Grenze International Journal of Engineering and Technology, June Issue

Adaptive Intrusion Detection in MANET Environments using PDF-Enhanced Quantized Spiking Neural Networks

Amruth Veerabhadraiah[1] and Devaraj Verma Chitragar[2]
[1]Assistant Professor, Department of Information Science and Engineering, Maharaja Institute of Technology Mysore and PhD Research Scholar, Jain (Deemed to be University), Bengaluru, India
[2]Professor, Department of CSE (AI), Jain (Deemed to be University), Bengaluru, India
Email: amruthv_ise@mitmysore.in

***Abstract*— Mobile Ad-hoc Networks (MANETs), characterized by their dynamic, decentralized, and infrastructure-less nature, are highly susceptible to security threats such as Black Hole (BHA), Wormhole (WHA), and Grey Hole (GHA) attacks. The inherent limitations of MANETs, including restricted bandwidth and device heterogeneity, often compromise the accuracy of traditional Intrusion Detection Systems (IDS). To address this, we propose a novel technique: the Probability Density Function-Quantization Spiking Neural Network (PDF-QSNN), specifically tailored for the MANET environment. The PDF component is integrated into the neural network to prioritize data instances that are statistically more likely to represent significant network behaviors or attack patterns, thereby improving classification robustness. Furthermore, the Adaptive Moth Flame Optimization (AMFO) algorithm is employed for feature selection, effectively reducing the high dimensionality of the simulated dataset and isolating the most critical features for intrusion detection. Tested on a simulated dataset encompassing BHA and WHA scenarios, the PDF-QSNN method demonstrates superior performance compared to existing deep learning models like Convolutional Neural Networks (CNN) and Stacked Recurrent Long Short Term Memory (SRLSTM). Specifically, the proposed model achieves a high classification accuracy of 92.86% for BHA and 91.45% for WHA, validating its efficacy as an adaptive and accurate IDS solution for dynamic MANETs.**

***Keywords*— AMFO, CNN, MANETs, SRLSTM, Black Hole, Wormhole, Grey Hole.**

I. INTRODUCTION

Mobile ad hoc Network (MANETs) consist of mobile nodes that frequently change their locations, making routing a challenging task due to their dynamic nature. Routing protocols in MANET must be continuously active to make dynamic routing decision, but this also increases the risk of packet loss due to potential attacks [1-2]. MANET routing protocols are designed to connect and secure the network nodes, but ensuring security is difficult due to heterogeneity of devices within the network. The role of Intrusion Detection System (IDS) is crucial in security framework of MANET particularly in monitoring and assessing risks[3-4]. The IDS approaches are essential not only for protecting individual nodes but also for defending entire network from various malicious attacks [5]. Traditional routing protocols in MANETs such as those utilizing Deep Learning (DL) techniques, aim to determine the optimal path before transmitting packets [6].

Grenze ID: 01.GIJET.12.2.375_21

Unlike conventional network, MANETs are infrastructure less meaning the routing function is distributed among the nodes rather than being handled by dedicated devices[7-8]. This work consider the simulated dataset based on BHA and WHA to analysis DL to mitigate various attacks and identify intrusion node in MANET. The model encourages the formation of node and selection the feature that potential improve the function for each node [9-10]. The energy constraints are addressed by processing simulated data within the MANET network using DL approach [11]. In this approach, secure nodes are identified and utilized for transmission within the network. During the initial transmission phase, multiple path is generated and an optimization approach is employed to select the best path [12]. The routing protocols in MANET assume that each node processes simulated data to detect and analyse vulnerabilities to various attacks, including sinkhole, black-hole and worm hole attack [13-14]. Despite optimal route selection, attacks by nodes that refuse to cooperate or follow routing rules still cause necessary routes to be dropped and effect detection efficiency and classification [15]. Although MANET offer decentralized management their restricted bandwidth makes them more susceptible to security threats, impacting classification accuracy. In this research, 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 patterns or behaviors in MANET environment.

