Indonesian Journal of Electrical Engineering and Computer Science
Vol. 43, No. 2, August 2026, pp. 460~471
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v43.i2.pp460-471

Probability density-based quantized spiking neural network for efficient intrusion detection in mobile ad hoc networks

Amruth Veerabhadraiah[1], Devaraj Verma Chitragar[2]
[1]Department of Information Science and Engineering, Maharaja Institute of Technology Mysore, Jain (Deemed to be University), Bengaluru, India
[2]Department of Computer Science and Engineering (Artificial Intelligence), Jain (Deemed to be University), Bengaluru, India

Article Info

Article history:

Received Sep 26, 2024
Revised May 27, 2026
Accepted Jun 29, 2026

Keywords:

Adaptive moth flame
Convolutional neural network
Long short-term memory
Mobile ad hoc network
Neural network
Probability density
Quantization spiking

ABSTRACT

Mobile ad hoc networks (MANETs) enable infrastructure-free wireless communication through decentralized and self-organizing network architectures, making them well suited for dynamic environments such as disaster recovery, military operations, and intelligent transportation systems. However, their distributed topology and continuously changing network structure expose them to sophisticated routing attacks, particularly blackhole attacks (BHA) and wormhole attacks (WHA), which significantly degrade network reliability and challenge conventional intrusion detection techniques. Existing deep learning approaches often struggle to accurately distinguish malicious from legitimate traffic because of high-dimensional feature spaces and limited computational resources in MANET environments. To address these challenges, this paper proposes a probability density-based quantized spiking neural network (PDF-QSNN) framework for efficient intrusion detection in MANETs. The proposed framework first employs adaptive moth flame optimization (AMFO) to identify the most informative features, thereby reducing data redundancy and computational complexity. Subsequently, probability density-based feature encoding generates a discriminative probabilistic representation of network behavior, while the quantized spiking neural network performs lightweight and energy-efficient intrusion classification. Experimental evaluations using simulated BHA and WHA datasets demonstrate that the proposed framework achieves classification accuracies of 92.86% and 91.56%, respectively, outperforming conventional convolutional neural networks (CNN) and stacked recurrent long short-term memory (SRLSTM) models. These results demonstrate the effectiveness of the proposed framework for accurate and computationally efficient intrusion detection in resource-constrained MANET environments.

Corresponding Author:

Amruth Veerabhadraiah
Department of Information science and Engineering, Maharaja Institute of Technology Mysore India and Jain (Deemed to be University)
Bengaluru, India
Email: amruthv_ise@mitmysore.in

1. INTRODUCTION

Mobile ad hoc networks (MANETs) consist of autonomous mobile nodes that communicate through wireless links without relying on a fixed network infrastructure. The highly dynamic topology, caused by frequent node mobility, makes routing a challenging task because routing protocols must continuously discover and maintain valid communication paths under rapidly changing network conditions [1], [2]. This

decentralized architecture also increases the vulnerability of MANETs to various routing attacks, resulting in packet loss, service disruption, and degradation of overall network performance. Although MANET routing protocols are designed to establish reliable communication among network nodes, ensuring network security remains difficult because of the heterogeneous characteristics of participating devices and the absence of centralized management [3], [4].

Intrusion detection systems (IDSs) play a critical role in strengthening the security of MANETs by continuously monitoring network activities and identifying malicious behavior before it compromises network operations. Among the various security threats, blackhole attacks (BHA) and wormhole attacks (WHA) are considered two of the most destructive routing attacks because they manipulate packet forwarding and routing information, thereby disrupting normal communication and significantly reducing network reliability [5]. Consequently, an effective IDS should not only protect individual nodes but also preserve the integrity, availability, and reliability of the entire network by accurately detecting and mitigating multiple attack types.

Traditional MANET routing protocols primarily focus on identifying efficient routing paths for packet transmission but often lack robust mechanisms for detecting sophisticated and evolving cyberattacks [6]. More recently, deep learning (DL)-based approaches have emerged as promising solutions because of their ability to automatically learn complex feature representations from large-scale network traffic data [7], [8]. Compared with conventional machine learning methods, DL models can capture nonlinear relationships and temporal dependencies in network traffic, making them particularly suitable for identifying subtle attack behaviors in dynamic MANET environments. However, achieving high detection accuracy remains challenging due to the high dimensionality of network features, continuously changing network topology, and limited computational resources available at mobile nodes.

This study employs simulated BHA and WHA datasets to investigate the effectiveness of DL for intrusion detection in MANETs. The primary objective is to improve intrusion detection performance by accurately distinguishing malicious nodes from legitimate network participants while enhancing overall classification accuracy. The proposed framework incorporates node behavior analysis and feature selection to identify the most informative network characteristics, thereby improving the efficiency and robustness of the detection process [9]–[11]. By learning complex traffic patterns and sequential communication behavior, the DL model can effectively recognize both normal and malicious network activities.

After the training phase, the proposed model continuously analyzes incoming network traffic and classifies each communication instance as either benign or malicious [12], [13]. In particular, the model identifies abnormal packet-dropping behavior and rapid packet loss responses that are characteristic of BHA, while simultaneously detecting abnormal routing shortcuts and unusually low hop-count values that indicate the presence of WHA [14], [15]. These capabilities enable the proposed intrusion detection framework to provide accurate and timely identification of routing attacks, thereby improving the security, reliability, and resilience of MANET communications.

