

CNN Based Cyber Defense Architecture for 802.11 Networks

Abstract

The 802.11 protocol, which forms the basis of Wi-Fi technology, enables computers, smartphones and other devices to connect to each other wirelessly via wireless local area networks (WLAN). In particular, the advent of the Internet of Things (IoT) has rendered Wi-Fi networks an indispensable component of modern connectivity. This situation is characterised by a multitude of security vulnerabilities. This study proposes a convolutional neural network (CNN) based method for the detection of cyber attacks on wireless networks. The performance of the proposed method is evaluated using Wireshark files from the AWID3 (Aegean Wi-Fi Intrusion Dataset) dataset. The following attacks were decomposed into 64 features with Tshark software; deauthentication, disassociation, (re)association, rogue AP, Krack, Kr00k, and evil twin attacks. Additionally, PCAP files belonging to the normal class in the AWID3 dataset were decomposed into 64 features. The most effective 36 features from the 64-feature dataset were selected with the InfoGain attribute evaluation algorithm. Each row of the dataset, comprising 36 features, was transformed into a 6x6 and 1-channel (grayscale) image. In the final stage of the process, the 6x6x1 dimensional images were classified using a convolutional neural network (CNN) deep learning model, resulting in an accuracy rate of 99.93%. Upon examination of the results and graphs obtained in the study, it becomes evident that the proposed model demonstrates remarkable efficacy in classifying the 8-class dataset extracted from the AWID3 dataset. Moreover, the study serves to assess the effectiveness of feature selection in the new dataset comprising 8 classes and 64 features extracted from the AWID3 dataset.

Keywords: 802.11 protocol, CNN, Image Processing, Intrusion Detection



802.11 Kablosuz Ağları için CNN Tabanlı Siber Savunma Mimarisi

Öz

802.11 protokolü, Wi-Fi teknolojisinin temelini oluşturmakta olup bilgisayarlar, akıllı telefonlar ve diğer cihazların kablosuz yerel alan ağları (WLAN) üzerinden birbirleriyle iletişim kurmasını sağlamaktadır. Özellikle Nesnelerin İnterneti (IoT) teknolojilerinin yaygınlaşmasıyla birlikte Wi-Fi ağları modern bağlantı altyapısının vazgeçilmez bir bileşeni haline gelmiştir. Ancak bu durum beraberinde çok sayıda güvenlik açığını da ortaya çıkarmıştır. Bu çalışmada, kablosuz ağlara yönelik siber saldırıların tespiti için evrimsel sinir ağı (CNN) tabanlı bir yöntem önerilmiştir. Önerilen yöntemin performansı, AWID3 (Aegean Wi-Fi Intrusion Dataset) veri setine ait Wireshark (PCAP) dosyaları kullanılarak değerlendirilmiştir. Deauthentication, disassociation, (re)association, rogue access point (AP), KRACK, KR00k ve evil twin saldırılarına ait veriler Tshark yazılımı ile 64 özelliğe ayrıştırılmıştır. Ayrıca normal sınıfa ait PCAP verileri de aynı şekilde işlenmiştir. Elde edilen 64 özellikten en etkili 36'sı InfoGain öznitelik değerlendirme algoritması ile

Research Article

10.65520/erciyesfen.1934250

Imprint:

Volume: 42(2)

Year: 2026

Page: 581-599

 Mehmet Ali Ceylan^a

 İlhan Firat Kilincer^{b*}

 Fatih Ertam^c

^a Digital Forensics Engineering, Firat University, maceylan35@gmail.com

^b Digital Forensics Engineering, Firat University, ifkilincer@firat.edu.tr

^c Digital Forensics Engineering, Firat University, fatih.ertam@firat.edu.tr

* Corresponding Author

Received: 4/20/2026

Accepted: 6/13/2026

Citation:

Mehmet Ali Ceylan, İlhan Firat Kilincer, Fatih Ertam (2026). CNN Based Cyber Defense Architecture for 802.11 Networks. *Erciyes University Journal of Institute Of Science and Technology*, 42(2), 581-599. <https://doi.org/10.65520/erciyesfen.1934250>

Screened by



Except where otherwise noted, content in this article is licensed under a Creative Commons 4.0 International license. Icons by Font Awesome.

seçilmiştir. Otuz altı özelliğten oluşan her veri satırı 6x6 boyutunda ve tek kanallı (gri seviye) görüntüleri dönüştürülmüştür. Son aşamada, 6x6x1 boyutlu bu görüntüler CNN tabanlı derin öğrenme modeli ile sınıflandırılmış ve %99,93 doğruluk oranı elde edilmiştir. Elde edilen bulgular, önerilen modelin AWID3 veri setinden türetilen 8 sınıflı veri üzerinde yüksek başarıyla sınıflandırma gerçekleştirdiğini göstermektedir. Ayrıca çalışma, 64 özelliğten 36 özelliğ indirgenen veri setinde öznetelik seçiminin model performansı üzerindeki etkisini ortaya koymaktadır.

Anahtar kelimeler: 802.11 Protokolü, Evrişimsel Sinir Ağları, Görüntü İşleme, Saldırı Tespiti



1.Introduction

With the widespread adoption of IoT (Internet of Things) applications and wireless communication in recent years, technology has become an indispensable element in almost every aspect of our daily lives [1], [2]. This situation, which provides many conveniences in our daily lives, also brings many security vulnerabilities. As the areas where technology is used increase, the cyber attack surface expands in parallel. For this reason, cyber security has gained great importance and has become an active research area. Cyber security ensures the security of information systems, the data stored in these systems and the services provided by these systems that can be accessed without authorization [3], [4].

Advances in modern computer networks and security applications are not sufficiently powerful to detect and prevent all cyber-attacks. Although traditional technologies such as firewalls, authentication mechanisms and cryptographic methods are widely used to detect cyber attacks, contemporary cyberattacks cannot be completely prevented by these mitigation techniques. Therefore, IDS (Intrusion Detection Systems) mechanisms are used to detect cyber attacks when conventional security technologies become insufficient. IDS systems analyze incoming and outgoing network traffic in depth and are designed to identify suspicious activities in a timely and accurate manner. Anomaly-based IDS systems, one of the IDS systems that have become an indispensable element of today, record normal network behavior. They generate alarms when there is a deviation in normal network behavior. Anomaly-based IDS systems utilize artificial intelligence methods to detect abnormal network traffic. For this reason, it has become a highly popular research area in both cyber security industry and academia [5]–[9].

Wi-Fi networks are among the most widely used technologies for wireless data communication by smartphones, personal computers and various IoT devices. Operating mainly at 2.4 GHz and 5 GHz frequencies, Wi-Fi networks provide high bandwidth and significant convenience for end users. However, despite their widespread use and convenience, Wi-Fi networks also introduce many security risks. Unencrypted and publicly accessible Wi-Fi networks used in places such as cafes and shopping centers to attract customers may lead to serious data breaches. Such public Wi-Fi networks, which do not require authentication are highly insecure, especially for sensitive data exchange [10], [11]. Data breaches in wireless networks have led researchers to develop Wireless IDS (WIDS). In this study, a novel method for detecting cyberattacks in wireless networks is proposed. The main contributions of the proposed method are summarized below;

- In the proposed method, the PCAP files in the AWID3 (Aegean Wi-Fi Intrusion Dataset) dataset were analyzed and a new dataset was created by extracting only the features related to Wi-Fi attacks.
- Instead of using all 254 features in the AWID3 dataset given as CSV format, the most significant 64 features representing Wi-Fi attacks were identified and these features were extracted from the PCAP files using the tshark tool.
- Each row of data was transformed into an image using the extracted features. Subsequently, the dataset was trained using CNN, one of the deep learning methods, and a highly successful model was developed for detecting attacks occurring in wireless networks, achieving an accuracy rate of up to 99.93%.

The high success rate in the study demonstrates that how accurately the features in the extracted from dataset were selected. Moreover, the proposed CNN-based model demonstrated the effectiveness of image-based processing for classification in WIDS models and provided a new perspective for researchers in this field. The remaining sections of the paper consist of Related Works, Background, Proposed Method, Experimental Results and Discussion and finally Conclusion and Future Works.

2. Related Works

With the widespread use of Wi-Fi networks, the number of attacks targeting these networks has also increased significantly. Detecting Wi-Fi attacks requires WIDS systems to remain in a state of perpetual evolution and adaptation. Numerous studies have contributed to the advancement of WIDS systems. Wang et al. [12] made significant strides in this field by utilizing Stacked Autoencoder (SAE) and Deep Neural Network (DNN) to protect Wi-Fi networks against cyber threats using the AWID-CLS-R-Trn and AWID-CLS-R-Test datasets. The AWID-CLS-R dataset used in their study contains data in four different classes: impersonation attack, injection attack, flooding attack and normal records. Thing et al. [13] classified AWID-CLS-R datasets using SAE algorithm in their study.

Wang et al. [14] proposed the Wi-Alarm model for the detection of attacks occurring in Wi-Fi networks. In their proposed Wi-Alarm model, it sends alarms to users with Wi-Fi signals in case of intrusion. In the model, CSI samples obtained with Channel State Information (CSI) tool are tested with a Support Vector Machine (SVM) based algorithm. Tian et al. [15] proposed Adaptive Indoor Passive Intrusion Detection (APID) system for Wi-Fi intrusion detection using CSI information of Wi-Fi signals. Satam et al. [16] introduced a WIDS system that is highly effective in identifying Wi-Fi attacks, delivering impressive accuracy and minimizing the risk of false alarms. In their study, normal user behavior in Wi-Fi network is modeled using n-grams. They tested their proposed model with machine learning methods and used the AWID-ATK-R dataset for the tests. Salah et al. [17] in addition to providing a comprehensive review of IDS systems, proposed a method for detecting anomalies in 5G and IoT environments using Machine Learning (ML) algorithms. In their proposed method, they used the AWID3 dataset, which is the first wireless dataset designed for wireless network security, focusing on the IEEE 802.11 standard. They also used feature selection approaches to improve the performance of their proposed model.

Zhou et al. [18] used the CFS-BA algorithm for feature selection based on the correlations among features in intrusion detection systems. In their study, they classified NSL-KDD, CIC-IDS2017, and AWID-CLS-R datasets with C4.5, Forest by Penalizing Attributes (Forest PA), and Random Forest (RF) algorithms. Wi-Fi networks, which are widely used today, bring great convenience to users, but they are also highly susceptible for manipulating users. One of the most prevalent methods of tricking users into compromising their security is the Evil Twin attack, which involves setting up a fraudulent Wi-Fi network that imitates a legitimate one. Silva et al. [19] proposed a method to detect Evil Twin attacks that frequently occur in Wi-Fi networks using the AWID3 dataset. In their proposed method, the dataset is subjected to various preprocessing steps and subsequently classified with the LightGBM algorithm. Normal traffic and Evil Twin attack classes were used in the classification. Aminanto et al. [20] used Artificial Neural Network (ANN) as a feature selector and SAE algorithm as a classifier to optimize their previously proposed method to detect impersonation attacks in the AWID dataset.

Duan et al. [21] classified the AWID-CLS-R dataset using CNN algorithm for the detection of attacks in wireless networks. Koliass et al. [22] used ML based classification methods to detect intrusions in wireless networks. They tested the performance of their proposed method on AWID-CLS and AWID-ATK datasets. Rezvy et al. [23] used DNN algorithm to anomaly detection in 5G and IoT networks. AWID dataset was used for performance evaluations. Aminanto et al. [24] classified AWID dataset using Unsupervised Stack Autoencoder and k-means clustering algorithms for intrusion detection in wireless networks.

Although there are numerous studies in the literature on intrusion detection in wireless networks, most of the literature studies have not analyzed the attack traffic on wireless networks in detail. In this study, in order to fill this gap in the literature, PCAP files of attacks on wireless networks

in the AWID3 dataset are analyzed separately and features specific to wireless attacks are extracted. In addition, most of the studies in the literature are ML based and it is thought that they cannot perform adequately in very large datasets. Therefore, a deep learning based CNN model is proposed in this study.

3. Background

3.1. AWID3 Dataset

As an augmentation of the AWID2 dataset, this dataset is specifically designed to detect vulnerabilities in Wi-Fi networks fortified with the IEEE 802.1X Extensible Authentication Protocol (EAP). In addition, the dataset is the first comprehensive empirical study that provides information about the IEEE 802.11w protocol, which is mandatory for Wi-Fi Protected Access (WPA3) certified devices. The testbed for the AWID3 dataset utilizes a total of 16 different physical devices and virtual machines to realistically emulate the enterprise network infrastructure. Various attacks, including Deauthentication, Rogue AP, Disassociation, Evil Twin, (Re)Association, SQL Injection, Kr00k, SSH Brute Force, Malware, Krack, Botnet, SSDP, and Website spoofing attacks were implemented in the AWID3 test environment. The PCAP files obtained during the attacks were shared publicly. In addition, the PCAP files obtained from WIDS were parsed and saved in CSV format. Parsing the PCAP files resulted in the extraction of 254 features; however, not all features were filled in every attack file [25]. In the AWID3 dataset, most of the wireless network attacks that may be encountered in real-life Wi-Fi networks are addressed. Brief descriptions of these attacks is given below.

Deauthentication attack: A type of cyber attack on a Wi-Fi network to disconnect the target device from the Access Point (AP) [26].

Disassociation attack: A type of DoS (Denial-of-Service) attack targeting Wi-Fi network. The attacker launches a deceptive maneuver by sending a fraudulent message to the AP, spoofing the target's credentials (MAC address). This trickery prompts the AP to terminate the connection of the client with the target MAC address [17], [26], [27].

Reassociation attack: A type of cyberattack in which the attacker uses false credentials or jamming techniques to prevent or manipulate the target client device from reconnecting to the AP in a wireless Wi-Fi network [17], [26], [27].

Rogue AP attack: The attacker attracts users by setting up a fake AP and broadcasting a broadcast similar to the real Wi-Fi network broadcast on this AP. Thus, the attacker tries to steal the user information of the target users [28], [29].

Krack (Key Reinstallation) attack: It is a replay attack against the WPA2 (Wi-Fi Protected Access 2) security protocol, which is widely used in wireless Wi-Fi networks. This attack exploits a vulnerability in the WPA2 protocol that allows an attacker to disrupt the communication between the target device and the Access Point (AP). [30].

Kr00k attack: Found in 2019 by ESET, uncovering a security flaw known as Kr00k that could potentially decrypt Wi-Fi traffic protected by WPA2 [31].

Evil Twin attack: Attacker creates a fake AP on a Wi-Fi network with similar characteristics to the real network and forces users to connect to the fake network. As a result of the attack, users' data may be stolen or network traffic can be manipulated [17], [27], [32].

SSH brute force attack: Attacker aims to gain unauthorized access to an SSH server using a combination of username and password. The attacker tries different username and password combinations using an automated tool or manually [33].

Botnet attack: It is a type of attack that hackers carry out using a network of compromised computers or systems. These compromised computers are called bots or zombie computers. Attackers can use these compromised computers as a tool for fraud, ransomware attacks, DoS or DDoS attacks and other malicious activities [34].

SSDP Amplification attack: It is caused by a vulnerability in the Universal Plug and Play (UPnP) protocol. It is a type of cyberattack by sending an excessive amount of traffic to a target system. The attacker redirects spoofed SSDP requests from multiple devices, increasing the response time of the target system [35].

SQL injection attack: It is when an attacker manipulates a database by injecting malicious SQL commands into a web application or database. In this type of attack, data may be stolen, modified or deleted using SQL commands [36].

Website spoofing attack: It is a type of cyberattack to steal credentials, credit card information or other sensitive data by redirecting users to a fake website. In this attack, the attacker creates a website that mimics the appearance and function of a legitimate website and then redirects users to this fraudulent website through various techniques[37].

3.2. Info Gain Attribute Evaluations

In the context of data mining processes, the identification of significant information within datasets is a recurrent concern. In this study, an attempt is made to determine the most significant features in the dataset with a method called information gain (IG). The IG method provides a more profound comprehension of the data by quantifying the extent to which a feature elucidates the classification problem [38]. In this study, the IG algorithm was utilized to select the most effective 36 features from a total of 64 features obtained from PCAP files. The rationale behind this selection is that these features are characterised by minimal information entropy, thus defining the purest subsets for the designated classification task. Consequently, the decision tree algorithm attains an optimal solution in a less complex and faster manner.

3.3. CNN

CNN, which is a cornerstone of image processing, is a sophisticated deep learning algorithm that deciphers visual information. This neural network model, adept at categorizing images based on their distinctive features, comprises Convolutional, Pooling, and Fully Connected layers. Images are prepared for the deep learning model by subjecting them to various processes in each layer [39]–[41].

