I.J. Wireless and Microwave Technologies, **2021, 4, 1-10**
Published Online August 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.04.01

CNN-based Security Authentication for Wireless Multimedia Devices

Gautham SK
Department of Computer Science and Engineering, BMS Institue of Technology and Management, Bengaluru, India
E-mail: skgautham007@gmail.com

Anjan K Koundinya
Department of Computer Science and Engineering， BMS Institute of Technology and Management，Bengaluru, India
E-mail: annjank2@gmail.com

Received: 10 June 2021; Revised: 02 July 2021; Accepted: 20 July 2021; Published: 08 August 2021

Abstract: Security is a major concern for wireless multimedia networks because of their role in providing various services. Traditional security techniques have inadequacies in identifying emerging security threats and also lacks in computing efficiency. Furthermore, conventional upper-layer authentication doesn't provide any protection for physical layer, thus leading to leakage of privacy data. Keep these issues in mind, the paper has envisioned an artificial intelligence-based security authentication system that is lightweight, adaptive and doesn't require any explicit programming. The neural network is built on convolutional filters which explore the data and learns the features or characteristic of the data. With this learned feature, the model will be able to recognize whether a wireless multimedia device present in a network is legitimate or not. Experimental analysis and validation have been performed on the trained model and ensure that the authentication of wireless multimedia devices can be achieved and also ensuring lightweight authentication system, which ensures less computation needs. The different neural model is also trained using gaussian noise of different standard deviation so that it can be used in a practical scenario like smart industry etc.

Index Terms: Wireless Multimedia Networks, Security, Neural Networks, Gaussian Noise, Convolutional Layer.

1. Introduction

The approach of advances in Internet of Things and 5G envoys [1,2,3,4,5] the appearance of the following flood of omnipresent society. Specifically, when artificial intelligence and multimedia networks convergence it brings wide range of applications based on different services like training, monitoring and working particularly for [6,7] smart home, healthcare, transportation and many more. Multimedia applications will significantly extend the manner in which people see the world and be applicable to individual's everyday lives. The complexity of multimedia frameworks that is drastically expanding utilization of multimedia sensors inside the smart process bring numerous securities as well as privacy challenges. For instance, when the multimedia network gathers different information through various sensors, the malicious/attacker sensors could delude the user by misusing communication and giving false messages to the frameworks [8,9]. Security attacks could prompt disastrous consequences what's more, can cause barrage [10] like damages in the wireless networks. Also, resource-controlled multimedia devices are defenseless against attacks, causing damages to the multimedia network through different wireless attacks. Thus, there is need of a security mechanism that protects the wireless multimedia systems that ensure secure communication. Normally, access control mechanism and authentication are the key security procedures and basic design for multimedia networks [11]. These procedures secure communication by affirming the identities of the users and their access to the approved network. In any case, the disposition of number of wireless multimedia devices brings new problems for security setups. Expressly, those multimedia devices that operates on low-latency communication transmissions couldn't uphold the authentication technique that require very high computational overhead, and the sensors contained in the network require lightweight processing cost to guarantee communication performance.

One of the existing solutions for wireless multimedia devices which is based on physical layer is build using different supervised machine learning model are trained using the physical layer attributes which in return can authenticate whether the wireless multimedia device is legitimate or not. But the problem here is as the amount of data increases the accuracy of model is varying and the model are not dynamic in nature. The model is also not trained to handle noise so they are not apt for a practical scenario. Traditional cryptography that is based on key [12], strategies require huge resources and high processing capabilities, which is not effective for wireless multimedia networks. Digital

key might be undermined in security management procedures, like key management or key transmission. Conventional security procedures may experience attacks from adversary due to increases use of multimedia sensors which leads to the increase in the complexity of network scenarios. Security strategies executed on upper layers of networks face difficult to ensure the balance between the cost and security, which leads to inability to secure legitimate communication. Due to this, the malignant devices can access the personal data and damage the authentication process. Therefore, artificial intelligence based lightweight authentication system will very much useful to overcome these security issues. Conventional authentication procedures require more efforts to extricate complex features to maximize the security levels, which leads to higher communication and processing overheads, which leading to communication latency. This is not acceptable for real-time wireless-multimedia networks. The traditional authentication procedures select the statistical characteristics manually which requires time, which is not a non-adaptive authentication process. Therefore, there is need for authentication mechanism which are adaptive in nature. Traditional authentication strategies face difficulties while establishing an accurate authentication model in a practical scenario. This is because, for the model to predict outcome, it is trained using limited statistical properties. These bring loopholes in the authentication model which is a threat for continuous learning. To improve the authentication measure, it is important to plan a shrewd verification approach that doesn't need explicit programming. So, to increase the authentication procedure, a model needs to be built which doesn't require any explicit programming. Hence, to protect wireless multimedia networks from the mentioned attacks, the paper focuses on the difficulties looked by traditional verification approach and proposes a new light weight security strategy method.

