A CLOUD-FOG-EDGE CLOSED-LOOP FEEDBACK SECURITYRISK PREDICTION METHOD

K. Dinesh Babu[1], S. Noordeen[2]

[1]*Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India.*
E-mail:racingdinesh123@gmail.com

[2]*Assistant Professor Grade-II, Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India*
Email: noordeen@avit.ac.in

ABSTRACT

In recent years, with the opening of the ``smart age'' curtain, smart devices dominated by technologies such as robots, drones, and intelligent perception have gradually moved to the center of the Intelligent CPSS stage. However, the new security risks of the Intelligent CPSS have also become increasingly prominent. Especially in recent years, in Ukraine and Venezuela's power attack incidents, a series of related attacks always occur simultaneously. This is a multi-task compound attack. This paper designs a set of Cloud-Fog-Edge closed-loop feedback security risk prediction strategies for multi-task compound attacks based on the offensive and defensive ideas of intelligent games, combining classified deep Boltzmann machines and Markov time-varying models. This strategy can be used for various types of power intelligent system terminals, and realizes security risk prediction with modularity, interoperability, open interfaces and compliance with open standards. Interoperability with other safety equipment can also be achieved through standardized interfaces to form system security protection capabilities to meet the actual needs of the industry Internet system.

Keywords: ***Risk Prediction, classification deep Boltzmann machine, Markov time-varying model.***

I. INTRODUCTION

In recent decades, energy demand around the globe has shown the increasing trend. In past, most of the power generation was being done from fossil fuels. However, to fulfil the increasing electricity demand with minimal emissions of greenhouse gases scientists have worked on the new means of electricity generation: renewable and sustainable energy resources (RSERs). But, the penetration of renewable energy sources (RESs) significantly increased power system complexity and dynamics, and the existing power system is not capable of maintaining its stability if the integration of RESs and distributed generation (DG) is done at a large scale. Edge Cloud, addresses this specific issues by augmenting the traditional data centers consisting of cloud models with service nodes placed at the network edges[1]. The proximity of edge nodes allows data processing to and from far remote clouds to be done at the edge. By

processing data locally through accelerated data streams it is possible to reduce network traffic bottlenecks. Clone clouds and computational off-loading provide a distributed mechanism of application execution thereby augmenting the resources of the smart device with cloud resources[2]. A clone allows the dynamic execution of various applications by alternating between clone and device. Fog computing gives the user option of performing cloud operations at locations closer to point of interest. It uses existing networks, routers in nearby locations to perform operations just like cloud[3]. In this paper difference between these technologies and their build types is discussed.

2. RELATED WORKS

``A novel network intrusion attempts prediction model based on fuzzy neural network,"

Identifying the intrusion attempts of the monitored systems is extremely vital for the next generation intrusion detection system. In this paper, a novel network intrusion attempts prediction model (FNNIP) is developed, which is based on the observation of network packet sequences. A new fuzzy neural network based on a novel BP learning algorithm is designed and then applied to the network intrusion attempts predicting scheme. After given the analysis of the features of the experimental data sets, the experiment process is detailed. The experimental results show that the proposed Scheme has good accuracy of predicting the network intrusion attempts by observing the network packet sequences.

``Security threat prediction in a local area network using statistical model,"

In today's large and complex network scenario vulnerability scanners play a major role from security perspective by proactively identifying the known security problems or vulnerabilities that exists across a typical organizational network. Identifying vulnerabilities before they can be exploited by malicious user often helps to test, maintain, and assess the risk of the existing network. Still there are many problems with currently available state of the art vulnerability scanners like hampering system resource. One possible solution to this problem might be reducing the number of vulnerability scans, along with the quantitative approach towards different vulnerability category in order to identify which class of vulnerability should enjoy preference in the risk mitigation procedure. This paper introduces a model that predicts vulnerabilities that will occur in near future on a local area network (LAN) by using statistical measures and vulnerability history data. Two case studies have also been presented to validate the model.

