Improving Manet Security using Crayfish Optimization and GRU-LSTM Classifier for Intrusion Detection and Prevention

Ragi G R
Department of Data Analytics
MG University,
Kottayam -686560, India
ragigr10@gmail.com

Dhanya G S
Department of Computer Applications
St Teresa's College,
Park Avenue, Marine Drive, Ernakulam, Kerala, India.
dhanyagnambiar@gmail.com

P. Mukilan
Department of Electronics and Communication Engineering,
Dhanalakshmi Srinivasan College of Engineering,
Coimbatore-641105, India.
venmukilan@ieee.org

Enoch Raja DG
Department of computer Science and Engineering
Vels Institute of Technology and Advanced Studie,s
Pallavaram, Chennai -600117 India.
enochrajadr@gmail.com

K. Sushita
Department of Electrical and Electronics Engineering
Vels Institute of Science, Technology & Advanced Studies,
Chennai, India.
sushita.se@vistas.ac.in

R. Senthil Kumar
Department of Electrical and Electronics Engineering
Vel Tech High Tech Dr Rangarajan Dr Sakunthala Engineering College,
Chennai, India.
rskumar.eee@gmail.com

2025 8th International Conference on Circuit, Power & Computing Technologies (ICCPCT) | 979-8-3315-4317-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICCPCT65132.2025.11176776

***Abstract*—Mobile Ad-Hoc Networks (MANETs) face significant security challenges owing to their dynamic nature, distributed structure and frequent mobility of the nodes. An efficient Intrusion Detection and Prevention Systems (IDPS) is necessary to provide security against malicious attacks or disruptions to its operation. Although traditional methods utilize a selection of Machine Learning (ML) and Deep Learning (DL) methods, susceptible to increased computational complexity, decreased system performance and high false-positive rates. Therefore, this paper presents a hybrid framework to protect MANETs by combining Crayfish Optimization Algorithm (COA) with a Gated Recurrent Units (GRU) and Long Short-Term Memory (LSTM) classifier for Intrusion Detection (ID) and prevention. COA used for enhancing MANET routing by identifying the shortest and efficient path for data transmission. The hybrid model classify/predict different types of intrusions accurately by integrating the complementary strengths of GRU-LSTM models. The proposed approach is implemented using Python software with WSN-DS datasets through various experiments demonstrating significant improvements in ID rates, accuracy of 95%, false positive rates, and system efficiencies to provide a robust approach to securing MANETs.**

Keywords—MANET, Intrusion Detection, Crayfish Optimization, Gated Recurrent Units and Long Short-Term Memory.

I. Introduction

A. Overview

A MANET involves many wireless nodes, which connect to form a network for a specified duration, enabling communication without the need for specific infrastructure. An ad hoc network easily established in any location with mobile devices and adding nodes to the network without difficulties, and network management costs are lower [1]. MANETs are often used in sensitive situations such as emergency response, where ID is crucial to ensures sensitive information, like personal or mission critical information, remains private and confidential especially in hostile or combat situations. [2] The decentralized and dynamic nature of MANETs make them instrumental in a variety of practical applications. However, this flexibility comes with an increasing level of vulnerability to security threats, specifically intruder attacks that reduce network performance through increased packet loss, latency, and congestion [3].

Intrusion actions significantly decrease MANET performance by creating network congestion, packet loss, and additional delay. Nonetheless, effective and rapid detection and removal of intruders, are essential to preserving network performance and provide dependable connectivity among mobile nodes. In healthcare or finance, regulatory requirements dictate the implementation of strict security mechanisms protecting sensitive data [4]. Intruder identification helps organizations to meet compliance requirements and mitigate the potential for legal and financial consequences due to data breaches or security events. Overall, ID is important for MANET security, reliability, and resilience to support secure and dependable communication challenging situations. Recent studies have examined a variety of techniques to enhance MANET detection capabilities, such as ML, DL algorithms, and swarm intelligence [5].