II. Literature Review

The related work on attack detecting in instruction detection in MANET environment is discussed below along with their benefits and disadvantages. Masoud Abdan and Seyed Amin Hosseini Seno [16] presented a DL based Convolutional Neural Network (CNN) is performed in classification by using simulated data, where relatively numerous nodes and factors require to trained the node in MANET. These was automatically extracting relevant features from raw data, reducing the need for manual feature and handle variation in data such as changes in node position, mobility patterns and environment condition in MANETs. However, CNN require large amounts of simulated data for analysis the attack, which has difficult to obtain in distributed and dynamic environment. Sherrial Sophie Maria Vincent and N. Duraipandian [17] introduced an attack detection cause loss of security maximum amount of drop packets minimized packet delivery ratio in MANET by using simulation data. These was considering optimization approaches for shortest path of node by using Particle Bee Colony Swarm Optimization Algorithm (PBCO) reduce the transformation using feature selection. The Ada-Boost –Random Forest (AB-RF) for the classification to effective performed to achieve better accuracy. However, AB-RF was difficult to interpret and involved multiple data to transmitted lack on the communication due to affect the classification accuracy. Mahendra Prasad et al. [18] presented a network has different attach working to transfer data to the destination through intermediate nods, monitor the attack from intrusion such as Mutation based Artificial Neural Network (MANN) classifier. These was performed simulated data, analysis the attack efficiently process in MANET allowing flexible routing and mutation process diversity in the ANN learning process helping explore a broader solution and potentially leading to better accuracy. However, MANN technique was analysis vulnerability of attack to detect involved simulated data which is occur overfitting it affect the classification accuracy.

M. Deivakani et al. [19] developed Stacked Recurrent Long Short Term Memory (SRLSTM) method was involved the attack detecting to analysis in intrusion detection for monitor data transmitted in MANET. These was capture long-term dependencies, where the network topology node behavior and communication patterns were dynamic involved in MANET environment. However, SRLSTM approaches requires to maximum overall performance of IDS framework by considering factor of node energy and lacks in classification because misclassify affect classification accuracy. Bala Krishnasamy et al. [20] developed a Dual Interactive Wasserstein Generative Adversarial Network (DIWGAN) approach involved the intrusion detections system analysis the simulation data in MANET environment. These was provided a more stable training process and learn the feature efficiently to analysis the attack by using simulated data in MANET, improving the accuracy and reliability of process. However, DIWGAN approach data variables were categorical, normal or Non-parametric was distributed the data for communication does not efficiently performed in the network. The overall analysis to facing challenging such as MANET potential to provide decentralized management, restricted bandwidth more vulnerable to security threats it affect classification accuracy. In this research, PDF-QSNN technique is efficiently performed in MANET environment, enhance the classification accuracy. The PDF utilized in neural network prioritize data that is more likely to represent significant patter or behaviours in MANET environment. Initial data obtained from the simulated data based on black hole, worm hole and sink hole attack in intrusion detection in MANET.

III. PROPOSED METHODOLOGY

In this research, proposed PDF-QSNN technique is efficiently performed in the MANET environment, enhance the classification accuracy. By utilizing the PDF, the neural network prioritize data that is more likely to represent significant patterns or behaviours in the MANET environment. This is analysis the attack effectively by using simulated data like OMNET++ then learn attack, which is crucial for selecting and intrusion detection in MANET. Feature selection using Adaptive Moth Flame Optimization (AMFO) algorithm is effective in handling high dimensional feature spaces which is often the simulation data and reduce the dimensionality by selecting essential feature and improve performance of classification stages. Figure 1 block diagram of proposed method.

A. Data Simulation

In this section, consider the BHA and WHA in finite number of nodes is simulated. It generated a topology consider the node and protocols in different network programs transfer packet over the network simulation process. This simulation is completed a MANET environment with 50 regular nodes and 2 malicious nodes. The topology is 1000×1000m^2 spontaneous node activity and 300 meter radio range of node are simulation environment. It gathered 4000 different samples continuing normal and malicious sample and dataset that is compiled and tagged with 20 attributes and high volume dataset for BHA and WHA created in ad hoc network context.

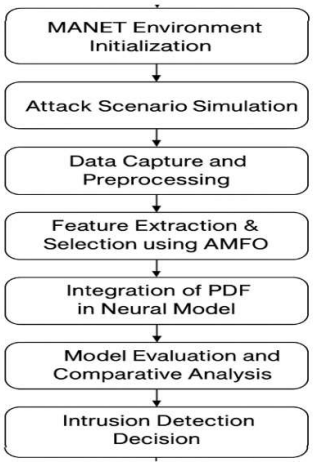

Fig 1: Block diagram of proposed method

B. Energy Model

To calculated reliability pair factor (F_{RP}), it is essential to know the remaining battery energy of nodes. The energy model assumes full battery energy of a node at start and remaining battery energy of node p at a time t is represented $(E_p^{rem}(t)$ by equation (1) shown below

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

Where, E_p^{Tr} denoted amount of energy required to transmit a single bit of data, k denoted number of bit transmitted from duration $q-1$ to q E_m^{Wc} denoted total energy taken for getting individual bit of information from time is $q-1$ to q is defined the equation (2) shown below;

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

At the initial time, remaining energy is assumed to be equal to full battery capacity of node.