Although MANET provides decentralized management, its limited bandwidth renders it vulnerable to security threats, negatively impacting classification accuracy. In this research, the probability density function-quantization spiking neural network (PDF-QSNN) technique is applied in MANET environments to enhance classification accuracy. The PDF within the neural network prioritizes data that is likely to represent significant attack patterns or behaviours in the MANET environment. The following sections discuss in detail the exisiting attack detection models in IDSs within the MANET environment, highlighting their advantages and disadvantages. Abdan and Seno [16] presented a DL-based convolutional neural network (CNN) for classification using simulated data. In this approach, a significant number of nodes and factors were required to effectively train the nodes in the MANET environment. Then, relevant features are automatically extracted from the raw data, reducing the need for manual features and handling other variations in data such as changes in node position, mobility patterns and environment conditions in MANETs. However, CNN required large amounts of simulated data for attack analysis, which made the model difficult to apply in distributed and dynamic environments. Vincent and Duraipandian [17] introduced an attack detection method to address security issues in MANETs, where reduced packet delivery ratios were identified on the simulated data. Their approach incorporated optimization techniques for determining the shortest path between nodes using the particle bee colony swarm optimization algorithm (PBCO) algorithm, along with feature selection. The ada-boost–random forest (AB-RF) for classification performed effectively with improved accuracy. However, AB-RF model was difficult to interpret and required the transmission of a large amount of data for efficient performance, leading to communication challenges that affected classification accuracy.

Prasad *et al.* [18] presented a mutation based artificial neural network (MANN) classifier network designed to transfer data to the destination through intermediate nods, and monitor intrusion attacks such. This approach was applied on the simulated data for attack analysis in MANETs, enabling flexible routing and incorporating diversity into the mutation process of ANN learning, which helped explore a broader range of solutions and enhanced accuracy. However, the MANN technique faced challenges in analyzing

vulnerability, as overfitting on simulated data affected classification accuracy. Deivakani *et al*. [19] developed stacked recurrent long short-term memory (SRLSTM) method for attack detection in IDSs, aimed at the monitoring of data transmission in MANETs. This approach captured long-term dependencies, reflecting the dynamic behaviour of network topology, node interactions and communication patterns within the MANET environment. However, SRLSTM approaches were obliged to maximise the overall performance of the IDS framework by considering factors such as node energy, because issues with misclassification negatively impacted the model's classification accuracy. Krishnasamy *et al*. [20] developed a dual interactive wasserstein generative adversarial network (DIWGAN) approach for analysing IDSs using the simulation data in MANETs. The model was provided with a more stable training process to learn features efficiently and analyse attacks using simulated data in the MANETs, promising improved accuracy and reliability. However, the DIWGAN approach faced challenges with data variables that were categorical, normally distributed or non-parametric, leading to inefficiency in communication within the network.

From the overall analysis, it is noted that the previous models carry the following limitations: MANET's limited potential to offer decentralized management and restricted bandwidth which made the model vulnerable to security threats, negatively impacting the model's classification accuracy. In this research, the PDF-QSNN technique is efficiently implemented in a MANET environment for enhanced classification accuracy. The PDF utilized in neural networks prioritizes data that is more likely to represent significant patterns or behaviours in the MANET environment. The raw data is obtained from the simulated data based on the black hole, wormhole and sinkhole attacks in intrusion detection in MANETs.

The main contributions of this research can be summarized as follows. First, an adaptive moth flame optimization (AMFO) algorithm is incorporated for feature selection to effectively address the high-dimensional nature of MANET simulation data. By identifying the most informative features while eliminating redundant and irrelevant attributes, the proposed feature selection strategy reduces computational complexity, improves model efficiency, and enhances the representation of network characteristics that are critical for intrusion detection. Second, this study proposes a PDF-QSNN framework for efficient intrusion detection in MANETs. The proposed framework employs probability density-based feature encoding to generate a more discriminative representation of network traffic patterns, enabling the quantized spiking neural network to distinguish normal and malicious behaviors more accurately. Consequently, the framework achieves improved classification performance by emphasizing significant behavioral patterns associated with network intrusions. Finally, the integration of probability density-based feature representation with AMFO-driven feature selection produces a robust and computationally efficient intrusion detection framework capable of identifying sophisticated routing attacks, including BHA and WHA. The AMFO algorithm effectively reduces feature dimensionality and computational overhead, while the PDF-QSNN framework enhances classification accuracy through lightweight neuromorphic learning. Together, these components provide an effective intrusion detection solution that is well suited to the dynamic, decentralized, and resource-constrained characteristics of MANET environments. The remainder of this paper is organized as follows. Section 2 presents the proposed PDF-QSNN framework and describes its architecture, feature selection strategy, and intrusion detection process. Section 3 discusses the experimental setup, performance evaluation, and comparative analysis with existing methods. Finally, section 4 concludes the paper and outlines potential directions for future research.

2. PROPOSED METHOD

The proposed PDF-QSNN technique demonstrates efficient performance in the MANET environment with an improved classification accuracy. By utilizing the PDF, the neural network prioritizes data that is more likely to represent significant patterns or behaviours in the MANET environment. Feature selection using the AMDO algorithm is effective in handling high dimensional feature spaces which are often the simulation data, reducing dimensionality by selecting an essential feature and improving the performance of classification stages. The (F_{RP}) represents the evaluated energy, which is essential for determining the critical energy of nodes [21]. The energy model assumes full energy of a node at start and remaining energy p at time t is represented $(E_p^{rem}(t))$ by (1) and (2).

$$(E_p^{rem}(t)) = E_p^{rem}(t-1) - E_p^{T_r} \times k(t-1,t) \quad (1)$$

$$E_m^{rem}(q) = R \quad (2)$$

Where, $E_p^{T_r}$ denotes the energy required to transfer a data bit, k denotes the amount of bit transmitted in the duration $q-1$ to q. E_m^{Wc} denotes the total energy required for acquiring an individual data bit from time $q-$

1 to q, as defined in (2). At the initial stage, the remaining energy is assumed to be full battery capacity. Figure 1 illustrates the block diagram of the proposed method.