B. Related Studies

In 2023 Mohamad T Sultan *et al,* have been developed Artificial Neural Network (ANN) classifiers for ID in MANETs that effectively detect Denial of Service (DoS) attacks. Nevertheless, ANNs often require significant amounts of training data, which is difficult to derived by resource constrained framework of MANETs [6]. In 2023 C. Edwin Singh *et al,* have introduced Principal Component Analysis based Fuzzy Extreme Learning Machine (PCA-FELM) model to enhance network security by increasing detection rates. However, this model requires additional parameters in detecting different types of network attacks [7]. In 2024 M. Sahaya Sheela *et al*, have combining an Adaptive

979-8-3315-4317-4/25/$31.00 ©2025 IEEE

Marine Predator Optimization Algorithm (AOMA) and a Deep Supervise Learning Classification (DSLC) mechanism to create an enhancement to the security and classification accuracy of ID for MANET systems. Although the process achieved high detection and classification accuracy but its higher computational time, along with misclassification, which still require further improvements for use in a real time MANET environment [8]. In 2023 G. Madhu *et al,* have presented an IDPS Model using COOT Optimization and a Hybrid LSTM-KNN Classifier for MANETs contribute to network security. This method improved detection accuracy, reduced false alarms, and a successful intrusion prevention scheme. However, its scalability limited when applied to larger and complex networks [9]. Thus, existing IDS are more dependent on sophisticated methods and implementation like ML, DL and optimization algorithms that are computationally intensive, complicated and highly challenging.

Research Gaps:

Despite progress, securing MANETs with crayfish optimization and GRU-LSTM classifiers faces challenges such as high false positives, slow detection, and poor adaptability to dynamic conditions. The use of crayfish optimization for feature selection and GRU-LSTM models lacks extensive real-time evaluation, especially in resource-limited settings. Limited validation on realistic datasets underscores the need for more efficient, adaptive, and lightweight security solutions.

To address these challenges, this study MANET Security developed the optimized Crayfish with GRU-LSTM Classifier model, for detect intrusions. The contribution of this work is,

- A successful ID approach is created to detect various forms of assaults in MANET, thus enhancing network security.
- COA improve MANET routing by identifying the shortest and most efficient path for data transmission.
- A hybrid GRU-LSTM classifier is designed to accurately predict various kinds of threats over the MANET.

II. Proposed System Description

The security of MANET with combinations of DL and optimization strategies as shown in Fig1. The initial phase is a dynamic MANET, composed of mobile nodes, such as laptops and smartphones that exchange information as an entirely decentralized network, rendering the system vulnerable to intrusion.

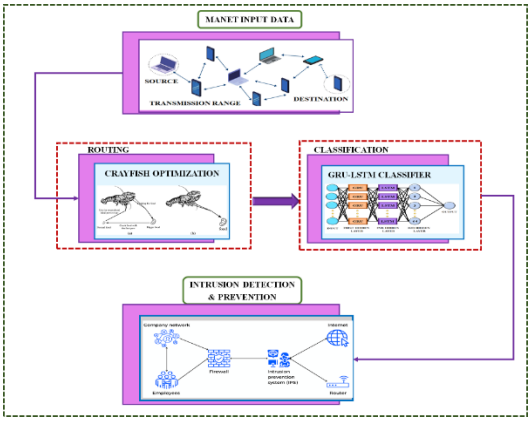

Fig. 1. Proposed diagram for secure MANET in IDS using crayfish optimized GRU-LSTM classifier

Input data from mobile nodes network traffic data is collected and deliver COA routing, which optimizes the route selection process for efficient and secure data transmission. The GRU-LSTM Classifier that evaluates temporal characteristics to identify threats such as DoS, blackhole and wormhole attacks accurately. Once the classification phase is completed, the output submitted to the intrusion decision and prevention module to decide appropriate development of achievement, whether it's an alert, blocking a suspicious node that aligns with the decisions made.

III. Proposed System Modelling

A. Crayfish Optimization Algorithm

COA is motivated by foraging patterns, competitive activities, and summer vacation habits of crayfish. It consists of different stages encompassing foraging and competition (exploitation stages) and summer vacation (exploration stage) as process in Fig. 2. The positions of crayfish colonies represent potential solutions, and behaviour of crayfish colony is based on the temperature of environment. In MANET intrusion detection, the crayfish colonies represent constantly changing routing solutions, with the behaviour being influenced by the conditions of the underlying network, such as traffic anomalies and attack.

