MACHINE LEARNING APPROACH TO INDUSTRIAL CONTROL SYSTEM HEALTH MONITORING AND CYBER SECURITY: SIMILARITIES, CONFLICTS AND LIMITATIONS

A. AYODEJI
Fundamental Science on Nuclear Safety and Simulation Technology Laboratory,
Harbin Engineering University,
Harbin 150001, China
Email: abiodun.ayodeji@hrbeu.edu.cn

Y.-k. LIU
Fundamental Science on Nuclear Safety and Simulation Technology Laboratory
Harbin Engineering University
Harbin 150001, China

Abstract

Most of the reported cyber-attacks carried out on industrial control systems usually affect the process measurement. Similarly, system failure or component fault is mostly indicated by process change, and these two "abnormal occurrences" could sometimes have a similar signature. However, the distinction is not evident in the recent approach that utilizes data-driven algorithms for cyber intrusion detection and fault diagnosis. This study reviews machine learning-based abnormal occurrence detection tools and techniques, and their application in complex systems. In this work, we identified and discuss the issues in the development of the machine learning-based intrusion detection and protection systems and the inherent limitation that affects their implementation. As a case study, the nuclear plant control system, its operating states and typical process changes that are similar to those obtainable during random system fault and cyber-attacks are discussed. Finally, recommendations on the future direction for efficient identification and classification of abnormal occurrences to enhance process monitoring and malicious attack detection in nuclear power plants are presented.

1. INTRODUCTION

Recently, digital devices have been introduced into industrial control consoles to replace aging and obsolete analog control systems and to enhance the decision-making process. In cyber-physical systems (CPS), the introduction of digital systems has produced a network of components that provide critical information used for control optimization and lifespan extension. However, shared device utilization exposes the conventional opacity common to legacy CPS control, as the vulnerabilities associated with these digital systems have been inherited by the industrial control systems. Cyber assaults on process control and monitoring system could lead to a significant control failure such as spurious valve position change, pump control loss, sudden feed water loss and failure of safety-critical components that could have serious safety or economic consequences as demonstrated by the Stuxnet worm attack [1], Davis-Besse nuclear plant attack [2] and California system operator attack [3].

Advancement in industrial data acquisition systems has spurred a renewed interest in data-driven approaches to curb the rise of industrial cyber-attacks. Most machine learning-based intrusion detection system (IDS) rely on monitoring traffic and dataflow at the system or network level to detect attacks targeted at the host or the network. In this approach referred to as the host intrusion detection system (HIDS) or network intrusion detection system (NIDS), the network traffic (or host-based) packet captures (PCAP) are preprocessed and applied in training the data-driven model. However, implementation of the data-driven solution in complex industrial systems is limited because cyber-attacks have a real and significant impact on the process variable or the physical system. Conversely, a number of process-based intrusion detection systems (PIDS) have also been developed using process measurements alone. This approach has the same weakness as NIDS because analyzing the process change in isolation would not provide a significant clue regarding the causal path.

In an attempt to improve the capability of existing IDS, researchers integrate both host/network traffic and process layer information to develop a robust detection system. A major drawback to adopting this approach is that process variable change could result from a number of other occurrences. The existing accounts fail to resolve the conflict between process change resulting from different initiating events. This limitation results in intrusion detection systems with a high false alarm rate, which has rendered many of the proposed solutions un-implementable.

This paper discusses the similarities, conflicts, and limitations in the tools commonly used by fault diagnosis and cybersecurity practitioners–two areas that are having increasing interaction with the advancements in machine learning and artificial intelligence techniques. This observation has severe implications for models that utilize system data for abnormal occurrence detection. To extensively discuss the main thesis of this paper, we present a brief description and characteristics of the industrial SCADA system and preliminaries on the existing ML algorithm in section 2. The following sub-sections describe each IDS development, its implementation challenges, and functional limitation. Then in section 3, we enumerate common data domain and techniques used in the development of ML-based intrusion detection systems for industrial control systems (ICS) with emphasis on the issues and limitations of the resulting algorithms. As a case study, the nuclear plant operating states and process changes that are similar to those obtainable during random system fault and cyber attacks are discussed in section 4. Section 5 presents the recommendation for the development of an effective abnormal occurrence detection system with the capability to recognize and recover from both fault occurrence and cyber-attacks without complicating the already complex systems and with no hindrance to other safety-related functions.