The Convolutional Layer, which is the core component of CNNs, acts as a feature extractor, meticulously identifying the salient characteristics of images. By applying specialized filters, this layer extracts both low-level and high-level details within the visual data. The input of the convolutional layer consists of an image of size $m \times m \times r$, where m represents the image's height and width of the image and r denotes the number of channels. For example, in an RGB image $r = 3$, while in a greyscale image $r = 1$. Therefore, for $n < m$ and $q \leq r$, the convolution layer will be a filter of size $n \times n \times q$. The images used in the study are greyscale and have dimensions of 6x6. Each image consists of one row of a 64-feature dataset extracted from the AWID3 dataset [42].

Pooling, a layer often added between successive convolutional layers in a Convolutional Network (CovNet), aims to reduce the size of the images and summarize important features. This reduces the computational burden and increases the generalization ability of the model. There are many pooling operations, but the most popular is max pooling. The equations of the Relu activation function and max pooling, which are widely used in CNN, are given in Equation 1 and Equation 2, respectively [42].

$$y_{ijk} = \max(0, X_{ijk}) \quad (1)$$

$$y_{ijk} = \max(y_{i'j'k'}, : i \leq i' < i + p, j \leq j' < j + q) \quad (2)$$

Neural networks receive their input data from a one-dimensional array. Therefore, the purpose of the flattening layer in CNN is to prepare the input data of the Fully Connected Layer. The flattening layer is a process used in neural networks to transform multidimensional data into a one-dimensional vector. The CNN model used in the study is given in Figure 1.

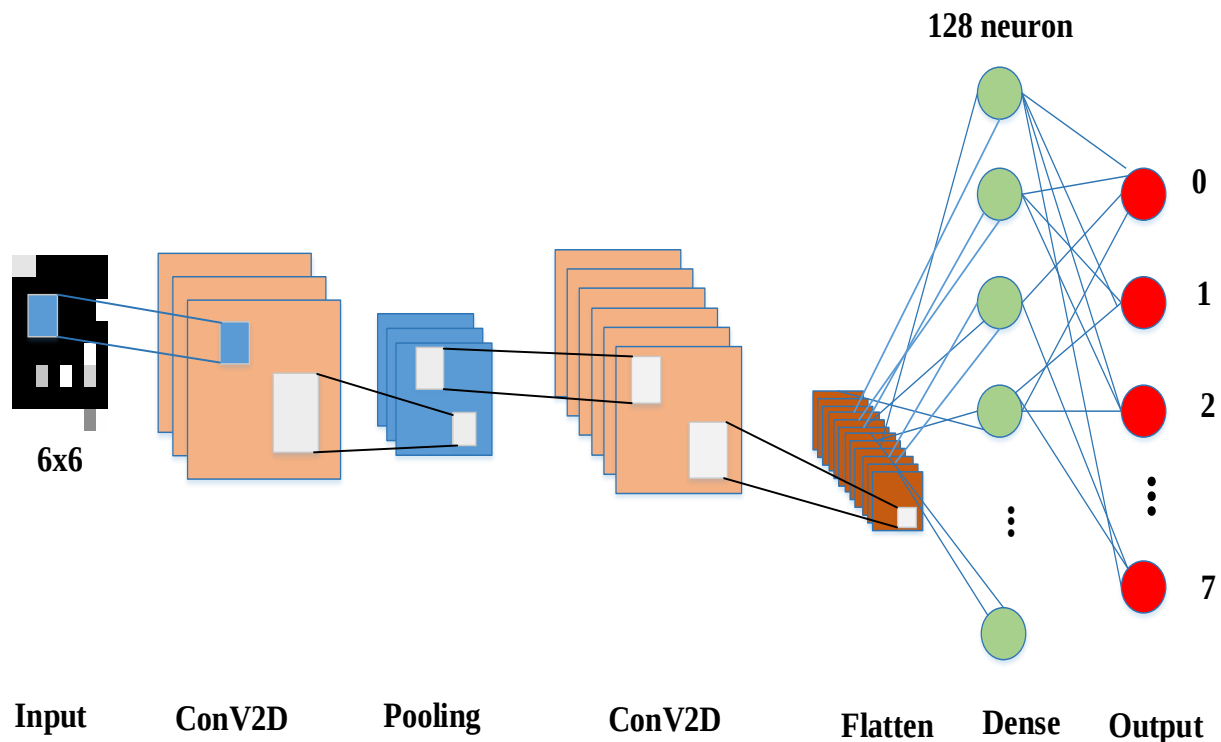


Figure 1. Proposed CNN model

The proposed CNN architecture, illustrated in Figure 1, comprises two Convolutional layers, one Pooling layer, one Flatten layer, and two Fully Connected (Dense) layers. The model processes 6x6 grayscale images as input. In this study, rather than feeding the 36 features extracted from the AWID3 dataset directly into classical classifiers, these features were converted into 6x6 grayscale images. The primary purpose of this transformation is to convert the features of network packets from simple numerical values into structural patterns that can be effectively interpreted by the model. Traditional machine learning algorithms tend to treat each feature as an independent input. In this study, the data is converted into images, and an artificial neighborhood relationship is established between features located close together. This allows the CNN to learn local patterns and nonlinear correlations between these pixels much more effectively through “kernel” filters. Furthermore, the superiority of the proposed CNN-based model over classical machine learning algorithms such as Support Vector Machine (SVM), Decision Tree (DT) and Random Forest (RF) has also been demonstrated by the results presented in Table 4.

4. Material and Method

4.1. Dataset Preparation

The AWID3 dataset provides a comprehensive perspective for WIDS systems and contains numerous types of attacks. However, SQLi, Website spoofing, Malware, Botnet, SSH Brute Force and SSDP attacks are not specific attacks for Wi-Fi networks. Since these attacks can be applied on any Ethernet network, the data of these attacks are not considered in this study. In this study, only Deauthentication, Disassociation, Krack, (Re)Association, Kr00k, Rogue AP and Evil Twin attacks on Wi-Fi networks are discussed. The dataset preparation process is illustrated in Figure 2.

