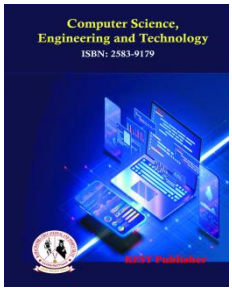
Computer Science, Engineering and Technology

Vol: 1(1), March 2023

REST Publisher; ISSN: 2583-9179 (Online)

Website: https://restpublisher.com/journals/cset/

DOI: https://doi.org/10.46632/cset/1/1/16



Mitigating Mobile Adhoc Network (MANET) Security Using Sequential Patterned Neural Network Method

[*]K. Gowsic, K. Rajeswari, P. Manjula, R. Arul Anand

Mahendra Engineering College, Namakkal, Tamil Nadu, India.

**Corresponding Author Email: gowsick@mahendra.info*

Abstract: *The Mobile Adhoc Network (MANET) is an autonomous network that can be adopted dynamically. There is no need of infrastructure as well as it has ability to access where the fixed configuration is not achievable. There are various routing protocol that has provided communication between the nodes in wireless network in which familiar and best routing protocol is Adhoc on-demand Distance Vector (AODV) protocol. Security is essential for all the devices in the network system in which MANET doesn't show any different. This research discuses about tackling various attacks of Denial-of-Service (DoS) in MANET as well as demonstrates that a broad classification model may fail in identifying these types of attacks because it cannot distinguish among network failures and an actual DoS attack. Moreover, the working of Machine Learning (ML) goal is about identification of complication pattern involved in AODV routing protocol of MANET which made decision with respect to the acquired results. One of the challenging security tasks is securing the routing path over implementation of MANET environment with no infrastructure. Therefore, proposed Neural Network (NN) with sequential pattern using Artificial NN (ANN) in AODV routing over MANET environment has generated suitable security for various DoS attacks. Thus, the approach of security has mainly focus on mitigating MANET security by identify and avoiding malicious nodes to generate secured routing path over MANET environment. Hence, the security approaches in MANETs mainly focus on mitigating security, eliminate malicious node as well as secure routing paths.*

Keywords: *Mobile Adhoc Network (MANET), Machine Learning (ML), Adhoc On-demand Distance Vector (AODV), sequential pattern, routing path.*

1. INTRODUCTION

Wireless networks can be classified as network with infrastructural central access point as well as ad hoc without access point. Because of its wireless nature, the MANET is capable of being built as multihop packet over networks in which wireless network has dynamic topology because of its mobile nature [1]. However, as we will see, MANET is made up of wireless devices that may exchange information as and when required with the other devices. Since it is an infrastructure network, the nodes are able to roam about and thus the network design changes with the growth of the network. In this network, the nodes are more susceptible to attack as compared to the normal networks because they are not well protected [2]. MANETs also offer another type of competence because of their difficult applications in civil and military applications, environmental and infrastructural projects [3]. They have limited chances to stand up against various kinds of malicious attacks in addition to their effectiveness. Nevertheless, many different security breaches occur as a result of MANETs' unique properties. As a result, MANET is more vulnerable to security vulnerabilities as compared with traditional wired networks. Actually, the MANET geometry is not established, and so cannot be encompassed. In a nomadic context, nodes can also relocate as frequently as they want in a network of wireless devices [4]. Once an opponent enters its radio range, it becomes able to connect with a node. The mobile nodes in MANET may be added to or removed from the network at any moment. A node in a distributed system may exhibit malicious behavior, making it difficult to determine if the node is malicious or not [5]. This is particularly vulnerable assault on the network compared to external attacks. Because of the malware infestation, these nodes are commonly referred to as compromised nodes. Due to the lack of a centralized management mechanism in MANETs, the following security issues can develop [6]. As a result, the attacks that might happen are extremely difficult to detect [7]. Managing traffic from a single node to another from a single location is not practicable. If the guide changes both the attack strategy and the attack target has developed towards simpler to avoid detection [8]. Apparently an enemy has destroyed the node