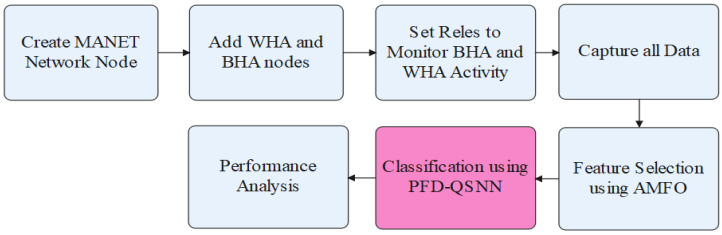

Figure 1. Block diagram of the proposed method

Mobility is designed to describe how mobile nodes move, with their location, velocity, and acceleration changing over time. The performance of the routing protocol is evaluated based on these mobility patterns. The initial location of the node considers the specific direction, evaluated velocity, and distance. Mobility models help calculate the performance of routing protocols by simulating node movement patterns. They assist in the design of efficient routing protocols by predicting the movement of nodes and adjusting network paths accordingly.

2.1. Data Simulation

The BHA and WHA [16] are considered with a finite number of nodes simulated in MATLAB 2019b setup. The topology is generated by considering the nodes and protocols across various network programs for transferring packets during the network simulation process. This simulation is completed in a MANET environment with 50 regular nodes and 2 malicious nodes. The topology spans a $1000 \times 1000m^2$ area, with spontaneous node activity and a 300-meter radio range for each node in the simulation. A total of 4000 samples are collected, comprising both normal and malicious samples. The dataset is compiled and labelled with 20 attributes, forming a high-volume dataset focused on BHA and WHA in the context of ad hoc networks.

2.2. Feature selection

The MOF [22], [23] algorithm is a heuristic optimization technique inspired by spiral navigation to analyse of MANET environment. In a MANET, the topology is constantly changing and the network is susceptible to various security threats. AMDO, inspired by moths' spiral navigation is efficiently explores and exploited by adjusting its search behavior based on proximity to a potential solution. This approach is highly effective in addressing the dimensionality reduction issue and selecting relevant features for learning attack patterns in intrusion detection using the simulated data. The AMDO algorithm enhances computational efficiency while significantly improving classification accuracy in MANETs. In the MFO algorithm, moths are treated as search agents represented in a matrix $M(t)$ that explores a D-dimension search space. The total number of moths in this matrix is denoted by N and moths are modelled using (3) and (4). Where, n represents the amount of moths and d denotes the dimensionality of the issue where each moth is navigating. The set OM is used to represent the fitness values as expressed in (4). Where, OM_1 represents the fitness values of the ith moth and other MFO population is denoted F, which is denoted in (5) and (6).

$$M = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{1d} \\ m_{21} & m_{22} & \dots & m_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nd} \end{bmatrix} \quad (3)$$

$$OM = \begin{bmatrix} OM_1 \\ OM_2 \\ \vdots \\ OM_n \end{bmatrix} \quad (4)$$

$$F = \begin{bmatrix} F_{11} & F_{12} & \dots & F_{1d} \\ F_{21} & F_{22} & \dots & F_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ F_{n1} & F_{n2} & \dots & F_{nd} \end{bmatrix} \quad (5)$$

$$OF = \begin{bmatrix} OF_1 \\ OF_2 \\ \vdots \\ OF_n \end{bmatrix} \quad (6)$$

The set of fitness values is described by (6), where OF_i represents fitness values of ith flame. The moths and flames represent candidate solutions, but are treated and updated differently during each iteration. Moths are actual moving agents within the search space, while flames denote the better positions that have been identified. Moths move around flames, with the recent optimal solutions being stored in the flame, which is updated when the best solution is discovered. This mechanism ensures that the algorithm is equipped with optimal solutions. The location of every moth is improved based on the formula provided in (7). Where, M_i denotes the ith moth, F_j denotes the jth flame, and S denotes the spiral function. The moth's spiral flame and logarithmic search is denoted by (8). Where, b denotes the constant shape of logarithmic spiral and t denotes an arbitrarily value within the range od $[-1,1]$, and D_i indicates the velocity between moth and flame which is denoted by (9).

$$M_i = S(M_i, F_j) \quad (7)$$

$$S(M_i, F_j) = D_i . e^{bt} . cos(2\pi t) + F_j \quad (8)$$

$$D_i = |F_j - M_i| \quad (9)$$

Where, M_i denotes ith moth, F_j denotes jth flame and D_i denotes distance between MANET of ith moth for jth flame. To further improve global exploitation and enhance the MFO search capability, a parameter r is introduced to increase the moth search speed with values ranging between $[r, 1]$. During the iteration process, r is linearly reduced from -1 to -2, allowing the moths to search by surrounding the flames rather than flying directly between them. This is defined by (10).

$$Flame_{no} = round\left(n - l * \frac{n-1}{T}\right) \quad (10)$$

Where, n denotes the maximum amount of flames, l denotes current iteration number and T denotes maximum iteration number. This balances global exploration and local exploration. To enhance local exploitation, a reduction mechanism for the number of flames is introduced, where flames decrease over time in the iteration process.

2.2.1. Proposed adaptive moth flame optimization

The MFO algorithm quickly reduces the number of flames over time. It involves various approaches to avoid getting trapped in local optima solutions. The multiple flame guidance mechanism is utilized to improve the population's search ability by using multiple flames simultaneously during the search process.

a. Adaptive flame number strategy

The adaptive flame does not occur in every generation. The global optimal value is updated, and the position is utilized in every generation, as shown in (11) and (12). The adaptive strategy improves the algorithm's ability to escape local optima, enhancing its performance in finding the global optimum. By dynamically adjusting exploration and exploitation, it avoids getting trapped in local optima and continues to explore a better search space.

$$= \begin{cases} Flame_{no} = Flame_{no} + max\ succes, \\ max\ Success = maxSuccess + max\ Success * adjust\ Success \end{cases} \quad (11)$$

$$= \begin{cases} Flame_{no} = Flame_{no} + max\ Failures, \\ max\ Failures = max\ Failures + max\ Failures * adjust\ Failures \end{cases} \quad (12)$$

In this context, the initial values for maximum successes and failures are used to enhance the phase count of flames, representing the number of flames. The success and failure rates are adjusted to determine the degree of change. Additionally, once the global optimum is improved, the number of flames gradually decreases, allowing for a more efficient balance between exploration and exploitation in the search space.

b. Multiple flame mechanism

The multiple flame mechanism is inspired by the differential evolution technique, where the various vectors between two flames are arbitrarily chosen from a flame population which is considered as the direction of the vector. To balance multiple flame guidance with the search of the spiral, parameter rc is arbitrarily choosen between the range [0,1]. The flame guidance mechanism is executed when condition d<rc is satisfied as shown in (13).

$$S(M_i, F_j) = \begin{cases} D_i.e^{bt}.cos(2\pi t) + F_j, & if\ r\ and < rc, \\ rand * (F_m - F_p) + F_j, & otherwise, \end{cases} \quad (13)$$

Where, j, m and p are distict indexes, M_i denotes ith moth, F_j denotes jth flame and $rand$ denotes arbitrarily in intervals of [0,1] respectively. This optimization process identifies the most relevant features by balancing exploration and exploitation, avoiding unnecessary updates that lead to premature convergence. Reducing the number of features helps focus on the most impactful attributes that are essential for distinguishing between normal network behaviour and attack patterns. The selected features are fed into the classification process, they help to improve accuracy.

2.3. Classification

A quantized SNN that utilizes the probability PDF enhances the approach for the efficiency of neural networks in MANET [24], [25]. Its ability to process temporal patterns makes it particularly useful for detecting these kinds of attacks in a dynamic MANET environment. This method integrates quantization with PDF to enhance the performance of neural networks in dynamic environments, and involves reducing the precision of neural network weights and activation leading for faster computation and reduced memory usage. The outcomes of layer l in ANN are represented by (14). Where, x^l, W^l, b^l denote input activation, weight and bias of layer is l respectively. Furthermore, $h(.)$ indicates ReLU and SNN activation function. Here, the model is implemented by replacing the standard ReLU non-linearity $(\max(0, x))$ with a spiking neuron model that discretizes its input signal input spikes. The neuron model with a soft rest mechanism is described at each timestamp t by (15) to (18).

$$y^l = h(x^l W^l + b^l),\ \ l\epsilon[1, n] \quad (14)$$

$$H^l(t) = V^l(t-1) + i^l(t) \quad (15)$$

$$i^l(t) = Z^{l-1}(t)W^l + b^l \quad (16)$$

$$z^l(t) = \Theta(H^l(t) - V_{th}) \quad (17)$$

$$V^l(t) = H^l(t)\big(1 - Z^l(t)\big) + H^l(t) - V_{th})Z^l(t) \quad (18)$$

Where, $H^l(t)$ and $V^l(t)$ denote membrane after integration and spike emission at time t, respectively. The spiking outcomes at time t by $Z^l(t)$ have a binary solution and input spiking neuron, $i^l(t)$ that is described as the weight product with binary signal and spikes caused by the preceding layer, plus a stable bias. Additionally, bias is added to membrane potential at every timestamp regardless of the values of $Z^{l-1}(t)$. In (17) and (18) describe the generation of a spike and soft rest operation, and function of $\Theta(.)$ denotes the Heaviside phase. The forward operation of SNN, as described in the previous equation is repeated over T timesteps. The outcomes of the spiking layer l are decoded as (19) and (20).

$$y_s^l = \frac{1}{T}\sum_{t=1}^{T} z^l(t) \quad (19)$$

$$\sum_{t=1}^{T} Z(t) = min\left\{T, \frac{\sum_{t=1}^{T}(Z^{l-1}(t)W^l) + bT}{v_{th}}\right\} \quad (20)$$

In this context, a decoding scheme for a rate-coded network is defined by (20), where data is encoded by spikes caused by spiking neurons over a fixed length of time T. The integration of $Z^l(t)$ parameter of binary leads to the quantization of the decoded outcome y_s^l. This process allows for the quantization function to integrate $\sum_{t=1}^{T}(Z^{l-1}(t)W^l) + bT$, which denotes the input of recent neural network, following i^l, over T timesteps. It involves $T + 1$ uniform quantization intervals; considering maximum

network latency, it is possible to reduce quantization noise. The PDF of input is then optimized to further minimize quantization noise, as described in the following sections.

2.3.1. Probability density function –quantization for spiking neurons

The PDF-QSNN provides a statistical representation of the likelihood of different data points or patterns occurring within the network. By applying the PDF-QSNN, it assigns weights or attention to more probable events, effectively emphasizing patterns with a higher likelihood of occurrence. The quantization process helps in compressing the data into manageable forms, while the PDF ensures that the most important data—those with higher probabilities—are processed more rigorously. This dual mechanism enhances the QSNN's effectiveness, which is critical in the context of MANETs where network conditions change rapidly due to mobility, attacks, or node failures. The proposed method demonstrates how the probability improves network performance in MANETs, as described in the previous (16) to (18). The integration of quantization with the PDF-based processing in the SNN technique reduces sensitivity while ensuring reliable performance in a dynamic environment.

