JOURNAL OF EDUCATION: RABINDRA BHARATI UNIVERSITY
ISSN: 0972-7175

ANALYSIS ON IOT-ENABLED CYBER-PHYSICAL SYSTEMS RECOGNITION AND PROVENANCE OF CYBER-ATTACKS

[1]Dr.Dinesh Kumar, [2]Dr. N. Chandra Mouli, [3]A.Sandhya
[1,2]Associate Professor, [3]Student [1,2,3] Dept. of Computer Science Engineering,
[1,2,3]Vaageswari College of Engineering, Karimnagar, Telangana.
E-Mail: sahni.dinesh@live.com, cmnarsingoju@gmail.com, chiduralasusheela@gmail.com

Abstract
Cyber physical systems (CPS) that are Internet of Things (IoT) enabled can be difficult to secure since security measures designed for general information / operational technology (IT / OT) systems may not work as well in a CPS environment. Consequently, this research provides a two-level ensemble attack detection and attribution framework created for CPS, and more particularly in an industrial control system (ICS). For identifying assaults in unbalanced ICS environments, a decision tree integrated with an unique ensemble deep representation learning model is created at the first level. An ensemble deep neural network is created for assault attribution at the second level. Using real-world datasets from the gas pipeline and water treatment system, the suggested model is assessed. Findings show that the suggested model performs better than other competing methods with a similar level of computational complexity.
Keywords: Cyber-attacks, Deep representation learning, Cyber threat detection, Cyberthreat attribution

INTRODUCTION

Cyber-physical systems (CPS) are becoming more and more integrated with Internet of Things (IoT) technology, including key infrastructure sectors like dams and utilities plants. IoT devices, also known as Industrial IoT or IIoT in these contexts, are frequently a component of an Industrial Control System (ICS), which is responsible for the safe operation of the infrastructure. ICS can be widely defined to include systems that use Mod bus protocols and programmable logic controllers (PLCs), distributed control systems (DCS), and supervisory control and data acquisition (SCADA) systems. However, by connecting ICS or IIoT-based systems to public networks, they expand their attack surfaces and vulnerability to cyber attacks. The Stuxnet campaign, which allegedly targeted Iranian centrifuges for nuclear enrichment in 2010, causing severe damage to the equipment [1], [2]. Another example is that of the incident targeting a pump that resulted in the failure of an Illinois water plant in 2011 [3]. BlackEnergy3 was another campaign that targeted Ukraine power grids in 2015, resulting in power outage that affected approximately 230,000 people [4]. In April2018, there were also reports of successful cyber-attacks affecting three U.S. gas pipeline firms, and resulted in the shutdown of electronic customer communication systems for several days [1]. Although security solutions developed for information technology (IT) and operational technology (OT) systems arerelatively mature, they may not be directly applicable to ICSs. For example, this couldbe the case due to the tight integration between the controlled physical environment and the cyber systems. Therefore, system-level security methods are necessary to analyze physical behavior and maintain system operation availability [1]. ICS security goals are prioritized in the order of availability, integrity, and confidentiality, unlike most IT/OTsystems (generally prioritized in the order of confidentiality, integrity, andavailability) [5]. Due to close coupling between variables of the feedback control loop and physical processes, (successful) cyber-attacks on ICS can result in severe and potentially fatal consequences for the society and our environment. This reinforces the importance of designing extremely robust safety and security measurements to detect and prevent intrusions targeting ICS.

RELATED WORK

We develop a novel two-phase ensemble ICS attack detection method capable of detecting both previously

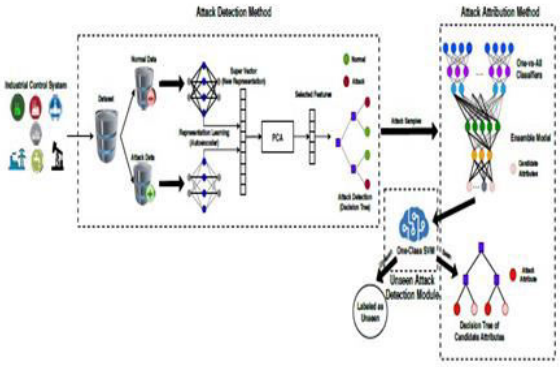
seen and unseen attacks. We will also demonstrate that the proposed method outperforms other competing approaches in terms of accuracy and f-measure. The proposed deep representation learning results in this method being robust to imbalanced data.

2) We propose a novel self-tuning two-phase attack attribution method that ensembles several deep one-vsall classifiers using a DNN architecture forreducing false alarm rates. The proposed method can accurately attribute attacks with high similarity. This is the first ML- based attack attribution method in ICS/IIoT at the time of this research. We analyze the computational complexity of the proposed attack detection and attack attribution framework, demonstrating that despite its superior performance, its computational complexity is similar to thatof other DNN-based methods in the literature.

PROPOSED SYSTEM

The proposed attack detection consists of two phases, namely representation learning and detection phase. Using a conventional unsupervised DNN on an imbalanced dataset yielded a DNN model that mainly learned majority class patterns and missed minority class characteristics. Most researchers have tried to address thischallenge by generating new samples orremoving certain samples to make the dataset balanced and then passing the data to a DNN. However, in ICS/IIoT security applications, generating or removing samples are not reasonable solutions. Due to the ICS/IIoT systems' sensitivity, generated samples should be validated in a real network, which is impossible since the generated attack samples may be harmful to the network and cause severe impacts on the environment or human life. In addition,

validation of the generated samples is time-consuming. Moreover, removing the normal data from a dataset is not the right solution since the number of attack samples in ICS/IIoT datasets is usually less than 10% of the dataset, and most of the dataset knowledge is discarded by removing 80% of the dataset.



