Classification Of Network Intrusion Detection System Using Recurrent Neural Networks

Velvizhi G[1], Shiyam kumarV[2], Naveen kumar C[3], Sathish kumar S[4]
[1]Assistant Professor
[2, 3, 4]Dept of Computer Science And Engineering and Technology
[1, 2, 3, 4]RAAK College of Engineering and Technology, Puducherry, Pin-605010, India

Abstract- *A Network Intrusion Detection System (NIDS) is a key technology in network security that detects packets of malicious or unwanted abnormal activity occurring in the network. These network intrusion detection systems have been studied together with machine learning and deep learning, but performance is not guaranteed in the actual environment, or the class balance problem has not been solved. In existing system, the performance of a discretization pre-processing method with a CNN-based classifier on the class imbalance problem of network traffic data has been investigated. The pre-processing method adds a discretization algorithm for continuous variables is the commonly used conventional pre-processing method. In proposed system, the project is expected to show better results by implementing Recurrent Neural Networks (RNN)*

Keywords- intrusion detection, deep learning, CNN techniques,RNN techniques.

I. INTRODUCTION

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered. While anomaly detection and reporting are the primary functions of IDS, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious Internet Protocol (IP) addresses [1]. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms [2]. IDS's can be detected suspicious activities using different methods, including the following

II. EXISITING WORK

Discrete Pre-processing Method and NIDS using Convolution Neural Network were proposed in existing system to solve the problems occurring in the learning-based NIDS. A Convolutional Neural Network (CNN) is a transformed neural network that uses convolution and aims to learn the feature representation of data. The basic layer structure of a CNN consists of a convolutional layer and a pooling layer, and various outputs such as classification and distance calculations between features can be used with a fully connected layer.

Discrete pre-processing

The discretization algorithm proceeds in two directions. First, it is the direction of discretization pre-processing only for the discrete features. Unlike pre-processing without discretization, instead of using a Min-Max scale for discrete features, the KBinDiscretise algorithm is used to change 22 properties to 80 properties by performing binning at regular intervals. Second, it is the direction of discretization pre-processing in continuous and discrete features. In the same way as 2), binning is performed at regular intervals through the KB InDiscretise algorithm. 32 features of NSL-KDD data are changed to 100 features, and in the case of CSE-CIC-IDS 2018 data, 60 features are changed to 350 features. Binary and categorical functions proceed the same as in the previous pre-processing method [8]

Convolutional neural network

A Convolutional Neural Network (CNN) is a transformed neural network that uses convolution and aims to learn the feature representation of data, it has the following differences compared to a DNN, which is the most basic neural network used for deep learning. The basic layer structure of a CNN consists of a convolutional layer and a pooling layer, and various outputs such as classification and distance calculations between features can be used with a fully connected layer depending on the purpose of the learning. The pooling layer reduces the parameters connected between the convolutional layers, thereby reducing the amount of computation and improving the acceptance field of the subsequent convolutional layers [8]

III. PROPOSED WORK

A recurrent neural network (RNN) is a class of artificial neural networks where connections between nodes can create a cycle, allowing output from some nodes to affect subsequent input to the same nodes. Recurrent Neural Networks enable you to model time-dependent and sequential data problems, like stock exchange prediction, artificial intelligence and text generation. Models under the Recurrent Neural Network are:

- Long Short Term Memory (LSTM)
- Gated Recurrent Unit (GRU)

Long short term memory

Long Short Term Memory (LSTM) is a kind of recurrent neural network (RNN) design applied in deep learningfield. LSTM has feedback connection that is unrelated to standard feed forward neural networks. It cannot only process sole data points but also entire sequences of information. LSTM unit consists of a cell, an input gate, an output gate and a forget gate. The cell recollects values over arbitrary time breaks and therefore the three gates control the data flow into and out of the cell. LSTM networks are compatible for categorizing, handling and producing guesses supported statistic data, subsequently there are often delays of unidentified period between main events during time sequences. LSTMs were established to overcome the discharging and disappearing gradient problems which will be come across when training traditional RNNs.

