Cyber and Physical Anomaly Detection in Smart-Grids

Daniel L. Marino [1], Chathurika S. Wickramasinghe [1], Kasun Amarasinghe [1], Hari Challa [2], Philip Richardson [2], Ananth A. Jillepalli [2], Brian K. Johnson [2], Craig Rieger [3], Milos Manic [1]
[1] *Virginia Commonwealth University*, Richmond, VA, USA
[2] *University of Idaho*, Moscow, Idaho, USA
[3] *Idaho National Laboratory*, Idaho Falls, Idaho, USA
{marinodl,brahmanacsw,amarasinghek}@vcu.edu, {challa, ajillepalli, bjohnson}@uidaho.edu,
craig.rieger@inl.gov, misko@ieee.org

***Abstract*—The inclusion of Information and Communication Technologies (ICTs) in industrial control systems (ICSs) has opened ICSs to several attack vectors, which are increasingly targeting critical infrastructure. Accurate detection and distinction between benign physical disturbances, malicious cyber-attacks, and malicious physical-attacks are necessary to protect critical infrastructure. While cyber sensors provide a useful tool to identify and mitigate cyber attacks, they often ignore the physical behavior of the system at hand. In this paper, we present a cyber-physical sensor called IREST (ICS Resilient Security Technology). The sensor takes a holistic approach in detecting anomalies by considering both cyber and physical disturbances in a complex system. The sensor was tested under different cyber-physical scenarios using the Idaho CPS SCADA Cybersecurity (ISAAC) testbed. The test scenarios capture different operational states of the CPS testbed, including various cyber and physical anomalies. The experiments show that the IREST sensor is able to detect both cyber and physical anomalies. The sensor has the benefit that training requires only normal data and is able to detect disturbances that have not been seen before. The presented approach provides a scalable framework for cyber-physical security research that can be expanded in the future.**

***Index Terms*—Cyber-physical systems, Machine Learning, Anomaly Detection, SCADA**

Abbreviations

ML - Machine Learning
ADS - Anomaly Detection System
CPS(s) - Cyber Physical Systems
HMI - Human Machine Interface
DNP3 - Distributed Network Protocol
HIL - Hardware In the Loop
ICS(s) - Industrial Control Systems
IREST - ICS Resilient Security Technology
ISAAC - Idaho CPS SCADA Cybersecurity testbed
SCADA - Supervisory Control and Data Acquisition
PCA - Principal Component Analysis
RTDS - Real Time Digital Simulator
WAN - Wide Area Network

I. Introduction

Cyber-physical systems (CPS) are a collection of interconnected physical and computing resources working together to accomplish a specific task [1]. These systems integrate computations, communications, control, and physical processes into a single system [1]. The operations of these systems are coordinated, controlled, integrated, and monitored by a computing and communication core [2]. CPS have been increasingly adopted in several industries in order to maximize profit, quality and resiliency [3]. This integration is particularly notable in the development of the smart-grid with the continuous integration of supervisory control and data acquisition (SCADA) industrial control systems (ICSs) [3].

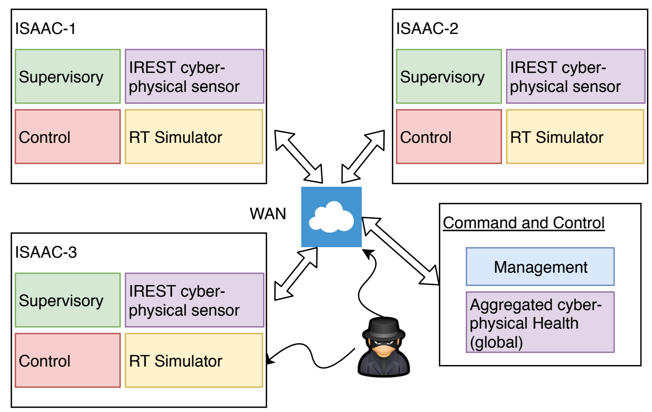


Fig. 1: High-level representation of IREST's implementation in ISAAC testbed

CPSs rely on information and communication technologies (ICTs) to support communication, control and supervisory tasks [4]. The inclusion of ICTs in ICSs has opened ICSs to numerous new attack vectors, targeting critical infrastructure [4]. Accurate detection and distinction between benign physical anomalies, malicious cyber-attacks, and malicious physical-attacks is necessary to protect critical infrastructure. To accurately identify anomalies in CPSs, we need to devise a novel strategy that considers both physical and cyber components in the system.

