PLOS ONE

- Published: December 12, 2022
- https://doi.org/10.1371/journal.pone.0278819

On the combination of adaptive neuro-fuzzy inference system and deep residual network for improving detection rates on intrusion detection

- Jia Liu ,
- Wang Yinchai,
- Teh Chee Siong,
- Xinjin Li,
- Liping Zhao,
- Fengrui Wei

Abstract

Deep Residual Networks (ResNets) are prone to overfitting in problems with uncertainty, such as intrusion detection problems. To alleviate this problem, we proposed a method that combines the Adaptive Neuro-fuzzy Inference System (ANFIS) and the ResNet algorithm. This method can make use of the advantages of both the ANFIS and ResNet, and alleviate the overfitting problem of ResNet. Compared with the original ResNet algorithm, the proposed method provides overlapped intervals of continuous attributes and fuzzy rules to ResNet, improving the fuzziness of ResNet. To evaluate the performance of the proposed method, the proposed method is realized and evaluated on the benchmark NSL-KDD dataset. Also, the performance of the proposed method is compared with the original ResNet algorithm and other deep learning-based and ANFIS-based methods. The experimental results demonstrate that the proposed method is better than that of the original ResNet and other existing methods on various metrics, reaching a 98.88% detection rate and 1.11% false alarm rate on the KDDTrain+ dataset.

Citation: Liu J, Yinchai W, Siong TC, Li X, Zhao L, Wei F (2022) On the combination of adaptive neuro-fuzzy inference system and deep residual network for improving detection rates on intrusion detection. PLoS ONE 17(12): e0278819. https://doi.org/10.1371/journal.pone.0278819

Editor: Rahul Gomes, University of Wisconsin-Eau Claire, UNITED STATES
Received: September 14, 2022; **Accepted:** November 25, 2022; **Published:** December 12, 2022

Data Availability: The NSL-KDD dataset used in this study is publicly available from the Canadian Institute for Cybersecurity (CIC) (https://www.unb.ca/cic/datasets/nsl.html).
Funding: This work was supported by the Industry-University-Research Innovation Fund of The Science and Technology Development Center of the Ministry of Education -- collaborative Innovation Project topic “Design and Research of ‘Intelligent’ Education Platform for College Students Based on Big Data and ARTIFICIAL Intelligence technology” 2020QT18.

Competing interests: NO authors have competing interests.

Introduction

Nowadays, leading technologies increase cyber risks for users and businesses. And, according to the *Cisco Annual Internet Report (2018–2023) White Paper* [1], the threat of network intrusions is growing year by year. There was a 776% growth in attacks between 100 Gbps and 400 Gbps from 2018 to 2019. 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 [1]. As one of the key technologies for ensuring network security, intrusion detection plays a more and more important role. However, under the changing network environment, new intrusion detection technologies need to be studied.

Deep learning algorithms bring new probabilities for intrusion detection. Deep learning algorithms can capture highly complex underlying patterns in the data. And, due to the great performance of deep learning in image recognition, various deep learning algorithms have been proposed. And, many of them have been applied in intrusion detection systems (IDSs), like artificial neural networks (ANN) [2], Long Short-Term Memory (LSTM) [3], and Convolutional Neural network (CNN) [4]. However, few studies have successfully applied ResNet to intrusion

detection. This is not only because the structure of ResNet is complex, but also because the ResNet algorithm is prone to overfit on problems with uncertainty, such as IDS problems.

We evaluate the performance of ResNet on the NSL-KDD (National security lab–knowledge discovery and data mining) dataset. Although, ResNet performs very well on image recognition, reaching a 4.92% error rate [5]. And it is considered one important breakthrough to help train deeper networks to recognize deeper patterns. However, when we trained and tested ResNet on intrusion detection's benchmark dataset NSL-KDD dataset (including the KDDTrain+ dataset and KDDTest+ dataset, some intrusion types only exist in the KDDTest+ dataset), the evaluating results shows a serious overfitting problem of ResNet on this dataset, as shown in Fig 1. Actually, Y. Xiao and X. Xiao [6] once pointed out that ResNet is prone to overfitting for low-dimensional and small-scale datasets, resulting in reduced generalization ability of the model, in 2019. And we think this is one of the reasons, the other reason is that the ResNet is easy to overfit on problems with uncertainty due to the too-detailed classification of ResNet. However, intrusion detection problems are fuzzy classification problems as shown in Fig 2. Thus, to address this problem, we improve the ResNet with fuzzy logic in this study and propose a new architecture for intrusion detection problems. The contributions of this study can be summarized below: