Data-Driven Correlation of Cyber and Physical Anomalies for Holistic System Health Monitoring

DANIEL L. MARINO 1, CHATHURIKA S. WICKRAMASINGHE 1, BILLY TSOUALAS 1, CRAIG RIEGER 2, AND MILOS MANIC 1(FIEEE)

1Virginia Commonwealth University, Richmond, VA 23220 USA (e-mail: {marinodl, brahmanacvw, tsouvalasv}@vcu.edu, misko@ieee.org)
2Idaho National Laboratory, Idaho Falls, Idaho, USA (e-mail: craig.rieger@inl.gov)

Corresponding author: Daniel L. Marino (e-mail: marinodl@vcu.edu).

This material is based upon work supported by the U.S. Department of Energy’s Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technology Office Award Number DE-0008775. Effort performed through Department of Energy under U.S. DOE Idaho Operations Office, Contract DE-AC07-05ID14517, as part of the Resilient Control and Instrumentation Systems (ReCIS) program of Idaho National Laboratory. This work was supported in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation and workforce development. For more information about CCI, visit cyberinitiative.org.

ABSTRACT

Concerns of cyber-security threats are increasingly becoming a part of everyday operations of cyber-physical systems, especially in the context of critical infrastructures. However, despite the tight integration of cyber and physical components in modern critical infrastructures, the monitoring of cyber and physical subsystems is still done separately. For successful health monitoring of such systems, a holistic approach is needed. In this paper, we present an approach for holistic health monitoring of cyber-physical systems based on cyber and physical anomaly detection and correlation. We provide a data-driven approach for the detection of cyber and physical anomalies based on machine learning. The benefits of the presented approach are: 1) an integrated architecture that supports acquisition and real-time analysis of both cyber and physical data; 2) a metric for holistic health monitoring that allows for differentiation between physical faults, cyber intrusion, and cyber-physical attacks. We present experimental analysis on a power-grid use case using the IEEE-33 bus model. The system was tested on several types of attacks such as network scan, Denial of Service (DOS), and malicious command injections.

INDEX TERMS

Anomaly Detection, Cyber-physical systems, System Health Monitoring, Cyber and Physical Anomalies.

I. INTRODUCTION

Cyber-Physical Systems (CPSs) are nowadays ubiquitous in the core of mission-critical infrastructure due to their significant competitive advantages, such as adaptability, scalability, and usability [1]. Such systems typically take the form of a collection of interconnected physical and computing resources to accomplish a specific task. They integrate computational resources, communication, control, and physical processes into a single system [2, 3]. Although the integration of cyber and physical systems has lead to improved efficiency, this integration makes CPS vulnerable to cyber-security threats, leading to a degradation of resiliency [4]. In order to address this issue, maintaining situational awareness becomes essential in the effort to ensure both efficiency and resiliency.

Maintaining situational awareness is critical for successful decision-making [5, 6]. Providing relevant and well-timed information to domain experts and system users is essential to understand the state of the system [7]. To this end, health monitoring of CPSs aims to provide a human-recognizable measure of misbehavior of a system caused by internal anomalies and external intrusions [8]. Health monitoring provides a compelling approach to inform operators of the presence and type of anomalies, serving as support for the execution of well-informed decisions to recover from disturbances (benign and malicious). Given the interdisciplinary nature of CPSs, characterizing the health of such systems requires holistic monitoring of both cyber and physical com-
ponents. However, despite the tight integration of cyber and physical components in CPSs, monitoring of these systems is traditionally performed by monitoring cyber and physical subsystems independently. Currently, there is limited work on the development of a metric that characterizes the health of a CPS by considering both cyber and physical components in the same context.

This paper presents a data-driven approach for cyber-physical health monitoring. Integrating data from physical as well as cyber elements allows for a comprehensive and holistic assessment of the health of the CPS. We employ data-driven Anomaly Detection Systems (ADSs), which combines anomaly detection on a physical and cyber level. The physical ADS performs analysis on data acquired by sensors in the physical system while the cyber ADS employs cyber-sensors to capture and analyze network packets in real-time. Three unsupervised algorithms were used for comparative analysis: one-class support vector machines (OCSVMs), Local Outlier Factor (LOF), and Autoencoders (AEs).

Cyber-physical health monitoring is a complex process that must be performed accurately in real-time, minimizing the time needed to detect and restore the system to a healthy state [9]. Regarding the state-of-the-art, there is limited related work that focuses on holistic real-time monitoring of CPS health, where both cyber and physical components are evaluated together in real-time [10]. Even though the importance of integrating the two is underlined in previous efforts, existing literature relevant to anomaly detection in CPSs mainly considers cyber and physical data separately [11] [12] [13]. Some efforts perform anomaly detection by using the physical process dynamics [14]. Certain attempts establish correlation schemes between cyber and physical data using Bayesian networks for anomaly detection, and root-cause isolation [15]. In [16], cross-correlation between anomaly detection on network flow data and parsed Supervisory Control and Data Acquisition (SCADA) log files is used to increase the confidence of security alerts. Unlike similar efforts that examine the temporal correlation of different anomaly detection outputs [16], we present a health monitoring metric that indicates the source of the disturbance (cyber or physical). The metric serves as a holistic health monitoring mechanism that provides a human-recognizable measure of misbehavior caused either by internal anomalies or external intrusions. The metric is presented along a full pipeline to acquire cyber and physical data for analysis using ADSs. Furthermore, we provide a comparative analysis of anomaly detection algorithms for distinctions between normal, physical faults, cyber intrusions, and cyber-physical attack scenarios.

Contributions of the presented approach:

- We present an integrated cyber and physical data-driven architecture that performs data acquisition, management, and analysis of both cyber and physical data.
- We introduce a health monitoring metric based on the correlation of cyber and physical Anomaly Detection Systems (ADS). We validate the presented approach by evaluating its capability to distinguish between physical faults, cyber intrusion, and cyber-physical attacks. We evaluate the presented metric using different combinations of three machine learning algorithms: One-Class-SVM, Local Outlier Factor, and Autoencoders.

The rest of the paper is organized as follows: Section II presents the related work; Section III presents the proposed data-driven cyber physical health monitoring; Section IV discusses the experiments and results; and finally, Section V presents the conclusions of the paper.

II. RELATED WORK

CPSs are a prime target for many cyber attack vectors such as Denial-of-Service (DOS), data injection, and interception schemes [17, 18]. Anomaly Detection Systems (ADSs) are becoming a common component of CPSs which are implemented to detect anomalies in CPS networks [19]. These anomalies may be signs that an intruder is attempting unauthorized access to the system [20]. ADSs are implemented to detect cyber-attacks, and intrusion attempts are referred to as anomaly-based Intrusion Detection Systems (IDS) [20]. Due to the complex nature of CPSs, various ADS strategies have been exploited in recent literature [14, 16, 17].