Traditional ad-hoc algorithms have limitations when dealing with complex and unexpected situations, like the ones in current CPS environments [5]. Autonomous data processing, based on machine learning (ML), seems to be a promising approach for characterizing CPSs to identify cyber-physical anomalies. ML approaches have been introduced in CPSs for performing health assessment and prognostics within them [5]. ML models can learn complex relationships from large quantities of data. These models can be used to create intelligent, adaptive, and accurate characterizations for CPSs and can be used to identify unexpected cyber-physical anomalies. To achieve this goal, ML models require representative data for training, development, testing, and benchmarking.

In this paper, we present a machine learning approach for detection of cyber and physical anomalies in CPSs. We present a cyber-physical sensor called IREST (ICS Resilient Security Technology). The sensor uses several ML models to characterize the CPS and detect both cyber and physical anomalies. We used the Idaho CPS SCADA Cybersecurity (ISAAC) testbed [6], [7] to collect data for development, training and testing of the ML-based anomaly detection algorithms used in the IREST sensor. The ISAAC testbed uses hardware-in-the-loop (HIL) to include industrial-grade hardware and protocols to simulate an industrial control system. Supervised as well as unsupervised ML models were implemented and tested within the proposed ADS system.

The proposed IREST cyber-physical sensor considers both cyber and physical features to construct a complete representation of the system. Each IREST sensor performs deep packet inspection on ISAAC simulation data. The results of deep packet inspection are used to learn a local ML model of the system. The ML model characterizes the normal behavior of the system, which is used to detect anomalous behavior.

For scalability, each IREST sensor is designed to learn a local model of the system. Future work will be conducted on the communication and integration of several sensors. Figure 1 presents a high-level representation of IREST's implementation in the ISAAC testbed. ISAAC uses a WAN emulator to represent large scale distributed systems in a real life ICS deployment environment. For the tests presented in this manuscript, we use several cyber-physical anomalies.

The paper has the following contributions:

- We present a ML approach for detecting cyber and physical anomalies in CPSs.
- We use the ML anomaly detection approach to design the IREST sensor: a cyber-physical sensor with capability to detect anomalies by considering both cyber and physical disturbances in a complex system.
- We present a testbed configuration to develop and test the cyber-physical anomaly detection approach.

The rest of the paper is organized as follows: Section II presents the related work; Section III describes the configuration of ISAAC testbed used; Section IV present our test scenarios; Section V describes the IREST cyber-physical sensor; Section VI presents the IREST anomaly detection results. Conclusion, a list of frequently used abbreviations and a complete list of references follow.

II. Related Work

The increased dependency of critical infrastructure organizations on CPSs have made them vulnerable to various kind of attacks such as replacement or removal of information, interception, malware releases and physical attacks [1], [8]. Machine Learning based approaches have been shown to be a viable solution to protect these systems by performing various security related actions such as anomaly detection, intrusion detection, access control, malware detection and classification [1].

Jones et al. have proposed a unsupervised learning algorithm to classify system output data into two categories: normal and anomalous [9]. They have used a signal temporal logic formula, to to express system properties of their system and, support vector machine classifier (SVM) to build their ADS.

Gob et al. have proposed a novel unsupervised anomaly detection system to identify cyber attacks [10]. They have used Recurrent Neural Network (RNN) which is a widely using machine learning algorithm to deal with time series data. They have tested their method on a complex dataset which is collected through a Secure Water Treatment Testbed (SWaT). Their system is capable of identifying anomalies as well as the sensor in CPS that was attacked.