a) Initialization

COA initialization stage begins an arbitrary set of candidate routing solutions in multi-dimensional space. For each crayfish is denoted by a 1 × dim matrix, and every column representing variable of interest's solution corresponds to routing paths between nodes. The variables within the solution are allowed to vary within upper and lower predetermined limits. The initialization stage generates only N number of candidate solutions that correspond to the possible network routes and intrusion detection paths. Eq. (1) depicts initialization process of COA.

$$X = [X_1, X_2, \ldots, X_N] = \begin{bmatrix} X_{1,1} \ldots X_{1,j} \ldots X_{1,dim} \\ \vdots \ \ldots \ \vdots \ \ldots \ \vdots \\ X_{i,1} \ldots X_{i,j} \ldots X_{i,dim} \\ \vdots \ \cdots \ \vdots \ \cdots \ \vdots \\ X_{N,1} \cdots X_{N,j} \cdots X_{N,dim} \end{bmatrix} \quad (1)$$

Here, $X, N \ and \ dim$ represents initial population position, number, and dimension, respectively. $X_{i,j}$ denotes position of individual $i \ in \ j$ dimension. Value of $X_{i,j}$ is determined from Eq. (2).

$$X_{i,j} = lb_j + \left(ub_j - lb_j\right) \times rand \quad (2)$$

Here $lb_j \ and \ ub_j$ stands lower bound of $j-th$ dimension. Random number denoted by $r \ and$.

b) Foraging Stage (exploitation)

During foraging phase, crayfish approach food depended on its size (Q), with differing feeding behaviours contingent on food size. When the food item is beyond a certain size (Q too large), crayfish modify to shredding food item with their claws; if food size is manageable, crayfish continue their trajectory toward the food item and consume it. The location of food is specified X_{food} and size of food Q:

$$X_{food} = X_G \quad (3)$$

$$Q = C_3 \times \left(fitness_i / fitness_{food}\right) \quad (4)$$

Here, C_3 stands for food factor, which indicates greatest food and constant value of 3. The food collected by crayfish that connected to their food consumption, hence the formula for foraging operates as below:

$$X_{i,j}^{t+1} = X_{i,j}^t + X_{food} \times p \times (cos(2 \times \pi \times rand) - \sin(2 \times \pi \times rand)) \quad (5)$$

In MANET intrusion detection, evaluate proceed toward the best routes based on the best fitness value from the network traffic. In the exploration of the network, crayfish modify their path to avoid the place under attack, which is essentially to process of identifying secure routing paths to mitigate risk of attack. In the foraging stage, the COA becomes increasingly near to best solution, thus enhancing the algorithm's capacity to exploit it and achieve good convergence.

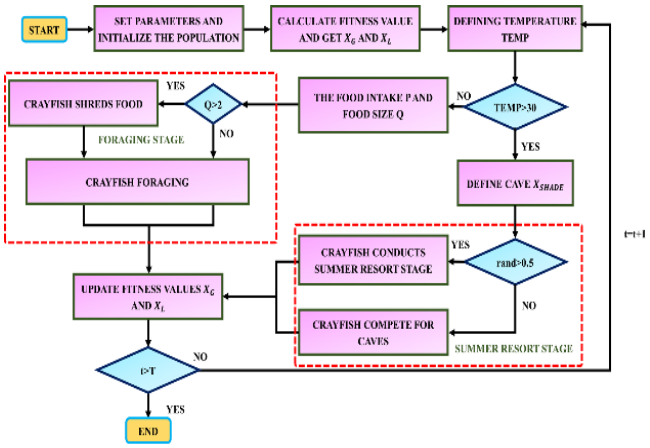

Fig. 2. Flowchart of COA

c) Competition Stage (exploitation)

If $temp > 30 \ and \ rand \geq 0.5$, it indicates other crayfish are searching in cave. During this point, they are going to battle over the cave. Using Eq. (6), crayfish battle in the cave.

$$X_{i,j}^{t+1} = X_{i,j}^t - X_{z,j}^t + X_{shade} \quad (6)$$

During, Competition stage, crayfish fight against each other, and crayfish X_i modifies its location in response to another crayfish's location X_z. This competition helps the algorithm to derive routing paths that minimize attacks, improve security, and enhance detection, although the crayfish adapt its position as an approach to improve the security of their network.

d) Summer Retreat Stage (exploration)