The LSTM unit contains a memory cell that has three gates described below:

Input gate (i): The input gate computes the sum of input that is allowed to pass through it and is calculated by:

$$i = \sigma (xt\ Ui + st\text{-}1\ Wi) \text{ ---- } (1)$$

The sigmoid function plots the input value between [0, 1] and this value is multiplied by the weight vector (Ui). This helps the gate manage the quantity of input that is transferred through the input gate.

Forget gate (f): The forget gate helps the network to choose what and how much information from the earlier level to transfer to the succeeding level. The sigmoid function maps the value of this function between 0 and 1. It is given by:

$$f = \sigma (xtUf + st\text{-}1\ Wf) \text{ ---- } (2)$$

If no input wants to be transferred to the next level, the previous memory is multiplied with the zero vector, that creates the input value zero. Likewise, if the memory at st-1 needs to pass to next level it is multiplied by 1 vector. If only some part of the input is to be passed, then the resultant vector is multiplied with the input vector

Output gate (o): The output gate, describes the output passed at each step of the network. It is given by:

$$o = \sigma (xtUo + st\text{-}1\ Wo) \text{ --- } (3)$$

BiLSTM means bidirectional LSTM, which means the signal transmits backward as well as forward in time.

Gated recurrent unit

GRU is a type of deep learning algorithm that is enhanced from the LSTM algorithm to minimize the complication of the algorithm by using update gate and reset gate. The update gate is used to regulate hidden state volume to be forwarded to the next state. The reset gate is used to define the consequence of the previous hidden state information.

Update Gate (z): It determines how much of the past information needs to be passed along into the future. It is similar to the Output Gate in an LSTM recurrent unit.

$$z = \sigma (x_t\ U^z + st\text{-}1\ W^z) \text{ ---- } (4)$$

Reset Gate (r): It defines how much of the past information to forget. It is similar to the combination of the Input Gate and the Forget Gate in an LSTM recurrent unit.

$$r = \sigma (x_t Ui + st\text{-}1\ W^r) \text{ ---- } (5)$$

BIGRU means Bidirectional GRU's are a kind of bidirectional recurrent neural networks allow for the use of information from both previous time steps and later time steps to make predictions about the current state

IV. CONCLUSION

In this existing model, a Discrete Pre-processing Method using standard scaler and NIDS using a Convolution Neural Network (CNN) were proposed to solve the problems occurring in the learning based NIDS. NSL-KDD dataset used to classify the normal and attack target. By using discretization in the pre-processing process, data consisting of mixed features were converted into data that can easily analyse the relationships between various feature

relationships. Using the least studied CNN-based NIDS model, we evaluated the generalization performance of the proposed pre-processing method. In future, the project is expected to show better results by implementing Recurrent Neural Networks (RNN) and the performance is compared with existing approaches

REFERENCES

[1] https://www.techtarget.com/searchsecurity/definition/intrusion-detectionsystem
[2] https://www.geeksforgeeks.org/intrusion-detection-system-ids/
[3] https://en.wikipedia.org/wiki/Intrusion_detection_system
[4] P Rajesh Kanna et al., "Unified Deep Learning approach for Efficient Intrusion Detection System using Integrated Spatial–Temporal Features", Knowledge-Based Systems, Volume 226, 2021, 107132.
[5] Jingmei Liu et al., "A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM", Computers & Security, Volume 106, July 2021, 102289.
[6] Keserwani, P.K. et al., "A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model", Journal of Reliable Intelligent Environment , 3–21 (2021).
[7] Basati, A. et al., "APAE: an IoT intrusion detection system using asymmetric parallel auto-encoder", Neural Computing & Applications (2021).
[8] JihoonYoo et al., "Study on Network Intrusion Detection Method Using Discrete Pre-Processing Method and Convolution Neural Network", IEEE Journal, 2021