|| Volume 6 || Issue 2 || February 2021 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

A SURVEY ON MACHINE LEARNING BASED CYBER-ATTACK DETECTION TECHNIQUES FOR DISTRIBUTION SYSTEMS

Miss. Trupti Ghotkar[1], Mrs. Dipalee D. Rane[2]

Post Graduate Student[1], Assistant Professor[2], Department of Computer Engineering, D. Y. Patil College of Engineering, Akurdi, Pune

-- ***--

Abstract:- **Critical infrastructure systems are of major importance to society as they have a great impact on people's lives and the economy. Examples include the energy systems, telecommunication systems and water supply. These cyber-physical systems are operated by means of computers and applications using two-way communication capabilities and distributed intelligence to enhance efficiency, reliability, and stability. Attacks on cyber-physical systems have recently increased in frequency, impact and publicity. Cyber-physical false data attack detection methods are presented in this research paper which can protect the operation of power transmission and distribution systems. This is achieved by automatically inferring underlying physical relationships using cross-sensor analytics in order to detect sensor failures, replay attacks and other data integrity issues in real-time.**

Keyword- *Cyberattack Detection, Machine Learning, Bayes Classification, LSTM*

-- ***--

I INTRODUCTION

The electric grid has evolved over the past century from a series of small independent community-based systems to perhaps the largest and most complex cyber-physical system in the world. The increasing demand for reliable energy has motivated the development of a smart electric grid. The smart grid expands the current capabilities of the grid's generation, transmission and distribution systems. It provides an infrastructure capable of handling future requirements for distributed generation, renewable energy sources, electric vehicles and the demand-side management of electricity. The increasing reliance on cyber-infrastructure to manage highly complex smart grids comes with the risk of cyber-attacks by adversaries around the globe. For example, the hacking of Ukrainian electrical power utilities in 2015 caused a sustained loss of electricity to roughly 80,000 customers. In addition, the cyber-attack on Pacific Gas & Electric's Metcalf substation in northern California caused more than $15 million in damage. Both of those attacks manipulated sensors to directly blind and disrupt the control centres. The successful functioning of complex cyber-physical systems depends on the reliable operation of a control loop that takes sensor data as input and produces control decisions as output. While some attacks are essentially cyber-attacks for example hacking into a controller and re-routing poweror physical attacks such as destroying physical equipment. All major attacks have also exclusively manipulated the operator control loop to hide or to exacerbate the attack's impact. The operator control loop is the feedback loop which operators use to assess the situation and make decisions. By manipulating this loop, even if no physical damage is created directly, it is possible for attackers to indirectly create wide-ranging and devastatingimpacts including brown-outs, surges and black-outs. All of these attacks have one thing in common which is that they compromise the integrity of the sensor data.

II LITERATURE SURVEY

In [1], a flexible machine learning based cyber-attack detection method is developed by using the Generalized Graph Laplacian (GGL) and flexible Bayes classifier (BC). Spatiotemporal patterns are quantitatively characterized by GGL which could be compromised when cyber-attacks occur. The flexible BC is used for training spatiotemporal patterns of system measurements and detecting cyber-attacks online. Numerical results of case studies verify the effectiveness of the developed cyber-attack detection method based on machine learning techniques.

Based on the electric waveform data measured by waveform sensors in the distribution power networks, in [2], Fangyu et al proposed a novel high-dimensional data-driven cyber physical attack detection and identification

DOI : 10.51319/2456-0774.2021.2.0029

approach (HCADI). Firstly, the cyber and physical attack impacts are analysed on electric waveforms in distribution power grids. Then, a high dimensional streaming data feature matrix based on signal analysis of multiple sensors in the network is constructed. A novel mechanism including leverage score-based attack detection and binary matrix factorization-based attack diagnosis is proposed. By leveraging the data structure and binary coding, HCADI approach does not need the training stage for both detection and the root cause diagnosis which is needed for machine learning/deep learning-based methods. It is the first attempt to use raw electrical waveform data to detect and identify the power electronics cyber/physical attacks in distribution power grids with Photovoltaics.

In [3], Ferragut et al investigated a neural network-based mechanism acting on voltage and current readings resulting from a wide variety of load conditions on the IEEE 30-bus power system standard and compared its performance with a support vector machine-based mechanism. Experiments showed that 99% detection accuracy of replay attacks was achieved using the proposed neural network mechanism. It was observed that the best approach was to use a neural network to automatically learn the laws and then use the outputs of that to build a classifier to identify whether and where data spoofing occurs. The proposed mechanism directly addresses the problem of sensor trustworthiness by identifying readings across multiple sensors that indicate states that are not physically possible. And hence it is concluded by the team that it is preferable to infer and exploit the physics using a single machine learning solution rather than to add features first and then build a detector.