If it $temp > 30$, crayfish choose to spend summer in the cave. The following is the definition of the cave X_{shade}:

$$X_{shade} = (X_G + X_L)/2 \quad (7)$$

Here X_G denotes best position and X_L stands best position in current population. Following Eq. (8), crayfish moving into cave for summer retreat.

$$X_{i,j}^{t+1} = X_{i,j}^t + C_2 \times rand \times \left(X_{shade} - X_{i,j}^t\right) \quad (8)$$

The crayfish begin to approach the caves guiding individuals toward the best solution and improving COA exploitation ability. This phase is an exploration phase where the crayfish algorithm, are exploring alternative routing paths and detection mechanisms in response to evolving attack patterns. After the COA optimizes the routing path by finding the shortest and most secure route, thus the data from these paths, including traffic patterns and node behaviours, is provided to the GRU-LSTM classifier, which analyses and detects potential security threats and abnormalities.

B. GRU-LSTM Classifier

GRU-LSTM classifier, uses to improve detecting and preventing intrusions in MANET. Considering, the sequential nature of the network traffic, the GRU-LSTM model detects an intrusion to a very high degree of

accuracy while adapting to dynamic network environments. This also provides a lean and reliable solution to reduce security threats to MANETs through real-time protective measures against hazardous actions.

a) Gated Recurrent Unit (GRU)

GRU model that uses gate structures to control information flow and it has two gates: reset and update, that compared to LSTM's combined input and forget gates. GRUs get better performance and have fewer parameters simply because of their structure. The reset and update gates of GRU are signified as:

$$m_s = \sigma\left(W_m\left[h_{(s-1)}, x_s\right] + U_m h_{(s-1)} + b_m\right) \quad (9)$$

$$n_s = \sigma\left(W_n\left[h_{(s-1)}, x_s\right] + U_n h_{(s-1)} + b_n\right) \quad (10)$$

Here m_s *and* n_s denotes reset and update gate at time step s. x_s stands input step time s and $h_{(s-1)}$ represents hidden state step time $s-1$. W_m and W_n denotes weight matrices of reset and update gates. σ stands sigmoid function. U_m *and* U_n represents weight matrices in hidden state. b_m and b_n denotes biases of reset and update gates. The following formula subsequently used to determine the candidate hidden state, $\check{h}_s$:

$$\check{h}_s = tanh\left(W\left[m_s * h_{(s-1)}, x_s\right\} + b\right) \quad (11)$$

Here W *and* b denotes weight matrix and bias label.

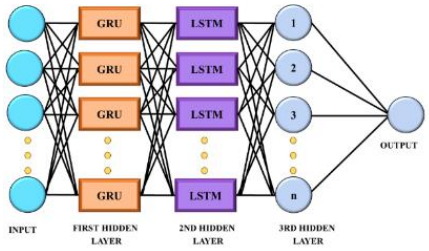

Fig. 3. Architecture diagram of GRU-LSTM

b) Long Short-Term Memory (LSTM)

An LSTM aimed to manage long-term dependencies that consists of three main gates: forget gate, input gate, and output gate. Forget gate adopts whether to retain data from previous cell state based on its relevance. Input gate controls which new data added to cell state, using a sigmoid function. The candidate cell state is generated by $tanh$ function, producing potential new values, which are selectively updated by the input gate, enabling the network to retain relevant information over time. Performance of input gate using mathematical equation below.

$$q_s = \sigma\left(W_{q[h_{s-1}, x_s]} + b_s\right) \quad (12)$$

$$v_s = tanh\left(W_{v[h_{s-1}, x_s]} + b_v\right) \quad (13)$$

Here q_s denotes input gate at time s, W_q stands weight matrix, h_{s-1} represents previous hidden state, x_s *and* b_s stands input and bias at time s, v_s stands cell state, W_v *and* b_v denotes weight matrix and bias vector. The output gate is responsible for generating output based on improved cell state. After selecting appropriate values to output utilizing sigmoid function, the $tanh$ function is used to modified cell state to produce the output. The following formula underlying output gate.

$$f_s = \sigma\left(W_{f[h_{s-1}, x_s]} + b_f\right) \quad (14)$$

$$h_s = f_s * tanh(v_s) \quad (15)$$

This research applies the combination of GRU and LSTM approaches for detecting modelling, as outlined in Fig. 3. The GRU-LSTM classifier handles sequential data such as traffic patterns and extracts information from both short-term and long-range dependencies to determine deviations from normal behaviour in order to identify intrusions.