2. PRELIMINARIES

2.1. Supervisory Control and Data Acquisition (SCADA) System

Supervisory Control and Data Acquisition (SCADA) has been consistently defined to include embedded systems, sensors and actuators used in monitoring and control of critical industrial and national infrastructures such as smart grid, transportation networks and power generating plants. Supervision, control and data acquisition functions of SCADA are achieved by a number of computers and computer-based applications, networks, and devices. Automatic and user-defined real-time monitoring and control of process measurements are performed through remote terminal units (RTU), intelligent field programmable devices and their network.

To address the security gaps observed in SCADA systems, some innovative approach to critical digital assets security has been presented. One way and dual-path data diode that allows data to flow in a single predetermined direction are being used to defend against the cyber threat in some US nuclear installations. This security device uses diodes to provide a form of air-gap physical separation between systems comprising digital instrumentation and control space and the information technology space in nuclear power facilities. Data diode has been praised for its simple set up and installation procedure, as well as its low maintenance cost [4]. However, it is inadequate, as complete isolation of critical cyber assets, single destination gateway, installation cost, software support and insider threat/human reliability issues still exist [4].

2.2. Common techniques for developing machine learning tools for SCADA Intrusion detection system

A number of researchers have utilized the real-time functionality of machine learning algorithms to detect malicious network traffic in SCADA systems [5] and for other intrusion and anomaly detection purposes [6]. Different SCADA intrusion and anomaly detection techniques have also been combined into a single hybrid system with decision rules[7]. Most of the available security solutions and protective techniques are focused on extending traditional IDS networking needs and requirements that generally match attack signatures using a signature-based IDS or detect network anomalies with machine learning techniques. In the development of signature-based IDS, attack patterns are aggregated and processed to train the algorithm. Each traffic data is labeled (supervised training) or clustered (unsupervised/semi-supervised training) according to a specific pattern generated during the attack. Anomaly-based systems utilize normal traffic data for training and testing, and anomaly is detected when there is exceptional changes or deviation from known traffic. Robust anomaly detection algorithms rely heavily on specific domain protocols and legitimate characteristics of the target system for efficient performance. It is unable to identify the kind of anomaly detected, necessitating additional expert input in traffic analysis. Signature-based IDS rely on historical attack signatures on specific systems for intrusion detection. This is a kind of hypothesize-and–match technique where signatures of known attacks are used to train the algorithm. However, signature-based IDS lack the capability to detect novel attacks, as it is impractical to acquire signatures of all types of attack in a single dataset.

2.3 Host/network domain-based IDS models

Network traffic features that contain SCADA communication protocols can be specifically targeted by corruption, interception, or tampering attacks. These can potentially lead to a loss of confidentiality, visibility, or device connectivity, also providing support to implement process-aware attacks, thus compromising safety and security. This technique uses anomaly-based or signature-based misuse detection models to detect system intrusion. As a signature-based model, this approach involves creating a database that contains all the signatures of the known payload attributes and single packet-based attacks on SCADA protocols and using this database in the development of the IDS. Considering the paucity of SCADA-specific training data challenge that limits the development of signature-based IDS, researchers now utilize anomaly detection algorithm. As an anomaly-based model, the algorithm is built with normal system traffic data, and any deviation from the normal traffic is flagged as an anomaly.

Anomaly-based IDS is relatively easy to build as the data requirement is almost homogenous, and it is convenient for application where the acquisition of attack signature is difficult. It has a relatively simple design as it only processes a single data stream from the network feed and does not require attack signatures. In practice, this model is limited because it lacks the capability to identify and localize attacks. Moreover, port registration, the legality of interception, and critical operational requirements for network packet inspection and port-based analysis are other issues to be resolved [8]. A more important limitation of this approach in critical infrastructures is that process measurement is essential in detecting attacks. Process control and safety is the fundamental ICS function which makes it an attractive target for sophisticated attackers. This is partly because of the technical sophistication and resources that are available for threat actors interested in such a facility. Hence, the historical behavior of the physical process provided by process parameters is critical to detect ICS cybersecurity incidence.

