CNN-LSTM Based Approach for Dos Attacks Detection in Wireless Sensor Networks

Salim Salmi*
Engineering, Systems and Applications Laboratory
National Schools of Applied Sciences
Sidi Mohamed Ben Abdellah University, Fez, Morocco

Lahcen Oughdir
Engineering, Systems and Applications Laboratory
National Schools of Applied Sciences
Sidi Mohamed Ben Abdellah University, Fez, Morocco

Abstract—**A denial-of-service (DoS) attack is a coordinated attack by many endpoints, such as computers or networks. These attacks are often performed by a botnet, a network of malware-infected computers controlled by an attacker. The endpoints are instructed to send traffic to a particular target, overwhelming it and preventing legitimate users from accessing its services. In this project, we used a CNN-LSTM network to detect and classify DoS intrusion attacks. Attacks detection is considered a classification problem; the main aim is to clarify the attack as Flooding, Blackhole, Normal, TDMA, or Grayhole. This research study uses a computer- generated wireless sensor network-detection system dataset. The wireless sensor network environment was simulated using network simulator NS-2 based on the LEACH routing protocol to gather data from the network and preprocessed to produce 23 features classifying the state of the respective sensor and simulate five forms of Denial of Service (DoS) attacks. The developed CNN-LSTM model is further evaluated on 25 epochs with accuracy, Precision score, and Recall score of 0.944, 0.959, and 0.922, respectively, all on a scale of 0-1.**

Keywords*—*Denial of Service (DoS); Wireless Sensor Networks (WSN); Convolutional Neural Network (CNN); Long Short-Term Memory (LSTM)

I. Introduction

Wireless Sensor Networks is regarded as one of the prominent research topics. The technology is an ideal solution for numerous applications in various fields like telecommunication, military, healthcare, research, and agriculture, amongst others [1]. Aziz et al. [2] reported the application of wireless sensor networks in detecting natural disasters such as earthquakes, flooding, or volcanoes. The widespread WSNs usage has introduced many security threats in the implementation and deployment phase. Wireless sensor networks are susceptible to different attacks due to unique constraints like storage capacity, restricted processing power, and battery power capacity.

People worldwide rely on networking systems to bring new ideas and answers to their issues and help them meet their basic requirements. New and most often used technological innovations include sensors that allow users to receive remote data and utilize it for their specific purpose. Sensors are being used by Internet of Things (IoT) devices [28], which are becoming more popular. Recently researchers' intention over Wireless Sensors Network (WSN) increased, and several research publications have been added over the research repositories. Despite the advantages of WSN, several security loopholes can be exploited to receive DoS attacks. While using WSN applications, users can face several types of security threats that can cause data breaches [29]. Researchers have been attempting to develop new security solutions in order to prevent DoS attacks from succeeding in their endeavors. Several technological advancements have helped develop novel approaches to infiltrate and prevent such attacks. Still, deep learning has brought about the most effective approaches for preventing such security risks and DoS attacks [30].

DoS attacks are attacks on a service (network or application) that overload the service and prevent it from delivering services to the rest of the network or application's users. When a DoS assault is launched, it floods your site or the supporting infrastructure with a large amount of traffic from various sources, often preventing access to the site for the duration of the attack. Cloudflare, for example, is one of the services that provide DoS protection for websites. When it comes to defending against DoS attacks, it might be pretty challenging. Because it is coming at you from all over the Internet and all over the globe, there is almost no way to block the transmission of that deluge of illicit material. You have no control over it. Fortunately, specific DoS attacks may be detected and blocked upstream from the target (with the assistance of the ISP/backbone that hosts the target/victim). In contrast, others transmit data indistinguishable from a genuine user [20].

With limited resources, inadequate infrastructure, and a massive quantity of WSN use on our hands, we were forced to deal with a slew of security challenges. Assaults on the World Wide Web (WSN) are commonly targeted by Distributed Denial of Service (DoS) attacks. DoS attacks may be identified and avoided by several security measures that have been put in place by researchers, but preventing them is not a straightforward task. In order to safeguard WSN against such assaults, researchers are deploying dependable and easy-to-use security measures based on deep learning techniques.

This study investigates the defense mechanism for denial-of-service attacks in wireless sensor networks. The results of this deep learning technique were evaluated on a specialized wireless sensor network dataset called WSN-DS, having numerous normal and numerous attack circumstances to authenticate their efficiency in detecting Denial of Service attacks. The denial of service attacks can take place at any of the layers of the TCP/IP protocol stack [3],[4]. Presented in Table I are the different types of denial of service attacks available in each layer of the TCP/IP protocol stack. However, there is a range of DoS attacks that exist at each layer.

