JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH

E-ISSN: 2980-9231
https://jce.bushehr.iau.ir

https://doi.org/10.30495/jce.2023.1992146.1215

Vol. 14/ No. 53/Autumn 2024

Research Article

# A Distributed Denial-of-Service (DDoS) Attack Detection Approach in Fog Layer Based on Distributed Blockchain Database and Machine Learning

Mohsen Eghbali, PhD Student [1] | Mohammad Reza Mollhoseini Ardakani, Assistant Professor[2*]

[1]Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran, m.eghbali@maybofiau.ac.ir

[2]Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran, mr.mollahoseini@iau.ac.ir

**Correspondence**
Mohammadreza Mollahoseini Ardakani, Associate Professor, Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran,
mr.mollahoseini@iau.ac.ir

**Received:** 24 July 2023
**Revised:** 27 August 2023
**Accepted:** 13 September 2023

## Abstract

DDoS attacks make network services unavailable to users by sending fake traffic by botnets. One of the methods to deal with DDoS attacks is to use machine learning, but these methods face challenges such as high volume of IoT traffic and data imbalance. This paper introduces a distributed intrusion detection system in the fog layer that detects network attack traffic in a decentralized manner. In this method, each fog node acts as an intrusion detection system, and by exchanging blacklists through the blockchain, they increase the secrecy of detecting attacks. Fog nodes identify the main features of network traffic using the Coati optimization algorithm and use these features to train a multilayer neural network in intrusion detection. The selection of features reduces traffic and increases the accuracy and speed of attack detection. Based on game theory, the GAN method is used to balance network traffic. Tests performed in MATLAB and on the NSL-KDD show that the proposed system has accuracy, sensitivity, and precision of 98.67%, 98.52%, and 98.34%, respectively. This method is more accurate in identifying network attacks than feature selection methods such as WOA, GWO, and HHO and more accurate than LSTM and CNN.

**Keywords**: The intrusion detection system, Fog layer, Machine learning, GAN neural network, Feature selection, Coati Optimization Algorithm (COA).

## Highlights

- Network traffic balancing in the fog layer with the game theory based on the GAN network.
- Presenting a binary version of the Kuati optimization algorithm presented in 2023 for feature selection.
- Maintaining the confidentiality of the proposed intrusion detection system with blockchain and exchanging the blacklist with blockchain between fog nodes.
- Providing a distributed intrusion detection system in the fog layer to detect attacks on IoT.

**Citation:** M. Eghbali, and M.R. Mollhoseini Ardakani “A Distributed Denial-of-Service (DDoS) Attack Detection Approach in Fog Layer Based on Distributed Blockchain Database and Machine Learning,” *Journal of Southern Communication Engineering*, vol. 14, no. 53, pp. 67–90, 2024, doi:10.30495/jce.2023.1992146.1215, [in Persian].

## 1. Introduction

Due to the rapid development of Internet of Things technology, more applications such as smart homes, smart cities, smart transportation, smart logistics management, etc. have become more regular in this industry [1]. In this regard, distributed denial of service (DDoS) attack is considered one of the serious security threats [2]. As a result, it is critical to develop a security measure to continuously and immediately learn and detect attacks such as DoS in IoT networks. Signature-based intrusion detection systems and anomaly-based intrusion detection systems are prominent as security solutions to reduce attacks and penetration into the Internet of Things network. In this study, an efficient distributed intrusion detection system is deployed in the fog layer. As a result, a large amount of network traffic is evaluated and analyzed in real-time.

Below, related works in the field of detecting attacks, especially DDoS, are reviewed. Subsequently, an overview of intrusion detection systems based on machine learning methods is provided. In [3], a network intrusion detection system was presented to detect DDoS attacks using deep autoencoders. In this study, a network intrusion detection system architecture based on a deep autoencoder trained on network stream data is proposed. The advantage of the proposed system is that there is no need for prior knowledge about the network topology or its underlying architecture. Experimental results show that the proposed model can detect anomalies caused by DDoS attacks with a high detection rate and negligible false alarms. In [4], a DDoS intrusion detection system based on the combination of CNN and LSTM was proposed. In this study, a new deep learning classification method was introduced through the combination of two common deep learning algorithms, namely convolutional neural networks and long short-term memory. The NSL-KDD dataset is used to test the model. This architecture consists of seven layers to achieve higher performance compared to traditional CNN and LSTM. The proposed model with an accuracy of 99.20% is considered to be the most efficient model compared to previous works.

