Toward Detection and Attribution of Cyber-Attacks in IOT-Enabled Cyber-Physical Systems

Dr.C.Ramesh Kumar [1] and Mr.P.Vinay Kumar [2]Dr.U.Ratnam[3]

[1] Assoc.Professor, Department of Information Technology, MREC (A), Hyderabad-500100
[2] Assistant Professor, Department of Information Technology, MREC (A), Hyderabad-500100
[3] Assoc.Professor, Department of CE, MREC (A), Hyderabad-500100

Abstract

Securing Internet of Things (IoT)-enabled cyber- physical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT / OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a decision tree combined with a novel ensemble deep representation- learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The proposed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

Keywords: IOT, CPS, IT, OT, ICS, ML, DNN.

I. Introduction

Infrastructure constitutes any physical asset capable of being utilized to produce services or support the structure and operation of a society or an enterprise and include roadways, bridges, airports and airway facilities, mass transportation systems, waste treatment plants, energy facilities, hospitals, public buildings and space or communication facilities. Critical infrastructure on the other hand consist of physical, virtual facilities and services that form the basis for a nation"s defense, a strong economy, health and safety of its citizens. It is charged with the provision of necessities such as water and food, electricity and gas, telecommunications and broadcasting, health services, the financial system and the transportation system. Every critical infrastructure constitute of an Industrial Control System (ICS) that is made up of

Supervisory Control and Data Acquisition (SCADA) systems and other types of control systems that monitor processes and control flows of information. ICS serve to regulate the flow of natural gas to a power generation facility or the flow of electricity from a grid to a home. Cyber systems form the central infrastructure of critical sectors as nearly all of them utilize IT to facilitate core business processes. Given their high value nature, the cyber systems of critical infrastructure have become targets for attack, and their disruptions have led to extensive economic, political and social effects. The cyber systems consist of various software, the development of which, according to Sebastian and Stephan (2018), comprises of diverse activities such as implementing new features, analyzing requirements, and fixing bugs. Universal satellite and data connectivity is one of the major advancements in seafaring. Many critical systems on board rely on the Global Navigation Satellite System (GNSS) for safe navigation, communication, emergency response, and traffic control. However, disrupted or manipulated Global Positioning System (GPS) signals can send ships off their course and cause collisions, groundings, and environmental disasters (Dennis et al., 2017).

Internet of Things (IoT) devices are increasingly integrated in cyber-physical systems (CPS), including in critical infrastructure sectors such as dams and utility plants. In these settings, IoT devices (also referred to as Industrial IoT or IIoT) are often part of an Industrial Control System (ICS), tasked with the reliable operation of the infrastructure. ICS can be broadly defined to include supervisory control and data

acquisition (SCADA) systems, distributed control systems (DCS), and systems that comprise programmable logic controllers (PLC) and Modbus protocols. The connection between ICS or IIoT-based systems with public networks, however, increases their attack surfaces and risks of being targeted by cyber criminals. One high-profile example is the Stuxnet campaign, which reportedly 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 April 2018, 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 are relatively mature, they may not be directly applicable to ICSs. For example, this could be 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 behaviour and maintain system operation availability [1]. ICS security goals are prioritized in the order of availability, integrity, and confidentiality, unlike most IT/OT systems (generally prioritized in the order of confidentiality, integrity, and availability) [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 [1]. Popular attack detection and attribution approaches include those based on signatures and anomalies. To mitigate the known limitations in both signature-based and anomaly-based detection and attribution approaches, there have been attempts to introduce hybrid-based approaches [6]. Although hybrid based approaches are effective at detecting unusual activates, they are not reliable due to frequent network upgrades, resulting in different Intrusion Detection System (IDS) typologies [7]. Beyond this, conventional attack detection and attribution techniques mainly rely on network metadata analysis (e.g. IP addresses, transmission ports, traffic duration, and packet intervals). Therefore, there has been renewed interest in utilizing attack detection and attribution solutions based on Machine Learning (ML) or Deep Neural Networks (DNN) in recent times. In addition, attack detection approaches can be categorized into network-based or host-based approaches. Supervised clustering, single-class or multi-class Support Vector Machine (SVM), fuzzy logic, Artificial Neural Network (ANN), and DNN are commonly used techniques for attack detection in network traffic. These techniques analyze real-time traffic data to detect malicious attacks in a timely manner. However, attack detection that considers only network and host data may fail to detect sophisticated attacks or insider attacks.

