SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I7P124

Volume 12 Issue 7, 305-314, July 2025


*Original Article*

# An Enhanced Hybrid Approach for Real-Time Application-Layer DDoS Detection and Resilience in MANET Environments

Kiran M. Salunke[1], Suresh Kurumbanshi[2]

[1,2]*Department of Computer Engineering, MPSTME, NMIMS University, Shirpur, India.*

[1]*Corresponding Author : kiran.salunke@nmims.edu*

Received: 13 May 2025 Revised: 14 June 2025 Accepted: 15 July 2025 Published: 31 July 2025

***Abstract*** *- Mobile Ad hoc Networks (MANETs) face growing security threats from application-layer distributed denial-of-service (DDoS) attacks, which create severe performance and reliability problems. This research develops a complete hybrid framework that combines Fuzzy Extrapolation System (FES) with Brownian Motion-enhanced Harris Hawks Optimization (BM-HHO) and an Extended Simplified Pulse-Coupled Neural Network (X-SPCNN) classifier. The BM-HHO algorithm identifies key features that reduce the input space to enhance model performance. The X-SPCNN system performs exact attack detection while the FES component assesses node trustworthiness and contextual factors to direct adaptive mitigation strategies. The proposed solution undergoes validation using a simulated MANET dataset, which includes malicious traffic patterns that simulate actual attack behaviour and real-world traffic of the Darknet. The framework demonstrates consistent detection accuracy above 99.2% with low false positives while operating effectively under typical MANET resource constraints. The combination of bio-inspired optimization techniques with neural classification and fuzzy reasoning enables a robust, scalable defense system that matches the dynamic decentralized characteristics of MANETs.*

***Keywords*** *- MANET security, DDoS attack detection, Fuzzy Extrapolation System, Harris Hawks Optimization, Feature selection, Pulse-Coupled Neural Network, Application-layer attacks, Real-time IDS.*

## 1. Introduction

The infrastructure-free communication capabilities of Mobile Ad hoc Networks (MANETs) make them suitable for vital situations such as disaster relief and tactical operations. MANETs become highly vulnerable to application-layer Distributed Denial-of-Service (DDoS) attacks because of their decentralized nature and restricted resources. These attacks use valid request patterns to send excessive traffic to services while using up node resources, so they avoid standard network-layer security measures. The combination of decentralized management with fluctuating bandwidth and energy constraints makes it difficult to detect threats in a timely manner. The differentiation between malicious behavior and legitimate traffic surges remains difficult to achieve accurately in real-time because of these constraints [9]. Traditional intrusion detection mechanisms for MANETs do not function effectively within changing network conditions. Signature-based detection models lack effectiveness against evolving attack methods, yet threshold-based anomaly detection systems produce numerous false alarms when handling dynamic network traffic patterns. The research has incorporated fuzzy logic together with trust-aware systems to address ambiguous traffic patterns. Fuzzy Extrapolation Systems have demonstrated their value in handling uncertain patterns and behavior-based intrusion detection mechanisms, with network indicators enhancing their accuracy. Distributed detection methods provide enhanced network-wide visibility, which enables detection of coordinated and persistent threats that stand beyond localized systems' capabilities [11].

The implementation of machine learning techniques and optimization algorithms has led to the development of flexible detection systems. Swarm intelligence and evolutionary algorithms serve to select features and adjust classifiers in intrusion detection systems. Harris Hawks Optimization (HHO) performance as a workflow refinement method for intrusion detection has been encouraging [12]. Deep neural networks paired with classification models result in significant detection accuracy improvements [13]. Deep learning models typically exceed the computational budget that resource-limited environments can support. PULSE-COUPLED NEURAL NETWORKS (PCNNs) represent lightweight spiking neural architectures that use biological inspiration to provide efficient detection with equivalent accuracy levels.

The research presents a single unified system that detects and blocks DDoS attacks in real-time within MANETs. This proposed solution merges Brownian motion-enhanced HHO for optimized feature selection with a lightweight X-SPCNN model for high-precision classification and a fuzzy Extrapolation system for context-driven risk assessment. The integration of these components allows for real-time, adaptable and scalable solutions with interpretability.

This integrated mitigation strategy uses the collected intelligence to actively control suspicious network traffic while safeguarding authorized communications. The three-component framework provides a balanced approach that unites focused feature detection with strong pattern identification and context-based decision-making.

The main difficulty in protecting MANETs from application-layer DDoS attacks remains the system's capability to distinguish between normal traffic bursts and malicious activities in real time under limited computing resources. The current IDS systems that use static signatures and fixed thresholds demonstrate poor adaptability because they either generate many false alarms or fail to detect stealthy attacks.