``Attack plan recognition and prediction using causal networks,"

Correlating and analyzing security alerts is a critical and challenging task in security management. Recently, some techniques have been proposed for security alert correlation. However, these approaches focus more on basic or low-level alert correlation. In this paper, we study how to conduct probabilistic

inference to correlate and analyze attack scenarios. Specifically, we propose an approach to solving the following problems: 1) How to correlate isolated attack scenarios resulted from low-level alert correlation? 2) How to identify attacker's high-level strategies and intentions? 3) How to predict the potential attacks based on observed attack activities? We evaluate our approaches using DARPA's grand challenge problem (GCP) data set. The results demonstrate the capability of our approach in correlating isolated attack scenarios, identifying attack strategies and predicting future attacks.

An incremental decision tree for mining multilabel data,"

Mining with multilabel data is a popular topic in data mining. When performing classification on multilabel data, existing methods using traditional classifiers, such as support vector machines (SVMs), k-nearest neighbor (k-NN), and decision trees, have relatively poor accuracy and efficiency. Motivated by this, we present a new algorithm adaptation method, namely, a decision tree–based method for multilabel classification in domains with large-scale data sets called decision tree for multi-label classification (DTML). We build an incremental decision tree to reduce the learning time and divide the training data and adopt the k-NN classifier at leaves to improve the classification accuracy. Extensive studies show that our algorithm can efficiently learn from multilabel data while maintaining good performance on example-based evaluation metrics compared to nine state-of-the-art multilabel classification methods. Thus, we draw a conclusion that we provide an efficient and effective incremental algorithm adaptation method for multilabel classification especially in domains with large-scale multilabel data.

3.EXISTING SYSTEM

It can be seen that the existing traditional centralized business model of electric power can no longer fully and efficiently meet the business requirements of all intelligent power systems. In this context, the power edge computing model is generated to improve the scene where the centralized model has shortcomings, forming the Power Intelligent CPSS, as shown . AMI means Advanced Metering Infrastructure. Power Intelligent CPSS increases the ability of application task execution and data caching and analysis processing, and migrates some or all of the original centralized business model computing tasks to the converging edge computing terminal node on the edge of the network, so as to reduce the computing load of the master station system.

DISADVANTAGES

- The hidden Markov model shows great value in the analysis of real system, it also has some disadvantages. One of the biggest disadvantages is that the assumption of the model is too simplified.
- However, due to the characteristics of Bayesian networks, if the number of attributes is relatively large or the

correlation between attributes is relatively large, there will be problems.

- However, in many practical problems, especially in network attack environments, the security state of the network is not fixed at different moments, and the transition probability of the state is constantly changing.

4. PROPOSED SYSTEM

Currently, network security prediction is a widely concerned direction in the field of network security, which is the premise and basis for preventing large-scale network attacks. For example, the network situational awareness, proposed by Tim Bass, was used to analyze the network environment, quickly obtain current states, predict future states, and finally provide appropriate responses. Thus, network security risk prediction aims to predict the next state of the network by analyzing the historical states and current states of the network.This paper proposes a status prediction method based on Classification Deep Boltzmann Machine and Markov time-varying Model for the power industrial internet. The method improves efficiency compared with the traditional Boltzmann Machine, and helps with the decision making for active security defense of the electric power control systems.

ADVANTAGES

- SVM has some advantages in solving the problems with small sample, nonlinear and high dimensional features.
- Support vector machine can rely on small samples to learn, which has the advantages of strong generalization ability, easy training, no local minimum and so on.
- SVM has its own unique advantages in solving the problems of small sample, nonlinear and high-dimensional pattern recognition.
- Through the discussion of the above common methods and the comparison of practical application, in order to better serve the Power Intelligent CPSS, the Boltzmann machine and Markov time-varying model are selected.