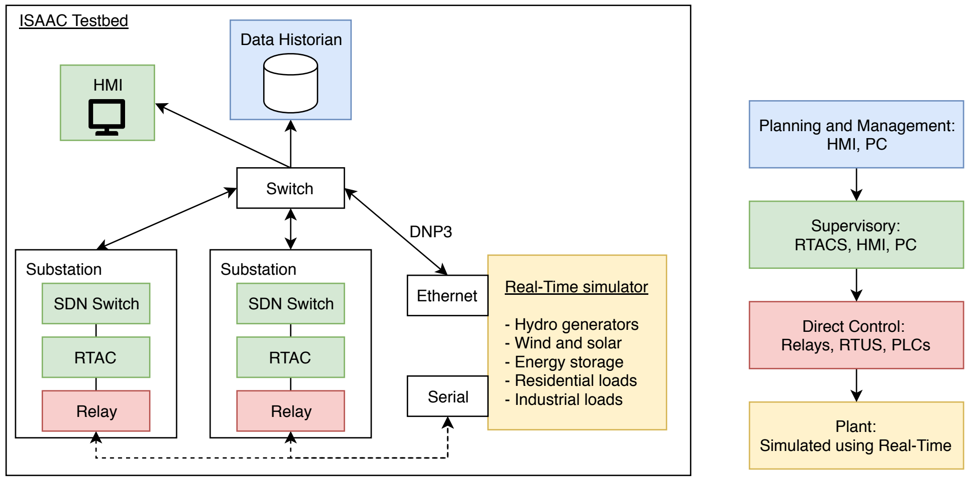
Abokifa et al. have demonstrated how smart water infrastructures are prone to cyber-physical attacks, that can lead to operational and assets damage [11]. They have developed a system to identify different types of anomalies in a distribution system. They used an artificial neural network based approach to detect abnormal operation behaviors in the system. Further, dimensional reduction techniques such as principal component analysis was used to decompose the real-time monitoring and control data.

III. Configuring ISAAC Testbed

ML models used in IREST require representative data for training, development, testing, and benchmarking. We obtain such data from the Idaho CPS SCADA Cybersecurity (ISAAC) testbed. The design and architecture of ISAAC testbed has been previously reported [6], [7]. The abilities of ISAAC include being able to simulate CPS environments under normal and cyber-physical abnormal scenarios. ISAAC is a reconfigurable testbed which can be deployed using different configurations for different projects. Here we discuss the ISAAC testbed configuration deployed for IREST research.

Figure 2 presents an overview of the ISAAC simulation components involved in IREST research. For accuracy, it is imperative that the testbed data is representative of real-world industrial systems. As such, we configured ISAAC to include industrial-grade hardware and protocols. We used Hardware-in-the-loop (HIL) to simulate a supervisory control and data acquisition (SCADA) industrial control system (ICS). A real-time digital simulator (RTDS) provides a cost-effective approach to simulate complex physical processes.

We configured ISAAC to emulate an enterprise industrial control system architecture consisting of: 1) several substations with automation controllers, relays, substation computers,



(a) (b)

Fig. 2: ISAAC's Simulation Components. a) Testbed architecture, b) Distributed Control System (DCS) Layers

SDN switches and network gateways; 2) a control center with SCADA HMI, data historian, and security servers; and 3) a real-time power-system simulation using an RTDS with DNP3 communication. The system components are interconnected via three software defined networking switches and two regular managed switches. A detailed description and a network diagram of the connections between the network siwtches can be found in previous publications [6], [7]. Synchronization of data between these components is managed by three Axions with RTACs (Real Time Automation Controllers).

The RTDS simulation of the micro-grid includes several components found in today's generation and distribution networks, including but not limited to: hydro generators; wind and solar; storage sources; variable residential loads; industrial loads. As such, we are able to collect representative data of cyber and physical interactions in a SCADA ICS environment. An IREST sensor is connected to ISAAC to record packet data during normal and abnormal operations. Abnormal operations are operations that have either physical or cyber disturbances. The IREST learns a representation of the CPS using both physical and cyber features, which are extracted from packet data. An attacker computer is connected to the testbed in order to execute a predefined set of attacks on the network. This allows us to simulate cyber anomalies on the grid and collect data to characterize their behavior.

