scientific reports

Check for updates

OPEN

A hybrid interpretable deep structure based on adaptive neuro-fuzzy inference system, decision tree, and K-means for intrusion detection

Jia Liu[1,2], Wang Yinchai[1]✉, Teh Chee Siong[3], Xinjin Li[2], Liping Zhao[2,4] & Fengrui Wei[2]

For generating an interpretable deep architecture for identifying deep intrusion patterns, this study proposes an approach that combines ANFIS (Adaptive Network-based Fuzzy Inference System) and DT (Decision Tree) for interpreting the deep pattern of intrusion detection. Meanwhile, for improving the efficiency of training and predicting, Pearson Correlation analysis, standard deviation, and a new adaptive K-means are used to select attributes and make fuzzy interval decisions. The proposed algorithm was trained, validated, and tested on the NSL-KDD (National security lab–knowledge discovery and data mining) dataset. Using 22 attributes that highly related to the target, the performance of the proposed method achieves a 99.86% detection rate and 0.14% false alarm rate on the KDDTrain+ dataset, a 77.46% detection rate on the KDDTest+ dataset, which is better than many classifiers. Besides, the interpretable model can help us demonstrate the complex and overlapped pattern of intrusions and analyze the pattern of various intrusions.

The leading technologies increase the cyber risk for users and businesses. According to *Cisco Annual Internet Report (2018–2023) White Paper*[1], the threat of network intrusions continues to grow. This report illustrated that there was a 776% growth in attacks between 100 and 400 Gbps from 2018 to 2019. And, over half of the operators experienced infrastructure outages. The advance in technologies such as e-commerce, mobile payments, cloud computing, Big Data and analytics, IoT, AI, machine learning, and social media is the main driver of economic growth but has also led to a higher incidence of cyberattacks. As one of the key technologies for ensuring network security, intrusion detection plays a more important role. In the new network environment, new technologies need to be studied to improve the intrusion detection methods.

Because the behaviors of intruders are bound to overlap with that of legitimate users, the overlap between normal behaviors and abnormal behaviors is uncertain, as shown in Fig. 1. Therefore, intrusion detection problems are fuzzy classification problems to some extent. To get better performance on intrusion detection, we need to adapt to the fuzzy characteristic of intrusion detection. Fuzzy logic is a choice. Fuzzy schemes have successfully detected intrusions and malicious behaviors in the presence of uncertain data[2]. A large number of fuzzy approaches have been successfully applied in IDSs (intrusion detection systems). However, in many fuzzy approaches used in intrusion detection, Mohammad Masdari and Hemn Khezri[2] illustrated that the ANFIS classifier is one mostly used classifier.

ANFIS is an algorithm that combines the uncertainty processing ability of fuzzy logic with the learning process of the ANNs (Artificial Neural Networks). ANFIS was first used in IDSs in 2007, in which Toosi and Kahani[3] used five ANFIS modules to explore intrusive activity, which reaching a 95.3% detection rate on the KDDCUP99 dataset. However, ANFIS algorithm has its own disadvantage. It only has five layers, resulting in the disability of identifying deep features. Meanwhile the advantage of ANFIS is also outstanding. It can generate fuzzy and overlapped fuzzy rules and use the parameters learning method like ANNs. Since it only has five layers, which make the architecture of ANFIS is more interpretable than deep ANNs.

[1]Faculty of Computer Science and Technology, University Malaysia Sarawak, 89007 Sarawak, Malaysia. [2]School of Big Data, Weifang Institute of Technology, Weifang 262500, China. [3]Faculty of Cognitive Sciences and Human Development, University Malaysia Sarawak, 89007 Sarawak, Malaysia. [4]College of Control Science and Engineering, China University of Petroleum, Qingdao 266580, China. ✉email: ycwang@unimas.my

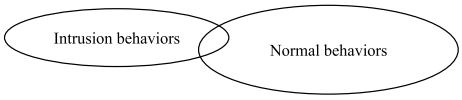

Figure 1. The overlap between intrusion behaviours and normal behaviours.

