Panamerican Mathematical Journal
ISSN: 1064-9735
Vol 33 No. 3 (2023)

Secure Routing and Hybrid SqueezenetFQuantumNN for Intrusion Detection in MANET

Sunita Usturge[1], Dr. T PavanKumar[2]

[1]Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

[2]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Article History:

Received: *11-06-2023*

Revised: *20-08-2023*

Accepted: *18-09-2023*

Abstract:

An efficient Intrusion Detection System (IDS) is essential to secure Mobile Ad-hoc Networks (MANETs) against malevolent attacks. The present IDS still faces challenges in enhancing detection accuracy and in decreasing the false alarm rate. To overcome the above issues, a secure routing protocol for intrusion detection in MANET has been proposed here. In the proposed model, initially, MANET is simulated, which is followed by routing based on Dynamic Source Routing (DSR) routing protocol. Then, intrusion detection is done at Base Station (BS). At the BS, the log files are acquired from the dataset at first and it is normalized using Quintile normalization to transform the data into a structured form. Then, the desired features are selected in the feature selection phase using Wave–Hedges metrics for removing redundant and irrelevant data. Finally, intrusion detection is performed using the proposed hybrid SqueezenetFQuantum Neural Network (SqueezenetFQuantumNN) which is devised by the fusion of Squeeze Net and Quantum Neural Network (QuantumNN). The effectiveness of the proposed SqueezenetFQuantumNN is measured depending on evaluation metrics and is found to attain accuracy of 95.72%, True Positive Rate (TPR) of 93.42%, and True Negative Rate (TNR) of 91.39%.

Keywords: Quintile normalization, Wave–Hedges metrics, Squeeze Net, Quantum Neural Network, Mobile Ad-hoc Networks.

1. Introduction

In communication systems, MANETs are considered as the future mode of communication [3]. MANET is the type of wireless network, which does not require any static structure or server or centralized administrator [6]. Due to its mobility nature, it has a dynamic topology and is regarded as a wireless network [7]. It includes the set of mobile nodes [4], where every node is outfitted with a receiver and transmitter, which enters them to link with the structure via bidirectional communication [2]. The nodes in a set-up converse with -other nodes if the devices are inside the coverage region [3]. These strategies can have diverse speeds, data rates, transmission ranges, and packet sizes. Some basic property of MANET are multihop [7], autonomous, versatile [4], and adaptive. Here, includes different types of MANET protocols, which are Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector (AODV), Destination Sequenced Distance Vector (DSDV), Destination Sequenced Distance Vector (DSDV), Reverse-AODV (RAODV), Temporarily Ordered Routing Algorithm (TORA), and Ad-hoc On-demand Multipath Distance Vector (AOMDV). These networks are also inhibited by packet losses, transmission ranges, Quality of Service (QoS), security, etc [7]. Thus, it requires a dynamic routing protocol for its appropriate functioning [3]. The major process of routing in MANET is to evaluate routes between mobile devices, which satisfy QoS necessities such as end-to-end delay (E2E), and bandwidth and should be capable to process within the narrow energy constraints [12][13][7]. Multipath routing of wireless networks is characteristically utilized to improve error tolerance. It is used for reducing the effects of tampering of packet [4].

In mobile computing devices, wireless technology is increased within the short range, and building benefits of MANETs have become more possible [3]. A valuable non-emergency application of MANET is to give telemedicine maintenance to isolated developing villages and under-developed countries. MANETs, which are characteristically targeted to receive the services under healthcare or emergency conditions, are typically called as healthcare MANETs. MIT Media Lab initiative, Dankest, is an example of h-MANET depending on the network of telemedicine in India [14],[9]. Owing to the characteristics of MANET’s openness, the packet-reducing attack becomes a main attack on the operation of communication in the MANET, which decreases the efficiency of the routing process [6]. These networks are affected by selfish attacks and malicious attacks, which are the vulnerable attacks. The selfish attacks denote a node’s non-cooperation to data sharing in the network. This non-cooperation from nodes, primarily to resend the information contained in a network demolishes more energy of the devices in a network. The malevolent thread is a compromised node, which has deliberately malicious [3]. These attacks cause difficulty in the function of communication between the transmitter and receiver via the dropping packets. The malicious device link fails and enables an illegal connection between the transmitter and receiver node by proceeding with the wrong data [6]. Thus MANET has used more IDS), which are rely on protocols of routing, considering that no node violates the protocols for functioning proper network [3]. The IDS concentrates on identifying the malevolent activity, commonly threads that have effectively infiltrated the defence structure.

The major process of a IDS is to identify the intrusion from the log data gathered from a network. Thus, IDS can give as another wall of a defence and has supreme significance in increased-security networks. Based on identification methods, IDSs in MANETs can be utilized in the detection of anomalies and detection of misuse [8]. The detection-based on misuse methods, also called signature-based, process databases including signatures of known attacks, implying that the methods uses examples or patterns of earlier known attacks and then executes a comparison with the present pattern to detect anomalies. The second famous method is the anomaly detection technique, which is processed depending on the cause of intrusive character changes from the usual user's data pattern data [11]. Both of these techniques can be recognized by a number of Machine Learning (ML) techniques [10]. ML tools, which are often applied in anomaly-based identification systems, have been established to attain a considerable increase in detection rate [11]. But the traditional ML techniques suffer from the small amount of labelled training learning sets and increasingly rely on extracted features using a human, which makes it complex for employment on increased platforms [10]. To protect the new network, Deep Learning (DL is commonly used [1]. DL includes different types of networks, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Restricted Boltzmann Machines (RBMs), and Deep Belief Networks (DBNs). These structures can be operated by training them in semi-supervised, or unsupervised ways [15][10]. DL is also able to automatically identify patterns of attacks or detect the attacks patterns that are revised from the normal character [1].

The prime intention of this method is to justify and develop a SqueezenetFQuantumNN for accomplishing intrusion detection in MANET. Initially, a MANET is simulated, and then, routing is executed based on the DSR routing protocol. Thereafter, intrusion detection is done at BS. At the BS, the log files are acquired from the dataset at first and it is normalized based on Quintile normalization to send the data into structured form. Then, desired features are selected in the feature selection phase using Wave–Hedges metrics for removing redundant and irrelevant data. Finally, intrusion detection is performed by using the proposed hybrid SqueezenetFQuantumNN which is devised by the fusion of Squeeze Net and QuantumNN.

The key component of this paper is given below,

Proposed SqueezenetFQuantumNN for intrusion detection in MANET: Here, a SqueezenetFQuantumNN is proposed for intrusion detection in MANET. Feature selection is done by Wave–Hedges, and intrusion detection in MANET is performed by SqueezenetFQuantumNN and the proposed SqueezenetFQuantumNN is newly devised by the integration of Squeeze Net and QuantumNN.

The remaining work of this paper is arranged as listed, section 2 includes the motivation and survey of conventional papers and their issues. Section 3 details the phases of the proposed SqueezenetFQuantumNN like routing, log file acquisition, normalization, feature selection, and intrusion detection. Section 4 represents the outcome and comparative discussion and finally, Section 5 indicates the conclusion of the paper and provides ideas for the future developments.

2. Motivation

While developing an intrusion detection mechanism in MANET, accurate detection rate, and memory consumption with minimum overhead are critical issues. MANETs have minimum bandwidth and therefore, a large amount of intrusion detection related traffic can cause severe congestion in the network and limit the flow of normal traffic. These issues motivated the conception of the proposed SqueezenetFQuantumNN.