C. Mobility Model

The mobility model is creating to described mobile nodes move to base on position and acceleration alter over time and mobility pattern is accessed in the routing protocols. The begin velocity of node c and d moves in particular direction with a varible velocity with angle φ_1 and φ_2 based on positive $x-$ axis respectively. The q,

node c and d transfers to position (x_6, y_6) and (x_3, y_3), Euclidean distance $(e_{(cd,0)})$ between the node $c(x_1, y_1)$ and $d(x_2, y_2)$ at $T = 0$ is expressed in equation (3) shown below;

$$\left(e_{(cd,0)}\right) = \sqrt{|x_1, x_2|}^2 + |y_1, y_2|^2 \quad (3)$$

D. Feature selection

The MOF algorithm is a heuristic optimization inspired by spiral navigation behavior of moths around a light source. This behavior originates from natural navigation mechanism of moths, which involves velocity in a straight line by maintaining a constant angle relative to moon.

However, when the light source is closer, this navigation mechanism lead moths into a spiral path toward light potentially resulting in demise. In the MFO algorithm, moths are treated as search agents represented in a matrix M(t) that explore a D-dimension search space.

The total number of moths in this matrix is denoted by N and moths are modeled using equation (4) shown below

$$M = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{1d} \\ m_{21} & m_{22} & \dots & m_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nd} \end{bmatrix}, \quad (4)$$

E. Adaptive Flame number strategy

The adaptive flame is does not occur in all generation in global optimal value is updated the position is utilized the all generation is equation (5) and (6) shown below;

$$= \begin{cases} \text{Flame}_{\text{no}} = \text{Flame}_{\text{no}} + \max \text{succes}, \\ \max \text{Success} = \max\text{Success} + \max \text{Success} * \text{adjust Success} \end{cases} \quad (5)$$

$$= \begin{cases} \text{Flame}_{\text{no}} = \text{Flame}_{\text{no}} + \max \text{Failures}, \\ \max \text{Failures} = \max \text{Failures} + \max \text{Failures} * \text{adjust Failures} \end{cases} \quad (6)$$

F. Multiple Flame Mechanism

The multiple flame mechanism is inspired by Differential evolution technique, where the various vector between two flames arbitrarily choose from flame population is considered as direction of vector. To balance multiple flame guidance mechanism and spiral search mechanism of MFO, parameter rc is added and arbitrarily choose from range [0,1]. The multiple flame guidance mechanism is execurted when the condition d<rc satisfied is shown formula (22) shown below.

$$S(M_i, F_j) = \begin{cases} D_i . e^{bt} . \cos(2\pi t) + F_j, & \text{if r and} < \text{rc}, \\ \text{rand} * (F_m - F_p) + F_j, & \text{otherwise}, \end{cases} \quad (7)$$

Where, j, m and p are distict indexes, M_i denoted ith moth, F_j denoted jth flame and rand denoted arbitrarily in interval of [0,1] repectively.

G. Classification

A quantized SNN that utilizes the probability PDF is enhance approach for efficiency of neural network in MANET. This method integrated quantization with PDF to enhance performance of neural network in dynamic and involves reducing the precision of neural network weights and activation leading to faster computation and reduced memory usage. The considering an n-layer fully connected to convolutional ANN, output of layer l is described by equation (7) shown below;

$$y^l = h\left(x^l W^l + b^l\right), \quad l \epsilon [1, n] \quad (8)$$

H. Probability Density Function –Quantization for Spiking Neurons

The PDF-QSNN is described the probability improve the network in MANET. The PDF help the SNN learn and adapt more effectively by emphasizing data that has higher probability of occurring, which is crucial for routing and intrusion detection in MANETs.

The combination of quantization and PDF-based processing making the SNN more to changes and fluctuation in network ensuring reliable performance in dynamic environment.