or there is a network issue. Because it does not exist a security relationship, therefore the nodes can't be labeled as trusted or untrusted. Invasive behaviors can degrade MANET efficiency by causing packet loss, high latency and network congestion [9]. By quickly detecting and neutralizing intruders, network performance may be maintained, ensuring excellent connectivity across mobile nodes. Compliance rules in particular applications, such as healthcare or finance, require the deployment of strong security measures to protect sensitive data. Intruder detection assists firms in meeting regulatory obligations while also avoiding potential legal and financial ramifications from data breaches or security events. Overall, intruder detection is critical to MANET security, reliability, and resilience, allowing for efficient and secure communication in dynamic and difficult contexts [10]. A light-weight Support Vector Machine detecting framework was designed to identify black hole attacks in networks, while a Secure SEAL was proposed by Simpson et al. to manage interruptions to IoT networks [11]. Using a trust metrics enhanced detection of threats and data throughput. The developed a neutral network-based method in detecting as well as mitigating black and gray whole attacks over vehicular networks, offering enhanced detection rates. Additionally, it explores probabilistic ML strategies to determine the preliminary threat Profile of MANETs, supplementing existing methodologies for threat evaluation [12]. Despite these efforts, the effectiveness of intruder detection and protection against attacks in MANETs remains an ongoing challenge. This research objective could be accomplished by monitoring the each packet forward time across every participating node involved in communication. The organization of this paper has delineated as follows, section 2 encompasses a survey pertaining to connected research endeavors, Section 3 delves into algorithmic and classification techniques, Section 4 discusses the simulation work for the proposed research, as well as Section 5 offers concluding remarks.

2. LITERATURE REVIEW

DoS attacks have consequently grown into a prominent security threat, engaging the attention of several researchers. However, none of the solutions suggested at present have effectively reduced the adverse effects of DoS attacks on MANET in real-time situations. The literature study explains that IDSs use multiple identification approaches and sequential pattern of ANN approach in identifying the secured AODV routing path in MANET. Srilakshmi et al. introduced a Secure Optimization Routing Algorithm (SORA) explicitly designed for MANETs [13]. The major objective was for enhancing the routing path security choices inside these networks. The SORA utilizes cryptographic methodologies to ensure communication confidentiality, integrity, and authenticity and to improve route selection efficiency. The evaluation findings revealed a PDR of 93%, an average end-to-end latency of 10 ms, and a routing cost of 6%. Nabati et al. proposed AGEN-AODV, a routing protocol designed to optimize energy consumption in heterogeneous MANET [14]. The AGEN-AODV protocol integrates artificial intelligence techniques to enhance energy efficiency in heterogeneous networks. The findings indicated a significant improvement in energy efficiency, resulting in a 20% decrease in energy use. The PDR reached 88%, and the routing overhead was decreased to 6%. Dalal et al. proposed an Adaptive Traffic Routing Approach (ATRA) as a solution for load balancing and congestion management on ad hoc networks inside the Cloud–MANET [15]. The ATRA is a dynamic mechanism that optimizes traffic pathways to distribute loads evenly and relieve congestion, improving the network's overall performance. The evaluation findings demonstrated effective load distribution, resulting in a throughput of 5 Mbps, a decrease in packet loss of 3%, and improved network stability. The Adaptive Trust-based Secure and Optimal Route Selection (ATSORS) for MANETs was developed by Ravi et al. This algorithm utilizes Hybrid Fuzzy Optimization techniques. The ATSORS system integrates trust-based and fuzzy logic methodologies to provide safe and optimum route selection. The findings revealed a significant degree of confidence at 92%, a latency of 12 ms for end-to-end communication, and a PDR of 90% [16]. Khan et al. proposed a Multi Attribute-based Trusted Routing (MATR) approach to embedded devices in MANETs and the IoT. The MANET routing protocol uses the MultiAttribute Analysis (MAA) technique to determine reliable routes. These routes are mainly designed for embedded IoT devices. The evaluation findings revealed a dependability level of 88%, a PDR of 93%, and a reduction in routing costs [17]. Kumar & Manjunath propose a Kangaroobased IDS system with Bi-LSTM and E-ART encryption, enhancing data transmission security and optimizing multipath using the Fire Hawk Optimization Algorithm (FHO), yet potentially increasing classification complexity [18]. Singh and Maria present a DNN Algorithm for intruder detection, achieving high accuracy but lacking specific techniques and results [19]. Zainab et al. propose intrusion detection using CBPNN, FNN, and CNN algorithms, leveraging various deep neural network designs, though algorithm complexity may cause delays in computing intruders [20]. Additionally, Edwin and Maria propose IDS-based ML algorithms with a Whale Optimized Deep NN Model and Whale Optimization Algorithm with Deep NN, offering high accuracy in intruder node prediction but potentially suffering from overload due to multiple algorithms [21]. while Edwin Singh and Maria propose a fuzzy-based intruder detection, achieving high accuracy in MATLAB simulations [21]. Finally, Veeraiah et al. introduce a routing protocol for IDS, providing trustworthy communication among nodes, although specific techniques and results are not specified for several methods. The table summarizes various methods employed in IDS for enhancing the security of MANETs. These methods range from machine learning-based