2.1. Literature Review

Meddeb, R., *et al.* [1] developed Deep-IDS with Stacked Auto-encoder (AE) for effective intrusion detection. The method had a better learning capacity and stronger fitting ability and was efficient in avoiding overfitting, but this method did not analyze the impact of an unbalanced dataset on detection performance. Srilakshmi, U., *et al.* [2] devised Bacteria for Aging Optimization Algorithm (BFOA) for the detection of intrusions. The model had the lowest energy usage and faster convergence rate, although the throughput of the model was less when selective forwarding attacks were considered in the model. Prasad, R., [3] devised a Secure Energy Routing (SER) protocol for securing intrusion detection. Low End-to-End (E2E) delay was achieved even with large packet size, but the performance of the model decreased with the increasing speed of nodes. Srilakshmi, U., *et al.* [4] introduced a Genetic Algorithm - Hill Climbing algorithm (GAHC) intrusion detection, and this method consumed less energy and achieved maximum throughput, although the model’s performance was not efficient with selective packet-dropping attacks.

Dilipkumar, S. and Durairaj, M., [5] devised a Centrality Epilson GreedySwarm - Gradient Deep Belief Classifier (CEGS-GDBC) for intrusion detection and this system achieved less memory consumption and computational time. However, this technique not implemented in real-time. Kowsigan, M., *et al.* [6] developed an Alleviating the effects of Black holes through Identification and Protection (ABIP) intrusion detection. This ABIP was effective in maximizing the data flow and had good detection accuracy, although this technique was unable to identify other attacks like gray hole attacks. Talukdar, M.I., *et al.* [7] introduced a Detected Black Hole AODV (D_BH_AODV) technique for intrusion detection, where lower overhead was achieved thus enhancing the network performance, but the scalability of the network was not achieved. Farahani, G., [8] introduced a K-nearest neighbor (KNN) clustering with fuzzy inference for the detection of intrusion. The method was successful in evaluating the trust of the nodes to any other with the measurement of reputation. The technique did not consider the detection of any other attacks other than black hole attacks.

2.2. Challenges

The challenges faced by the techniques based on secure routing for intrusion detection in MANET are organized as follows,

- Stacked AE devised in [1] exhibited greater accuracy than the other existing techniques, but it was unable to build decentralized IDS for processing distributed and heterogeneous data.
- CEGS-GDBC for multi-attack intrusion detection in [5] and this algorithm had fast convergence speed, although this technique had high computational complexity.
- In [6], ABIP was devised for intrusion detection, where avoiding the malevolent node for achieving good rote selection, but it failed to provide a full-fledged intrusion detection system.
- The KNN clustering with fuzzy inference proposed in [8] had a good capability in distinguishing malicious nodes from normal nodes. But the model did not consider other decision-making methods such as neural networks, SVM, naive Bayes, and decision trees to enhance the efficiency of clustering.
- The conventional methods for node of malicious detection were not effective in focusing on consumption time and the execution time was also huge in more cases. Further, more of the conventional systems utilized static threshold value, and is does not adapted to MANET, because of its non-static behavior and was not able in resolving security-associated problems.

3. MANET Model

The interrelation of WSN and MANET is processed in smart environments of IoT, and it is highly prominent among users and is effectively flourishing. In addition, an interface between MANET and wireless sensor with IoT creates a novel model, called as MANET-IoT method. The architecture of MANET-IoT contains the best movement for the user as well as minimizes the computation cost of a network. One of the major aspects affecting the nodes in the MANET-IoT structure isenergy balancing, so the IoT method commonly depends on different MANET methods and wireless sensors and mainly concentrates on selecting a low lengthy, and efficient way for transmitting. Moreover, consider the IoT network,

$$A = \{A_1, A_2, ..., A_b\} \tag{1}$$

Here, A indicates a total number of nodes, and is based on area of coverage. Here, a connection used to link the IoT node is represented as B, and the packets are transferred from the source node to another destination node. IoT nodes are isolated in a gradual manner, where source nodes are positioned in the location of ω_a, ϑ_a. Commonly, the nodes are chosen depending on the factor of trust, which is more improved to choose the cluster head and generate the routing path so that transmission is processed through the secure path. Figure 1 indicates the MANET-IoT system model.

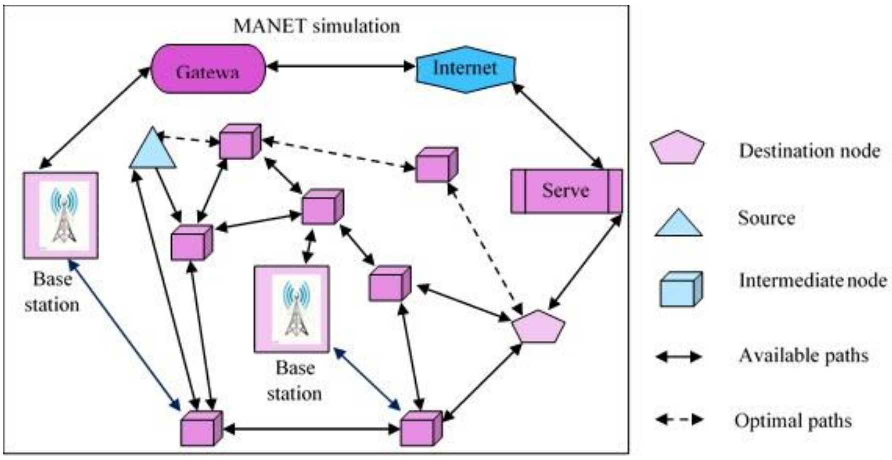


Figure 1. MANET simulation

4. Proposed SqueezenetFQuantumNN for Intrusion Detection in MANET

An efficient routing process is essential to secure MANETs against malicious attacks, and developing such an approach is the major intention of the paper. In the proposed model, initially, MANET is simulated, which is followed by routing based on DSR [16] routing protocol. After the routing process, log files are created which is utilised for the intrusion detection at the base station. Then, intrusion detection is done at BS. At the BS, the log files are acquired from the dataset at first and then it is normalized based on Quantile normalization [17] to transform the data into a structured form. Then, desired features are selected in the feature selection phase using Wave–Hedges metrics [18] for removing redundant and irrelevant data. Finally, the intrusion detection is performed by using the proposed hybrid SqueezenetFQuantumNN, which is devised by the fusion of SqueezeNet [19] and Quantum NN [20], and figure 2 explains the structural framework of the proposed SqueezenetFQuantumNN for intrusion detection in MANET.