2.4. Process measurement-based model for IDS

The discovery of attackers with partial or total control of the sensor or actuator operation has led to the proposal of several intrusion detection schemes for ICS using data collected from physical sensors. To achieve the maximum return on attack, most SCADA penetration targets critical control devices such as sensors and actuators. The exploit of these devices results in a significant impact on the process measurements and the physical system. To develop robust IDS, a number of researchers consider the application of process variables. The logic considers attack scenarios such as false data injection and other deceptive man-in-the-middle (MITM) attacks that could mask the real process state or present spurious parameter measurement to manipulate the control response. For instance, an attacker with access to process configuration could launch an attack to modify process set-point and trigger undesirable system response.

Li et al [9] demonstrated the utility of process parameters in detecting cyber intrusion by investigation false sequential logic attacks on a SCADA system using process-level parameters. Analysis of the physical effect of the attack on a simplified pump-valve control system shows the possibility of serious process disruption and equipment damage. Anomalies in a water supply control system were detected using signals variation on power monitoring of endpoints from a control system to train and evaluate k-nearest neighbor (KNN), support vector machine (SVM) and Random Forest algorithms[10]. In this approach, process parameter deviations and process variables non-conformity to natural behavior are used as indicators of the anomaly. In the implementation phase, the algorithm monitors the real-time operation of the system and compares the real-time features with the features derived from normal operations. In some applications, a dynamic threshold is set to flag the comparison result that is beyond a certain level of deviation from the normal features. This is usually based on the possibility that an attacker may pass a deceptive measurement in place of real measurements and manipulate control response, an instance of data injection or false operation attack. Behavioral modeling tools such as autoregressive model is being used to monitor for changes to high-value variables that would normally stay constant, such that process control attacks that aim to change static configuration parameters could be detected[11]. The state change information, process control knowledge and internal representation of the SCADA system are utilized for intrusion detection. Also, detecting an advanced persistent threat in the SCADA system is possible through process monitoring.

Nonetheless, the model still depends on a single stream of information to detect complex attacks. The limitation in this model further explains the simplistic approach and the reluctance in the real-world implementation of some of the researched intrusion detection systems. Some researchers[12, 13] recognized the inherent weakness in the PID system, and considered integrating process-level information with the system and network traffic data for robust intrusion detection.

2.5. Multi-domain data mining technique for IDS development

To address the issues identified with homogenous data-driven intrusion detection systems, a number of researchers developed IDS algorithms built on both host/network traffic data as well as process-level knowledge to strengthened ICS security. Morris and Gao [14] utilized network traffic information and state-based payload content features such as sensor measurements and distributed control state to detect anomaly in a SCADA system. Zhang et al [13], utilized heterogeneous data derived from the simulation of five attacks on a private ICS testbed. They compared the classification performance of K-means, random forest and decision tree on the data from the testbed. However, this approach also suffers from the limitation of the process level intrusion detection model, because the implementation fails to distinguish between many other process change initiating events. The application of such a model in a real-world system is bound to result in a high false alarm rate. Table 1 summarizes the available IDS techniques and decision engines utilized.

TABLE 1. COMMONLY USED TECHNIQUE FOR DEVELOPING ICS INTRUSION DETECTION SYSTEMS, DATA TYPE AND THE DECISION ENGINE UTILIZED

IDS Technique	Training Dataset source	Data type	Decision engine	References
Network traffic/host-based	Testbed*	**Synthetic	OCSVM; K-mean clustering	[18]; [19]
	KDD	Real	ANN, Neighborhood outlier factor	[20]
	NSL-KDD	Synthetic	GA-SVM; FNN	[21, 22]
	UNS-NB15	Synthetic	DNN	[23]
	DARPA 1998	Real	ANN, SVM, MARS	[24]
	ADFA dataset	Synthetic	ANN, SVM, HMM, ELM, STIDE	[25]
	Testbed	Synthetic	SVM; KNN, Decision tree; Random forest	[26]
Process variable-based	Testbed	Synthetic	Association rules	[27]
	Suez water distribution dataset	Real	One-class SVM	[28]
Integrated approach (Network traffic and process variables)	***CIPC-MSU water dataset	Synthetic	SVM, ANN	[29],[30]
	ORNL dataset	Synthetic	EM clustering, KNN,	[31]
	iTrust –SwaT Dataset	Real data	ANN;DNN	[32]
	Testbed	Real data	KNN, decision tree, random forest	[13]

*Testbeds include the scaled-down version of SCADA system that controls a real physical process or uses a hardware-in-the-loop (HIL) simulation of the physical process.