We configured ISAAC to be able to scale the environment between small and large scale deployment methods. We accomplished this scalability by virtualizing several computers involved in the control center module of the testbed. The computers that were virtualized retain their ability to function as if they were real devices. Virtualization also allowed us to create multiple copies of the same type of devices. For example, by virtualizing the HMI computer, we are able to create tens of HMI computers to emulate a large organization that uses tens of HMIs. Similarly, scaling down is also made easy by virtualizing some computers. Note that the virtualization does neither extend nor affect HIL (Hardware In the Loop) devices.

IV. Simulation Scenarios for Testing

We designed our test scenarios to be representative of realistic normal and abnormal cyber-physical scenarios in complex CPS environments. Defining these scenarios was performed in an iterative way. Starting from a basic set of scenarios, we perform exploratory data-analysis followed by ML model training and refinement to characterize the given scenarios. Then, we identify data gaps to update the list of target scenarios. This approach provides a guided data-driven exploratory approach to define interesting and representative scenarios.

The following are our current test scenarios. We intend to expand this list in the future to include scenarios of higher complexity across both normal and abnormal scenarios.

Normal Operations Scenarios

- Normal 1 (Typical Weekday): Commercial and residential loads, both increase and decrease from 9 am to 5pm respectively.
- Normal 2 (Typical Weekend): Commercial loads do not increase between 9 am and 5 pm.
- Normal 3 (Early Workday): Commercial loads start increasing at 4 am and turn off at 1 pm.

Abnormal Cyber Scenarios

- Scanning & reconnaissance: Ping sweeping, port scanning, and network mapping.
- Replay attacks: Record data for X seconds, modify the destination header, and replay the recorded packets at a higher frequency.
- DOS attacks: Denial of service attacks by flooding the server with billions of ping requests.

Abnormal Physical Scenarios

- Physical 1: Load breakers are opened at 10 am and 7 pm.
- Physical 2: Generators turned off at 9 am and 6 pm.

TABLE I: TCP packet-level features

Feature Name	Feature Description
Timestamp	Time of recording
Sequence Number	Sequence number of the packet
Acknowledgement Number	Acknowledgement number of the packet
Protocol type	Indicate the protocol type which used to send data
Window Size	The maximum amount of data that the receiver can accept
Data length	Indicated the length of the entire IP packet including the header and data segment
Control Flag Code	Indicates connection states
Source IP address	The IP address of the source
Destination IP address	The IP address of the destination
Source port	Sending port
Destination port	Receiving port
Time to live	Life span of the packet
Urgent	Whether the packet data is urgently required or not

V. IREST CYBER-PHYSICAL SENSOR

Here we discuss the proposed IREST cyber-physical sensor for ML-based anomaly detection in CPSs. Figure 3 illustrates the sensor connected to a CPS, presenting an overview the components of the system. The IREST sensor has the following main components:

- Packet sniffer: for data collection.
- Cyber-features extractor: to characterize the cyber behavior.
- DNP3 parser: to extract physical data.
- ML-based anomaly detection algorithm: to detect abnormal behavior in the system.

The following sections present the cyber and physical characterization of the CPS.

A. Cyber Characterization

Cyber features: We used a packet sniffer to collect the entire set of packets that are exchanged in the network. The cyber data is acquired from TCP packets using the transport layer attributes. A set of TCP packet level features are extracted using the SCAPY library [12]. SCAPY is a powerful interactive packet manipulation program. It is able to decode packets belonging to different protocols and is one of most popular packet capture/manipulation libraries implemented on Python. Packet level features are necessary to identify possible cyber threats in a data stream. The cyber threat identification process aggregates packet features to reveal a pattern of abnormalities in the system. Table I presents the set of packet level features extracted with the IREST sensor.

Once packet level features are extracted, a windowing technique was used to extract a set of statistical features. The idea of the windowing technique is to generate statistical features by using a set of neighboring packets within a given time window. The duration of the windowing technique used for this paper was 1 second. It has to be noted that the ”window size” packet feature in Table I is different from the duration of the window mentioned in here. These generated features can be used to learn the normal behavior in the system such that deviations can be detected as attacks or abnormalities. Table II presents the cyber features extracted using windowing technique.