Some efforts have attempted to exploit the procedural constraints of CPS to detect anomalies and to identify specific cyber attacks. For example, in [21], researchers have employed pattern matching methodologies over specific communication protocols to build ADSs. The network traffic characteristics and their importance have been used in [22] to detect anomalies. Some other efforts have been implemented in a more attack-centric manner where the evaluation of a systems cybersecurity by investigating specific attacks such as malware attacks [23–25], attacks on communication protocols [26–28], DOS attacks [25, 29], Man-In-the-Middle attacks [30], false sequential [31], data or code injection attacks[32], and other integrity attacks [33]. Some recent attempts have used neural-network based approached to build ADSs. In [34], researchers have trained Autoencoders (AEs) and Generative Adversarial Networks (GANs) using GAF images to identify and detect anomalies in system components. In [35], authors have converted time-series data from sensors into time-frequency images for detecting anomalies using Convolutional Neural Networks (CNN).

Proposed solutions to recognizing anomalies have also been targeted towards Cyber-Physical System Health Monitoring and Management (HMM) systems [36]. They consist of ADS implementations that employ different types of modern Machine Learning and Neural Network methodologies to perform real time health monitoring of CPSs. Some efforts identify the faulty components by implementing a Fault Signature Matrix (FSM), which associates the sensors and target system components with the rules that describe the normal behavior of the system [37]. Other system health implementations, such as Hackmann et al [38], propose a Structural Health Monitoring (SHM) system which focuses
on structural deficiencies (environmental corrosion, persistent traffic, and wind loading) that occur during the lifetime of CPSs. Other approaches use the dynamic constraints of physical systems to detect anomalous behavior in physical data [14].

Cross correlation of several anomaly detection systems has been recognized in literature as an approach to provide more accurate detection of anomalies in CPSs [16]. In [16], a combination of Autoencoders and parsers are used to detect anomalies by analysing network flows and SCADA log files. In [15], bayesian networks are used to identify anomalous behavior using network events and physical data. In [17], physical data is extracted by parsing captured packet data. One Class SVMs and PCA are used to perform anomaly detection on cyber and physical data. The detection is performed in parallel but results are presented independently.

In our approach, we used three machine learning algorithms, namely One-Class Support Vector Machines (OCSVMs), Local Outlier Factor (LOFs), and Autoencoders (AEs). These algorithms were selected as they represent a set of frequently used unsupervised machine learning algorithms for anomaly detection in the recent literature [39–43]. Since these algorithms are unsupervised machine learning algorithms, they do not require any labeled data to train these algorithms. Many real-world systems bring the challenge of collecting unlabeled data because the data labeling process is very expensive[44]. In addition, it is a time-consuming task that requires domain experts to manually analyzing data[45]. Further, Cyber-physical Systems generate large volumes of data rapidly, making the labeling process inefficient and impractical. Therefore, these unsupervised algorithms are a viable solution for benefiting from the abundance of unlabelled data generated in these CPSs. Below, a brief description of the anomaly detection algorithms is presented:

- One-class Support Vector Machines: OCSVMs are widely used unsupervised machine learning algorithms for anomaly detection. They are trained using the system’s normal behavior, and any unseen behavior is identified as an anomaly or an attack. OCSVMs are extensions of Support Vector Machines (SVMs) [46, 47]. They can learn a decision boundary of a single class. In the case of anomaly detection in CPS, they learn the decision boundary of the normal behavior class. Any behavior which is different from the learned normal behavior will be detected as an outlier [48, 49]. There have been several proposed solutions and enhancements based on OSVMs [50–52].
- Local Outlier Factor: The Local Outlier Factor (LOF) algorithm is clustering-based unsupervised anomaly detection method that computes the local density deviation of a given data point with respect to its neighbors [53]. It identifies outliers or anomalies as data records that have a significantly lower density compared to its neighbor data points [54]. This has been widely employed for anomaly detection in CPSs [55–57].
- Autoencoder: Autoencoders (AEs) are widely used neural network architectures which have the capability to learn encoding of input data. The architecture of AEs consist of two part: encoder and decoder. The encoder converts input data into an abstract representation which is then reconstructed using the decoder [18, 45]. In anomaly detection, the difference between input and the reconstruction indicates whether the data record is an anomaly or not. AEs have been successfully used in CPSs for malicious code detection, malware detection, and anomaly detection [18, 58].

III. PRESENTED DATA-DRIVEN CYBER-PHYSICAL HEALTH MONITORING

This section describes the presented approach for data-driven cyber-physical health monitoring. The presented approach monitors cyber and physical data in order to identify internal anomalies and external intrusions through the use of anomaly detection algorithms. The information is consolidated in a metric that uses the correlation of cyber and physical anomalies as the basis for characterization of the health of the system.

The overall architecture is presented in Figure 1. The architecture provides the support for managing data streams of cyber and physical data through a publisher/subscriber model. The approach consolidates data coming from different sensors, communication media, and protocols. Physical data is collected from measurements obtained by field devices and communicated to a master using industrial protocols.
data is provided by a cyber-sensor that collects and analyzes packet data. Cyber and physical data streams are managed by Kafka, which collects, stores, and serves the data to any process that requires it.

Kafka was chosen as the publisher/subscriber architecture to manage cyber and physical data. Kafka is an open-source distributed streaming platform based on the publish/subscribe architecture. The main benefits of Kafka included high scalability, fault tolerance, and support to most common programming languages. DNP3 was chosen as the industrial protocol for collecting physical data. The protocol supports communication between different field devices and master stations in SCADA systems via TCP/IP encapsulation. In the presented application, the master in Figure 1 uses the DNP3 protocol to collect data from DNP3 outstations located in the field devices. To the best of our knowledge, the presented framework can be adopted to use any other industrial protocols, but DNP3 was chosen for demonstration purposes. DNP3 is one of the primary industrial protocols for SCADA systems and it is commonly found in electric power grid systems [59, 60].

In order to assess the presence of internal anomalies and external intrusion, the cyber and physical data is analyzed using data-driven Anomaly Detection Systems (ADSs). Physical ADS analyzes the data provided by the field devices. Cyber ADS analyzes the packet data collected by the cyber sensor. The result from the physical ADS and the cyber ADS is fed into a cyber-physical metric that provides a quantitative value of the health of the system. The following sections describe the cyber sensor, the anomaly detection, and the cyber-physical metric.