5.ARCHITECTURE DIAGRAM

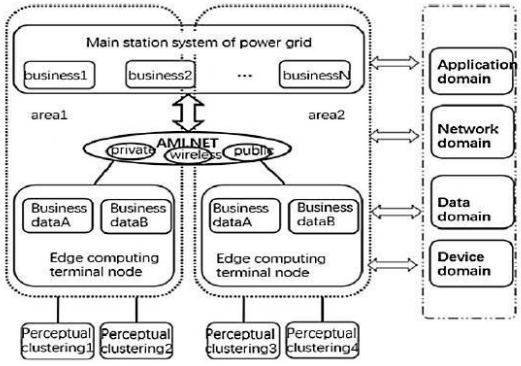

Fig – 1 Architecture Diagram

6. MODULE DESCRIPTION

6.1 Cyber physical social systems:

The Cyber-Physical-Social Systems (CPSS) includes the Cyber-Physical-Systems (CPS), and further incorporates social information and

artificial system information in the virtual space. CPSS extends its research scope to social network systems, which includes systems engineering such as ubiquitous embedded environment perception, dynamic analysis of human organization behaviour, network communication, and network control. CPSS enables physical systems with computing, communication, precise control, remote collaboration, and autonomous functions. The Power Intelligent Internet is a typical Intelligent CPSS.

6.2 Closed loop feedback intelligent system:

The closed-loop feedback intelligent system security architecture of Power Intelligent CPSS has the following modules and functions: First, security resource awareness: Under a single system, it can accurately sense the number and status of various resources such as the platform's own security vulnerability scanning, security status monitoring, malicious behaviour tracking, and security event prevention. In the case of multiple systems, the position, quantity, and status of multiple system security resources can be accurately sensed. The second is the description of the safety task: the safety task can be described in multiple layers using digital methods to form a qualitative and quantitative safety task list. Ability to break complex safety tasks into clear subtasks.

6.3 Network security:

In the field of network security, network security prediction has received much attention recently, which is the premise and basis for preventing the large-scale network attacks. Currently, research in this field is still in its early stage. Although some studies on the prediction of a single intrusion event have already been conducted, they cannot provide effective security risk prediction for the future trend of the entire network in general. Integrated attack is one of the main forms of network intrusion. Accurately predicting it becomes a core task of active defence research.

6.4 Principal component analysis:

In addition, this model adopts the Principal Component Analysis (PCA) method in data sampling classification which can reduce the data dimensionality and computational burden efficiently, but to a hydraulic power generation industrial control network system, the requirements for data rigor and accuracy of results are high and PCA cannot maintains the integrity of the sample. SVM has some advantages in solving the problems with small sample, nonlinear and high dimensional features. Thus, it was used to establish a network security assessment system, which divided the network status into five types. Although five types of network status is not too large, the accuracy of SVM is still not high enough to ensure an accurate prediction of network risks which is more important in the power industrial control systems.

7.RESULTS

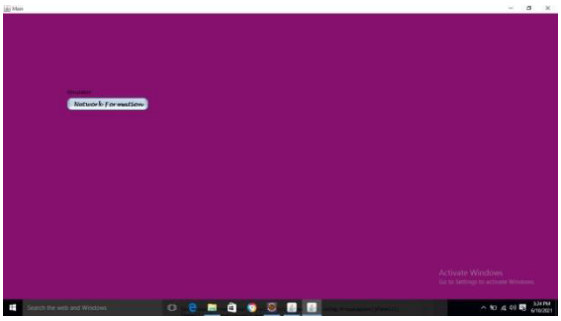

Fig – 2 Simulation network formation

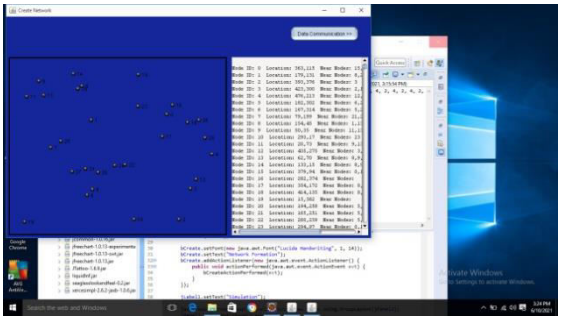

Fig -3 Create network data communication

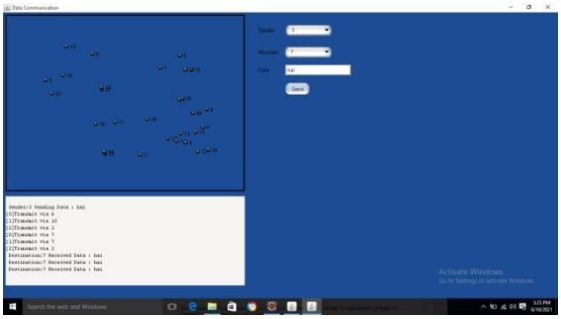

Fig – 4 Data communication sender receiver data creating

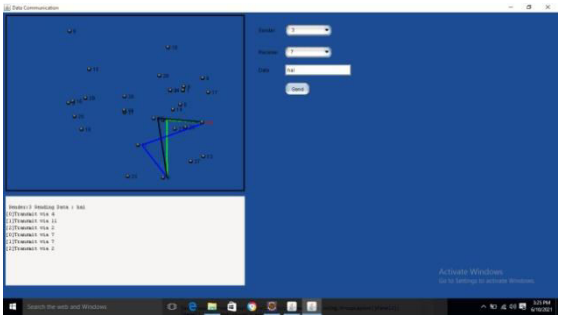

Fig – 5 Data communication transmit via

8. CONCLUSION

Facing the complexity of Power Intelligent CPSS and their network environments, this project proposes a Cloud-Fog- Edge closed-loop feedback security risk prediction model, a Markov model with time varying based on classification Deep Boltzmann machine, for Power Intelligent CPSS systems to predict the network security risk accurately in real time. This model uses a classification Deep Boltzmann machine based on hybrid training to extract the feature and classify the data smartly. It not only adapts the working environment of power industrial control systems, but also solves the defects of the original Markov model with time-varying. Consequently, it outperforms the traditional classification algorithms and inherits the advantages of the Markov model with time-varying.

REFERENCES

[1] G. Zhang and J. Sun, ``A novel network intrusion attempts prediction model based on fuzzy neural network," in Computational Science (Lecture Notes in Computer Science), vol. 3991. Berlin, Germany: Springer, 2006, pp. 419_426.

[2] S. Bhattacharya and S. Ghosh, ``Security threat prediction in a local area network using statistical model," in Proc. IEEE Int. Parallel Distribute. Process. Symp., Mar. 2007, pp. 1_8.

[3] X. Qin and W. Lee, ``Attack plan recognition and prediction using causal

networks," in Proc. 20th Annu. Computer. Security Appl. Conf., Apr. 2005, pp. 370_379.

[4] P. Li, X. Wu, X. Hu, and H. Wang, ``An incremental decision tree for mining multilabel data," Appl. Artif. Intell., vol. 29, no. 10, pp. 992_1014, Nov. 2015.

[5] P. Li, H. Wang, K. Q. Zhu, Z. Wang, X. Hu, and X. Wu, ``A large probabilistic semantic network based approach to compute term similarity," IEEE Trans. Knowl. Data Eng., vol. 27, no. 10, pp. 2604_2617, Oct. 2015.

[6] V. S. Sheng, B. Gu,W. Fang, and J.Wu, ``Cost-sensitive learning for defect escalation," Knowl.-Based Syst., vol. 66, pp. 146_155, Aug. 2014.

[7] V. S. Sheng, ``Studying active learning in the cost-sensitive framework," in Proc. 45th Hawaii Int. Conf. Syst. Sci., Jan. 2012, pp. 1097_1106.

[8] W. Ren, J. X. Hao, and S. TanFeng, ``RBFNN-based prediction of networks security situation," Comput. Eng. Appl., vol. 42, no. 31, pp. 136_138, 2006.

[9] Z. xiang, H. C. Zhen, and L. S. Hang, ``Research on network attack situation forecast technique based on support vector machine," Comput. Eng., vol. 11, pp. 10_12, Nov. 2011, doi: 10.1016/j.cageo.2006.02.011.

[10] L. Jibao, W. Huiqiang, and Z. Liang, ``Study of network security situation awareness model based on simple additive weight and grey theory," in Proc. Int. Conf. Comput. Intell. Secur., vol. 2, Nov. 2006, pp. 1545_1548.