ScienceDirect

Materials Today: Proceedings

Volume 80, Part 3, 2023, Pages 3086-3091

Deep learning binary fruit fly algorithm for identifying SYN flood attack from TCP/IP

Vankayalapati Nagaraju, Arun Raaza, V. Rajendran, D. Ravikumar

Show more

Share Cite

https://doi.org/10.1016/j.matpr.2021.07.171

Get rights and content

Referred to by 5 Nano 2021 – Expression OF CONCERN – PART 3
Materials Today: Proceedings, Volume 80, Part 3, 2023, Pages 1703
View PDF

Abstract

SYN Flood Attack is one form of distributed denial of service attack that attains the handshake process of TCP. This attack consumes all available server resources and provokes legitimate traffic which aims to make the server unavailable. It causes serious damage to cloud server and networking protocols. The main objective of this research work is to train the neural network for detecting the attack and to secure network connection. A novel binary fruit fly optimization algorithm with deep learning is proposed to predict the syn flood attack. The proposed algorithm is implemented using the KDD cup dataset. DL- BFFA algorithm has achieved 99.96% detection accuracy for detecting the SYN Flood Attack. A comparison study is conducted to validate the proposed model.

Introduction

Nowadays the internet offers online banking, e-commerce, and education services online. SYN flood attack is a type of cyber threat that can affect the internet services such as email, online accounting, and public networking. This attack occurs, and then the users aren't able to access network resources, devices, and information systems. SYN flood attack is a method to create a connection between the client and server in a transmission control protocol TCP/IP network. It can occupy the available connections in the port and leaves an incomplete handshake. The send request will be continued by an attacker until all open ports are saturated with their requests. It has denied the connection to the legitimate users in the network. In the big data field, this type of attack is increased due to political, e-commercial, and personal reasons. The main target of this attack is to harm web-based applications, media, and software industries. The schematic example of an SYN flood attack on the network is shown in Fig. 1.

In 1994, SYN flood attacks were discovered by Bill Cheswick and Steve Bellovin. CERT published an article for mitigating SYN flood attacks [1]. It is very crucial for secure communication in the network. The traditional approaches are mainly focused on manual recognition and statistical analysis. New techniques are based on data mining, machine learning, and neural networking. Entropy-based lightweight DDOS flood attack detection model has achieved fine anomaly detection accuracy [2]. In a network security system, a software-defined network (SDN) is deployed using programming languages such as java and python with security functionality methods [3], [4], [5]. A TCP connection initiated using a three-way handshake technique has led to vulnerability to the attack [6]. In 2018, Kaspersky has revealed that 50% of the cyber attack is based on the TCP SYN attack only [7].

Most of the research work focuses on the detection approaches are based on offline analysis and simulation methods such as patterns during normal and attack states, network traffic characteristics. Due to this limitation, the authors propose a deep learning-based model to predict the SYN flood attack in real-time. The main contribution of this is as follows.

- A novel binary fruit fly optimization algorithm with deep learning is proposed to predict the syn flood attack.
- Train the neural network model for detecting the attack to secure network connection.

This research paper is organized as follows: Section 2 addresses the detection and mitigation solution for SYN flood attacks. Section 3 discusses the data collection and feature selection techniques. The proposed BFFA model implementation details are described in section 4. The performance analysis and the results are presented in section 5. Section 6 concludes the model and future work to carry out the reproductively of the model [23], [24], [25].

Section snippets

Related work

Many researchers have produced solutions for DDOS detection using static-based and machine learning-based approaches. The authors have proposed a novel deep learning model combined with the optimization algorithm to detect the SYN flood attack. Research works related to the statistical and machine learning models are discussed as follows:

Proposed methodology

The proposed Binary Fruit Fly Algorithm (BFFA) with deep learning model analyses the syn flood attacks and the network traffic. This model comprises data collection, feature extraction, input layer, dense layer, and output layer. Fig. 2, Depicts the architecture of the BFFA model to detect the attacks in the network.

Experimental results and discussion

The BFFA model is implemented using a python programming language. The packages such as NumPy, sklearn, pickle, tqdm, pandas, sea born and matplotlib are used to implement the model. It is carried out by the two datasets KDD cup. This dataset has 41 features and is grouped into three categories such as content, traffic, and intrinsic features. The model performance is evaluated using accuracy metrics.$Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$ where,

True-positive (TP)=Number of data correctly predicts an attack.

Evaluation metrics

The proposed model is evaluated using a confusion matrix. It is a n*n matrix where n is the number of the actual classes. This matrix compares the actual class to the predicted class by using the deep learning model. Each column represents the actual value of the class and rows are related to the predicted class of the data. The validation size of the data is 5469. Fig. 6. Show the confusion matrix for the BFFA model. This model correctly predicts the attacks on 5466 data and only three data

Comparison of the proposed model

The authors of [20], [21], [22] proposed a deep learning model to detect the DDoS attack using a recurrent neural network classifier. This model has achieved an error rate of 2.1% for detecting the attacks. This classifier was used to trace the network attack activities and the sequences of the network traffic. Our proposed BFFA model improves 3.5% detection accuracy as compared to the existing classifier model. The revised feature extraction technique is used to extract important features to

Conclusion

In DDoS attack detection, the deep learning-based classifier produces better accuracy and less prediction time as compared to other deep learning algorithms. This algorithm can able to handle different kinds of attacks in the network system. In this research work, the authors presented a novel BFFA algorithm by utilizing the swarm intelligence approach for optimal parameter findings. The neural network parameters are tuned by using the optimal metric values. Conventional deep learning models

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Special issue articles Recommended articles

References (25)

R. Sridhar *et al.*
Design and development of material behavior of line follower automated vehicle
Mater. Today: Proceedings (2021)

N.K. Chandramohan *et al.*
Comparison of chassis frame design of Go-Kart vehicle powered by internal combustion engine and electric motor
Mater. Today: Proceedings (2021)

A. Shiravi *et al.*
Toward developing a systematic approach to generate benchmark datasets for intrusion detection
Computers Security (2012)

X. Yu *et al.*
Design of DDoS attack detection system based on intelligent bee colony algorithm
Int. J. Comput. Sci. Eng. (2019)

S. Saravanakumar *et al.*
The static structural analysis of torque converter material for better performance by changing the stator angle
Mater. Today: Proceedings (2021)

C.C. Center, Cert advisory ca-1996-21 TCP SYN flooding and IP spoofing attacks,...

R. Wang, Z. Jia, L. Ju, An entropy-based distributed DDOS detection mechanism in software-defined networking in Trust...

A. Sangodoyin, B. Modu, I. Awan, J. Pagna Disso, An approach to detecting distributed denial of service attacks in...

L. Barki, A. Shidling, N. Meti, D.G. Narayan, M.M. Mulla, Detection of distributed denial of service attacks in...

S. Hameed *et al.*
SDN Based collaborative scheme for mitigation of DDoS attacks
Future Internet (2018)

View more references

Cited by (2)

Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches

2024, Egyptian Informatics Journal

Show abstract

A SYN Flood Attack Detection Method Based on Hierarchical Multihead Self-Attention Mechanism ↗

2022, Security and Communication Networks

View full text