International Journal of Pharmaceutical Research and Applications
Volume 7, Issue 4 July-Aug 2022, pp: 180-185 www.ijprajournal.com ISSN: 2456-4494

Detection of Intrusion via Wireless

Vyshaka B L, Ms. Jyothi P K, Dr. Ravikumar G K
Dept. of CSE, BGS Institute of Technology, Adichunchanagiri University, BG Nagar, Karnataka,India-571448.
Dept. of R&D, BGS Institute of Technology, Adichunchanagiri University, BG Nagar, Karnataka, India-571448
Professor& Head(R&D), Dept. of CSE, BGS Institute of Technology, Adichunchanagiri University, BG Nagar, Karnataka, India-571448

Submitted: 01-07-2022 Accepted: 10-07-2022

ABSTRACT— WiFi was already popular and extensively utilized to provide wireless Internet access in the home, office, and even stadiums, and due to its integration with 5G cellular networks, It will play a significant role in the future wireless communication. Due to the open topology of the communication network and the availability of WiFi intrusion tools, security concerns remain a major worry for WiFi. As a result, it is necessary to detect previously experienced intrusions in order to apply additional intrusion response strategies. Intrusion detection and prevention methods based on basic machine learning algorithms, on the other hand, often have low detection accuracy and necessitate extensive human involvement. In this context, this study provides a WiFi intrusion detection technique based on convolutional neural networks (CNNs). First, we'll go over the identification methodology, This begins with data pre-processing before teaching a CNN to detect attacks. The dropout method is used to reduce the risk of data overfitting as well as the amount of time needed to apply this technique, and several network architectures are studied. Our system outperforms existing ones, with a detection performance of more than 99 percent, AWID, an open data set, yielded the following conclusions of the experiment.

Keywords—CNN, WiFi, Cellular Networks.

I. INTRODUCTION

WiFi wireless networks are increasingly being used to provide Internet access in residences, businesses, arenas, and other structures[1]. WiFi networks will continue to be an important aspect in developing indoor network services in the anticipated integrated information and communications technology (ICT).However, because the communication network is open-source and open-source WiFi infiltration toolchains are readily available,, WiFi networks are vulnerable to serious security risks such as impersonation, flooding, injection, and so on. It is vital to detect and identify network assaults in order to re-establish authorised network service while protecting user privacy The two categories of intrusion detection systems (IDS) proposed for WiFi connections are presently signature-based IDS and anomaly detection-based IDS[5]. To detect future threats, a signature-based IDS examines key attributes from recent assaults[6]. Anomalies detection technology, on the other hand, constructs a model for normal network behavior and qualifies any divergence as an unusual attack[7].

The model's validity, as well as the difficulty of model building and feature engineering, are all factors to consider, will have a substantial impact on its detection accuracy. As a result of its effectiveness in a variety of fields, including face recognition and speech recognition, some recent projects have utilized neural networks for IDS design. Ji et al. created a ladder network-based deep learning approach [8]. Investigations on an open data set, on the other hand, have demonstrated that their plan is still inaccurate. Due to the growing number of internal and external network threats, WID technology is an essential component of any platform or enterprise that is interconnected and has broadband communication within it. WIDS systems are used to foresee and identify threats to mobile networks, such as flooding and ding.denial-of-service attacks, and evil doppelgängers, all of which have a negative impact on system availability. Artificial intelligence is a prominent approach that can help you design a good network intrusion detection system.

This is critical to these systems' capacity to study complex behaviours and then utilise the learnt mechanism to detect and prevent network threats. In these paper, They employed a classification model combined with a DNN deep methodology to detect intrusion and vulnerabilities

International Journal of Pharmaceutical Research and Applications
Volume 7, Issue 4 July-Aug 2022, pp: 180-185 www.ijprajournal.com ISSN: 2456-4494

in 5G mobile networks.The dataset used was the Aegean Wi-Fi Intrusion dataset (AWID). With a 99 percent prediction performance for the information malicious activities of overflow, impersonation, and injecting, our WIDS looked impressive. Because of the enormous variety of operations and capacities that wireless networks may provide, that make our lives simpler, they are being created on a daily basis. It's a hot topic that's gotten a lot of attention. The 5G (fifth-generation mobile network) is a "growing international communication network after 1G, 2G, 3G, and 4Gigabit ethernet that enables a new form of the network meant to practically connect everybody and everyone collectively, incorporating organizations, things, and devices," according to Wikipedia. The capacity to achieve higher multi-Gbps maximum data speeds, ultra-low latency, better reliability, huge available bandwidth, increasing prevalence, superior efficiency, and efficiency gains are only some of the benefits of 5G digital networks."