In [5], an efficient network intrusion detection model for the Internet of Things security using a K-NN classifier was presented. In this study, principal component analysis, univariate statistical tests, and genetic algorithms were used separately to select features and improve data quality. The Bot-IoT dataset was used to evaluate the method. The experimental results showed that the application of feature selection led to the reduction of training time from 22.51182 seconds to less than one minute. In [6], a dynamic feature selection technique was presented for DDoS attack detection. In order to select effective features, a voting-based hybrid feature selection technique was applied. The hybrid method not only reduces the dimensions of the features and the redundancy rate but also extracts the relevant features for classification. The experimental results showed that multilayer perceptron with genetic algorithm (MLP-GA) as a classifier with an accuracy of 98.8%, false positive rate of 0.6%, and early detection capability has a better performance than conventional classifiers.

## 2. Innovation and contributions

The advantage of the proposed method over other intrusion detection systems is the implementation of a distributed architecture in the fog layer. Unlike the centralized architecture, the distributed architecture uses multiple intrusion detection systems simultaneously and analyzes large volumes of network traffic. Due to the decentralized architecture, when an intrusion detection system in the fog layer is attacked by DDoS, other fog nodes are still able to detect intrusion attacks. Another important advantage of the proposed intrusion detection system is balancing the training traffic with new techniques such as game theory, which in turn increases the accuracy of the proposed model. Also, the proposed method selects the important features of the network traffic with a swarm intelligence based on the behavior of Coati presented in 2023 and reduces the dimensions of the network traffic based on the extracted features. Minimizing the dimensions of traffic in the fog layer enhances the learning speed and attack detection speed. Among the innovations of this paper, the following can be stated:

This article is organized into five sections. In the second section, a literature review and related work in the field of network attack detection are presented. In the third section, the proposed intrusion detection system is presented based on game theory, GAN neural network, and Coati optimization algorithm, and blockchain. The proposed method is implemented and analyzed in the fourth section. Finally, the results and findings of the research are presented in the fifth section.

## 3. Materials and Methods

An intrusion detection system based in the fog layer is presented in the form of the proposed method. According to the presented framework, the network traffic is initially fed to the fog layer as an input. To increase the accuracy of machine learning models, it is desirable to normalize the lower and upper bounds of all features of the data set in the range [a,b]. Then the network traffic is balanced by the GAN deep learning method. The GAN network is a neural network based on game theory, including two separate parts, the generator and the discriminator. Based on noisy and random information and data and their impact on real data, the generator tries to produce synthesis and fake data. The generator wins if the tricked discriminator treats the fake data as real data.

Subsequently, the binary version of the Coati algorithm is used to select features in the fog layer. Transformation functions such as S and V are used to binarize solutions or feature vectors in the Coati optimization algorithm. Transformation functions convert the continuous space into a discrete and binary space.

Important features are fed as inputs to the multilayer neural network. The artificial neural network classifies network traffic into two distinct categories, attack and normal. Then each fog node updates its blacklist. The blacklist is exchanged between fog nodes with the blockchain so that attackers cannot manipulate the blacklists. Nodes periodically exchange their blacklist every 10 minutes. Reducing the desired time increases the overhead of sending and receiving messages in the fog layer. To transfer and share the blacklist in the blockchain, fog nodes use the following steps.

- The fog node inserts its blacklist in the data part of a block.
- The node sends the block to other fog nodes.
- Fog nodes authenticate the sending node. If all nodes reach a consensus about the authenticity of the fog node, the blacklist is added to the blockchain.

