International Journal of Engineering & Technology, 7 (4) (2018) 5084-5089

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.23170
Research paper

Deep Learning Algorithm using Transfer-Entropy measures for Anomaly Detection in Cyber-Physical Systems

Dr. Valliammal. N [1] *, Dr. Padmavathi. G [2]

[1] *Assistant Professor (SS), Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamilnadu, India*
[2] *Professor, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamilnadu, India*
**Corresponding author E-mail: vallinarayancbe@gmail.com*

Abstract

Generally, in cyber-physical systems, there are various attacks detected such as internet-based load altering attacks, False-Data Injection Attack (FDIA), stealthy deception attacks, covert attacks, time synchronization attacks, etc. Over the past decades, attack detection and secure control system design has a high interest due to the rapid growth of cyber security challenges by sophisticated attacks in cyber-physical system like Internet-of-Things (IoT). Among various techniques, Transfer Entropy Measure (TEM) was introduced to detect four types of attacks like Denial-of-Service (DoS), replay, innovation-based deception attack and data injection attacks. Since, it discovers the interaction behavior among pairs of entities generating by each cyber-physical systems. As well, conventional machine-learning based attack detection mechanisms have been successfully employed in IoT i.e., wireless sensors to detect cyber-attacks. However, such mechanisms have less accuracy and scalability with high computational complexity. Hence in this article, a novel distributed deep learning algorithm is proposed for cyber attack detection in IoT since deep learning algorithms try to learn high-level features from data in an incremental manner and solve the problem end to end. Here, the transfer-entropy is measured with different parameters like node, network and channel for sensor measurements. Then, the obtained values are gathered as training dataset. Subsequently, Artificial Neural Network (ANN) and Deep Neural Network (DNN) are trained with training dataset to detect the existence of the attacks in cyber-physical system. Finally, the average detection accuracy values of ANN and DNN are evaluated through the simulation results as 98.9% and 99.6% respectively.

Keywords: *Cyber-Physical Systems; Cyber Attacks; Transfer-Entropy; ANN; DNN; Causality Countermeasures.*

1. Introduction

Nowadays, reinforced safety and security requirements in cyber-physical systems are excitedly designed due to its emergence and significance of communication networks. The security related accidents and smart grid attacks [1] are obviously indicating the impedance of such requirements since vulnerabilities in civil infrastructures and commercial processes may cause destroying consequences to financial system, public security and individual life. Many attack detection and secure control system design on certain types of attacks have the objective of designing detection schemes and constructing attack-resilient controllers according to the feature of the considered attacks. In several scenarios, such designs have high complexity for understanding what type of attacks to be inserted into the system. Conversely, detection of attack types is not always required since the major target is detecting the existence of the attacks and removing it for ensuring secure function. Therefore, systematic approaches have been developed for attack detection and secure estimation policies applicable to different attack scenarios. The problem of cyber attacks detection was resolved by using system and graph-theoretic schemes, cryptographic techniques and machine-learning algorithms.
As well, efficient countermeasures are required to detect the existence of different attacks for dynamic systems which are affected by noises or other disturbances. As a result, TEM were introduced for anomaly detection in cyber-physical systems like IoT, smart grids, process control systems, etc [2]. In this method, transfer entropy was evaluated for both sensor measurements and innovation sequences based on data-driven manner without relying on a model of the underlying dynamic system to detect the four types of attacks were considered such as Denial-of-Service (DoS), replay, innovation-based deception and data injection attacks [3]. The relationship between the countermeasures and the system parameters including noise statistics was estimated and also the time convergence of the countermeasures was ensured according to the conditions provided to observe an abnormal characteristic of the transfer entropy.
However, the novel and emerging IoT application requires advanced cyber security controls, models and decisions distributed at the network. Though the above mentioned approach achieves better solutions, factors like system development flaws, increased attack surfaces and hacking skills have confirmed the certainty of detection mechanisms. Also, they have less accuracy and scalability for cyber-attack detection in fog computing. Therefore, anomaly detection in cyber-physical systems requires an improvement on detection performance by unsupervised deep learning algorithms. Hence in this article, a novel distributed deep learning scheme of cyber-attack detection in IoT is adopted. Deep learning algorithm provides more accurate and fast processing since it has self-learning capability. It has been used in different fields such as