The current research field lacks an integrated solution that simultaneously optimizes feature efficiency and classification accuracy, and behavioral context assessment. Deep learning models achieve high detection rates, but their computational intensity makes them impractical for MANET deployment. The use of fuzzy systems as a standalone solution does not provide enough sensitivity to detect fast-evolving threat vectors.

The development of a unified detection mechanism that suits resource-constrained MANETs remains an open research challenge. Our proposed hybrid system combines Brownian motion-enhanced HHO for robust feature selection with X-SPCNN for efficient pattern detection and FES for contextual trust evaluation.

The complete fusion system enhances real-time performance while decreasing false alarms and making it possible to deploy within MANET limitations. The framework has been validated using a synthetically generated dataset emulating benign activity and malicious noise characteristics of real-world scenarios.

The combined detection system demonstrates better detection performance than existing systems, along with faster response times, thus making it suitable as a defense solution for dynamic decentralized networks. The upcoming sections of this paper explain the related work, describe the system structure, explain the experimental design, display assessment results and present future study paths.

## 2. Related Work

The recent progress in securing Mobile Ad Hoc Networks (MANETs) against application-layer DDoS attacks focuses on developing adaptive, lightweight, scalable solutions. Singh et al. established a fundamental defense system that matches the decentralized characteristics of MANETs [1]. Deepa et al. built upon this work by developing clustering-based defensive mechanisms and later creating an entropy-based system for detecting anomalies early [2, 3]. Anjum et al. developed a mobile agent-based load balancing scheme with trust evaluation integration to address traffic distribution issues [4]. Islabudeen and Kavitha Devi created a smart dual-layer IDPS that provides dynamic threat response capabilities [5]. Batchu and Seetha developed a machine learning system that uses hybrid feature selection and tuning methods to detect DDoS attacks effectively in limited resource settings [6]. Beitollahi et al. used cuckoo search optimization to train radial basis classifiers for better accuracy on unbalanced data sets [7]. Legashev et al. developed a layered anomaly detection system that functions in distributed wireless networks [8]. These works demonstrate a trend toward developing hybrid intelligent defense systems that can be deployed in real-world MANET environments.

The initial research into MANET security showed that flooding-based denial-of-service attacks, particularly those that target route discovery like RREQ flooding, can severely affect network performance. The study conducted by Ahmed et al. (2013) used fuzzy rule-based systems to identify network events through the analysis of RREQ frequencies and unique request origins, which demonstrates the capability of fuzzy logic to interpret unclear traffic patterns. The researchers demonstrated that fuzzy Extrapolation systems can distinguish between attacks and normal network activity using their post-attack forensic tool. The run-time DDoS defense proposed by Rajpoot et al. (2020) utilized node isolation based on behavioral indicators at the routing layer. The approach enhanced network throughput under attack [14], yet this improvement came with the risk of mistakenly isolating good nodes through incorrect identification.

Many researchers have studied trust-based systems to address these security risks. The mechanisms use dynamic trust scoring of nodes through observation of packet forwarding success, anomalies in communication patterns, and response latency metrics. According to Janakiraman et al. [15], the use of trust models based on a single parameter proves to be misleading. Energy usage that increases and high data rates could indicate normal activities instead of malicious actions. These problems led to the development of context-aware frameworks that enhance precision through parallel evaluation of multiple indicators. The Integrated Context-Based Mitigation Framework (ICMF) by Janakiraman et al. solved Rendezvous Point Attacks in MANETs through data rate analysis, throughput variation and delay assessment, and

energy consumption metrics to calculate a composite risk score. This multi-metric framework, implemented by Grey system theory, delivered better results than systems using single-factor models.

Fuzzy logic shows compatibility with these research methods. The system uses qualitative terms such as "Low", "Medium", and "High" risk to evaluate different inputs such as packet drop rates or node latency, thereby enabling precise network state-based decisions. A Fuzzy Extrapolation System (FES) within this research calculates trust scores through the assessment of energy depletion rate and latency impact on neighboring nodes in a context-specific manner. The system uses this trust score to enhance classifier results by identifying behavioral anomalies that match normal patterns.

Machine learning classifiers now serve as essential tools to identify DDoS attacks from benign network activities because of rising traffic complexity. The combination of Support Vector Machines (SVM) and deep learning networks with classical methods has led to substantial accuracy improvements. The achievement of effective performance under MANET constraints depends on selecting appropriate features. The three metaheuristic algorithms known as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and Harris Hawks Optimization (HHO) have become standard tools for this particular task.

The bio-inspired HHO technique demonstrates a strong exploration-exploitation balance, which makes it particularly effective for its applications. The implementation of chaotic dynamics and crossover strategies in enhanced HHO systems has produced excellent outcomes for cybersecurity operations [16]. Sokkalingam and Ramakrishnan (2022) used a hybrid HHO system to optimize SVM for DDoS detection, which achieved above 97% accuracy [18].