In this study, the gradient method involves the composite derivation of the Heaviside phase during error back-propagation, where $\Theta'(x) = \sigma'(x)$ indicates the approximation of step function and sigmoid $\left(\sigma(x) = \frac{1}{1+e^{-x}}\right)$ respectively. The spiking neuron is trained with inputs i and z, and the upstream gradient to neuron in $\frac{\partial L}{\partial Z}$. The notation of simplicity is defined as $q = (H(t) - V_{th})$ input of the Heaviside step function, as represented by (21) to (24).

$$\frac{\partial L}{\partial V_{th}} = \frac{\partial L}{\partial Z} \cdot \frac{\partial z}{\partial q} \cdot \frac{\partial q}{\partial V_{th}} \tag{21}$$

$$\frac{\partial z}{\partial q} = \sigma'(q) \tag{22}$$

$$\frac{\partial q}{\partial V_{th}} = -1 \tag{23}$$

$$\frac{\partial L}{\partial V_{th}} = -\frac{\partial L}{\partial Z} . \sigma'(q) \tag{24}$$

Where, q denotes derivative function of gradient z with respect to q and substituting (22) and (23) into (24) to obtain an approximation of downstream gradient solution. The neuron output $\hat{y}$ is evaluated based on spiking sequence after T timesteps, with the values of V_{th} that minimized quantization error in neuron identified and the optimization process analysed for feature selection in a single spiking neuron. The loss function is expressed by (25), where the RMS error between input and outcomes of the neuron is calcuated.

$$L(i, \hat{y}) = \mathbb{E}[(i - \hat{y})^2] \tag{25}$$

Where loss function in QSNN is minimized for a given input distribution and simulated data for MANET with a fixed threshold $V_{th} = 1$. The threshold is modified during the learning process. This process applies a uniform quantization scheme to the input distribution of neurons, reducing quantization error by increasing the size of the quantization step. The quantization process converts continuous values of network features into discrete levels, which enhances performance. When combined with the PDF, it helps distribute features and classify them efficiently using the PDF-QSNN technique.

3. EXPERIMENTAL SETUP

In this research, the PDF-QSNN technique is simulated in the MATLAB 2020b environment, 16 GB RAM, intel i5 Processor, Windows 10 operation system, 6 GB GPU and 1 TB SSD. The performance measures used for evaluation and the outcomes of feature selection and classification are explained in section 4.1. The performance of the proposed method is calculated using several performance metrics, including accuracy, precision, f1-score, and recall, which are defined in (26) to (30). Where, $TP, TN, FP,$ and FN denote true positive, true negative, false positive, and false negatives, respectively.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{26}$$

$$Precision = \frac{TP}{TP+FP} \quad (27)$$

$$Recall = \frac{TP}{TP+FN} \quad (28)$$

$$Specificity = \frac{TP}{(TN+FP)} \quad (29)$$

$$Sensitivity = \frac{TP}{(TP+FN)} \quad (30)$$

3.1. Performance analysis

In this section, the feature selection process of the proposed AMFO model and the classification process of PDF-QSNN are evaluated based on accuracy, precision, F1-score, and recall, as presented in Tables 1 to 5. The evaluation is carried out using data from the simulated dataset, with the feature selection and classification results described in these tables. The performance of various optimization techniques on the simulated datasets is evaluated based on accuracy, precision, recall, specificity, and sensitivity, as shown in Table 1. The existing feature selection techniques: dipper throated optimization (DTO), pelican optimization algorithm (POA), antlion optimization algorithm (ALO), and crisscross optimization algorithm (COA), are compared against the proposed AMFO model. The AMFO method achieves an accuracy of 92.86%, precision of 91.65%, recall of 91.25%, specificity of 91.43%, and sensitivity of 91.06%. The results demonstrate that the AMFO method effectively handles black hole attacks, offering superior performance attributed to its effective feature selection process, which enhances the model's ability to accurately identify attacks by optimizing relevant features and minimizing noise.

Table 1. Performance analysis of feature selection on BHA attack

Methods	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	Sensitivity (%)
DOA	88.25	87.49	87.47	87.46	87.26
POA	89.63	88.26	88.26	88.49	88.41
ALO	90.75	89.56	89.56	89.56	89.38
COA	91.56	90.45	90.16	90.45	90.65
MDO	92.86	91.65	91.25	91.43	91.06

The performance of simulated dataset classification is calculated based on accuracy, precision, F1-score, and recall, as described in Table 2. The existing feature selection methods namely, CNN, LSTM, SNN and GNN are evaluated against the proposed method. The PDF-QSNN method achieves a high accuracy of 92.86%, precision of 91.65%, recall of 91.25%, Specificity of 91.43% and Sensitivity of 91.06%. The simulated data analysis shows that the AMFO method handles black hole attacks efficaciously. This superior performance is attributed to its effective classification process, which enhances accuracy.

Table 2. Performance of different classification on BHA

Methods	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	Sensitivity (%)
CNN	88.25	87.49	87.47	87.46	87.26
LSTM	89.63	88.26	88.26	88.49	88.41
SNN	90.75	89.56	89.56	89.56	89.38
GNN	91.56	90.45	90.16	90.45	90.65
PSF-QSNN	92.86	91.65	91.25	91.43	91.06

The performance of the proposed PDF-QSNN model’s simulated dataset classification is calculated based on accuracy, precision, F1-score, and recall as described in Figure 2. The existing methods using CNN, LSTM, SNN and GNN feature selection techniques are evaluated. The AMFO and PDF-QSNN method achieves a superior accuracy of 92.86%, precision of 91.65%, recall of 91.25%, specificity of 91.43% and sensitivity of 91.06%. The AMFO and PDF-QSNN methods achieve a better accuracy in detecting BHA due to their advanced feature selection and classification techniques. The AMFO optimizes feature relevance, while PDF-QSNN improves data representation, enhancing attack detection and classification accuracy.