routing protocols to cryptographic techniques and secure communication approaches [22]. Sultan Mohamad, Sayed Hesham, and Khan Manzoor have mostly concentrated on modeling and researching the application of ANNs as a means of intrusion detection in MANETs. The primary goal of this study was to analyze, simulation, and evaluation the application of feed forward NNs with back propagation (FFBP) in MANETs. The input parameters of this strategy are calculated utilizing an extracted dataset created from MANET simulations, and the RMSR has utilized as a metric to assess the effectiveness of the suggested ANN modeling. The suggested framework can be employed for identifying DoS attacks in MANET. The better outcome in ANNs for FFBP networks with Tan-Sigmoid functionality are associated with the 4-15-10-1 network, which yield RMSE=0.045 for 14 epochs of training and RMSE=0.051 to testing data [23].

3. RESEARCH METHODOLOGY

The purpose of this suggested sequential ANN model with modified hidden layer has been utilized for determining the security present over MANET by selecting various optimizers. The purpose of the optimizer is to initiate the better learning rate during training. There are various features provided as an input by for identifying the attack type status in the MANET dataset shown in figure 1.

	id	Time	Is_CH	who CH	Dist_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	dist_CH_To_BS	send_code	Expaned Energy	Attack type
0	101000	50	1	101000	0.00000	1	0	0	25	1	0	0	0	1200	48	130.08535	0	2.46940	Normal
1	101001	50	0	101044	75.32345	0	4	1	0	0	1	2	38	0	0	0.00000	4	0.06957	Normal
2	101002	50	0	101010	46.95453	0	4	1	0	0	1	19	41	0	0	0.00000	3	0.06898	Normal
3	101003	50	0	101044	64.85231	0	4	1	0	0	1	16	38	0	0	0.00000	4	0.06673	Normal
4	101004	50	0	101010	4.83341	0	4	1	0	0	1	25	41	0	0	0.00000	3	0.06534	Normal

FIGURE 1. Attack type status in MANET dataset

After collecting the data and data wrangling is done that assist in removing missing data whereas the missing value imputation is performed. Subsequent to missing imputation procedure, the data pre-processing is done using labelEncoder for converting the object data type towards an integer or float data type that is then considered a continuous variable. Finally, the 18 input variables are preprocessed to ensure that each variable unit is unique employing standardscaler. The dataset is divided into two ratio namely 75% for training and 25% for testing. Figure 2 illustrate the proposed sequence pattern of ANN in which the sequence layer involves dense layer, input activation layer and output activation layer. Initially four different pattern is generated in which dense layer of input is 32, 16 and 8. Table 1 illustrates the four sequence pattern with respect to input layer, input activation function, output activation function.

TABLE 1. Four different sequence pattern parameters

Pattern Dense Layer	Input Activation	Output Activation
Input dense: 32 Output dense: 5	Relu	Sigmoid
Input dense: 32 Output dense: 5	Leaky Relu	Sigmoid
Input dense: 32, 16 Output dense: 5	Relu	Sigmoid
Input dense: 32, 16, 8 Output dense: 5	Relu	Sigmoid

According to the sequence pattern, best ANN parameter is defined as an optimal ANN sequence in which various optimizers like adam, Stochastic Gradient Descent (SGD) and rmsprop to accomplish better prediction in AODV protocol routing in MANET.