In [4], a machine learning based anomaly detection (MLAD) method is developed for load forecasting under cyber-attacks. The predicted load data is first used to reconstruct the benchmark and scaling data by using the k-means clustering. The naive Bayes classification is then used to determine the specific attack template. Finally, the dynamic programming is utilized to calculate both the occurrence and the parameter of one cyber-attack on load forecasting data. Compared with the widely-used Symbolic Aggregation approXimation method, the effectiveness and robustness of the proposed method is verified by numerical simulations on the publicly load data.

In [5], Yaokai Feng et al focused on the issue of feature selection for early detection of distributed cyber-attacks. Implementation is done by the early detection by detecting Command &Control(C&C) communication of distributed attacks because those communication is at the preparation phase of distributed attacks. Based on the previous research using 55 features to detect C&C communication, in this paper investigation is done considering the following thought: what if we remove the features from those of the least importance. This is done for the purpose of finding that what features are actually critical for early detection of distributed attacks. From the experiments conducted using traffic data collected by honeypots, it is observed that the detection performance is generally getting better if more features are utilized. However, after the number of features has reached around 40, the detection performance will not change much even more features are used. The top-10 important features for detecting C&C traffic are found and it is also verified that some bad features would deteriorate the detection performance.

In [6], a novel detection model for the detection of cyber-attacks is proposed using remote sensing data on water distribution systems i.e., pipe flow sensor, nodal pressure sensor, tank water level sensor, and programmable logic controllers by machine learning approaches. The most commonly used and well-known machine learning algorithms i.e., k-nearest neighbour, support vector machine, artificial neural network, and extreme learning machine were compared to determine the one with the best detection performance. After identifying the best algorithm, several improved versions of the algorithm are compared and analysed according to their characteristics. Their quantitative performances and abilities to correctly classify the state of the urban water system under cyber-attack were measured using various performance indices. Out of all the algorithms, the extreme learning machine (ELM) was found to exhibit the best performance. This study not only has identified excellent algorithm among the compared algorithms but also has considered an improved version of the outstanding algorithm. In this paper, the comparison was performed using various representative performance indices to quantitatively measure the prediction accuracy and select the most appropriate model. Hence, it can be considered that this study provides a new perspective on the characteristics of various versions of machine learning algorithms and their application to different problems. In the paper proposed by Soner Can Kalkan and OzgurKoraySahingoz[7], an Intrusion Detection System is proposed which aims to detect the attacks in the Controller

Area Network (CAN) bus structure of the cars. For the implementation of the system, a machine learning based approach is preferred with 6 different learning models. The results of the experiments conducted showed that the contain tree-based and ensemble learning approach are more efficient. In [8], Patric Nader and team proposed to use machine learning techniques, in particular one-class classification, in order to bring the necessary and complementary help to Intrusion Detection Systems in detecting cyber-attacks and intrusions. One-class classification algorithms have been used in many data mining applications where the available samples in the training dataset refer to a unique/single class. A simple one-class classification approach based on a new novelty measure, namely the truncated Mahalanobis distance in the feature space is proposed. The tests are conducted on a real dataset from the primary water distribution system in France, and the proposed approach is compared with other well-known one-class approaches. In [9], Nguyen et al proposed a novel framework that leverages a deep learning approach to detect cyber-attacks in mobile cloud environment. Through experimental results it is shown that the proposed framework not only recognizes diverse cyber-attacks but also achieves a high accuracy up to 97.11% in detecting the attacks. It presents the comparisons with current machine learning-based approaches to demonstrate the effectiveness of the proposed solution. The main purpose of [10] paper is to review and summarize the work of deep learning on machine health monitoring. The applications of deep learning in machine health monitoring systems are reviewed mainly from the following aspects: Autoencoder (AE) and its variants, Restricted Boltzmann Machines and its variants including Deep Belief Network (DBN) and Deep Boltzmann Machines (DBM), Convolutional Neural Network (CNN) and Recurrent Neural Networks (RNN). Advantage is that the Deep Learning-based Machine Health Monitoring System(MHMS) do not require extensive human labour and expert knowledge. The applications of deep learning models are not restricted to specific kinds of machines. Disadvantage is that the performance of DL-based MHMS heavily depends on the scale and quality of datasets. Hoyeop Lee and team proposes the use of a stacked denoising autoencoder (SdA) which is a deep learning algorithm used to establish a Fault Detection and Classification model for simultaneous feature extraction and classification. The SdA model [11] can identify global and invariant features in the sensor signals for fault monitoring and is robust against measurement noise. An SdA is consists of denoising auto encoders that are stacked layer by layer. This multi-layered architecture is capable of learning global features from complex input data such as multivariate time-series datasets and high-resolution images. Proposes a novel deep learning-based recurrent neural networks (RNNs) model [12] for automatic security audit of short messages from prisons which can classify short messages which are secure and non-insecure. In this paper, the feature of short messages is extracted by word2vec which captures word order information and each sentence is mapped to a feature vector. Words with similar meaning are mapped to a similar position in the vector space and then classified by RNNs. The RNNs model achieves an average 92.7% accuracy which is higher than SVM. Taking advantage of ensemble frameworks for integrating different feature extraction and classification algorithms to boost the overall performance. Disadvantage of the proposed method is that it is applied on only short messages not large-scale messages. Signature-based feature technique as a deep convolutional neural network [13] in a cloud platform is proposed for plate localization, character detection and segmentation. Extracting significant features makes the License Plate Recognition System(LPRS) to adequately recognize the license plate in challenging situations such as congested traffic with multiple plates in the image or plate orientation towards brightness. The proposed algorithm has better accuracy of recognizing License Plate rather than other traditional LPRS. In [14] paper, a deep learning approach for anomaly detection using a Restricted Boltzmann Machine (RBM) and a deep belief network are implemented. This method uses a one-hidden layer RBM to perform unsupervised feature reduction. The resultant weights from this RBM are passed to another RBM producing a deep belief network. The pre-trained weights are passed into a fine-tuning layer consisting of a Logistic Regression (LR) classifier with multi-class soft-max. The proposed methodachieves 97.9% accuracy. It produces a low false negative rate of 2.47%. It is observed that there is a need to improve the method to maximize the feature reduction process in the deep learning network and to improve the dataset.