A. Contributions

To address these mentioned challenges, a neural network-based security authentication system is proposed which is built on convolutional layers. The proposed model is adaptive to noise, lightweight authentication system and doesn't require any explicit programming. In summary, the contribution is as follows.:

- As discussed, the attacks and challenges of wireless multimedia networks, the paper as proposed a neural network-based learning model by understanding the physical-layer attributes of wireless multimedia devices. The studies have shown that, physical layer attributes of the devices are simple, efficient and easily portable, which makes a lightweight authentication system which will not cause any communication overload or latency.
- The neural network-based authentication system is trained using the physical layer attributes of wireless multimedia devices which gives the learned feature space of the devices which builds a classification model whose complexity is reduced and the model can recognize four types of wireless network attacks, namely sybil attack, black hole attack, jamming attack and exhaustion attack which belong to each class.
- The analysis and validation result on the proposed neural network based on feature learning shows have shown very good accuracy results to classify each class i.e., different wireless attacks.

B. Organization

The organization of the paper is as followed. Section I discussed about the problems of traditional authentication system. Section II is talks about the related work. Section III describes the system model and the layer used to build the neural network and also how the proposed convolutional layer network is built. Section IV is showing the performance analysis and validation results of the build neural network. Section V is about future research scope. Section VI includes the conclusion of the paper and the references.

2. Related Work

Authentication verification and AI technologies problems have been free exploration research topics. Up to this point, cross-disciplinary investigations have arisen in these two regions. Despite the fact that security validation has been examined in [13,14,15] another viewpoint on neural network-based validation will help to outperform the limitation and ensure the security prerequisites for the new networks. To safeguard against rogue attackers by understanding the multi-dimensional qualities of the wireless in varying wireless networks an extreme ML model is trained using the physical layer attributes is proposed in [16].

A two-layer encryption-based system is proposed in [17], here the cryptosystem is a combination of two homomorphic encryption algorithm that ensure the protection of data privacy.

Threshold based authentication system build using machine learning techniques that exploits the physical layer attributes but with less computation steps. I order to identify spoofers, [18] represents many versatile estimation algorithms that is based on profound neural networks which increases the training rate of the model and leads to low-latency and ensures a lightweight authentication system. Also, neural network explored in [19] are utilized to streamline the encoding and decoding capacities, and become familiar with the compromise between dependable communication and pattern of data to recognize eavesdroppers. The creators in [20] represents a safe semi-supervised model dependent on twofold technique, which is utilized to investigate the downfall the unlabeled cases as indicated by the characterization results. A system based on learning [21] intended to permit constant verification for wireless hubs

furthermore, to recognize spoofers from the real multimedia devices by understanding their physical layer attributes. A deep learning-based authentication system [22] to recognize different attackers, furthermore, investigate the authentication model in two-class and multiclass characterization. As of late, a developing number of studies that works on AI technologies into the field of security insurance [22,23,24,25,26]. For instance, audits the capability of applying neural based adaptable learning approaches with regards to future networks. Moreover, with the assistance of AI based algorithms, authentication system can be planned by using channel correspondence, explicit correspondence interface attributes, and characteristics of devices [27,28,29]. The prologue to AI based lightweight physical layer security is introduced [30], managing numerical models. Also, to ensure the security of wireless communication medium, a feed-forward neural system is introduced in [31,32,33] to group adversarial attackers. In the meantime, during the time spent while preparing and processing data, the program isolates the trust of the devices into various levels and assess its performance.

New advancement of smart authentication accomplishes security improvement by investigating ML, there are lacks in defeating the above explicit difficulties. Specifically, we bring up that computational as well as communication overheads just as long deferrals may increment because of delay in feature extraction and training steps. All the more significantly, the majority of the convectional strategies actually have restrictions in statistical properties, which implies precise predication and authentication structure configuration is missing. Giving dependable security confirmation to wireless network is the main impetus in the work. Subsequently, we center around imagining new counterfeit insight which helped security strategies to conquer the difficulties depicted in [34,35] and carry out secure validation in the devices. The paper [36] talks about machine learning based security authentication mainly for wireless multimedia devices. Here different machine learning model mainly supervised machine learning algorithm are trained using the physical layer attributes of the multimedia devices and the trained model is used as a data collection center and are used to classify whether the upcoming multimedia devices are legitimate or not.

