International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Detection of Cyber Attacks on Network Using Machine Learning Techniques

CH SIVASANKAR[1], E AKASH[2], G PRATHYUSHA[3],B PRAVEEN KUMAR[4], Y V S A YASWANTH[5]
[1]Assitant professor, [2,3,4,5] Students, Dept of CSIT
[1,2,3,4,5] Siddharth Institute of Engineering & Technology, Puttur-517583

Abstract

Cyber-physical systems(cps) have made significant progress in many dynamic applications due to the integration between physical processes, computational resources, and communication capabilities. However, cyber-attacks are a major threat to these systems. Some of these attacks which are called deception attacks, inject false data from sensors or controllers, and also by compromising with some cyber components, corrupt data, or enter misinformation into the system. If the system is unaware of the existence of these attacks, it won't be able to detect them, and performance may be disrupted or disabled altogether. Therefore, it is necessary to adapt algorithms to identify these types of attacks in these systems. The proposed method in this study is to use the structure of deep neural networks for the detection phase, which should inform the system of the existence of the attack in the initial moments of the attack.

Keywords: Cyber-physical systems(cps).Cyber attacks, Machine Learning, KidneyIntroduction

Introduction

Recent advances in technology have led to the introduction of cyber-physical systems, which due to their better computational and communicational ability and integration between physical and cyber-components, has led to significant advances in many dynamic applications. But this improvement comes at the cost of being vulnerable to cyber-attacks. Cyber-physical systems are made up of logical elements and embedded computers, which communicate with communication channels such as the Internet of Things(IoT). More specifically, these systems include digital or cyber components, analog components, physical devices and humans that designed to operate between physical and cyber parts. In other words, a cyber-physical system is any system that includes cyber and physical components and humans, and has the ability to trade between the physical and cyber parts. In cyber-physical systems, the security of these types of systems becomes more important due to the addition of the physical part.

The security of cyber-physical systems to detect cyber-attacks is an important issue in these systems . It should be noted that cyber-attacks occur in irregular ways, and it is not possible to describe these attacks in a regular and orderly manner. In general, cyber attacks in cyber-physical systems are

divided into two main types: denial of service(Dos) and deception attacks. In denial of service, the attacker prevents communication between network nodes and communication channels. However, in the deception attacks that inject false data to system, which are carried out by abusing system components , such as sensors or controllers and it can corrupt data or enter incorrect information into the system and cause misbehaving.

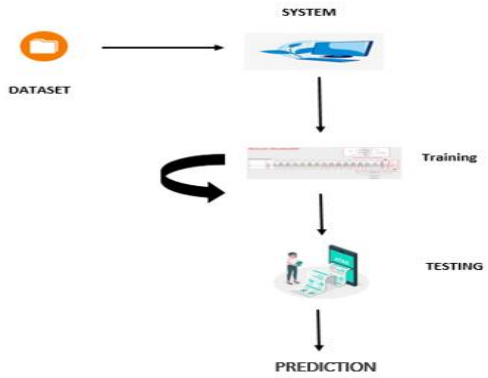
These attacks can be detected by system monitoring in the system. But if the attacker can plan a high-level attack to prevent himself from being identified, these attacks are called stealthy deception attacks, and other common methods of counteracting such attacks will not work. Therefore, it is important to be aware of the attacks that occur in order to respond in a timely manner to attackers. In other words, the security system must be aware of the attack, otherwise it will not be able to detect and control the attack. Cyber defence can be improved by using security analytic to search for hidden patterns and how to deceive.

Related Work

1.Objective

The primary goal of this project is to determine the cyber-attack whether there will be attack or not and to know this we have used the Support Vector, Random forest and Neural network classification techniques.

2. Architecture:



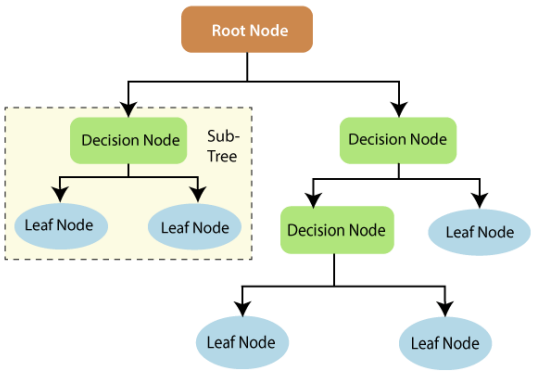
3. Algorithm

3.1 Random Forest Classifier

A random forest is a machine learning technique that's used to solve regression and classification problems. It utilizes ensemble learning, which is a technique that combines many classifiers to provide solutions to complex problems.