II. RELATEDWORK

[1] Qiang Duan This research employs a CNN model to classify attacks in WiFi cellular networks, Taking advantage of the model's capacity to identify the underlying observed data presented by a variety of attacks.To reduce noise and redundancy, the data is initially pre-processed. A CNN model training technique is provided in the second section. Finally, an open dataset namely AWID, which was launched in 2016, is used to evaluate our approach.Our idea outperforms 5 other proposals in terms of overall recognition rate for four scenarios, according to experimental results.[2] Bayana alenazi This project resulted in the implementation of a 5G wireless Intrusion Detection System (WIDS) with Deep Learning; the above method recognizes attacks in real-time utilising a framework that was trained using various deep learning classification techniques, then used with autoencoder and DNN algorithms, and then analysed. The system was trained utilizingthe AWID wireless inputs, that comprises a wide range of threats to wifi communication. Finally, the system ensures that the results are accurate, timely, and easy to understand[3] Abdulsalam In real-time applications, the suggested solution focused on identifying anomalies and safeguarding the SDN platform from attackers. The proposed approaches accomplished two jobs at once: detecting whether or not there was an assault and determining the sort of attack (Dos, probe, U2R, R2L). We analyze three classic tree-based machine learning techniques, Random Forest, Decision Trees, and XGBoost, to find the best algorithm. We look at them using a range of evaluation metrics to see what the drawbacks and benefits are of utilizing one or more of them. The proposed XGBoost model excelled in more than seven NIDS algorithms using six various evaluation criteria.

[4] Yanxia Sun Although intrusion detection systems (ids) are crucial for securing hardware and communications systems, many IDS still have compatibility problems. Furthermore, standard machine learning-based IDS algorithms lose a lot of accuracies as the feature space expands. To provide a deep learning-based IDS, we use feed-forward deep neural networks (FFDNNs) and a filter-based component evaluation technique in this research. The FFDNN-IDS is evaluated alongside earlier ML techniques such as SVM, decision trees, K-Nearest Neighbor, The Bayesian Network using the well-known NSL-knowledge acquisition and data mining (NSL-KDD) dataset.The experimental findings suggest that the FFDNN-IDS achieves a greater level of accuracy than earlier techniques.Amr Attia[5]to detect harmful patterns, this study offers an effective Network Intrusion Detection Systems (NIDS) the structure that uses state-of-the-art machine/deep learning technologies as well as progressive probabilistic dampening features of particles.A systematic evaluation study of eXtreme Gradient Boosting (XGBoost) and ANN is conducted, To reduce system complexity and provide quick responses, matrix factorization methodologies including such Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) are being incorporated into the simulations. Machine/deep learning methods are highly good for malware identification on known assaults when matched with the correct characteristics gathered, according to several experimental runs.Abdulhammed Razan [6] The proposed approach returns four groups of attributes, each with 32, 10, 7, or 5 properties. In terms of the number of classes, characteristics, and reliability, the classifiers had good precision and low false-positive rates, and the suggested work outperformed entire list work. With a 10-fold cross-validation technique, the suggested study attained a maximum accuracy of 99.64 percent for Random Forest with the availability test and 99.99 percent for Random Forest using J48.