- A copy of the blockchain including the shared blacklist is sent to all nodes.

Finally, the trained model is evaluated using test data and compared with similar methods regarding accuracy and sensitivity.

## 4. Results and Discussion

According to the experimental results, without balancing the data set and feature selection, the accuracy, sensitivity, and precision of the proposed method for intrusion detection are equal to 89.65%, 88.34%, and 87.64%, respectively. The combination of the Coati optimization algorithm and artificial neural network without balancing the dataset leads to accuracy, sensitivity, and precision equal to 92.63%, 91.58%, and 91.82%, respectively. In the case of balancing the data set with GAN deep learning and feature selection with the Coati optimization algorithm in the fog layer, the accuracy, sensitivity, and precision of the proposed method are 98.67%, 98.2%, and 98.34%, respectively.

The experiments performed in MATLAB and comparisons proved that the proposed method has more accuracy, sensitivity, and precision compared to the wall optimization algorithm (WOA), gray wolf optimization (GWO), Harris hawks optimization (HHO), and spotted hyena optimizer (SHO). The greater accuracy of the proposed method compared to the peer meta-heuristic algorithms is a trade-off between exploration and exploitation and a better search of the feature space to find the optimal features. The number of selected features for detecting attacks in GTO-BSA, GTO, BSA, HGS, MVO, HHO, and PSO methods is 14.75, 18.5, 21.13, 18.62, 16.50, 19.62, and 14/87, respectively. At the same time, the average number of features extracted in the experiments is equal to 13.62. This means that the proposed method has reduced the dimensions of the feature space by 66.78%.

The evaluations show that the accuracy of the proposed method is higher compared to AE-CNN, LSTM, and LSTM-RNN. Also, AE-CNN, LSTM, and LSTM-RNN deep learning methods for detecting attacks achieved 99.93%, 94.11%, and 96.96% accuracy, respectively, which is lower than the accuracy of the proposed method. The reason for the superiority of the proposed method in detecting attacks is the balancing of the dataset and intelligent feature selection. Also, due to the use of blockchain, the proposed method has a high authentication capability and guarantees the security of the exchanged blacklist.

## 5. Conclusion

The experimental results on the NSL-KDD dataset proved that the proposed method is more accurate than conventional meta-heuristic feature selection methods such as WOA, GWO, SHO, and HHO. Also, compared to learning methods such as LSTM and CNN, the proposed method is more capable and accurate in detecting attacks. The advantages of the proposed method are the accuracy of the selection of features and the reduction of network traffic dimensions compared to peer meta-heuristic methods. Also, superior detection accuracy compared to deep learning methods is one of the prominent advantages of the proposed method.

## 6. Acknowledgement

I would like to thank for the sincere support of Dr. Mohammad Reza Mollhoseini Ardakani, Assistant Professor of Meybod Islamic Azad University.

## 7. References

[1] Z. Shah, I. Ullah, H. Li, A. Levula and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031094.

[2] N. Elsayed, Z. ElSayed and M. Bayoumi, "IoT Botnet Detection Using an Economic Deep Learning Model," *IEEE World AI IoT Congress (AIIoT), Seattle*, WA, USA, 2023, pp. 0134-0142, doi: 10.1109/AIIoT58121.2023.10174322.

[3] I. Ortega-Fernandez, M. Sestelo, J. C. Burguillo and C. Pinon-Blanco, "Network intrusion detection system for DDoS attacks in ICS using deep autoencoders," *Wireless Networks*, vol. 30, pp. 5059-5075, 2023, doi: 10.1007/s11276-022-03214-3.

[4] A. S. A. Issa and Z. Albayrak, "Ddos attack intrusion detection system based on hybridization of cnn and lstm. Acta Polytechnica Hungarica," *Acta Polytechnica Hungarica*, vol. 20, no. 3, pp. 1-19, 2023, doi: 10.12700/APH.20.3.2023.3.6.