IV. Result And Discussion

This work presents a novel approach to enhancing network security through Crayfish Optimization and a GRU-LSTM classifier for intrusion detection and prevention, with the results obtained, as detailed below.

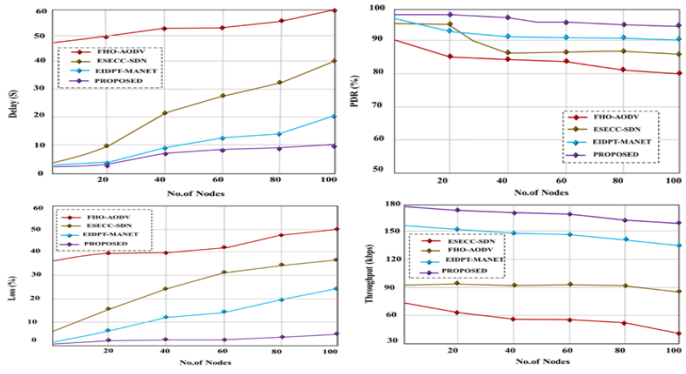

Fig. 4. Comparison of Delay, PDR, loss and throughput

Fig. 4 compares delay PDR, loss and throughput performance of FHO-AODV [10], ESECC-SDN [11], EIDPT-MANET [9], and proposed method as the number of nodes increases. The proposed method achieves significantly lower delay, maintains a consistently higher delivery rate, loss consistently low and highest throughput than all others existing methods. This proves its superior ability to handle high data traffic and maintain performance under network load.

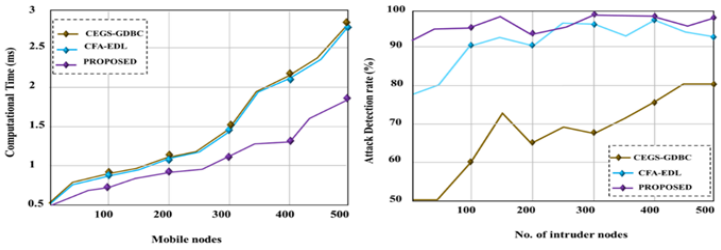

Fig. 5. Comparison of computational time and Attack detection rate

Fig. 5 shows mobile nodes increase, computational time & attack detection rate grows for CEGS-GDBC [12] and CFA-EDL [13], and the proposed method. This indicates that the proposed approach offers faster computation, better scalability and achieving the highest detection accuracy to the existing approaches.

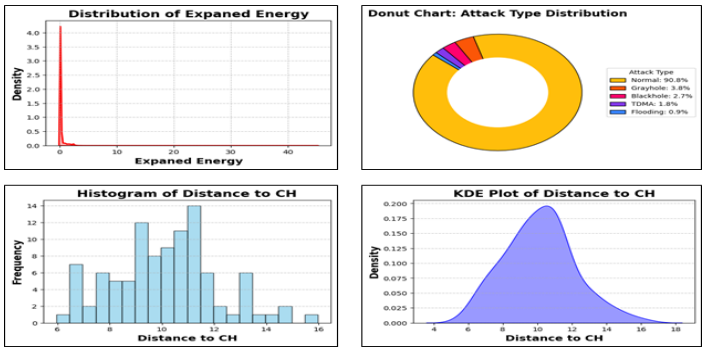

Fig. 6. Distribution of expand energy, attack types, distance CH with histogram & KDE plot

Fig. 6 represents a Distribution of expand energy, attack types, and distance CH with histogram & KDE plot. Expand energy has a sharp peak above 4.0 at very low energy values close to 0.1, with the distribution quickly tapered off as values increase up to around 45. Different attack type's shows Normal class dominates with 90.8%, followed by Grayhole (3.8%), Blackhole (2.7%), TDMA (1.8%), and Flooding (0.9%). The frequency of different distances to the Cluster Head (CH) values range from 6 to 16, with the most frequent values appearing between 10 and 12, and the highest reaching a frequency of around 14. KDE plot that shows density distribution of distances to the CH, which has a smooth peak slightly below 0.2 around 10, with the values crossing from about 4 to 18.

