Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System

# Kuang Lieh Lu; Guo-Qiang Zeng; Xizhao Luo et al.

## 2021

We proposed two novel methods to detect cyber-attacks of supervisory control and data acquisition network traffic in industrial automation and control systems by employing population extremal optimization algorithm and ensemble strategy

# Abstract

Industrial automation and control systems (IACS) are tremendously employing supervisory control and data acquisition (SCADA) network. However, their integration into IACS is vulnerable to various cyber-attacks. In this article, we first present population extremal optimization (PEO)-based deep belief network detection method (PEO-DBN) to detect the cyber-attacks of SCADA-based IACS. In PEO-DBN method, PEO algorithm is employed to determine the DBN's parameters, including number of hidden units and the size of mini-batch and learning rate, as there is no clear knowledge to set these parameters. Then, to enhance the performance of single method for cyber-attacks detection, the ensemble learning scheme is introduced for aggregation of the proposed PEO-DBN method, called EnPEO-DBN. The proposed detection methods are evaluated on gas pipeline system dataset and water storage tank system dataset from SCADA network traffic by comparing with some existing methods. Through performance analysis, simulation results show the superiority of PEO-DBN and EnPEO-DBN.

# Study subjects

**8449 samples**

In addition, due to the large number of normal traffic, the class distribution will be imbalanced. **Some samples of normal traffic are discarded and 8449 samples are used in the simulations, where 7600 samples are used as training samples and the others are testing samples**. From the description of proposed methods, we can see that the proposed methods can be extended to different types of datasets

# Scholarcy Highlights

* T HE Internet of Things (IoT) can interconnect electrical equipment with servers and enable collection and aggregation of data [1]
* The cyber-attacks detection method can receive any response from programmable logic controllers (PLCs)/remote terminal units (RTUs) to master terminal unit (MTU) or query from MTU to PLC/RTU
* Deep belief network (DBN) [18] and long short-term memory neural network (LSTM) [29] belong to deep learning, and to further illustrate the performance of population extremal optimization (PEO)-DBN, these two deep learning-based methods are used as the competitors
* decision tree-based method (DT) [28], ensemble of SVM (EnSVM) [7], and ensemble of DBN (EnDBN) [7], as the ensemble methods including the shallow and deep machine learning, are used as the competitors to show the performance of EnPEO-DBN
* We proposed two novel methods (PEO-DBN and EnPEO-DBN) to detect cyber-attacks of supervisory control and data acquisition (SCADA) network traffic in industrial automation and control systems (IACS) by employing PEO algorithm and ensemble strategy
* In PEO-DBN, PEO was employed for automatic parameter optimization of DBN rather other manual setting

# Scholarcy Summary

## Introduction

T HE Internet of Things (IoT) can interconnect electrical equipment with servers and enable collection and aggregation of data [1].

In industrial IoT (IIoT) networks [2], there are massive amount of supervisory control and data acquisition (SCADA)-based IACS.

This structure is composed of physical layer, cyber layer, and operation/corporate layer.

The cyber layer is used to monitor and control the various devices in local control layer.

Massive devices are linked to SCADA-based IACS, which facilitates the less-expensive data communication and acquisition.

These devices of SCADA network are vulnerable to various cyber-attacks [3]

## Methods

A. Proposed EnPEO-DBN Method We give a novel ensemble method to enhance the detection performance of cyber-attacks in IACS based on PEO-DBN detection method .

M base classifiers are obtained based on Xk. In other words, after training process accomplished, M different PEO-DBN-based classifiers are obtained.

After training process accomplished, M different PEO-DBN-based classifiers are obtained

These classification results are integrated by the majority voting scheme mentioned in (7).

The cyber-attacks detection method can receive any response from PLC/RTU to master terminal unit (MTU) or query from MTU to PLC/RTU.

The main parts of method for detecting cyber-attacks are given as follows

## Results

According to (8), we can obtain the fitness value Fi of each solution Si in P.

Based on the Algorithm 3: Initialization operation (InitializeOperation).

Input: Population size N P , the lower and upper values of adjustable parameters XL, XU.

P (i) ← XL + (XU − XL) × Rmi; 3: end for 4: return P.

Input: The population P , training dataset tr\_x, tr\_y

## Conclusion

We proposed two novel methods (PEO-DBN and EnPEO-DBN) to detect cyber-attacks of SCADA network traffic in IACS by employing PEO algorithm and ensemble strategy.

The simulation indicates that the proposed PEO-DBN and EnPEO-DBN can be considered as competitive cyber-attacks detection methods for SCADA-based IACS.

The proposed PEO-DBN can automatically tune the parameters in DBN, the fitness evaluation costs much time in the whole process of PEO.

To address this problem, we can use the surrogate-assisted model, e.g., Gaussian process regression or Bayesian optimization to further accelerate the fitness evaluation in further work

# Confirmation of earlier findings

Although the evolutionary DBN can automatically adjust the parameters, the single method can be further improved by ensemble learning method. **Ensemble learning schemes [13] have shown the superiority over single-model-based method by employing a certain scheme for aggregation of the results obtained by single method**

# Contributions

In this article, we proposed two novel methods (PEO-DBN and EnPEO-DBN) to detect cyber-attacks of SCADA network traffic in IACS by employing PEO algorithm and ensemble strategy. In PEO-DBN, PEO was employed for automatic parameter optimization of DBN rather other manual setting. In EnPEO-DBN, three PEO-DBNs with different features separately learned the mapping function between the traffic features and cyber-attacks types and then the majority voting scheme was used to obtain the final detection results. To verify the effectiveness of PEO-DBN and EnPEO-DBN, two real SCADA network datasets, i.e., gas pipeline system and water storage tank system, were chosen as the case studies by comparing with ELM [27], SVM [7], DT [28], DBN [18], EnSVM [7], EnDBN [7], and LSTM [29] in terms of different evaluation metrics. The simulation indicates that the proposed PEO-DBN and EnPEO-DBN can be considered as competitive cyber-attacks detection methods for SCADA-based IACS.Although the proposed PEO-DBN can automatically tune the parameters in DBN, the fitness evaluation costs much time in the whole process of PEO. To address this problem, we can use the surrogate-assisted model, e.g., Gaussian process regression or Bayesian optimization to further accelerate the fitness evaluation in further work.

# Future work

Considering the advantages of PBT, the performance of PBT-based DBN for cyber-attacks detection can be further investigated in future work.