TABLE I. DoS Attacks on TCP/IP Protocol Stack [5]

Protocol Layer	**Attacks**
Physical Layer	Droplet Attack
	Jamming
	Node Tampering and Obliteration
Data Link Layer	Denial of Sleep
	Power Exhaustion
	Unfairness
Network Layer	Wormhole
	Blackhole
	Homing
	Spoofing, routing control traffic, replaying
	Misdirection
	Selective Forwarding
	Acknowledge Spoofing
	Sybil
Transport Layer	Desynchronization Attack
	SYN Flood
Application Layer	Overwhelming Sensors
	Reprogramming
	Path-based DoS

II. Literature Review

In recent years, there has been a rise in published studies on Wireless Sensors Networks (WSN). Despite the benefits of WSN, it is vulnerable to DoS assaults because of several security flaws. Users using WSN services may be exposed to various security risks, some of which may result in data breaches. DoS attacks are becoming more common, and researchers prevent them from succeeding. There have been several technological breakthroughs that have made it easier to penetrate and protect against these assaults. However, the most successful techniques to avoid such security threats and DoS assaults have been developed using deep learning.

Numerous studies have detected and classified attacks in overall security architecture and wireless sensor network attacks. The study presented by Alsheikh [6] discussed different algorithms, applications, and strategies of machine learning in a wireless sensor network. The study also highlighted some notable challenges facing the performance of wireless sensor networks, such as quality of service (QoS), query processing, security, energy awareness, and event identification, though the study only highlights the qualitative evaluation of this work.

In the work of Gundunz et al. [5], a survey of machine learning solutions for identifying denial of attacks was presented. This study reviewed the DoS discrepancy available at each layer of the TCP/IP protocol stack and concentrated on the network layer attacks.

Sudar et al. [20] proposed an ML model in SDN to identify DoS attacks in KDD99 dataset . They have used SVM and Decision tree algorithm to detect the attacks due to its accurate classification and less complexity. They claimed that the proposed algorithm (SVM) gives a good performance level of 80% .

Anomaly detection in big data analytics addressed by [21]. based on a big data analytics framework , in which the authors handled structured and unstructured data streams and batch processing techniques. The authors used the WIDE backbone dataset gathered in real time . They recognized 5 types of attacks, which are DoS attacks, HTTP flashcrowd attacks, flooding attacks, abnormal UDP and TCP using machine learning. The attack was identified by using 5 supervised machine learning techniques: Decision Trees (DT), Na¨ıve Bayes (NB), Neural Networks (NN),Support Vector Machines (SVM) and Random Forest (RF).

Almomani et al. [22] used eight different machine learning models in detecting DoS attacks which are: Naive Bayes (NB), Decision Trees (DT), Random Forests (RF), Support Vector Machine (SVM), J48, Artificial Neural Networks (ANN), K-Nearest Neighbor (KNN) and Bayesian Networks (BN). They used the WSN-DS dataset for their experiment and performed feature selection based on expert survey. The authors reported that the Random Forest algorithm achieved the best results with a True positive of 99.7% accuracy, out-performing the ANN model with a True positive of 98.3%.

In [23], the authors have proposed a method provides two level of security , they have implemented suspicious detection module In the first level of security , and they imposed machine learning based C4.5 decision tree model in the second level. First inbound traffic is handled by a suspicious data detection engine.If traffic is suspected to be an attack based on entropy values, a temporary alert is generated and sent to OpenFlow switches the controller to save that particular flow. This module facilitates early detection of attacks This module results once again through Level 2 security. This module provides results by analyzing additional characteristics of the traffic. The output of this module is considered the final result. This module helps detect attacks with a low false positive rate. If it is an attack, this module sends an alert to drop packets and remove the flow from the flow table. By using these two levels autors can help for early detection of DoS attack with low false alarm rate .

Wu et al. [24] proposed a CNN+RNN hierarchical neural network, which they named LuNet. It consists of multiple layers of CNN and RNN, both networks learn together from their input data. Their proposed model was tested on the NSL-KDD and UNSW-NB15 datasets [25]. They performed binary and multi-class classification and achieved maximum accuracies of 99.36% and 99.05%, respectively. Both results are in the NSL-KDD dataset.