**Synthesized data include those generated from SCADA mimics, workbenches, and sanitized data.

Acronyms: ELM= Extreme learning machine; HMM= Hidden Markov Model EM= expectation-maximization STIDE: Sequence Time-Delay Embedding; DNN= Deep neural network; FNN=fuzzy neural network; MARS= Multivariate Adaptive Regression Splines

3. SIMILARITIES AND CONFLICTS IN ML-BASED ICS FAULT MONITORING AND CYBERSECURITY

Despite the utility of the multi-domain, heterogeneous approach to advanced cyber-attack detection, the method also has certain weaknesses. The attractiveness of this method is beclouded by the fact that there are a number of initiating events for process change. Observed deviation could be a result of normal operating transients, incipient system fault, component degradation, sensor drift, cyber-attacks or the combination of a number of these occurrences. Figure 1 shows the likely cause of the observed process change in complex industrial systems.

Incidentally, the real-time pattern attribute in the process measurements also make it suitable for diagnosing system/component faults. This attribute has been utilized to build independent machine learning models for fault diagnostic purposes using only process measurement. For instance, process deviation has been used to diagnose the reactor coolant system and component faults using neural network [15], and support vector machine[16]. Evolutionary algorithms and optimized statistical models have been used to diagnose leakages in industrial steam generators [17]. Moreover, some of the reported cyber-attacks seek to compromise ICS by first defeating the safety measures put in place. This method of attack could be easily mistaken for random fault and diagnosing the breach and identifying the root cause takes time and expertise. For instance, trend change of a process variable for offset or geometric attack that involves constant or time-dependent addition of spurious values to the sensor or actuator output and variable trend noticed for an incipient leakage in heat exchanger pipes or reactor pump seal leakage is difficult to differentiate. The similarity in trend and signature may obscure the causal path and eventually result in - at best - false positive or - worst case- a more serious misdiagnosis resulting in a security breach and other consequences of successful advanced persistent attacks. An attempt to distinguish between different anomalies by analyzing the anomaly behavior based on the instrument output data has been proposed by Jie et.al. [27]. They argued that instrument output beyond a fixed band, transfer function similarities in the input-output relationship between two adjacent switch devices and logical relationships in state values can be used to distinguished between system failure, DoS attack, and false data injection. However, they also utilized process level measurement alone for the analysis. Moreover, the simple system analyzed to evaluate the method does not represent the dynamics observed in complex systems. Also, setting a fixed threshold for a system with such dynamics is not viable. In addition, a similar method is prominent in fault identification and isolation research works, especially for fault isolation and localization involving sensor drifts.