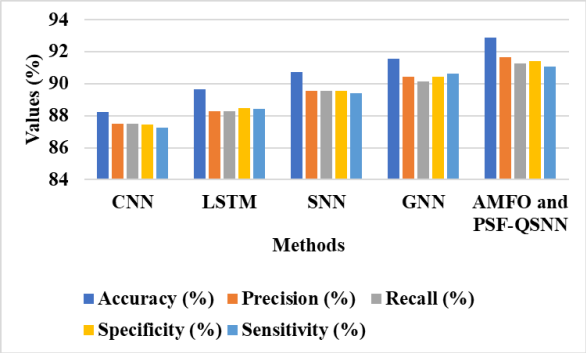

Figure 2. Graphically represented the classification process on BHA

In Table 3, the performance comparison is carried out based on accuracy, precision, recall, specificity and sensitivity as described. The existing methods, DTO, BWO, ALO and COA are compared for analysis. The AMFO method achieves a high accuracy of 91.56%, a precision of 90.45%, a recall of 90.16%, a specificity of 90.45% and a sensitivity of 90.65%. The AMFO algorithm uses feature selection to identify relevant features and reduce dimensionality, while maintaining a consistent focus on efficient feature selection with reduced noise. It also emphasizes mainly on the critical features, resulting in superior accuracy in identifying WHA.

Table 3. Performance analysis of feature selection on WHA

Methods	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	Sensitivity (%)
DOA	89.56	86.29	86.15	86.89	86.13
POA	90.48	87.45	87.75	87.78	87.98
ALO	91.25	89.36	89.35	89.47	89.69
COA	92.45	90.48	90.46	90.14	90.36
MDO	91.56	90.45	90.16	90.45	90.65

The performance of simulated dataset classification is evaluated based on accuracy, precision, F1-score, and recall, as shown in Table 4. Existing methods using feature selection techniques, such as CNN, LSTM, SNN, and GNN, were also assessed. The AMDO and PDF-QSNN methods achieve an accuracy of 91.56%, precision of 90.45%, recall of 90.16%, specificity of 90.45%, and sensitivity of 90.65%. The proposed PDF-QSNN technique efficiently detects WHA and achieves better accuracy compared to other methods.

Table 4. Performance of classification on WHA

Methods	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	Sensitivity (%)
CNN	87.56	86.29	86.15	86.89	86.13
LSTM	88.48	87.45	87.75	87.78	87.98
SNN	89.25	88.36	88.35	88.47	88.69
GNN	90.45	89.48	89.46	89.14	89.36
PDF-QSNN	91.56	90.45	90.16	90.45	90.65

The performance of simulated dataset classification is also calculated based on accuracy, precision, F1-score, and recall, as presented in Figure 3. The existing methods using feature selection techniques, such as CNN, LSTM, SNN, and GNN, were evaluated. The AMDO and PDF-QSNN methods achieve an accuracy of 91.56%, precision of 90.45%, recall of 90.56%, specificity of 90.45%, and sensitivity of 90.65%.

Table 5 presents the classification results of the proposed PDF-QSNN with different K-fold values on the simulated dataset. K-values of 2, 4, 7, and 9, used in the 5-fold cross-validation method, ensure that the model is trained on a substantial portion of the data while also validating on a reasonable subset. This balanced approach facilitates better generalization to unseen data, minimizing the risk of overfitting and ensuring sufficient training data to effectively capture underlying patterns.

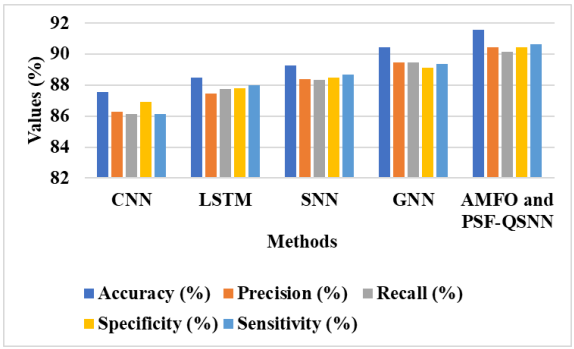

Figure 3. Graphically represented of the classification process on WHA

Table 5. Performance analysis of K-fold values on BHA

K-fold values	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	Sensitivity (%)
2	88.25	87.49	87.47	87.46	87.26
4	89.63	88.26	88.26	88.49	88.41
5	92.86	91.65	91.25	91.43	91.06
7	91.56	90.45	90.16	90.45	90.65
9	90.75	89.56	89.56	89.56	89.38

Figure 4 presents the classification results using different K-fold values for the proposed PDF-QSNN on the simulated dataset. K-fold values of 2, 4, 7, and 9, applied in 5-fold cross-validation, ensure that the model is trained on a substantial portion of the data while also validating on a reasonable subset. This balanced approach facilitates better generalization to unseen data, minimizing the risk of overfitting and ensuring sufficient training data to effectively capture underlying patterns.

