Anomaly Detection in Critical Infrastructure Using Probabilistic Neural Network

M. R. Gauthama Raman[1], Nivethitha Somu[2], and Aditya P. Mathur[1(✉)]

[1] iTrust–Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore, Singapore
gauthamaraman_mr@live.com, aditya_mathur@sutd.sg.edu

[2] Smart Energy Informatics Laboratory (SEIL), Indian Institute of Technology, Bombay, Mumbai, India
nivethithasomu@iitb.ac.in

Abstract. Supervisory Control and Data Acquisition (SCADA) systems forms a vital part of any critical infrastructure. Such systems are network integrated for remote monitoring and control making them vulnerable to intrusions by malicious actors. Such intrusions may lead to anomalous behavior of the underlying physical process. This work presents a Probabilistic Neural Network (PNN) based anomaly detector to detect anomalies arising consequent to a cyber attack. Experimental validation was conducted using the dataset obtained from an operational water treatment testbed, namely Secure Water Treatment (SWaT). The impact of the smoothening parameter on the performance of the PNN-based anomaly detector was analyzed. Experimental evaluations indicate the significance of the PNN-based anomaly detector, compared with several competing detectors, in terms of precision, F-score, false alarm rate, and detection rate.

Keywords: Anomaly detection · Cyber physical systems · Cyber attacks · Industrial control systems · Intrusion detection system · Probabilistic Neural Network

1 Introduction

Critical infrastructure, such as water treatment systems and power grid, consists of an Industrial Control System (ICS) that controls the underlying physical process using sensors and actuators [6,25]. A Supervisory Control and Data Acquisition (SCADA) system is an integral part of ICS. Moreover, such critical infrastructure is also a Cyber Physical System (CPS) that includes cyber and physical components. Increased connectivity through communications network within the ICS components, and possibly through the Internet, exposes such CPS to a range of cyber threats [3,10,23,24,35].

V. S. Shankar Sriram et al. (Eds.): ATIS 2019, CCIS 1116, pp. 129–141, 2019.
https://doi.org/10.1007/978-981-15-0871-4_10

A cyber or physical attack on an ICS will likely result in anomalous process behavior. In general, approaches for anomaly-based intrusion detection can be categorized based on rules, statistics, and computational intelligence. Among these, computational intelligence based anomaly detection approaches have gained the attention of researchers as the rest of the approaches require a detailed understanding of the process flow, physical laws, and configuration of components in the CPS [2,14,18]. Moreover, the application of machine learn-

Table 1. Related work.

Technique(s)	Dataset	Performance metrics
Unsupervised anomaly detection approaches		
CNN [19]	SWaT	F-Score
DAE [27]	SWaT; Power grid control system	Precision, F–Score, and Recall
GAN [20]	SWaT	Classification Accuracy, Recall, F–Score, Precision, and False Positive Rate
O-SVM; DNN [16]	SWaT	Precision, Recall, and F–Score
RNN [12]	SWaT	Classification Accuracy
Supervised anomaly detection approaches		
NSA [6]	SWaT	Classification Accuracy
SVM; Artificial immune system [34]	Simulation, KDD Cup 1999	False Positive and False Negative Rates
NB, RF; One R; J48; Non-nested generalized exemplars; SVM [4]	Gas pipeline system at Mississippi State University	Precision and Recall
Neural Network [28]	SWaT	F–Score, NAB Score, Precision, and Recall
Deep belief network; SVM [15]	Real time SCADA network	Classification Accuracy
J48 [29]	IoT security testbed	Classification Accuracy, F–Measure, Recall, Precision
LSTM [8]	Gas and oil plant heating loop	Precision, Recall, and F–Score
RNN [7]	Tennessee Eastman Process	NAB Score
LSTM based Autoencoder [21]	Power demand	True Positive Rate, F–Score, and False Positive Rate
Neural network; SVM; Random forest; J48 [18]	SWaT	Accuracy, Precision, Recall, and False Alarm Rate

ing algorithms for anomaly detection is found to be fast and relatively easy to develop since the behaviour and process flow of the entire CPS system can be learned with reasonable accuracy from the multivariate historical data [27]. A summary of research on computational intelligence based anomaly detection approaches is given in Table 1.