image processing, pattern recognition and computer vision for its advantages in training stability and scalability of huge amount of data. Due to merits of this algorithm, the investigations are carried out in application of deep learning algorithm in security domains. In this algorithm, the transfer-entropy estimation problem is formulated as an adaptive estimation problem. The transfer-entropy based causality countermeasures are obtained with different parameters like node, network and channel for sensor measurements. Then, the obtained values are gathered as training dataset. Moreover, the deep learning algorithms such as ANN and DNN are trained with training dataset to generate different attack models. As a result, the relationship between the counter measures and the considered parameters is learned from training dataset. This learned model is utilized for predicting existence of attacks in cyber-physical system by improving the accuracy, scalability and reducing the computational complexity. This proposed model differs from the conventional approaches by learning the transfer entropy measures using deep learning algorithm and providing the simplest attack detection. The rest of the article is organized as follows: Section 2 presents the research works related to the cyber-attacks detection mechanisms. Section 3 explains the proposed methodology in IoT. Section 4 illustrates the performance effectiveness of the proposed technique. Section 5 concludes the research work.

2. Literature survey

In this section, the existing methods for different attacks detection in cyber-physical systems are discussed in brief. In addition, the limitations in those methods are also observed to improve the detection performance. Distributed internet-based load altering attacks [4] were proposed against smart power grids. Such attacks were launched by compromising direct load control command signals, demand side management price signals or cloud computation load distribution algorithms for affecting the load at the most significant positions in the grid to cause the circuit overflow or the other malicious activities and damage the power system equipment. By using this technique, different types of practical loads that can be vulnerable to internet-based load altering attacks were identified. In addition, preventive techniques were studied to mitigate such attacks or reduce the damage caused by them. However, the cost of load prevention was high.

Detection of FDIA [5] was proposed in cyber-physical DC micro grids. In this technique, the attack detection problem was formulated as detecting a modification in the set of candidate invariants. The candidate invariants were generated by using Hynger that provides an interface between Simulink/Stateflow (SLSF) models and the Daikon tool. Also, a hybrid automation of cyber-physical DC microgrid was presented for obtaining the reach sets via reachability analysis. As well, the original invariants were obtained after verifying whether the reach sets were contained within the candidate invariants. But, the computational complexity of this method was high.

Centralized and distributed monitors [6] were proposed for attack detection and identification. Initially, optimal centralized attack detection and identification monitors were designed. Then, an optimal distributed attack detection filter was designed based on the waveform relaxation scheme. Furthermore, a sub-optimal distributed attack identification process was designed to ensure the performance guarantees. However, the computational complexity of this method was high.

Secure estimation and control [7] was proposed for cyber-physical systems under adversarial attacks. In this approach, a novel simple characterization of the maximum number of attacks was provided that can be detected and corrected as a function of the pair of the system. Also, the state of a system was not precisely reconstructed when more than half the sensors were attacked. As well, a secure local control loop was designed for improving the resilience of the system. Moreover, an efficient algorithm was proposed for estimating the state of the plant despite attacks while number of attacks was smaller than a threshold. However, computational complexity was high due to one-shot estimator.

On finite-state stochastic modelling and secure estimation of cyber-physical systems [8] were proposed. In this method, the problem of secure state estimation and attack detection in cyber-physical system was considered. Initially, a stochastic modelling method was proposed and attacked system was modelled as a finite-state hidden Markov model with switching transition probability matrices controlled by a Markov decision process. According to this method, a joint state and attack estimation problem was formulated and resolved. An un-normalized joint state and attack distribution conditioned on the sensor measurement data was introduced by using the change of probability measure scheme for optimal estimation by evaluating the normalized marginal conditional distributions. However, computation burden was high and the parameter estimation problem for the attack process was not resolved.

Through this survey, it is observed that the previous approaches are mostly based on statistical measures. Such conventional statistical measure models or machine learning approaches have high computational complexity due to requirement of large amount of data and less detection accuracy. As a result, deep learning algorithm like DNN and ANN are applied to detect the attacks on cyber-physical systems with reduced computational complexity and maximized detection accuracy.

3. Proposed methodology

In this proposed technique, a simple system model [3] is considered for linear Gaussian process that serves as a reasonable approximation of the considered system. Also, it is useful to understand how the countermeasures control the detection of the modifications caused by the secret attacks. The main aim of this technique is introducing deep learning based generic countermeasures that are having the ability for detecting the existence of attacks and evaluating the effectiveness of the countermeasures in attack detection. Four types of attacks are considered such are described in below.

- DoS Attacks: It denies the successful transmission of data between nodes in the control systems. The types of DoS attacks are given in Fig. 1.