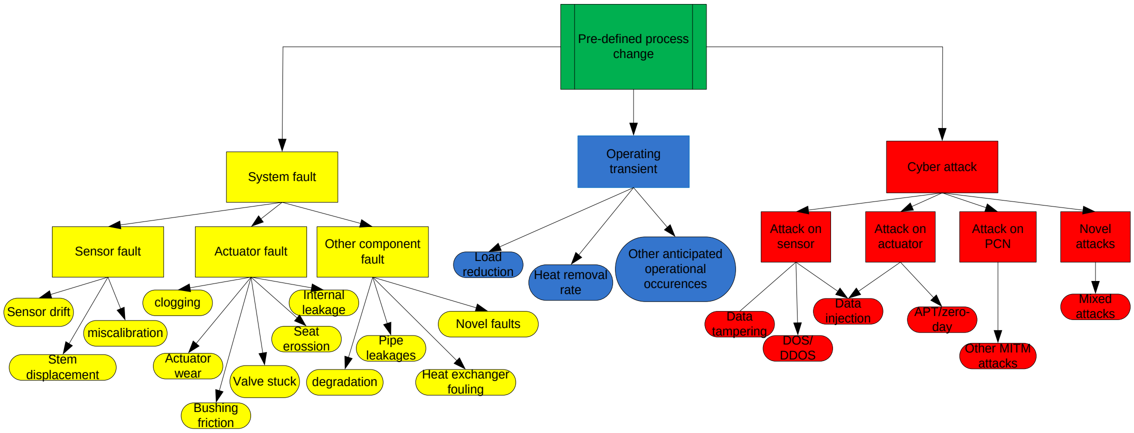

FIG 1: Industrial process parameter change initiating events

3.2. Case study: Process measurement change initiating events in the nuclear power plant

In complex systems such as nuclear power plant, there are a number of operating transients and load changes that characterizes the normal operation of the plant. To ensure the balance of plant, a typical nuclear power plant utilizes a number of distributed control and safety systems designed to ensure safe operation and - in case of an accident - safe shut down and cooling of the reactor core. In normal operation, the neutron population and fission rate is being controlled by a number of systems such as control rod and chemical shim. In a typical PWR, minor reactivity or power adjustment is done with the aid of the chemical and volume control system (.i.e. boric acid). Also, based on the turbine-generator configuration with respect to the reactor, changes in the power demand from the grid could also necessitate a corresponding change in the power supply from the reactor. All these changes introduce a unique dynamic into the control of the nuclear power plant which needs to be considered for the development of a robust abnormal occurrence detection. Figure 2 shows a simplified representation of the nuclear power plant control system.

In Fig 2, Layer 1 is the physical level where the sensor and actuators are utilized to control the physical system. The second layer (Layer 2) is the distributed controllers responsible for implementing automated control based on the current state of the component being monitored. The controllers utilize the automatic feedback response from the current process measurement output to set the next stage of the process. Layer 3 is the process control network, where the detection, control, and monitoring functions are usually performed. Control and communication protocols such as Modbus, DNP3, etc are used to ensure effective flow of control and safety signals. Beyond the automated functions in Layer 2, additional safety and control signals are routed through the process control network. Layer 4 is the supervisory control and data acquisition layer with a direct connection to the process control network. Here, the process measurements are stored in a data historian. Data in this historian are analyzed for fault diagnosis and maintenance purposes. This layer also contains systems such as the control consoles, workstations, servers, network equipment and systems with a human-machine interface where operators can monitor and control the physical process.

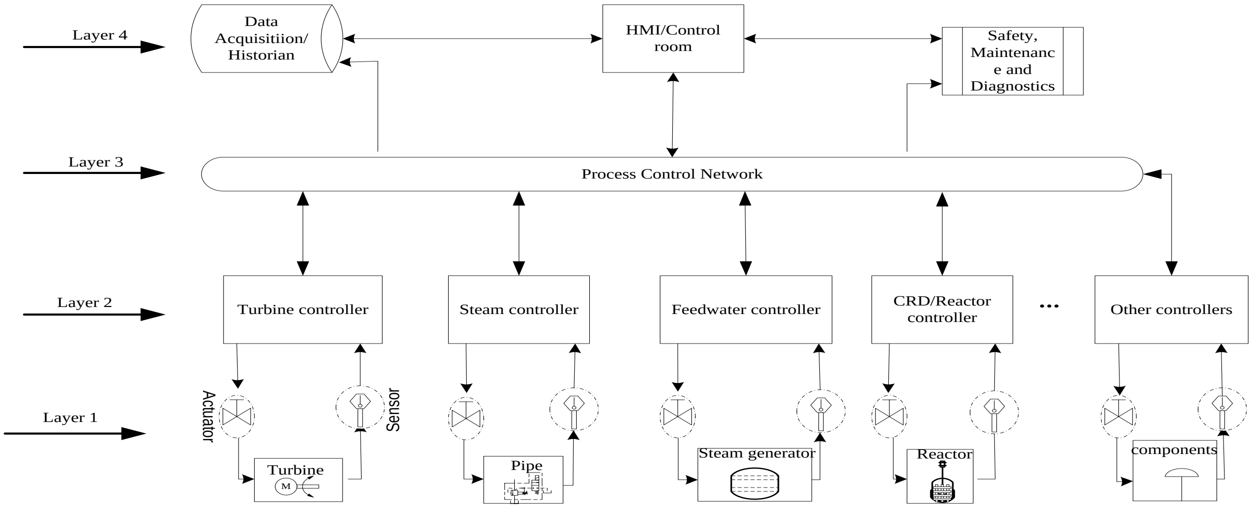

FIG 2. A simplified process control system for a typical nuclear power plant

A key aspect of this ICS security is the validity of the data values sent from programmable logic controllers to the HMI. An attacker could gain remote access to Level 2 sensors and actuators modify their software or their environment or intercept the transmission. With this access, attackers could launch coordinated attacks on the physical system through the process being controlled. An attacker who is able to manipulate the data values can mount attacks with severe consequences. Access to layer 2 devices could also empower the attacker to trick the human operator by sending spurious measurements[33]. Another major consideration is the process measurement dynamics introduced when complex ICS system undergoes routine maintenance or part replacement. These dynamics also affect the process measurement trends used in the development of some intrusion detection systems. In constructing robust IDS applicable to the complex system utilized in the control of a nuclear plant, it is pertinent to consider the nuances introduced by the control of the plant, as well as the causal path of other possible abnormal occurrences.

