving as attacking devices for each of the 28 networks. Overall performance included average $\text{RRR} \approx 92.2\%$ across a total of 336 individual rogue attack assessments. This was achieved using a probability-based MVNPDF measure of similarity which is shown to provide superior performance (nearly 12% higher average RRR) when compared with a Euclidean-based distance measure.

The favorable PHY layer based (waveform-level) CB-DNA discrimination results herein are supportive of an envisioned real-time Radio Frequency Fingerprinting (RFF) capability for augmenting existing critical infrastructure security architectures. These architectures are highly dependent on higher-layer (bit-level) protection mechanisms and, as with demonstrations in (Peng et al., 2019; Rondeau et al., 2018a), results here highlight the benefits of constellation-based RFF methods. PHY layer security augmentation methods remain worthy of further consideration for application in more complex environments. This includes applications ranging from smaller scale floor-sized plant operations (e.g., manufacturing process monitoring and control) to larger scale yard-sized operations (e.g., petroleum, oil, and lubricant distribution).

ACKNOWLEDGMENT

The views 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. Paper approved for public release, Case#: 88ABW-2020-2506.

REFERENCES

Aksoy S, Haralick RM. Probabilistic vs. geometric measures for image retrieval. 2000 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Cat. No. PR00662. Hilton Head Island SC, USA, 2000.

Bhatt S, Tseng FH, Maranzana N, Segonds F. Scientometric study of product lifecycle management international conferences: A decade overview. In: Bouras A, Eynard B, Foufou S, Thoben KD (eds); Product lifecycle management in the era of internet of things. IFIP Advances in Information and Communication Technology. Springer, Cham. 2016:467:672-683, 2015.

Carbino TJ, Temple MA, Lopez J. A Comparison of PHY-Based Fingerprinting Methods Used to Enhance Network Access Control. In: Federrath H., Gollmann D. (eds) ICT Systems Security and Privacy Protection. SEC 2015. IFIP Advances in Information and Communication Technology, Vol 455. Springer, Cham. 2015.

Defense Standardization Program Office (DSPO). SD-22 diminishing manufacturing sources and material shortages: A guidebook of best practices for implementing a robust DMSMS management program; January 2016. Available from: http://www.dmsmsmeeting.com/2013/media/SD_22_DMSMS_Guidebook_8-1-12.pdf [Accessed: 30 September 2020].

Duda RO, Hart PE, Stork DG. Pattern classification, Second ed. New York: John Wiley & Sons; 2001.

Ettus Research. SBX Wide Bandwidth Transceiver; 2019. Available from: https://kb.ettus.com/SBX [Accessed: 30 September 2020].

Gopal K, Romo TD, Sacchettini JC, Ioerger TR. Efficient retrieval of electron density patterns for modeling proteins by X-ray crystallography. 2004 IEEE Int'l Conference on Machine Learning and Applications (ICMLA'04), Louisville KY, USA, 2004.

Hastie T, Tibshirani R, Friedman J. The elements of statistical learning; data mining, inference, and prediction; 2001. New York, NY, USA: Springer-Verlag.

Hua J, H. Sun, Z. Shen, Z. Qian and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information", 2018 IEEE Conference on Computer Communications (INFOCOM 2018). Honolulu, HI, USA, April 2018.

Institute of Electrical and Electronics Engineers (IEEE). IEEE 802.15.4: Low-rate wireless personal area networks (LR-WPANs); 2011.

Institute of Asset Management (IAM). Asset management – an anatomy; 2015. Version 3. Available from: https://theiam.org/media/1781/iam_anatomy_ver3_web.pdf [Accessed 30 September 2020].

James G, Witten D, Hastie T, and Tibshirani R; 2017. An introduction to statistical learning with applications in R. New York: Springer.

Keefe M. Timeline: critical infrastructure attacks increase steadily in past decade. Computer World; 2012. Available from: https://tinyurl.com/y5um5jck [Accessed 30 Sep 2020].

Kleinberg J, Tardos É. Algorithm Design, First ed., Pearson New International Edition, Pearson Education Limited, Essex; 2014.

Leef S. Supply chain hardware integrity for electronics defense (SHIELD). Software and Supply Chain Assurance Winter Forum, McLean, VA, USA, Dec 2018.

Lopez J, Liefer NC, Busho CR, Temple MA. Enhancing critical infrastructure and key resources (CIKR) level-0 physical process security using field device distinct native attribute features; 2018. IEEE Trans on Info Forensics & Security; 13(5):1215-1229.

López-Rubio, E. A Histogram Transform for Probability Density Function Estimation; 2014 IEEE Trans on Pattern Analysis and Machine Intelligence; 36:644-656.

Matsui YZ. Near real-time Zigbee device discrimination using CB-DNA features; 2020. US Air Force Institute of Technology Masters Thesis, AFIT-ENG-MS-20-M-043, Mar 2020.

Miller MB. Mathematics and statistics for financial risk management. Second ed. Hoboken, New Jersey: John Wiley & Sons; 2014.

Nakamura ET, Ribeiro SL. A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems; 2018. 2018 Global Internet of Things Summit (GIoTS), Bilboa, Spain, Jun. 2018.

National Instruments (NI). Software Defined Radio Reconfigurable Device. USRP-2950/2952/2953/2954/2955; 2016. Available from: https://www.ni.com/pdf/manuals/376355c.pdf [Accessed 30 September 2020].

Neuhaeusler C. Generation of IEEE 802.15.4 Signals; Jan 2016. Rohde & Schwarz Application Note, Doc #1GP105_1E.