This research [27] aims to evaluate the effectiveness of machine learning classification algorithms in detecting flooding,grey hole, and black hole distributed denial of service attacks in wireless sensor networks. We conducted our review using a WSN-based dataset, referred to as WSN-DS, and took the accuracy and speediness measures into account. The results show that the J48 approach is the most accurate and fastest way for identifying grey hole and black hole attacks. At the same time, the Random Tree method is the most accurate and fastest method for detecting flooding assaults. The J48 approach is the most efficient for speed, requiring an average of 0.54 seconds of processing time per sample.

III. Security Objectives in Wireless Sensor Networks (WSNs)

In wireless sensor networks, the security objectives are essential aspects of WSNs that must be addressed to avoid security compromise of any kind. There has been an ever-growing application of WSNs in penetrating security environments;

nodes are the network interface through which the attack nodes destroy the network. Routing is regarded as a trust-based process within nodes; the process serves as a good platform for attackers to disrupt the network. Security investigations in networks are carried out individually; thereby, networks are usually designed without pre-planning and are employed for a short period. Therefore, it is imperative to implement countermeasures to secure the wireless sensor networks from security attacks.

DoS is one of the most common attacks in wireless sensor networks. Figure 1 presents the wireless sensor networks with denial of service attacks. One profound effect of DoS involves refraining the radio from switching into sleep mode and draining the system battery completely. In the normal operating conditions, operating situations, the energy consumption ratio in the sensor reduces the battery capacity in months, while DoS reduces the battery in days by keeping the transmitter system incorporated in the sensor nodes [7],[8] and [9].

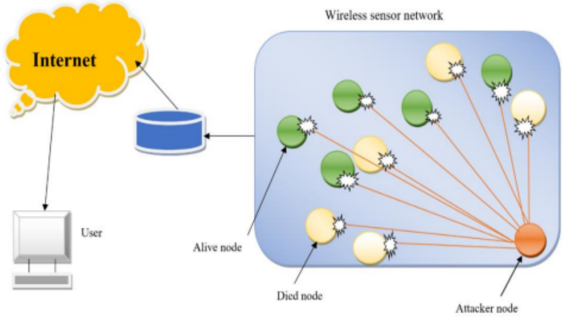

Fig. 1. WSNs with DoS Attack [10].

The security goals are based on the well-known triangle of CIA, namely confidentiality, integrity, and availability of information safety, and this describes what they represent in wireless sensor networks [11].

A. Confidentiality

In wireless sensor networks, the two most critical requirements are security and efficiency. There are several applications of WSNs, namely medical, military, research, agriculture, environmental monitoring and others. It is essential to avoid data leakage from sensor networks to neighbouring networks to avoid data confidentiality breaches. Securing the confidentiality of data is essential in protecting the data from attacks like spying [12]. The standard security measure in concealing confidential data is encryption before data transmission with a secret key acknowledged only by a particular receiver. Secure communication channels are established between source and sink, and other secure channels are triggered later if required [13].

B. Integrity

Wireless sensor nodes are susceptible to different security attacks threatening the reliability of the data, mainly in the interruption of the flow of information or data fraud [14]. In Sensor networks, transmitted data is considered by nodes to choose the right moves; this further confirms the importance of data integrity. There are two main parts of transmitted data, namely, updated or deleted. To secure data information, data transmitted from the node should arrive at the destination without an alteration in the transmission. The most suitable means of providing data integrity is wireless sensor networks are by checking the data at the receiver end [15].

C. Availability

Wireless sensor network nodes should continue operating excellently and not disturbed even when attacked. The implementation of sensors ensures the accessibility of authorized when the data is needed. Information gathered from wireless sensor networks is essential only if the correct user gain access to it at the appropriate time. It is known that WSNs is used in numerous fields, loss of information may lead to damaging consequences. In all the attacks, the most common attack intended at data availability is a denial-of-service attack [16].The CNN-LSTM model was trained using 10 and 25

IV. Methodology

This section covers the steps involved in the data acquisition process, attack detection and classification process, algorithms used, and model design for the research. The block diagram is presented in Figure 2 for the proposed system, which used a CNN-LSTM network to detect and classify intrusion attacks. The model layer explanation, dataset properties, data process, model training, and many other methodologies are discussed in this section. After this stage comes to the main model development stage, then the inference stage, where the performance evaluation for the model was determined.