3. Proposed Model

A neural network is set of algorithms that can recognize the relationship with the data through a process that is similar to how human brain works. Convolutional Neural Network (CNN) is one of the types in which a neural network can be build.

A. Convolutional Neural Network

It is majorly built by convolutional layer which perform an operation known as convolution. A convolution is a simple process where a filter convolves through the input which results in an activation. Repeating the same process with the same filter to an input forms a map of activation's called a feature map, which indicates the relationship and strength of the detected feature present in the data. Generally, convolution operates in linear fashion that involves cross product with weight values and the data. Specifically, cross product is performed between the array of input data and filters which are array of weights.

We need to ensure that the size of the filter is always smaller than the input array and the multiplication operation that is between the filter sized input array and the filter is dot product which performs element wise multiplication and the result that is obtained is summed, which is a single value. The operation that's performed is often referred as real number because the result obtained could be a single value. the scale of the filter is intentionally set to a size smaller than the input, in order that the identical filter i.e., weights, will be multiplied multiple times with the input array at different points on the input which incorporates left to right, top to bottom. This systematic approach of same filter convolving across the input brings out a robust idea which is usually referred to as translation in-variance, where the filter that's designed to detect specific type feature from the input, then the method of the filter that systematically moves across the whole input allows the filter to get the precise feature present anywhere within the input. The output of the multiplication operation may be a single value, because the operation is preformed multiple times, it results to a two-dimensional array which is named as feature map.

B. Rectified Linear Unit (ReLU)

ReLU is an implementation that mixes non-linearity and therefore the rectification layer of a CNN. It's a linear function which is represented as:

$$Y(l)_i = \max(0, Y(l-1)_i) \quad (1)$$

ReLU effectively propagate the gradient thereby reducing the vanishing gradient problem that commonly seen within the deep neural architecture. It solves the cancellation problem by thresholds the negative values to zero which ends in additional sparse activation function within the output. ReLU consists of easy operations like comparison which is efficient to implement in CNN.

C. Pooling Layer

One of the restrictions of feature map which is generated by the convolutional layer is that they store the precise location of every feature present within the input, so if there's a little movement within the position of feature within the input it'll cause a special feature map. So, an approach to resolve this problem is down sampling also called pooling layer. This layer ignores the weakest features that are present within the input, retaining only the strongest features that are present within the input thereby reducing the scale of the feature map. This layer comes after the ReLU layer. It works the same as the convolutional layer where a pooling filter that performs a particular operation convolves through the feature map. The scale of the filter is smaller than the input feature map. Two common pooling operations are:

- Max Pooling: It calculates the utmost value present in each patch of feature map.
- Average Pooling: It calculates the typical value present in each patch of feature map.

D. Fully-Connected Layer

It is simple feed forward neural-network. These networks don't contain any loops, the knowledge moves forward from the input node to the hidden nodes and the results at the output node. The output generated at the pooling layer is flattened given as input to the next layer which is the fully connected layer. Flattening is a process where the output from the pooling layer is converted into a vector. This layer works just like the synthetic neural network. The calculation performed at each layer of fully connected network is:

$$g(W\,x + b) \tag{2}$$

where,
x: Input vector with dimension [pl, 1].
W: Weight matrix with dimension [pl, nl].
b: Bias vector with dimension [pl, 1].
g: Activation Function.
pl: Number of neurons in the previous layer.
nl: Number of neurons in the current layer.

The last layer of fully connected layer is softmax activation function which provides the probability of an input which belongs to a specific class.

E. Methodology

The choice of channel feature is restricted while using conventional techniques and also need time to manually select the characteristics which isn't an adaptive process. So, the employment of convolutional neural network comes into picture, where the input to then neural network is that the channel matrix. The convolutional process collects the valid features from the physical layer properties. The loss function accustomed predicts the authentication model and therefore the different true classes is softmax loss function, which is represented by:

$$L = -\sum_{k=1}^{k} yk\ logsk \tag{3}$$

Where,
y_k represent the corresponding classes in the prediction model.
log_{sk} represent the k^{th} output vector of softmax.

The purpose of the convolutional layer is that it exploits the physical layer attributes using each neuron and produce a group of features that's beyond any knowledge. The specification which produces more complex features depend upon the filter size, the way within which the layer is placed and therefore the number of layers in it. the fundamental structure of the neural model is the:

- Input Matrix
- Convolutional Layer
- Max Pooling
- Dense Layer (Simple Feed Forward)
- Output Matrix

Convolution layer are usually filter which have a set height, width and depth, which are specified because the attributes of the convolutional layer during declaration.