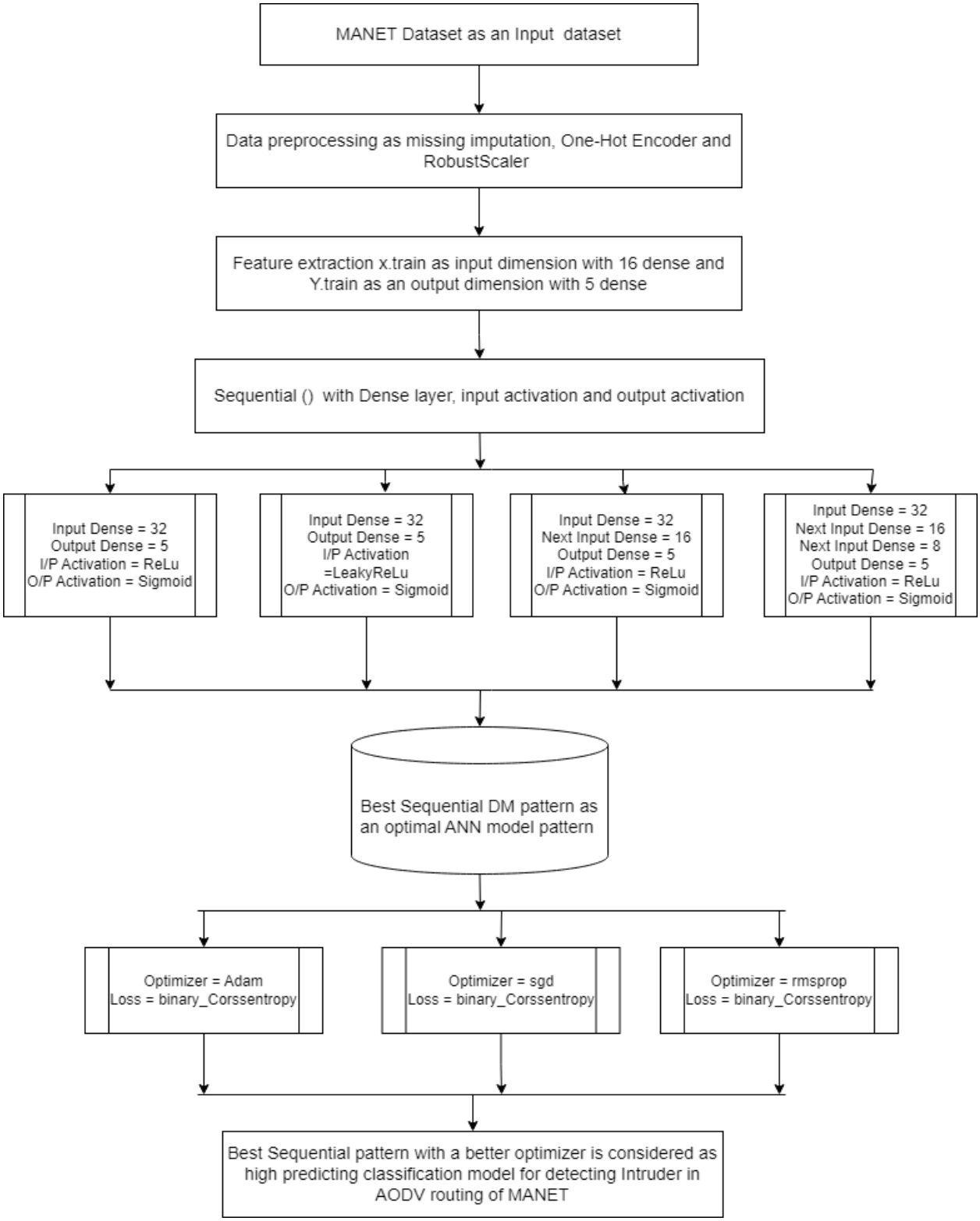


FIGURE 2. ANN sequential patterns with various optimizers for mitigating security in MANET

Working of ANN method

The NN discover from data patterns as well as tried for creating predictions as precise as possible. Let set the data X pairs consists of the variables and the results, (m^1, t^1), (m^2, t^2), ….(m^X, t^X)

Where,

m^i = input value

t^i = target value for i= 1, 2, 3, …, X.