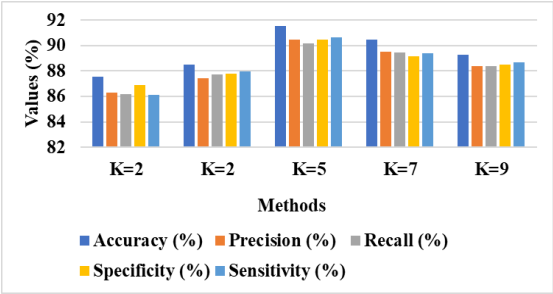

Figure 4. Performance analysis of K-fold values on WHA

3.2. Discussion

The investigation of outcomes from the PDR-QSNN approach is discussed in detail in this section. The PDR-QSNN is involved in classification using simulated data for attack analysis. The CNN method [16] requires large volumes of simulated data for effective analysis, which is challenging to obtain in a distributed and dynamic environment. The AB-RF approach [17] is difficult to interpret and often leads to communication issues due to the transmission of multiple data points, negatively impacting classification accuracy. The MANN technique [18] analyzes attack vulnerabilities using simulated data but tends to overfit, adversely affecting classification accuracy. SRLSTM approaches [19] aim to maximize the overall performance of the IDS framework by considering node energy factors but often misclassify, compromising accuracy. The DIWGAN approach [20] faces challenges when handling categorical data and non-parametric distributed variables, resulting in inefficient performance in network communication. The proposed PDF-QSNN technique efficiently performs in a MANET environment, enhancing classification accuracy. The PDF-QSNN approach improves classification accuracy in MANETs, making it a promising method for real-time attack detection. Future advancements will focus on refining detection capabilities, enhancing efficiency, and ensuring adaptability to evolving cyber threats. The findings demonstrate that the PDF-QSNN approach improves classification accuracy in MANETs, which is crucial for applications requiring efficient,

adaptive, and real-time decision-making in dynamic network environments such as IoT, military communication, and disaster recovery systems. These findings support the scientific consensus on the benefits of spiking neural networks (SNNs) in resource-constrained and dynamic environments. However, the experiment faced challenges due to the constrained diversity of simulation data, which impacted the generalization of the PDF-QSNN model in real-world MANET environments. Variations in BHA and Wormhole WHA attacks caused fluctuations in classification accuracy due to their dynamic behavior and complex propagation patterns. Future improvements will include integrating real-world datasets, adversarial learning, and lightweight architectures to improve robustness and adaptability.

4. CONCLUSION

In conclusion, this paper proposed a PDF-QSNN framework for efficient intrusion detection in MANETs. By integrating probability density-based feature representation with a quantized spiking neural network, the proposed framework effectively captures discriminative network traffic patterns and improves the classification of malicious activities in dynamic MANET environments. Furthermore, the incorporation of the AMFO algorithm enables efficient feature selection by eliminating redundant and irrelevant attributes from high-dimensional simulation data, thereby reducing computational complexity while enhancing intrusion detection performance. Experimental results demonstrate that the proposed PDF-QSNN framework achieves classification accuracies of 92.86% for BHA and 91.56% for WHA, outperforming conventional DL approaches, including CNN and SRLSTM models. These findings confirm that combining probabilistic feature encoding with lightweight neuromorphic learning provides an effective and computationally efficient solution for intrusion detection in resource-constrained MANETs. Nevertheless, this study is limited by its reliance on simulated datasets, which may not fully capture the complexity and variability of real-world MANET deployments. Future research will therefore focus on validating the proposed framework using real-world network traffic datasets, improving computational efficiency for edge deployment, enhancing robustness against diverse and evolving attack types, and extending the framework to classify multiple attack subcategories. In addition, comprehensive benchmarking against state-of-the-art intrusion detection models under various MANET scenarios will be conducted to further evaluate the scalability, generalization capability, and practical applicability of the proposed PDF-QSNN framework.

REFERENCES

[1] R. Vatambeti, S. V. Mantena, K. V. D. Kiran, S. Chennupalli, and M. V. Gopalachari, "Black hole attack detection using Dolphin Echo-location-based machine learning model in MANET environment," *Computers and Electrical Engineering*, vol. 114, p. 109094, Mar. 2024, doi: 10.1016/j.compeleceng.2024.109094.

[2] R. Reka, R. Karthick, R. Saravana Ram, and G. Singh, "Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET," *Computers & Security*, vol. 136, p. 103526, Jan. 2024, doi: 10.1016/j.cose.2023.103526.

[3] S. B. Ninu, "An intrusion detection system using exponential henry gas solubility optimization based deep neuro fuzzy network in MANET," *Engineering Applications of Artificial Intelligence*, vol. 123, p. 105969, Aug. 2023, doi: 10.1016/j.engappai.2023.105969.

[4] J. Ryu and S. Kim, "Reputation-based opportunistic routing protocol using q-learning for MANET attacked by malicious nodes," *IEEE Access*, vol. 11, pp. 47701–47711, 2023, doi: 10.1109/access.2023.3242608.

[5] A. Abdelhamid, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A lightweight anomaly detection system for black hole attack," *Electronics*, vol. 12, no. 6, p. 1294, Mar. 2023, doi: 10.3390/electronics12061294.

[6] K. Nirmaladevi and K. Prabha, "A selfish node trust aware with optimized clustering for reliable routing protocol in MANET," *Measurement: Sensors*, vol. 26, p. 100680, Apr. 2023, doi: 10.1016/j.measen.2023.100680.

[7] W. Liu, Z. Chen, X. Yu, and X. Zhou, "A cluster-based approach against wormhole attacks in MANETs among smart grid," *Frontiers in Energy Research*, vol. 10, 2022, doi: 10.3389/fenrg.2022.1017932.

[8] V. Mankotia, R. K. Sunkaria, and S. Gurung, "AFA: anti-flooding attack scheme against flooding attack in MANET," *Wireless Personal Communications*, vol. 130, no. 2, pp. 1161–1190, Mar. 2023, doi: 10.1007/s11277-023-10325-3.

[9] S. Kaushik, K. Tripathi, R. Gupta, and P. Mahajan, "Enhancing reliability in mobile ad hoc networks (MANETs) through the K-AOMDV routing protocol to mitigate black hole attacks," *SN Computer Science*, vol. 5, no. 2, Feb. 2024, doi: 10.1007/s42979-023-02585-4.