IV. Results and Discussion

The proposed AMFO involving feature selection and PDF-QSNN classification processes is evaluated using several performance metrics, including Accuracy, Precision, F1-score, and Recall, which was presented in Tables 1 and 2.

Table I: Performance Analysis of Feature Selection on BHA attack

Methods	Accuracy (%)	Precision (%)	F1 score (%)	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

Table II: Performance of Different Classification on BHA

Methods	Accuracy (%)	Precision (%)	F1 score (%)	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
PDF-QSNN	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 figure 2. The existing methods using feature selection techniques such as CNN, LSTM, SNN and GNN evaluated. AMFO optimizes feature relevance, while PDF-QSNN improves data representation, both enhancing attack detecting and classification accuracy.

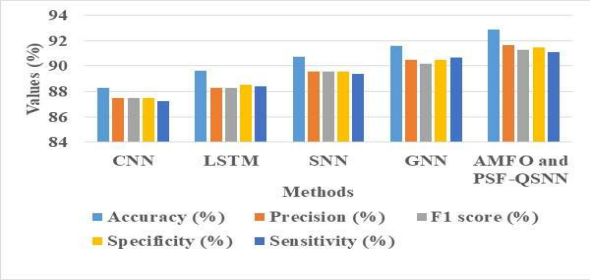

Fig 2: Graphically represented of the classification process on BHA

The performance of different optimization technique on simulated dataset is evaluated based on accuracy, precision, recall, specificity and sensitivity as described in table 3.

Table III: Performance Analysis of Feature Selection on WHA

Methods	Accuracy (%)	Precision (%)	F1 score (%)	Specificity (%)	Sensitivity (%)
CNN	89.56	86.29	86.15	86.89	86.13
LSTM	90.48	87.45	87.75	87.78	87.98
SNN	91.25	89.36	89.35	89.47	89.69
GNN	92.45	90.48	90.46	90.14	90.36
PDF-QSNN	91.56	90.45	90.16	90.45	90.65

The performance of simulated dataset classification is calculated based on accuracy, precision, F1-score, and recall as described in Table 4.

Table IV: Performance of classification on WHA

Methods	Accuracy (%)	Precision (%)	F1 score (%)	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 calculated based on accuracy, precision, F1-score, and recall as described in figure 3.

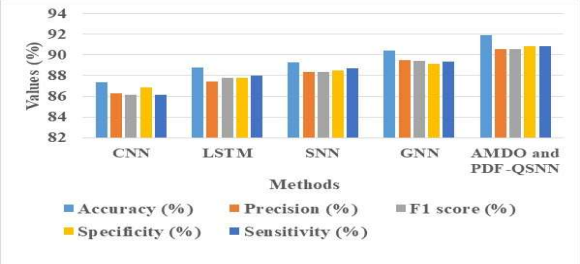

Fig 3: graphically represented of the classification process on WHA

Table.5 presents classification results using different K-fold values for the proposed PDF-QSNN on the simulated dataset.

TABLE V: PERFORMANCE ANALYSIS OF K-FOLD VALUES ON BHA

K-fold values	Accuracy (%)	Precision (%)	F1 score (%)	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 classification results using different K-fold values for the proposed PDF-QSNN on the simulated dataset.

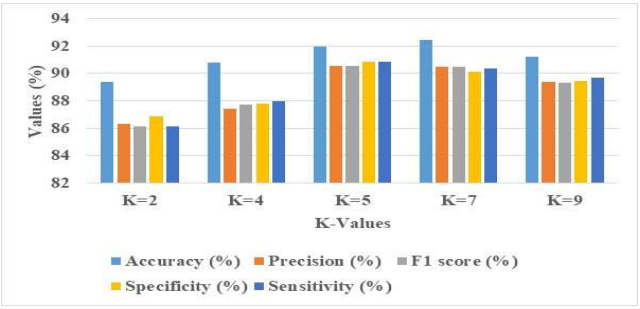

Fig 4: Performance analysis of K-fold values on WHA

V. CONCLUSION

In this section, proposed PDF-QSNN technique is efficiently performed in MANET environment, enhance the classification accuracy. The PDF utilized in neural network prioritize data that is more likely to represent significant patter or behaviours in MANET environment. Initial data obtained from the simulated data based on black hole, worm hole and sink hole attack in intrusion detection in MANET. The feature selection using AMFO algorithm is effective in handling high dimensional feature space which is often the simulation data and reduce the dimensionality by selecting essential feature. Compared to existing techniques like CNN and SRLSTM, the proposed PDF-QSNN method achieves a high accuracy of 91.45% on the simulated dataset. Future work will focus on classifying and detecting various attacks to identify vulnerability.

