International Journal of Advanced Technology and Engineering Exploration, Vol 5(49)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2018.547030

Review Article

Deep learning algorithm based cyber-attack detection in cyber-physical systems-a survey

Valliammal N.[1*] and Barani Shaju[2]
Assistant Professor, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India[1]
Research Scholar, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India[2]

Abstract
Over the last years, cyber-attack detection and control system design has become a significant area in cyber-physical systems (CPSs) due to the rapid growth of cyber-security challenges via sophisticated attacks like data injection attacks, replay attacks, etc. The effect of different attacks may provide system failure, malfunctioning, etc. As a result, an improved security system may require to implement the cyber defense system for upcoming CPSs. The different deep learning algorithm based cyber-attack detection schemes have been designed to detect and mitigate the different types of cyber-attacks through CPSs, smart grids, power systems, etc. This article presents a detailed survey of various deep learning algorithms proposed for CPSs to achieve cyber defense. At first, different algorithms developed by previous researchers are studied in detail. Then, a comparative analysis is carried out to know the limitations in each algorithm and provide a suggestion for further improvement of CPSs with more efficiently.

Keywords
Cyber-physical systems, Cyber-attacks, Cyber-security, Deep learning algorithms.

1.Introduction
Generally, an interconnection of physical systems is known as CPSs which are used for mission-essential tasks. For instance, water management and distribution plants, power grids and autonomous vehicles. Mostly, these systems are connected to support secluded monitoring and control. Due to the improved consequence of communication networks in control systems, the CPSs have supported protection and defence requests. Once those systems are related to the net, they emerge as vulnerable to cyber-attacks. For examples, cyber-attack on a Ukraine power plant in 2016, the Stuxnet malicious program that targeted a nuclear power plant and the insider risk on Australia's Moochy water services that occurred in 2000. Thus, there is a critical necessity for securing such CPSs against those situations given that vulnerabilities in industrial tasks may cause overwhelming consequences to the economic system, public protection and even individual life-style [1]. During the past decades, different attack detection and control techniques have conveyed a numerous interest.

A number of solutions spotlight on a specific type of attacks and the goals are designing the detection techniques or constructing the attack-resilient controllers in accordance with the characteristics of the considered attacks like denial-of-service (DoS) attacks, false data injection attacks, replay attacks, etc. However, those schemes have additional complexity in many situations for accepting a prior awareness about the type of attacks to be inserted into the system. For example, precise policies used for creating the counterfeit measurement data are unusual and not easy to be differentiated till the attacks are detected. In fact, detection of the attack types is not constantly mandatory, because the imperative idea is detecting a survival of the attack and then removing it for making sure the protection [2]. Therefore, systematic techniques have been developed to discover attacks and estimate the suitable security policies for different attack situations.

Many researchers have intention on CPSs and focused on the anomaly detection using deep learning algorithms. On the other hand, such designs and algorithms have their own limitations and challenges for detecting and removing several types of cyber-

*Author for correspondence

attacks economically. In this article, an overview of previous researches associated with the anomaly detection in CPSs using deep learning algorithms. The key objective of this paper is to study the detailed information on different deep learning algorithms utilized for anomaly detection in CPSs. In addition, their limitations are addressed to further improve the detection of attacks in CPSs efficiently.

The remaining of the article is structured as follows: Section 2 provides the previous researches related to anomaly detection using deep learning algorithms. Section 3 compares the performance efficiency of those algorithms and section 4 concludes the survey that reviews an entire discussion.

2.Survey on cyber-attack detection schemes

In this section, the works related to the cyber-attack detection schemes are studied in detail. Machine learning algorithms [3] were used for classifying the measurements as being secure or attacked in the smart grids. This framework was provided for exploiting prior information about the system and surmounting limitations from the sparse composition in the machine learning. Here, decision and feature level fusion were used along with well-known batch and online learning algorithms for modeling the attack detection problem. Also, unobservable attacks were detected by using statistical learning methods and analyzing the relationships between statistical and geometric properties of attack vectors in the attack scenarios.

Artificial neural network (ANN) based intrusion detection system [4] was proposed for analyzing internet of things (IoT) threats. The most important goal of this system was to classify the ordinary and treat patterns on IoT network for detecting distributed DoS (DDoS)/DoS attacks. In this system, a multi-level perceptron was trained by using internet packet traces. After that, the trained model was assessed on its capability to thwart DDoS attacks. Moreover, the overall performance of the ANN was analyzed against a simulated IoT network.