TABLE II: Window based TCP packet stream features

Feature Name	Feature Description
Packet_rate	No. of packets
Num_src_IP	No. of different source IP addresses
Num_dst_IP	No. of different destination IP addresses
Num_src_port	No. of different source ports
Num_dst_port	No. of different destination ports
Min_data_length	min. data length of packets
Max_data_length	max. data length of packets
Avg_data_length	average data length of packets
Min_win	min. window size of packets
Max_win	max. window size of packets
Avg_win	average window size of packets
Min_time_intv	min. time gap between packets
Max_time_intv	max. time gap between packets
Avg_time_intv	average time gap between packets
Min_pkt_src	min. no. of packets per single source IP
Max_pkt_src	max. no. of packets per single source IP
Avg_pkt_src	average no. of packets per single source IP
Min_pkt_dst	min. no. of packets per single destination IP
Max_pkt_dst	max. no of packets per single destination IP
Min_ttl	min. time to live value of packets
Max_ttl	max. time to live value of packets
Avg_ttl	average time to live value of packets
Num_byt	No. of bytes transmitted by packets
Same_src_dst	No. of packets with same src IP and dst IP
Same_ports	No. of packets with same src port and dst port
Same_src_src_port	No. of packets with same src IP and src port
Same_src_dst_port	No. of packets with same src IP and dst port
Same_dst_src_port	No. of packets with same dst IP and src port
Same_dst_dst_port	No. of packets with same dst IP and dst port
Same_IP_port	No. of packets with src IP== dst IP and src port== dst port
Num_urg	No. of urgent packets in a window
Num_win_zero	No. of packets with zero window size
no_pkts_dst_prt_src	No. of packets with same dst port and src IP

Cyber ML anomaly detection: We considered supervised and unsupervised ML approaches for characterizing normal cyber behavior. Unsupervised ML techniques are being increasingly used in cyber-physical anomaly detection research during past couple of years due to the abundance of unlabeled data generated in real world industrial settings [13]. Unsupervised ML is also popular for detecting previously unseen disturbances [1]. In this experiment One Class SVM (OCSVM) used to characterize the normal behavior of the system and identify anomalies without requiring any data about possible abnormalities/attacks. OCSVM is widely used unsupervised ML approach for anomaly detection because it only requires data from normal behavior of the system [1], [14].

Supervised ML algorithms were used to evaluate the performance of the unsupervised anomaly detection system. We used two supervised ML models: decision trees and random forest [15]. Further, these models can be used to perform feature selection technique which can be used to improve the performance of unsupervised ML mosels. Both, unsupervised and supervised models use window-level features as input. We

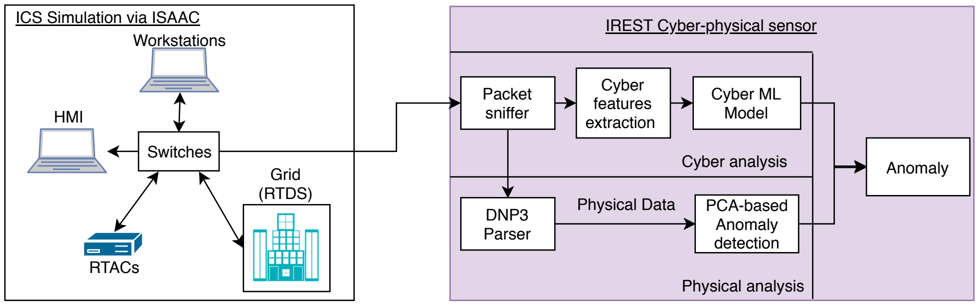


Fig. 3: IREST cyber-physical sensor

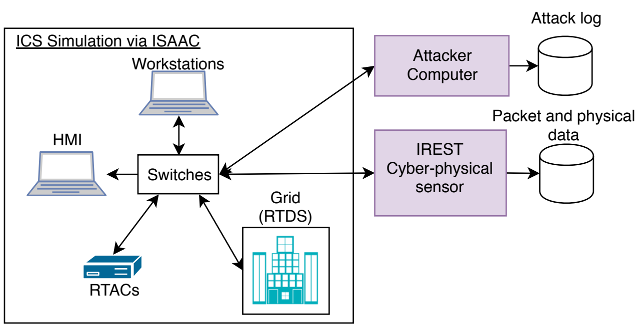


Fig. 4: Data collection

considered One Class SVM (OCSVM) [14] for unsupervised analysis.

