IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

Anomaly-Based Intrusion Detection/Prevention System using Deep Reinforcement Learning Algorithm

O. E. Taylor[1], P. S. Ezekiel[2], & C.G. Igiri[3]

Rivers State, Computer Science, Rivers State University, Port Harcourt, Nigeria[1,2,3]

Abstract: Cyber security has become an increasingly important area in computer science in response to the expansion of private sensitive information. Intrusion can be defined as an uncertified access, which aims to compromise integrity, confidentiality and availability of data. Conventional intrusion prevention method such as access control firewalls and encryption cannot fully prevent system from advanced attacks. Intrusion Detection System has become a crucial part of computer security, which is used in detecting the above-mentioned threat.This paper presents an agent based Anomaly intrusion detection and prevention system using Reinforcement Learning Technique. The system uses two agents, the first agent attacks the network system while the second agent detects the attack and classify it to be either normal, dos, probe, u2l and u2r attack, the orange line represents the reward receive by the attacking agent while the blue line represents the reward of the agent detecting and classifying the attack. The attacking agent receives a total reward 5 while the defending agent received a total reward of 95. This means that the defending agents performs more better in detecting and classifying attacks that is being carried out by attacking agent. The diagram also shows the loss values of the both agent during training. The both agent has a loss value below 0.5 during training. Figure 5 shows the performance of the defending agent in classifying an attack currently. The agent obtained individual accuracy in each of the attack. The accuracy are as follows, normal 0.79%, DoS 0.94%, R2L 088%, Probe 0.94% and U2R 0.99%.

Keywords: Reinforcement Learning, Deep Q-learning Network, Intrusion detection, Anomaly attack.

INTRODUCTION

Cyber security has become an increasingly important area in computer science in response to the expansion of private sensitive information. Intrusion can be defined as an uncertified access, which aims to compromise integrity, confidentiality and availability of data [1]. Conventional intrusion prevention method such as access control firewalls and encryption cannot fully prevent system from advanced attacks. Intrusion Detection System has become a crucial part of computer security, which is used in detecting the above-mentioned threat. Many researchers have been trying to develop a more accurate model to detect intrusion attack. Intrusion detection method can be classified as two categories, which are, Misuse or Anomaly Based and Signature Based Method. Signature based approach is used in detecting only known intrusion attacks whose signatures are kept on the database while Anomaly Based approach is used in detecting attacks that are not just know or kept on the database. Important data is always enticing to cyber attackers and therefore endangered to intensive network attacks. Intrusion refers to the procedure by which a cyber-attacker forwards noxious packets to the users system in other to alter or degenerate any private or significant data. An attack refers to the illegitimate forwarding of network packets through the network. The intrusion can take place over the system or serverdue to the weakness of the system, such as user abuse, inappropriate configuration of system, or program absconds. A Robust intrusion system can be built by assembling numerous vulnerability. Globally, huge amount of online administrations and millions of large servers are running in the system. Such organizations become more alluring to more attackers and subsequently require a robust intrusion detection agent to defend their network system [2].

In early days, intrusion detection is finished utilizing rule-based methodologies, where specialists characterize a sets of rules for typical and anomalous conditions. These systems turn out better for realized attacks yet neglect to identify obscure attacks. In later 1990s, scientists concentrated to create programmed intrusion detection strategies. Numerous analysts utilized information mining and Artificial Intelligent in detecting attacks that are not known. Among different intrusion detection strategies, Fuzzy Logic based techniques assume a significant job. From writing audit, it is discovered that grouping strategies are generally utilized methodologies in intrusion recognition system [3]. This paper presents a reinforcement learning technique in detecting and preventing anomaly-based intrusion attack using Deep Q-Learning Algorithm.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

I. LITERATURE REVIEW

Anomaly based Intrusion Detection using Modified Fuzzy Clustering [3] presents a framework for Anomaly-based intrusion detection using fuzzy clustering. Their proposed framework is made of three steps, which are removing duplicate data from the dataset by means of pre-processing, selecting the most suitable columns by means of feature extraction and collecting network data by making use of an intelligent Spatial Kernel Fuzzy C-Means (RSKFCM) algorithm. RSKFCM is an alternative of conventional Fuzzy C-Means, which examine the neighborhood integration data and make use of kernel distance metric. In evaluating their proposed framework, they carried out experiments on a quality dataset and collate the results with state-of-the-art methods. They made use of cluster validity indices, false positive rate as and accuracy as execution metrics. K-means clustering had accuracy of 66.46%, K-Medoids 77.71%, and Fuzzy C-Means 86.26%. Their proposed framework had the highest accuracy result when compared with other frameworks.

Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model [4]Presents a new hybrid framework that will be used in estimation the range of the intrusion threshold valuebased on the network proceedings data's optimal features that were made available for training. Their findings uncovered that the hybrid framework significantly affected the minimization of the computational and time multifaceted nature included while deciding the element affiliation sway scale. The exactness of the proposed framework was estimated as 99.81% and 98.56% for the twofold class and multiclass NSL-KDD informational indexes, separately. In any case, there are issues with acquiring high false and low false negative rates. A hybrid framework with two principle parts was proposed to address these issues. To begin with, information should be sifted utilizing the Vote calculation with Information Gain that joins the likelihood disseminations of these base students to choose the significant highlights that emphatically influence the exactness of the proposed framework. Next, the half and hybrid algorithm comprises of following classifiers: J48, Meta Pagging, RandomTree, REPTree, AdaBoostM1, DecisionStump and NaiveBayes. In view of the outcomes acquired utilizing the proposed model, they noticed improved precision, high false negative rate, and low false positive rule.

Toward a reliable anomaly-based intrusion detection in real-world environments [5] presents another technique for making intrusion information bases. The goal is that the information bases ought to be anything but difficult to refresh and duplicate with genuine and substantial traffic, delegate, and openly accessible. Utilizing their proposed technique, they propose another assessment plot explicit to the AI interruption location field. Sixteen interruption information bases were made, and every one of the suspicions much of the time embraced in concentrates in the interruption location writing with respect to organize traffic conduct was approved. To make Artificial Intelligent discovery plans achievable, they propose another multi-target include choice strategy that thinks about genuine organization properties. The outcomes show that a large portion of the presumptions oftentimes applied in concentrates in the writing do not hold when utilizing an Artificial Intelligent recognition plot for network-based intrusion detection. In any case, the proposed multi-target include determination strategy permits the framework precision to be improved by considering certifiable organization properties during the model creation measure.

Application of deep reinforcement learning to intrusion detection for supervised problems [6] applied different reinforcement learning algorithm in detecting network intrusion on a labelled dataset. The dataset used are NSL-KDD and AWID datasets. As a novel methodology, they have made an applied alteration of the exemplary Deep Reinforcement Learning worldview (in light of cooperation with a live environment), supplanting the environment with an inspecting capacity of recorded preparing intrusions. This new pseudo-environment, notwithstanding inspecting the preparation dataset, produces rewards dependent on errors discovered during preparing. They present the facts of applying their strategy to four of the most applicable Deep Reinforcement Learning algorithms such as Deep Q-Network (DQN), Double Deep Q-Network (DDQN), Policy Gradient (PG) and Actor-Critic (AC). The best outcomes are gotten for the DDQN algorithm. They show that Deep Reinforcement Learning algorithms, with our framework and some parameter changes, can improve the after effects of intrusion detection in examination with current Artificial Intelligent methods.

Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues [7] study thoroughly audits and reviewed the key past Deep learning centered computer security studies. Through a broad audit, this study gives a novel fine-grained scientific classification that sorts the present status of-the-workmanship Deep learning-based Intrusion Detection Systems concerning various features, including input information, discovery, arrangement, and assessment systems. Every aspect is additionally grouped by various standards. This review likewise looks and talks about the related assessment solutions proposed as deep learning-based IDSs. By dissecting the exploratory investigations, this study examines the part of Deep learning in intrusion identification, the effect of interruption recognition datasets, and the proficiency and viability of the proposed approaches. The discoveries show that further exertion is needed to improve the present status of-the workmanship. At last, open examination challenges are recognized, and future exploration bearings for deep learning-based Intrusion Detection Systems are suggested.