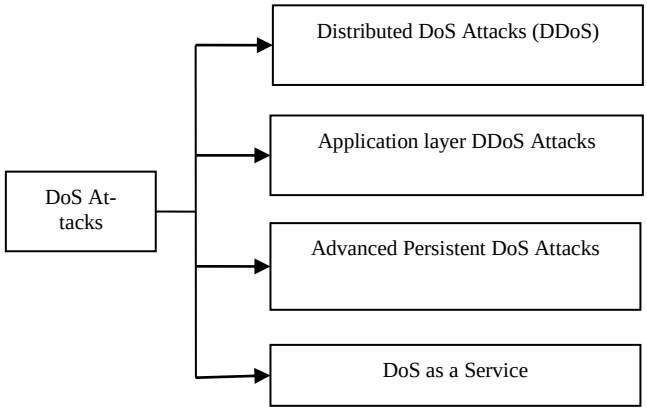

Fig. 1: Types of DoS Attacks.

- Replay Attacks: It prevents the system nodes from knowing the true data and generally consists of two phases. In the first phase, an adversary records the process data for a specific time period and replays the recorded data continuously in the second phase. Thus, destruction on the system is performed in silent manner.
- Innovation-based Deception Attacks: While the measurements are pre-processed on the sensor such that innovation sequences are transmitted to the remote controller, an adversary will try for degrading the system performance by performing attacks on the innovation process.

- Data Injection Attacks: It allows an adversary to inject untrusted input to the system that alters the normal system functions resulting in data loss, data theft, etc. Assume the type of attack on the system is anonymous.

The transfer-entropy (T) [9] between two sensor measurement processes y^1 and y^j as well innovative processes z^1 and z^jat time $k+\tau$ is defined by using the positive integer-valued parameters τ, μ, l and $k \geq \max\{\mu, l\}$ as follows:

$$T_{y^l \to y^i}(k+\tau) = \int a \times b \tag{1}$$

Where $a = f\left(y^i_{k+\tau}, y^i_{k-\mu+1:k}, y^j_{k-l+1:k}\right)$,

$$b = \log \frac{f\left(y^i_{k+\tau} \middle| y^i_{k-\mu+1:k}, y^j_{k-l+1:k}\right)}{f\left(y^i_{k+\tau} \middle| y^i_{k-\mu+1:k}\right)} \times dy^i_{k+\tau} dy^i_{k-\mu+1:k} dy^j_{k-l+1:k} \tag{2}$$

Similarly,

$$T_{z^l \to z^i}(k+\tau) = \int c \times d$$

Where $c = f\left(z^I_{k+\tau}, z^i_{k-\mu+1:k}, z^j_{k-l+1:k}\right)$,

$$d = \log \frac{f\left(z^i_{k+\tau} \middle| z^i_{k-\mu+1:k}, z^j_{k-l+1:k}\right)}{f\left(z^i_{k+\tau} \middle| z^i_{k-\mu+1:k}\right)} \times dz^i_{k+\tau} dz^i_{k-\mu+1:k} dz^j_{k-l+1:k}$$

In above equations, $f(\cdot)$ is the relevant Probability Density Functions (PDF). For the above transfer-entropy measures, the convergence property is analysed using two conditions [3]. In addition, different parameters such as node, network and channel parameters are also estimated for both sensor and innovative processes. Node parameter refers node density, capacity, etc. Network parameter refers delay, packet loss, etc. Channel parameter refers Signal-to-Noise Ratio (SNR), transmission bandwidth, etc. The estimated parameter values are gathered as training database. Once the training dataset is obtained, ANN and DNN are used to train the dataset for creating the different types of attack models by providing the dataset with those measured parameters as input. Here, four types of attacks are identified such as DoS, replay, innovation-based deception and data injection attacks. Fig. 2 show that the attack detection mechanism using this proposed system.

3.1. ANN and DNN classification

The estimated parameters are given to train the ANN classifier. ANN has three layers namely input, hidden and output layer. The probabilities are denoted as $f(x) = x$ are given to the input layer of neurons. In this work, x includes transfer entropy of sensor measurement and innovative processes, node, network and channel parameters. The hidden layer of ANN is defined as tan-sigmoid transfer function.

$$f(x) = \frac{2}{1+e^{-2x}} - 1 \tag{3}$$

Each input has its own weight values as $w_1, w_2, \ldots, w_n$ and the weighted sum of the inputs is done by the adder function as follows:

$$u = \sum_{i=1}^{n} w_i x_i \tag{4}$$

The output layer of ANN is described by the following equation:

$$y = f(\sum_{i=1}^{n} w_i x_i + b_i) \tag{5}$$

In the equation (5), y is the output neuron value; $f(x)$ is the transfer function, w_i refers the weight values, x_i denotes input data values and b_i refers to the bias value. Based on the output neuron values, the relationship between countermeasures and the considered parameters is learned which generates the attack models. By using this learned attack models, the existence of different types of attacks in cyber-physical system is predicted. The basic structure of ANN and DNN is shown in Fig. 3 and Fig. 4. The parameter values for deep learning algorithms are given in Table 1.