A. CYBER ANOMALY DETECTION
A cyber sensor was designed and implemented to capture and analyze packet data in real-time in order to detect anomalous behavior. As presented in Figure 1, the cyber-sensor is connected to a network switch to monitor the communication between devices in the network. The sensor uses Scapy to capture and analyze the network traffic. The sensor is connected to a switch port analyzer (SPAN port). All incoming and outgoing communication passing through the switch is mirrored to the SPAN port, allowing the cyber-sensor to have access to all packets communicated through the switch. The data acquired through the cyber-sensor is processed in a multi-processing pipeline which is presented in Figure 2. A rolling window of one second is used to analyze sections of data in the communication. To increase throughput, TCP/UDP packet dissection is performed in parallel. Packet level and window level features are extracted from dissected TCP/UDP packets to train data-driven anomaly detection algorithms. PCAP data is stored for further analysis. Alarm notifications are delivered to the Kafka database, which is used to generate notification alerts.

The anomaly detection system of the cyber-sensor was developed to identify any anomalous behaviors in the communication network. To achieve that, the normal behavior of the system is learned by the machine learning algorithm so that any behaviors that are different from previously seen data are flagged as anomalies. The anomalous events are sent to the Kafka database for generating alert notifications.

To train the machine learning models, a set of features were extracted from the stream of raw packet data. The machine learning models are trained using only data from normal operation. As presented in Figure 2, raw data is grouped in windows of one second. TCP/UDP packets are then dissected in parallel. A set of packet features is obtained from the dissection of TCP/UDP packet headers. Then, packet features within each window are used to obtain a set of window features that capture a series of statistical behaviors within the one second window. Appendix A presents the window features extracted from the packet data. During training, the window features characterize the behavior of communications and are used to define the baseline behavior of the system. During deployment, the extracted features are fed into the trained machine learning algorithms (OCSVMs, LOFs, or AEs) for detecting anomalies.

B. PHYSICAL ANOMALY DETECTION
Physical anomaly detection analyzes the physical data collected from a distributed network of sensors to identify situations when the physical state of the system has considerably deviated from expected behavior. Physical data include voltage, current, and power measurements. Data is measured by field devices and sent to a master using the DNP3 protocol. Each field devices hosts a DNP3 outstation that serves the measured data. The master collects the data from all DNP3 outstations and publish it to a Kafka topic. Once the data is located in Kafka, any process with access to the Kafka broker can read the data. In particular, the presented approach uses a process to store the data for offline analysis while a different process analyzes the data in real time.
The physical ADS accesses the physical data by subscribing to the DNP3 Kafka topic. The physical ADS uses one of the previously discussed anomaly detection systems: LOF, OCSVM, or Autoencoders. The physical ADS analyzes all the data collected from the DNP3 outstations. It uses the data directly as it is provided, which in this case consist of voltages, currents, and power measurements. The only pre-processing performed on the data is normalization to zero mean and unit variance when using the Autoencoder model. The ADS is trained exclusively with data recorded during normal operation of the system. Deviations from the expected normal behavior are flagged by the physical ADS and reported to the cyber-physical metric (see Fig. 1).

C. METRIC FOR CYBER-PHYSICAL HEALTH MONITORING

The output of the cyber and physical ADS is used to construct a metric that informs the operator of the cyber-physical health of the system. The objective of the metric is to provide an intuitive set of numbers in the range 0-1 that informs an operator of the cyber-physical health of the system. A tuple (0,0) indicates normal operation while (1,1) indicates a cyber and physical fault. Together, they provide a holistic view of the state of the system. An element of labeled data used for tuning: Given a dataset of labels $Y$ and a set of vectors $A$, $M_c = \sigma(A^T w_c + b_c)$ and $M_p = \sigma(A^T w_p + b_p)$ where $A$, $w_c$, $w_p$, $b_c$, and $b_p$ are parameters used to control the sensitivity of the sigmoid function.

We use the sigmoid function in order to ensure the output of the cyber component $(M_c)$ is constrained to the range of 0-1.

The output of the cyber-physical ADS is used to construct a metric that informs the operator of the cyber-physical health of the system. The objective of the metric is to provide an intuitive set of numbers in the range 0-1 that informs an operator of the cyber-physical health of the system. A tuple (0,0) indicates normal operation while (1,1) indicates a cyber and physical fault. Together, they provide a holistic view of the state of the system. An element of labeled data used for tuning: Given a dataset of labels $Y$ and a set of vectors $A$, $M_c = \sigma(A^T w_c + b_c)$ and $M_p = \sigma(A^T w_p + b_p)$ where $A$, $w_c$, $w_p$, $b_c$, and $b_p$ are parameters used to control the sensitivity of the sigmoid function.

The parameters of the metric are obtained by minimizing the cross-entropy between the output of the metric and a set of labeled data used for tuning: Given a dataset of labels $Y$ and a set of vectors $A$ representing the output of the cyber ADS and physical ADS, the cross-entropy loss is defined as follows:

$$\mathcal{L}(Y, A) = -\frac{1}{D} \sum_{i=1}^{D} H(y, M_{cps}(A_i))$$

where the label $y \in \mathbb{R}^2$ is a tuple of two elements (cyber and physical respectively) where 0 indicates normal behavior and 1 abnormal behavior, $D \in \mathbb{R}$ is the number of samples in the training dataset, $Y$ and $A$ are the ith sample from the dataset, where $Y_i \in \mathbb{R}^2$, $A_i$ is the set of cyber and physical anomaly vectors $(A_c, A_p)$ used to compute the metric $M_{cps}$, where $A_c \in \mathbb{R}^N$ and $A_p \in \mathbb{R}^N$. The parameters obtained by minimizing the cross-entropy include the weights of the weighted average $(w_c, w_p)$, the sensitivity of the sigmoid functions $(k_c, k_p)$, and the shift of the sigmoid functions $(b_c, b_p)$. The minimization is performed using stochastic gradient descent (SGD). A softmax is used in order to ensure that weights $(w_c, w_p)$ meet the constraints of a weighted average. This results in a parameterization of the weights as $w_c = \text{Softmax}(\hat{w}_c)$ and $w_p = \text{Softmax}(\hat{w}_p)$, where $(\hat{w}_c, \hat{w}_p)$ are a set of free parameters that can be directly optimized with SGD. This parameterization ensures that the elements of the weights $(w_c, w_p)$ are in the range of 0-1 and the sum is equal to 1. Figure 3 shows the overview of the metric calculation.
Figure 4: IEEE 33 bus model

Figure 5: Cyber architecture for the IEEE 33 bus model case study

IV. EXPERIMENTS

This section presents the experimental procedure and results for cyber-physical health monitoring. For experimental evaluation, we chose the IEEE 33 bus distribution system, shown in Figure 4. The original version of the IEEE 33 bus distribution system was proposed by Baran & Wu [61]. The IEEE 33 Bus system is a generic model which facilitate customization for more specific studies. It consists of 33 buses and 32 lines and has a voltage of 12.66kV, load size of 3.715MW and 2.3MVar [62]. For our study, the 33 bus model is divided into six ASRs (Aggregated System Resources [63]) which are a logically grouped set of assets shown in Figure 4. The ASRs are connected by lines with breakers that provide protection in case of voltage unbalance or over-current.