The Brownian Motion-based HHO (BM-HHO) functions as our system's feature selection method. Brownian motion's chaotic nature enables the exploration of multiple feature combinations, which avoids premature termination of the search process. The evaluation of subsets through classifier performance makes BM-HHO superior to filter-based selection since it delivers features that enhance detection outcomes. Our detection system uses a neural model known as X-SPCNN, which provides accuracy and efficiency.

The traditional PCNN system has shown success in image segmentation, so we have modified its architecture for network traffic analysis. The X-SPCNN model uses convolutional-like spiking layers to detect patterns in time and distribution anomalies. The system operates at a reduced depth, providing quick processing and deployability on mobile platforms.

The research by Palle et al. [17] demonstrated how multi-layer PCNNs achieve high detection rates on cloud datasets when combined with optimization. Our system maintains high accuracy through BM-HHO preselection together with FES contextual filtering while maintaining a lightweight footprint. Three defense layers, including context-aware fuzzy logic, optimized feature pruning and efficient neural classification, work together to create a robust, scalable and accurate defence system for application-layer DDoS attacks in MANETs.

The detection accuracy improved through deep HT-CNNs [16] and PCNNs [17], but their complex nature made real-time operation on MANET nodes challenging. The research collectively shows that a lightweight detection system that integrates context-awareness and maintains high accuracy, fast response, and low computational cost is needed to fill the gap that our hybrid framework addresses through BM-HHO, X-SPCNN and FES.

## 3. Proposed Methodology

The proposed defence framework operates in two distinct phases: offline training and online detection with real-time mitigation. The offline training phase starts with historical network traffic data pre-processing to make it ready for analysis, as illustrated in Figure 1. A feature selection mechanism applies the Extra Trees Classifier during this stage to evaluate the relative importance of each feature. The model retains only the most significant features to decrease dimensionality and enhance its ability to generalize. A Random Forest (RF) classifier receives the optimized feature subset for training to produce a lightweight detection model with high accuracy.

The trained model functions as an online traffic monitor during the second phase of operation. The RF model receives processed HTTP request features in real-time after pre-processing each incoming request. The classifier identifies traffic instances as either benign or an attack. The system uses a mitigation module to detect malicious patterns, which then activates a response mechanism to limit or discard suspicious traffic while allowing legitimate traffic to pass with priority to maintain Quality of Service (QoS).

The framework uses the CIC-Darknet2020 dataset for evaluation, which includes labelled flows that combine benign traffic with multiple attack types, including botnet-induced HTTP floods. The analysis focuses on application-layer attack Behaviour through an examination of session-level characteristics that derive from HTTP request/response interactions. The pre-processing pipeline includes several critical steps, Data cleaning fixes half-written records and fills in blanks; normalization shrinks wild number ranges so one big value doesn't drown the others; aggregation rolls raw packets up into easier-to-read session stats, like average request rate, total requests, and distinct URL counts per visit;

finally, encoding turns text tags such as HTTP methods and response codes into useful numbers, either by sprinkling one-hot columns or by slapping on label codes, so every feature sits on the same tidy bench.

The processed data creates a feature matrix X together with a label vector Y, which are divided into training and test sets with an 80:20 ratio to maintain equal distributions of benign and malicious samples. The training data serves two purposes: it supports both feature selection and classifier training, and the test set functions to assess model generalization.

A proposed system for protecting Mobile Ad Hoc Networks (MANETs) from application-layer Distributed Denial of Service (DDoS) attacks uses a dual-track design that analyzes traffic data and behavioral context simultaneously before merging into a unified defensive plan. The system design appears in Figure 1. The system operates through two independent processing streams: traffic analysis and contextual trust evaluation. The first track in the upper analysis process examines network features, including packet dimensions, together with request speed and time intervals between packets and protocol-specific activities. The feature selection process uses Brownian Motion-enhanced Harris Hawks Optimization (BM-HHO) to optimize discriminative attributes from the input features. The X-SPCNN receives this refined data as input to classify traffic as malicious or normal by producing attack probability or decision outputs.

The lower track runs a Fuzzy Extrapolation System (FES) to assess behavioral and situational context for each network node in parallel with the upper track. The system evaluates performance indicators, including end-to-end delay patterns and node power consumption, packet transmission statistics, and historical irregularities. The FES produces trust scores between 0 and 1 by applying expert-defined rules to fuzzy sets to determine suspicion levels.

The outputs merge at the Mitigation & Response Module. The system implements rules to decide on mitigation actions: full protection occurs when both systems identify threats, while cautious rate limiting happens when one system is suspicious and passive monitoring starts when only minor issues exist. This system uses independent network behavior insights to minimize incorrect detection of both genuine and fake events.