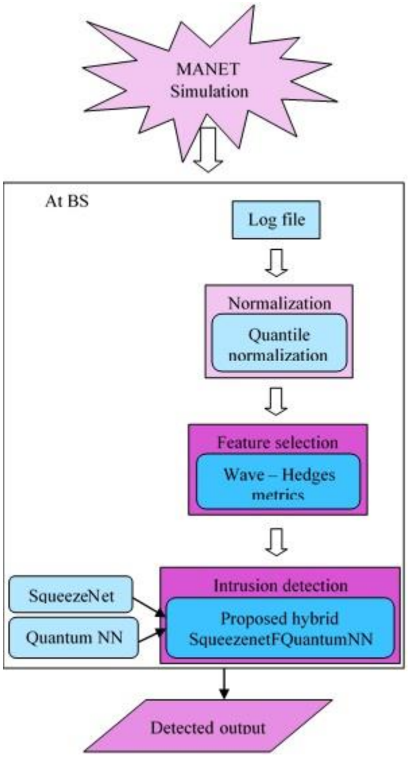


Figure 2 Structure of SqueezenetFQuantumNN for intrusion detection in MANET

4.1 DSR routing protocol-based routing

A route request is flodded via the network in DSR, where nodes join their own address to the routing record and the request is rebroadcasted [16]. This route record is evaluated, whether or not to ensure the determination of the routing performance. Route metrics, which are utilized to make this resolution are connected strength, available energy at a connect vertex, and amount of hops present in the path. The solution to following with a network broadcast is discovered through a fuzzy logic method being sent to a fuzzifier, which transformss them into fuzzy sets. If a route is considered as potential one, then a route request is rebroadcasted and extracts the node and stores the route record. When a route request is reached at the required destination, a route reply is created and transmitted to a sender of the route request by considering a path saved in a route record.

4.2 Intrusion detection at BS

After routing is perfomed, intrusion detection is done at BS. At the BS, the log files are acquired from the dataset at first and then it is normalized using Quantile normalization [17] to transform the data into a structured form. Then, desired features are selected in the feature selection phase using Wave–Hedges metrics [18] for removing redundant and irrelevant data. Finally, the intrusion detection is performed by using proposed hybrid SqueezenetFQuantumNN, which is devised by the fusion of SqueezeNet [19] and Quantum NN [20].

4.2.1. Log file creation

Based on the above DSR routing log file is recorded, where recording is done based on the time, packet size and so on, and it is expressed as,

$$D = \{D_1, D_2, D_\wp, ...D_j\} \tag{2}$$

where, D represents the log file, and the total countd of log file is detailed by j and $D_\wp$ signifies the $\wp$ log file, which has a dimension $g \times h$ and $D_\wp$ is fed to the Normalization process.

4.2.2. Normalization

The acquired log file $D_\wp$ is subjected to the normalization process, where normalization is used for to eliminate the duplication and to avoid the problems with modification of data, which is carried out by quantile normalization [17], and data from the log file is normalized here and its output is denoted as E, which has a size of $e \times f$.

i) Quantile Normalization

This technique entails ranking of data based on the magnitude, which is calculated considering the average value of data occupying a similar rank, and after substituting the values of all data occupying the specific rank with this average value [17]. The consequent step is to rearrange the data of every set in its original order.

4.2.3 Feature selection

The normalized output E is subjected to the feature selection phase. Feature selection technique is used to minimize the amount of input variables by removing the redundant features, where features are selected by Wave Hedges [18] and it is depicted as F, with dimension $e \times l$.

i) Wave Hedges

Feature section of the network is done by wave Hedges [18] and it is formulated as,

$$\delta_{WH} = \sum_{m=1}^{n} \left(1 - \frac{G(I_m, J_m)}{H(I_m, J_m)} \right) \tag{3}$$

where I_m is represented the candidate feature, J_m is signified as the targeted feature, and n is a total number of features and its outcome denoted as, $F_{e \times l}$ where $f > l$, G indicates the minimum, and H represents the maximum.

After computing the Wave Hedges similarity for every feature, the top β features with a high score are selected and applied to the SqueezenetFQuantumNN for intrusion detection.

4.2.4. SqueezenetFQuantumNN

Here, intrusion detection is processed by SqueezenetFQuantumNN, which is created based on the fusion of Squeezenet [19] and QuantumNN [20]. The SqueezenetFQuantumNN includes various laters, such as the residual SqueezeNet model, residual SqueezeNetFQuantum layer, and QuantumNN model. Here, the normalized output E is fed to the residual squeeze net model, which processes the normalized data for detecting intrusions and produces an outcome Z_1, which along with the selected features output F are fed to the residual SqueezeNetFQuantum layer. In this residual SqueezeNetFQuantum layer, fusion is performed to combine the selected features output F, and the detected output Z_1. To improve the output of the fusion, Fractional Calculus (FC) [22] is utilized for combining the terms based on regression modeling. FC is a method for solving complex problems by converting them into Laplace domain.Then, the fusion outcome Z_2 and selected features outcome F is forwarded to the QuantumNN for producing the final detcected output, which is denoted as Z_3. Figure 3 indicates the structural framework of squeezeNetFQuantumNN.

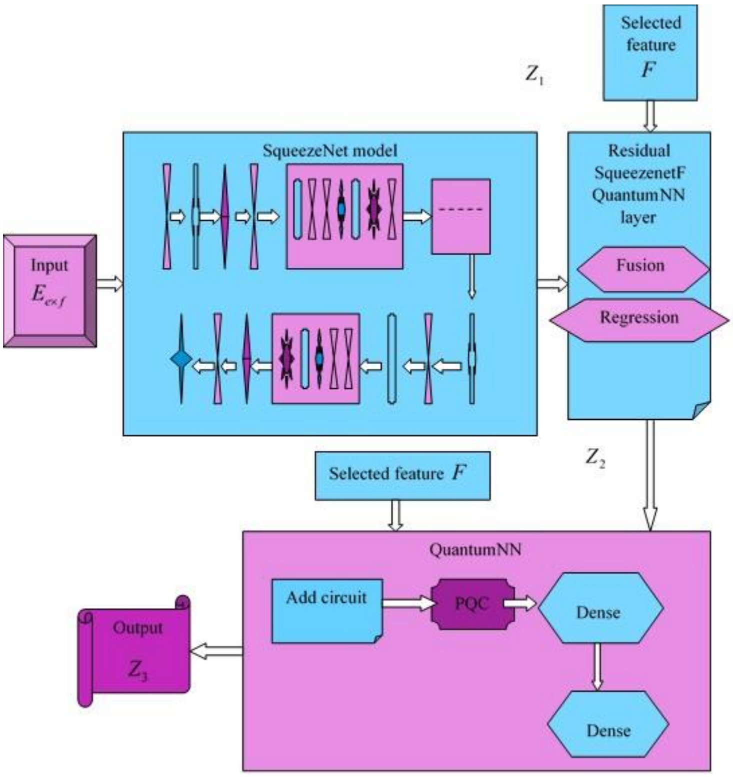


Figure 3. Structural framework of SqueezenetFQuantumNN

i) Squeeze net model

The Squeeze Net model is applied with the selected features $F_{e\times l}$, and it contains a number of parts, which are 1D CNN, residual connection, and squeeze connection [19].

A. 1-D CNNs

The variant of existing 2-D CNN acts as 1-D CNN, where 1-D data takes as input. The CNN includes input and output layers and also has a number of hidden layers. Usually, a hidden layer is consisted as pooling layer and a convolution layer and the architecture of full CNN is designed by stacking these layers. The 1- D CNN utilizes 1D arrays in replacement of 2-D matrix for feature map and kernels and feature map have a number of channels, which can be formulated as,

$$k^o = \beta(p^o * q + r) \tag{4}$$

where, β indicates the activation function, p^o is weight of the o^{th} kernel and $o=\{1,2,...L\}$, L is total convolution kernels, $*$denotes the operation of convolution, q is input sample, k indicates the output sample, and r indicates the bias.