To further elaborate on the similarities in some stated attack and incipient fault formation, consider the development of a state-aware intrusion detection system for stealthy man-in-the-middle attacks against ICS field-bus water tank level control system discussed in [34]. The study depicts a false data injection attack where the attacker gains root access to sensor measurement and actuator command (level 2 as illustrated in Fig 2) and forces a decrease in water level in a simulated industrial water tank. The attacker slowly changes the sensor reading of the tank level controller using a small constant increment trying to remain undetected. In addition, the study designs a detection mechanism that relies on the residual which is basically the difference between sensor measurement for the water level and its estimated value. There are obvious similarities in the signatures generated in this instance and many diagnostic approaches for incipient, slowly-developing faults that also rely on process level change [35] and residual generation for system fault detection.

Moreover, modeling and simulating the transients described above is not a trivial task. Researchers utilize a number of computer codes to simulate process control and acquire process parameter deviations. However, the outputs of the codes are estimates with limited applications. Similar constraints are present in NIDS development. Simulating attacks that represent real-world exploit to retrieve signatory data, or to evaluate ML model performance is difficult. Hence, most researchers rely on publicly-sourced data to train, test and evaluate the intrusion detection system. The composition, suitability and reliability of public data repositories used for the development of these algorithms also need to be examined.

4. DISCUSSION AND FUTURE DIRECTIONS

Predicting and responding to assault against cyber-physical systems is an art because of the range of novelty involved in cyber-attacks. Moreover, the fuzziness of the attack surfaces, modernization, and sophistication of the attack and threat actors also make the defense of the industrial control system a challenge. Most critical is the non-parametric characteristic of the cyber attacker and the physical consequence of a successful attack on ICS with increasingly short detection and response time before the adversary violates the monitored system. Application of data-driven tools to the monitoring and detection of cyber-attack comes with a lot of promises. However, the rate of false alarm generated in real-world applications is a serious issue. In the development of a robust SCADA defense system, the questions about the influence of diverse cause of abnormal occurrence on the rate of false alarm generated by the IDS needs to be addressed. A critical analysis is needed to establish the nuances between different industrial control system configurations, the process behavior, component and its failure conditions, and how this information can be used to defeat attacks on ICS

In addition, proper development and implementation of a data-driven algorithm that seeks to identify and localize attacks based on dataset require a certain level of domain expertise. We observed some knowledge gaps in the development of ML algorithms used in intrusion detection tasks. Multidisciplinary approach and domain knowledge are crucial to precisely define the expected operating conditions, analyze the available data, distill the output result, evaluate the performance of the algorithm, and characterize the nature of the detected anomalies. First, we observed that different data segmentation and selection methods are implemented to process data for algorithm development. Some researchers randomly select features or instances of data from the database for training the algorithm. Testing is done by another round of randomly selected features or instances, while others used the whole dataset for training and evaluation. In the literature reviewed, there is no study that describes the effect of these data sampling methods on the performance of the algorithm. For instance, against prior evidence, worse algorithm performance with a larger dataset has been reported [36]. This lack of domain expertise and oversight in requisite preprocessing that goes into building an effective decision engine has limited the application of these engines in real systems. Secondly, most studies do not present a hyperparameter selection method or optimization technique for the model, while some studies have no cognitive justification for the data preprocessing technique or model evaluation method used. Although we found some dated research that discusses issues on testing intrusion detection systems [37], we recommend a new study in this area, considering the rate of development in the field.

Moreover, efforts need to be directed to address the issues that constraints extensive evaluation of available algorithms. Dataset lifespan is being shortened and “benchmark” datasets are fast becoming obsolete because threat actors are highly dynamic and sophisticated, and the corresponding upgrade in modern systems generate different data composition. Developing a new, comprehensive dataset requires detailed consideration for modern attack surface and well-defined dataset structure. Performing extensive evaluation of the system, to obtain a robust dataset that considers zero-day and other modern exploits, is expensive. Where successfully done, extending such evaluation to different network architecture present further difficulties. In the absence of a robust historical database for specific real-world SCADA intrusions, establishing unified criteria to evaluate the effectiveness of existing IDS is difficult. For instance, the performance of IDS built on data from privately owned protocol-specific testbeds cannot be independently repeated. Also, testing an algorithm developed with data from a different SCADA configuration may not scale well on these testbeds. A good start is the development of open-source, high fidelity large scale testbeds or SCADA virtual architectures, network and system simulators and programmable logic controllers to design, test and validate these algorithms [38,39]. A predictable issue with publicly available SCADA virtual architecture is that this architecture is also available to attackers to test their exploits. False-positive can be triggered intentionally by attackers with knowledge of the specially crafted data manipulation to feed into the system, which presents the defense against cyber-attack as a second-order chaotic problem.