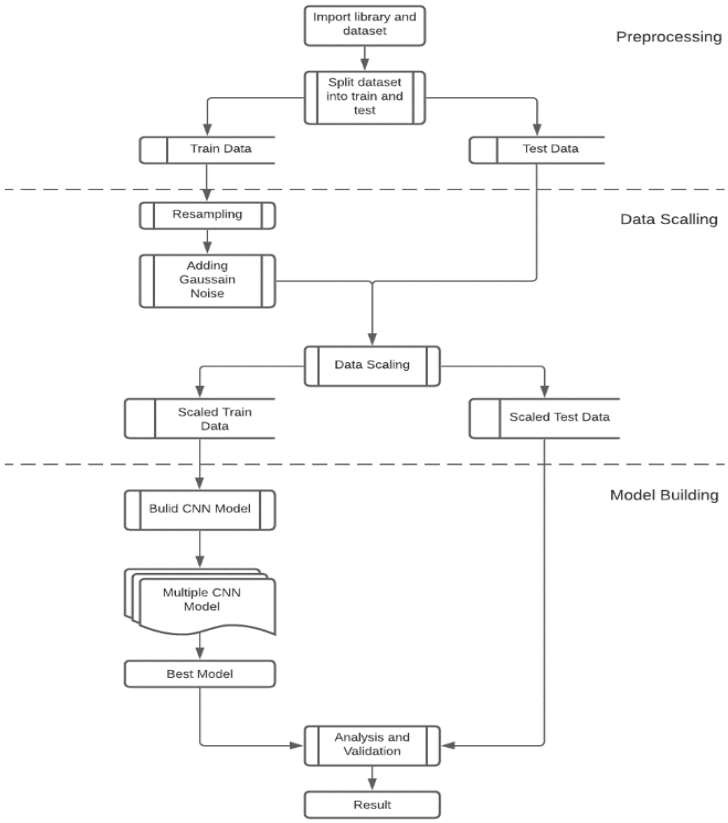

Fig.1. The proposed Authentication system.

The fig.1 represents the proposed neural network-based security authentication is formed of three convolutional layers to find out the feature. Each convolutional layer is accompanied to a batch normalization layer so directly connected to the pooling layer, which is max-pooling layer. The max-pooling layer optimizes the feature map that's generated by removing the weak attributes present in it thereby by reducing the dimensionality. The input for the flatten layer which is a layer that connects the convolutional layer with the dense layer is given by the pooling layer, which convert the output matrix to 1 dimension which is the input to the dense layer also called fully connected layer, which include simple feed forward neural network which is the target classifier.

The authentication build is build is three steps. First the neural network is trained by the physical layer attributes of the multimedia devices. The neural network will create multiple models which is tested using the test dataset and is also validated using the validation dataset and accuracy result for each model is generated during each epoch. The maximum epochs are defined as 100, but an early stop function is defined with a patience value of 10, where if the model loss value remains the same for 10 epochs, then the training process is stopped. At this current stage, multiple models will be generated, within these multiple models, the model with best accuracy is selected as the best and final model.

4. Performance Analysis

The neural network is built by recognizing the physical layer attributes of wireless multimedia devices such as RSS (Received Signal Strength), DAS (Distance between Adjacent Signal), CIR (Channel Impulse Response) and PCC (Pearson Coefficient Correlation). The trained neural network is validated using the validation data and the required validation and analysis is performed. The expected experimental result is to generate neural network model that gives a very good accuracy result and the difference between the trained model and the validation model must not too different. There should be similarity between them. This characteristic ensures that the model is good. This relationship can visualize by the graphs represented below.

The authentication system is trained with gaussian noise with standard deviation ranging from 0.1 to 0.5. First the system is trained without noise, then the system is trained with gaussian noise with standard deviations from 0.1 to 0.5.

Each graph represented below are generated by the IDE and each graph represent the relationship between the trained neural model and the validation model. This graph shows as how much similar is the trained model and the validation model. The similar helps us to understand the accuracy. The orange line represents the accuracy result of the validation model and the blue line represents the accuracy result of the trained model.

```
evaluate_model(history,X_test,y_test,model)
y_pred=model.predict(X_test)
```

```
Accuracy: 98.13%
<tensorflow.python.keras.callbacks.History object at 0x0000024CB28758C8
>
```

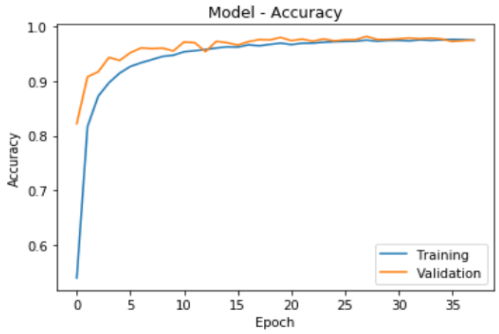

Fig.2. Model Accuracy- Neural model without noise.