This research focus on creating NN as Y so that ideally is expressed in equation 1

$$Y(m^i) = t^i \quad (1)$$

However, typically the error is permitted as $\in^i$. Let n represent the ANN output is expressed in equation 2 and 3.

$$n^i = Y(m^i) \quad (2)$$

And

$$t^i = n^i + \in^i \quad (3)$$

However, the n^i is defined with respect to the parameter based on weight as well as bias that became as an optimizer problem. According to ANN setting, Y has minimized the error function representation is expressed in equation 4.

$$E = \frac{1}{N}\sum_{i=1}^{X}\left\|t^i - n^i\right\|^2 \quad (4)$$

Where,

N = training pattern number.

When the ANN determines two-way classification whereas N = 2. and E is a parameter function of F, that needed to determine the weight values which reduce the error by differentiating E. Thus, the research concentrates on single term summation and it is expressed in equation 5.

$$\|t - n\|^2 = (t_1 - n_1)^2 + (t_2 - n_2)^2 + \cdots + (t_x - n_x)^2 \quad (5)$$

The values of input and output are fixed as well as the only parameter considered is weight. Differentiating both side for identifying the weight is determined through an equation 6.

$$\frac{\partial}{\partial w_{ij}}(\|t - n\|^2) = -2(t - n).\frac{\partial n}{\partial W} \quad (6)$$

Currently, this is highly specific and it fits the NN concept. With respect to ANN the output defined as $n^i = W_{ij}m^i + b$.

Finally, the dependence of output is weight of the features and it get differentiated both side with respect to W_{ij} by chain rule as per equation 6 is expressed in equation 7

$$\frac{\partial}{\partial \mathrm{w_{ij}}}(\|\mathrm{t - n}\|^2) = -2(\mathrm{t_i - n_i})\mathrm{m_i} \quad (3.7)$$

Where,

$m_j$is in the i th coordinate position.

The derivative that results indicates the path to the maximum, therefore in order to find the minimum location, we follow the opposite direction of the gradient. Furthermore, we want to observe this derivative as as close to zero as feasible for the purpose to minimize mistake.

Optimization

The procedure of optimization has aim in minimizing network error. This has a significant impact on model correctness. The optimizer variations are SGD, Adam, and RMSProp. SGD is an incremental gradient descent method that iteratively searches for the smallest error. In each iteration, models make predictions as well as compared to predicted outcomes. The difference among the expected value as well as the actual result is identified as an error. The error has employed to modify the network weights as well as internal model parameters. The method of backpropagation follows this update approach. It fails to function effectively with a low learning rate since it impede the algorithm's learning and with a high learning rate because it may cause instability. Furthermore, SGD has trouble exiting the saddle points. For manipulating RMSprop, ADAM, and SGD are considered as saddle point that are the most widely used. Nesterov has enhanced gradient gets employed in

updating the gradient to the slope as well as faster the SGD.To address the AdaGrad issue, two type of optimizers are developed independently namely RMSProp and AdaDelta. Both working are similar with the sole differentiation being that Adadelta lacks an early learning rate constant. Adam is an added type of optimizer that associates the advantages of Adadelta and RMSprop which calculates the learning rate for every parameter. From the overall optimizer, Adam was considered a decent choice because it outperformed RMSProp and Adadelta. As a result, in this paper, the selected optimizers are Adam, RMSProp, and SGD. The sequential pattern ANN can efficiently extract complicated characteristics among the significant factors of recognizing an intrusion in the AODV routing, while optimizer selecting is critical in enhancing the section of optimum route path in the MANET's. It may be determined by improving forecast accuracy with the predictive tool. Thus, the AODV model efficiency was increased by optimizing the best acquired sequence for boosting the predicted security accuracy using the ANN method.

