IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

Deep Learning Based Efficient Network Anomaly Detection Model using BAT-MC

Geetha Nandini Velugubantla[1] and Dr. M. Radhika Mani[2]
Department of Computer Science and Engineering[1]
Professor & HOD, Department of Computer Science and Engineering[2]
Pragati Engineering College, Surampalem, AP, India

Abstract: *Intrusion detection can identify unknown attacks from network traffics and has been an effective means of network security. Nowadays, existing methods for network anomaly detection are usually based on traditional machine learning models, such as KNN, SVM, etc. Although these methods can obtain some outstanding features, they get a relatively low accuracy and rely heavily on manual design of traffic features, which has been obsolete in the age of big data. To solve the problems of low accuracy and feature engineering in intrusion detection, a traffic anomaly detection model BAT is proposed. The BAT model combines BLSTM (Bidirectional Long Short-term memory) and attention mechanism.*

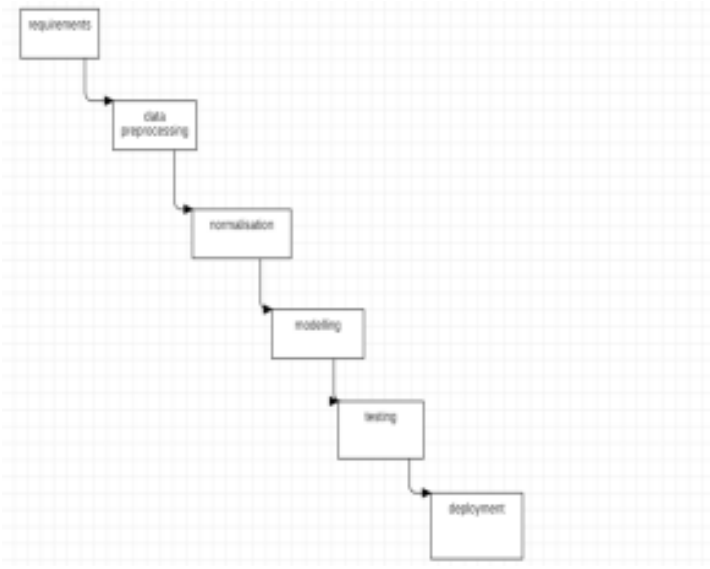
Keywords: BLSTM (Bidirectional Long Short-term memory), DoS (Denial of Service attacks), R2L (Root to Local attacks), U2R (User to Root attack) and Probe (Probing attacks).

I. INTRODUCTION

A deep learning model BAT-MC that mainly combines bidirectional long-term memory (BLSTM) and attention mechanism. BLSTM is used to learn the characteristics of each packet and get the vector corresponding to each packet. The use of Self-taught Learning (STL) on NSL-KDD dataset for network intrusion. It proposes an intrusion detection method using deep belief network (DBN) and probabilistic neural network (PNN).

II. MODEL DIAGRAM

By making full use of the structure information of network traffic, the BAT-MC model can capture features more comprehensively. Evaluate our proposed network with a real NSL-KDD dataset.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

A Survey: Intrusion Detection Techniques for Internet of Things
Authors: Sarika Choudhary and Nishtha Kesswani
The latest buzzword in internet technology now a days is the Internet of Things. The Internet of Things (IoT) is an ever-growing network which will transform real-world objects into smart or intelligent virtual objects.This research article focuses on IoT introduction, architecture, technologies, attacks and IDS

Network Intrusion Detection
Authors: B. Mukherjee, L.T. Heberlein and K.N. Levitt
Intrusion detection is a new, retrofit approach for providing a sense of security in existing computers and data networks, while allowing them to operate in their current "open" mode.

Survey on SDN Based Network Intrusion Detection using Machine Learning Approach
Authors: N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad
Software Defined Networking Technology (SDN) provides a prospect to effectively detect and monitor network security problems ascribing to the emergence of the programmable features. Recently, Machine Learning (ML) approaches have been implemented in the
SDN-based Network Intrusion Detection Systems (NIDS).

Network Intrusion Detection System: A Machine Learning Approach
Authors: Mrutyunjaya Panda, Ajith Abraham, Swagatam Das and Manas Ranjan Patra
Intrusion detection systems (IDSs) are currently drawing a great amount of interest as a key part of system defense. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network.

III. SYSTEM ANALYSIS

3.1 Existing System

Machine learning methods have been widely used in intrusion detection to identify malicious traffic.It proposes a new method of feature selection and classification based on support vector machine (SVM). Experimental results on NSL-KDD cup 99 of intrusion detection data set showed that the classification
accuracy of this method with all training features reached 99%. Combination k-mean clustering on the basis of KNN classifier. The experimental results on NSL-KDD dataset show that this method greatly improves the performance of KNN classifier.

A. Disadvantages

- Low Accuracy
- False Positive Rate

3.2 Problem Statement

The problem statement is to identify various malicious network traffics, especially unexpected malicious in network traffics. To solve the problems in network intrusion detection, a traffic anomaly detection model BAT is proposed.

3.3 Proposed System

The accuracy of the BAT-MC network can reach 84.25%, which is about 4.12% and 2.96% higher than the existing CNN and RNN model, respectively.