Consequently, it is necessary to develop a comprehensive abnormal occurrence detection system. A much more systematic approach that identifies various initiating events (shown in Fig 1.), their interaction and their real-time effect on the observed process deviation is critical to towards the development of a robust data-driven abnormal occurrence detection algorithm. The system would possess a mechanism to detect component faults and cyber-attacks independently while using redundant reconfiguration to achieve safety functions if the control system is under attack. Since process variables deviate due to a number of different reasons, weights could be attached to reduce the contribution of other considerations in the final intrusion detection output. Real-time implementation of this system is critical, to completely eliminate manual data sorting and additional data processing requirements.

5. CONCLUSION

In the control of a physical process, for every signal sent to the actuator, there is an expected process change, rate of change or process measurement expected from the sensor. If the expected feedback and the received feedback do not correlate, then abnormality is detected in the system. In a complex industrial system, the uncorrelated measurement or deviation could result from a number of incidences. For a robust assessment of the causation of the deviation detected and to take appropriate control decisions, there is a need for a robust system that considers the properties of the feedback signal and the interaction of other systems and components. A robust and sufficient security solution demands a comprehensive consideration of all critical interactions in the systems. Classifying attacks manipulating critical process parameters and random system fault resulting in process change is not considered by many IDS proposals. This results in user-dependent monitoring systems with a high false alarm rate and low reliability.

In this work, we hypothesize that the major contribution to the false alarm generation is the failure to identify the difference between the inherently similar signature that defines transients common to a complex system, and abnormal occurrences such as incipient/slowly-developing fault and cyber intrusion with physical impact on the process information. To support our hypothesis, we discuss nuclear plant control system characteristics that account for observed process measurement change and could also influence the high false alarm rate observed in the industrial intrusion detection system. In addition, to aid a robust IDS development, we recommended an approach that considers the nuances in the data used in the development of machine learning algorithms. The present findings and recommended course of action serve as a foundation for the development of robust IDS with a significant reduction in the false alarm problem common to current intrusion detection systems.

REFERENCES

[1] Farwell, J.P. and Rohozinski, R., Stuxnet and the future of cyber war. Survival, 2011. 53(1): p. 23-40.

[2] Kesler, B., The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010. Strategic Insights, Spring 2011, 2011.

[3] Stamp, J., et al., Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories, 2003.

[4] Scott, A., Tactical data diodes in industrial automation and control systems. SANS Institute InfoSec Reading Room, 2015.

[5] Nader, P., Honeine, P., and Beauseroy, P., Norms in one-class classification for intrusion detection in SCADA systems. IEEE Transactions on Industrial Informatics, 2014. 10(4): p. 2308-2317.

[6] Hota, H. and Shrivas, A.K., Data mining approach for developing various models based on types of attack and feature selection as intrusion detection systems (IDS), in Intelligent Computing, networking, and informatics. 2014, Springer. p.845-851.

[7] Aburomman, A.A. and Reaz, M.B.I., A survey of intrusion detection systems based on ensemble and hybrid classifiers. Computers & Security, 2017. 65: p. 135-152.

[8] Nguyen, T.T. and Armitage, G.J., A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys and Tutorials, 2008. 10(1-4): p. 56-76.

[9] Li, W., et al., False sequential logic attack on SCADA system and its physical impact analysis. Computers & Security, 2016. 58: p. 149-159.

[10] Robles-Durazno, A., et al. A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system. in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2018. IEEE.

[11] Hadžiosmanović, D., et al. Through the eye of the PLC: semantic security monitoring for industrial processes. in Proceedings of the 30th Annual Computer Security Applications Conference. 2014. ACM

[12] Krotofil, M., J. Larsen, and D. Gollmann. The process matters: Ensuring data veracity in cyber-physical systems. in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. 2015. ACM.