The length K of output k is determined by padding mode. If no padding is functioned and K can be evaluated as,

$$K=\phi\left(\frac{O-P+1}{Q}\right) \tag{5}$$

where, the length of stride value is denoted as Q, ϕ indicates the ceil function, input length is represented as O, and padding mode is denoted as P.

Padding $P-1$ zeros to input is a general exercise to make sure the output size irrespective of kernel size, such a way that, the length is calculated as,

$$K=ceil\left(\frac{O}{Q}\right) \tag{6}$$

B. Residual connections

1-D CNNs have a limited capacity, so the deep structure is adopted aiming to receive the best model with greater complexity. Here, a residual connection is introduced and it depends on the hypothesis that the hybridization of residual mapping, is better than the basic mapping of unreferencing. Commonly, the amount of residual units in a 2 or 3 residual block. Here, the input block is transferred propagation from each shallower block to each deeper block, and it can be represented as,

$$q_M = q_s + \sum_{m=s}^{M-1} L(q_m, N_m) \tag{7}$$

where $L(q_m, N_m)$ is denoted as residual mapping function, N is indicated as a set of weights, the shallower block is denoted as s, and the deeper block is indicated as M.

The connection of residual is presented not only in a single block and also presented among any block M and block s and shallower block's gradient can be expressed below and is based on the backpropagation.

$$\frac{\partial\theta}{\partial q_s}=\frac{\partial\theta}{\partial q_M}\frac{\partial q_M}{\partial q_s}=\frac{\partial\theta}{\partial q_M}\left(1+\frac{\partial}{\partial q_s}\sum_{m=s}^{M-1} L(q_m N_m)\right) \tag{8}$$

where, θ is signified as loss function.

The connection of residual blocks among the 2 blocks includes zero-padding for downsampling and maximizing the dimension is functioned by utilizing the convolution layer with 1×2 stride.

C. Squeeze operation

The intention of fusing channels to receive the features of coupling, and to change the network of residual by modifying the kernel of the first convolution layer of the second block into a kernel of squeeze various size and it is expressed as,

$$Z_1 = \sum_{o1=1}^{L1} \sum_{m=1}^{R} p_m^{o2} q_m^{o1} \tag{9}$$

where, $L1, L2$ indicates the feature maps, $o1 = \{1,2,..L1\}$ and $o2 = \{1,2,...L2\}$, p states that the squeeze operation and R represents the length of the signal, and Z_1 signifies the SqueezeNet outcome.

The output of the squeeze operation can be interpreted as a weighted combination of the feature maps of different channels. By decreasing the error during the training function, an optimal connection of weight is received and figure 4 indicates the structure of SqueezeNet.

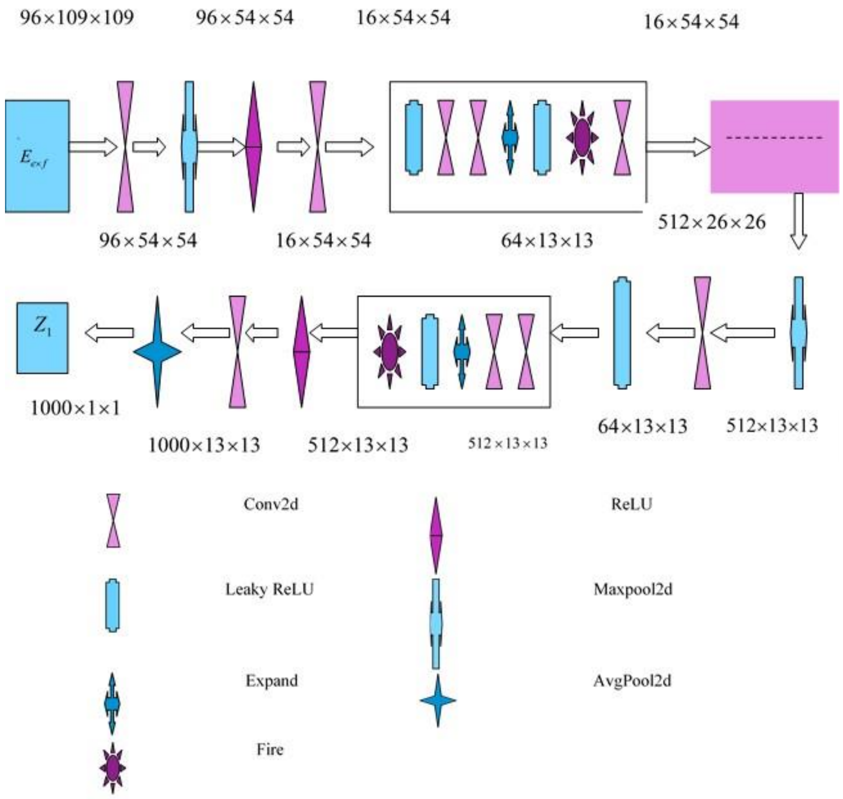


Figure 4. Structure of SqueezeNet.

ii) Residual SqueezeNetFQuantumNN Layer

The SqueezeNet’s output Z_1 and selected features F output fed to the Residual SqueezeNetFQuantumNN layer. Here, both the inputs are combined based regression modeling by FC [22] and is expressed as follows,

$$t = \sum_{i=1}^{w} \sum_{j=1}^{x} F_{i,j} \tag{10}$$

where, w, x indicates the size of the selected features, and t is output from the c^{th} interval, and $F_{e,l}$ indicated selected feature outcme.

From FC [22],

$$q(c+1) = yq(c) + \frac{1}{2} yq(c-1) \tag{11}$$

$$q(c+1) = yt + \frac{1}{2} h\ell_1 \tag{12}$$

$$q(c+1) = y\sum_{u=1}^{w}\sum_{v=1}^{x} S_{u,v} + \frac{1}{2} y\ell_1 = \ell_2 \tag{13}$$

where, y is constant and it's outcome represented as Z_2.

iii) Quantum NN model

The fusion outcome Z_2 and selected features outcome $F_{e\times l}$ is subjected to the process of QuantumNN, which contains layers, add circuit, PQC, and dense block. First layer, Add circuit can either prepend or append to the input batch of circuits, After construction of the network, PQC is performed, which consists of Qconv and QPool layer and is processed the excited state and nonexcite state.Finally, the dense blockis link all layers directly with each other.

The little building block of a QuantumNN is the quantum analog, and quantum perceptron, which are used in classical machine learning (ML) [20]. The arbitrary unitary operator of quantum perceptron has input and output qubits. The initial state of input qubits is a probably unknown mixed state and a fiducial product state is output qubits. The direct cascade of the quantum-circuit architecture of QuantumNNs can carry out a universal quantum structure, although perceptrons have 2 input and one output qubit. Moreover, the observation is in such a way that, each quantum perceptron processes on 4-level qudits in QuantumNN, where every layer is able to do the universal quantum computation.

Quantum neuro is a direct cascade of the quantum-circuit architecture of the QuantumNNs, which can be done by computation of universal quantum, still for two input and one-output qubit perceptrons. A more number of remarkable ability, however, is the concentration that a QuantumNN contains quantum perceptrons perform on 4 level qudits, which travel within every layer, is still able to do the computation of universal quantum. Furthermore, the exchange of qudit perceptrons suffice, it is found actually as a suitable practice to develop noncommuting perceptrons processing on qubits. So one could not expect several more common notations of a quantum perceptron.