Park H, Leemis L. Ensemble confidence intervals for binomial proportions; 2019. Statistics in Medicine, John C. Wiley & Sons Ltd., DOI: 10.1002/sim.8189.

Peng L, Hu A, Zhang J, Jiang Y, Yu J, Yan Y. Design of a hybrid RF fingerprint extraction and device classification scheme; 2019. IEEE Internet Things J.; 6(1) 349–360.

Pepperl+Fuchs. WHA-BLT-F9D0-N-A0-* WirelessHART adapter; 2015. TDOCT-4909_ENG. Available from: https://files.pepperl-fuchs.com/webcat/navi/productInfo/doct/tdoct4909__eng.pdf?v=20200320035850 [Accessed 30 September 2020].

Reising DR, Temple MA, Jackson JA. Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints; 2015. IEEE Trans on Information Forensics and Security, 10(6):1180–1192.

Rondeau CM, Betances JA, Temple MA. Securing ZigBee commercial communications using CB-DNA fingerprinting; 2018. Jour of Security and Communication Networks (SCN), Wiley, Vol. 2018, ID. 1489347. 2018a

Rondeau CM, Temple MA, Betances JA. "IIoT cross-layer forensics for WirelessHART." 2018 Industrial Control System Cybersecurity Conference (ICSCC), Atlanta GA, USA, 2018b.

Rondeau CM, Temple MA, Lopez J. Industrial IoT cross-layer forensic investigation; 2019. Wiley Interdisciplinary Reviews (WIREs): Forensic Science. ID#: E1322, Feb 2019 1(1).

Sayfayn N, Madnick S. Cybersafety analysis of the Maroochy Shire sewage spill. Working paper CISL# 2017-09; 2017. Available from: http://web.mit.edu/smadnick/www/wp/2017-09.pdf [Accessed 30 September 2020].

Shrivastava P, Jamal MS, Kataoka K, EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi; 2020. IEEE Trans on Network and Service Management; 17(1):89-102.

Siemens. WirelessHART Adapter Sitrans AW210 – 7MP311, November 2012. Compact Operating Instructions, Doc ID#: DM1101120UBA. Available from: https://support.industry.siemens.com/cs/document/61527753/wirelesshart-adapter-sitrans-aw210-7mp3111?dti=0&lc=en-GT [Accessed 30 September 2020].

Talbot CM, Temple MA, Carbino TJ, Betances JA. Detecting rogue attacks on commercial wireless Insteon home automation systems; 2017. Jour of Computers and Security, Special Issue (Internet and Cloud of Things), pp. 296–307.

Tharwat, A. Classification assessment methods. Applied Computing and Informatics; 2018. Available from: https://doi.org/10.1016/j.aci.2018.08.003 [Accessed 30 September 2020].

U.S. DHS. Advisory (ICSA-10-201-01C) USB malware targeting Siemens control software. U.S. Department of Homeland Security; 2010. Available from: https://www.us-cert.gov/ics/advisories/ICSA-10-201-01C [Accessed 30 September 2020].

U.S. DHS. ICS joint security awareness report (JSAR-12-241-01B): Shamoon/DistTrack malware (Update B); U.S. Department of Homeland Security; 2012. Available from: https://www.us-cert.gov/ics/jsar/JSAR-12-241-01B [Accessed 30 September 2020].

U.S. DHS. Alert (TA17-163A): CrashOverride malware; U.S. Department of Homeland Security; 2017.Available from: https://www.us-cert.gov/ncas/alerts/TA17-163A [Accessed 30 September 2020].

Wang W, Sun Y, Li H, Han Z. Cross-Layer attack and defense in cognitive radio networks. 2010 IEEE Global Communications Conference (GLOBECOM), Miami FL, USA, 2010.

Weiss J. Cyber security of sensors are not being addressed and vulnerabilities are not correlated to system impacts; Control-Unfettered Blog; 2018. Available from: https://www.controlglobal.com/blogs/unfettered/cyber-security-of-sensors-are-not-being-addressed-and-vulnerabilities-are-not-correlated-to-system-impacts/ [Accessed 30 September 2020].

Weller-Fahy DJ, Borghetti BJ, Sodemann AA. A survey of distance and similarity measures used within network intrusion anomaly detection; 2015. IEEE Communication Surveys & Tutorials; 17(1):70-91.

Yang K, Forte D, Tehranipoor MM, "CDTA: A comprehensive solution for counterfeit detection, traceability, and authentication in the IoT supply chain; 2017. ACM Trans on Design Automation of Electronic Systems, 22(3) Article #42.

Zetter K. Countdown to zero day: Stuxtnet and the launch of the world's rirst digital weapon; 2015. Danvers, MA, USA: Broadway Books.

Zhang K, Liang X, Lu R, Shen X. Sybil attacks and their defenses in the internet of things; 2014. IEEE Internet Things J.; 1(5):372–383.

Zhang Z, Hasegawa H, Yamaguchi Y, Shimada H. Rogue Wireless AP Detection using Delay Fluctuation in Backbone Network. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, Jul 2019.

Zhuo F, Huang Y, Chen J. Radio frequency fingerprint extraction of radio emitter based on I/Q imbalance; 2017. Procedia Computer Science, 107:472–477.

Zoltowski M. Equations for the raised cosine and square-root raised cosine shapes; 2019. Available from: http://www.commsys.isy.liu.se/TSKS04/lectures/3/MichaelZoltowski_SquareRootRaisedCosine.pdf [Accessed 30 September 2020].