The paper [15] proposes a deep learning-based approach for developing an efficient and flexible Network Intrusion Detection System(NIDS). A sparse autoencoder and soft-max regression-based NIDS is implemented. Self-taught Learning (STL), a deep learning-based technique on NSL-KDD - a benchmark dataset for network intrusion is used. STL achieves a classification accuracy rate more than 98% for all types of classification. Also, there is a need to implement a real-time NIDS for actual networks using deep learning technique. In [16] paper choose multi-core CPU's as well as GPUs to evaluate the performance of the Deep Neural Network based Intrusion Detection System (IDS) to handle huge network data. The parallel computing capabilities of the neural network make the Deep Neural Network (DNN) to effectively look through the network traffic with an accelerated performance. Advantages are: The DNN based IDS is reliable and efficient in intrusion detection for identifying the specific attack classes with required number of samples for training. The multicore CPUs was faster than the serial training mechanism. In [17] paper, proposes a mechanism for detecting large scale network-wide attacks using Replicator Neural Networks (RNNs) for creating anomaly detection models. The proposed approach is unsupervised and requires no labelled data. It also accurately detects network-wide anomalies without presuming that the training data is completely free of attacks. The proposed methodology is able to successfully discover all prominent (Distributed Denial of Service) DDoS attacks and *SYN Port* scans injected. Proposed methodology is resilient against learning in the presence of attacks, something that related work lacks. It is concluded that there is a need to improve proposed methodology by using stacked autoencoder deep learning techniques. Based on the flow-based nature of Software Defined Networking (SDN), a flow-based anomaly detection system using deep learning is proposed. In [18] paper, a deep learning approach for flow-based anomaly detection in an SDN environment is applied. Advantage is that it finds an optimal hyper-parameter for DNN and confirms the detection rate and false alarm rate. The model gets the performance with the accuracy of 75.75% which is reasonable from using six basic network features only.It is observed that it will not work on real SDN environment.

III CONCLUSION

Cyber-physical false data attacks in power networks can be detected and located in real-time using machine learning classifiers. Exploiting the physics-based features of the system has improved the accuracy of detecting replay attacks. According to the survey, it can be said that it is preferable to infer and exploit the physics using a single machine learning solution rather than to add features first and then build a detector.

IV FUTURE SCOPE

After doing the research on all the existing methods for cyber-attack detection it can be said that deep learning techniques for example Long Short-term Memory (LSTM) etc. can be further involved as an enhancement to the existing techniques. That is to say, the spatiotemporal patterns will be mapped to a linear space by using the LSTM network to improve the potential detection accuracy for cyberattacks.