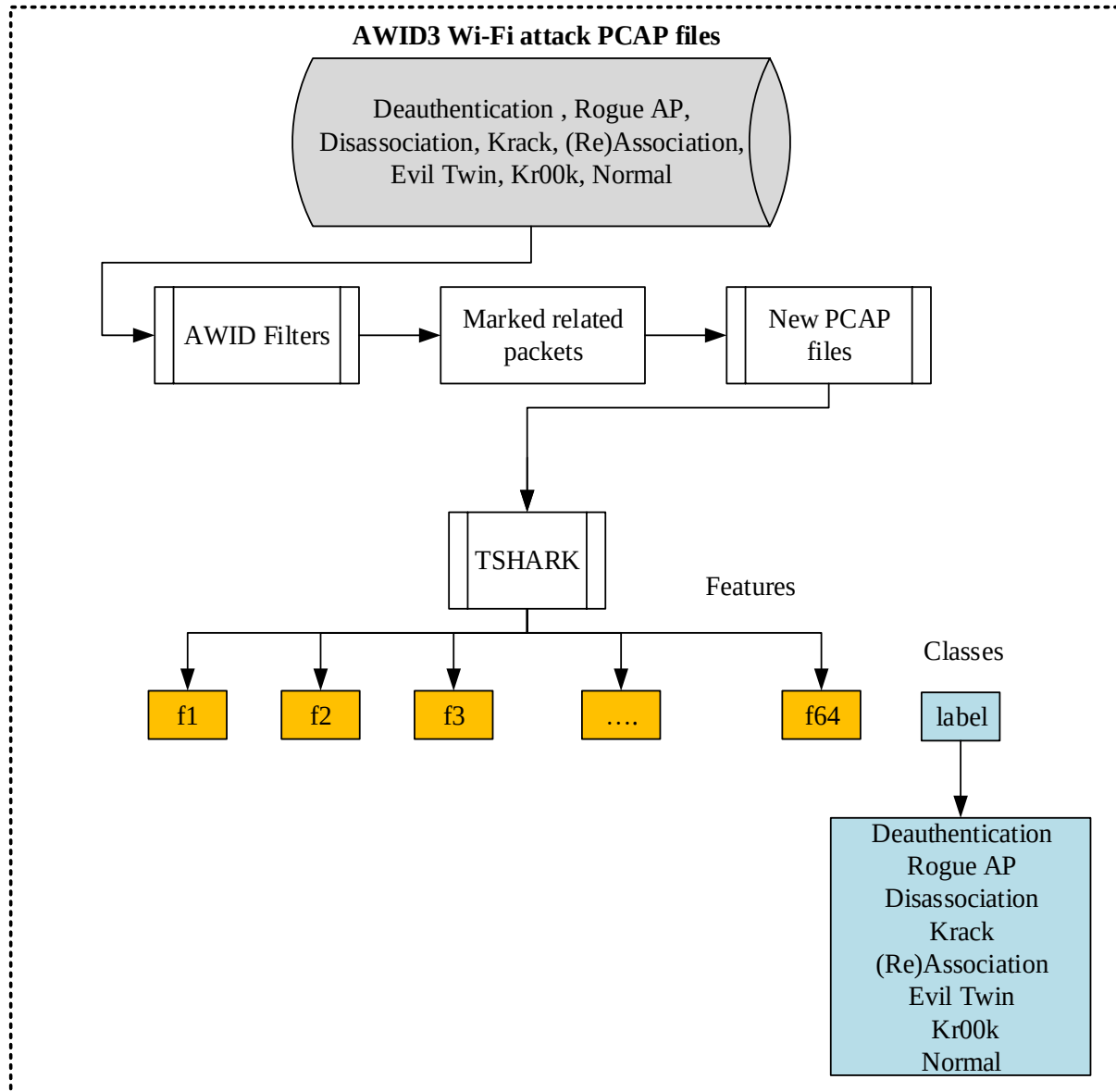


Figure 2. Dataset Preparation

Figure 2 illustrates the steps of creating the proposed dataset extracted from the PCAP files of attack types related to Wi-Fi networks in the AWID3 dataset. Accordingly, since each Wi-Fi attack PCAP file contains normal network traffic as well as attack packets, filters indicating the relevant attack were used and the data packets obtained as a result of these filters were marked in Wireshark and saved as a new file. The filters for the packets of each attack are provided on the AWID3 website [43]. Each PCAP file was analyzed separately and the 64 most appropriate packets indicating Wi-Fi attacks were identified and parsed into features with the Tshark tool. The PCAP files parsed into features with Tshark were converted into CSV files and all attack types were labeled by merging all CSV files. In addition, packets belonging to normal network behaviors were filtered and included in the dataset under the "Normal" label. As a result, a dataset consisting of 64 features and 8 classes (Deauthentication, Rogue AP Disassociation, Krack, (Re)Association, Evil Twin, Kr00k, Normal) was extracted. The 64 features extracted from AWID3 Wi-Fi attack packets are given in Table 1.

Table 1: Features extracted from AWID3 dataset

frame.len	radiotap.present.dbm_tx_power	radiotap.flags.fcs	wlan.fc.moredata
frame.cap_len	radiotap.present.antenna	radiotap.flags.data pad	wlan.fc.protected
frame.marked	radiotap.present.db_ant signal	radiotap.flags.badfcs	wlan.fc.order
frame.ignored	radiotap.present.db_ant noise	radiotap.flags.shor tgi	wlan.duration
radiotap.version	radiotap.present.rxflags	radiotap.datarate	wlan.frag
radiotap.pad	radiotap.present.xchannel	radiotap.channel.f req	wlan.seq
radiotap.length	radiotap.present.mcs	radiotap.dbm_ant signal	wlan.ba.control.ack policy
radiotap.present.tsft	radiotap.present.ampdu	radiotap.antenna	wlan.wep.key
radiotap.present.flags	radiotap.present.vht	radiotap.rxflags.ba dplcp	wlan.qos.tid
radiotap.present.rate	radiotap.present.rtap_ns	wlan.fc.type_subt ype	wlan.qos.priority
radiotap.present.channel	radiotap.present.vendor _ns	wlan.fc.version	wlan.qos.eosp
radiotap.present.fhss	radiotap.present.ext	wlan.fc.type	wlan.qos.ack
radiotap.present.dbm_ant signal	radiotap.mactime	wlan.fc.subtype	wlan.qos.txop_dur _req
radiotap.present.dbm_ant noise	radiotap.flags.cfp	wlan.fc.ds	data.len
radiotap.present.lock_quali ty	radiotap.flags.preamble	wlan.fc.frag	
radiotap.present.tx_attenu ation	radiotap.flags.wep	wlan.fc.retry	
radiotap.present.db_tx_atte nuation	radiotap.flags.frag	wlan.fc.moredata	

While preparing the dataset, attention was paid to ensure that all the selected features are the features that show Wi-Fi network traffic. As a result of the dataset preparation process, the features of the new dataset produced from the AWID3 dataset are given in Table 2.

Table 2: New dataset driven from AWID3

Confusion matrix number	Class	Data count	Data Count After SMOTE
0	Deauthentication	6600	7313
1	Disassociation	6667	7319
2	Evil Twin	7321	7318
3	Kr00k	5903	7317
4	Krack	6449	7321
5	Normal	5674	7315
6	Rogue AP	1310	7321
7	Reassociation	5503	7313
	Total	45427	58537

The new dataset extracted from the AWID3 dataset consists of a total of 58537 lines of data. When examining the data volumes for each attack class in the dataset, it is observed that, generally, the data volumes are similar to each other, except for the Rogue AP class. To address the data imbalance problem, synthetic data was generated using the Synthetic Minority Over-sampling Technique (SMOTE) algorithm. The SMOTE algorithm increases the number of minority data points by creating a synthetic bridge between existing data points. Initially the algorithm selects a random sample from the minority group and identifies its closest similar neighbors (k-nearest neighbors). Subsequently, it creates a virtual vector between this selected main data point and one of its neighbors. A new artificial data sample is generated at a random point on this vector. In this way, the model avoids memorizing data and completes missing data with logical predictions [44], [45]. The SMOTE algorithm was chosen for this study because of these advantages. Finally, the data from all attack scenarios was merged into a single CSV file.

4.2. Proposed Method

The new dataset extracted from the AWID3 dataset, which contains many current Wi-Fi attacks, is used to propose a CNN-based method to improve the intrusion detection capability of WIDS systems. This study aims to address cyberattack detection as a pattern recognition problem by remodeling network data as 6x6 pixel grayscale matrices. The proposed CNN-based WIDS system consists of four phases and is summarized in Figure 3.

