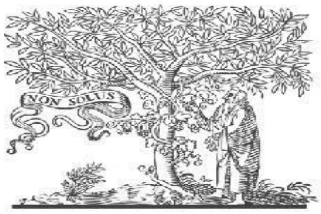
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT



ELSEVIER
SSRN

2023IJIEMR.Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 07th Jan 2023. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-1

DOI: 10.48047/IJIEMR/V12/ISSUE 01/47

Title **Aiming For Cyber-Attack Detection And Attribution In Internet-Of-Things-Enabled Cyber-Physical Systems**

Volume 12, Issue 1, Pages: 524-532

Paper Authors
Mrs. P.Shailaja Rani, V.Harisha, N.v.Chandana, P.Sravani, M.Harsha Bai

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Aiming For Cyber-Attack Detection And Attribution In Internet-Of-Things-Enabled Cyber-Physical Systems

Mrs. P.Shailaja Rani, Assistant professor, Dept. of Information Technology, Sridevi Women's Engineering College, Hyd. swec.shailajarani@gmail.com

V.Harisha, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

N.v.Chandana, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

P.Sravani, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

ABSTRACT— Cyber-physical systems (CPS) enabled by the Internet of Things (IoT) provide unique security challenges since security solutions designed for traditional IT/OT systems may not be adequate in a CPS environment. Therefore, this research introduces a two-tiered ensemble attack detection and attribution framework fit for CPS, and more especially in an industrial control system (ICS). In order to identify assaults in unbalanced ICS settings, a decision tree is paired with an unique ensemble deep representation-learning model. For the next step, we use a deep neural network ensemble to help with assault attribution. Data sets from the gas pipeline and water treatment system are used to test the proposed model in the wild. The results show that the suggested model performs better than competing methods of equivalent computing complexity.

INTRODUCTION

Cyber-physical systems (CPS) now routinely include IoT devices, even in mission-critical settings like dams and power plants. Industrial Internet of Things (IIoT) devices are often integrated into an ICS, whose primary responsibility is to ensure the secure functioning of the aforementioned infrastructure. Systems that use programmable logic controllers (PLC) and Modbus protocols, as well as SCADA systems for monitoring and controlling machinery, fall under the umbrella term "industrial control system" (ICS). However, when ICS or IIoT-based systems are linked to the internet, their attack surfaces and susceptibilities to cyber attacks grow. In 2010, for instance, the Stuxnet campaign apparently targeted Iranian centrifuges used in nuclear enrichment, inflicting extensive

damage to the machinery. Another event that illustrates this point is the 2011 attack on a pump that caused the breakdown of an Illinois water facility. System-level security solutions are required for this reason in order to conduct a thorough analysis of physical behaviour and guarantee the continued availability of the system. Unlike IT/OT systems, the objectives of ICS security are ordered from most important to least important, starting with availability and ending with secrecy (generally prioritised in the order of confidentiality, integrity, and availability) A (successful) cyber-attack against ICS may have devastating effects for people and the planet because of the intricate interplay between the variables of the feedback control loop and the underlying physical processes. This highlights the need for very effective safety and security measures to be designed to detect and prevent attacks targeting ICS. Signature and anomaly-based attack detection and attribution methods are widely used. It has been attempted to offer hybrid-based techniques to detection and attribution, which combine the strengths of signature-based and anomaly-based methods. Different Intrusion Detection System (IDS) typologies have emerged as a consequence of the regular changes to networks, making hybrid-based methods to anomaly detection less trustworthy. The next step is network information analysis, which is where most traditional attack detection and attribution methods start and end (e.g. IP addresses, transmission ports, traffic duration, and packet intervals). As a result, recently there has been a resurgence of enthusiasm for using attack detection and attribution options grounded on Machine Learning (ML) or Deep Neural Networks (DNN). There are two main types of methods used to spot attacks: network-based and host-based. Methods such as supervised clustering, fuzzy logic, Artificial Neural Networks (ANN), Support Vector Machines (SVM) (both single- and multi-class),On order to identify attacks in network traffic, DNNs are widely utilised. In order to quickly identify malicious assaults, these methods monitor traffic data in real time. Network and host-based attack detection, however, may miss more sophisticated forms of assault, including those launched from inside an organisation.