The fig.2 represents the neural network which is trained without any noise which gives an accuracy of 98.13% and the similarity between the trained and the validation model is very much close as shown in the figure. The model loss of the above-mentioned neural network is represented in fig.3.

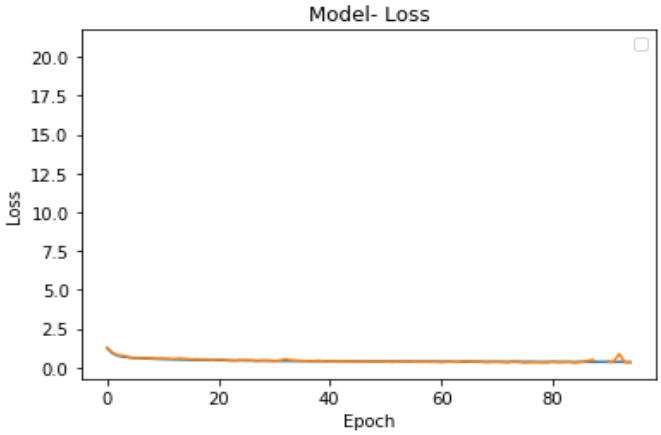

Fig.3. Model loss - Neural model without noise.

```
evaluate_model(history,X_test,y_test,model)
y_pred=model.predict(X_test)
```

```
Accuracy: 94.21%
<tensorflow.python.keras.callbacks.History object at 0x0000027F88FEC388>
```

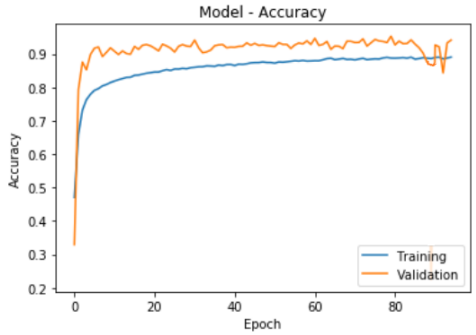

Fig.4. Model Accuracy- Neural model with noise 0.1

The fig.4 represents the neural network which is trained without any noise which gives an accuracy of 94.21% and the similarity between the trained and the validation model is much closer as shown in the figure. The model loss of the above-mentioned neural network is represented in fig.5.

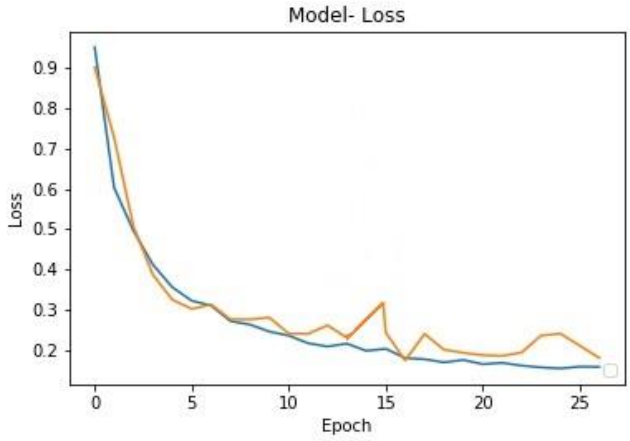

Fig.5. Model loss - Neural model with noise 0.1.

```
1 evaluate_model(history,X_test,y_test,model)
2 y_pred=model.predict(X_test)
```

```
Accuracy: 92.83%
<tensorflow.python.keras.callbacks.History object at 0x0000027F9948DB88>
```

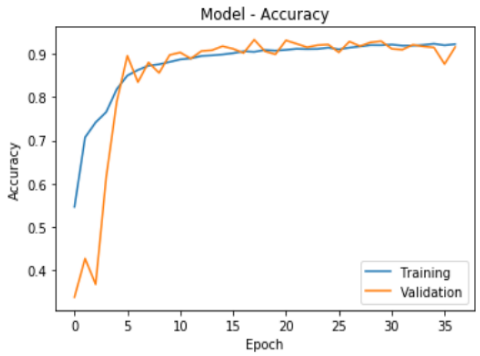

Fig.6. Model Accuracy - Neural model with noise 0.2.