This work describes a study wherein the Probabilistic Neural Network (PNN) framework is selected as a modeling approach for the design of an anomaly detector. Competing approaches include Convolutional Neural Network (CNN), Deep Neural Network (DNN), Naives Bayes (NB), One class-Support Vector Machine (O-SVM), Random Forest (RF), Recurrent Neural Network (RNN), Long Short Term Memory (LSTM), Deep Autoencoders, and others. PNNs are unique in their characteristic of mapping the input variables to class labels using Bayesian strategy [12,17,21,31]. Unlike other variants of neural networks, PNN is robust, faster, mostly independent of parameters, and has the ability to handle imbalanced datasets- a key reason for exploring it in this work. PNN has been effectively used for the design of anomaly detectors in various applications [9,13,32,33] however to the best of our knowledge, this is the first work to employ PNN for anomaly detection in an ICS, especially in a SwaT operational plant.

Novelty and Contributions: (a) A PNN-based anomaly detector for critical infrastructure, and (b) Validation of the performance of the PNN-based anomaly detector using live data from an operational CPS, namely, SWaT [22].

Organization: This paper is structure as follows. An introduction to PNN is in Sect. 2. Experimental assessment of the effectiveness of a PNN-based anomaly detector in detecting anomalies resulting from cyber attacks, is in Sect. 3. This section contains a description of the architecture of the testbed and its dataset used in the evaluation, impact of smoothening parameter on the performance of PNN, and a detailed comparison with seven other neural network based methods. Conclusions from this work are in Sect. 4.

2 PNN-Based Anomaly Detector

In this section, we provide a detailed insight on the application of PNN for the design of an anomaly detector for CPS. In general, any data driven anomaly detector designed for CPS should be fast, reliable, scalable, and sensitive to noisy data generated by the heterogeneous physical and control components as the CPS environment is dynamic, operates in real time, and the sensor data are often generated at high frequency [27]. Further, the ability to predict the anomalies in the unknown samples based on a similar set of samples in the training dataset forms an important criterion for assessing the performance of a data driven anomaly detector [9,30]. The above mentioned requirements of an anomaly detector for a critical infrastructure led to the choice of PNN in this work.

As shown in Fig. 1, a PNN is comprised of artificial neurons arranged in four layers as detailed below.

1. ***Input layer:*** Passes the unknown sample X_s to the pattern layer without any computation
2. ***Pattern layer:*** Number of neurons in this layer corresponds to the number of training samples. Each neuron corresponds to the training samples and its output is defined in Eq. 1.

$$y_k^i = exp\left[\frac{-|X_s - x_k^i|^2}{2\sigma^2}\right] \tag{1}$$

where, x_k^i is the i^{th} training sample of the k^{th} class and σ is the smoothening parameter.

3. ***Summation layer:*** The average of the pattern layer's output that belongs to the same class is computed using Eq. 2.

$$S_i = \frac{1}{n}\sum_{k=1}^{n} exp\left[\frac{-|X_s - x_k^i|^2}{2\sigma^2}\right] \tag{2}$$

4. ***Output layer:*** The output layer consists of one neuron that decides the class of the unknown sample using Eq. 3.

$$C = argmax(S_i), \forall i = (1, 2, \ldots, C_n) \tag{3}$$

Given the conditional attribute (x), decisional attributes (Y), classes in the training set (C), and smoothening factor (σ), PNN computes the class of the unknown sample [26,30].