REFERENCES

[1] Cui, Mingjian; Wang, Jianhui; Chen, Bo (2020). Flexible Machine Learning Based Cyberattack Detection Using Spatiotemporal Patterns for Distribution Systems. IEEE Transactions on Smart Grid, (), 1–1. doi:10.1109/TSG.2020.2965797

[2] IEEE JOURNAL OF EMERGING AND SELECTED TOPICS IN POWER ELECTRONICS, VOL. X, NO. X, XX 2019 1 Detection and Identification of Cyber and Physical Attacks on Distribution Power Grids with PVs: An Online High-Dimensional Data-driven Approach Fangyu Li, Rui Xie, Bowen Yang, Lulu Guo, Ping Ma, Jianjun Shi, Jin Ye, WenZhan Song DOI 10.1109/JESTPE.2019.2943449

[3] Ferragut, Erik M.; Laska, Jason; Olama, Mohammed M.; Ozmen, Ozgur (2017). [IEEE 2017 International Conference on Computational Science and Computational Intelligence (CSCI) - Las Vegas, NV, USA (2017.12.14-2017.12.16)] 2017 International Conference on Computational Science and Computational Intelligence (CSCI) - Real-Time Cyber-Physical False Data Attack Detection in Smart Grids Using Neural Networks. , (), 1–6. doi:10.1109/CSCI.2017.1

[4] Cui, Mingjian; Wang, Jianhui; Yue, Meng (2018). Machine Learning Based Anomaly Detection for Load Forecasting Under Cyber-attacks. IEEE Transactions on Smart Grid, (), 1–1. doi:10.1109/TSG.2018.2890809

[5] Feng, Yaokai; Akiyama, Hitoshi; Lu, Liang; Sakurai, Kouichi, 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and

Technology Congress(DASC/PiCom/DataCom/CyberSciTech) - Feature Selection for Machine Learning-Based Early Detection of Distributed Cyber-attacks, 173–180. doi:10.1109/DASC/PiCom/DataCom/CyberSci

[6] Choi, Young Hwan; Sadollah, Ali; Kim, JoongHoon (2020). Improvement of Cyber-Attack Detection Accuracy from Urban Water Systems Using Extreme Learning Machine. Applied Sciences, 10(22), 8179–. doi:10.3390/app10228179

[7] Kalkan, Soner Can; Sahingoz, OzgurKoray (2020). [IEEE 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) - Kharagpur, India (2020.7.1-2020.7.3)] 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) - In-Vehicle Intrusion Detection System on Controller Area Network with Machine Learning Models. , (), 1–6. doi:10.1109/icccnt49239.2020.9225442

[8] Nader, Patric; Honeine, Paul; Beauseroy, Pierre (2016). [IEEE 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC) - Beirut, Lebanon (2016.4.21-2016.4.23)] 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC) - Detection of cyber-attacks in a water distribution system using machine learning techniques. , (), 25–30. doi:10.1109/ICDIPC.2016.7470786

[9] Nguyen, Khoi Khac; Hoang, Dinh Thai; Niyato, Dusit; Wang, Ping; Nguyen, Diep; Dutkiewicz, Eryk (2018). [IEEE 2018 IEEE Wireless Communications and Networking Conference (WCNC) - Barcelona, Spain (2018.4.15-2018.4.18)] 2018 IEEE Wireless Communications and Networking Conference (WCNC) - Cyber-attack detection in mobile cloud computing: A deep learning approach. (), 1–6. doi:10.1109/WCNC.2018.8376973

[10] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring: A survey," Submitted to IEEE Trans. Neural Netw. Learn. Syst., 2016. [Online]. Available: http://arxiv.org/abs/1612.07640

[11]H. Lee, Y. Kim, and C. O. Kim, "A deep learning model for robust wafer fault monitoring with sensor measurement noise," IEEE Transactions on Semiconductor Manufacturing, vol. 30, no. 1, pp. 23–31, Feb. 2017.

[12] L. You, Y. Li, Y. Wang, J. Zhang, and Y. Yang, "A deep learning based RNNs model for automatic security audit of short messages," in Proc. 16th Int. Symp. Commun. Inf. Technol., Qingdao, China, Sep. 2016, pp. 225–229.

[13] R. Polishetty, M. Roopaei, and P. Rad, "A next-generation secure cloud based deep learning license plate recognition for smart cities," in Proc. 15th IEEE Int. Conf.Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016, pp. 286–293.

[14] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proc. 15th IEEE Int. Conf. Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016, pp. 195–200.

[15] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. 9th EAI Int.Conf. Bio-Inspired Inf. Commun. Technol., 2016, pp. 21–26. [Online]. Available: http://dx.doi.org/10.4108/eai.3-12-2015.2262516

[16] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom., Berlin, Germany, Sep. 2016, pp. 1–8.

[17] C. Garcia Cordero, S. Hauke, M. Muhlhauser, and M. Fischer, "Analyzing flow-based anomaly intrusion detection using replicator neural networks," in Proc. 14th Annu. Conf. Privacy, Security. Trust, Auckland, New Zeland, Dec. 2016, pp. 317–324.

[18] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. Int. Conf. Wireless Netw. Mobile Commun., Oct. 2016, pp. 258–263