The fig.6 represents the neural network which is trained without any noise which gives an accuracy of 92.83% and the similarity between the trained and the validation model is very much close as shown in the figure. The model loss of the above-mentioned neural network is represented in fig.7.

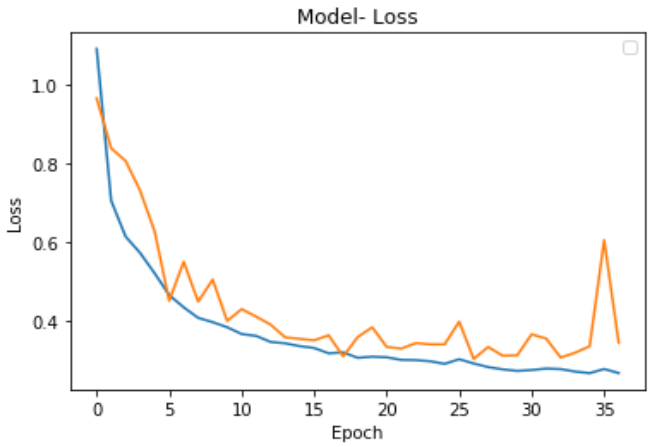

Fig.7. Model loss - Neural model with noise 0.2.

```
evaluate_model(history,X_test,y_test,model)
y_pred=model.predict(X_test)
```

```
Accuracy: 89.74%
<tensorflow.python.keras.callbacks.History object at 0x0000027F89654DC8>
```

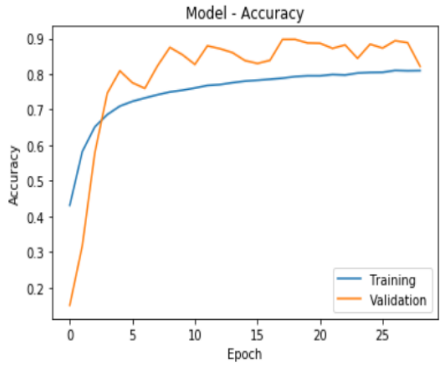

Fig.8. Model Accuracy - Neural model with noise 0.3

```
evaluate_model(history,X_test,y_test,model)
y_pred=model.predict(X_test)
```

```
Accuracy: 86.63%
<tensorflow.python.keras.callbacks.History object at 0x0000016CA169FF48>
```

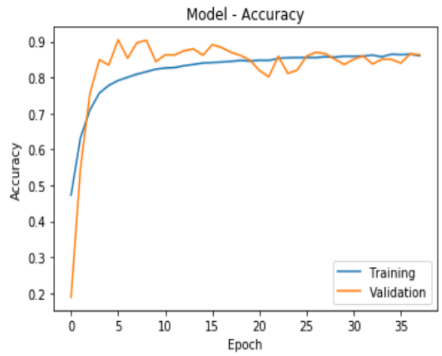

Fig.9. Model Accuracy - Neural model with noise 0.4

The Fig.8 and Fig.9 represents the model accuracy of neural network that is trained using the standard gaussian noise of 0.3 and 0.4.

Table 1. Accuracy Results

Noise	Accuracy
-	98.36%
0.1	94.21%
0.2	92.83%
0.3	89.93%
0.4	86.09%
0.5	85.43%

The table 1 shows summary the accuracy results of different neural network without noise and with gaussian noise of different deviation starting from 0.1 – 0.5 and there corresponding accuracy results. Each result is also accompanied by the model accuracy graph and model loss graph. As the noise deviation increased there are changes in the accuracy results and slight changes in the model loss, these can be gradually decreased by increasing the number of epochs.

5. Future Scope

Feature selection will be challenging if it is depended on statistical method which is applicable to all algorithms. Because when it comes for an adversarial case, the estimated signal or attribute preprocessing is an important aspect of the authentication system. So, a method to preprocess the signals can be done using deep learning, because it can solve the uncertainty that are present in the wireless multimedia networks by mining of channel feature and deep feature mapping. It also provides multiple operators that help to transform the system into an analytical based security

authentication system. Optimally, the safety should rely upon the knowledge, not the authentication model. The proposed authentication system works well in a standard and gaussian noise ranging from 0.1 to 0.5 with varying accuracy range. But with question for interesting direction for future research, suggest that the model ensure a reinforcement type authentication model that can that can make different assumptions based on noise which is from a practical perspective that will boost the adaptability of the authenticator.