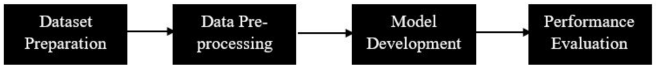

Fig. 2. Block Diagram of the Proposed Intrusion Detection Model.

A. DataSet

This research study uses a computer-generated wireless sensor network-detection system dataset developed by Almomani et al. [17]. The wireless sensor network environment was simulated using network simulator NS-2 based on the LEACH routing protocol to gather data from the network and preprocessed to produce 23 features classifying the state of the respective sensor and simulate five forms of Denial of Service (DoS) attacks, namely; Flooding, Blackhole, Normal, TDMA, and Grayhole. WSN dataset was gathered as an intrusion detection dataset tailored towards machine learning and deep learning techniques to identify and classify Denial of Service attacks. 365788 occurrences of records were extracted; it has 19 different attributes. The simulation parameters of the WSN dataset is presented in Table II.

TABLE II. WSN DATASET PARAMETERS [17].

Parameter	Value
Cluster Number	5
Location of the Sink	(50, 175)
Packet header size	25 bytes
Data packet size	500 bytes
Network area dimension	100m×100m
Routing protocol	LEACH
Simulation time	3600s
Nodes number	100 nodes

The WSN dataset has the following data points; Normal has 332040, Grayscale has 13909, Blackhole has 10049, TDMA has 6633, and flooding has 3157 data points.

B. DoS attacks types Description

DoS attacks types are described below [26]:

1) Black Hole attacks: the attacker plays the CH role. Then the attacker will keep dropping packets and not forwarding them to the sink node.
2) Grayhole attacks: the attacker advertising itself as a CH for other nodes. After the forged CH receives packets it selectively or randomly discarding packets, therefore it will prevent the legitimate packets to be delivered.
3) Flooding attacks: flooding attacks targeting LEACH protocol by sending a large number to the sensor to advertise itself as an advertising CH. This will lead to consuming energy, memory, and network traffic.
4) Scheduling attack: It occurs during the setup phase when CHs set up TDMA schedules for the data transmission time slots. The attacker will change the behavior of the TDMA schedule from broadcast to unicast to assign all nodes the same time slot to send data. This will cause a packet collision which leads to data loss.

C. Data Preprocessing

WSN dataset has been employed for testing and assessing intrusion detection techniques. It possesses a good understanding of different intrusion behaviours. Figure 3 presents the importing procedure of the WSN dataset; the dataset was imported to SQL server to implement different statistical measurements values such as occurrences distribution, classes of attacks, and percentage of the occurrences.

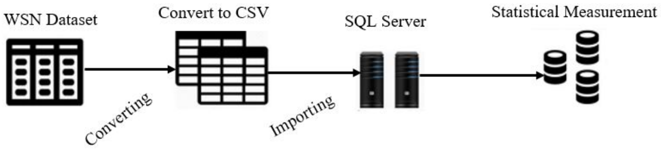

Fig. 3. Importing Procedure of WSN Dataset.

D. Data Split

The dataset was split into two sections: A training set dedicated to training the detection algorithm and a testing set that is completely hidden from the training process. The two subsets use the 80:20 approaches. 80% of the total dataset is used for the training and validation set, while 20% is used for the test set.

V. MODEL DESIGN AND DEVELOPMENT

To detect the intrusion attacks within the WSN dataset, a neural network that uses multi-layers that are interlinked together was used. The model used an eight-layered neural network structure to implement this study. These numerous layer neural networks used the same activation function (ReLU). The multiple layer networks learn over the input data using a selected kernel filter to extract essential features seen as necessary in the intrusion detection system. The developed model has one last layer, the dense layer; softmax activation function was considered for this layer due to its capability to hand classification of multi-classes. The summary of the developed CNN-LSTM model is illustrated in Table III and Table IV.

TABLE III. SUMMARY OF THE CNN MODEL PARAMETERS

Layer(type)	Output Shape	Param #
conv1d (Conv 1D)	(None, 18, 64)	256
conv1d (Conv 1D)	(None, 18, 64)	12352
max_pooling1d (MaxPooling1D)	(None, 9, 64)	0
flatten (Flatten)	(None, 576)	0
dense (Dense)	(None, 64)	36928
dropout (Dropout)	(None, 64)	0
dense_1 (Dense)	(None, 5)	325