Adversarial environment reinforcement learning algorithm for intrusion **detection** [8] presents the principal utilization of ill-disposed reinforcement learning for intrusion detection, and gives a novel strategy that consolidates the environment's conduct into the learning cycle of a changed reinforcement learning algorithm. They demonstrate that the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

proposed technique is sufficient for a supervised learning issue dependent on a marked dataset. They approve its performance by contrasting it and other notable Artificial Intelligent models for two datasets. The proposed model outflanks different models in the weighted Accuracy (>0.8) and F1 (>0.79) measurements, and particularly dominates in the outcomes for the under-spoke to marks.

A context-aware robust intrusion detection system: a reinforcement learning-based approach [9] presenteda context-adaptive Intrusion Detection System made use of different reinforcement learning agent for accurate detection network intrusion attack. They conducted an extensive assessment using three datasets on their trained model. The datasets are UNSW-NB15, NSL-KDD, and AWID. Their trained model had a better accuracy (78.67%) and false positive rate (2.80%) result when compared to the state-of-the-art systems. Further, they carried out an analysis on the robustness of their trained model against antipathetic attack and noticed a small decrease in accuracy when compared to other models. They executed concept of denoisingautoencoder in other to prove the robustness of their proposed system. In real life, their model changes the pattern of the attack.

An intrusion detection approach based on improved deep belief network [10] presented an improved deep belief network that will reduce the problem of low performance accuracy and high false positive rate result on intrusion detection system. They processed NSL-KDD and UNSW-NB15 using Min-Max normalization, encoding, and probabilistic mass function (PMF) method to data simplification. They also presented a non-mean Gaussian distribution Kullback-Leibler (KL) divergence in the likelihood function of the unsupervised training stage of the deep belief network, in other to avoid the hitch of overfitting and feature homogeneity. Finally, incentive assessments are performed on the NSL-KDD and UNSW-NB15 public datasets. The proposed framework achieves an accuracy of about 96.17% on the NSL-KDD and 86.49% UNSW-NB15, respectively. Their results show that when their proposed framework is compared with the state-of-the-art methods, the proposed framework achieves a better result in classification accuracy and false positive rate.

Automatic Intrusion Detection System Using Deep Recurrent Neural Network Paradigm [11] addressed the problem of low false positive rate and high accuracy result on intrusion detection system by building an illustrative model using different Deep Recurrent Neural Network (RNNs). Recurrent Neural Network models has the capacity to theorize the knowledge that ca n be used to detect both known and unknown threats. This theorization comes from Recurrent Neural Network abilities to define in its terms the normal attack and anomaly attack. They tested four Recurrent Neural Network models NSL-KDD dataset, which is a quality test dataset for network intrusion. The proposed system outperforms other deployed models in terms of the ensign measurements: accuracy, recall, precision and f-measure. The accuracy of the four Recurrent Neural Network model are BLSTM 77.2%, LSTM 71.6%, BRNN 74.1%, and RNN 74.2%.