4. RESULTS AND DISCUSSION

The experimental research is performed using general setting GTX 1050 GPU with i7-7400 processor running at 5.00 GHz. The machine contains an x64 processor and 16.00 GB of RAM. Python was used for training the models using the Keras environment. The models were assessed with Tensorflow library. The models have been checked using the following parameters such as number of layers, number of hidden units, activation function for input and output, epoch count, batch size and optimization function. Choosing a sequential search space for each optimizer is an important fundamental decision when performing an empirical comparison between optimizers. However, this assumes that similarly-named variables ought to acquire identical values across optimizers, which is not often true. Figure 3 has illustrated the iteration by defining batch size, along with optimizer, dense layer, input/output activation function.

```
[ ] model_3.fit(X_train, y_train, validation_data=(X_test, y_test), batch_size=5, epochs=10)

    Epoch 1/10
    7168/7168 [==============================] - 34s 5ms/step - loss: 0.2604 - accuracy: 0.7285 - val_loss: 0.1748 - val_accuracy: 0.7643
    Epoch 2/10
    7168/7168 [==============================] - 38s 5ms/step - loss: 0.1657 - accuracy: 0.7945 - val_loss: 0.1540 - val_accuracy: 0.8362
    Epoch 3/10
    7168/7168 [==============================] - 33s 5ms/step - loss: 0.1284 - accuracy: 0.8682 - val_loss: 0.1117 - val_accuracy: 0.8809
    Epoch 4/10
    7168/7168 [==============================] - 38s 5ms/step - loss: 0.1055 - accuracy: 0.8879 - val_loss: 0.0993 - val_accuracy: 0.8921
    Epoch 5/10
    7168/7168 [==============================] - 39s 5ms/step - loss: 0.0901 - accuracy: 0.9173 - val_loss: 0.0798 - val_accuracy: 0.9381
    Epoch 6/10
    7168/7168 [==============================] - 34s 5ms/step - loss: 0.0695 - accuracy: 0.9511 - val_loss: 0.0597 - val_accuracy: 0.9575
    Epoch 7/10
    7168/7168 [==============================] - 30s 4ms/step - loss: 0.0536 - accuracy: 0.9649 - val_loss: 0.0558 - val_accuracy: 0.9628
    Epoch 8/10
    7168/7168 [==============================] - 21s 3ms/step - loss: 0.0482 - accuracy: 0.9664 - val_loss: 0.0473 - val_accuracy: 0.9699
    Epoch 9/10
    7168/7168 [==============================] - 22s 3ms/step - loss: 0.0453 - accuracy: 0.9685 - val_loss: 0.0476 - val_accuracy: 0.9702
```

FIGURE 3. Epochs for adam optimizer with input dense 32 and 16 as sequential ANN model

TABLE 2. Sequential ANN model with various parameters

Sl.No	ANN sequence model	Optimizer and sequential pattern parameter
1	ANN sequence 1	I/P – Dense : 32, 16 O/P – Dense : 5 I/P Activation: ReLu O/P Activation: Sigmoid Optimizer: ADAM
5	ANN sequence 2	I/P – Dense : 32, 16 O/P – Dense : 5 I/P Activation: ReLu O/P Activation: Sigmoid Optimizer: SGD
6	ANN sequence 3	I/P – Dense : 32, 16 O/P – Dense : 5 I/P Activation: ReLu O/P Activation: Sigmoid Optimizer: RMSPROP

Table 2 illustrates the three different optimizer with better sequence pattern as involved parameters are input dense as 32 and 16, output dense as 5 with input and output activation function as ReLu and sigmoid. The optimizer used in the ANN sequence 1 is ADAM followed by ANN sequence 2 and ANN sequence 3 is SGD and RMSPROP.