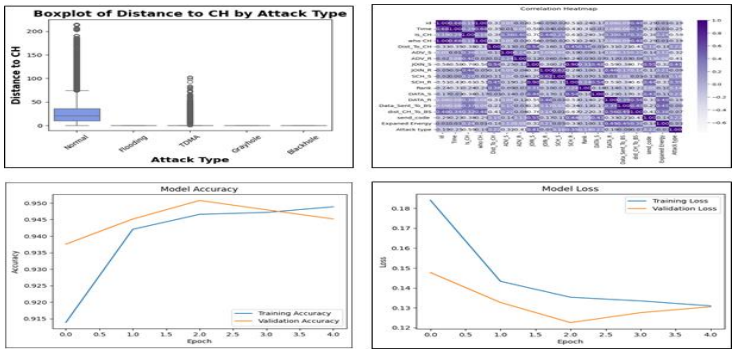

Fig. 7. Distance to CH by attack type, correlation heatmap, model accuracy & loss

Fig. 7 showing Distance to CH by attack type, correlation heatmap, model accuracy & loss. The distribution of distance to the CH for various attack types involve normal flooding, TDMA, Gray hole & black hole. Heatmap displaying the correlation between various features in the dataset. It visually highlights which features have strong, moderate, or weak relationships with each other, helping to identify patterns or potential dependencies among them. Model training & loss over 5 epochs that the accuracy reaches about 0.955, while the losses drop to around 0.1 respectively, showing learning progress.

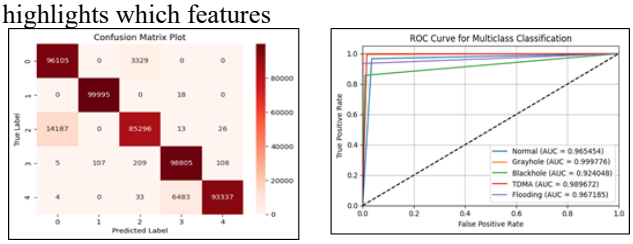

Fig. 8. Confusion matrix & ROC curve

Fig. 8 represents a confusion matrix and ROC curve evaluating classification performance across five classes. Confusion matrix shows high accuracy for most labels with minimal misclassifications, indicating that the GRU-LSTM classifier effectively distinguishes between normal and various attack types. ROC curves evaluating the proposed model's performance across all classes. AUC values are high for all classes: Gray hole (0.999776), TDMA (0.989672), Flooding (0.967185), Normal (0.965454), and Blackhole (0.924048), showing excellent classification capability in detecting a wide range of attacks in MANETs.

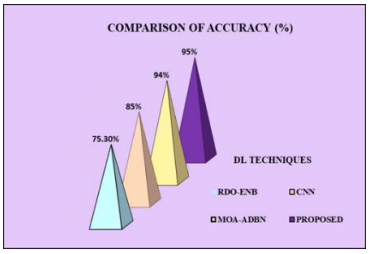

Fig. 9. Comparison of accuracy

Fig. 9 compares accuracy of different existing techniques, like RDO-ENB [14], CNN [15], and MOA-ADBN [16] achieve 75.30%, 85%, and 94% respectively. The proposed method outperforms all with the highest accuracy of 95%, classification performance for ID in MANETs.

TABLE I. COMPARISON OF RECALL ACROSS VARIOUS METHODS

Techniques	Recall (%)
PROPOSED	95%
MOA-ADBN [16]	93.48%
HYBRID LSTM-KNN [9]	82%

Table 1 compares recall of different techniques, involves MOA-ADBN, hybrid LSTM-KNN with the proposed method outperforms all other listed methods.

V. CONCLUSION

The paper proposes an effective Crayfish Optimization and GRU-LSTM Classifier-based IDPS model for MANET, for network security. COA identify important attributes and classify normal and abnormal nodes based on trust values; therefore, it has better detection accuracy, and the GRU-LSTM hybrid model is effectively classifying and predicting different kinds of intrusions. The overall results of the proposed system show great performance using all metrics with increased accuracy of 95%, precision of 95.4%, recall of 95.2%, f1-score of 95.4% while reducing errors. Also, the proposed system having a low average delay, a high packet delivery ratio, high throughput, and non-packets losses, with hight detection characteristic and a low computational time, all points to an efficient detection and prevention of malicious attacks in MANET environments. The results imply the proposed IDS with Crayfish Optimization and GRU-LSTM models enhanced the security and reliability of MANETs and is a promising approach to countering attacks to the network.