B. Physical Characterization

DNP3 Parser: we obtain physical data directly from DNP3 packets being transmitted on the network. Using this approach, the IREST sensor is able to access the commands, control signals, and sensor measurements sent throughout the network. This information is used by the IREST sensor to characterize the physical status of the system.

PCA anomaly detection: We use PCA (Principal-Component-Analysis) to characterize the physical behavior of the system by using the correlation between physical signals sent through DNP3. Normal behavior is characterized by the PCA model which is trained using only data from normal scenarios. The reconstruction error of the PCA model is used to identify anomalies. We define an anomaly score to quantify if an anomaly is occurring. The anomaly score is defined as the euclidean distance (error) between the current sensor signals $\boldsymbol{x}$ and the reconstructed principal components $\boldsymbol{z} = \text{PCA}(\boldsymbol{x})$.

$$\text{score} = \|\boldsymbol{x} - \text{PCA}^{-1}(\boldsymbol{z})\| \tag{1}$$

TABLE III: Cyber Anomaly Detection Performance

model	accuracy	precision	recall	f1
OCSVM	0.988	0.987	0.999	0.993
Decision Tree	0.990	1.000	0.863	0.926
Random Forest	0.990	1.000	0.869	0.930

where PCA^{-1} represents the PCA reconstruction operation. The score in Eq. (1) should be low for all normal scenarios. The objective is to identify abnormal scenarios when the score in Eq. (1) is higher than any of the normal scenarios.

VI. Experiments

This section presents the results obtained with the IREST cyber-physical sensor algorithms on the ISAAC testbed.

Data collection: A set of datasets were collected by running the scenarios described in section IV. The IREST sensor is connected to the ISAAC testbed to collect packet communication data transmitted in each scenario (see Fig. 4).

To collect abnormal cyber data, an attack computer is connected to the testbed network to run a set of scheduled cyber-attacks (see Fig. 4). The attack computer saves the attack timestamps in a log file, indicating when each attack starts and stops. These timestamps are used to label the dataset, indicating which packets correspond to normal state and which packets correspond to cyber anomalies.

To collect data of normal and abnormal physical scenarios, we run each scenario separately and keep the collected data in separate files. Packet data is recorded using the IREST sensor. Sensor data from the simulated physical system is extracted from DNP3 packets.

Cyber anomaly detection: Table III shows the cyber-anomaly detection performance for different ML algorithms using window features. Decision trees and random forest were trained using a supervised approach to classify normal communication against cyber anomalies. The OCSVM algorithm was trained unsupervised using only normal data. The table shows the performance on test data that was not used for training. Decision tree and random forest provide comparable results, with 100% prediction score. This means that the

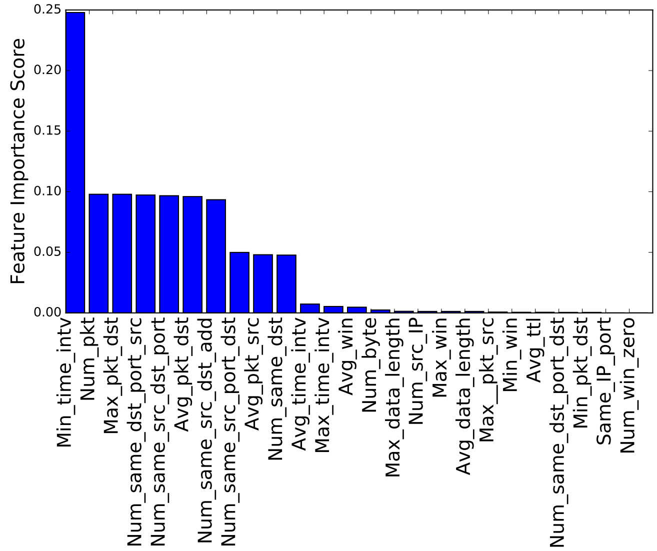


Fig. 5: Feature Importance Scores

algorithm correctly identifies all normal communication. On the other hand, the recall performance tells us that some of the cyber-anomaly communication is being incorrectly identified as normal. OCSVM trades precision performance to improve recall, thus providing the best f1 score.