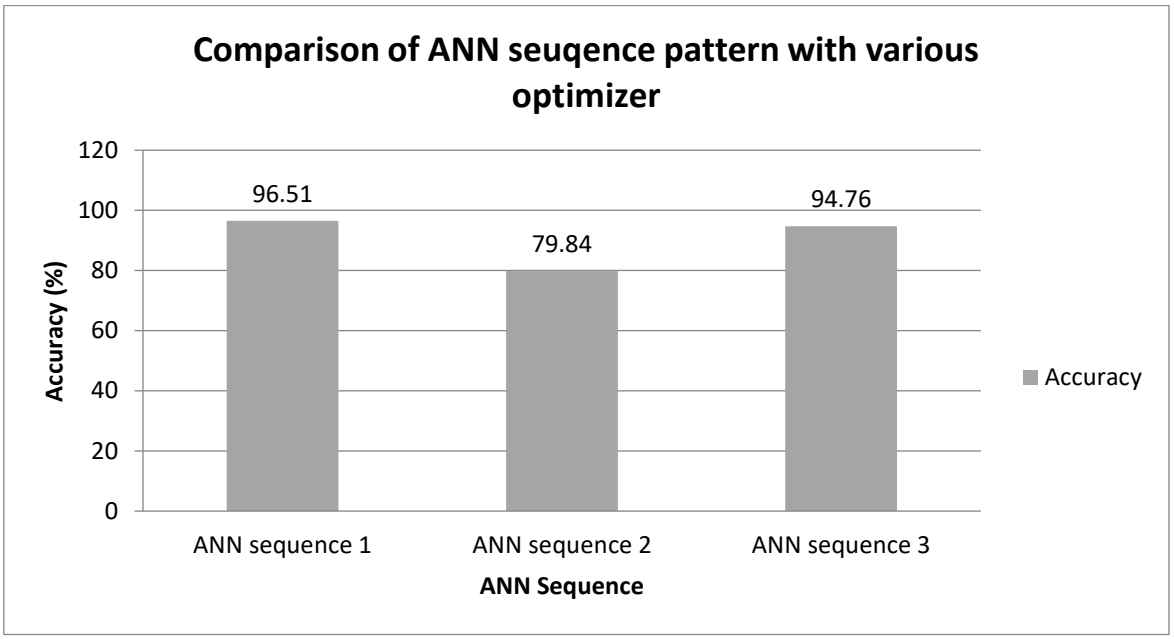


FIGURE 4. Accuracy for different optimizer ANN models

Figure 4 illustrates the accuracy of three different ANN sequence whereas the ANN sequence 1 has accuracy as 96.51% which consist of ADAM optimizer is comparatively better than ANN sequence 2 and ANN sequence 3 are 79.84% and 94.76% respectively.

5. CONCLUSION

To ensure security, it's important to prevent unauthorized access to information as well as defend from unauthorized changes or deletion of user data. The classic definition of security equals it with confidentiality, integrity, and availability. The important aspects of WSN include encouraging numerous researchers to make decisions depending on a variety of security criteria. To address the aforementioned issues, an ANN method with a distinct sequential pattern as the classifier is used in detecting intruder as well as route finding in securing the network from various DoS attacks. The MANET gets trained utilizing the various keras sequence of ANN to identify malicious nodes that exist in the network, with nodes identified based on factors such as energy consumption, delay, etc. The route is modified by removing the malicious nodes from the route, and the network is safeguarded. Furthermore, the suggested sequential ANN model with the best optimizer improved data interpretation and resulted in a high predicted accuracy of 96.51%, which is greater than previous ANN models. Thus, the suggested ANN model produced strong security recognition while also monitoring the shortest path in the AODV protocol for routing over MANET.

REFERENCES

[1]. T. Salam and M. S. Hossen, "Performance analysis on homogeneous LEACH and EAMMH protocols in wireless sensor network," Wireless Personal Communications, vol. 113, no. 1, pp. 189–222, 2020.
[2]. Eltahlawy, A. M., Aslan, H. K., Abdallah, E. G., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A survey on parameters affecting Manet Performance. Electronics, 12(9), 1956.
[3]. Quy, V. K., Nam, V. H., Linh, D. M., & Ngoc, L. A. (2022). Routing algorithms for MANET-IoT networks: a comprehensive survey. Wireless Personal Communications, 125(4), 3501-3525.
[4]. Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V. (2021). An improved hybrid secure multipath routing protocol for MANET. IEEE Access, 9, 163043-163053.
[5]. Sivapriya, N., & Mohandas, R. (2022). Analysis on essential challenges and attacks on MANET security appraisal. Journal of Algebraic Statistics, 13(3), 2578-2589.
[6]. Eltahlawy, A. M., Aslan, H. K., Abdallah, E. G., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A survey on parameters affecting Manet Performance. Electronics, 12(9), 1956.