TABLE IV. SUMMARY OF THE CNN-LSTM MODEL PARAMETERS

Layer(type)	Output Shape	Param #
conv1d_2 (Conv 1D)	(None, 18, 64)	256
conv1d_3 (Conv 1D)	(None, 18, 64)	12352
max_pooling1d_1 (MaxPooling1D)	(None, 9, 64)	0
conv1d_4 (Conv 1D)	(None, 9, 128)	24704
conv1d_5 (Conv 1D)	(None, 9, 128)	49280
max_pooling1d_2 (MaxPooling1D)	(None, 4, 128)	0
conv1d_6 (Conv 1D)	(None, 4, 256)	98560
conv1d_7 (Conv 1D)	(None, 4, 256)	196864
max_pooling1d_3 (MaxPooling1D)	(None, 2, 256)	0
lstm (LSTM)	(None, 70)	91560
Dropout_1 (Dropout)	(None, 70)	0
dense_2 (Dense)	(None, 5)	355

A. Model Architecture

This section describes the steps taken in achieving the intrusion detection technique. The model takes in an input having an unknown type of attack; the second step involves processing the input data by converting it to an acceptable model format. Then the model carries out a detection process by comparing the features of the present input attack data with the learned features of different kinds of attacks it has been trained with. If the model refuses to detect an attack, the system will return to step 2. If the model detects an attack, then the classification process takes place to ascertain the actual type of attack.

B. Model Hyperparameter Setting

The model hyperparameters are a set of values well-defined to improve the training process of the developed model and its general performance.

The model hyperparameters acknowledged in this study include activation function, epoch, learning rate, verbose, patience, optimization technique, and loss function, as presented in Table V.

These hyperparameters are set at optimal values after many rounds of random search to enhance model optimization. The number of the epoch is the number of times the training data is exposed to the model while training; it is the total number of iterations the whole training data passes through the developed model.

The CNN-LSTM model was trained using 10 and 25 epochs. Activation function was introduced into the model training to incorporate non-linearity effects into the developed model due to the non-linear type of data used. The two activation function used for this study is the softmax function and Rectifier Linear Unit (ReLU).

The softmax function is employed as an activation function in the output layer; it was the selected activation function in the output layer due to its excellent performance when used as a classifier.

Conversely, ReLU is an element-wise activation function; it is fast and straightforward to implement. Also, ReLU is computationally efficient to compute than other kinds of activation functions.

An exponential decay where the learning rate reduces exponentially, a learning rate of 0.001 was optimal for this study.

TABLE V. MODEL HYPERPARAMETER

Hyperparameter	Value
Epoch	10, 25
Activation Function	ReLU, Softmax
Loss Function	Categorical Cross Entropy (CCE)
Optimization algorithm	Adam
Learning rate	0.001
Verbose	1

C. Model Optimization

These are processes employed in ensuring the developed model reach a consistent and efficient level to achieve peak performance.

The adaptive moment estimation (Adam) is the optimizer used to minimize the loss function in this work. Adam is an efficient stochastic optimization that only requires a first-order gradient with its memory requirements. Adam was selected as the preferred choice of optimizer due to requiring a stationary objective.

Categorical Cross-Entropy (CCE) was employed in this study to ensure a better classification process in the CNN-LSTM model. CCE was selected for this work due to its improved choice for cost function, and Ho and Wookey [18] described CCE mathematically using Equation (1).

$$J_{CCE} = -\frac{1}{M}\sum_{K=1}^{K}\sum_{m=1}^{M} W_K \times Y_m^k \times \log\left(h_\Theta\left(x_m, k\right)\right) \quad (1)$$

where M represent the number of training examples, W_K represent the weight for class k, Y_m^k represent the target label for training example m for class k, K represent the number of classes, x_m represent the input for training example m , h_Θ represent the model with neural network weights Θ.

D. Model Implementation and Environment

The study was implemented using Python 3.7.7. Python language was selected as there is a lot of support from an active community for image classification using TensorFlow with Keras [19]. The study was started and completed on a laptop running on core i7, 8GB DDR RAM, a web IDE for Python (Google Colab) with Windows 10 operating system.

E. Performance Evaluation Metrics

The developed model was evaluated using various performance metrics. The assessment metrics used to estimate the model's performance include precision, accuracy, recall, and f1-score.

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (4)$$

where TP is the True Positives, TN is the Tue Negatives, FP is the False Negatives, FN False Negatives.

VI. THE EXPERIMENTAL RESULTS

This section describes the implementation of the intrusion detection model of all classes of attack on the network using the CNN-LSTM model. All the research details, results, and discussion of each experiment are presented. The results of the experiment are shown in different graphs and tables.