[5] M. Mohy-eddine, A. Guezzaz, S. Benkirane and M. Azrour, "An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 23615–23633, 2023, doi: 10.1007/s11042-023-14795-2.

[6] U. S. Chanu, K. J. Singh and Y. J. Chanu, "A dynamic feature selection technique to detect DDoS attack," *Journal of Information Security and Applications*, vol. 74, p. 103445, May 2023, doi: 10.1016/j.jisa.2023.103445.

## Appendix

**Table 1.** Summary of reviewed studies in the field of network attack detection

| Research | Method | Advantage | Defect |
|---|---|---|---|
| In [3], 2023 | Network intrusion detection for DDoS attacks using deep autoencryptors | High detection rate and low false alarms | Not applying feature selection and not balancing the data set |
| In [32], 2023 | Different types of classifiers to detect attacks | Using two data sets | Lack of distributed architecture to detect attacks in real time |
| In [34], 2023 | Random forest algorithm for feature selection | More accuracy than Bayesian network, support vector machine and logistic regression | Imbalance of dataset and centralized architecture of intrusion detection system |
| In [35], 2023 | A kernel-based RBF-SVM model for attack detection | More accuracy than vector machine algorithm | It requires a lot of training data |
| In [36], 2023 | Fast R-CNN and gradient methods to detect attacks | More accuracy than convolutional neural network | High complexity |
| In [37], 2023 | A kernel-based RBF-SVM model for attack detection | Accuracy over 98% | Poor comparisons and unbalanced data sets |
| In [38], 2023 | BPN neural network using particle optimization algorithm | The accuracy of their method is 96.5% | Using the old data set |
| In [39], 2023 | To optimize the weight of LSTM neural network with PSO algorithm | More accurate than LSTM | Only IP related properties are checked. |
| In [40], 2023 | Adaptive fuzzy neural inference in seizure detection | It has better performance than similar neural networks | Their certainty is not high |
| In [48], 2023 | Network penetration detection based on multilayer artificial neural network and feature selection with random forest and IG method | Reducing network traffic dimensions from 41 features to 23 features | Average accuracy |
| In [49], 2023 | K-NN classifier | Reduce training time | The nearest neighbor method is not very intelligent |
| In [50], 2023 | Filter feature selection techniques | The ability to detect web attacks on the network | Average precision and imbalance of the data set |
| In [51], 2023 | Improved African vulture optimization algorithm in attack detection | Analysis on two data sets | The high complexity of the Vulture algorithm and the imbalance of the data set |
| In [6], 2023 | Dynamic feature selection technique for attack detection | Accuracy 98.8% | The combination of genetic algorithm and neural network increases the training time |
| In [53], 2022 | Combination of CNN and LSTM neural network in cloud layer attack detection | More accuracy than CNN and LSTM neural network | High computational complexity |
| In [54], 2022 | Identification of multivariate outliers and selection of ReliefF feature in attack detection | Detect sophisticated attacks | Lack of distributed architecture and lack of data set balancing |
| In [55], 2021 | Feature selection based on PCA and random tree | More accurate than random tree | Failure to recognize effective features in attacks |

**Table 2.** Index of accuracy, sensitivity and accuracy in detecting network attacks

| Mode | Exact | Sensitivity | accuracy |
|---|---|---|---|
| MLP | 89.65 | 88.34 | 87.64 |
| COA+MLP | 92.63 | 91.58 | 91.82 |
| GAN+COA+MLP(GCM) or Proposed Method | 98.67 | 98.52 | 98.34 |

**Declaration of Competing Interest:** Authors do not have conflict of interest. The content of the paper is approved by the authors.

**Publisher's Note:** All content expressed in this article is solely that of the authors, and does not necessarily reflect the views of their affiliated organizations or the publisher, editors, and reviewers. Any content or product that may be reviewed and evaluated in this article is not guaranteed or endorsed by the publisher.

**Author Contributions:** All authors reviewed the manuscript.

**Open Access:** Journal of Southern Communication Engineering is an open access journal. All papers are immediately available to read and reuse upon publication.