6. Conclusion

The neural network-based authentication system for wireless multimedia devices proposed in this paper has significant practical importance. The neural network not only ensures the privacy of the multimedia devices but also ensures a light weight authentication system. The experimental analysis prove that the system build effectively learns the physical layer attributes of the devices, which are manually selected by the algorithm. In short, the neural network has good detection performance and less leading the lesser communication latency. The neural network-based security authentication which is based on the physical layer attributes of the multimedia devices can achieve better accuracy if the dimension of the features becomes large. So, if the dimension of the security authentication can be increased the neural network will have bigger accuracy rate of the wireless multimedia device.

References

[1] D. Wu, Zhihao Zhang, Shaoen Wu, J. Yang, and Ruyang Wang. Biologically inspired resource allocation for network slices in 5g-enabled internet of things. IEEE Internet of Things Journal, 6:9266–9279, 2019.

[2] Puning Zhang, Xuyuan Kang, Xuefang Li, Yuzhe Liu, Dapeng Wu, and Ruyan Wang. Overlapping community deep exploring-based relay selection method toward multi-hop d2d communication. IEEE Wireless Communications Letters, 8(5):1357– 1360, 2019.

[3] Zufan Zhang, Chun Wang, Chenquan Gan, Shaohui Sun, and M. Wang. Automatic modulation classification using convolutional neural network with features fusion of spwvd and bjd. IEEE Transactions on Signal and Information Processing over Networks, 5:469–478, 2019.

[4] Zhidu Li, Hailiang Liu, and Ruyan Wang. Service benefit aware multi-task assignment strategy for mobile crowd sensing. Sensors, 19(21), 2019.

[5] Zhidu Li, Yuming Jiang, Yuehong Gao, Lin Sang, and Dacheng Yang. On buffer constrained throughput of a wireless-powered communication system. IEEE Journal on Selected Areas in Communications, 37(2):283–297, 2019.

[6] Dapeng Wu, Hang Shi, Honggang Wang, Ruyan Wang, and Hua Fang. A feature based learning system for internet of things applications. IEEE Internet of Things Journal, 6(2):1928–1937, 2019.

[7] Puning Zhang, Xuyuan Kang, Dapeng Wu, and Ruyan Wang. High-accuracy entity state prediction method based on deep belief network toward iot search. IEEE Wireless Communications Letters, 8(2):492–495, 2019.

[8] Dapeng Wu, Shushan Si, Shaoen Wu, and Ruyan Wang. Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. IEEE Internet of Things Journal, 5(4):2958–2970, 2018.

[9] Dapeng Wu, Lingli Deng, Honggang Wang, Keyu Liu, and Ruyan Wang. Similarity aware safety multimedia data transmission mechanism for internet of vehicles. Future Generation Computer Systems, 99:609–623, 2019.

[10] He Fang, Angie Qi, and Xianbin Wang. Fast authentication and progressive authorization in large-scale iot: How to leverage AI for security enhancement? CoRR, abs/1907.12092, 2019.

[11] Mian Ahmad Jan, Muhammad Usman, Xiangjian He, and Ateeq Ur Rehman. Sams: A seamless and authorized multimedia streaming framework for wmsn-based iomt. IEEE Internet of Things Journal, 6(2):1576–1583, 2019.

[12] Xiaoying Qiu, Ting Jiang, Sheng Wu, and Monson Hayes. Physical layer authentication enhancement using a gaussian mixture model. IEEE Access, 6:53583–53592, 2018.

[13] Ning Xie and Changsheng Chen. Slope authentication at the physical layer. IEEE Transactions on Information Forensics and Security, 13(6):1579–1594, 2018.

[14] E. Jorswieck, S. Tomasin, and A. Sezgin. Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing. Proceedings of the IEEE, 103:1702–1724, 2015.

[15] Ning Xie and Shengli Zhang. Blind authentication at the physical layer under time-varying fading channels. IEEE Journal on Selected Areas in Communications, 36(7):1465–1479, 2018.

[16] Ning Wang, Ting Jiang, Shichao Lv, and Liang Xiao. Physical-layer authentication based on extreme learning machine. IEEE Communications Letters, 21(7):1557– 1560, 2017.

[17] Koundinya, A.K. and Gautham, S.K., 2021. Two-Layer Encryption based on Paillier and ElGamal Cryptosystem for Privacy Violation.

[18] Run-Fa Liao, Hong Wen, Jinsong Wu, Fei Pan, Aidong Xu, Yixin Jiang, Feiyi Xie, and Minggui Cao. Deep-learning-based physical layer authentication for industrial wireless sensor networks. Sensors, 19(11), 2019.