A. Detection of Attacks using the Collected Dataset

Attacks detection is considered a classification problem; the main aim is to clarify the attack as Flooding, Blackhole, Normal, TDMA, or Grayhole. Presented in Table VI are the classes of attacks in the dataset and their percentage distribution. Figure 4 presents the graphical representation of all the five kinds of attacks present in the dataset and their distribution.

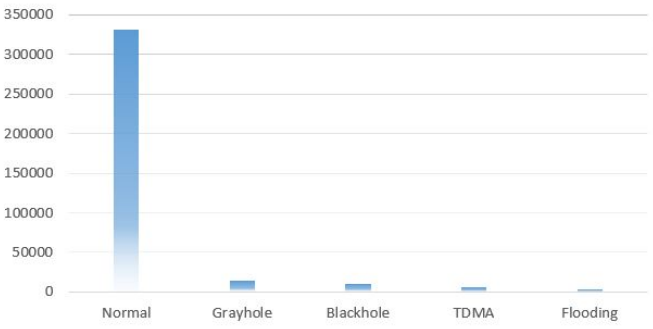

Fig. 4. WSN Dataset Distribution.

TABLE VI. DoS Attacks and Percentage Distribution

S/N	DoS Attacks	Distribution%
1	Normal	90.774
2	Grayhole	3.802
3	Blackhole	2.747
4	TDMA	1.813
5	Flooding	0.863

B. Intrusion Detection Model

The WSN dataset was used to train the CNN-LSTM model. The developed model gives a promising outcome in the attack detection process. The model successfully classifies the given attacks with a training accuracy of 91% on ten epochs and 97% on 25 epochs using a learning rate of 0.001.

The softmax activation function was selected in the output layer of this model due to its capability to handle multi-classification excellently well. The execution time achieved by the CNN-LSTM model on 10 and 25 epochs was 805 and 1103 secs, respectively.

C. Training Phase

During this phase, the training set was employed to train the intrusion detection model. The developed CNN-LSTM model recorded a training loss of 41.7%, training accuracy of 91.07%, validation loss of 47.01% and validation accuracy of 89.44% on 10 epochs, as illustrated in Figures 5 and 6.

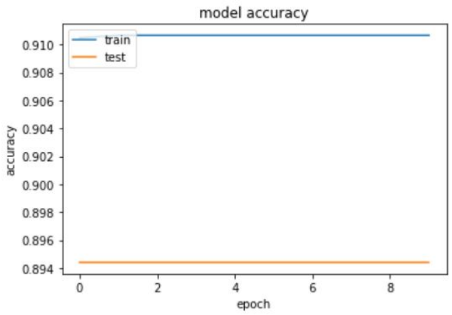

Fig. 5. Snippet of Model Training Accuracy with 10 Epochs.

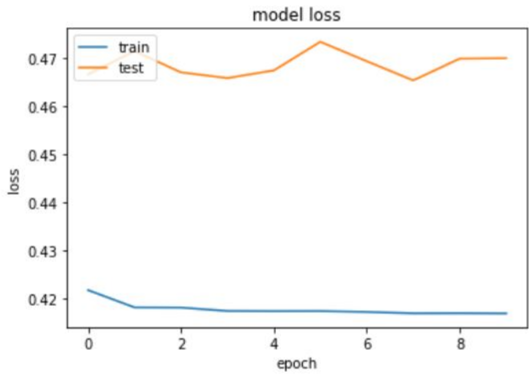

Fig. 6. Snippet of Model Training Loss with 10 Epochs.

The developed CNN-LSTM model recorded a training loss of 8.91%, training accuracy of 96.57%, validation loss of 11.47% and validation accuracy of 94.36% on 25 epochs, as illustrated in Figures 7 and 8.

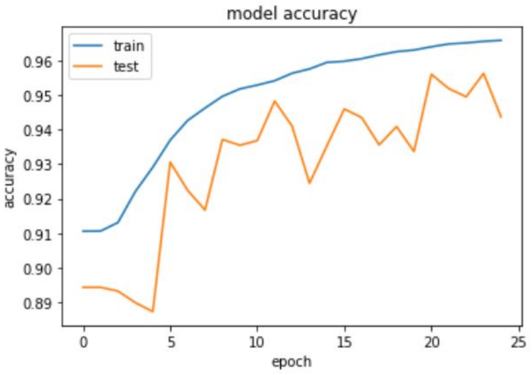

Fig. 7. Snippet of Model Training Accuracy with 25 Epochs.