Table 1: DNN Parameters

Parameters	Values
Input layer neurons	120
First hidden layer neurons	80
Second hidden layer neurons	80
Third hidden layer neurons	50
Output layer neurons	2
Learning rate	0.01
Transfer function	Tan-Sigmoid
Maximum number of iteration	50

During training, learning rate is used to control the weight and bias value changes in each iteration process i.e., each updation of weight and bias values. By configuring the parameters mentioned in Table 1, training dataset can be trained using deep learning algorithms.

Pseudocode of the Proposed System

Step 1: Initialize the cyber-physical system using number of sensors with set of process.
Step 2: Estimate the transfer entropy of each process using (1) and (2).
Step 3: Compute the different parameters like node, network and channel.
Step 4: Collect the training dataset with number of computed parameters and transfer entropy.
Step 5: Learn the training dataset using ANN and DNN algorithm.
Step 6: Predict the existence of the attacks.

4. Result and discussion

In this section, the performance effectiveness of the proposed method is evaluated in MATLAB 2018a by using the most popular dataset such as DARPA's NSL-KDD dataset that consists of selected records of the complete KDD dataset [13, 14]. It has both training and testing dataset and widely used in attacks detection. This dataset has different advantages as follows:

- There are no duplicate records in the testing dataset. Hence, the performance of the learners is not biased by the detection methods which have better detection accuracies on the frequent records.
- The amount of records in the training and testing datasets are realistic which makes it inexpensive for performing the experiments on the complete dataset without the requirement for randomly selecting a small segment.
- It does not contain redundant records in the training dataset. Therefore, the classifiers will not be biased towards more frequent records.

It includes 10% of original dataset i.e., approximately 4,94,020 single connection vectors and each of which has 41 features such as time period, protocol, service type, source bytes, destination bytes and normal or specific attack labels. The traffic distribution of NSL-KDD dataset is given in Table 2.

Table 2: Traffic Distribution of NSL-KDD Dataset

Traffic	Training	Testing
Normal	67,343	9,711
Attack	58,630	12,833
Total	1,25,973	22,544

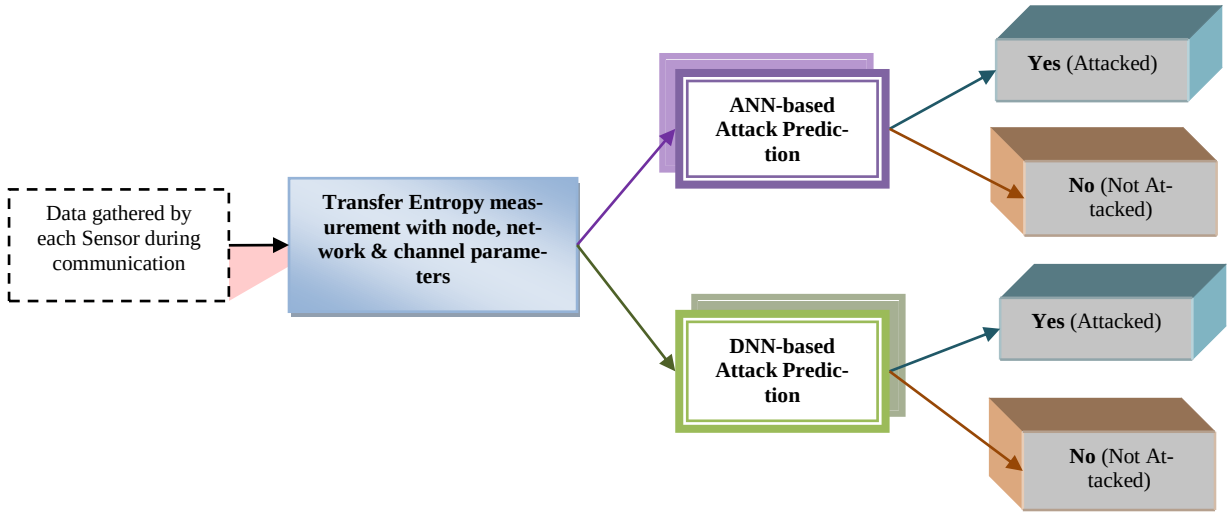

Fig. 2: Proposed System for Cyber Attack Detection.