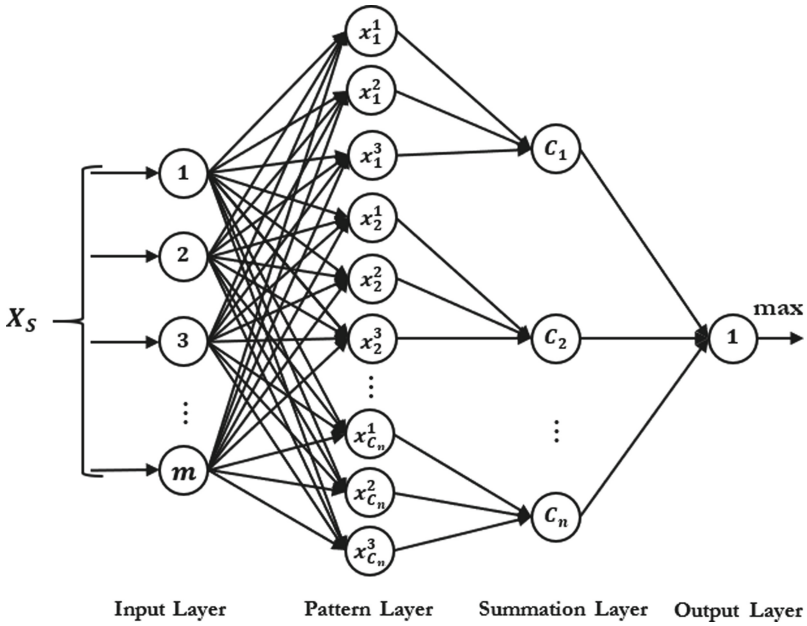

Fig. 1. Probabilistic neural network.

3 Experimental Evaluation

The PNN-based approach proposed in this work was evaluated using the dataset obtain from the SWaT testbed. The architecture of SWaT, summary of the dataset and data preprocessing techniques can be found in [18]. To demonstrate the predominance of the proposed anomaly detector, performance validations were carried out by comparing the effectiveness of the PNN-based anomaly detector with that of the existing machine learning models in terms of classification accuracy, precision, detection rate, F-Score, and false alarm rate. The models used for the comparison include Naives Bayes (NB), Support vector machine (SVM), Random forest (RF), and Multi layer perceptron (MLP).

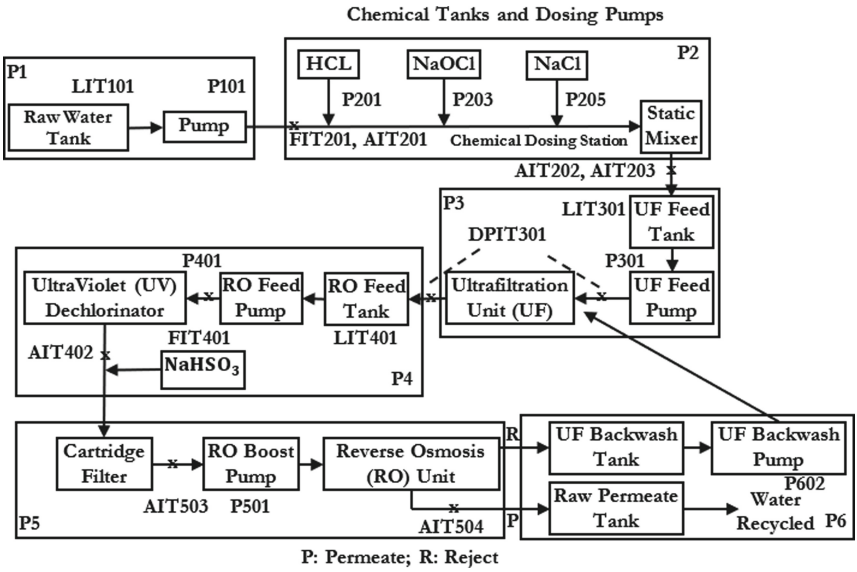

Fig. 2. Stages P1 through P6 in SWaT. AITxxx: chemical property meters, FITxxx: flow rate meters, LITxxx: level sensors; Pxxx: pumps.

3.1 SWaT Architecture

SWaT is a fully operational small footprint water treatment plant at the Singapore University of Technology and Design (SUTD). Details of SWaT are available in [22].