A critical parameter of QuantumNN definition is such a way that network outcome can be illustrated as the integration of a cascade of totally positive layer-to-layer transition maps.

$$\lambda^{out} = \chi^{out}(\chi^{M}(....^{2}(\chi^{1}(\chi^{in})).....)) \tag{14}$$

where, $\chi^{k}(X^{k-1}) = tr_{y-1}(\prod_{v=w_s}^{1} T_v^{l}(U^{k-1} \otimes |0...0\rangle_k \langle 0...0|) \prod_{v=`}^{w_l} T_v^{k}) \quad (15)$

T_v^l considers the v^{th} perceptrons processing on layers $k-1$and k, w represents the total quantity of perceptrons processing on layers k $k-1$, χ^{in} denotes the input qubit, and γ^{out} represents the output qudit.

The properties of the output based on no nonzero quantum channel capacity and cannot carry out general quantum computation.The major outcome is the basic quantum analog of the backpropagation method, where final outcome is denoted as Z_3 and figure 5 portrays the Quantum NN.

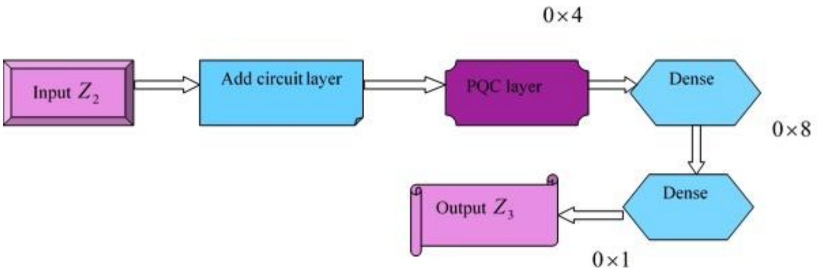


Figure 5. Structure of QuantumNN

Table 1 depicts the algorithm of the proposed SqueezenetFQuantumNN for intrusion detection in MANET

Table1. Algorithm of Proposed SqueezenetFQuantumNN for intrusion detection in MANET

1	**Simulation of MANET**
i	Set up of ns simulator
ii	Setup topography object
iii	Setup of Node parameters
iv	To make path list from source to destination
2	Secure Routing is enhanced using DSR protocol
3	**Log files are created**
	the log files are acquired from the dataset at the dataset
4	**Normalisation-Quantile normalisation**
	to transform the data into a structured form
5	**Feature selection using wave-Hedges metrics**
	to minimize the amount of input variables by removing the redundant features
5	**Intrusion detection using SqueezenetFQuantumNN**
	the normalized output E is fed to the residual squeeze net model, which processes the normalized data for detecting intrusions and produces an outcome

5. Results and Discussion

The proposed SqueezeNetFQuantumNN is analysed for intrusion detection in MANETs. Consequent examination of the proposed SqueezenetFQuantumNN is offered along with the description of the dataset, and evaluation measures utilized are also included.

5.1. Experimental set-up

The experimentation of the proposed SqueezeNetFQuantumNN for intrusion detection is employed utilizing NS2 using the BoT-IoT dataset [21].

5.2. Dataset description

The dataset BoT-IoT [21] is generated by structuring a practical network environment in the Cyber Range Lab of UNSW Canberra. The network structure includes the integration of normal and botnet traffic. The source file of datasets are contained in various formats, providing the real pcap files, which creates csv files and argus files. The files are split, based on attack classification and subclassification to better help of labellng process. The captured pcap file size is 69.3 GB, with more than 72.000.000 records. The extracted traffic flow in csv format size is 16.7 GB. The dataset contains DoS, Service Scan, DoS, and OS

5.3. Evaluation measures

Evaluation measures, such as accuracy, TNR, and TPR are utilized to measure the efficacy of the proposed SqueezenetFQuantumNN.

a) Accuracy

The accuracy rate is calculated in relation to correctly detected output and a whole quantity of utilized log file and which is formulated as,

$$\Delta = \frac{W_a + W_b}{W_a + W_b + X_a + X_b} \tag{16}$$

where Δ symbolizes accuracy, W_a indicates the true positive, W_b denotes the true negative, X_a represents the false positives, and X_b qualifies false negative.

b) TPR

This indicates the ratio of intrusion samples, which are accurately detected by the SqueezenetFQuantumNN out of positive samples and is represented as,

$$\Omega = \frac{W_a}{W_a + X_b} \tag{17}$$

where, Ω indicates the TPR.

c) TNR

TNR is number of normal events correctly recognized to total number of normal events and is represented as,