Table III shows that the unsupervised OCSVM approach provides comparable performance with respect to supervised approaches, providing a higher f1 score. This is important as unsupervised learning offers several advantages over supervised methods. In our case, unsupervised learning is especially useful as no attack data is needed for training. The OCSVM approach is able to detect attacks that have not been seen before.

Figure 5 shows the feature importance score that IREST uses in determining if the sample corresponds to normal communication or a cyber anomaly. The feature importance was obtained using the trained random forest classifier. The figure shows that most important features relate one way or another to packet rate (e.g. num_pkt, avg_time_intv, same_dst_dst_port). At the same time, the data length feature is found to have lower importance.

Physical anomaly detection: Figure 6 shows the PCA anomaly detection results. Training was performed using only a small portion of the normal data collected. Figure 6a shows in blue the anomaly score (Eq. 1) obtained for different normal scenarios. Figure 6b shows in blue the anomaly score obtained for different physical abnormal scenarios. We observe that the score for normal behavior is much lower than for abnormal scenarios. Even when we only used a small portion of normal data for training the PCA algorithm, the score is low for all normal data.

Figure 6b shows that the PCA method is able to identify all abnormal scenarios with a score that surpasses the normal threshold (red line) significantly. All abnormal scenarios can be identified by the high abnormal score provided by this method. The results shows that the presented method is able to correctly identify abnormal scenarios after being trained using only normal data.

VII. Conclusion

In this paper we presented a Machine Learning approach for cyber and physical anomaly detection on Smart-Grid Cyber-Physical Systems. We presented the IREST sensor which uses packet data to detect cyber and physical abnormal behavior. The sensor uses machine learning models to characterize the normal behavior of the system. IREST considers both cyber and physical data in order to construct a complete representation of a CPS. Data collection, testing and validation of the IREST sensor was performed on the ISAAC tested. IREST used unsupervised learning for training the cyber and physical ML anomaly detection algorithms. The results showed that unsupervised learning provided comparable performance with respect to supervised approaches, with the added benefit that abnormal behavior data is not required for training. Thanks to the success of the unsupervised methods, the IREST sensor is able to detect previously unseen cyber and physical anomalies.

The presented approach, which includes the IREST cyber-sensor and the ISAAC testbed, provides a powerful and scalable framework for future cyber-physical security research. Scalability to large scale systems and continuous development and exploration were special considerations that were taken for the design of the testbed, the sensor and the experimental setup. Future work includes the integration of several local IREST sensor analytics in large scale distributed HIL simulations. Integrating state estimation algorithms into the IREST sensor is also a thread of potential future research.

Acknowledgements

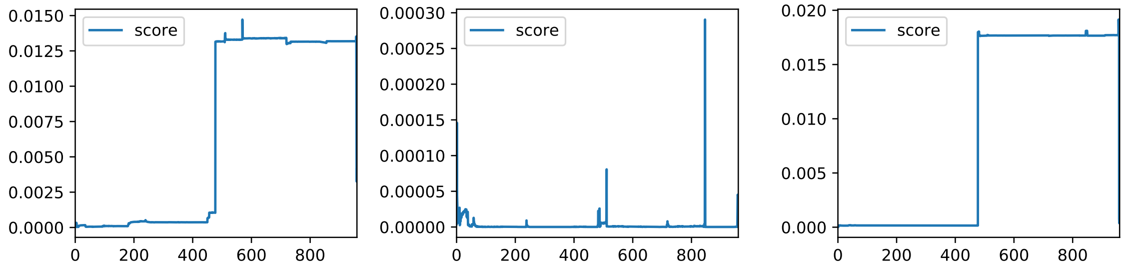
This manuscript has been authored by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy, performed as part of the Resilient Controls and Instrumentation Systems (ReCIS) of Idaho National Laboratory. We would also like to acknowledge a grant from the M. J. Murdock (MJM) Foundation that sponsored the University of Idaho test bed environment leveraged for this effort. We are grateful to Ibukun A. Oyewumi, Daniel Conte de Leon, Victor J. House, John Jacksha, John McFarland, and other staff and faculty involved.