REFERENCES

[1] Vatambeti, R., Mantena, S.V., Kiran, K.V.D., Chennupalli, S. and Gopalachari, M.V., 2024. Black hole attack detection using Dolphin Echo-location-based machine learning model in MANET environment. Computers and Electrical Engineering, 114, p.109094.

[2] Reka, R., Karthick, R., Ram, R.S. and Singh, G., 2024. Multi head self-attention gated graph convolutional network based multi attack intrusion detection in MANET. Computers & Security, 136, p.103526.

[3] Ninu, S.B., 2023. An intrusion detection system using exponential Henry gas solubility optimization based deep neuro fuzzy network in MANET. Engineering Applications of Artificial Intelligence, 123, p.105969.
[4] Ryu, J. and Kim, S., 2023. Reputation-based opportunistic routing protocol using q-learning for manet attacked by malicious nodes. IEEE Access, 11, pp.47701-47711.
[5] Abdelhamid, A., Elsayed, M.S., Jurcut, A.D. and Azer, M.A., 2023. A lightweight anomaly detection system for black hole attack. Electronics, 12(6), p.1294.
[6] Nirmaladevi, K. and Prabha, K., 2023. A selfish node trust aware with Optimized Clustering for reliable routing protocol in Manet. Measurement: Sensors, 26, p.100680.
[7] Liu, W., Chen, Z., Yu, X. and Zhou, X., 2022. A cluster-based approach against wormhole attacks in MANETs among smart grid. Frontiers in Energy Research, 10, p.1017932.
[8] Mankotia, V., Sunkaria, R.K. and Gurung, S., 2023. AFA: Anti-flooding attack scheme against flooding attack in MANET. Wireless Personal Communications, 130(2), pp.1161-1190.
[9] Kaushik, S., Tripathi, K., Gupta, R. and Mahajan, P., 2024. Enhancing reliability in mobile ad hoc networks (MANETs) through the K-AOMDV routing protocol to mitigate black hole attacks. SN Computer Science, 5(2), p.263.
[10] Subburayalu, G., Duraivelu, H., Raveendran, A.P., Arunachalam, R., Kongara, D. and Thangavel, C., 2023. Cluster based malicious node detection system for mobile ad-hoc network using ANFIS classifier. Journal of Applied Security Research, 18(3), pp.402-420.
[11] Veeraiah, N. and Krishna, B.T., 2022. An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence, pp.1-15.
[12] Lakshmi, G.V. and Vaishnavi, P., 2023. A trusted security approach to detect and isolate routing attacks in mobile ad hoc networks. Journal of Engineering Research.
[13] Mankotia, V., Sunkaria, R.K. and Gurung, S., 2023. DT-AODV: A dynamic threshold protocol against black-hole attack in MANET. Sādhanā, 48(4), p.190.
[14] Srilakshmi, U., Alghamdi, S.A., Vuyyuru, V.A., Veeraiah, N. and Alotaibi, Y., 2022. A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 10, pp.14260-14269.
[15] Shukla, M., Joshi, B.K. and Singh, U., 2024. A Novel Machine Learning Algorithm for MANET Attack: Black Hole and Gray Hole. Wireless Personal Communications, pp.1-26.
[16] Abdan, M. and Seno, S.A.H., 2022. Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). Wireless Communications and Mobile Computing, 2022(1), p.2375702.
[17] Vincent, S.S.M. and Duraipandian, N., 2024. Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm. Expert Systems with Applications, 249, p.123765.
[18] Prasad, M., Tripathi, S. and Dahal, K., 2023. A probability estimation-based feature reduction and Bayesian rough set approach for intrusion detection in mobile ad-hoc network. Applied Intelligence, 53(6), pp.7169-7185.
[19] Deivakani, M., Sheela, M.S., Priyadarsini, K. and Farhaoui, Y., 2024. 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, 43, p.101021.
[20] Krishnasamy, B., Muthaiah, L., Kamali Pushparaj, J.E. and Pandey, P.S., 2023. DIWGAN optimized with Namib Beetle Optimization Algorithm for intrusion detection in mobile ad hoc networks. IETE Journal of Research, pp.1-20.