[19] Rick Fritschek, Rafael F. Schaefer, and Gerhard Wunder. Deep learning for the gaussian wiretap channel. In ICC 2019 - 2019 IEEE International Conference on Communications (ICC), pages 1–6, 2019.

[20] Haitao Gan, Zhenhua Li, Yingle Fan, and Zhizeng Luo. Dual learning-based safe semi-supervised learning. IEEE Access, 6:2615–2621, 2017.

[21] Baibhab Chatterjee, Debayan Das, Shovan Maity, and Shreyas Sen. Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning. IEEE Internet of Things Journal, 6(1):388–398, 2019.

[22] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, and Xinzheng He. A deep learning approach for intrusion detection using recurrent neural networks. Ieee Access, 5:21954–21961, 2017.

[23] Chunxiao Jiang, Haijun Zhang, Yong Ren, Zhu Han, Kwang-Cheng Chen, and Lajos Hanzo. Machine learning paradigms for next-generation wireless networks. IEEE Wireless Communications, 24(2):98–105, 2017.
[24] Aidin Ferdowsi and Walid Saad. Deep learning for signal authentication and security in massive internet-of-things systems. IEEE Transactions on Communications, 67(2):1371–1387, 2019.
[25] Hao Ye, Geoffrey Ye Li, and Biing-Hwang Fred Juang. Power of deep learning for channel estimation and signal detection in ofdm systems. 2017.
[26] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? IEEE Signal Processing Magazine, 35(5):41–49, 2018.
[27] Qian Mao, Fei Hu, and Qi Hao. Deep learning for intelligent wireless networks: A comprehensive survey. IEEE Communications Surveys Tutorials, 20(4):2595–2621, 2018.
[28] Xiaoying Qiu, Ting Jiang, and Weixia Zou. Physical layer security in simultaneous wireless information and power transfer networks. In 2017 17th International Symposium on Communications and Information Technologies (ISCIT), pages 1–4, 2017.
[29] Xiaoying Qiu and Ting Jiang. Safeguarding multiuser communication using full duplex jamming receivers. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pages 1–5, 2017.
[30] Timothy O'Shea and Jakob Hoydis. An introduction to deep learning for the physical layer. IEEE Transactions on Cognitive Communications and Networking, 3(4):563– 575, 2017.
[31] Olakunle Ibitoye, Omair Shafiq, and Ashraf Matrawy. Analyzing adversarial attacks against deep learning for intrusion detection in iot networks, 2019.
[32] Xiaoying Qiu. IET Communications, 12:1805–1811(6), September 2018.
[33] Xinlei Wang, Wei Cheng, Prasant Mohapatra, and Tarek Abdelzaher. Enabling reputation and trust in privacy-preserving mobile sensing. IEEE Transactions on Mobile Computing, 13(12):2777–2790, 2014.
[34] Sebastian Henningsen, Bj ̈orn Scheuermann, and Stefan Dietzel. Challenges of misbehavior detection in industrial wireless networks. In Ad Hoc Networks, pages 37–46, 2018.
[35] He Fang, Xianbin Wang, and Lajos Hanzo. Learning-aided physical layer authentication as an intelligent process. IEEE Transactions on Communications, 67(3):2260– 2273, 2019.
[36] Koundinya, A.K. and Gautham, S.K., Machine Learning Based Security Authentication for Wireless Multimedia Network, Fifth International Conference on Information and Communication Technology for Competitive Strategies, 2020.

Authors' Profiles

Gautham SK received the BTech degree from Kerala Technical University (KTU), in 2019. He is currently a MTech scholar in BMS IT & T, Bengaluru, India. His research interest includes authentication, physical layer security, machine learning and deep learning.

Dr. Anjan K Koundinya has received his B.E (CSE), M.Tech (CSE), and Ph.D. degree from Visvesvaraya Technological University (VTU), Belagavi, India. He has been awarded Best Performer PG 2010, First Rank Holder (M. Tech CSE 2010) and recipient of Best PhD Thesis Award by BITES, Karnataka for the academic year 2016-17. He has served in industry and academia in various capacities for more than a decade. He is currently working as Associate Professor and PG Coordinator in Dept. of CSE, BMSIT&M, Bengaluru.

How to cite this paper: Gautham SK, Anjan K Koundinya, " CNN-based Security Authentication for Wireless Multimedia Devices", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.4, pp. 1-10, 2021.DOI: 10.5815/ijwmt.2021.04.01