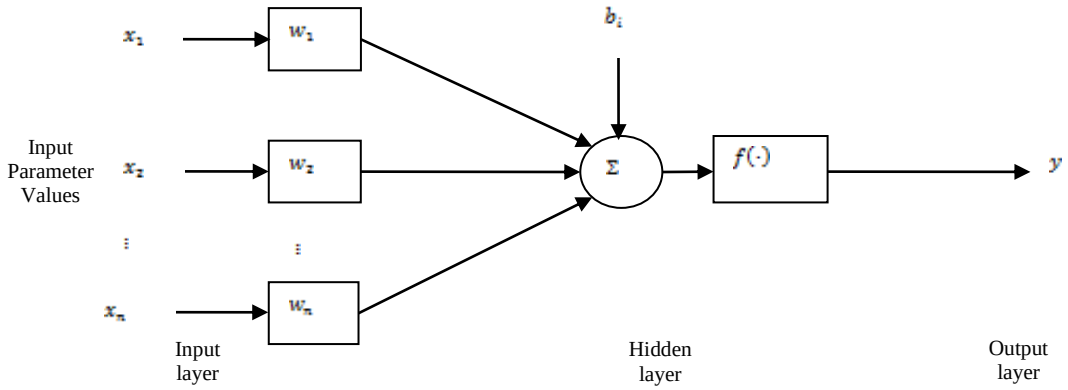

Fig. 3: Basic Structural Design of ANN.

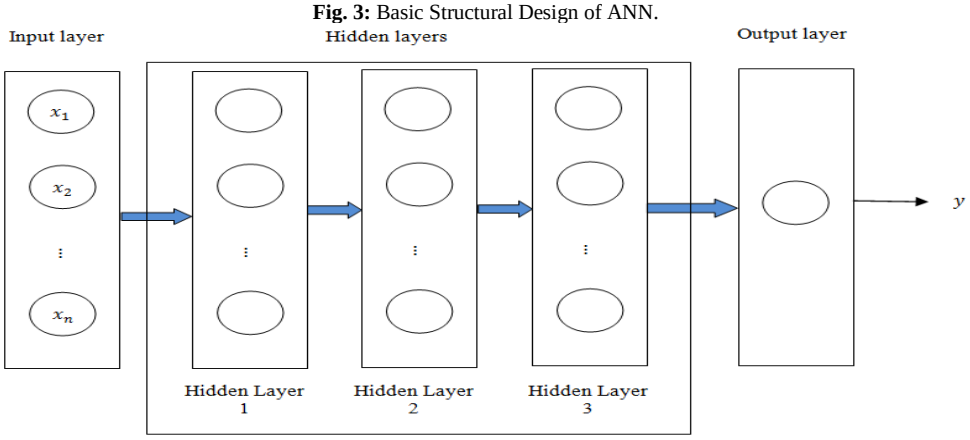

Fig. 4: Architecture of DNN Algorithm.

In this experiment, the detection accuracy and sensitivity of ANN and DNN based cyber attacks detection schemes for each type of attack is compared to the existing TEM approach. Since sensitivity evaluates how good the system is performed a positive detection and also detection accuracy measures how correctly a detection system detects and excludes a given condition. In addition to these metrics, Receiver Operating Characteristic (ROC) is also analysed. These metrics are considered for scalability measure.

4.1. Detection accuracy

Detection accuracy is defined as the fraction of anomaly systems and normal cyber-physical systems correctly detected. It is calculated as follows:

$$\text{Detection Accuracy} = \frac{TP+TN}{TP+TN+FN+FP} \times 100\% \quad (6)$$

Here, TP is True Positive, TN is True Negative, FN is False Negative and FP is False Positive. Table 3 shows the detection accuracy values of proposed and existing approaches in cyber attack detection.

Table 3: Comparison of Detection Accuracy (%)

Types of Attacks	TEM	ANN	DNN
DoS Attack	93.33	95.33	98
Replay Attack	88	90	94
Innovation-based Deception Attack	85.88	88.24	91.76
Data Injection Attack	91.46	94.51	96.95

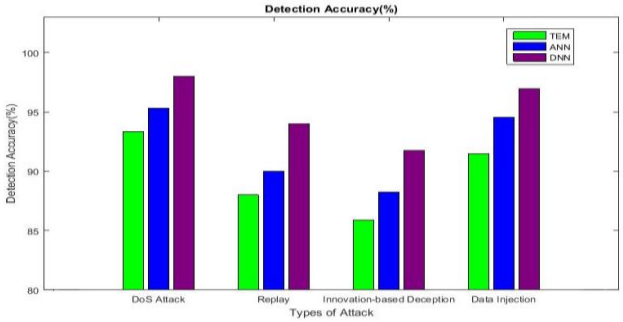

Fig. 5: Comparison of Detection Accuracy.