REFERENCE

[1] C. E. Singh, and S. M. C. Vigila, "An investigation of machine learning-based intrusion detection system in mobile ad hoc network," International Journal of Intelligent Engineering Informatics, vol. 11, no. 1, pp. 54-70, 2023.

[2] S. Hemalatha, T. V. Rao, S. Shalini, S. S. Nair, S. L. K. Vinti and D. G. K. Mohan, "Mobile Adhoc Network Intruder Node Detection, and Prevention for Efficient Packet Transfering," Journal of Theoretical and Applied Information Technology, vol. 102, no. 23, 2024.

[3] S. M. Hassan, M. M. Mohamad, and F. B. Muchtar, "Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks," IEEE Access, 2024.

[4] E. Sandhya, K. S. Sk, S. V. Mantena, V. S. Desanamukula, C. Koteswararao, S. R. Vemula, and M. Vemula, "Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection," Scientific Reports, vol. 15, no. 1, pp. 818, 2025.

[5] C. Edwin Singh, and S. M. Celestin Vigila, "WOA-DNN for Intelligent Intrusion Detection and Classification in MANET Services," Intelligent Automation & Soft Computing, vol. 35, no. 2, 2023.

[6] M. T. Sultan, H. E. Sayed, and M. A. Khan, "An intrusion detection mechanism for MANETs based on deep learning artificial neural networks (ANNs)," arXiv preprint arXiv, vol. 2303, no. 08248, 2023.

[7] C. E. Singh, and S. M. C. Vigila, "Fuzzy based intrusion detection system in MANET," Measurement: Sensors, no.26, pp. 100578, 2023.

[8] M. S. Sheela, A. G. oundari, A. Mudigonda, C. Kalpana, K. Suresh, K. Somasundaram, and Y. Farhaoui, "Adaptive Marine Predator Optimization Algorithm (AOMA)-Deep Supervised Learning Classification (DSLC) Based IDS Framework for MANET Security," Intelligent and Converged Networks, vol. 5, no. 1, pp. 1-18, 2024.

[9] G. Madhu, "Design of Intrusion Detection and Prevention Model Using COOT Optimization and Hybrid LSTM-KNN Classifier for MANET," EAI Endorsed Trans. Scalable Inf. Syst, vol. 10, no. 3, pp. e2, 2023.

[10] J. A. Rathod, and M. Kotari, "TriChain: Kangaroo-based intrusion detection for secure multipath route discovery and route maintenance in MANET using advanced routing protocol," International Journal of Computer Networks and Applications, vol. 11, no. 1, pp. 61-81, 2024.

[11] V. A. Vuyyuru, Y. Alotaibi, N. Veeraiah, S. Alghamdi, and K. Sirisha, "EsECC_SDN: Attack Detection and Classification Model for MANET," Computers, Materials & Continua, vol. 74, no. 3, 2023.

[12] V. G. Krishnan, A. P. Saleem, N. Kirubakaran, S. Veeramalai, A. K. Kumar, C. Jehan, J. Deepa, and G. Dhanalakshmi, "Ensemble Deep Learning Classifier with Optimized Cluster Head Selection for NIDS in MANET," J. Inf. Sci. Eng, vol. 39, no. 6, pp. 1233-1246, 2023.

[13] S. Dilipkumar, and M. Durairaj, "Epilson Swarm Optimized Cluster Gradient and deep belief classifier for multi-attack intrusion detection in MANET," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 3, pp. 1445-1460, 2023.

[14] M. Sasikumar, and K. Rohini, "Expedient Intrusion Detection System in MANET Using Robust Dragonfly-Optimized Enhanced Naive Bayes (RDO-ENB).

[15] M. Sasikumar, and K. Rohini, "Intrusion Detection System through deep learning in routing MANET networks," Intelligent Automation & Soft Computing, vol. 37, no. 1, 2023.

[16] R. Ramamoorthy, S. Ramu, and R. K. Ranganathan, "Optimized Deep Learning for Cyber Intrusion Detection and Secured Communication in MANET," Yanbu Journal of Engineering and Science, vol. 21, no. 2, pp. 67-73, 2024.