II. METHODOLOGY

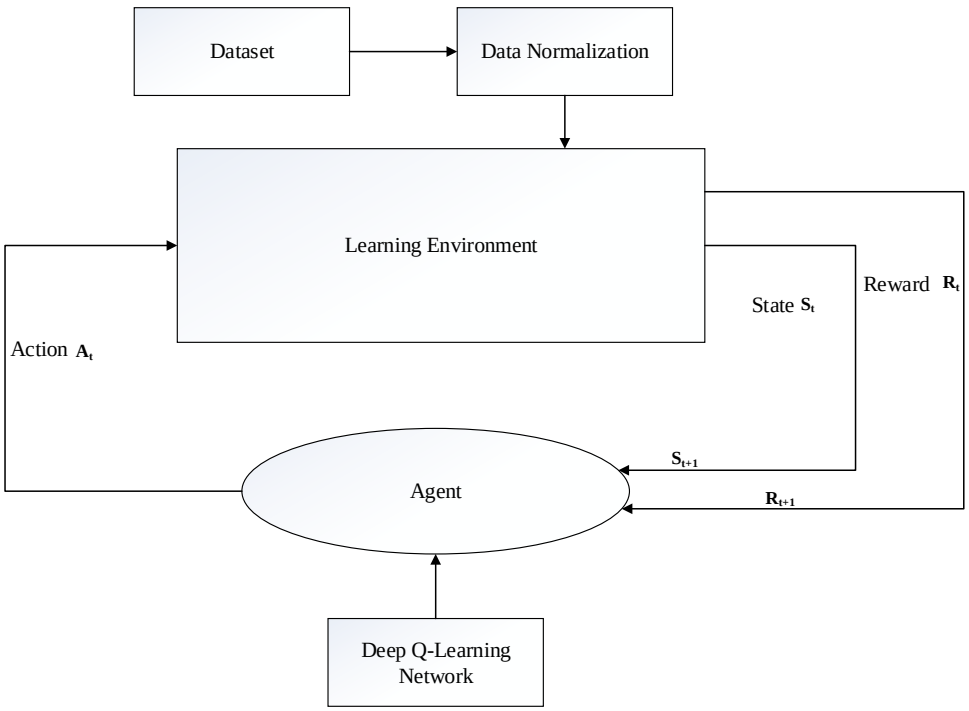

Figure 1: Architecture Diagram of the Proposed System

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

The proposed system uses a Reinforcement Learning Technique in detecting and preventing Anomaly-based intrusion attack. The proposed system uses a Deep Q-Learning algorithm in training the agent. The architectural components of the proposed system can be explained as follows:

Dataset: The system made use of a National Security Letter-Knowledge Discovery in Database (NSL-KDD) dataset in training the reinforcementlearning agent. The dataset is a standard benchmark for intrusion detection. The dataset is made up of a training data, which include the type of attack and difficulty levels, and a test data, which also include attack-type labels and difficulty levels. The dataset has been preprocessed, removing all redundant data in the training data, so that the agent will not be biased towards values that are more frequent and duplicate data has been removed as well in the testing data.

Data Normalization: The dataset will be normalized using the normalize function which we imported from the pre-processing library in resizing the estimated attributes into 0 and 1, in other for our agent to have better performance in terms in terms of accuracy, lesser false positive rate.

Learning Environment: The environment is made up of a set of state, reward and actions of which the Reinforcement Learning Agent interacts with in other to decide on what action to take. The states describes the current condition of the environment. The action is the choice or decision taken by the agent at each state. The action of the agent is to detect/classify the type of attack carried out on the system. The attack can either be Normal, Denial of Service (Dos), Remote to Local (R2L), User to Root (U2L) and Probe-response attack.

Agent: We will be training two Reinforcement Learning agents using Deep Q-Learning algorithm. The agent learn and interacts with the learning environment in other to make optimal choices. The creation of the agent begins with some declaration of some variables with some parameters. The Variables used are epoch_num, max_step, memeory_size, batch_size, epsilon, epsilon_decrease, epsilon_min, learning_rate and gammatotal_rewards.

Deep Q-Learning Network: Q-Learning is a value-built Reinforcement Learning Algorithm, which is used in finding the best action/choices using Q Function. This helps the Reinforcement Learning agent in taking the right action/choices in a given state. The Deep Q Learning make use of a neural network to estimate the Q-Values Function. The State will be taken as an input and the Q-Value of all feasible actions/choices will be bring about the output.

$$Q(s, a) = r(s, a) + \gamma \max_{a} Q(s', a) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$Q(s, a) \rightarrow \gamma Q(s', a) + \gamma^2 Q(s'', a) \ldots\ldots\ldots \gamma^n Q(s''^{\ldots n}, a) \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$Q(S_t, A_t) \leftarrow Q(S_t, A_t) + \alpha[R_{t+1} + \gamma \max_{a} Q(S_{t+1}, a) - Q(S_t, A_t)] \ldots\ldots\ldots (3)$$

Where:

Q is the Q learning factor

s and a are actions carried out by the agent on a particular state

γ is the gamma

α is the rate at which the agent learns in the environment

t is the time taken by the agent in completing one action in a state

Algorithm for Deep Q-Learning:

Step1: Initialize Q Table

Step2: Choose an Action

Step3: Perform an Action

Step4: Measure Reward

Step5: Update Q Table by repeating Step2-Step4

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

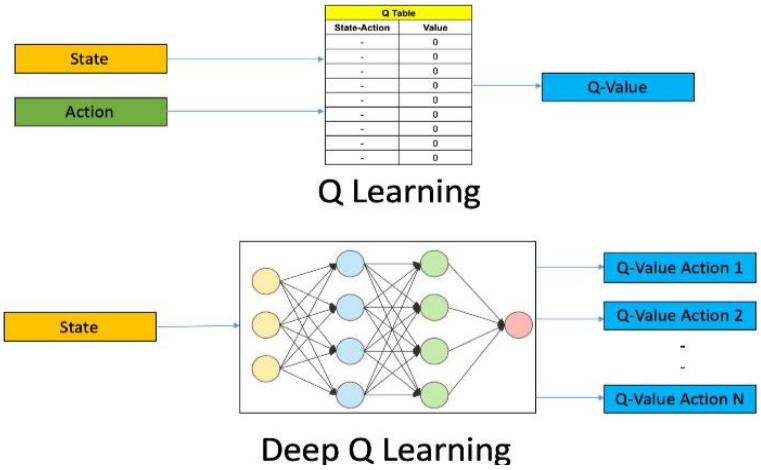

Figure 2: Deep Q-Learning Architecture

III. Result and Discussion

This paper presents an agent based Anomaly intrusion detection and prevention system using Reinforcement Learning Technique. The system uses a Deep Q Learning algorithm in training our agent. We start by using a NSL-KDD dataset for training and testing the performance of our agent. The dataset consists of some labeled attack types and some difficult levels. The dataset was normalized using normalization function from pre-processing library in python in other to have a better training performance. We created a learning environment in which the agent can learn and interact with, by making use the NSL-KDD dataset. The environment consist of state, action and reward. The state is the representation of the environment; the action is the movement of the agent within the state or the choice/decision made by the agent at a given state. We trained two Reinforcement Learning agents namely attacking agent and defending agent. The goal of the attacking agent is to penetrate the network system using diverse attack like Dos attack, probe attack, R2L attack and U2R attack, while the goal of the defending agent is to defend the network system from the mentioned attacks. The attacking agent starts by identifying the type of attack, and then taking a proper action on the found attack. The defending agent gets a reward each time it identifies the attack carried out by the attacking agent correctly so as the attacking agent gets a reward whenever it succeeds in carrying out a successful attack. This following are the parameters used in training our agents, epoch_length = 100, epsilon = 1,min_epsilon = 0.01, gamma = 0.001, hidden_size = 100, hidden_size = 3, minimum_batch_size = 100, memory_size = 1000, learning_rate = 0.00025. After training our Reinforcement Learning agents, we had a total reward of 5% for the attacking agent and a total reward of 95% for the defending agent. Figure 5 shows the performance of the defending agent in classifying an attack currently and Table 1 shows the accuracy, precision, f measure and recall of the individual attack. The accuracy are as follows, normal 0.79%, DoS 0.94%, R2L 088%, Probe 0.94% and U2R 0.99%.

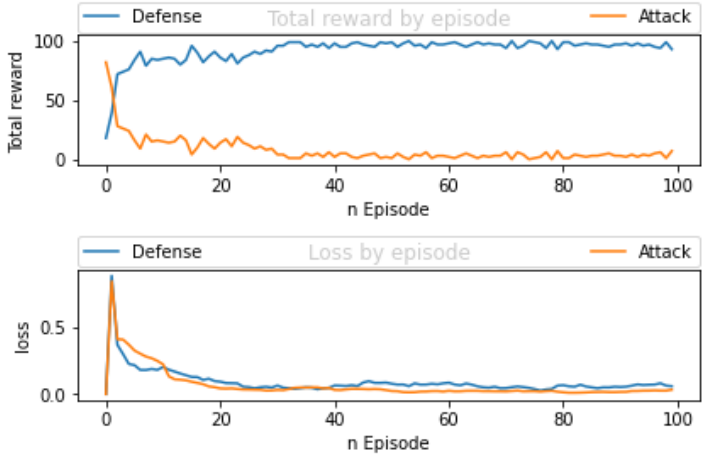

Figure 3: Showing the total reward and loss received by both agents.