Alzahrani, Hamdan A. [7] The improved

International Journal of Pharmaceutical Research and Applications
Volume 7, Issue 4 July-Aug 2022, pp: 180-185 www.ijprajournal.com ISSN: 2456-4494

approach lowers the risk of denial-of-service (DoS) attacks against a WBAN. It's critical to control noise, which could skew the data collected by the sensors. The degree of noise at which the machine-learning model can be trusted is demonstrated in this research since it can impair the efficiency of the ML algorithms. Since there is no noise, the findings demonstrate that J48 is the best model, with an accuracy of 99.66 percent, when compared to the ANN algorithm. With noisy datasets, however, ANN exhibits a greater tolerance for noise.Kasongo[8] Although intrusion monitoring technologies are crucial for safeguarding computer and network infrastructure, many IDS still have performance issues. Furthermore, as the feature space grows larger, the efficiency of current Machine Learning (ML)-based IDS approaches plummets. We present a Deep Learning (DL)-based IDS that employs Feed Forward Deep Neural Networks (FFDNN) and a filter-based attribute extraction technique in this study. The FFDNN-IDS is compared to the Support Vector Machines (SVM), Decision Tree (DT), KNearest Neighbor (KNN), and Naive Bayes algorithms using the well-known NSL-KDD dataset (NB).As per the findings of the studies, the FFDNN-IDS outperforms the competition in aspects of correctness.

III. RESEARCH METHODOLOGY

A. Data Collection

Data-driven sequential training became a major study paradigm in these area of wireless cybersecurity, thanks to the rise of automation and artificial intelligence. An accessible and trustworthy data set is the basis for a strong platform.The NSL-KDD, UNSW-NB15, ADFA-LD, KDDCUP99, and AWID data sets are presently the most often used network attack data sets [11]. For example, the KDDCUP99 data set and the NSL-KDD data set were both acquired ten years ago and are no longer widely used.The AWID data set was compiled by the Aegean University in Greece in 2015 through field simulators of WiFi intrusions, and it will be used to verify my study method. Fraudulent attacks, overflow attacks, and injecting attacks are all included in the AWID dataset. Table I [12] shows the prevalence of the AWID data set.

B. Intrusion Detection in Wireless Networks

Aminanto et al. employed stacked auto-encoders (SAE) to identify relevant data to monitor network hazards, mix them only with innovative parts, sort, reduce redundant features, and use SVM [13]. Zhu et al. have introduced a multi-aims IDS characteristic choosing technique. These method employs both techniques for the advancement of society: a unique control mechanism and a predetermined multi-objective search. It can tell the difference between normal and abnormal traffic quite well.

TABLE I. THE DISTRIBUTION OF AWID DATA SET

	Normal	Injection	Impersonation	Flooding
AWID-CLS-R -Trn	1633190	65379	48522	48484
AWID-CLS-R -Tst	530785	16682	20079	8097

VI. PROPOSED SYSTEM

They would interact differently in their WiFi connections due to the distinct objectives of various attacks. This will shed some light on the identification framework's design. To put it another way, we can tell the difference between different types of attacks. if the deep neural networks can mine their respective WiFi connection patterns. Using this concept as a springboard, we create a framework for classifying various attacks that uses CNN as the pattern-digger. Figure 1 depicts the CNN-based attack classification system.The framework does data pre-processing, which is divided into three stages, based on the acquired and labeled data1) the retrieved original data, which may include a diverse range of input data data types, is transformed into the initial input; 2) To improve the model's identification performance, the data collected is standardised and centralised, and 3) redundant characteristics are completely removed through compression techniques to decrease the model's learning time and increasing its pattern classification effectiveness. We followed the pre-processing steps outlined in [1] and used the AWID set of statistics as an example.

The first step is to convert the unprocessed information into a system-readable format, followed by normalizing the system input data to improve the model's detection performance; and the third step is to remove or decrease unnecessary features. Extra features can be removed from the input data to

International Journal of Pharmaceutical Research and Applications
Volume 7, Issue 4 July-Aug 2022, pp: 180-185 www.ijprajournal.com ISSN: 2456-4494

reduce the feature dimension to increase the categorization effectiveness of the system. The CNN-based categorization model is the framework's second component. The network structure has one input layer, two convolutional layers, and one fully connected layer. The method of regularisation Dropout is a technique for avoiding over-fitting during the training phase. The main purpose of Dropout is to increase parameter unpredictability and decrease dependency by causing certain neurons to fail, forcing the system to communicate more infrequently..