Fig. 5 shows that the comparison of detection accuracy for both ANN and DNN-based cyber attacks detection compared to the TEM. From the graph, it is observed that the DNN and ANN based cyber attack detection achieves better detection accuracy compared to the TEM according to the various types of attacks. Clearly, it demonstrates that existence of the attacks is efficiently predicted by learning the transfer-entropy measures that reduces the computational complexity.

4.2. Sensitivity

Sensitivity is defined as the fraction of anomaly systems correctly detected and is used for evaluating the uncertainty in the output of attack model may be assigned to different sources of uncertainty in its inputs. It is computed as follows:

$$\text{Sensitivity} = \frac{TP}{TP+FN} \times 100\% \quad (7)$$

Table 4 shows the sensitivity values of proposed and existing approaches in cyber attack detection.

Table 4: Comparison of Sensitivity

Types of Attacks	TEM	ANN	DNN
DoS Attack	0.93	0.95	0.98
Replay Attack	0.71	0.83	0.92
Innovation-based Deception Attack	0.50	0.75	0.75
Data Injection Attack	0.91	0.94	0.97

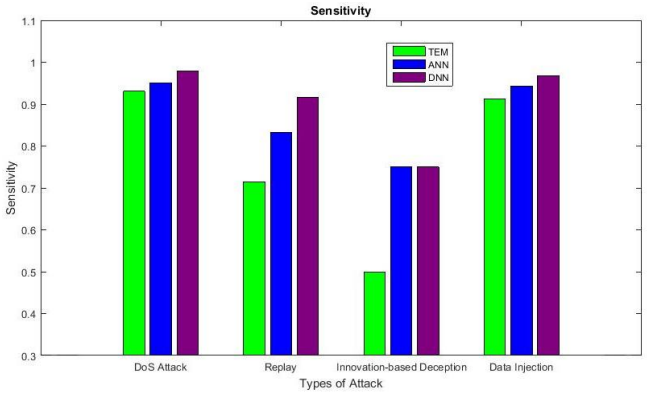

Fig. 6: Comparison of Sensitivity Analysis.

Fig. 6 illustrates that the analysis of sensitivity for both ANN and DNN-based cyber attacks detection compared to the TEM approach. From the graph, it is observed that the DNN and ANN-based cyber attack detection achieves better sensitivity compared to the TEM approach according to the various types of attacks. Obviously, it proves that existence of the attacks is efficiently predicted by learning the transfer-entropy measures that reduces the computational complexity.

4.3. ROC analysis

The ROC curve is defined as the relation between the FP rate and TP rate. The values of ROC curves of TEM, ANN and DNN methods for detecting DoS attacks are given in Table 5.

Table 5: Comparison of ROC Curves for DoS Attack

FP Rate	TP Rate			% of Improvements	
	TEM	ANN	DNN	DNN & TEM	DNN & ANN
0	0.9	0.95	0.98	8.89%	3.15%
0.2	0.89	0.92	0.96	7.87%	4.35%
0.4	0.87	0.91	0.96	10.34%	5.50%
0.6	0.86	0.91	0.96	11.63%	5.50%
0.8	0.86	0.91	0.96	11.63%	5.50%
1	0.86	0.91	0.96	11.63%	5.50%

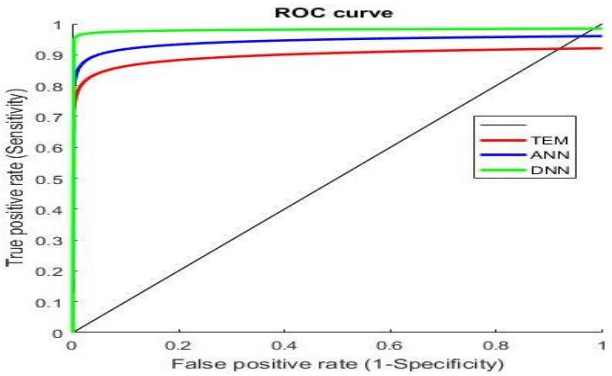

Fig. 7: ROC Curves for Dos Attack.

Fig. 7 illustrates that the analysis of ROC curves for DoS attack detection using both ANN and DNN-based cyber attacks detection compared to the TEM approach. From the graph, it is observed that the effectiveness of DNN in that the TP value is 0.96 while the FP value accounts less than 0.2. As a result, DNN-based cyber attack detection behaves observably better than the other approaches for detecting DoS attacks.

The values of ROC curves of TEM, ANN and DNN methods for detecting replay attacks are given in Table 6.