II. Survey of Research

According to Tobby (2017),the Internet of Things (IoT) is a vital concept embedded within a larger spectrum of networked products and digital sensors. This technology has caused an explosion of applications, marking a fundamental shift in the way human beings interact with the Internet and presenting both opportunities and challenges, particularly with respect to critical infrastructure. For instance hackers have used IoT devices such as printers, thermostats and videoconferencing equipment to breach security systems. The Internet-enabled infrastructures have facilitated home automation, energy-management systems, smart homes, network-enabled medical gadgets, intelligent vehicles, networked traffic systems, road and bridge sensors, innovations in agricultural, industrial, energy production and distribution. Although this has opened up numerous avenues for efficiency, the unregulated rise of the IoT raises a plethora of issues such as security and privacy of people, telecoms networks and power utilities. This is due to illegitimate breaches of the networks undergirding critical infrastructure since the efficiency of Internet connectivity also accelerates susceptibility to security violations through the misuse of IoT data. Although an ICS is air-gapped and hence a closed system, it may not be vulnerable to virtual attacks but is still susceptible to attacks perpetrated through physical access such as from infected removable devices. As technology continues to grow, a number of ICSs have been connected to the Internet, making them vulnerable to multifarious attacks. Computers and communications being critical infrastructures in their own right are increasingly connecting other infrastructures together. The increased connectivity means that a disruption in one network may lead to disruption in another and hence reliance on computers and networks increases critical infrastructure‟s vulnerability to cyber attacks.

According to Arash and Stuart (2015), CPS provides the control of physical components through cyber based commands and its operations are integrated, monitored, or controlled by a computational core. By integrating actuators, control processing units, sensors, and communication cores, a CPS forms a control loop for each of the physical component of the system. The major components of a CPS are SCADA, distributed control system (DCS), and program logic controller (PLC). The SCADA systems gather and control geographically dispersed assets ranging from controlling sensors within a plant to controlling power dissemination in a country. They are heavily utilized in various critical infrastructures such as electrical power grids, water distribution systems, and oil refineries. On the other hand, DCS manages the controllers that are grouped together to carry out a specific task within the same geographically location. Both SCADA and DCS employ PLC devices to manage industrial components and processes. PLCs are typically programmed from a Windows-based machine by an operator. The operators utilizes SCADA and DCS for various controlling tasks such as process monitoring and configuring control parameters. In their paper, Lange et al., (2016) point out that the success of a business mission is highly dependent on the Communications and Information Systems (CIS) that support the mission. As such, cyber attacks on CIS degrade or disrupt the performance and completion of

the associated mission capability. On an operational level, an electrical grid‟s mission is to deliver electricity from suppliers to consumers. For monitoring and control purposes, they are connected to CIS. The operability, performance, or reliability of an application may depend on multiple network services spanning multiple network devices and sub-networks of an infrastructure. The risks associated with vulnerable software deployed in enterprise environments have exposed customer data or intellectual property and can be caused by attackers exploiting weaknesses in web applications or desktop software. Lack of consistent, proactive policies to manage vulnerabilities associated with the Bring Your Own Device (BYOD) trend. Mobile devices come with one huge challenge of ensuring that all valuable information is secure and the increasing number of these devices elevates the threat of accidental and intentional security breaches. As such, verifying the security of the software being downloaded to those devices is becoming a business priority. This is important since platforms such as Google‟s Android do minimal vetting of the safety of applications before permitting consumers to download from their App store.