$$\Phi = \frac{W_b}{W_b + X_a} \tag{18}$$

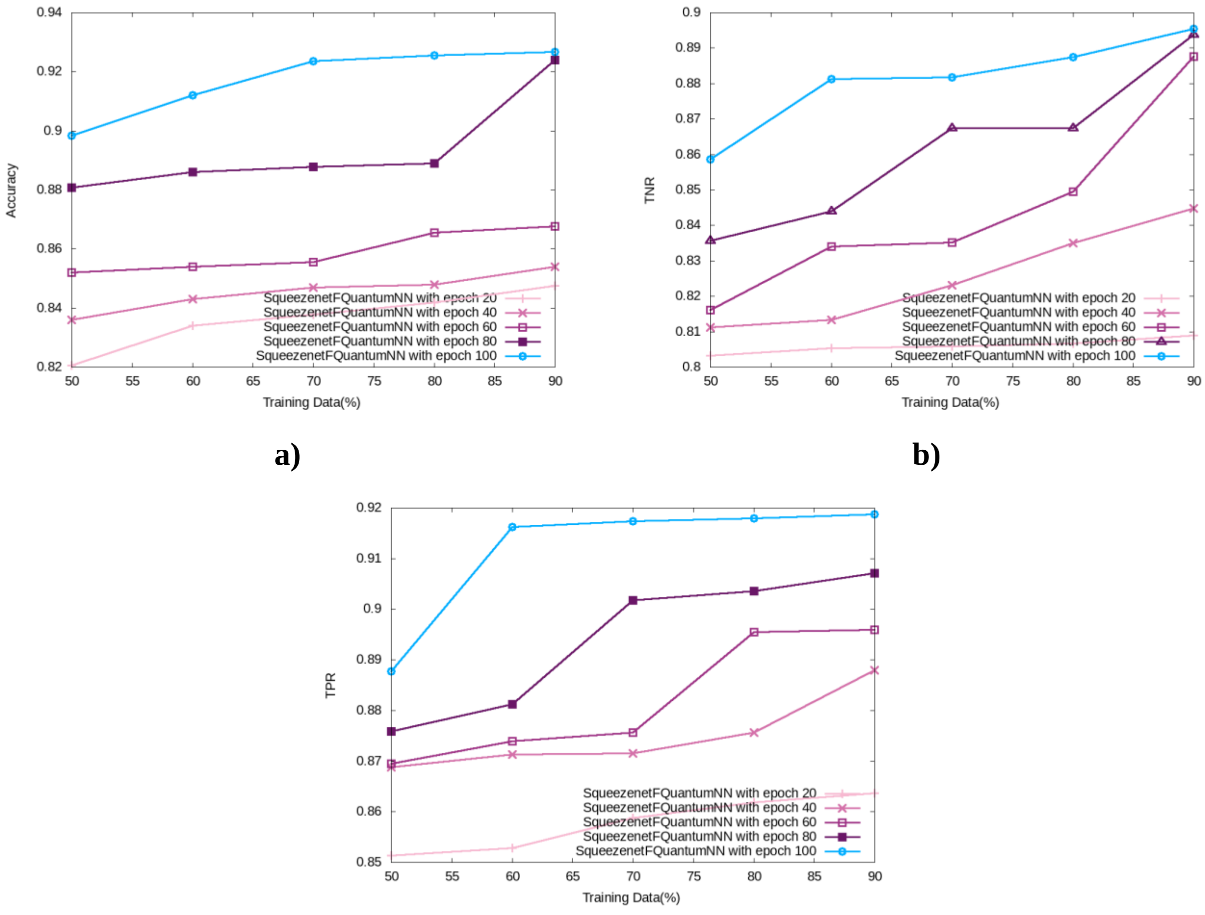
where, Φ represents the TNR

5.4 Performance Analysis

The performance of the proposed SqueezenetFQuantumNN is analyzed based on training data in terms of various epochs like 20,40,60,80, and 100, considering various performance measures, which is expounded on here,

5.4.1 Performance analysis based on training data

Figure 6 displays the performance analysis based on the various performance metrics and it is drawn between training data and number of metrics for different epochs. Figure 6a) exhibits the accuracy-based performance analysis of proposed SqueezenetFQuantumNN. While considering the training data as 90%, the accuracy of SqueezenetFQuantumNN at different epochs like, 20 is 84.76%, 40 is 85.40%, 60 is 86.76%, 80 is 92.39%, 100 is 92.67%. The performance evaluation based on TNR value of proposed SqueezenetFQuantumNN is indicated in figure 6b). The TNR of proposed SqueezenetFQuantumNN computed at various epochs, such as 20 is 80.67%, 40 is 83.50%, 60 is 84.95%, 80 is 86.74% and 100 is 88.75%, with 80% training data. Figure 6c) represents the proposed SqueezenetFQuantumNN's performance evaluation rekated to TPR. For the training data of 80%, the TPR of proposed SqueezenetFQuantumNN's at epoch of 20,40,60,80, and 100 is 86.18%, 87.56%, 89.55%,90.36%, and 91.80%.



a)

b)

c)

Figure 6 Performance examinations of proposed SqueezenetFQuantumNN a) accuracy, b) TNR, and c) TPR

5.5. Comparative techniques

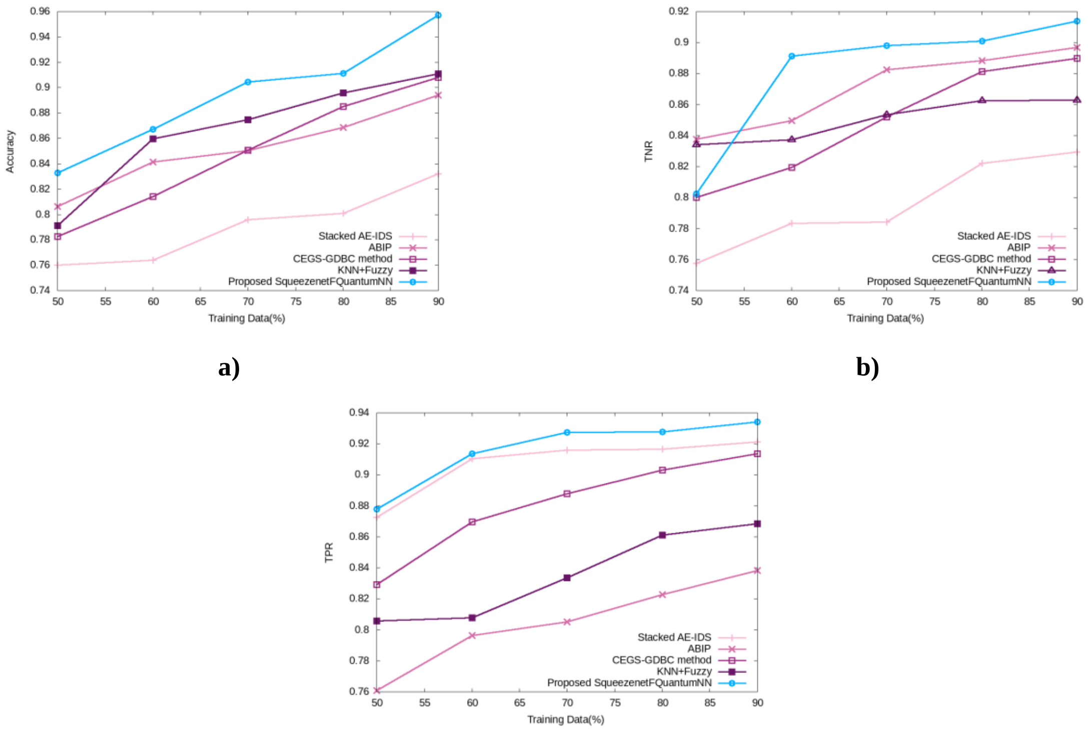
Stacked AE-IDS [1], ABIP[6], CEGS-GDBC method [5], and KNN+Fuzzy[8] are some of the comparative methods for secure routing for intrusion detection in MANET.

5.6 Comparative assessment

Comparative assessment of proposed SqueezenetFQuantumNN for an efficient routing-based ID is essential to secure MANETs against malicious attacks, which is evaluated based on the training data and K value in terms of various performance metrics.

5.6.1 Comparative assessment based on training data

Figure 7) indicates the comparative assessment of proposed SqueezenetFQuantumNN based on various performance measures and adjusting training data. Figure 7a) displays the comparative evaluation based on the accuracy of proposed SqueezenetFQuantumNN. For the training data of 70%, the accuracy of different techniques, such as Stacked AE-IDS is 79.60%, ABIP is 85.02%, CEGS-GDBC method is 85.06%, KNN+Fuzzy is 87.46%, and proposed SqueezenetFQuantumNN is 90.46%, where improved performance of proposed SqueezenetFQuantumNN is 3% better than compared to conventional KNN+Fuzzy technique. The proposed SqueezenetFQuantumNN's TNR value comparative analysis is signified in figure 7b). Considering the training data of 80%, the TNR of the proposed SqueezenetFQuantumNN is 90.09%, and the TNR of other conventional techniques, such as Stacked AE-IDS is 82.22%, ABIP is 88.83%, CEGS-GDBC method is 88.12%, and KNN+Fuzzy is 86.24%. The performance development of proposed technique is 2.2% superior than CEGS-GDBC method. The TPR based comparative assessment is indicated in figure 7c).The TPR measured by various methods is 91.60% for Stacked AE-IDS, 80.52% for ABIP, 88.77% for CEGS-GDBC method, 83.37% for KNN+Fuzzy, and 92.74% for proposed SqueezenetFQuantumNN, for 70% training data. Here, proposed SqueezenetFQuantumNN is 10.10% better than to KNN+Fuzzy.



a)