Figure 5 shows the configuration of the cyber components in the IEEE 33 bus model. The cyber architecture is composed by field devices, an attack PC, a cyber-sensor, and the cyber-physical health monitoring. All devices are connected to a single switch. The cyber-sensor is connected as shown in Figure 1. We consider two types of field devices: 1) ASR outstations, 2) Line (LN) outstations. Field devices interact directly with the physical system, collecting sensor data and executing control actions. ASR outstations collect voltage, current, power, and reactive power data from all lines in their respective ASR. Line outstations collect data and implement a protection algorithm that checks for over currents, voltage unbalance, and low voltage. Line outstations also open/close a breaker when commanded by a remote master. All outstations communicate sensor and control data using DNP3. For experimental analysis, the physical model is simulated using Simulink, while the communication network is emulated using Mininet [64].

In order to test the presented cyber-physical health monitoring approach, we consider the following scenarios for experimentation and analysis:

- **Normal:** Under this scenario, the system performs under normal operating conditions. The physical devices exhibit normal operating behavior, and the collection of data leads to the establishment of the expected behavior baseline for the anomaly detection. All cyber communication follows the normal behavior pattern.
- **Physical fault:** Under this scenario, the normal operating behavior of physical devices is disrupted due to a fault in the physical system. For the experiments, we simulate line faults (e.g. line-to-ground fault) which trip the protection breakers causing loss of power.
- **Cyber intrusion:** Under this scenario, the normal cyber communication of the system is disrupted due to various cyber-attacks. We executed a series of cyber attack scenarios such as IP scan, ping sweep, port scan, and DOS flood. Physical behavior is not affected during these attacks.
- **Cyber-physical attack:** In this scenario, a cyber attack is executed to disrupt the normal operating behavior of a physical component of the system. A DNP3 command injection is used to close the breakers, causing loss of power in the corresponding ASRs.

A. CYBER ANOMALY DETECTION

This section presents the analysis on the cyber data collected from the cyber sensor and the results from trained anomaly detection algorithms.

As described in the previous section, the algorithms are trained only on normal network communication data collected using the windowing technique. In order to test the performance of trained algorithms, a collection of cyber attacks were executed. The executed attacks are IP scan, ping sweep, port scan, and DOS flood.

Figure 6 shows measurements obtained from the cyber sensor. It shows the average number of packets communicated between two devices during normal communication and during attack communication (IP scan, port scan, ping sweep). The figure uses the IP addresses to represent the devices in the network. The figure shows that the average number of packets communicated between IP addresses is higher during attack communications. Further, during the attack, abnormal communication between the system components and the attacker IP address (30.2.2.151) can be observed. These figures are useful to identify active commu-
During Normal Communication

Master

Attacker

Source IP

Destination IP

Master

During DOS attack Communication

Master

Attacker

Source IP

Destination IP

FIGURE 6: Average number of packets communicated between two devices during normal communication (left) and during attack communication (right)

FIGURE 7: T-SNE embeddings of cyber data for normal, cyber intrusion, and cyber-physical attack.

nications and possible unexpected devices that should not be in the network. The right side color bar represents the rate of packets communicated between two devices. Changes of these color bar also act as an indication for possible abnormal behaviors in the communication.

Figure 7 shows the T-SNE embeddings of cyber features for Normal, cyber intrusion, and cyber physical attack scenarios. T-SNE is an algorithm useful for visualization of high dimensional data in a low dimensional embedded space [65]. The combined view in the figure shows the embeddings for three scenarios in a single plot: normal, cyber intrusion, and cyber-physical attack. We observe a high overlap in the embeddings for the scenarios, especially between normal and cyber-physical attack scenarios. Data from cyber intrusion scenarios also have considerable overlap, however we observe clusters of data from the cyber intrusion scenario, which are considerably separated from data in normal and cyber-physical attack scenarios.

Figure 8 presents an example of how the extracted window feature values change over time during normal communication and attack communication. The figure shows the number of packets over time for normal and attack scenarios. Figure 8b shows the labels of the attacks that were executed during the experimental scenarios. In figure 8b we can clearly observe surges in features as a consequence of the attacks. These peaks provide indication of attack/abnormal behaviors of the system. IP information can also be used to identify anomalous behavior (as shown in Figure 6), however to ensure generalization of the approach and because IP addresses are easy to spoof, IP address information is not directly used as part of the cyber features for the ADS. Figure 8c shows the output of the cyber ADS during the attack scenarios. The results were obtained using an Autoencoder ADS algorithm. The figure shows that the cyber ADS reports anomalies during all attack scenarios, providing evidence that a cyber attack is being executed.

B. PHYSICAL ANOMALY DETECTION

Figure 9 shows the output of the Physical ADS during a physical fault scenario and a cyber-physical attack scenario. The physical ADS uses Voltages, Currents, Power, and Reactive Power from all lines in the system as data features. The figure shows the output of the ADS along with the value of the current in line 1 for illustration purposes. We observe that the physical ADS is able to detect changes during physical fault
and cyber-physical attack scenarios. Although an operator can carefully select threshold values to detect this specific set of anomalies, a data-driven ADS allows to automate the detection process. The data used to train and test the physical ADS included random variations in the power loads with ±10% from the nominal value specified by the IEEE 33 Bus model.