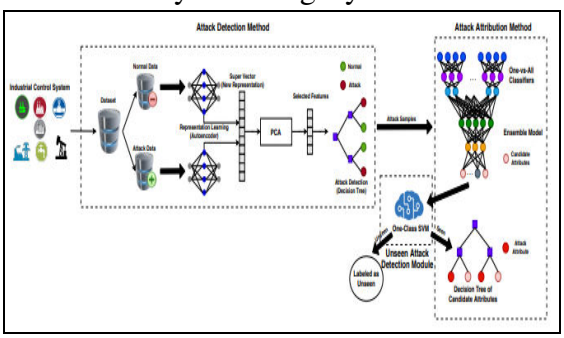
The comparative summary suggested that the RF algorithm has the best attack detection, with a recall of 0.9744; the ANN is the fifth-best algorithm, with a recall of 0.8718; and the LR is the worst- performing algorithm, with a recall of 0.4744. The authors also reported that the ANN could not detect 12.82% of the attacks and considered 0.03% of the normal samples to be attacks. In addition, LR, SVM, and KNN considered many attack samples as normal samples, and these ML algorithms are sensitive to imbalanced data. In other words, they are not suitable for attack detection in ICS. In [12], the authors presented a KNN algorithm to detect cyber-attacks on gas pipelines. To minimize the effect of using an imbalanced dataset in the algorithm, they performed oversampling on the dataset to achieve balance. Using the KNN on the balanced dataset, they reported an accuracy of 97%, a precision of 0.98, a recall of 0.92, and an f-measure of 0.95. In [13], the authors presented a Logical Analysis of Data (LAD) method to extract patterns/rules from the sensor data and use these patterns/rules to design a two-step anomaly detection system. In the first step, a system is classified as stable or unstable, and in the second one, the presence of an attack is determined. They compared the performance of the proposed LAD method with the DNN, SVM, and CNN methods. Based on these experiments, the DNN outperformed the LAD method in the precision metric; however, the LAD performed better in recall and f-measure.

Unsupervised models that incorporate process/physical data can complement a system’s monitoring since they do not rely on detailed knowledge of the cyber-threats. In general, a sophisticated attacker with sufficient knowledge and time, such as a nation state advanced persistent threat actor, can potentially circumvent robust security solutions. Furthermore, most of the existing approaches ignore the imbalanced prop- erty of ICS data by modeling only a system’s normal behavior and reporting deviations from normal behavior as anomalies. This is, perhaps, due to limited attack samples in existing datasets and real-world scenario.

III. Proposed Methodology

A critical transportation infrastructure integrated with the Internet of Things based wireless sensor network, operates as a cyber-physical system. However, the new form of IoT enabled transportation infrastructure is susceptible to cyber-physical attacks in the sensing area, due to inherent cyber vulnerabilities of IoT devices and deficient control barriers that could protect it. Traditional risk assessment processes, consider the physical and cyber space as isolated environments, resulting in IoT enabled transportation infrastructure not being assessed by stakeholders (i.e., operators, civil and security engineers) for cyber-physical attacks. In this paper, a new risk assessment approach for cyber-physical attacks against IoT based wireless sensor network is proposed. The approach relies on the identification and proposal of novel cyber-physical characteristics, in the aspect of threat source (e.g., motives), vulnerability (e.g., lack of authentication mechanisms) and types of physical impacts (e.g., casualties). Cyber-physical risk is computed as a product of the level and importance of these characteristics. Monte Carlo simulations and sensitivity analysis are performed to evaluate the results of an IoT enabled bridge subjected to cyber-physical attack scenarios. The results indicate that 76.6% of simulated cases have high-risk and control barriers operating in physical and cyber space can reduce the cyber-physical risk by 71.8%. Additionally, cyber-physical risk differentiates when the importance of the characteristics that are considered during risk assessment is overlooked. The approach is of interest to stakeholders who attempt to incorporate the cyber domain in risk assessment procedures of their system.