SWaT consists of six stages (P1-P6) as shown in Fig. 2. Each stage comprises of a combination of physical and control components for processing raw water. Each stage is equipped with sensors to measure flow rate, water level in tanks, chemical properties of water, etc., and actuators such as pumps and valves. The cyber part of SWaT consists of a two layered communications network with

Programmable Logic Controllers (PLCs), SCADA workstation, Human Machine Interface (HMIs) and a historian. Level 0 network in the testbed consists of a ring for each stage through which all sensors and actuators transfer measurements, and receive commands, to and from the corresponding PLCs via. wired and wireless links. Similarly, Level 1 network consists of a STAR architecture that enables communications between SCADA workstation and the PLCs.

Table 2. Attacks considered in experiments.

Attack ID	Type	Target	Duration (Secs.)	Expected impact	Unexpected impact
1	SSSP	MV-101	539	Tank overflow	
2	SSSP	LIT-101	300	Tank Underflow; damage P-101	
3	SSSP	MV-504	300	Halt RO shut down sequence; reduce life of RO	
4	SSSP	DPIT-301	500	Backwash process is started again and again; normal operation stops; Decrease in water level of tank 401. Increase in water level of tank 301	
5	SSSP	AIT-504	200	RO shut down sequence starts after 30 min. Water should go to drain	RO did not shut down; water does not drain
6	SSMP	MV-101, LIT-101	501	Tank overflow	
7	MSMP	P-602, DIT-301, MV-302	251	System freeze	
8	MSSP	P-101, LIT-301	251	Stop inflow of tank T-401	
9	MSSP	AIT-402, AIT-502	251	Water enters the drain due to overdosing	Water does not drain
10	SSSP	LIT-302	501	Tank overflow	Rate of decrease of water level reduced after 1:33:25 PM

3.2 SWaT Dataset

For data collection, the entire plant was operated for 11-days. For the first 7-days, the plant was operated under normal mode. Subsequently, for the remaining 4-days, the attacks were launched by spoofing the sensor values, issuing fake commands, etc. Attack timings, target, expected outcome, and effects are available in [11].

During 11-days of data collection, a total of 946,723 labelled records were collected from the historian. Each record consists of 51 attributes corresponding to the individual sensor values. Note that selecting the entire 946,723 instances for the experiment would bias the PNN to the 'normal' class since the normal instance dominates the instances related to the attacks. However, if we consider 449,921, i.e., instances recorded under the attack scenario, reduce the dominating nature and hence the imbalanced nature of dataset is avoided. Therefore, a total of 449,921 records collected during 28th Dec 2015 to 2nd Jan 2016 were used for experimentation.

During the last four days of data collection, a total of ten attacks, referred to as A1-A10 [11], were launched by injecting fake sensor values to the PLCs (Table 2). For each attack, two different subsets of the entire dataset were created using 'random sampling without replacement' to train and validate the learning model. The attacks can be categorized as: (i) Single Stage Single Point attack (SSSP), (ii) Single Stage Multi Point attack (SSMP), (iii) Multistage Single Point attack (MSSP), and (iv) Multi-Stage Multi Point attack (MSMP). Attack duration varies based on the nature of the attack. For example, the duration of attack A1 that targets MV101, and attack A9 that targets chemical sensors AIT 402 and AIT 502, are 539 and 251 s, respectively.

3.3 Results and Discussion

Data was collected from the experiments and analyzed. Results from the analysis are presented next.

Impact of Smoothening Parameter: Note from Eq. 1 that σ is a single tunable parameter which is significant in determining the width of the kernel parameter in the pattern layer which in turn has a significant impact on the performance of the PNN. Since the smoothening parameter relies on the characteristics of the input data, it is important to analyze its impact on the performance of the detector. Therefore, the experiments were conducted by varying σ in the range [0.1,0.9] at intervals of 0.1. For each experiment, the average values of the considered performance metrics were computed. The corresponding plots are given in Figs. 3, 4, 5 and 6. From the plots, it is evident that to achieve the optimal value for the considered performance metrics, σ ought to be in [0.1,0.3].