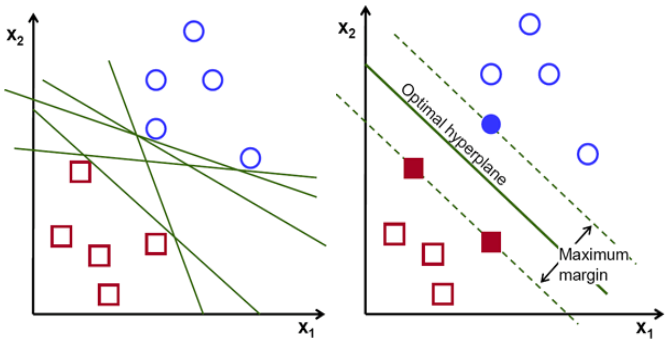
A random forest eradicates the limitations of a decision tree algorithm. It reduces the over fitting of datasets and increases precision. It generates predictions without requiring many configurations in packages (like Scikit-learn).

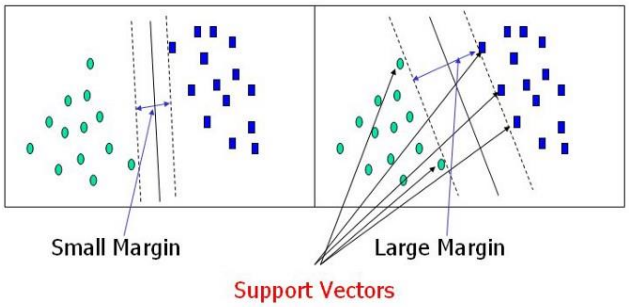
- It's more accurate than the decision tree algorithm.
- It provides an effective way of handling missing data.
- It can produce a reasonable prediction without hyper-parameter tuning.



3.1 Support Vector Machines

The objective of the support vector machine algorithm is to find a hyper plane in an N-dimensional space (N — the number of features) that distinctly classifies the data points.

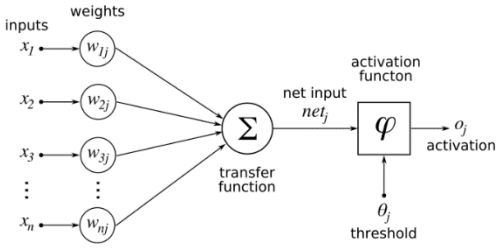




3.3 Neural Network

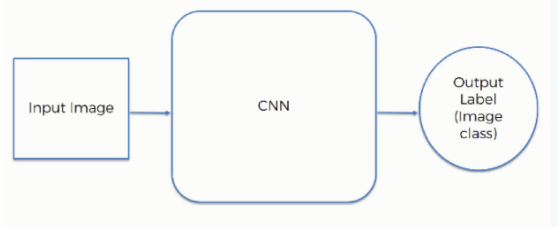
An artificial neural network (ANN) is the piece of a computing system designed to simulate the way the human brain analyzes and processes information. It is the foundation of artificial intelligence (AI) and solves problems that would prove impossible or difficult by human or statistical standards. ANNs have self-learning capabilities that enable them to produce better results as more data becomes available.

An ANN initially goes through a training phase where it learns to recognize patterns in data, whether visually, aurally, or textually. During this supervised phase, the network compares its actual output produced with what it was meant to produce—the desired output. The difference between both outcomes is adjusted using backpropagation. This means that the network works backward, going from the output unit to the input units to adjust the weight of its connections between the units until the difference between the actual and desired outcome produces the lowest possible error.



3.4 Convolutional Neural Network

A convolutional neural network, or CNN, is a deep learning neural network designed for processing structured arrays of data such as images. Convolutional neural networks are widely used in computer vision and have become the state of the art for many visual applications such as image classification, and have also found success in natural language processing for text classification.