Proposed attack detection and attribution framework

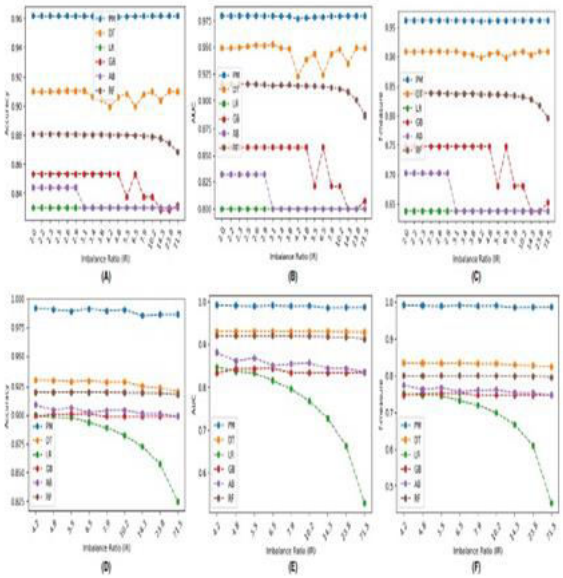
EXPERIMENTAL SETUP

SWaT Dataset				Pipeline Dataset				
Method	Pre	Rec	f-measure	Method	ACC	Pre	Rec	f-measure
Proposed method	**0.9999**	**0.9999**	**0.9998**	Proposed method	96.20	0.9617	**0.9620**	**0.9618**
DT	0.8411	0.8284	0.8346	DT	91.11	0.9092	0.9111	0.9099
LAD-ADS [13]	0.936	0.891	0.914	SVM [28]	92.50	0.782	0.936	0.852
DNN [26]	0.9829	0.6785	0.8028	K-means [25]	56.80	0.8319	0.5728	0.6751
1D CNN [29]	0.868	0.854	0.861	NB [25]	90.36	0.8195	0.7692	0.8595
MADGAN [30]	0.9897	0.6374	0.77	AllKNN [12]	**97**	**0.98**	0.92	0.95
Tabor [31]	0.8617	0.7880	0.8232	LSTM [32]	92	0.94	0.78	0.85
LSTM [33]	0.951	0.627	0.756					
ST-ED [33]	0.949	0.705	0.809					

Comparison Of The Proposed Attack Detection Method With Other Techniques On The Gas Pipeline And Swat Datasets

Model	NMRI	CMRI	MSCI	MPCI	MFCI	DoS	Recon.
Proposed attack detection method	0.97	0.95	0.97	0.95	1	1	1
AHKNN [12]	0.93	0.76	0.68	0.85	1	0.98	1
LSTM [32]	0.88	0.67	0.62	0.80	1	0.94	1
K-means [25]	0.19	0.20	0.73	0.66	0.52	0.56	0.75
NB [25]	0.81	0.84	0.73	0.67	0.52	0.79	0.50

Comparison between the Recall of the Proposed Attack Detection Method and Other Techniques On The Gas Pipeline Dataset Attack Attributes.



Comparison of accuracy , AUC, and f- measure of the proposed attack detection method and other basic classifiers onoriginal representation for different attack IR (A), (B), and (C) on the gas pipeline dataset and (D), (E), and (F) on the SWaT dataset. In the figures, PM is the proposed attack detection method, DT is the Decision Tree, LR is the Logistic Regression, GB is the Gradient Boosting, AB is the AdaBoost M1, and RF is the Random Forest.

CONCLUSION

A unique two-stage ensemble deep learning-based attack detection and attack attribution paradigm for imbalanced ICS data was proposed in this research. The attack detection stage applies a DT to identify the attack samples after mapping the samples to the new higher dimensional space using deep representation learning. This stage can identify previously undiscovered assaults and is resistant to imbalanced datasets. Each one-vs-all classifier in the attack attribution stage has been trained on a different attack attribute. As shown, the entire model creates a complicated DNN with a component that is both partially and fully connected and can correctly identify cyber attacks. Although the proposed framework has a complicated design, the training and testing phases' computational complexity is only O(n4) and O(n2), (n is the number of training samples), which are similar to those of other DNN-based techniques in the literature. Moreover, the proposed framework can detect and attribute the samples timely with a better recall and f-measure than previous works.

REFERENCES

1. F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, “Multilayer Data- Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data,” IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362–4369,2019.
2. R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, “Stealthy Attack Against Redundant Controller Architectureof Industrial Cyber- Physical System,” IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9783–9793, 2019.

3. E. Nakashima, “Foreign hackers targeted U.S. water plant in apparentmalicious cyber attack, expert says.”
4. G. Falco, C. Caldera, and H. Shrobe, “IIoT Cybersecurity Risk Modeling for SCADA Systems,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4486– 4495, 2018.
5. 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.
6. S. Ponomarev and T. Atkison,“Industrial control system networkintrusion detection by telemetry analysis,” IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252– 260, 2016.