Analysis of data from the experiments indicates that the identification of multiple optimal values of σ for effective detection of various anomalies in the process flow of SWaT might further enhance the performance of the PNN-based anomaly detector. Therefore, the design of the PNN-based anomaly detector

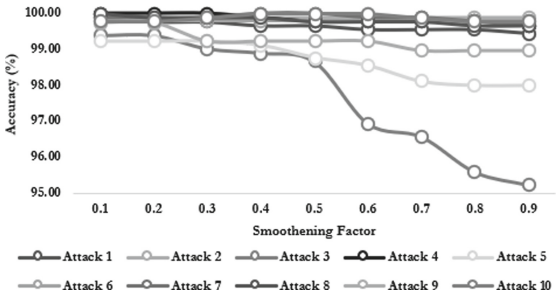

Fig. 3. Smoothening parameter vs. Classification accuracy

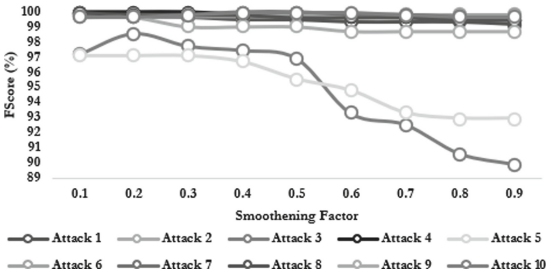

Fig. 4. Smoothening parameter vs. F-score

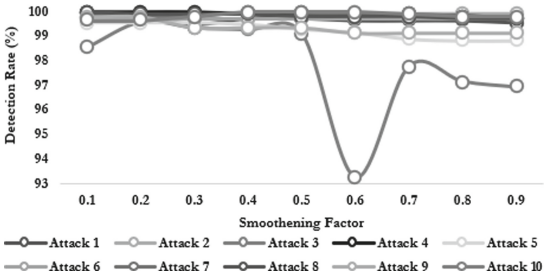

Fig. 5. Smoothening parameter vs. Detection rate

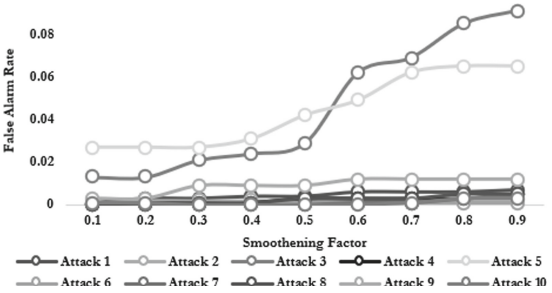

Fig. 6. Smoothening parameter vs. FAR

Table 3. Performance analysis of all classifiers for Attacks 1- 10

Attack ID	Algorithm	Accuracy	Precision	Detection rate	F-Score	False alarm rate
1	NB	97.72	97.8	97.7	97.7	**0**
	SVM	80.29	84	80.3	78.1	0.03
	MLP	98.92	99	98.9	98.9	0.02
	RF	98.99	99	99	99	0.02
	PNN	**99.8**	**100**	**99.91**	**99.84**	0.001
2	NB	81.7	85.1	81.7	75	0
	SVM	80.22	84.2	80.2	71.8	0
	MLP	95.17	95.4	95.2	94.9	0
	RF	94.03	94.4	94	93.6	0.42
	PNN	**100**	**100**	**100**	**100**	**0**
3	NB	90.31	90.1	90.3	90.1	0.23
	SVM	92.45	93.1	92.5	91.9	**0**
	MLP	72.26	87.5	72.3	74.6	1.25
	RF	97.33	97.6	97.3	97.4	0.11
	PNN	**99.38**	**100**	**99.61**	**98.58**	0.013
4	NB	97.52	97.5	97.5	97.5	0.03
	SV	69.43	79.1	69.4	59.4	0
	MLP	95.1	95.2	95.1	95.1	1.13
	RF	91.48	92.5	91.5	91.1	0
	PNN	**100**	**100**	**100**	**100**	**0**
5	NB	88.94	90.2	88.9	85.4	**0**
	SVM	87.46	89.1	87.5	82.4	**0**
	MLP	90.34	89.4	90.3	89	0.3
	RF	91.75	92.5	91.8	90.1	**0**
	PNN	**99.22**	**100**	**94.44**	**97.14**	0.027
6	NB	88.44	90.2	88.4	87.9	0.18
	SVM	97.11	97.2	97.1	97.1	0.04
	MLP	84.42	86.6	84.4	83.4	0.23
	RF	89.94	91.3	89.9	89.5	0.16
	PNN	**99.79**	**100**	**99.6**	**99.79**	**0.001**
7	NB	98.65	98.7	98.7	98.7	0.04
	SVM	69.57	79.1	69.6	59.7	0
	MLP	98.05	98.1	98.1	98.1	0.04
	RF	93.9	94.4	93.9	93.7	0
	PNN	**100**	**100**	**100**	**100**	**0**
8	NB	41.86	76.9	41.9	28.4	0.6
	SVM	40.15	76.6	40.2	24.9	0.6
	MLP	97.05	97.1	97.1	97.1	0.04
	RF	39.84	76.5	39.8	24.3	0.61
	PNN	**100**	**100**	**100**	**100**	**0**
9	NB	41.86	76.9	41.9	28.4	0.6
	SVM	40.15	76.6	40.2	24.9	0.6
	MLP	97.05	97.1	97.1	97.1	0.04
	RF	39.84	76.5	39.8	24.3	0.61
	PNN	**99.74**	**100**	**99.34**	**99.67**	**0.003**