Figure 10 shows a visualization of the physical data for normal, physical fault, and cyber-physical attack scenarios. The visualization uses T-SNE embeddings to visualize the data in two dimensions. The visualization helps us see that physical data from normal scenario is clearly separated from normal, physical fault, and cyber-physical attack scenarios.
C. METRIC FOR CYBER-PHYSICAL HEALTH MONITORING

Figure 11 shows the results of cyber and physical anomaly detection in different scenarios. Results of the cyber ADS are shown above the results of the physical ADS in each scenario. The figure shows the output of cyber and physical ADSs, where 0 means no anomaly and 1 means anomaly detected. We plot one of the cyber and physical features alongside each ADS output for illustration purposes. For the cyber plot, the figure shows the value of packets per second over time with the corresponding output of the cyber ADS. For the physical plot, the figure shows the value of the current $I_a$ in line 1 with the corresponding output of the physical ADS. Figure 11a shows the cyber and physical ADS output from Normal scenario. The physical ADS does not report any anomaly during the normal scenario. The cyber ADS only reports one false positive anomaly during the normal scenario. These false positives are filtered later on by the cyber-physical metric. Figure 11b shows the result for the physical fault scenario. The cyber ADS does not report any anomaly while the physical ADS reports anomalies after the first fault occurs. Figure 11c shows the result for the cyber intrusion scenario. As expected, the physical ADS reports no anomaly. The cyber ADS reports several anomalies when the scan attacks are executed. Figure 11d shows the result for the cyber-physical attack scenario. As expected, both cyber and physical ADS report anomalies when the DNP3 command injection attacks are introduced.

Figure 12 shows a visualization of the cyber-physical metric for normal, physical fault, cyber intrusion, and cyber-physical attack scenarios. A value of 1 represents an anomaly, whereas a value of 0 represents normal behavior. The figure displays the value of the metric computed for each rolling window in the experimental scenarios. The metric values are displayed in a 2D plot, where the x-axis corresponds to the cyber component of the metric, while the y-axis correspond to the physical component of the metric. We observe that for normal scenarios, the cyber-physical metric reports values close to (0,0). Pure physical faults are also clearly distinguished, with the metric output close to (0,1). Cyber intrusion are characterized by most metric values being close to (1,0). Although a few segments of the cyber intrusion have metric values between (0,0) and (0.75, 0), the majority of the intrusion scenarios have high values of $Mc$, with the maximum value of the metric being (0,1), demonstrating that the metric is able to identify the cyber intrusion. Considering the cyber-physical attack scenario, we clearly detect several cyber communication anomalies along with a disruption in the physical system, leading to metric values approaching (1,1). The figure shows that the metric successfully differentiates between normal, physical fault, cyber intrusion, and cyber-physical attack.

D. COMPARATIVE ANALYSIS

For comparative analysis, we considered three types of anomaly detection algorithms: Local Outlier Factor (LOF),...
We tested the performance of the presented metric with several combinations of anomaly detection algorithms for cyber and physical ADS. We evaluated the performance of the metric on distinguishing between the four experimental scenarios: normal, physical fault, cyber intrusion, cyber-physical attack. Table 2 shows a comparative analysis for different combinations of ADS algorithms used with the cyber-physical health monitoring metric. The accuracy measures the ability of the metric with different ADS algorithms to differentiate between the four types of experimental scenarios. For example, if the metric reports values below (0.5, 0.5), these are considered as part of a normal scenario. The accuracy measures the ratio of outputs correctly mapped to the respective scenario category. The accuracy is measured using k-fold validation, and we report average accuracy values for training and testing datasets. The data for each fold is selected by keeping data from individual runs of the scenarios together, i.e., data from a contiguous run of a scenario is not split, ensuring that contiguous data reside either completely in training or completely in testing folds. Table 2 shows the accuracy of the metric when using different combinations of algorithms for cyber ADS and physical ADS. Compared with the results in Table 1, which evaluates the ADS models separately, Table 2 shows the accuracy obtained with the presented metric, which uses the output of both cyber and physical ADS over a window of time. For Table 2, we use the output of the cyber ADS and physical ADS in a window of N=120 seconds to compute the metric (see Eq. 2 and 4).

Table 2 shows that OCSVM provided better performance when used for physical ADS, while LOF performed better when used for cyber ADS. AE performed well for both cyber and physical ADS. The two combinations with the highest accuracy were (AE, AE) and (AE, OCSVM).

Table 2 shows that a metric that uses AE for cyber and physical ADS provides the highest accuracy. When compared with the results in Table 1, we observe that AE also provided the lowest FPR, when evaluating cyber and physical ADS independently. Although OCSVM and LOF provided higher TPR than AE, the higher accuracy of the metric obtained with AE (Table 2) suggests that lower FPR are preferable to higher TPR for this application. By using and combining the outputs of the individual ADS systems over the last N seconds, Table 2 shows that the metric is able to identify scenarios with high accuracy, even when the TPR of individual ADSs are relatively low.

Figure 13 shows the confusion matrix obtained after averaging the results of k-fold validation on the testing data. The figure shows the results for the cyber-physical metric with AE for both cyber and physical ADS, which is the best performing configuration in the comparative analysis. The figure shows that the metric correctly characterizes all normal and fault samples as part of normal and fault scenarios, respectively. For cyber intrusion samples, 97% of samples are correctly characterized as part of the intrusion scenarios, with the remaining characterized as normal. According to the obtained results, the most challenging scenario is the cyber-physical attacks with 95% accuracy, with a small percentage of samples characterized as part of fault and attack scenarios.

As shown in Figures 10 and 7, there is a larger overlap in cyber features between scenarios than in physical data, which illustrates why cyber intrusion and cyber-physical attacks scenarios are more difficult to characterize. The results in figure 13 demonstrate that the presented approach is able to use the output of both cyber and physical ADS to successfully differentiate between scenarios that otherwise have overlapping representations, as illustrated in figures Figure 10 and Figure 7.
V. CONCLUSIONS

This paper presented an approach for data-driven correlation of cyber and physical anomalies for holistic system health monitoring of cyber physical systems. We performed real-time data acquisition and management of both cyber and physical data using a publisher/subscriber model, which can consolidate data coming from different protocols, communication media, and sensors. The collected cyber and physical data were analyzed using data-driven anomaly detection systems that employed machine learning algorithms to identify anomalous data. We used three unsupervised machine learning algorithms and performed a comparative analysis of anomaly detection between them. The best performance for anomaly detection was obtained using Autoencoders for both cyber and physical ADSs. Cyber and physical ADSs were used to introduce a metric for health monitoring that provides a holistic view of the state of the system. We tested our approach on the IEEE-33 bus model under four scenarios: normal, physical fault, cyber intrusion, and cyber-physical attack. The presented approach was able to distinguish between normal state, physical faults, cyber intrusion, and cyber-physical attacks. Future work will explore more elaborate models for combining cyber and physical ADSs based on the presented foundational work, with a special focus on maintaining interpretability and limited use of labeled data.

APPENDIX. A: WINDOW BASED TCP PACKET FEATURES

Table 3 presents the set of cyber features used for the cyber ADS presented in section III-A. Features are computed using packet windows of 1 second.
REFERENCES

[1] Cyber-physical systems (cps). [Online]. Available: https://www.nsf.gov/pubs/2021/nsf21551/nsf21551.htm.