References

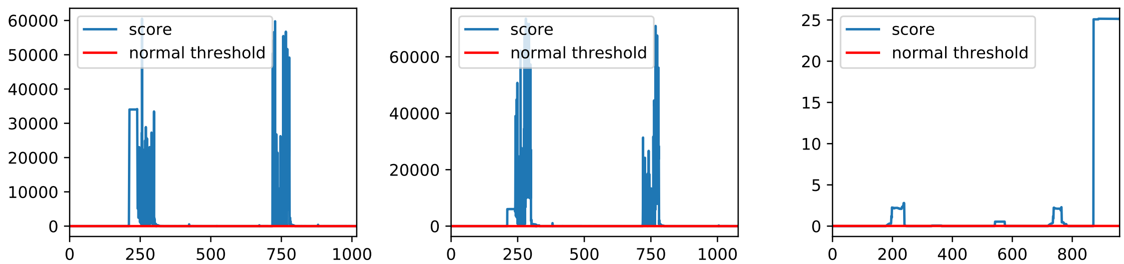
[1] K. Amarasinghe, C. Wickramasinghe, D. Marino, C. Rieger, and M. Manicl, "Framework for data driven health monitoring of cyber-physical systems," in *2018 Resilience Week (RWS)*, Aug 2018, pp. 25–30.

[2] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference*, June 2010, pp. 731–736.

[3] A. A. Jillepalli, F. T. Sheldon, D. C. de Leon, M. Haney, and R. K. Abercrombie, "Security management of cyber physical control systems using nist sp 800-82r2," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, June 2017, pp. 1864–1870.



(a) Normal Behavior



(b) Physical Anomalies

Fig. 6: Physical anomaly detection

[4] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[5] B. Bagheri, S. Yang, H.-A. Kao, and J. Lee, "Cyber-physical systems architecture for self-aware machines in industry 4.0 environment," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 1622 – 1627, 2015, 15th IFAC Symposium onInformation Control Problems inManufacturing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2405896315005571

[6] I. A. Oyewumi, A. A. Jillepalli, P. Richardson, M. Ashrafuzzaman, B. K. Johnson, Y. Chakhchoukh, M. A. Haney, F. T. Sheldon, and D. C. de Leon, "Isaac: The idaho cps smart grid cybersecurity testbed," in *2019 IEEE Texas Power and Energy Conference (TPEC)*, Feb 2019, pp. 1–6.

[7] I. A. Oyewumi, H. Challa, A. A. Jillepalli, P. Richardson, Y. Chakhchoukh, B. K. Johnson, D. Conte de Leon, F. T. Sheldon, and M. A. Haney, "Attack scenario-based validation of the idaho cps smart grid cybersecurity testbed (isaac)," in *2019 IEEE Texas Power and Energy Conference (TPEC)*, Feb 2019, pp. 1–6.

[8] 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*, Oct 2018, pp. 745–751.

[9] A. Jones, Z. Kong, and C. Belta, "Anomaly detection in cyber-physical systems: A formal methods approach," in *53rd IEEE Conference on Decision and Control*, 2014, pp. 848–853.

[10] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, 2017, pp. 140–145.

[11] A. Abokifa, K. Haddad, C. Lo, and P. Biswas, "Real-time identification of cyber-physical attacks on water distribution systems via machine learning based anomaly detection techniques," *Journal of Water Resources Planning and Management*, vol. 145, 07 2018.

[12] P. Biondi. Scapy: Packet crafting for python2 and python3. [Online]. Available: https://scapy.net/

[13] C. S. Wickramasinghe, K. Amarasinghe, and M. Manic, "Deep self-organizing maps for unsupervised image classification," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[14] "One-class support vector machinesan application in machine fault detection and classification," *Computers and Industrial Engineering*, vol. 48, no. 2, pp. 395 – 408, 2005.

[15] L. Breiman, "Random forests," *Machine learning*, vol. 45, no. 1, pp. 5–32, 2001.