10	NB	79.49	84.3	79.5	76.3	0
	SVM	69.3	79	69.3	59.2	0
	MLP	95.1	95.1	95.1	95.1	0.07
	RF	82.97	86.4	83	81	0
	PNN	**100**	**100**	**100**	**100**	**0**

with multiple σ values and accurate modeling of the physical process of SWaT, resulted in high detection rate and minimal false alarm rate.

Performance Analysis: Performance of PNN was compared with the machine learning techniques mentioned earlier. The results of the comparison are summarized in Table 3. The best values of each metric are highlighted in bold. From the table, it can be noted that PNN outperforms the existing machine learning techniques in terms of all quality metrics expect in a few cases. For example, Naive Bayes and SVM classifier attain the least false alarm rate of 0% when compared with PNN for attack 1 and attack 3.

From the above set of experimental results, some emergent facts observed about data driven anomaly detectors are (i) PNN exhibits an ideal classifier behaviour for attacks 2, 4, 7, 8, and 10, and (ii) The performance of classifiers varies with the nature of the attack, i.e., MLP has a better performance for attacks 1, 2, 4, 5, 7, 8, 9, and 10 when compared with the rest.

Lastly, the performance of the PNN-based anomaly detector over the existing machine learning techniques was analyzed in terms of their respective fault detection ability. In general, attacks 6, 7, 8, and 9 were found to be more difficult to detect as they target multiple sensors across multiple stages. However, PNN achieves 100% detection rate and 0% false alarm rate for attacks 7 and 9. A near optimal outcome was achieved for detecting attacks 6 and 8. This inherent ability of a PNN-based anomaly detector was due to the proper tuning of the smoothening parameter (σ).

To summarize, PNN, and the considered machine learning techniques, either detect the attacks during the initial stage of occurrence or the attack is left undetected. This nature of data driven models is preferred over the existing anomaly detection models, as they do not wait for the behaviour of CPS to exceed any pre-specified threshold for attack identification and therefore possess high detection rate and low false alarm rate [18]. However, they provide worst performance for the attacks that last for a shorter duration since they are left unidentified.