[2] K. Amarasinghe, C. Wickramasinghe, D. Marino, C. Rieger, and M. Manic, “Framework for data driven health monitoring of cyber-physical systems,” in 2018 Resilience Week (RW), 2018, pp. 25–30. DOI: 10.1109/RWEEK.2018.8473535.

[3] D. L. Marino, C. S. Wickramasinghe, K. Amarasinghe, H. Challa, P. Richardson, A. A. Jillepalli, B. K. Johnson, C. Rieger, and M. Manic, “Cyber and physical anomaly detection in smart-grids,” in 2019 Resilience Week (RWS), vol. 1, 2019, pp. 187–193. DOI: 10.1109/RWS47064.2019.8972003.

[4] Y. Guan and X. Ge, “Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks,” IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 1, pp. 48–59, 2018. DOI: 10.1109/TISP.2017.2749959.

[5] B.-M. Cho, M.-S. Jang, and K.-J. Park, “Channel-aware congestion control in vehicular cyber-physical systems,” IEEE Access, vol. 8, pp. 73193–73203, 2020. DOI: 10.1109/ACCESS.2020.2987416.

[6] M. Eckhart, A. Ekelhart, and E. WeiPfl, “Enhancing cyber situational awareness for cyber-physical systems through digital twins,” in 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1222–1225. DOI: 10.1109/ETFA.2019.8869197.

[7] H. Muccini and M. Sharaf, “Caps: Architecture description of situational aware cyber physical systems,” in 2017 IEEE International Conference on Software Architecture (ICSA), 2017, pp. 211–220. DOI: 10.1109/ICSA.2017.21.

[8] L. Shangguan and S. Gopalswamy, “Health monitoring for cyber physical systems,” IEEE Systems Journal, vol. 14, no. 1, pp. 1457–1467, 2020. DOI: 10.1109/JSYST.2019.2922982.

[9] G. Wu, J. Sun, and J. Chen, “A survey on the security of cyber-physical systems,” Control Theory and Technology, vol. 14, pp. 2–10, 2016.

[10] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, “Anomaly detection based on zone partition for security protection of industrial cyber-physical systems,” IEEE Transactions on Industrial Electronics, vol. 65, no. 5, pp. 4257–4267, 2018. DOI: 10.1109/TIE.2017.2772190.

[11] M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, and I. Khalil, “An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems,” IEEE Transactions on Sustainable Computing, 2019.

[12] A. Bezemskij, G. Loukas, R. J. Anthony, and D. Gan, “Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle,” in 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS), IEEE, 2016, pp. 61–68.

[13] M. Raciti and S. Nadjm-Tehrani, “Embedded cyber-physical anomaly detection in smart meters,” in Critical Information Infrastructures Security, B. M. Hämmerli, N. Kalstad Svendsen, and J. Lopez, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 34–45, ISBN: 978-3-642-41485-5.

[14] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, “Anomaly detection based on zone partition for security protection of industrial cyber-physical systems,” IEEE Transactions on Industrial Informatics, vol. 65, no. 5, pp. 4257–4267, 2017.

[15] S. Krishnamurthy, S. Sarkar, and A. Tewari, “Scalable anomaly detection and isolation in cyber-physical systems using bayesian networks,” in Dynamic Systems and Control Conference, American Society of Mechanical Engineers, vol. 46193, 2014, V002T26A006.

[16] F. Skopik, M. Landauer, M. Wurzenberger, G. Vormay, J. Milosevic, J. Fabini, W. Prüggler, O. Kruschitz, B. Widmann, K. Truchtenhanner, et al., “Synergy: Cross-correlation of operational and contextual data to timely detect and mitigate attacks to cyber-physical systems,” Journal of Information Security and Applications, vol. 54, p. 102544, 2020.

[17] D. L. Marino, C. S. Wickramasinghe, K. Amarasinghe, H. Challa, P. Richardson, A. A. Jillepalli, B. K. Johnson, C. Rieger, and M. Manic, “Cyber and physical anomaly detection in smart-grids,” in 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1222–1225. DOI: 10.1109/ETFA.2019.8869197.

[18] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, “Generalization of deep learning for cyber-physical system security: A survey,” in IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2018, pp. 745–751.

[19] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. D. Yao, “Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities,” ACM Comput. Surv., vol. 54, no. 5, May 2021, ISSN: 0360-0300. DOI: 10.1145/3453155. [Online]. Available: https://doi.org/10.1145/3453155.

[20] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges,” computers & security, vol. 28, no. 1-2, pp. 18–28, 2009.

[21] D. Yang, A. Usynin, and J. W. Hines, “Anomaly-based intrusion detection for scada systems,” in 5th intl. topical meeting on nuclear plant instrumentation, control and human machine interface technologies (npic&hmit 05), 2006, pp. 12–16.

[22] M. Mantere, M. Sailio, and S. Noponen, “Network traffic features for anomaly detection in specific indus-
trial control system network,” *Future Internet*, vol. 5, no. 4, pp. 460–473, 2013.

[23] I. Nai Fovino, A. Carcano, M. Masera, and A. Trombetta, “An experimental investigation of malware attacks on scada systems,” *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 139–145, 2009, ISSN: 1874-5482. DOI: https://doi.org/10.1016/j.ijcip.2009.10.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548209000419.

[24] R. Leszczyna, I. N. Fovino, and M. Masera, “Simulating malware with malsim,” *Journal in computer virology*, vol. 6, no. 1, pp. 65–75, 2010.

[25] E. Ciancamerla, M. Minichino, and S. Palmieri, “Modeling cyber attacks on a critical infrastructure scenario,” in *IISA 2013*, 2013, pp. 1–6. DOI: 10.1109/IISA.2013.6623699.

[26] J. M. Moya, A. Araujo, Z. Bankovic, J.-M. De Goyeneche, J. C. Vallejo, P. Malagon, D. Villanueva, D. Fraga, E. Romero, and J. Blesa, “Improving security for scada sensor networks with reputation systems and self-organizing maps,” *Sensors*, vol. 9, no. 11, pp. 9380–9397, 2009, ISSN: 1424-8220. DOI: 10.3390/s91109380. [Online]. Available: https://www.mdpi.com/1424-8220/9/11/9380.

[27] Dong Jin, D. M. Nicol, and Guanhua Yan, “An event buffer flooding attack in dnp3 controlled scada systems,” in *Proceedings of the 2011 Winter Simulation Conference (WSC)*, 2011, pp. 2614–2626. DOI: 10.1109/WSC.2011.6147969.