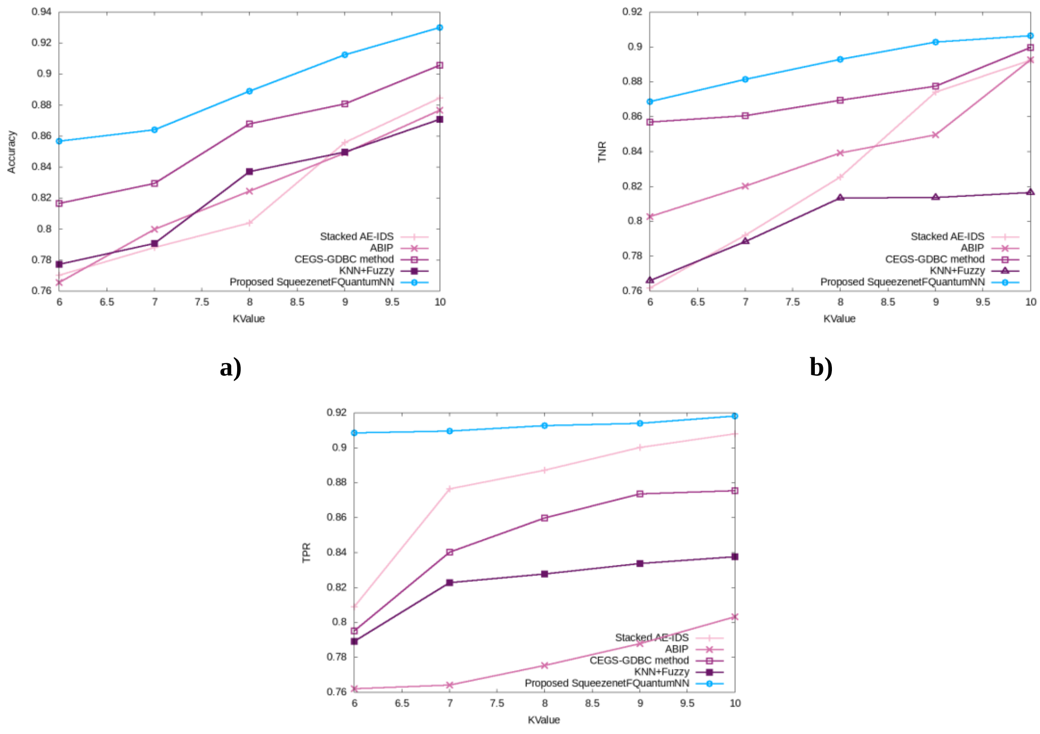
b)

c)

Figure 7 Comparative examination of proposed SqueezenetFQuantumNN based on traing data a) accuracy, b)TNR and c)TPR

5.6.2 Comparative analysis based on K value

Figure 8) signifies the comparative evaluation of the proposed SqueezenetFQuantumNN consideirng various performance measures and adjusting K value. Figure 8a) represents the accuracy based comparative analysis of proposed SqueezenetFQuantumNN. For K value of 10, the accuracy of various techniques, such as Stacked AE-IDS is 88.46%, ABIP is 87.68%, CEGS-GDBC method is 90.58%, KNN+Fuzzy is 87.07%, and proposed SqueezenetFQuantumNN is 93.00%, where performance development of proposed SqueezenetFQuantumNN is 6.3% better than KNN+Fuzzy technique. The TNR based comparative evaluation is indicated in figure 8b). When K value is 9, the TNR of the proposed SqueezenetFQuantumNN is 90.27%, and other conventional technique’s TNR value is Stacked AE-IDS is 87.42%, ABIP is 84.97%, CEGS-GDBC method is 87.74%, and KNN+Fuzzy is 81.37%. The proposed SqueezenetFQuantumNN is 2.8% better compared to CEGS-GDBC method. The figure 8c) signifies the TPR-based comparative analysis. While taking the K value as 8, the TPR figured is 91.28% for proposed SqueezenetFQuantumNN and for other conventional technique, it is 88.71% for Stacked AE-IDS, 77.53% for ABIP, 85.98% for CEGS-GDBC method, and 82.77% for KNN+Fuzzy. Here, proposed SqueezenetFQuantumNN is 5.8% greater than KNN+Fuzzy technique.



a)

b)

c)

Figure 8 Comparative examination of proposed SqueezenetFQuantumNN based on traing data a) accuracy, b)TNR andc)TPR

5.6. Comparative discussion

A comparative discussion of proposed SqueezenetFQuantumNN is represented in table 1 and it is obtained using the log data from the BoT-IoT dataset based on the 90% training data and k value is 10. By analysing the 90% training percentage, the proposed SqueezenetFQuantumNN’ s accuracy is 95.72% and other conventional techniques like, Stacked AE-IDS has 83.22%, ABIP has 89.40%, CEGS-GDBC method has 90.81%, KNN+Fuzzy has 91.09%. Here, usage of Quantile normalization in the proposed SqueezenetFQuantumNN resulted in achieving a superior accuracy. The TNR of various technique, such as 82.95% for Stacked AE-IDS, 89.67% for ABIP, 88.99% for CEGS-GDBC method, 86.29% for KNN+Fuzzy and proposed SqueezenetFQuantumNN is 91.39%. Here, feature selection is done by wave hedge metrics, which led to the high TNR. The TPR of proposed SqueezenetFQuantumNN is 93.42% and the TPR of other conventional methods, like Stacked AE-IDS has 92.11%, ABIP has 83.84%, CEGS-GDBC method has 91.37%, KNN+Fuzzy is 86.85%, and proposed SqueezenetFQuantumNN is 93.42%. The fusion of Squeezenet and QuantumNN resulted in a better TPR value.

Table 1. Comparative examination

Variation	Evaluation metrics	Stacked AE-IDS	ABIP	CEGS-GDBC method	KNN+Fuzzy	Proposed SqueezenetFQuantumNN
Training data	**Accuracy (%)**	83.22	89.40	90.81	91.09	**95.72**
	TNR (%)	82.95	89.67	88.99	86.29	**91.39**
	TPR (%)	92.11	83.84	91.37	86.85	**93.42**
K value	**Accuracy (%)**	88.46	87.68	90.58	87.07	93.00
	TNR (%)	89.24	89.26	89.97	81.66	90.65
	TPR (%)	90.79	80.32	87.55	83.77	91.83

6. Conclusion

MANET is a wireless network of decentralized type, which is thus recommended to utilize intrusion detection, which adjusts the method to discover additional security issues. Hence, the efficient intrusion detection technique is introduced in MANET. Initially, MANET is simulated and is followed by the routing based on DSR routing protocol. Then, intrusion detection is done at BS. At the BS, the log file is acquired from the dataset and it is transmitted to the normalization module, where normalization is done by Quintile normalization. Then, the required features are chosen in the feature selection module, which is performed based on Wave–Hedges metrics. At last, intrusion detection is processed by the proposed hybrid SqueezenetFQuantumNN, which is devised by the fusion of Squeeze Net and QuantumNN. Moreover, the effectiveness of proposed SqueezenetFQuantumNN is evaluated based on several performance metrics, like accuracy, TPR, and TNR and it reached the greater values of 95.72% for accuracy, 93.42% for TNR, and 91.39% for TPR. Furthermore, in consequent work, more feature selection techniques will be included for more effective intrusion detection in MANET.

References

[1] Meddeb, R., Jemili, F., Triki, B. and Korbaa, O., “A Deep Learning based Intrusion Detection Approach for MANET”, 2022.

[2] Srilakshmi, U., Alghamdi, S.A., Vuyyuru, V.A., Veeraiah, N. and Alotaibi, Y., “A secure optimization routing algorithm for mobile ad hoc networks”, IEEE Access, vol.10, pp.14260-14269, 2022.