The system uses two agents, the first agent attacks the network system while the second agent detects the attack and classify it to be either normal, dos, probe, u2l and u2r attack, the orange line represents the reward receive by the attacking

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

agent while the blue line represents the reward of the agent detecting and classifying the attack. The attacking agent receives a total reward 5 while the defending agent received a total reward of 95. This means that the defending agents performs more better in detecting and classifying attacks that is being carried out by attacking agent. The diagram also shows the loss values of the both agent during training. The both agent has a loss value below 0.5 during training.

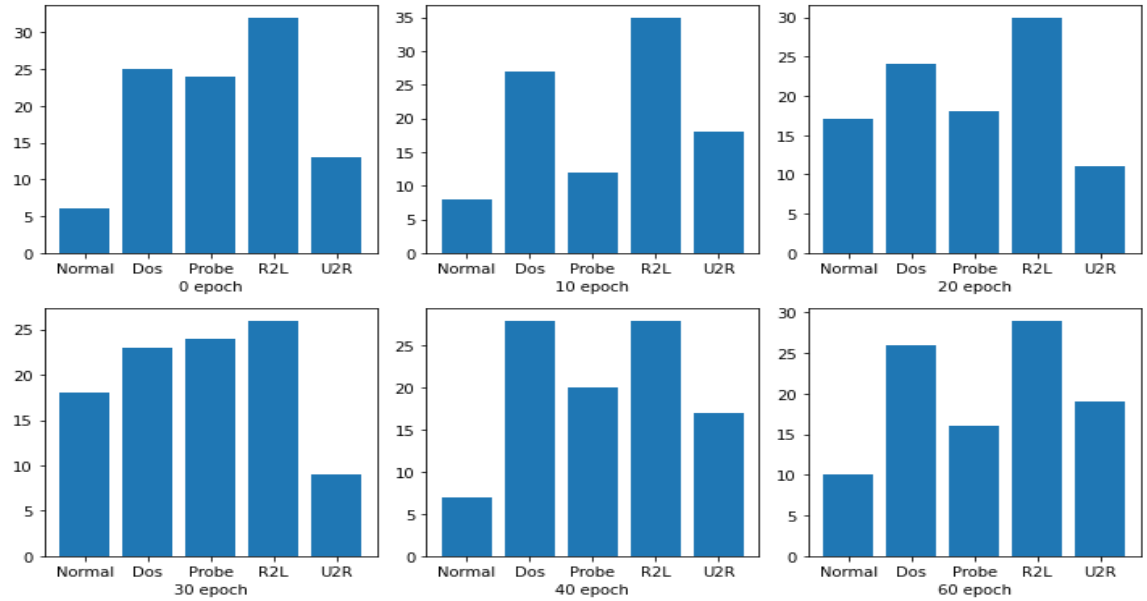

Figure 3 showing the distributed attacks carried out by the attacking agent at each epoch level

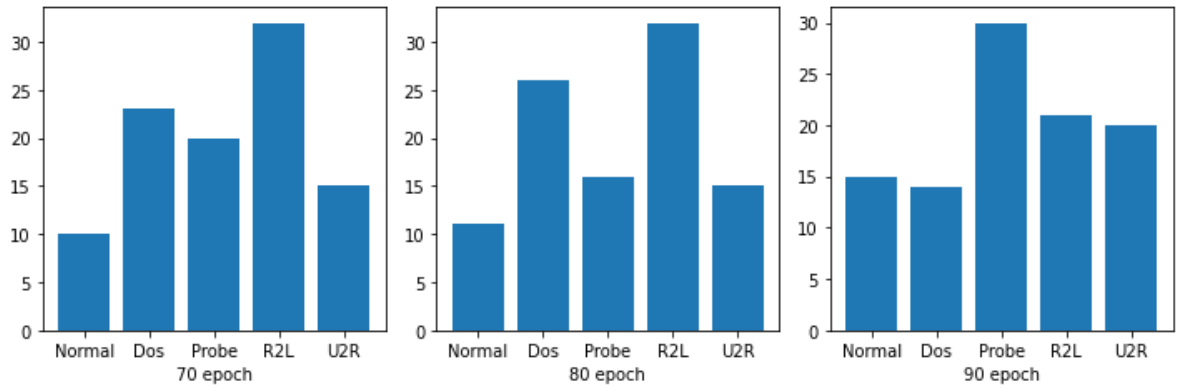

Figure 4: showing the continuation of figure 3

The attacking agent carried out diverse attack on the network system at the different epoch level. For the 0 epoch, the attacking agent performed a Dos attack 25 times, probe attack 24, R2L 35 and U2R 14 while at the final epoch level, Dos attack was 14, probe 29, R2L 21, and U2R 20.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