Anomaly detection [5] was proposed in the CPSs by means of recurrent neural network (RNN). The foremost aim of this system was providing a novel method to behavioral-based intrusion detection in CPSs. In this system, long short-term memory (LSTM)-RNN was used as a predictor to model the normal data characteristics in CPSs. After that, the cumulative sum method was used for identifying the abnormalities in a water management plant. Anomaly-based detection approach [6] was proposed to detect and classify the attacks in CPS. Initially, anomaly detection was used for defining normal system characteristics based on the computation of outlier scores. After that, this model was compared with the new data for detecting anomalies. Furthermore, the supervised attacks model was trained by using a Bayes classifier. Then, the abnormality was classified by applying the attack model and measuring the prediction confidences for trained classes.

A detection scheme [7] for DDoS attacks detection in smart grids was proposed in which a discrete wavelet transform was applied to input data for extracting the features. Additionally, a convolutional neural network (CNN) was trained by using the extracted features and testing was performed for detecting anomalous characteristics in the data according to the threshold value. Anomaly detection in a water management system [8] was proposed based on the unsupervised machine learning algorithm. In this technique, deep neural network (DNN) and one-class support vector machine (SVM) were adapted to time series data generated by a CPS. Such methods were evaluated against data from the secure water treatment (SWaT) testbed. Initially, the detectors for both methods were trained by using a log generated through SWaT operating under different attack conditions. Moreover, LSTM framework was used for prediction of dynamic behavior of SWaT.

An intelligent sensor attack detection method [9] was proposed based on DNN algorithm for an automotive CPS. The core objective of this approach was detecting the deception attacks without any prior information. In this method, an autonomous vehicle with inertial measurement unit (IMU) and wheel encoder sensors were investigated under uncertainty and nonlinearity conditions during driving. Initially, types of attacks on the sensors were identified and a model was chosen to design its framework.

Moreover, the performance was trained and validated on real measurement data gathered from unmanned ground vehicles. A novel data analytical approach [10] was proposed for false data injection attack mitigation in smart grids. In this approach, the false data injection attacks were detected according to the data-centric paradigm which employs margin setting algorithm (MSA). Based on the data gathered, MSA was trained to detect the threat patterns and achieve anomaly detection in CPS with high accuracy. In

addition, the performance analysis was performed based on both theoretical and practical manner.

Real-time detection of false data injection attacks [11] was proposed in smart grids by using a deep learning-based intelligent method. In this approach, the chronological data and the captured features were used to identify the false data injection attacks in real-time. Also, an optimization model was proposed for characterizing the behavior of false data injection attack that compromises the inadequate number of state measurement of the power system for electricity theft. Distributed attack detection scheme [12] was proposed by using deep learning for internet-of-things. The main objective of this scheme was adopting deep learning to cyber security for enabling the attacks detection in social IoT.

Cyber-attack detection [13] was achieved by using a deep learning approach with the aim of utilizing the training dataset to train the pre-established neural network in offline mode with adjusting weights of the neural network. After that, the neural network was used for detecting the cyber-attacks in the cloud system in online mode. Moreover, the performance was evaluated by considering three empirical public datasets namely KDDcup 1999, NSL-KDD and UNSW-NB15. To detect cyber-attacks efficiently, the most significant features from those datasets were selected through Principal Component Analysis (PCA) which reduces the computational complexity. Intrusion detection [14] was proposed in CPS based on the Petri Net (PN). The main aim of this technique was simultaneously detecting misuse and anomaly characteristics of the CPSs. This technique was suitable to supervisory control and data acquisition (SCADA) system at the highest level of CPSs. Here, Neural First Order Hybrid Petri Net model (NFOHPN) with online fast Independent Component Analysis (ICA) was proposed for anomaly detection. The detection was achieved by extracting some features of KDD 99 dataset.

Dynamic detection of false data injection attack [15] was proposed in smart grid by using deep learning. In this approach, a CNN and a LSTM network were adopted that observes both data measurements and network level features for mutually learning system states. Deep learning algorithm using transfer-entropy measures [16] was proposed for anomaly detection in CPS. In this method, a novel distributed deep learning algorithm was proposed to detect cyber-attacks in IoT by learning high-level features from data in an incremental manner. Initially, transfer-entropy was measured including with various parameters such as node, channel and network for sensor measurements. After that, the measured values were collected and trained by using deep learning classifiers. Here, both ANN and DNN were used to train the data that detects the existence of the cyber-attacks in CPSs.

3.Results and discussions

This section presents a detail about merits and demerits of different cyber-attacks detection systems whose functional information is discussed in the previous section. Through the review on cyber-attack detection using deep learning algorithms, the following challenges are addressed.