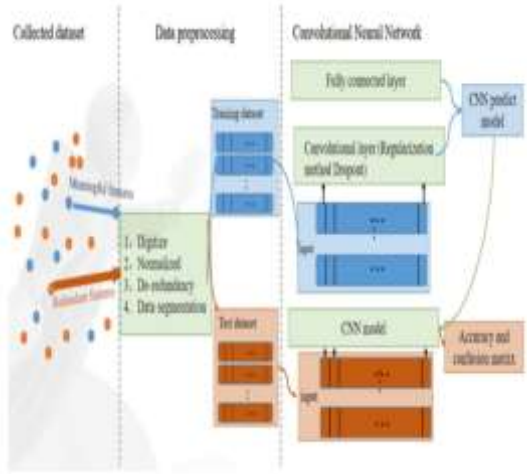

Fig1.The CNN-based attack classification system.

Algorithm 1 depicts the CNN-based framework and approach to algorithm learning.

Algorithm 1: CNN-based attack classification algorithm
Input: learning sample, network attack data to be detected
Output: CNN model, recognition rate, confusion matrix

1:**For** each *j* **do**
2: Initialize the w_j and θ_j of the network.
3: **End For**
4:**While** Termination conditions are not met
5: **For** Hidden or output layer for each unit j
6: $I_j = \sum_i \omega_j O_i + \theta_j$; // I_j is the net input
7: $O_j = 1/(1+e^{-I_j})$; // O_j is the net output
8: **End for**
9: **For** Each unit j of the output layer
10: $Err_j = O_j(1-O_j)(T_j - O_j)$;
11: $Err_j = O(1-O_j)\sum_i Err_i \omega_{ij}$;
12: **End for**
13: **For** Every ω_{ij} in the network {
14: $\Delta\omega_{ij} = (l) Err_j O_i$; // l is the learning rate
15: $w_{ij} = w_{ij} + \Delta w_{ij}$;
16: **End for**
17: **For** Each deviation θ_j in the network
18: $\Delta\theta_j = (l) Err_j$; // Deviation increment
19: $\theta_j = \theta_j + \Delta\theta_j$; // Deviation update
20: **End for**
21:**End while**

The first three phases are to initialize network parameters and set neuron thresholds.Forward propagation is depicted in steps 4-12, while reverse propagation is shown in steps 13-21.

IV. RESULTS AND DISCUSSIONS

These paragraph initially outlines the research circumstances to comparing our methodology to traditional categorization techniques in order to evaluate its performance; next, the findings are discussed, as also the influence of crucial variables.

A. Parameter Settings

As demonstrated in Section III-A, there are 45 data characteristics after preprocessing. The proposed CNN model is composed of three phases; To prevent data prediction error, the perceptron is ReLU, and the dropout approach is used. There are ten training epochs in total. There are 100 people in each session, and the training error is 0.001. After that, Algorithm 1 is utilized to check the algorithm's validity. The training nodes are used to estimate the test set, To calculate the fit ratio and confusion matrix, the predicted categories are compared to the true labels. In Table II, the CNN's specs are listed.

International Journal of Pharmaceutical Research and Applications
Volume 7, Issue 4 July-Aug 2022, pp: 180-185 www.ijprajournal.com ISSN: 2456-4494

TABLE II. CNN PARAMETER SETTINGS

	Convolution kernel size	Activation function
Input layer	100	ReLU
Convolutional layer 1	120	ReLU
Convolutional layer 2	80	ReLU
Dropout	0.5	
Fully connected layer		softmax

B. Parameter Impact Investigation

Table III shows the classification accuracy of our system with batch sizes ranging from 50 to 300.

TABLE III . RECOGNITION RATE OF DIFFERENT BATCH SIZES

Batch size	50	100	200	300
Training epochs	10	10	10	10
Recognition rate(%)	99.51	99.84	99.74	99.6
Processing time (s)	5	3	3	2

The table shows that as the batch size grows, the detection performance first rises, then falls. The recognition rate peaks at 99.84 percent When the sample size is fixed to 100, the average quantity of hours necessary for every training period reduces with time when the same settings are used. It's worth noting that increasing the scale factor won't improve the detection performance because excessively large batches will eventually settle to a localised excessive degree, lowering the rate.