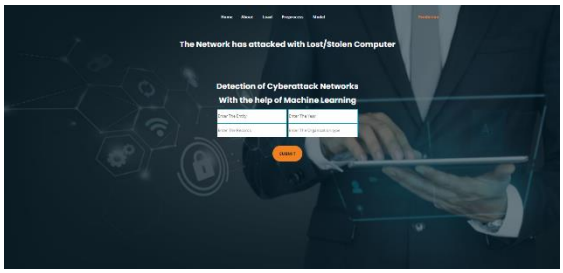


Procedure:

- Upload the dataset of data-breaches which contain the cyber-attacks data for loading .
- Data Pre-processing is a fashion that's used to convert the raw data into a clean data set.
- Removing the null values, filling the null values with meaningful value, removing indistinguishable values, removing outliers, removing unwanted attributes.
- If dataset contains any categorical records means convert those categorical variables to numerical values.
- For that we split the data into two parts for training and testing.
- Then we choose the algorithm and check it's accuracy.
- Finally we can check the type of attack by filling the data.

4. Result:

After filling the data the system replies with the detected attacks as shown in the below image



5. Conclusion:

In this study, an attempt was made to use the resilient control consensus method in complex discrete cyber-physical networks with a number of local attacks off. By applying this control method, it was observed that even in the presence of cyber-attacks, the system can remain stable and isolate the attacked node and the performance of the system is not weakened. Using the neural network used in this study, it was observed that with a deep neural network, with 7 hidden layers, the system shows better performance. Also in a recurrent neural network integrated with a deep neural network, a deep layer network with a linear function performs better. Therefore, it can be said that the system has less complexity. So With deep learning method, systems can analyze patterns and learn from them to help prevent similar attacks and respond to changing behavior. In short, machine learning can make cyber security simpler, more proactive, less expensive and far more effective. After observing the state of the system reported by the neural network, the control system makes decisions based on it and, if there is an attack, detects it and isolates it, so as not to have a detrimental effect on the behavior of other agents. In future research, more attacks on agents can be considered, also data mining and other machine learning methods, such as support vector machine (SVM) algorithms or other types of neural networks such as neural networks to evaluate system performance improvements.

6. References:

1. Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang. ”Security analysis for cyber-physical systems against stealthy deception attacks.” In 2013 American control conference, IEEE (2013): 3344-3349.
2. Pajic, Miroslav, James Weimer, Nicola Bezzo, Oleg Sokolsky, George J. Pappas, and Insup Lee. ”Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators.” IEEE Control Systems Magazine 37, no. 2 (2017): 66-81.
3. Sheng, Long, Ya-Jun Pan, and Xiang Gong. ”Consensus formation control for a class of networked multiple mobile robot systems.” Journal of Control Science and Engineering 2012 (2012).
4. Zeng, Wente, and Mo-Yuen Chow. ”Resilient distributed control in the presence of misbehaving agents in networked control systems.” IEEE transactions on cybernetics 44, no. 11 (2014): 2038-2049.
5. Sun, Hongtao, Chen Peng, Taicheng Yang, Hao Zhang, and Wangli He. ”Resilient control of networked control systems with stochastic denial of service attacks.” Neurocomputing 270 (2017): 170-177.
6. Zhang, Haotian, and Shreyas Sundaram. ”Robustness of information diffusion algorithms to locally bounded adversaries.” In 2012 American Control Conference (ACC), IEEE (2012): 5855-5861.
7. Fu, Weiming, Jiahu Qin, Yang Shi, Wei Xing Zheng, and Yu Kang. ”Resilient Consensus of Discrete-Time Complex Cyber-Physical Networks under Deception Attacks.” IEEE Transactions on Industrial Informatics (2019).
8. Ozay, Mete, Inaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor. ”Machine learning methods for attack detection in the smart grid.” IEEE transactions on neural networks and learning systems 27, no. 8 (2015): 1773-1786.
9. Tianfield, Huaglory. ”Data mining based cyber-attack detection.” System simulation technology 13, no. 2 (2017): 90-104.
10. Pasqualetti, Fabio, Florian Dorfler, and Francesco Bullo. ”Attack detection and ¨ identification in cyber-physical systems.” IEEE Transactions on Automatic Control 58, no. 11 (2013): 2715-2729.