RELATED WORK

Multi-Layer Network, System, and Process Data-Driven Cyber-Attack Detection System for Industrial Control Systems

Cybersecurity threats to industrial control systems have increased in recent years due to an increase in assaults on cyber-physical systems (ICSs). Firewalls, data diodes, and other intrusion prevention technologies form the backbone of ICS cybersecurity today, but they may not be enough to fend off the increasingly sophisticated and targeted cyberattacks that are being launched by determined adversaries. A cyber-attack detection system is designed for ICS that makes use of network traffic data, host system data, and monitored process parameters to improve ICS cybersecurity. This assault detection system offers layered protection to buy the defenders some time before the attack does irreparable damage to the physical system. The suggested detection method is shown using data from a live ICS demonstration platform. In order to replicate the effects of a cyberattack and collect data for data-driven detection models, five types of assaults are performed: man-in-the-middle (MITM), denial of service (DoS), data exfiltration (DX), data tampering (DT), and fake data injection (FI). In order to provide a backup line of defence for cyber-attack detection in case the intrusion prevention layer fails, the literature reviews four classical classification models based on network data and host system data: k-nearest neighbour (KNN), decision tree (DT), bootstrap aggregating (bagging), and random forest (RF). The results of intrusion detection tests indicate that KNN, bagging, and RF provide accurate and reliable detection of MITM and DoS assaults with low missed alert and false alarm rates. Traditional process monitoring systems look out for cyberattacks such command manipulation and bogus data injection assaults by an insider, which may not be seen by monitoring network and host system data. The suggested detection method investigates an auto-associative kernel regression model to improve attack detection in its early stages.

Subtle Exploitation of Vulnerabilities in Industrial CyberPhysical Systems' Redundant Controller Architecture

The controller's function is crucial to ensuring the steady operation of an industrial cyber-physical system (iCPS). Since this is the case, common iCPSs like distributed control systems (DCS), supervisory control and data acquisition (SCADA), and others all make use of a redundant controller architecture. They keep an eye on and manage vital operations in the power plant, chemical plant, water treatment facility, and other industries. In light of the

unpredictability of mechanical breakdowns, a redundancy-rich architecture for controllers has been developed and widely deployed. This structure was recommended to provide dependability and safety, however there is a chance that an attacker may use it to conduct covert assaults on the network. This article examines the security hole caused by duplicate controller architecture and suggests a covert, multi-pronged attack strategy against systems using this design. We discover many zero-day vulnerabilities in production devices from three manufacturers and then deploy the combined assault against them. Our testing findings on a wide range of real-world devices demonstrate that the redundant controller design can be used to covertly infiltrate all tested systems. Additionally, we provide recommendations for lowering the danger level.

METHODOLOGY

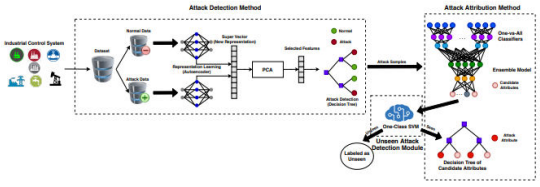
Both a representation-learning and a detection phase make up the proposed attack detection. Applying a standard unsupervised DNN on an uneven dataset resulted in a DNN model that focused on learning properties of the dominant class at the expense of those of the minority. This problem has been addressed by most studies by either creating fresh samples or eliminating certain samples from the dataset so that it is more evenly distributed before feeding it to a DNN. It is not practical to generate or eliminate samples in ICS/IIoT security applications. Due to the critical nature of ICS/IIoT systems, it is difficult to test produced samples in a real network, since doing so would expose the network to attack and potentially endanger people and the environment. It also takes a long time to verify the quality of the produced samples.

Since the number of attack samples in ICS/IIoT datasets is often less than 10% of the dataset and most of the dataset information is destroyed by deleting 80% of the dataset, discarding the normal data from a dataset is not the proper option.This research presented a novel deep representation learning approach to equip the DNN to deal with unbalanced datasets without resorting to sample generation, manipulation, or removal in order to circumvent the aforementioned difficulties.Specifically, this model used a pair of unsupervised stacked autoencoders, each of which was tasked with discovering patterns inside its own respective class.Given that each model seeks to isolate the abstract patterns of a single class while

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ignoring all others, the results accurately reflected the inputs used to train that model. A total of three layers of input and output representations were used in the stacked autoencoders. The encoder layers transformed the input representation into higher dimensional spaces of 800, 400, and 16 respectively. An autoencoder's encoding capability is represented by Equation 1. Conversely, the decoder layers began with the 16-dimensional new representation and mapped it to the 400-dimensional, 800-dimensional, and input representations in an effort to recover the input representation. The autoencoder decoder . Through trial and error, the optimal f-measure performance and minimal architectural complexity hyperparameters were determined.