4 Conclusions

A SCADA specific PNN-based anomaly detector is presented. The detector uses a supervised approach to detect anomalies possibly resulting from attacks targeted at a CPS. The novelty of the proposed detector lies in its ability to identify anomalies resulting from single– and multi– stage attacks. Experimental validation on the dataset obtained from SWaT demonstrates the significance of PNN-based anomaly detector over the existing machine learning techniques in terms of various quality metrics. Also analysed in this study was the impact of the smoothening parameter on the performance of the PNN-based anomaly detector.

In the proposed PNN-based anomaly detector, a supervised approach needs training with both attack and normal signatures. However, in an operational plant, especially during the unavailability of appropriate attack patterns, one

may employ the supervised learning model in [1] for efficient anomaly detection. In the case of an imbalanced dataset, along with the smoothening parameter, the training samples play a vital role in determining the performance of PNN. Unlike in traditional RNN models, PNN does not rely on the temporal dependencies among the samples. Hence, the application of properties such as hypergraph coarsening, dual hypergraph, etc., for the identification of informative samples, aids in improving the performance of PNN in detecting short term attacks [5]. Further, the analysis and implementation of PNN variants such as heteroscedastic PNN, weighted PNN, arithmetic residue PNN, etc., for efficient anomaly detection in a CPS, is a potential challenge that needs to be focussed.

Acknowledgements. This work was supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2016NCR-NCR002-023) and administered by the National Cybersecurity R&D Directorate.

References

1. Adepu, S., Mathur, A.: An investigation into the response of a water treatment system to cyber attacks. In: IEEE 17th International Symposium on High Assurance Systems Engineering, pp. 141–148. IEEE (2016)
2. Adepu, S., Mathur, A.: Distributed attack detection in a water treatment plant: method and case study. IEEE Trans. Dependable Secure Comput. 11 (2018). https://doi.org/10.1109/TDSC.2018.2875008
3. Ball, T.: Top 5 critical infrastructure cyber attacks. https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/. Accessed 15 Jan 2019
4. Beaver, J., Borges-Hink, R., Buckner, M.: An evaluation of machine learning methods to detect malicious SCADA communications. In: 12th International Conference on Machine Learning and Applications, pp. 54–59. IEEE (2013)
5. Berge, C., Minieka, E.: Graphs and Hypergraphs. North-Holland Pub. Co., Amsterdam (1973)
6. Clotet, X., Moyano, J., Len, G.: A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of critical infrastructures. Int. J. Crit. Infrastruct. Prot. **23**, 11–20 (2018)
7. Filonov, P., Kitashov, F., Lavrentyev, A.: RNN-based early cyber-attack detection for the tennessee eastman process. arXiv preprint arXiv:1709.02232 (2017)
8. Filonov, P., Lavrentyev, A., Vorontsov, A.: Multivariate industrial time series with cyber-attack simulation: fault detection using an LSTM-based predictive data model. arXiv preprint arXiv:1612.06676 (2016)
9. Gauthama Raman, M., Somu, N., Kirthivasan, K., Sriram, V.: A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems. Neural Networks **92**, 89–97 (2017)
10. Ginter, A.: The top 20 cyber attacks against industrial control systems. https://waterfall-security.com/20-attacks. Accessed 15 Jan 2019
11. Goh, J., Adepu, S., Junejo, K., Mathur, A.: A dataset to support research in the design of secure water treatment systems. In: International Conference on Critical Information Infrastructures Security, pp. 88–99. IEEE (2016)