[28] I. Nai Fovino, A. Coletta, A. Carcano, and M. Masera, “Critical state-based filtering system for securing scada network protocols,” *IEEE Transactions on Industrial Electronics*, vol. 59, no. 10, pp. 3943–3950, 2012. DOI: 10.1109/TIE.2011.2181132.

[29] J. D. Markovic-Petrovic and M. D. Stojanovic, “Analysis of scada system vulnerabilities to ddos attacks,” in *2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*, vol. 02, 2013, pp. 591–594, DOI: 10.1016/TELSKS.2013.6704448.

[30] P. Maynard, K. McLaughlin, and B. Haberler, “Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks,” in *2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014)* 2, 2014, pp. 30–42.

[31] W. Li, L. Xie, Z. Deng, and Z. Wang, “False sequential logic attack on scada system and its physical impact analysis,” *Computers & Security*, vol. 58, pp. 149–159, 2016, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2016.01.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740481600031.

[32] G. Hug and J. A. Giampapa, “Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012. DOI: 10.1109/TSG.2012.2195338.

[33] Y. Mo, R. Chabukswar, and B. Sinopoli, “Detecting integrity attacks on scada systems,” *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014. DOI: 10.1109/TCST.2013.2280899.

[34] J. Mao, H. Wang, and B. F. Spencer Jr, “Toward data anomaly detection for automated structural health monitoring: Exploiting generative adversarial nets and autoencoders,” *Structural Health Monitoring*, p. 1475921709424601, 2020.

[35] Z. Tang, Z. Chen, Y. Bao, and H. Li, “Convolutional neural network-based data anomaly detection method using multiple information for structural health monitoring,” *Structural Control and Health Monitoring*, vol. 26, no. 1, e2296, 2019.

[36] Y. Zhang, I. L. Yen, F. B. Bastani, A. T. Tai, and S. Chau, “Optimal adaptive system health monitoring and diagnosis for resource constrained cyber-physical systems,” in *2009 20th International Symposium on Software Reliability Engineering*, 2009, pp. 51–60. DOI: 10.1109/ISSRE.2009.21.

[37] Y. Zhang, I.-L. Yen, F. B. Bastani, A. T. Tai, and S. Chau, “Optimal adaptive system health monitoring and diagnosis for resource constrained cyber-physical systems,” in *2009 20th International Symposium on Software Reliability Engineering*, IEEE, 2009, pp. 51–60.

[38] G. Hackmann, W. Guo, G. Yan, Z. Sun, C. Lu, and S. Dyke, “Cyber-physical codesign of distributed structural health monitoring with wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 63–72, 2014. DOI: 10.1109/TPDS.2013.30.

[39] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, “Scikit-learn: Machine learning in Python,” *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[40] D. Kwon, H. Kim, J. Kim, S. Suh, I. Kim, and K. Kim, “A survey of deep learning-based network anomaly detection,” *Cluster Computing*, vol. 22, Jan. 2019. DOI: 10.1007/s10586-017-1117-8.

[41] S. Agrawal and J. Agrawal, “Survey on anomaly detection using data mining techniques,” *Procedia Computer Science*, vol. 60, pp. 708–713, 2015, Knowledge-Based and Intelligent Information & Engineering Systems 19th Annual Conference, KES-2015, Singapore, September 2015 Proceedings, ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2015.08.220. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915023479.
[42] S. Eltanbouly, M. Bashendy, N. AlNaimi, Z. Chkiban, and A. Erbad, “Machine learning techniques for network anomaly detection: A survey,” in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 156–162. DOI: 10.1109/ICIoT48696.2020.9089465.

[43] O. Alghushairy, R. Alsini, T. Soule, and X. Ma, “A review of local outlier factor algorithms for outlier detection in big data streams,” Big Data and Cognitive Computing, vol. 5, no. 1, 2021, ISSN: 2504-2289. DOI: 10.3390/bdcc5010001. [Online]. Available: https://www.mdpi.com/2504-2289/5/1/1.

[44] M. Längkvist, L. Karlsson, and A. Loutfi, “A review of unsupervised feature learning and deep learning for time-series modeling,” Pattern Recognition Letters, vol. 42, pp. 11–24, 2014.

[45] C. S. Wickramasinghe, D. L. Marino, and M. Manic, “Resnet autoencoders for unsupervised feature learning from high-dimensional data: Deep models resistant to performance degradation,” IEEE Access, vol. 9, pp. 40,511–40,520, 2021.

[46] B. Schölkopf, R. C. Williamson, A. J. Smola, J. Shawe-Taylor, J. C. Platt, et al., “Support vector method for novelty detection,” in NIPS, Citeseer, vol. 12, 1999, pp. 582–588.

[47] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, “Estimating the support of a high-dimensional distribution,” Neural Computation, vol. 13, no. 7, pp. 1443–1471, 2001.

[48] M. Amer, M. Goldstein, and S. Abdennadher, “Enhancing one-class support vector machines for unsupervised anomaly detection,” in Proceedings of the ACM SIGKDD Workshop on Outlier Detection and Description, ser. ODD ’13, Association for Computing Machinery, 2013, 8–15, ISBN: 9781450323325, DOI: 10.1145/2500853.2500857. [Online]. Available: https://doi.org/10.1145/2500853.2500857.

[49] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, “High-dimensional and large-scale anomaly detection using a linear one-class svm with deep learning,” Pattern Recognition, vol. 58, pp. 121–134, 2016, ISSN: 0031-3203. DOI: https://doi.org/10.1016/j.patcog.2016.03.028. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0031320316300267.

[50] K.-L. Li, H.-K. Huang, S.-F. Tian, and W. Xu, “Improving one-class svm for anomaly detection,” in Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 03EX693), IEEE, vol. 5, 2003, pp. 3077–3081.

[51] M. Amer, M. Goldstein, and S. Abdennadher, “Enhancing one-class support vector machines for unsupervised anomaly detection,” in Proceedings of the ACM SIGKDD workshop on outlier detection and description, 2013, pp. 8–15.

[52] R. Perdisci, G. Gu, and W. Lee, “Using an ensemble of one-class svm classifiers to harden payload-based anomaly detection systems,” in Sixth International Conference on Data Mining (ICDM’06), IEEE, 2006, pp. 488–498.

[53] M. Alshawabkeh, B. Jang, and D. Kaeli, “Accelerating the Local Outlier Factor Algorithm on a GPU for Intrusion Detection Systems,” in Proceedings of the 3rd Workshop on General-Purpose Computation on Graphics Processing Units, ser. GPGPU-3, Pittsburgh, Pennsylvania, USA: Association for Computing Machinery, 2010, 104–110, ISBN: 9781605589350. DOI: 10.1145/1735688.1735707. [Online]. Available: https://doi.org/10.1145/1735688.1735707.