The recent years have garnered huge attention towards the Internet of Things (IoT) because it enables its consumers to improve their lifestyles and professionally keep up with the technological advancements in the cyber-physical world. The IoT edge devices are heterogeneous in terms of the technology they are built on and the storage file formats used. These devices require highly secure modes of mutual authentication to authenticate each other before actually sending the data. Mutual authentication is a very important aspect of peer-to-peer communication. Secure session keys enable these resource-constrained devices to authenticate each other. After successful authentication, a device can be authorized and can be granted access to shared resources. The need for validating a device requesting data transfer to avoid data privacy breaches that may compromise confidentiality and integrity.



IV. Results Discussion

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 this challenge by generating new samples or removing 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. To avoid the above mentioned problems in handling imbalanced datasets, this study proposed a new deep representation learning method to make the DNN able to handle imbalanced datasets without changing, generating, or removing samples. This model consisted of two unsupervised stacked auto encoders, each responsible for finding patterns from one class. Since each model tries to extract abstract patterns of one class without considering another, the output of that model represented its inputs well. The stacked auto encoders had three decoders and encoders with input and final representation layers. The encoder layers mapped the input representation to a higher, 800-dimensional space, a 400-dimensional space, and the final 16-dimensional space. The encoder functions of an auto encoder. The decoder layers did the opposite and tried to reconstruct the input representation by starting from the 16-dimensional new representation and mapping it to the 400-dimensional, 800-dimensional, and input representations. The decoder function of an auto encoder. These hyper parameters were selected using trialand-error to have the best performance in f-measure with the lowest architectural complexity.

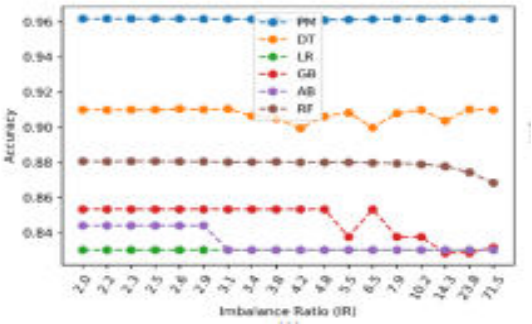


Fig.1. Output results with attacks.

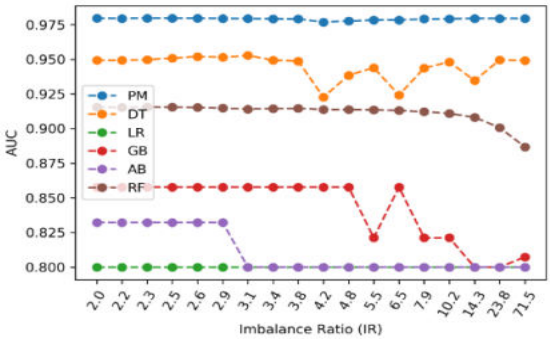


Fig.2. Ratio of imbalance.

V. Conclusion

This paper proposed a novel two-stage ensemble deep learning-based attack detection and attack attribution framework for imbalanced ICS data. The attack detection stage uses deep representation learning to map the samples to the new higher dimensional space and applies a DT to detect the attack samples. This stage is robust to imbalanced datasets and capable of detecting previously unseen attacks. The attack attribution stage is an ensemble of several one-vs-all classifiers, each trained on a specific attack attribute. The entire model forms a complex DNN with a partially connected and fully connected component that can accurately attribute

cyberattacks, as demonstrated. Despite the complex architecture of the proposed framework, the computational complexity of the training and testing phases are respectively O(n 4) and O(n 2), (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. Future extension includes the design of a cyber-threat hunting component to facilitate the identification of anomalies invisible to the detection component for example by building a normal profile over the entire system and the assets.

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.