- By using multi-layer perceptron (MLP)-based intrusion detection scheme, a mean square error was slightly high.
- The ability of LSTM-RNN was not effective to validate the false positives.
- Due to the utilization of the Bayes classifier for detecting anomalies, only specific types of attacks such as DoS attacks and man-in-the-middle attacks were detected.
- The processing time was increased by using CNN for anomaly detection and also it has less accuracy.
- The efficiency of intelligent sensor attack detection was less since it does not has the ability to operate under complex driving conditions like slope, turning, etc.
- Moreover, MSA based attack mitigation scheme does not handle numerous amount of data during attack detection process.
- Detection time and energy consumption were required to analyze by using neural network based cyber-attack detection.
- The computation cost of DNN and NFOHPN-based intrusion detection methods was high.

Table 1 shows the comparison of different cyber-attack detection schemes using different deep learning algorithms.

Table 1 Comparison of different cyber-attack detection schemes using different deep learning algorithms

Ref. No.	Methods	Advantages	Disadvantages	Performance effectiveness
[3]	Well-known batch and online learning algorithms with decision and feature level fusion	Comparative study has been done.	Concept drift or dataset drift was occurred when the samples were independent identically distributed from non-stationary distributions.	SVM with linear kernel: Accuracy=90%, Precision=0.1,Recall=1 KNN: Accuracy=95%, Precision=0.2,Recall=0.96
[4]	ANN-based intrusion detection	Better detection accuracy.	For MLP, mean absolute error was high.	Simple linear regression: mean absolute error (MAE)=0.0059, root mean square error (RMSE)= 0.0439,Accuracy=89.53%. MLP: MAE=0.1776,RMSE=0.2123, Accuracy=90.18%
[5]	LSTM-RNN for behavioural-based intrusion detection	Different types of attacks can be detected efficiently.	The ability was less for validating the false positives.	Nil
[6]	Bayes classifier based anomaly detection	It has the ability to detect and classify the anomaly behaviors.	This classifier detects only specific types of attacks and the performance was not analyzed.	Nil
[7]	CNN based detection approach	Allows detection of attacks in real-time.	Processing time was increased and accuracy was not improved.	One-stage CNN: Accuracy=56.1% One-stage pre-processed CNN: Accuracy=80.77%
[8]	DNN and SVM-based anomaly detection	Better precision and F-measure.	Computation cost was high.	DNN: Precision=0.983, Recall=0.678, F-measure=0.803 One-class SVM: Precision=0.925, Recall=0.699, F-measure=0.7963
[9]	DNN based intelligent sensor attack detection	Detection speed and accuracy were high.	The efficiency was less since it does not function under complex driving situations like turning, slope, etc.	Detection accuracy for LSTM=97.33%, Detection accuracy for gated recurrent unit (GRU)=97.11%
[10]	MSA based false data injection attack mitigation	Better accuracy with minimum error.	It handles only a small amount of data during the detection process.	Accuracy for different datasets (Playback Attack): McDonald=97.69%, Harris=98.27%, Austin=98.51%, WACO=98.51%, UT Pan=97.51%, UT 3=98.39% Accuracy (Time Attack): McDonald=96.57%, Harris=96.76%, Austin=97.31%, WACO=97.54%, UT Pan=97.06%, UT 3=97.18%
[11]	Real-time false data injection attacks detection using deep learning-based intelligent model	High detection accuracy.	It requires an improved model to analyze the minimum number of the sensing units required for increasing the detection accuracy.	Detection accuracy: Compromised label=95.89%, Normal label=96.43%
[12]	Distributed deep learning scheme	Better detection of cyber-attacks.	Network payload data was required to detect intrusion efficiently.	2-Class: Accuracy=99.20%, Detection rate=99.27%, False alarm rate=0.85% 4-Class: Accuracy=98.27%, Detection rate=96.5%, False alarm rate=2.57%
[13]	Neural network based cyber-attack detection	High accuracy.	Detection time and energy consumption were not analyzed.	NSL-KDD dataset: Accuracy=90.99%, Precision=81.95%, Recall=77.48% UNSW-NB15 dataset:Accuracy=95.84%, Precision=83.40%, Recall=79.19% KDD cup 1999 dataset:

Ref. No.	Methods	Advantages	Disadvantages	Performance effectiveness
				Accuracy=97.11%, Precision=94.43%, Recall=92.77%
[14]	NFOHPN based intrusion detection	Better accuracy.	Computation cost was high.	Normal attack: Detection rate=98.2%, False positive rate=2.9% Probe attack: Detection rate=99.5%, False positive rate=1.2%, Running time=6sec
[15]	Dynamic detection of false data injection attack using deep learning	Can detect attack when state vector estimator fails.	High complexity.	Accuracy=90%
[16]	DNN with transfer-entropy measure based anomaly detection	Very high accuracy.	Computation time was high.	DoS attack Accuracy=98%,Sensitivity=0.98 Replay attack: Accuracy=94%, Sensitivity=0.92 Innovation-based deception attack: Accuracy=91.76%,Sensitivity=0.75Data injection attack: Accuracy=96.95%, Sensitivity=0.97