[3] Sable, N.P., Rathod, V.U. (2023). Rethinking Blockchain and Machine Learning for Resource-Constrained WSN. In: Neustein, A., Mahalle, P.N., Joshi, P., Shinde, G.R. (eds) AI, IoT, Big Data and Cloud Computing for Industry 4.0. Signals and Communication Technology. Springer, Cham. https://doi.org/10.1007/978-3-031-29713-7_17.

[4] Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S.A., Khalaf, O.I. and Subbayamma, B.V., “An improved hybrid secure multipath routing protocol for MANET”, IEEE Access, vol.9, pp.163043-163053, 2021.

[5] Dilipkumar, S. and Durairaj, M., “Epilson Swarm Optimized Cluster Gradient and deep belief classifier for multi-attack intrusion detection in MANET”, Journal of Ambient Intelligence and Humanized Computing, pp.1-16, 2021.

[6] Nilesh P. Sable, Vijay U. Rathod, Parikshit N. Mahalle, Jayashri Bagade, Rajesh Phursule ; Internet of Things-based Smart Sensing Mechanism for Mining Applications, Industry 4.0 Convergence with AI, IoT, Big Data and Cloud Computing: Fundamentals, Challenges and Applications IoT and Big Data Analytics (2023) 4: 132. https://doi.org/10.2174/9789815179187123040012.

[7] Kowsigan, M., Rajeshkumar, J., Baranidharan, B., Prasath, N., Nalini, S. and Venkatachalam, K., "A Novel Intrusion Detection System to Alleviate the Black Hole Attacks to Improve the Security and Performance of the MANET", Wireless Personal Communications, 2021.

[8] Sable, Nilesh P. , Rathod, Vijay U. , Parlewar, Pallavi , Rathod, Smita B. , Waghmode, Santosh T. & Rathod, Rahul R. (2024) Efficient lightweight cryptography for resource-constrained WSN nodes, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-A, 349–359, DOI: 10.47974/JDMSC-1888.

[9] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F. and Ahmed, A.S., "Performance improvements of AODV by black hole attack detection using IDS and digital signature", Wireless Communications and Mobile Computing, pp.1-13, 2021.

[10] Farahani, G., "Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks", Security and Communication Networks, pp.1-15, 2021.

[11] Das, S., Mukhopadhyay, A., Saha, D. and Sadhukhan, S., "A markov-based model for information security risk assessment in healthcare MANETs", Information Systems Frontiers, vol.21, pp.959-977, 2019.

[12] N. P. Sable, V. U. Rathod, M. D. Salunke, H. B. Jadhav, R. S. Tambe, and S. R. Kothavle, "Enhancing Routing Performance in Software-Defined Wireless Sensor Networks through Reinforcement Learning", International Journal of Intelligent Systems and Applications in Engineering (IJISAE), vol. 11, no. 10s, pp. 73–83, Aug. 2023.

[13] Lansky, J., Ali, S., Mohammadi, M., Majeed, M.K., Karim, S.H.T., Rashidi, S., Hosseinzadeh, M. and Rahmani, A.M., "Deep learning-based intrusion detection systems: a systematic review", IEEE Access, vol.9, pp.101574-101599, 2021.

[14] Y. Mali, V. U. Rathod, D. Ajalkar, D. S. Khemnar, S. Kolpe and S. Patil, "Role of Blockchain in Health Application using Blockchain Sharding," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10306760.

[15] Nishani, L. and Biba, M., "Machine learning for intrusion detection in MANET: a state-of-the-art survey", Journal of Intelligent Information Systems, vol.46, pp.391-407, 2016.

[16] Adam, S.M. and Hassan, R., "Delay aware reactive routing protocols for QoS in MANETs: A review", Journal of applied research and technology, vol.11, no.6, pp.844-850, 2013.

[17] Malathy, S., Porkodi, V., Sampathkumar, A., Hindia, M.N., Dimyati, K., Tilwari, V., Qamar, F. and Amiri, I.S., "An optimal network coding based backpressure routing approach for massive IoT network", Wireless Networks, vol.26, pp.3657-3674, 2020.

[18] Pentland, A., Fletcher, R. and Hasson, A., "Daknet: Rethinking connectivity in developing nations", Computer, vol.37, no.1, pp.78-83, 2004.

[19] Rathod, V.U. and Gumaste, S.V., 2022. Role of Neural Network in Mobile Ad Hoc Networks for Mobility Prediction. International Journal of Communication Networks and Information Security, 14(1s), pp.153-166.

[20] Zhang, Q., Yang, L.T., Chen, Z. and Li, P., "A survey on deep learning for big data", Information Fusion, vol.42, pp.146-157, 2018.

[21] M. D. Salunke, V. U. Rathod, Y. K. Mali, R. S. Tambe, A. A. Dange and S. R. Kothavle, "A Prediction and Classification Process for DDoS Attacks Using Machine Learning," 2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCUBEA58933.2023.10392278.

[22] Zhao, Y., Wong, L. and Goh, W.W.B., "How to do quantile normalization correctly for gene expression data analyses", Scientific reports, vol.10, no.1, pp.1-11, 2020.

[23] Vijay U. Rathod* & Shyamrao V. Gumaste, "Effect Of Deep Channel To Improve Performance On Mobile Ad-Hoc Networks", J. Optoelectron. Laser, vol. 41, no. 7, pp. 754–756, Jul. 2022.

[24] Cha, S.H., "Comprehensive survey on distance/similarity measures between probability density functions", City, vol.1, no.2, pp.1, 2007.

[25] V. U. Rathod and S. V. Gumaste, "An Effect on Mobile Ad-Hoc Networks for Load Balancing Through Adaptive Congestion Routing," 2023 International Conference on Integration of Computational Intelligent System (ICICIS), Pune, India, 2023, pp. 1-5, doi: 10.1109/ICICIS56802.2023.10430257.

[26] Beer, K., Bondarenko, D., Farrelly, T., Osborne, T.J., Salzmann, R., Scheiermann, D. and Wolf, R., "Training deep quantum neural networks", Nature communications, vol.11 no.1, p.808, 2020.

[27] V. U. Rathod and S. V. Gumaste, "Role of Deep Learning in Mobile Ad-hoc Networks", IJRITCC, vol. 10, no. 2s, pp. 237–246, Dec. 2022.

[28] V. U. Rathod, N. P. Sable, P. Dhamdhere, R. R. Rathod, S. Y. Zurange and D. R. Naik, "Exploring the Horizons of Speaker Recognition: Contemporary Advancements and Prospective Trajectories in the Age of Deep Learning," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1-5, doi: 10.1109/I2CT61223.2024.10543582.

[29] Guan, W., Zhou, H., Su, Z., Zhang, X. and Zhao, C., "Ship steering control based on quantum neural network", Complexity, pp.1-10, 2019.

[30] Y. K. Mali, V. U. Rathod, N. P. Sable, R. R. Rathod, N. A. Rathod and M. N. Rathod, "A Technique for Maintaining Attribute-based Privacy Implementing Blockchain and Machine Learning," 2023 Global Conference on Information Technologies and Communications (GCITC), Bangalore, India, 2023, pp. 1-4, doi: 10.1109/GCITC60406.2023.10426183.