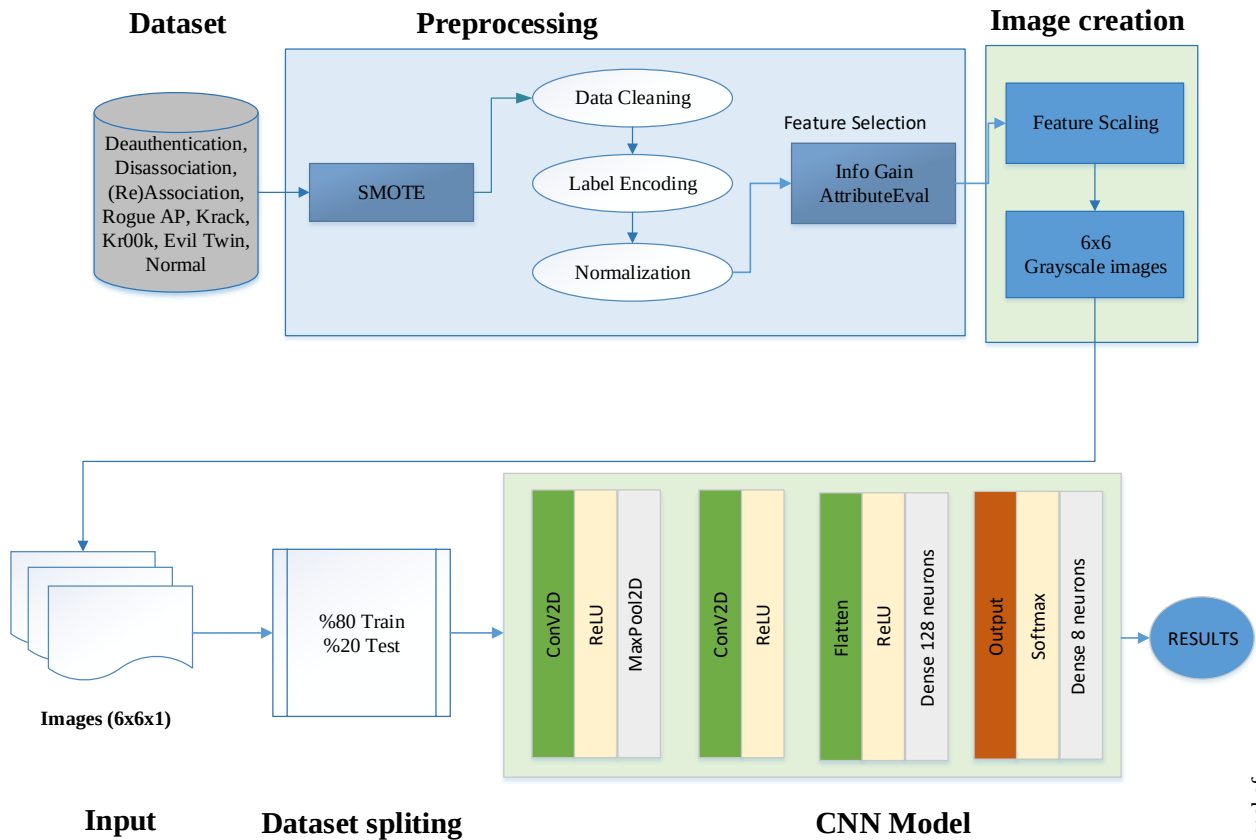


Figure 3. Proposed method

As illustrated in Figure 3, the dataset obtained solely from the PCAP files of Wi-Fi attacks underwent a pre-processing phase. As can be seen in Table 2, there is data imbalance between the classes. To address the data imbalance problem in the dataset, synthetic data was generated in the attack classes with a small number of data points using the SMOTE algorithm in the first stage of the preprocessing process. After generating the synthetic data, the null (NaN) values in the dataset were

replaced with the average of the existing data in each column. The categorical variables in the dataset were digitized by encoding them with the LabelEncoder in the Scikit-Learn library, and then the dataset was normalized with min-max normalization. The final stage of the pre-processing step involved the selection of the most effective features. The selection of the most informative features in the dataset, and the features that best affect the model's predictions, is critical to the model's performance. Furthermore, the purification of the dataset from unnecessary features has been demonstrated to reduce the prediction time of the artificial intelligence model and to provide results in a substantially more expeditious manner. In this study, the Info Gain Attribute Evaluations algorithm was utilised to identify the most effective features from 64 features extracted from PCAP files in the AWID3 dataset. The proposed feature selection algorithm was employed to select 36 features, with each feature being weighted. The features and impact values obtained as a result of the Info Gain Attribute Evaluations feature selection algorithm are visualized in Figure 4.

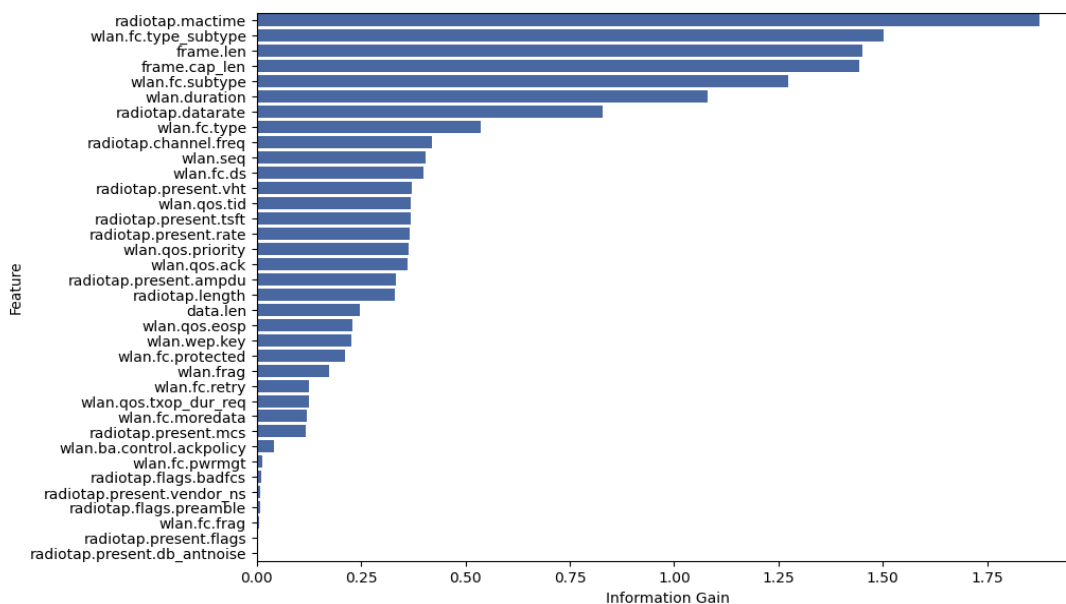


Figure 4. Feature Importance based on Information Gain

The effectiveness of the AWID3 dataset in simulating real-world network traffic has been widely demonstrated in the literature. Although packets extracted from the same PCAP file may have similar header structures, the InfoGain-based feature selection strategy we applied in this study minimizes this generalization. In this process, the discriminatory power of the data was maximized by focusing on 36 critical features that best represent the temporal and behavioral characteristics that distinguish seven different attack types from normal network traffic. Subsequent to the pre-processing phase, in the image creation phase, the features were scaled to the range of 0-255 to create an image from each row of data. In this stage, the data scaled to the range of 0-255 were converted to 6x6 image files. The grayscale images obtained from each row of data were stored in different folders as 80% training and 20% test data. Furthermore, a file-based separation process was implemented in our study to prevent data leakage. Accordingly, the data was first organized into folders according to their classes, and then each class was randomly shuffled and copied to physically different directories with 80% training and 20% testing data.

In the last stage, the grayscale images in the training and testing folders were subjected to classification with the CNN algorithm proposed in the study. The input of the proposed CNN model consists of 58537 6x6 and 1-channel (grayscale) images generated from 58537 rows of data. The initial layer of the model employs a Convolutional layer to extract salient features from the input images. This layer utilizes 32 filters, each measuring 3x3 to process the incoming 6x6 images. A ReLU activation function is applied within the Convolutional layer to introduce nonlinearity. In the pooling layer,

MaxPooling2D was used. In this layer, it selects the maximum value from each feature map using a 2x2 window. This reduced the size of the feature maps, lowered the computational cost and made the model more robust to small translations. In the subsequent Convolutional layer, 64 filters of size 3x3 are applied to extract more complex features from the images. A ReLU activation function is employed to introduce nonlinearity and enhance the model's ability to learn from the data. In the Flatten layer, the multidimensional feature maps are reduced to a one-dimensional vector and thus become input to the Fully Connected (Dense) layer. In the dense layer, 128 neurons are used to learn and model complex relationships from the data. ReLU was used as the activation function. In the last layer, the output layer, since the dataset consists of 8 classes, there are 8 neurons and the Softmax activation function is used.

5. Experimental Results

In this study, the dataset obtained from the PCAP files of the AWID3 dataset was tested on a computer equipped with an Intel I7 processor, 32GB of RAM, and the Python programming language. Details regarding the training process, hyperparameter choices, and technical environment used for the proposed CNN model are presented in Table 3.

Table 3. CNN parameters for classification

Parameters	Explanation
Optimizer	Adam
Learning Rate	0.001
Loss Function	Categorical Crossentropy
Batch Size	32
Epoch	30
Activation Functions	ReLU in the hidden layers, Softmax in the output layer
Validation Split	%20
Input Shape	6x6x1

In this study, the dataset extracted from the AWID3 dataset created for anomaly detection in Wi-Fi networks and containing only Wi-Fi attacks was processed according to the flowchart given in Figure 3. Validation data was generated from 20% of the images obtained from the dataset. Accuracy (Acc), Precision (Pr), Recall (R) and F1 Score (F1) metrics were measured to evaluate the performance of the proposed method. The order of the equations of the performance metrics used are given in Equations 3, 4, 5 and 6 [40], [46], [47].

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$Pr = \frac{TP}{TP+FP} \quad (4)$$

$$R = \frac{TP}{TP+FN} \quad (5)$$

$$F1 = 2 * \frac{Pr * R}{Pr + R} \quad (6)$$

In the equations, TP represents True Positive, TN denotes True Negative, FP signifies False Positive, and FN indicates False Negative predictions. The results obtained from the proposed method and traditional machine learning algorithms are presented in Table 4.