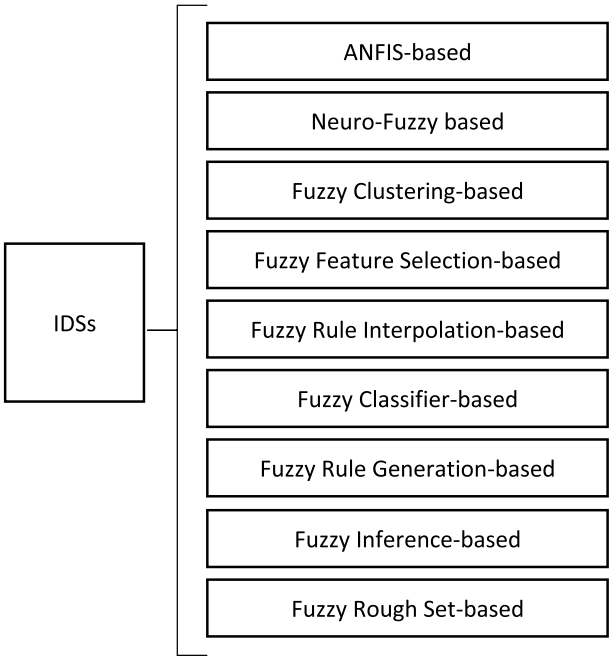

Figure 2. Classification of fuzzy IDSs.

So, for generating a more interpretable and deep structure for IDS, we combine the ANFIS and CART (classification and regression tree) to co-train and identify the deep intrusion patterns. To improve the training and predicting efficiency of the proposed algorithm, we use Pearson Correlation analysis, standard deviation, and a new adaptive K-means are used to select attributes and make fuzzy interval decisions, to minimize the number of fuzzy rules.

Related work

Norbert Wiener, the founder of cybernetics, pointed out that man's superiority over the most perfect machine is that man is capable of using fuzzy concepts. This shows that there is an essential difference between the human brain and the computer. This also shows how important fuzzy logic can be in simulating the human brain and dealing with fuzzy problems.

Fuzzy schemes have successfully detected intrusions and malicious behaviours in the presence of uncertain data[2]. Therefore, a large number of fuzzy approaches have been successfully applied in IDSs. Mohammad Masdari and Hemn Khezri[2] categorized various fuzzy intrusion detection schemes into nine categories, as shown in Fig. 2. They also illustrated that the ANFIS classifier is one mostly used classifier in various misuse detection schemes.

ANFIS algorithm is an algorithm that combines the uncertainty processing ability of fuzzy logic with the learning process of the ANNs. ANFIS was first used in IDSs in 2007. Toosi and Kahani[3] used five ANFIS modules to explore intrusive activity, which reaching a 95.3% detection rate on the KDDCUP99 dataset.

Then, Chan et al.[4] presented a policy-enhanced fuzzy model with ANFIS characteristics. Devi et al.[5] introduced an IDS scheme using ANFIS to detect security attacks on 5G wireless networks.

In combination with other algorithms, Karaboga and Kaya[6] proposed a hybrid artificial bee colony (ABC) algorithm to train ANFIS. This algorithm uses arithmetic crossover to converge quickly r and has better efficiency than the standard ABC algorithm.

Altyeb Altaher presented an IDS scheme EHNFC in[7], which is an evolutionary neuro-fuzzy classifier for malware classification. It can use fuzzy rules to detect fuzzy malware and improve its detection accuracy by learning new fuzzy rules to evolve its structure. In addition, it uses an improved fuzzy rule updating clustering method to update the centroid and radius of the clustering permission feature. These changes to the application of clustering methods improve the convergence of clustering and create rules that adapt to the input data, thereby improving the accuracy.