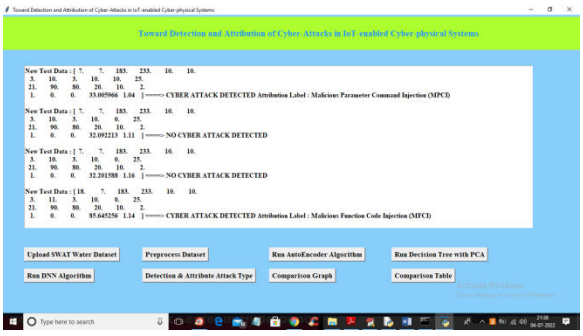
$$h_i = \sigma(w_i x_i + b_i)$$



Proposed attack detection and attribution framework

RESULT AND DISCUSSION

By clicking the "Open" button to import the dataset, we can see that the "NORMAL" class has a large number of records while the other attack classes have relatively few, highlighting a data imbalance issue that can be addressed using AutoEncoder, Decision Tree, and Deep Neural Networks (DNNs). We first normalised the data by removing any outlying or missing values. After the values have been normalised (that is, converted to a value between 0 and 1), the whole number of records in the dataset, as well as the numbers for the train and test sets, are shown. To use AutoEncoder for dataset training, click the Run AutoEncoder Algorithm button.



With the ⍰sign, we can see the detected ATTACK TYPE and, by scrolling up above the text box, we can see all detections.

DNN performed very well across the board, achieving excellent precision, recall, accuracy, and FSCORE scores.

CONCLUSION

An original approach for attack detection and attack attribution using ensembles of deep learners was developed for use with unbalanced ICS data in this article. In order to map the samples to a database that can identify attacks, deep representation learning is used in the attack detection step.

to a new, higher-dimensional realm and uses a DT to spot the attack samples. Since this step may identify attacks that haven't been seen before, it's also resistant to datasets that aren't evenly distributed. Attributing attacks requires an ensemble of several one-vs-all classifiers, each of which is trained to recognise a different kind of assault. As a whole, the model is a complicated DNN with a partly connected and completely connected section that can correctly identify cyberattacks. Training and testing phases have computational complexity of O(n 4) and O(n 2), (n is the number of training samples), respectively, which is comparable to that of other DNN-based approaches in the literature despite the proposed framework's complicated design.In addition, the suggested framework is able to recognise and assign the samples in a timely manner with increased recall and f-measure.Designing a cyber-threat hunting component to help spot abnormalities missed by the detection component, such as by creating a baseline profile of the system and its assets, is an area for potential growth.

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 Architecture of Industrial CyberPhysical 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 apparent malicious cyber attack, expert says.” [Online]. Available: https://www.washingtonpost.com/blogs/checkpointwashington/post/foreign-hackers-broke-into-illinois-water-plant-controlsystem-industry-expert-says/2011/11/18/gIQAgmTZYN blog.html

[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 network intrusion detection by telemetry analysis," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252–260, 2016.

[7] J. F. Clemente, "No cyber security for critical energy infrastructure," Ph.D. dissertation, Naval Postgraduate School, 2018.
[8] C. Bellinger, S. Sharma, and N. Japkowicz, "One-class versus binary classification: Which and when?" in 2012 11th International Conference on Machine Learning and Applications, vol. 2, 2012, pp. 102–106.

[9] I. Goodfellow, Y. Bengio, and A. Courville, Deep learning. MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org
[10] Y. Bengio, A. Courville, and P. Vincent, "Representation learning: A review and new perspectives," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp. 1798–1828, 2013.

[11] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822–6834, 2019.

[12] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," IEEE Access, vol. 7, pp. 89 507–89 521, 2019.

[13] T. K. Das, S. Adepu, and J. Zhou, "Anomaly detection in industrial control systems using logical analysis of data," Computers & Security, vol. 96, p. 101935, 2020.

[14] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3271–3280, 2018.
[15] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial iot," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8462–8471, 2020.