Table 4. Performance evaluation (%)

Method	Acc	Pr	R	F1-Score
SVM	97.61	97.78	97.56	97.64
RF	92.87	92.25	92.87	92.56
DT	93.34	91.13	93.34	92.04
Proposed method	99.93	100	99.96	99.98

As can be seen from Table 4, the proposed method achieved an accuracy rate of 99.93% in detecting Wi-Fi attacks. The traditional machine learning models used in this study were structured with optimized hyperparameters to prevent overfitting and to build more generalized structures in high-dimensional data. Accordingly, the RF model was established with 20 decision trees ($n_estimators=20$) to increase stability, a maximum depth of 2 ($max_depth=2$) to limit complexity, at least 2 splitting samples ($min_samples_split=2$) to control branching, a minimum of 4 samples per leaf ($min_samples_leaf=4$), and a square root-based feature subset selection ($max_features='sqrt'$) to narrow the feature space. In the SVM model, which was trained with a strong regularization strategy, a low penalty coefficient ($C=0.1$) was preferred to increase tolerance to error margin and prevent overfitting, a sigmoid kernel was used to detect nonlinear boundaries, and a dynamically sensitive scale parameter ($gamma='scale'$) was chosen to match the data dimensionality. Finally, in the DT model, a maximum depth of 4 ($max_depth=4$) was applied to prevent excessive deepening, a minimum number of splits of 10 ($min_samples_split=10$) was used to prevent branching with insufficient samples, a minimum of 4 samples per leaf node ($min_samples_leaf=4$), and a feature subset constraint ($max_features='sqrt'$) was implemented; additionally, thanks to the cost-complexity pruning coefficient ($ccp_alpha=0.005$) added to the model, unnecessary branches of the tree were pruned, maximizing the generalization ability of the model. DT and its ensemble version, RF algorithms, struggle to distinguish the line between signal and noise when working with high-dimensional data spaces; while DT makes strict splits from a single tree, RF selects random feature subsets for each tree, leading to irrelevant features dominating the decision-making mechanisms as the data size increases. In these models, high performance can be achieved by updating hyperparameters such as max_depth , $min_samples_split$, and $min_samples_leaf$; however, this intervention eliminates the model's flexibility, directly leading to overfitting. The proposed CNN overcomes this dimensionality crisis through convolutional layers, processing high-dimensional raw data hierarchically; starting from low-level edges, it creates progressively more abstract representations, deciding which features are important through learnable filters. In this process, unnecessary information is automatically suppressed, so while increasing dimensionality can cause tree-based models to collapse and fall into the overfitting trap, unlike CNN, it allows for the learning of richer patterns, and the 99.93% success rate achieved by the proposed method demonstrates that it overcomes the disadvantages of traditional models in high-dimensional data.

Table 5. Class by class performance evaluations

Method	Pr	R	F1-Score
EvilTwin	1.00	1.00	1.00
Disass	1.00	0.9966	0.9983
Deauth	0.9966	0.9979	0.9973
Krack	1.00	1.00	1.00
Kr00k	0.9980	1.00	0.9990
Normal	1.00	1.00	1.00
ReAssoc	1.00	1.00	1.00
RogueAP	1.00	1.00	1.00

Tables 4 and 5, which demonstrate the success of the proposed method in detecting Wi-Fi attacks, show that the model exhibits high stability both overall and class-based. According to the overall performance data, the proposed CNN-based method achieved a very high accuracy rate of 99.93%. The data in Table 5, which shows the class-based performance values, supports this success; while 100% accuracy and sensitivity are achieved against critical attack types such as EvilTwin, Krack, and RogueAP, it is observed that the F1-Score values remain above 99% even in classes such as Disass and Deauth, where the margin of error is extremely low. These results prove that the developed method has both high sensitivity against various network attack vectors and keeps the false alarm rate at a minimum level. Confusion matrix obtained in model training is given in Figure 5.

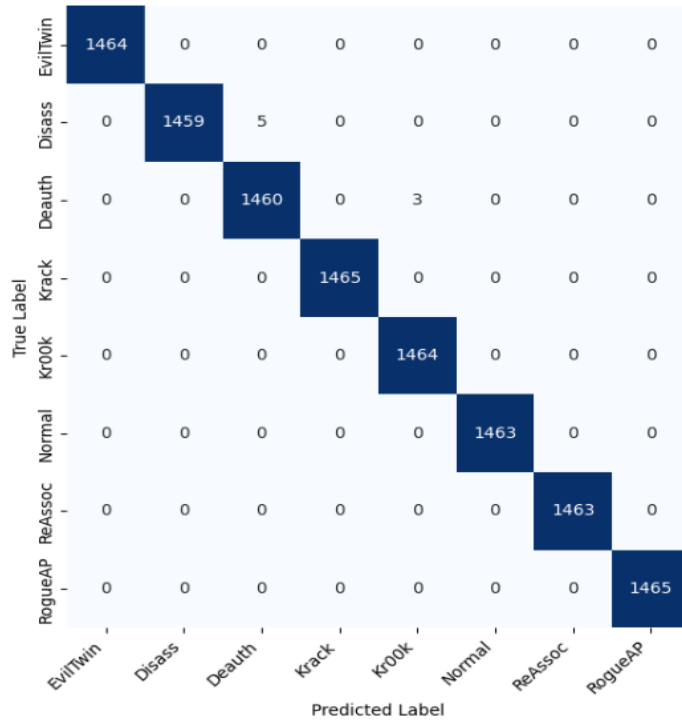


Figure 5. Confusion matrix of proposed method

In the test phase of the proposed method, 30 epochs were used. The training and validation loss and training and validation accuracy graphs obtained according to the epoch value are given in Figure 6.

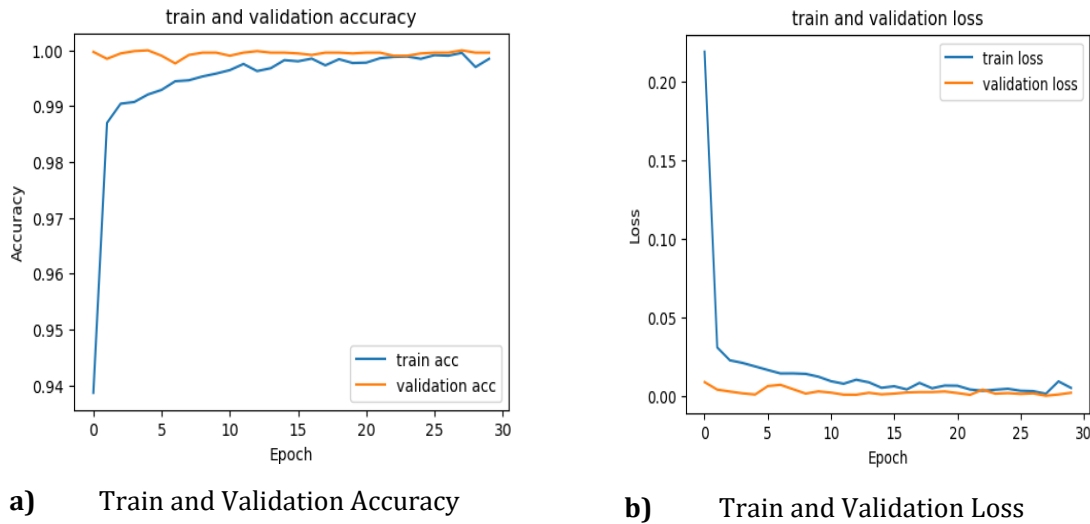


Figure 6. Proposed method results

As can be seen in Figure 6, the training loss line decreases steadily during the first 15 epochs, while the training accuracy line starts with an accuracy value of 0.94 and increases steadily during the first 15 epochs. The training accuracy graph then starts to stabilize and reaches a maximum value of around 0.995. This indicates that the model learns well from the training data. The validation accuracy (validation acc) line remain approximately within the range 0.99 - 1.00, indicating that the model successfully classifies the validation data.

The training loss line starts around 0.2 and decreases steadily during the first 20 epochs. It then starts to stabilize and reaches a minimum around 0.02. This demonstrates that the model learns well from the training data. The Validation Loss line remains within the range 0.00 - 0.05. This graph indicates that the model successfully generalizes to the validation data with minimal loss. The gap between training and validation loss is relatively small throughout the training process. This indicates that the model does not overfit the training data. The high performance achieved by the proposed model stems from the conversion of tabular data into 6x6 grayscale images. CNNs are inherently superior at capturing spatial correlations and patterns that traditional machine learning models might overlook. Furthermore, the InfoGain algorithm used in the study effectively eliminated noisy features. The resulting 36 features, when visualized as images, reveal a dataset where classes exhibit distinct structural patterns.