Table 6: Comparison of ROC Curves for Replay Attack

FP Rate	TP Rate			% of Improvements	
	TEM	ANN	DNN	DNN & TEM	DNN & ANN
0	0.92	0.93	0.99	7.61%	6.45%
0.2	0.90	0.92	0.99	10%	7.61%
0.4	0.89	0.91	0.99	11.24%	8.80%
0.6	0.89	0.91	0.99	11.24%	8.80%
0.8	0.89	0.91	0.98	10.11%	7.70%
1	0.89	0.91	0.97	8.99%	6.60%

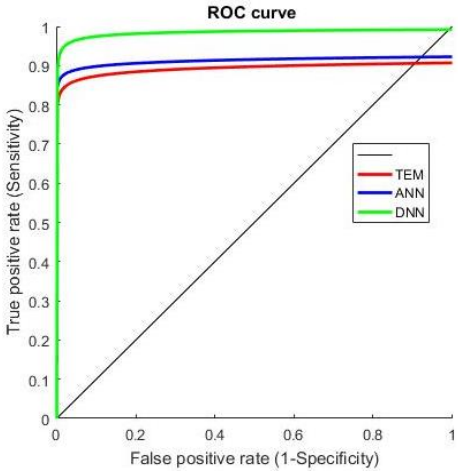

Fig. 8: ROC Curves for Replay Attack.

Fig. 8 illustrates that the analysis of ROC curves for replay attack detection using both ANN and DNN-based cyber attacks detection compared to the TEM approach. From the graph, it is observed that the effectiveness of DNN in that the TP value is 0.99 while the FP value accounts less than 0.2. Consequently, DNN-based cyber attack detection behaves noticeably better than the other approaches for detecting DoS attacks.

The values of ROC curves of TEM, ANN and DNN methods for detecting innovation-based deception attack are given in Table 7.

Table 7: Comparison of ROC Curves for Innovation-Based Deception Attack

FP Rate	TP Rate			% of Improvements	
	TEM	ANN	DNN	DNN & TEM	DNN & ANN
0	0.90	0.96	0.99	10%	3.13%
0.2	0.86	0.89	0.99	15.12%	11.24%
0.4	0.85	0.89	0.98	16.47%	10.11%
0.6	0.85	0.89	0.98	16.47%	10.11%
0.8	0.85	0.89	0.972	14.35%	9.21%
1	0.85	0.89	0.96	12.94%	7.87%

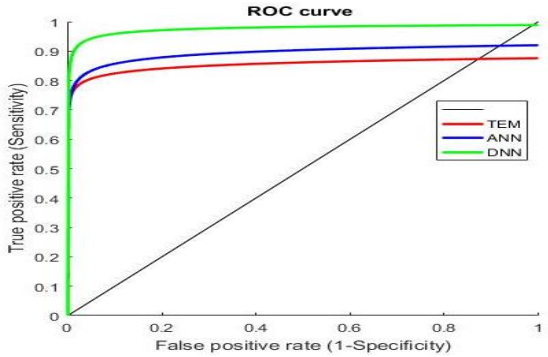

Fig. 9: ROC Curves for Innovation-based Deception Attack.

Fig. 9 illustrates that the analysis of ROC curves for innovation-based deception attack detection using both ANN and DNN-based cyber attacks detection compared to the TEM approach. From the graph, it is observed that the effectiveness of DNN in that the TP value is 0.99 while the FP value accounts less than 0.2. Accordingly, DNN-based cyber attack detection behaves clearly better than the other approaches for detecting innovation-based deception attack.

The values of ROC curves of TEM, ANN and DNN methods for detecting data injection attacks are given in Table 8.

Table 8: Comparison of ROC Curves Data Injection Attack

FP Rate	TP Rate			% of Improvements	
	TEM	ANN	DNN	DNN & TEM	DNN & ANN
0	0.86	0.90	0.99	15.12%	10%
0.2	0.84	0.89	0.99	17.86%	11.24%
0.4	0.82	0.88	0.98	19.51%	11.36%
0.6	0.82	0.88	0.975	18.90%	10.80%
0.8	0.82	0.88	0.968	18.05%	10%
1	0.82	0.88	0.96	17.07%	9.10%

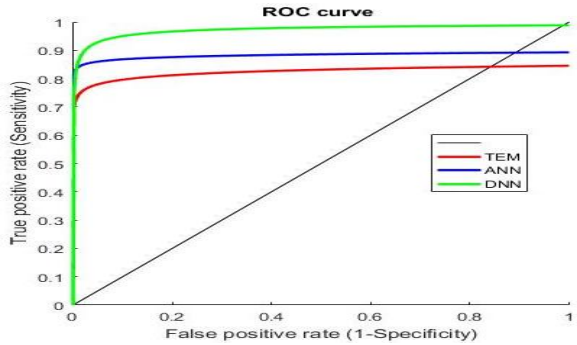

Fig. 10: ROC Curves for Data Injection Attack.