- It proposes an end-to-end deep learning model BAT-MC that is composed of BLSTM and attention mechanism.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

- The introduce the attention mechanism into the BLSTM model to highlight the key input. Attention mechanism conducts feature learning on sequential data composed of data package vectors.

A. Advantages

- Better Performance
- High Accuracy

IV. SYSTEM REQUIREMENTS SPECIFICATION

4.1 Functional Requirements

A. Benchmark Datasets

The NSL-KDD dataset is mainly composed of KDDTrain+ training dataset,KDDTest+ and KDDTest-21 testing dataset, which can make a reasonable comparison with different methods of the experimental results. The NSL-KDD dataset have different normal records and four different types of abnormal records. The KDDTest-21 dataset is a subset of the KDDTest+ and is more difficult for classification.

B. Evaluation Metric

Accuracy (A) is used to evaluate the BAT-MC model. Except for accuracy, false positive rate (TPR) and false positive rate (FPR) are also introduced.. True Negative (NP) represents a normal user classified correctly. False Negative (FN) represents an instance where the intruder is incorrectly classified as a normal user.

C. Experimental Settings

In order to test the performance of BAT-MC model proposed, NSL-KDD dataset is used for verification. The data samples of the NSL-KDD dataset are divided into two parts: one is used to build a classifier, that is called the training dataset.

4.2 Non-Functional Requirements

A. Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. Three key considerations involved in the feasibility analysis are

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

V. SYSTEM DESIGN

5.1 System Specifications

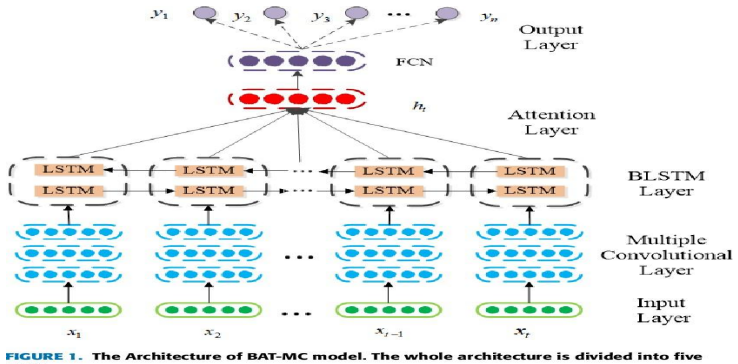


FIGURE 1. The Architecture of BAT-MC model. The whole architecture is divided into five parts.

Figure: Architecture for BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

5.2 Data Preprocessing Layer

There are three symbolic data types in NSL-KDD data features: protocol type, flag and service. We use one-hot encoder mapping these features into binary vectors. One-Hot Processing: NSL-KDD dataset is processed by one-hot method to transform symbolic features into numerical features.

5.3 Testing Strategies

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product.

A. Types of Testing

- Unit testing: Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration.
- Integration testing: Integration testing is specifically aimed at exposing the problems that arise from the combination of components.
- White Box testing: It is used to test areas that cannot be reached from a black box level.
- Black Box testing: Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested.
- Unit testing: Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.
- Test Results: All the test cases mentioned above passed successfully. No defects encountered.
- Acceptance Testing: User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.
- Test Results: All the test cases mentioned above passed successfully. No defects encountered.

VI. RESULTS AND DISCUSSION

Epoch Values of GRU: Again, after the LSTM () is performed. The GRU analysis is done where 5 epochs are considered where the accuracy increases after each epoch and the loss decreases after each epoch.

VII. CONCLUSION

The current deep learning methods in the network traffic classification research don't make full use of the network traffic structured information. Drawing on the application methods of deep learning in the field of natural language processing, it proposes a novel model BAT-MC via the two phases learning of BLSTM and attention on the time series features for intrusion detection using NSL-KDD dataset. BLSTM layer which connects the forward LSTM and the backward LSTM is used to extract features on the traffic bytes of each packet. Each data packet can produce a packet vector. These packet vectors are arranged to form a network flow vector.

Attention layer is used to perform feature learning on the network flow vector composed of packet vectors. Performance of the BAT-MC method is tested by KDDTest+ and KDDTest-21 dataset. Experimental results on the NSL-KDD dataset indicate that the BAT-MC model achieves pretty high accuracy. By comparing with some standard classifier, these comparisons show that BAT-MC models results are very promising when compared to other current deep learning-based methods. Hence, it believes that the proposed method is a powerful tool for the intrusion detection problem.

REFERENCES

[1]. B. B. Zarpelo, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ''A survey of intrusion detection in Internet of Things, ''J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

[2]. B. Mukherjee, L. T. Heberlein, and K. N. Levitt, ‘‘Network intrusion detection,’’ IEEE Netw., vol. 8, no. 3, pp. 26–41, May 1994.

[3]. S. Kishorwagh, V. K. Pachghare, and S. R. Kolhe, ‘‘Survey on intrusion detection system using machine learning techniques,’’ Int. J. Control Automat., vol. 78, no. 16, pp. 30–37, Sep. 2013.

[4]. N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, ‘‘Survey on SDN based network intrusion detection system using machine learning approaches,’’ Peer-to-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Mar. 2019.