In general, the graphs indicate that the proposed model classifies the data with high accuracy and low loss. In addition, the graphs indicate that there is no overfitting in the proposed model. The model is able to learn from the training data and generalizes well to the validation data. In summary, the graphs are a good indication that the model performs well and can classify invisible data with high performance.

6. Discussion

In this study, a new dataset with 64 features and 8 classes was extracted from by parsing the PCAP files of attacks specific to Wi-Fi networks in the AWID3 dataset. Each row of data in the obtained dataset was converted into an image file and processed with a CNN-based deep learning model and accuracy values reaching 99.93% were obtained for WIDS systems. Some of the literature studies on WIDS systems are given in Table 6.

Table 6. Literature view about WIDS systems

Referance	Dataset	Method	Classes	Accuracy(%)
[12]	AWID-CLS-R	DNN	Normal	98.46
			injection	99.99
			impersonation	98.39
			flooding	73.12
[13]	AWID-CLS-R	SAE	Normal	99.80
			injection	82.71
			impersonation	57.47
			flooding	98.49
[16]	AWID-ATK-R	ML	4 class (Over all accuracy)	98.80
[17]	AWID3	Logistic Regression (LR)	2 class (Normal and Anomaly)	99.40
[18]	AWID-CLS-R	CFS-BA feature selection and Ensemble model	4 class (over all accuracy)	99.50
[19]	AWID3	LightGBM	2 class (Normal and Evil Twin)	99.28
[21]	AWID-CLS-R	CNN	4 class (over all accuracy)	99
[22]	AWID-CLS AWID-ATK	J48	4 class (over all accuracy)	96.19
[23]	AWID-CLS	DNN	4 class (over all accuracy)	99.9
[24]	AWID-CLS AWID-ATK	k-means clustering	4 class (over all accuracy)	94.81
Proposed method	AWID3	CNN	8 class	99.93

As can be seen from the table, most of the WIDS literature studies are based on the AWID2 dataset. Although the AWID2 dataset is a large-scale dataset, it does not contain many attack types against the 802.11x standard that are included in the AWID3 dataset. The AWID3 dataset addresses the limitations of the AWID2 dataset and contains a large attack vector. Therefore, AWID3 dataset is used in this study.

When the literature studies are examined, it is seen that the studies conducted with both AWID2 and AWID3 datasets use the ready-made CSV files in the datasets. This indicates that the literature studies work directly with ready-made datasets without analyzing the PCAP files. In this study, the PCAP files for each Wi-Fi attack in the AWID3 dataset were analyzed with expert knowledge and a new dataset was extracted from the AWID3 dataset.

Another limitation in the literature is that studies with AWID2 dataset usually use four classes and studies with AWID3 usually use two classes. The method proposed in this study is applied to the 8-class dataset extracted from the PCAP files of the AWID3 dataset. In addition, when the studies on WIDS are analyzed, it is seen that most of the studies are machine learning based studies. In this study, the data in each row of the dataset was converted into 6x6 images and the new dataset obtained from the images was subjected to the classification process with the CNN deep learning method. When Table 6 is examined, it is seen that the proposed method is more successful than the other studies in the literature with 99.93% classification success although the dataset used has 8-classes. In this context, it is clear that the proposed study has the potential to make a significant contribution to the advancement of WIDS systems. When examining the studies in the literature presented in Table 6, it is seen that each study uses different AWID variations and classification schemes. This makes a direct and absolute comparison of the presented success rates methodologically difficult. However, the large-scale structure of our proposed method, covering 8 different attack classes, and its 99.93% accuracy rate, are consistent with the general performance benchmark of the existing literature and offer a more comprehensive solution than many multi-class approaches.

7. Conclusion and Future Works

The ever-increasing use of wireless networks and Internet of Things (IoT) devices has made network infrastructures a broader and more vulnerable target for cyber threats. Although there are numerous studies in the literature to improve the performance of WIDS systems, the continuous increase in the attack surface requires continuous improvement of WIDS systems. The use of wireless networks in almost every field is one of the biggest reasons that increase the attack surface. Although there are many literature studies on the detection of attacks on wireless networks, the desired success has not yet been achieved. In this study, 64 features were extracted from raw pcap files using the tshark software tool. The most effective features were extracted using the InfoGain algorithm. The data imbalance problem in the dataset was corrected using the Smote algorithm, and the final dataset was converted into 6x6x1 grayscale images. Converting the numerical features extracted from the AWID3 dataset into 6x6 grayscale images by processing them through Smote, QuantileTransformer, and normalization processes played a significant role in the success of the model. A five-layer CNN-based deep learning model is proposed to enhance WIDS performance in detecting network intrusions. By effectively leveraging image creation techniques during preprocessing, the proposed framework reached a near-perfect accuracy rate of %99.93. This clearly shows the positive impact of the proposed model and the features in the dataset extracted from the AWID3 dataset on intrusion detection in wireless networks. It is predicted that the proposed model will be very useful in the development of WIDS systems.

In future studies, it is planned to transfer the processes carried out in this study to a physical network laboratory. On the physical Wi-Fi testbed to be established, the model's resilience will be measured with live traffic data, and scenarios targeting network continuity, especially Denial of Service (DoS) attacks, will be examined in depth. Furthermore, the goal is to develop an autonomous software pipeline that parses PCAP files obtained from Wi-Fi networks into feature vectors in real time and feeds this into the CNN model. This will enable the integration of deep learning models with high success rates into practical network security solutions, contributing to the construction of more secure

wireless communication ecosystems.



Peer-review: External, Independent.

Acknowledgements:

This work is supported by TUBITAK (Scientific and Technological Research Council of Turkey) 1001 project number 123E706.

Declarations:

1. Statement of Originality:

This work is original.

2. Author Contributions:

Concept: MAC,IFK; **Conceptualization:** MAC,IFK,FE; **Literature Search:** MAC; **Data Collection:** MAC,IFK; **Data Processing:** MAC,IFK,FE; **Analysis:** MAC,IFK,FE; **Writing – original draft:** MAC,IFK,FE; **Writing – review & editing:** MAC,IFK,FE.

3. Ethics approval:

Not applicable.

4. Funding/Support:

This work has not received any funding or support.

5. Competing Interests:

The authors declare no competing interests.

6. GenAI Usage Statement:

No GenAI tools were used at any stage of the study.

7. Sustainable Development Goals:



REFERENCES

- [1] M. Çakmak, Z. Albayrak, and C. Torun, "Performance comparison of queue management algorithms in lte networks using NS-3 simulator," Teh. Vjesn., 2021, doi: 10.17559/TV-20200411071703.
- [2] Z. ALBAYRAK, H. MUSA, and M. ÇAKMAK, "Performance Evaluation of WBANs MAC Protocols in Different dBm and OMNet++," J. Intell. Syst. Theory Appl., 2021, doi: 10.38016/jista.758312.
- [3] S. Dwivedi, "Detecting anonymous attacks in wireless communication medium using adaptive grasshopper optimization algorithm," Cogn. Syst. Res., 2021, doi: 10.1016/j.cogsys.2021.04.003.
- [4] E. Mahdavi, A. Fanian, A. Mirzaei, and Z. Taghiyarrenani, "ITL-IDS: Incremental Transfer Learning for Intrusion Detection Systems," Knowledge-Based Syst., 2022, doi: 10.1016/j.knosys.2022.109542.
- [5] M. Mohammadi et al., "A comprehensive survey and taxonomy of the SVM-based intrusion