[10] G. Subburayalu, H. Duraivelu, A. P. Raveendran, R. Arunachalam, D. Kongara, and C. Thangavel, "Cluster based malicious node detection system for mobile ad-hoc network using ANFIS classifier," *Journal of Applied Security Research*, vol. 18, no. 3, pp. 402–420, Nov. 2021, doi: 10.1080/19361610.2021.2002118.

[11] S. Shafi, S. Mounika, and S. Velliangiri, "Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET," *Procedia Computer Science*, vol. 218, pp. 2309–2318, 2023, doi: 10.1016/j.procs.2023.01.206.

[12] G. Vidhya Lakshmi and P. Vaishnavi, "A trusted security approach to detect and isolate routing attacks in mobile ad hoc networks," *Journal of Engineering Research*, vol. 12, no. 3, pp. 379–386, 2024, doi: 10.1016/j.jer.2023.100149.

[13] V. Mankotia, R. K. Sunkaria, and S. Gurung, "DT-AODV: a dynamic threshold protocol against black-hole attack in MANET," *Sādhanā*, vol. 48, no. 4, 2023, doi: 10.1007/s12046-023-02227-8.

[14] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022, doi: 10.1109/access.2022.3144679.

[15] M. Shukla, B. K. Joshi, and U. Singh, "A novel machine learning algorithm for MANET attack: black hole and gray hole," *Wireless Personal Communications*, vol. 138, no. 1, pp. 41–66, Aug. 2024, doi: 10.1007/s11277-024-11360-4.
[16] M. Abdan and S. A. H. Seno, "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/2375702.
[17] S. S. M. Vincent and N. Duraipandian, "Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm," *Expert Systems with Applications*, vol. 249, p. 123765, 2024, doi: 10.1016/j.eswa.2024.123765.
[18] M. Prasad, S. Tripathi, and K. Dahal, "A probability estimation-based feature reduction and Bayesian rough set approach for intrusion detection in mobile ad-hoc network," *Applied Intelligence*, vol. 53, no. 6, pp. 7169–7185, 2022, doi: 10.1007/s10489-022-03763-2.
[19] M. Deivakani, M. S. Sheela, K. Priyadarsini, and Y. Farhaoui, "An intelligent security mechanism in mobile Ad-Hoc networks using precision probability genetic algorithms (PPGA) and deep learning technique (Stacked LSTM)," *Sustainable Computing: Informatics and Systems*, vol. 43, p. 101021, 2024, doi: 10.1016/j.suscom.2024.101021.
[20] B. Krishnasamy, L. Muthaiah, J. E. Kamali Pushparaj, and P. S. Pandey, "DIWGAN optimized with namib beetle optimization algorithm for intrusion detection in mobile ad hoc networks," *IETE Journal of Research*, vol. 70, no. 5, pp. 4422–4441, 2023, doi: 10.1080/03772063.2023.2223181.
[21] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET," *Evolutionary Intelligence*, vol. 15, no. 2, pp. 1313–1327, Mar. 2020, doi: 10.1007/s12065-020-00388-7.
[22] S. K. Sahoo *et al.*, "Moth flame optimization: theory, modifications, hybridizations, and applications," *Archives of Computational Methods in Engineering*, vol. 30, no. 1, pp. 391–426, Aug. 2022, doi: 10.1007/s11831-022-09801-z.
[23] M. Alazab, R. A. Khurma, A. Awajan, and D. Camacho, "A new intrusion detection system based on Moth–Flame Optimizer algorithm," *Expert Systems with Applications*, vol. 210, p. 118439, Dec. 2022, doi: 10.1016/j.eswa.2022.118439.
[24] N. A. S. Al-Jamali, I. R. K. Al-Saedi, A. R. Zarzoor, and H. Li, "A new imputation technique based a multi-spike neural network to handle missing data in the internet of things network (IoT)," *IEEE Access*, vol. 11, pp. 112841–112850, 2023, doi: 10.1109/access.2023.3323435.
[25] J. Saikam and K. Ch, "EESNN: hybrid deep learning empowered spatial–temporal features for network intrusion detection system," *IEEE Access*, vol. 12, pp. 15930–15945, 2024, doi: 10.1109/access.2024.3350197.

BIOGRAPHIES OF AUTHORS

Amruth Veerabhadraiah is an expert in the theory of computations, MANETs, algorithms, and Python programming. He has published numerous papers in prestigious conferences and journals, and holds two patents for his innovative work. Alongside his technical expertise, Amruth is also a talented artist and musician, blending creativity with logic in both fields. He currently serves as an assistant professor in the Department of Information Science and Engineering at Maharaja Institute of Technology, Mysore, while pursuing his PhD at Jain (Deemed-to-be University), Bangalore. He can be contacted at email: amruthv_ise@mitmysore.in.

Devaraj Verma Chitragar is a Professor in the School of Computer Science and Engineering at Jain (Deemed to be University). He holds a Bachelor's and a Master's degree in Computer Science and Engineering. Dr. Verma is a qualified professor with NET and KSET certifications and a lifetime member of professional bodies like ISTE, IACSIT, and IAENG. His research focuses on artificial intelligence, specifically developing a computational model for the diversity of the mind. Dr. Verma's research interests span cognitive science, image processing, IoT, and machine learning in the context of artificial intelligence. He has published over 25 research papers in national and international conferences. He serves as a reviewer for the book "Artificial Intelligence: Theories and Applications" by Dr. Lavika Goel. As a research supervisor, Dr. Verma guides eight research scholars at Jain (Deemed to be University). He can be contacted at email: c.devaraj@jainuniversity.ac.in.