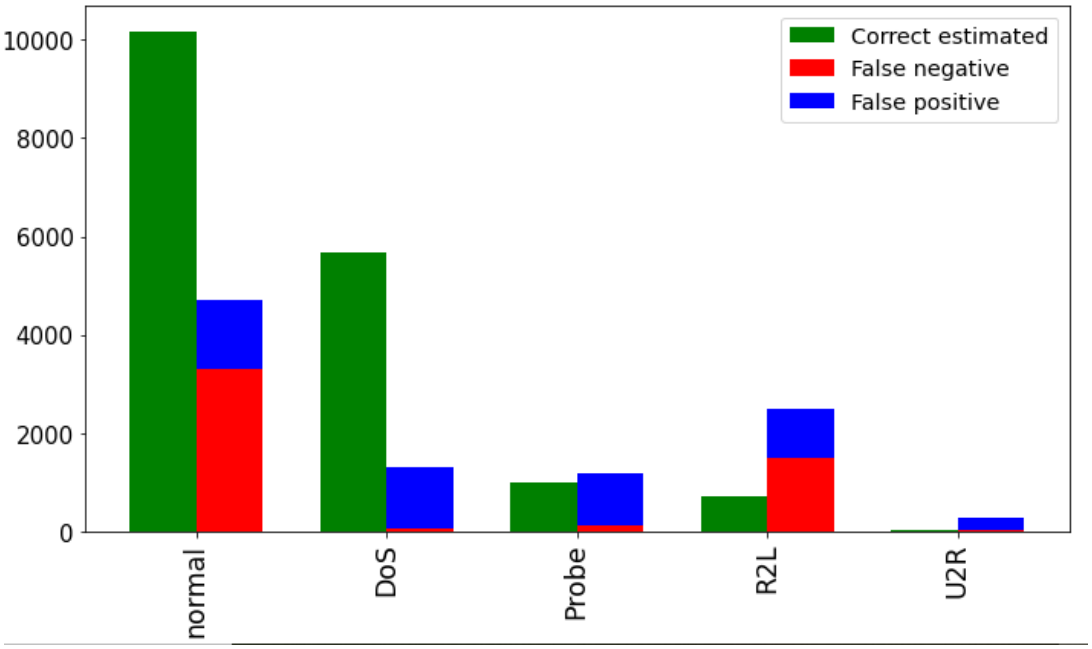

Figure 5: showing the performance of the defending agent.

By correct estimate, we mean when the defending agent classifies an attack correctly, false negative is when the agent fails to detect an attack when there is an attack while false positive is when the agent wrongly detect an attack when there is none.

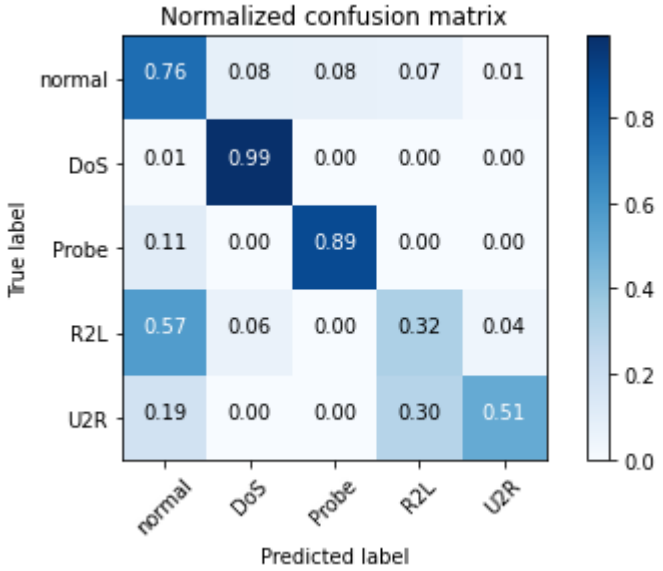

Figure 6: showing a normalized confusion matrix

This shows the summarizing performance of the defending agent, it shows the true label vs the predicted label.