- detection systems,” *Journal of Network and Computer Applications*. 2021, doi: 10.1016/j.jnca.2021.102983.
- [6] P. Reddy and N. Shariff, “An anomaly-based intrusion detection system using recursive feature elimination technique for improved attack detection,” *Theor. Comput. Sci.*, vol. 1, pp. 1–9, 2022, doi: 10.1016/j.tcs.2022.07.030.
 - [7] F. Nie, W. Liu, G. Liu, and B. Gao, “M2VT-IDS: A multi-task multi-view learning architecture for designing IoT intrusion detection system,” *Internet of Things (Netherlands)*, vol. 25, no. January, p. 101102, 2024, doi: 10.1016/j.iot.2024.101102.
 - [8] E. Caville, W. W. Lo, S. Layeghy, and M. Portmann, “Anomal-E: A self-supervised network intrusion detection system based on graph neural networks,” *Knowledge-Based Syst.*, 2022, doi: 10.1016/j.knosys.2022.110030.
 - [9] N. O. Aljehane, H. A. Mengash, S. B. H. Hassine, F. A. Alotaibi, A. S. Salama, and S. Abdelbagi, “Optimizing intrusion detection using intelligent feature selection with machine learning model,” *Alexandria Eng. J.*, vol. 91, no. January, pp. 39–49, 2024, doi: 10.1016/j.aej.2024.01.073.
 - [10] M. Sangeen, N. A. Bhatti, K. Kifayat, A. A. Alsadhan, and H. Wang, “Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks,” *Comput. Commun.*, 2023, doi: 10.1016/j.comcom.2023.07.011.
 - [11] R. G. Brody, K. Gonzales, and D. Oldham, “Wi-Fi Hotspots: Secure or Ripe for Fraud?,” *J. Forensic Investig. Account.*, 2013.
 - [12] S. Wang, B. Li, M. Yang, and Z. Yan, “Intrusion detection for wifi network: A deep learning approach,” 2019, doi: 10.1007/978-3-030-06158-6_10.
 - [13] Vrizlynn L. L. Thing, “IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach,” *IEEE Wirel. Commun. Netw. Conf.*, 2017.
 - [14] T. Wang, D. Yang, S. Zhang, Y. Wu, and S. Xu, “Wi-alarm: Low-cost passive intrusion detection using WiFi,” *Sensors (Switzerland)*, 2019, doi: 10.3390/s19102335.
 - [15] Z. Tian, Y. Li, M. Zhou, and Z. Li, “WiFi-Based Adaptive Indoor Passive Intrusion Detection,” 2018, doi: 10.1109/ICDSP.2018.8631613.
 - [16] P. Satam and S. Hariri, “WIDS: An Anomaly Based Intrusion Detection System for Wi-Fi (IEEE 802.11) Protocol,” *IEEE Trans. Netw. Serv. Manag.*, 2021, doi: 10.1109/TNSM.2020.3036138.
 - [17] Z. Salah and E. Abu Elsoud, “Enhancing Network Security: A Machine Learning-Based Approach for Detecting and Mitigating Krack and Kr00k Attacks in IEEE 802.11,” *Futur. Internet*, 2023, doi: 10.3390/fi15080269.
 - [18] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” *Comput. Networks*, 2020, doi: 10.1016/j.comnet.2020.107247.
 - [19] L. M. Da Silva, V. M. Andregretti, R. A. F. Romero, and K. R. L. J. C. Branco, “Analysis and Identification of Evil Twin Attack through Data Science Techniques Using AWID3 Dataset,” 2023, doi: 10.1145/3635638.3635665.
 - [20] M. E. Aminanto and K. Kim, “Detecting impersonation attack in wifi networks using deep learning approach,” 2017, doi: 10.1007/978-3-319-56549-1_12.
 - [21] Q. Duan, X. Wei, J. Fan, L. Yu, and Y. Hu, “CNN-based Intrusion Classification for IEEE 802.11 Wireless Networks,” 2020, doi: 10.1109/ICCC51575.2020.9345293.
 - [22] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks:

- Empirical evaluation of threats and a public dataset," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 184–208, 2016, doi: 10.1109/COMST.2015.2402161.
- [23] S. Rezvy, Y. Luo, M. Petridis, A. Lasebae, and T. Zebin, "An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks," 2019, doi: 10.1109/CISS.2019.8693059.
- [24] M. E. Aminanto and K. Kim, "Improving Detection of Wi-Fi Impersonation by Fully Unsupervised Deep Learning," 2018, doi: 10.1007/978-3-319-93563-8_18.
- [25] E. Chatzoglou, G. Kambourakis, and C. Kolias, "Empirical Evaluation of Attacks against IEEE 802.11 Enterprise Networks: The AWID3 Dataset," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3061609.
- [26] R. Cheema, D. Bansal, and S. Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks," *Int. J. Comput. Appl.*, 2011, doi: 10.5120/2901-3801.
- [27] I. Attacks, M. Aye, C. Aung, and K. P. Thant, "IEEE 802.11 Attacks and Defenses," pp. 186–191.
- [28] İ. F. KILINÇER, F. ERTAM, and A. ŞENGÜR, "Automated Fake Access Point Attack Detection and Prevention System with IoT Devices," *Balk. J. Electr. Comput. Eng.*, 2020, doi: 10.17694/bajece.634104.
- [29] T. Zhou, Z. Cai, B. Xiao, Y. Chen, and M. Xu, "Detecting Rogue AP with the Crowd Wisdom," 2017, doi: 10.1109/ICDCS.2017.31.
- [30] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for Wi-Fi and WPA3," *Electron.*, 2018, doi: 10.3390/electronics7110284.
- [31] "CVE-2019-15126." <https://nvd.nist.gov/vuln/detail/CVE-2019-15126>.
- [32] H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, and D. Sicker, "Practical defenses for evil twin attacks in 802.11," 2010, doi: 10.1109/GLOCOM.2010.5684213.
- [33] J. Park, J. Kim, B. B. Gupta, and N. Park, "Network Log-Based SSH Brute-Force Attack DetectionModel," *Comput. Mater. Contin.*, vol. 68, no. 1, pp. 887–901, 2021, doi: 10.32604/cmc.2021.015172.
- [34] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2015.2457491.
- [35] M. Anagnostopoulos, S. Lagos, and G. Kambourakis, "Large-scale empirical evaluation of DNS and SSDP amplification attacks," *J. Inf. Secur. Appl.*, 2022, doi: 10.1016/j.jisa.2022.103168.
- [36] I. S. Crespo-Martínez, A. Campazas-Vega, Á. M. Guerrero-Higueras, V. Riego-DelCastillo, C. Álvarez-Aparicio, and C. Fernández-Llamas, "SQL injection attack detection in network flow data," *Comput. Secur.*, 2023, doi: 10.1016/j.cose.2023.103093.
- [37] M. Ahmed et al., "PhishCatcher: Client-Side Defense Against Web Spoofing Attacks Using Machine Learning," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.3287226.
- [38] D. Akgun, S. Hizal, and U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity," *Comput. Secur.*, 2022, doi: 10.1016/j.cose.2022.102748.
- [39] N. Li, A. Iosifidis, and Q. Zhang, "Collaborative edge computing for distributed CNN inference acceleration using receptive field-based segmentation," *Comput. Networks*, 2022, doi: 10.1016/j.comnet.2022.109150.
- [40] S. Wang, W. Xu, and Y. Liu, "Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things," *Comput. Networks*, 2023, doi: 10.1016/j.comnet.2023.109982.
- [41] K. Hassini, S. Khalis, O. Habibi, M. Chemmakha, and M. Lazaar, "An end-to-end learning approach

- for enhancing intrusion detection in Industrial-Internet of Things,” *Knowledge-Based Syst.*, vol. 294, no. April, p. 111785, 2024, doi: 10.1016/j.knosys.2024.111785.
- [42] F. Özyurt, T. Tuncer, E. Avci, M. Koç, and İ. Serhatlioğlu, “A Novel Liver Image Classification Method Using Perceptual Hash-Based Convolutional Neural Network,” *Arab. J. Sci. Eng.*, 2019, doi: 10.1007/s13369-018-3454-1.
- [43] “The AWID3 Dataset.” <https://icsdweb.aegean.gr/awid/awid3>.
- [44] G. A. Pradipta, R. Wardoyo, A. Musdholifah, I. N. H. Sanjaya, and M. Ismail, “SMOTE for Handling Imbalanced Data Problem : A Review,” 2021, doi: 10.1109/ICIC54025.2021.9632912.
- [45] A. B. Mohammed, E. Chamseddine, and A. ElAdel, “Enhancing real-time IoT intrusion detection using KAN-based frameworks with SMOTE,” *J. Netw. Comput. Appl.*, vol. 249, no. February, p. 104461, 2026, doi: 10.1016/j.jnca.2026.104461.
- [46] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, “An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset,” *Comput. Networks*, 2020, doi: 10.1016/j.comnet.2020.107315.
- [47] N. Omer, A. H. Samak, A. I. Taloba, and R. M. Abd El-Aziz, “A novel optimized probabilistic neural network approach for intrusion detection and categorization,” *Alexandria Eng. J.*, 2023, doi: 10.1016/j.aej.2023.03.093.