[16] W. Yan, L. K. Mestha, and M. Abbaszadeh, "Attack detection for securing cyber physical systems," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8471–8481, 2019.

[17] A. Cook, A. Nicholson, H. Janicke, L. Maglaras, and R. Smith, "Attribution of Cyber

Attacks on Industrial Control Systems," EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, vol. 3, no. 7, p. 151158, 2016.

[18] L. Maglaras, M. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis, "Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures," ICST Transactions on Security and Safety, vol. 5, no. 16, p. 155856, 2018.

[19] M. Alaeiyan, A. Dehghantanha, T. Dargahi, M. Conti, and S. Parsa, "A Multilabel Fuzzy Relevance Clustering System for Malware Attack Attribution in the Edge Layer of Cyber-Physical Networks," ACM Transactions on Cyber-Physical Systems, vol. 4, no. 3, pp. 1–22, 2020.

[20] U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo, "A machine learning-based FinTech cyber threat attribution framework using highlevel indicators of compromise," Future Generation Computer Systems, vol. 96, pp. 227–242, 2019.
[21] S. Wold, K. Esbensen, and P. Geladi, "Principal component analysis," Chemometrics and Intelligent Laboratory Systems, vol. 2, no. 1, pp. 37 – 52, 1987, proceedings of the Multivariate Statistical Workshop for Geologists and Geochemists.

[22] A. N. Jahromi, J. Sakhnini, H. Karimpour, and A. Dehghantanha, "A deep unsupervised representation learning approach for effective cyber-physical attack detection and identification on highly imbalanced data," in Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering, ser. CASCON '19. USA: IBM Corp., 2019, p. 14–23.

[23] T. Morris, Z. Thornton, and I. Tunipseed, "Industrial control system simulation and data logging for intrusion detection system research," in 7th Annual Southeastern Cyber Security Summit, 2015.

[24] J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, "A dataset to support research in the design of secure water treatment systems," in Critical Information Infrastructures Security, G. Havarneanu, R. Setola, H. Nassopoulos, and S. Wolthusen, Eds. Cham: Springer International Publishing, 2017, pp. 88–99.

[25] S. N. Shirazi, A. Gouglidis, K. N. Syeda, S. Simpson, A. Mauthe, I. M. Stephanakis, and D. Hutchison, "Evaluation of anomaly detection techniques for scada communication resilience," in 2016 Resilience Week (RWS), 2016, pp. 140–145.

[26] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," IEEE International Conference on Data Mining Workshops, ICDMW, vol. 2017-November, pp. 1058–1065, 2017.

[27] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," Proceedings of the ACM Conference on Computer and Communications Security, no. 1, pp. 72–83, 2018.

[28] S. D. Anton, A. Hafner, S. Sinha, and H. Schotten, "Anomaly-based intrusion detection in industrial aata with SVM and random forests," in the 27th International Conference on Software, Telecommunicationsand Computer Networks (SoftCOM). IEEE, 2019.

[29] M. Kravchik and A. Shabtai, "Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca," IEEE transactions on dependable and secure computing, pp. 1–1, 2021.

[30] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S. K. Ng, "MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 11730 LNCS, pp. 703–716, 2019.

[31] Q. Lin, S. Verwer, S. Adepu, and A. Mathur, "TABOR: A graphical model-based approach for anomaly detection in industrial control systems," ASIACCS 2018 - Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security, pp. 525–536, 2018.

[32] C. Feng, T. Li, and D. Chana, "Multi-level anomaly detection in industrial control systems via package signatures and lstm networks," in 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017, pp. 261–272.

[33] M. Macas and W. Chunming, "Enhanced cyber-physical security through deep learning techniques," CEUR Workshop Proceedings, vol. 2457, no. 38, 2019.

[34] C.-t. Chu, S. Kim, Y.-a. Lin, Y. Yu, G. Bradski, K. Olukotun, and A. Ng, "Map-reduce for machine learning on multicore," in Advances in Neural Information Processing Systems, B. Scholkopf, J. Platt, and T. Hoffman, ¨ Eds., vol. 19. MIT Press, 2007, pp. 281–288.

[35] J. Su and H. Zhang, "A fast decision tree learning algorithm," in Proceedings of the 21st National Conference on Artificial Intelligence - Volume 1, ser. AAAI'06. AAAI Press, 2006, p. 500–505.