[54] W. Wang and P. Lu, “An efficient switching median filter based on local outlier factor,” IEEE Signal Processing Letters, vol. 18, no. 10, pp. 551–554, 2011. DOI: 10.1109/LSP.2011.2162583.

[55] R. Sandhya, J Prakash, and B. V. Kumar, “Comparative analysis of clustering techniques in anomaly detection wind turbine data,” Journal of Xi’an University of Architecture & Technology, vol. 12, no. 3, pp. 5684–5694, 2020.

[56] M. Ahmed, A. Anwar, A. N. Mahmood, Z. Shah, and M. J. Maher, “An investigation of performance analysis of anomaly detection techniques for big data in scada systems,” EAI Endorsed Trans. Indust. Netw. & Intellig. Syst., vol. 2, no. 3, e5, 2015.

[57] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, “LoF: Identifying density-based local outliers,” in Proceedings of the 2000 ACM SIGMOD international conference on Management of data, 2000, pp. 93–104.

[58] C. Zhou and R. C. Paffenroth, “Anomaly detection with robust deep autoencoders,” in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ser. KDD ’17, Halifax, NS, Canada: Association for Computing Machinery, 2017, 665–674, ISBN: 9781450348874.

[59] R. Amoah, S. Camtepe, and E. Foo, “Securing dnp3 broadcast communications in scada systems,” IEEE Transactions on Industrial Informatics, vol. 12, no. 4, pp. 1474–1485, 2016.

[60] S. East, J. Butts, M. Papa, and S. Shenoi, “A taxonomy of attacks on the dnp3 protocol,” in Critical Infrastructure Protection III, C. Palmer and S. Shenoi, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 67–81.

[61] S. Hacopian Dolatabadi, M. Ghorbanian, P. Siano, and N. Hatziargyriou, “An enhanced ieee 33 bus benchmark test system for distribution system studies,” IEEE Transactions on Power Systems, vol. PP, pp. 1–1, Nov. 2020. DOI: 10.1109/TPWRS.2020.3038030.

[62] V. Vita, “Development of a decision-making algorithm for the optimum size and placement of distributed generation units in distribution networks,” Energies,
B. Vaagensmith, V. K. Singh, R. Ivans, D. L. Marino, C. S. Wickramasinghe, J. Lehmer, T. Phillips, C. Rieger, and M. Manic, “Review of design elements within power infrastructure cyber–physical test beds as threat analysis environments,” Energies, vol. 14, no. 5, 2021, ISSN: 1996-1073. DOI: 10.3390/en14051409. [Online]. Available: https://www.mdpi.com/1996-1073/14/5/1409.

B. Lantz, B. Heller, and N. McKeown, “A network in a laptop: Rapid prototyping for software-defined networks,” in Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, ser. Hotnets-IX, Monterey, California: Association for Computing Machinery, 2010, ISBN: 9781450304092. DOI: 10.1145/1868447.1868466. [Online]. Available: https://doi.org/10.1145/1868447.1868466.

L. Van der Maaten and G. Hinton, “Visualizing data using t-sne,” Journal of machine learning research, vol. 9, no. 11, 2008.

BILLY TSOUVALAS received his B.Sc. in Electrical and Computer Engineering and M.Sc. in Computer Science and Electronics, with a concentration on Computer and Information Security from the University of Patras, Greece. He is an IBM Certified Cybersecurity Analyst and his areas of interest include: Malware Analysis, Detection, and Classification, Critical Infrastructure, Cybersecurity, Machine Learning, Generative Adversarial Learning, Network Security, Intrusion Detection, and Forensics.

MILOS MANIC (SM’06-M’04-StM’96) is a Professor with the Computer Science Department and Director of VCU Cybersecurity Center at Virginia Commonwealth University. He completed over 40 research grants in data mining and machine learning applied to cyber security, critical infrastructure protection, energy security, and resilient intelligent control. Dr. Manic has given over 40 invited talks around the world, authored over 200 refereed articles in international journals, books, and conferences, holds several U.S. patents and has won 2018 R&D 100 Award for Autonomic Intelligent Cyber Sensor (AICS), one of top 100 science and technology worldwide innovations in 2018. He is an inductee of US National Academy of Inventors (class of 2019) and a Fellow of Commonwealth Cyber Initiative (specialty in AI & Cybersecurity). He is an IEEE Fellow, recipient of IEEE IES 2019 Anthony J.Hornfeck Service Award, 2012 J. David Irwin Early Career Award, 2017 IEM Best Paper Award and serves as an associate editor of Transactions on Industrial Informatics, Open Journal of Industrial Electronics Society, and is IES Officer and Senior AdCom member. He served as associate editor of Trans. on Industrial Electronics, was a founding chair of IEEE IES Technical Committee on.

CHATHURIKA S. WICKRAMASINGHE received her B.Sc. degree in computer science from the University of Peradeniya, Sri Lanka, in 2016. She is currently working as a research assistant while reading for her doctoral degree in computer science at Virginia Commonwealth University, Richmond. Her research interests include machine learning, unsupervised learning, explainable AI, generalization and visual data mining.

DANIEL L. MARINO received his B.Eng. in automation engineering from La Salle University, Colombia, in 2015. He is currently a research assistant and a doctoral student at Virginia Commonwealth University. His research interests include stochastic modeling, deep learning and optimal control.

CRAIG RIEGER (SM’08) received the B.S. and M.S. degrees in chemical engineering from Montana State University, Bozeman, MT, USA, in 1983 and 1985, respectively, and the Ph.D. degree in engineering and applied science from Idaho State University, Pocatello, ID, USA, in 2008. He is the Chief Control Systems Research Engineer and a Directorate Fellow with Idaho National Laboratory (INL), Idaho Falls, ID, pioneering interdisciplinary research in the areas of nuclear security, Machine Learning, Generative Adversarial Learning, Network Security, Intrusion Detection, and Forensics.

BILL Y TSOUVALAS received his B.Sc. in Electrical and Computer Engineering and M.Sc. in Computer Science and Electronics, with a concentration on Computer and Information Security from the University of Patras, Greece. He is an IBM Certified Cybersecurity Analyst and his areas of interest include: Malware Analysis, Detection, and Classification, Critical Infrastructure, Cybersecurity, Machine Learning, Generative Adversarial Learning, Network Security, Intrusion Detection, and Forensics.