12. Goh, J., Adepu, S., Tan, M., Lee, Z.: Anomaly detection in cyber physical systems using recurrent neural networks. In: IEEE 18th International Symposium on High Assurance Systems Engineering, pp. 140–145. IEEE (2017)
13. Hajdarevic, A., Dzananovic, I., Banjanovic-Mehmedovic, L., Mehmedovic, F.: Anomaly detection in thermal power plant using probabilistic neural network. In: 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1118–1123. IEEE (2015)
14. Han, S., Xie, M., Chen, H., Ling, Y.: Intrusion detection in cyber-physical systems: techniques and challenges. IEEE Syst. J. **8**, 1052–1062 (2014)
15. Huda, S., Yearwood, J., Hassan, M., Almogren, A.: Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. Appl. Soft Comput. J. **71**, 66–77 (2018)
16. Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C., Jun, S.: Anomaly detection for a water treatment system using unsupervised machine learning. In: IEEE International Conference on Data Mining Workshops, pp. 1058–1065. IEEE (2017)
17. Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C., Sun, J.: Anomaly detection for a water treatment system using unsupervised machine learning. In: IEEE International Conference on Data Mining Workshops ICDMW, pp. 1058–1065. IEEE (2017)
18. Junejo, K.N., Goh, J.: Behaviour-based attack detection and classification in cyber physical systems using machine learning. In: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, pp. 34–43. ACM (2016)
19. Kravchik, M., Shabtai, A.: Detecting cyber attacks in Industrial Control Systems using convolutional neural networks. In: ACM Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, pp. 72–83. ACM (2018)
20. Li, D., Chen, D., Goh, J., Ng, S.: Anomaly detection with generative adversarial networks for multivariate time series. In: 7th International Workshop on Big Data, Streams and Heterogeneous Source Mining: Algorithms, Systems, pp. 1–10. ACM (2018)
21. Malhotra, P., Ramakrishnan, A., Anand, G., Vig, L., Agarwal, P., Shroff, G.: LSTM-based encoder-decoder for multi-sensor anomaly detection. arXiv preprint arXiv:1607.00148 (2016)
22. Mathur, A.P., Tippenhauer, N.O.: SWaT: A water treatment testbed for research and training on ICS security. In: International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), pp. 31–36. IEEE, USA, April 2016
23. McMillen: Attacks targeting Industrial Control Systems (ICS) up 110 percent. https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/. Accessed 15 Jan 2019
24. Myers, D., Suriadi, S., Radke, K., Foo, E.: Anomaly detection for industrial control systems using process mining. Comput. Secur. **78**, 103–125 (2018)
25. Nazir, S., Patel, S., Patel, D.: Assessing and augmenting scada cyber security: a survey of techniques. Comput. Secur. **70**, 436–454 (2017)
26. Raman, M.G., Somu, N., Krithivasan, K., Sriram, V.S.: A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems. Neural Networks **92**, 89–97 (2017)
27. Schneider, P., Bottinger, K.: High-performance unsupervised anomaly detection for cyber-physical system networks. In: ACM Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, pp. 1–12. IEEE (2018)
28. Shalyga, D., Filonov, P., Lavrentyev, A.: Anomaly detection for water treatment system based on neural network with automatic architecture optimization. arXiv preprint arXiv:1807.07282 (2018)

29. Siboni, S., et al.: Security testbed for the Internet of Things Devices. IEEE Trans. Reliab. **68**, 1–12 (2018)
30. Somu, N., Gauthama Raman, M.R., Kalpana, V., Krithivasan, K., Shankar, V.: An improved robust heteroscedastic probabilistic neural network based trust prediction approach for cloud service selection. Neural Networks **108**, 339–354 (2018)
31. Specht, D.: Probabilistic neural networks. Neural Networks **3**, 109–118 (1990)
32. Tran, T.P., Jan, T.: Boosted modified probabilistic neural network (BMPNN) for network intrusion detection. In: The 2006 IEEE International Joint Conference on Neural Network Proceedings, pp. 2354–2361. IEEE (2006)
33. Yu, S.N., Chen, Y.H.: Electrocardiogram beat classification based on wavelet transformation and probabilistic neural network. Pattern Recogn. Lett. **28**(10), 1142–1150 (2007)
34. Zhang, Y., Wang, L., Sun, W., Green, I., Robert, C., Alam, M.: Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans. Smart Grids **2**, 796–808 (2011)
35. Zonouz, S., Davis, C.M., Davis, K.R., Berthier, R., Bobba, R.B., Sanders, W.H.: SOCCA: a security-oriented cyber-physical contingency analysis in power infrastructures. IEEE Trans. Smart Grid **5**(1), 3–13 (2014)