Fig. 10 illustrates that the analysis of ROC curves for data injection attack detection using both ANN and DNN-based cyber attacks detection compared to the TEM approach. From the graph, it is observed that the effectiveness of DNN in that the TP value is 0.99 while the FP value accounts less than 0.2. Thus, DNN-based cyber attack detection behaves evidently better than the other approaches for detecting data injection attacks.

5. Conclusion

In this article, cyber attack detection is improved by proposing a novel distributed deep learning scheme in cyber-physical systems. By using this scheme, the transfer-entropy based causality countermeasures are obtained with node, network and channel parameters for both sensor measurements and innovation sequences to form training dataset. Then, ANN and DNN are applied to the training dataset for creating four types of attack models. Moreover, the relationship between the countermeasures and the considered parameters is learned from training dataset. This learned model is utilized to predict the existence of attacks in cyber-physical system. Thus, the proposed scheme achieves better cyber security than the classical cyber attack detection schemes and scalability in terms of detection accuracy, sensitivity and ROC. Through the simulation results, it is noticed that anomaly detection using DNN achieves higher performance than the other attacks detection approaches.

References

[1] Liu Y, Ning P, & Reiter MK (2011), "False data injection attacks against state estimation in electric power grids", *ACM Transactions on Information and System Security (TISSEC)*, *14*(1), 13. https://doi.org/10.1145/1952982.1952995.

[2] Mo Y, Chabukswar R, & Sinopoli B (2014), "Detecting integrity attacks on SCADA systems", *IEEE Transactions on Control Systems Technology*, *22*(4), 1396-1407. https://doi.org/10.1109/TCST.2013.2280899.

[3] Shi D, Guo Z, Johansson KH, & Shi L (2018), "Causality countermeasures for anomaly detection in cyber-physical systems", *IEEE Transactions on Automatic Control*, *63*(2), 386-401. https://doi.org/10.1109/TAC.2017.2714646.

[4] Mohsenian-Rad AH, & Leon-Garcia A (2011), "Distributed internet-based load altering attacks against smart power grids", *IEEE Transactions on Smart Grid*, *2*(4), 667-674. https://doi.org/10.1109/TSG.2011.2160297.

[5] Beg OA, Johnson TT, & Davoudi A (2017), "Detection of false-data injection attacks in cyber-physical dc microgrids", *IEEE Transactions on Industrial Informatics*, *13*(5), 2693-2703. https://doi.org/10.1109/TII.2017.2656905.

[6] Pasqualetti F, Dörfler F, & Bullo F (2013), "Attack detection and identification in cyber-physical systems", *IEEE Transactions on Automatic Control*, *58*(11), 2715-2729. https://doi.org/10.1109/TAC.2013.2266831.

[7] Fawzi H, Tabuada P, & Diggavi S (2014), "Secure estimation and control for cyber-physical systems under adversarial attacks", *IEEE Transactions on Automatic Control*, *59*(6), 1454-1467. https://doi.org/10.1109/TAC.2014.2303233.

[8] Shi D, Elliott RJ, & Chen T (2017), "On Finite-State Stochastic Modeling and Secure Estimation of Cyber-Physical Systems", *IEEE Trans. Automat. Contr.*, *62*(1), 65-80. https://doi.org/10.1109/TAC.2016.2541919.

[9] Yu W, & Yang F (2015), "Detection of causality between process variables based on industrial alarm data using transfer entropy", *Entropy*, *17*(8), 5868-5887. https://doi.org/10.3390/e17085868.

[10] Duan P, Yang F, Chen T, & Shah SL (2013), "Direct causality detection via the transfer entropy approach", *IEEE transactions on control systems technology*, *21*(6), 2052-2066. https://doi.org/10.1109/TCST.2012.2233476.

[11] Duan P, Yang F, Shah SL, & Chen T (2015), "Transfer zero-entropy and its application for capturing cause and effect relationship between variables", *IEEE Transactions on Control Systems Technology*, *23*(3), 855-867. https://doi.org/10.1109/TCST.2014.2345095.

[12] Marques VM, Munaro CJ, & Shah SL (2015), "Detection of causal relationships based on residual analysis", *IEEE Transactions on Automation Science and Engineering*, *12*(4), 1525-1534. https://doi.org/10.1109/TASE.2015.2435897.

[13] Tavallaee M, Bagheri E, Lu W, & Ghorbani, AA (2009), "A detailed analysis of the KDD CUP 99 data set", In *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on* (pp. 1-6). IEEE. https://doi.org/10.1109/CISDA.2009.5356528.

[14] KDD'99 Competition Dataset. Available on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 1999.