4.Conclusion

In this article, a detailed review of cyber-attack detection schemes based on deep learning algorithms in CPSs was presented. Obviously, it shows all researchers have experienced in various deep learning algorithms for detecting and mitigating the cyber-attacks in CPSs in order to enhance the cyber-security than the traditional machine learning algorithms or other detection algorithms. According to this analysis, DNN with the transfer-entropy measure based anomaly detection in CPS has better performance than all other cyber-attack detection systems. However, it has high computational time complexity. Therefore, the future extension of this work could be further enhancement on DNN with the transfer-entropy measure based anomaly detection in CPS based on the advanced hybrid deep learning algorithms to improve further efficiency and reduce the computational cost significantly.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Majhi SK, Patra G, Dhal SK. Cyber physical systems & public utility in India: state of art. Procedia Computer Science. 2016; 78:777-81.

[2] Sebestyen G, Hangan A. Anomaly detection techniques in cyber-physical systems. Acta Universitatis Sapientiae, Informatica. 2017; 9(2):101-18.

[3] Ozay M, Esnaola I, Vural FT, Kulkarni SR, Poor HV. Machine learning methods for attack detection in the smart grid. IEEE Transactions on Neural Networks and Learning Systems. 2016; 27(8):1773-86.

[4] Hodo E, Bellekens X, Hamilton A, Dubouilh PL, Iorkyase E, Tachtatzis C, et al. Threat analysis of IoT networks using artificial neural network intrusion detection system. In international symposium on networks, computers and communications 2016 (pp. 1-6). IEEE.

[5] Goh J, Adepu S, Tan M, Lee ZS. Anomaly detection in cyber physical systems using recurrent neural networks. In international symposium on high assurance systems engineering 2017 (pp. 140-5). IEEE.

[6] Kreimel P, Eigner O, Tavolato P. Anomaly-based detection and classification of attacks in cyber-physical systems. In proceedings of the international conference on availability, reliability and security 2017. ACM.

[7] Ghanbari M, Kinsner W, Ferens K. Detecting a distributed denial of service attack using a pre-processed convolutional neural network. In electrical power and energy conference 2017 (pp. 1-6). IEEE.

[8] Inoue J, Yamagata Y, Chen Y, Poskitt CM, Sun J. Anomaly detection for a water treatment system using unsupervised machine learning. In international conference on data mining workshops 2017 (pp. 1058-65). IEEE.

[9] Shin J, Baek Y, Eun Y, Son SH. Intelligent sensor attack detection and identification for automotive cyber-physical systems. In symposium series on computational intelligence 2017 (pp. 1-8). IEEE.

[10] Wang Y, Amin MM, Fu J, Moussa HB. A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids. IEEE Access. 2017; 5:26022-33.

[11] He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Transactions on Smart Grid. 2017; 8(5):2505-16.

[12] Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for internet of things. Future Generation Computer Systems. 2018; 82:761-8.
[13] Nguyen KK, Hoang DT, Niyato D, Wang P, Nguyen D, Dutkiewicz E. Cyberattack detection in mobile cloud computing: a deep learning approach. In wireless communications and networking conference 2018 (pp. 1-6). IEEE.
[14] Ghazi Z, Doustmohammadi A. Intrusion detection in cyber-physical systems based on petri net. Information Technology and Control. 2018; 47(2):220-35.
[15] Niu X, Sun J. Dynamic detection of false data injection attack in smart grid using deep learning. arXiv preprint arXiv:1808.01094. 2018.
[16] Shi D, Guo Z, Johansson KH, Shi L. Causality countermeasures for anomaly detection in cyber-physical systems. IEEE Transactions on Automatic Control. 2018; 63(2):386-401.

N. Valliammal is the Assistant Professor (SS) in the Department of Computer Science in Avinashilingam Institute for Home Science and Higher Education for Women. She has more than 20 Years of teaching Experience. Her research interests include Cyber Security, IoT and Big Data Analytics. She has more than 16 publications at International and National level. She is a Life member of one of the professional organization in Indian Science Congress Association and CSI. She has acted as a reviewer of IJCNC and IJCSEA.
Email: vallinarayancbe@gmail.com

Barani Shaju is a part time Research scholar in Department of Computer Science at Avinashilingam University, Coimbatore. Her domain of work can be sheltered under the umbrella of Data science, Analytics and Cyber Security. At work front, she is a Technology Specialist at Robert Bosch Engineering and Business Solutions at Keeranatham, Coimbatore. Her core technical strengths are on JEE frameworks, Perl, Python with Data science library and database – Oracle, MySQL.