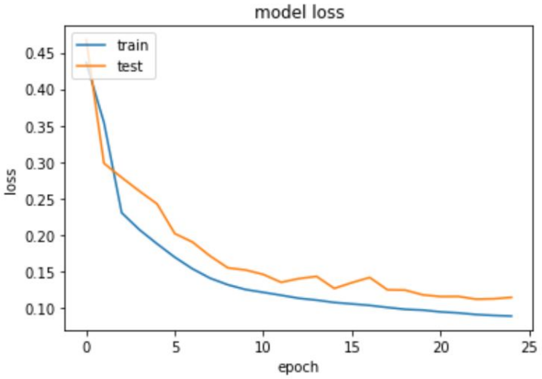

Fig. 8. Snippet of Model Training Loss with 25 Epochs.

D. Performance Evaluation of the Intrusion Model

The entire test set of the overall dataset was tested on the intrusion detection model. The test samples for each attack class were randomly selected. The CNN-LSTM intrusion detection model is evaluated to give the accuracy, Precision score, and Recall score of 0.89, 0.894, and 0.894, respectively, on ten epochs, all on a scale of 0-1. The developed CNN-LSTM model is further evaluated on 25 epochs with accuracy, Precision score, and Recall score of 0.944, 0.959, and 0.922, respectively, all on a scale of 0-1.

VII. Conclusion

Intrusion Detection System is an essential tool used in cyber-security to determine and track intrusion attacks. The rising development of information technology lately has further increased the usage of computer networks for several applications such as finance, business, industry, health and other various aspects of human life. Therefore, developing and deploying secure and reliable networks are critical to information technology administrators. This rapid development of information technology has produced several threats to building a robust and reliable network. There are many kinds of attacks threatening the confidentiality, integrity, and availability of computer networks. Some of these are Flooding, Blackhole, Normal, TDMA, or Grayhole, and they are regarded as harmful attacks.

The DOS attacks are the most common harmful attacks that temporarily denies several services of the end-users, consume computer and network resources. To avoid DoS attacks on computer networks, it is very important to detect and identify the actual type of attacks invading the network. This study developed a neural network model that detects the type of attack affecting the overall system network.

Wireless Sensor Networks Dataset (WSN) having five types of attacks was used in this study. The CNN-LSTM learning model was trained over 10 and 25 epochs with a 0.001 learning rate to ideally detect and classify the attacks. The overall learning algorithm registered a training accuracy of 96.57%; the detection model detected the five kinds of attacks available successfully. The CNN-LSTM intrusion detection model is evaluated to give the accuracy, Precision score, and Recall score of 0.89, 0.894, and 0.894, respectively, on ten training epochs, all on a scale of 0-1. The developed CNN-LSTM model is further evaluated on 25 training epochs with accuracy, Precision score, and Recall score of 0.944, 0.959, and 0.922, respectively, all on a scale of 0-1. The model has successfully extracted essential features of the five kinds of attacks considered.

This study is suitable for detecting intrusion attacks of computer networks, thereby enabling a secured environment for the system's proper functioning.

References

[1] Alsulaiman, L. and Al-Ahmadi, S., 2021. Performance Evaluation of Machine Learning Techniques for DoS Detection in Wireless Sensor Network. arXiv preprint arXiv:2104.01963.

[2] Aziz, N.A.A. and Aziz, K.A., 2011, February. Managing disaster with wireless sensor networks. In 13th International Conference on Advanced Communication Technology (ICACT2011) (pp. 202-207). IEEE.

[3] López, J. and Zhou, J. eds., 2008. Wireless sensor network security (Vol. 1). Ios Press.

[4] Das, S.K., Kant, K. and Zhang, N., 2012. Handbook on securing cyber-physical critical infrastructure. Elsevier.

[5] Gunduz, S., Arslan, B. and Demirci, M., 2015, December. A review of machine learning solutions to denial-of-service attacks in wireless sensor networks. In 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA) (pp. 150-155). IEEE.

[6] Alsheikh, M.A., 2014. S. lin, D. Niyato and H.-P. Tan,". Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications", IEEE Communications Survers & Tutorials, 16, pp.1996-2018.

[7] Juneja, V. and Gupta, D.V., 2018, August. Security against vampire attack in ADHOC wireless sensor network: detection and prevention techniques. In International Conference on Wireless Intelligent and Distributed Environment for Communication (pp. 25-38). Springer, Cham.