[7]. Sankar, S. M., Dhinakaran, D., Deboral, C. C., & Ramakrishnan, M. (2023). Safe routing approach by identifying and subsequently eliminating the attacks in MANET. arXiv preprint arXiv:2304.10838.
[8]. Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Ghafoor, M. I., & Sakr, H. A. (2023, January). In MANET: An improved hybrid routing approach for disaster management. In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1-6). IEEE
[9]. Pushpender Sarao" Performance Analysis of MANET under Security Attacks "Journal of Communications Vol. 17, No. 3, March 2022. doi:10.12720/jcm.17.3.1 94-202.
[10]. Borkar, G. M., & Mahajan, A. R. (2020). A review on propagation of secure data, prevention of attacks and routing in mobile ad-hoc networks. International Journal of Communication Networks and Distributed Systems, 24(1), 23.
[11]. Abdelhamid, A., Elsayed, M. S., Jurcut, A. D., &Azer, M. A. (2023). A Lightweight Anomaly Detection System for Black Hole Attack. Electronics, 12(6): 1294. doi: 10.3390/electronics12061294. http://dx.doi.org/10.1504/IJCNDS.2020.100.25198.
[12]. Michael, Hosein, and Aqui Jedidiah. (2022). Mobile Adhoc networks-an overview of risk identification, intrusion detection and machine learning techniques used. 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC). IEEE.
[13]. Srilakshmi, U., Alghamdi, S.A., Vuyyuru, V.A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 10, 14260-14269.
[14]. Nabati, M., Maadani, M., & Pourmina, M.A. (2021). AGEN-AODV: an intelligent energyaware routing protocol for heterogeneous mobile ad-hoc networks. Mobile Networks and Applications, 1-12.
[15]. Dalal, S., Seth, B., Jaglan, V., Malik, M., Surbhi, Dahiya, N., & Hu, Y.C. (2022). An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks. Soft Computing, 26(11), 5377-5388.
[16]. Ravi, S., Matheswaran, S., Perumal, U., Sivakumar, S., & Palvadi, S.K. (2023). Adaptive trustbased secure and optimal route selection algorithm for MANET using hybrid fuzzy optimization. Peer-to-Peer Networking and Applications, 16(1), 22-34.
[17]. Khan, A.F., & Rajalakshmi, C.N. (2022). A multi-attribute based trusted routing for embedded devices in MANET-IoT. Microprocessors and Microsystems, 89.
[18]. Jayantkumar A Rathod & Manjunath Kotari " TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol" International Journal of Computer Networks and Applications (IJCNA) Volume 11, Issue 1, January - February (2024) ISSN: 2395- 0455 . DOI: 10.22247/ijcna/2024/224436.
[19]. C. Edwin Singh and Maria Celestin Vigila " WOA-DNN for Intelligent Intrusion Detection and Classification in MANET Services" Intelligent Automation & Soft Computing, 1737- 1751 , IASC, 2023, vol.35, no.2 ,DOI: 10.32604/iasc.2023.028022.
[20]. Zainab Ali Abbood, Dog˘u Çag˘daş Atilla and Çag˘atay Aydin "Intrusion Detection System through Deep Learning in Routing MANET " Networks Intelligent Automation &Soft Computing, 2023,269 - 280 vol.37, no.1 DOI: 10.32604/iasc.2023.035276.
[21]. C. Edwin Singh, S. Maria Celestin Vigila, Fuzzy based intrusion detection system in MANET, Measurement: Sensors, Volume 26, 2023, 100578, ISSN 2665-9174,https://doi.org/10.1016/j.measen.2022.100578.
[22]. Veeraiah, N., & Krishna, B. T. (2020). An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence. https://doi.org/10.1007/s12065-020-00388- 7.
[23]. Sultan, Mohamad & Sayed, Hesham& Khan, Manzoor., An Intrusion Detection Mechanism for MANETs Based on Deep Learning Artificial Neural Networks (ANNs), International Journal of Computer Networks & Communications (IJCNC) Vol.15, No.1, January 2023.