C. The Effect of Nonlinear Activation Selection on Detection Performance

We apply the activation function to improve the model's generalisation capacity in order to address the inadequacies of the CNN's sequential design. The tanh, Sigmoid, and ReLU functions are the most widely utilised at the moment. These three functions' recognition rates at various iteration times are listed below. Figure 2 shows that the ReLU function as an activation function has a much faster convergence rate than the Sigmoid and tanh functions, as well as a higher recognition rate.

The overall classification effect is achieved by the ReLU function, whereas the worst is achieved by the Nonlinear function. When the training algorithm is Sigmoid, this phenomenon occurs because when the arc continues to merge, its divergence is close to zero, causing differential dispersion throughout back propagation, As a result, the identification rate is reduced due to overfitting. The ReLU function is sparse, unlike the Hyperbolic tangent convolution process, because a piece of it is presumed to be zero, resulting in no gradient variation. This is a quadratic correction function, which takes substantially less time to compute than the Gradient descent, leads to faster computational efficiency.

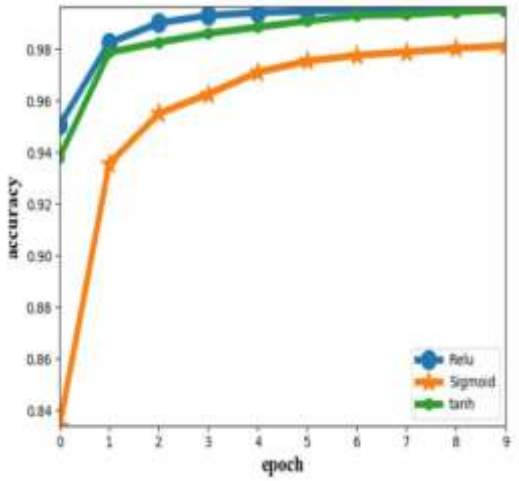

Fig2. Varying activation functions have different recognition rates.

V. CONCLUSION

This study uses a CNN model to classify assaults in WiFi wireless connections, utilising its opportunity to collect the underlying observed data provided by various attackers. To remove interference and complexity, the data is initially pre-processed. Next, the development of a CNN system will be explained. Finally, an open dataset named AWID, which was published in 2016, is used to evaluate their approach. The average detection performance of our approach for four scenarios is better than 99 percent, and it significantly beats five existing methods, according to experimental findings. In the future, In aiming to widen the usefulness of our technique, we will test it against various forms of attacks..

REFERENCES

[1]. Mustafa H, Xu W. CETAD: Detecting Evil Twin Access Point Attacks in Wireless

Hotspots[J]. 2014:238-246.
[2]. Aminanto M E, Choi R, Tanuwidjaja H C, et al. Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection [J]. IEEE Transactions on Information Forensics & Security, 2018:1-1.
[3]. Thing V L L. IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach [C]// 2017 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2017.
[4]. Qurashi M A, Angelopoulos C M, Katos V. An architecture for resilient intrusion detection in ad-hoc networks[J]. Journal of Information Security and Applications, 2020, 53:102530.
[5]. Choi J, Min A W, Shin K G. A Lightweight Passive Online Detection Method for Pinpointing Misbehavior in WLANs [J]. IEEE Transactions on Mobile Computing, 2011, 10(12):1681-1693.
[6]. Kolias C, Kambourakis G, Stavrou A, et al. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1):184-208.
[7]. Zhou Y, Cheng G, Jiang S, et al. Building an Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier[J]. 2019.
[8]. Ran, Jing & Ji, Yidong & Tang, Bihua. (2019). A Semi-Supervised Learning Approach to IEEE 802.11 Network Anomaly Detection. 1-5. 10.1109/VTCSpring.2019.8746576.
[9]. Agarwal M, Purwar S, Biswas S, et al. Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real time discrete event system[J]. IEEE/CAA Journal of Automatica Sinica, 2017.
[10]. Thing V L L. IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach[C]// 2017 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2017.