[8] Peng, S., Zhou, Y., Cao, L., Yu, S., Niu, J. and Jia, W., 2018. Influence analysis in social networks: A survey. Journal of Network and Computer Applications, 106, pp.17-32.

[9] Zhang, D., Ge, H., Zhang, T., Cui, Y.Y., Liu, X. and Mao, G., 2018. New multi-hop clustering algorithm for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 20(4), pp.1517-1530.

[10] Osanaiye, O.A., Alfa, A.S. and Hancke, G.P., 2018. Denial of service defence for resource availability in wireless sensor networks. IEEE Access, 6, pp.6975-7004.

[11] Neogy, S., 2015, June. Security management in wireless sensor networks. In 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-4). IEEE.

[12] Di Pietro, R., Michiardi, P. and Molva, R., 2009. Confidentiality and integrity for data aggregation in WSN using peer monitoring. Security and Communication Networks, 2(2), pp.181-194.

[13] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E., 2002. SPINS: Security protocols for sensor networks. Wireless networks, 8(5), pp.521-534.

[14] Acharya, R. and Asha, K., 2008, December. Data integrity and intrusion detection in wireless sensor networks. In 2008 16th IEEE International Conference on Networks (pp. 1-5). IEEE.

[15] Talzi, I., Schönborn, S., and Tschudin, C. 2008 "Providing data integrity in intermittently connected wireless sensor networks," in 5th International Conference on Networked Sensing Systems, 2008, IEEE, pp. 11–18 .

[16] Pelechrinis, K., Iliofotou, M. and Krishnamurthy, S.V., 2010. Denial of service attacks in wireless networks: The case of jammers. IEEE Communications surveys & tutorials, 13(2), pp.245-257.

[17] Almomani, I., Al-Kasasbeh, B. and Al-Akhras, M., 2016. WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. Journal of Sensors, 2016.

[18] Ho, Y., and Wookey, S. (2019). The real-world-weights cross-entropy loss function: Modelling the costs of mislabeling. IEEE Access, Vol. 8, pp. 4806-4813.

[19] Ketkar, N., 2017. Introduction to Keras. In Deep learning with Python (pp. 97-111). Apress, Berkeley, CA.

[20] Sudar, K. Muthamil, et al. "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques." 2021 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2021.

[21] SUDAR, K. Muthamil, NAGARAJ, P., DEEPALAKSHMI, P., et al. Analysis of Intruder Detection in Big Data Analytics. In : 2021 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2021. p. 1-5.

[22] Almomani, Iman M., and Mamdouh Alenezi. "Efficient Denial of Service Attacks Detection in Wireless Sensor Networks." J. Inf. Sci. Eng. 34.4 (2018): 977-1000.

[23] MUTHAMIL SUDAR, K. et DEEPALAKSHMI, P. A two level security mechanism to detect a DoS flooding attack in software-defined networks using entropy-based and C4. 5 technique. Journal of High Speed Networks, 2020, vol. 26, no 1, p. 55-76.

[24] WU, Peilun, GUO, Hui, et BUCKLAND, Richard. A transfer learning approach for network intrusion detection. In : 2019 IEEE 4th international conference on big data analytics (ICBDA). IEEE, 2019. p. 281-285.

[25] MOUSTAFA, Nour et SLAY, Jill. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In : 2015 military communications and information systems conference (MilCIS). IEEE, 2015. p. 1-6.

[26] AL-AHMADI, Saad. Performance evaluation of machine learning techniques for DOS detection in wireless sensor network. International Journal of Network Security & Its Applications (IJNSA) Vol, 2021, vol. 13.

[27] Wazirali, R., & Ahmad, R. (2022). Machine learning approaches to detect DoS and their effect on WSNs lifetime. Comput. Mater. Contin., 70(3), 4922-4946.

[28] Kopetz, H. (2011). Internet of things. In Real-time systems (pp. 307-323). Springer, Boston, MA.

[29] Abidoye, A. P., & Obagbuwa, I. C. (2018). DDoS attacks in WSNs: detection and countermeasures. IET Wireless Sensor Systems, 8(2), 52-59.

[30] Zaib, M. H., Bashir, F., Qureshi, K. N., Kausar, S., Rizwan, M., & Jeon, G. (2021). Deep learning-based cyberbullying early detection using distributed denial of service flow. Multimedia Systems, 1-20.