Name	Accuracy	F1	Precision	Recall
Normal	0.79	0.81	0.88	0.76
DoS	0.94	0.89	0.82	0.99
R2L	0.89	0.36	0.41	0.32
Probe	0.94	0.62	0.48	0.89
U2R	0.99	0.12	0.06	0.51

Table 1: Showing the performance matrix of each of the attack.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10114

IV. CONCLUSION

Cyber security has become an increasingly important area in computer science in response to the expansion of private sensitive information. Intrusion can be defined as an uncertified access, which aims to compromise integrity, confidentiality and availability of data. Conventional intrusion prevention method such as access control firewalls and encryption cannot fully prevent system from advanced attacks. This paper presents an agent based Anomaly intrusion detection and prevention system using Reinforcement Learning Technique. The system uses two agents, the first agent attacks the network system while the second agent detects the attack and classify it to be either normal, dos, probe, u2l and u2r attack, the orange line represents the reward receive by the attacking agent while the blue line represents the reward of the agent detecting and classifying the attack. The attacking agent receives a total reward 5 while the defending agent received a total reward of 95. This means that the defending agents performs more better in detecting and classifying attacks that is being carried out by attacking agent. The diagram also shows the loss values of the both agent during training. The both agent has a loss value below 0.5 during training. Figure 5 shows the performance of the defending agent in classifying an attack currently. The agent obtained individual accuracy in each of the attack. The accuracy are as follows, normal 0.79%, DoS 0.94%, R2L 088%, Probe 0.94% and U2R 0.99%. This paper can further be extended by implementing the trained agent in a real time network intrusion system in other to check for performance in detecting and classifying an attack correctly.

REFERENCES

[1]. Ahmed, Mohiuddin, A.N. Mahmood, J. Hu. "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19-31, 2016.
[2]. D.P. Gaikward, R.C. Thool, "Intrusion detection system using bagging with partial decision tree base classifier", Proceeding of International Conference on Advanced in Computing, Communication and Control vol. 49, pp. 92–98 2015.
[3]. B. S. Harish and S. V. Aruna Kumar "Anomaly based Intrusion Detection using Modified Fuzzy Clustering" International Journal of Interactive Multimedia and Artificial Intelligence, Vol.4, issue.6, pp.54-59, 2015.
[4]. S. Aljawarneha, M. Aldwairi, M.B. Yassein "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model", Journal of Computational Science, vol.628, issue.9, pp.1-9, 2017.
[5]. E. K. Viegas , A. O. Santina, L. S. Oliveira "Toward a reliable anomaly-based intrusion detection in real-world environments" Computer Networks, vol.127, issue.2017, pp.200-216, 2017.
[6]. M. L. Martin, B. Carro, A. S. Esguevillas "Application of deep reinforcement learning to intrusion detection for supervised problems" Expert System with applications, Volume 141, issue.1, pp.11-19, 2020.
[7]. A. Aldweesh, A. Derhab, A. Z. Emam "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues" Knowledge-Based Systems vol. 185, issue.1, pp.105-124, 2020.
[8]. G. Caminero, M. Lopez-Martin, B. Carro "Adversarial environment reinforcement learning algorithm for intrusion detection" Computer Networks, vol.9, issue.4, pp.96-109, 2019.
[9]. K. Sethi, E.S. Rupesh, P. Bera, Y.V. Madhav "A context-aware robust intrusion detection system: a reinforcement learning-based approach" International Journal of Information Security, vol.19, issue.2, pp.657-678, 2020.
[10]. Q. Tian, D. Han, K. Ching-Li, X. Liu "An intrusion detection approach based on improved deep belief", Journal of Applied Intelligence, vol.50, issue.3, pp.3162-3178, 2020.
[11]. A. Elsherif"Automatic Intrusion Detection System Using Deep Recurrent Neural Network Paradigm", Journal of Information Security and Cybercrimes Research (JISCR), vol.1, issue.1, pp.28-41, 2018.