[13] Zhang, F., et al., Multi-Layer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System and Process Data. IEEE Transactions on Industrial Informatics, 2019.

[14] Morris, T. and W. Gao. Industrial control system traffic data sets for intrusion detection research. in International Conference on Critical Infrastructure Protection. 2014. Springer

[15] Ayodeji, A., Liu, Y.-k., and Xia, H., Knowledge base operator support system for nuclear power plant fault diagnosis. Progress in Nuclear Energy, 2018. 105: p. 42-50.

[16] Ayodeji, A. and Liu, Y.-k., Support vector ensemble for incipient fault diagnosis in nuclear plant components. Nuclear Engineering and Technology, 2018. 50(8): p. 1306-1313.

[17] Ayodeji, A. Liu, Y.-k. (2019). PWR heat exchanger tube defects: Trends, signatures and diagnostic techniques. Progress in Nuclear Energy 112(171-184).

[18] Maglaras, L.A. and Jiang, J., A novel intrusion detection method based on OCSVM and K-means recursive clustering. ICST Trans. Security Safety, 2015. 2(3): p. e5.

[19] Almalawi, A., et al., An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Computers & Security, 2014. 46: p. 94-110.

[20] Jabez, J. and Muthukumar, B., Intrusion detection system (IDS): anomaly detection using outlier detection approach. Procedia Computer Science, 2015. 48: p. 338-346.

[21] Gauthama Raman, M.R., et al., An efficient intrusion detection system based on hypergraph - Genetic algorithm for parameter optimization and feature selection in support vector machine. Knowledge-Based Systems, 2017. 134: p. 1-12.

[22] Ashfaq, R.A.R., et al., Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences, 2017. 378: p. 484-497.

[23] Muna, A.-H., Moustafa, N., and Sitnikova, E., Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 2018. 41: p. 1-11.

[24] Mukkamala, S., Sung, A.H., and Abraham, A., Intrusion detection using an ensemble of intelligent paradigms. Journal of network and computer applications, 2005. 28(2): p. 167-182.

[25] Creech, G., Developing a high-accuracy cross platform Host-Based Intrusion Detection System capable of reliably detecting zero-day attacks. 2014, University of New South Wales, Canberra, Australia

[26] Frazão, I., et al. Denial of Service Attacks: Detecting the Frailties of Machine Learning Algorithms in the Classification Process. in International Conference on Critical Information Infrastructures Security. 2018. Springer.

[27] Jie, X., et al., Anomaly behavior detection and reliability assessment of control systems based on association rules. International Journal of Critical Infrastructure Protection, 2018. 22: p. 90-99.

[28] Nader, P., Honeine, P. and Beauseroy, P., Detection of cyberattacks in a water distribution system using machine learning techniques. in 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC). 2016.

[29] Yeckle, J. and Abdelwahed, S., An Evaluation of Selection Method in the Classification of Scada Datasets Based on the Characteristics of the Data and Priority of Performance. in Proceedings of the International Conference on Compute and Data Analysis. 2017.ACM

[30] Turnipseed, I.P., A new scada dataset for intrusion detection research. 2015, Mississippi State University.

[31] Keshk, M., et al. Privacy preservation intrusion detection technique for SCADA systems. in 2017 Military Communications and Information Systems Conference (MilCIS). 2017. IEEE.

[32] Kravchik, M. and Shabtai, A., Detecting cyber attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. 2018. ACM.

[33] Erez, N. and Wool, A., Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems. International Journal of Critical Infrastructure Protection, 2015. 10: p. 59-70.

[34] Urbina, D.I., et al. Attacking Fieldbus Communications in ICS: Applications to the SWaT Testbed. in SG-CRC. 2016.

[35] Ayodeji, A. and Liu, Y.-k., SVR optimization with soft computing algorithms for incipient SGTR diagnosis. Annals of Nuclear Energy, 2018. 121: p. 89-100.

[36] Zhou, L., et al., Automatic fine-grained access control in SCADA by machine learning. Future Generation Computer Systems, 2019. 93: p. 548-559.

[37] Mell, P., et al., An overview of issues in testing intrusion detection systems. 2003.

[38] Alves, T. and Morris, T., OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research. Computers & Security, 2018. 78: p. 364-379.

[39] Holm, H., et al. A survey of industrial control system testbeds. in Nordic Conference on Secure IT Systems. 2015. Springer.