The performance assessment of the classifier depends on accuracy measurements or multiple performance metrics from a training dataset. The feature subset improvement progresses through simulation phases that replicate hawk exploration and exploitation techniques. The application of Brownian motion in both initial and update stages of the process allows for extensive exploration of the feature space through diverse coverage.

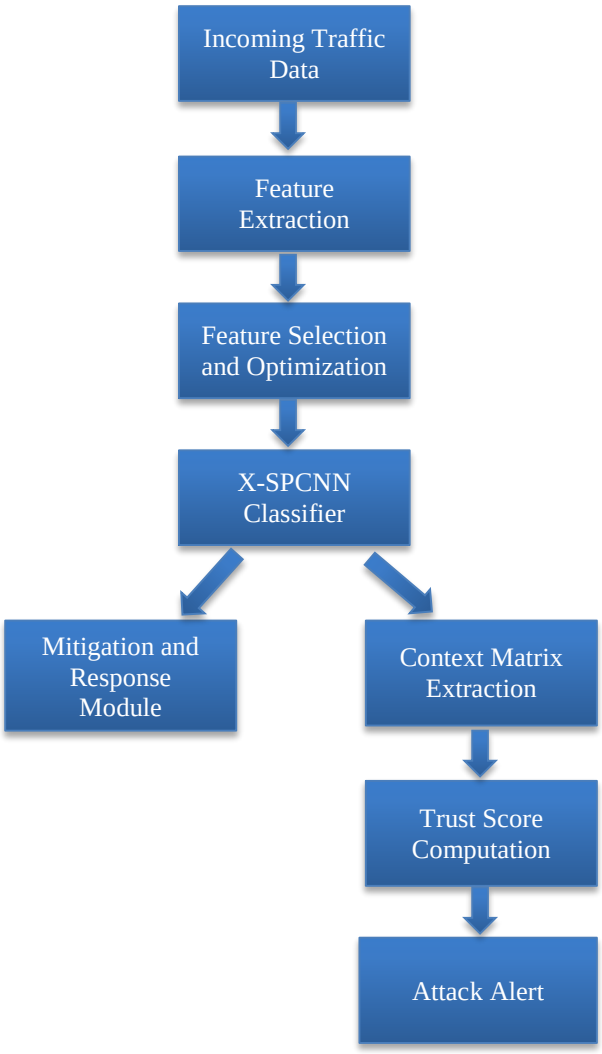


**Fig. 1 The proposed hybrid architecture**

The optimization stops either when performance stops improving or after reaching the maximum number of allowed iterations. The resulting feature subset decreases computation requirements while enhancing detection performance, which is vital for resource-constrained MANET nodes.

The X-SPCNN operates as a basic two-layer neural network that implements PCNN principles to distinguish between attack traffic and normal traffic through binary classification. The first processing layer contains convolutional filters that process both sequential data in sliding windows and instantaneous features. The system produces thwarts to recognize meaningful signals through its mechanism, which replicates biological signal detection processes. The system uses limited lateral inhibition to suppress unwanted signals and enhance recognizable attack patterns. The output neuron collects these activations through an aggregation process and then uses a sigmoid transformation to generate a probability output. The model trains with

backpropagation alongside substitute gradient methods. X-SPCNN operates efficiently because of its simple design and minimized feature inputs, making it suitable for deployment on MANET nodes and edge devices. The system architecture demonstrates resistance to traffic variations because it detects attack surges through observations made within a single window.

The FES system assesses behavioral data that regular traffic features do not detect. The system tracks four performance metrics, including energy consumption patterns, delay indicators, forwarding statistics, and neighbor-to-neighbor information reports. Fuzzy sets with overlapping membership functions represent each metric through {Low, Medium, High} categories. A set of expert-defined fuzzy rules infers a trust score. The system generates Trust = Low when it detects High Traffic Rate combined with Low Throughput and High Energy usage. The Mamdani Extrapolation method, coupled with centroid defuzzification, produces a numerical trust level. The FES operates with caution because it evaluates time-based patterns to prevent false alarms from temporary increases. The FES system can benefit from Recent_Alerts information to enhance its decision-making process when configured as an optional feature, which produces a hybrid system. This multiple-stage assessment technique makes the detection system stronger against mimicry attacks and insider threats. The Fuzzy Extrapolation System (FES) and Trust Score Computation are illustrated mathematically using Equations 1 and 2, respectively.

$$\mu_{Low}(x) = \begin{cases} 1, & x \le a \\ \frac{b-x}{b-a}, & a < x < b \\ 0, & x \ge b \end{cases} \quad (1)$$

Equation 1 illustrates Fuzzification (Membership Function for 'Low') where $a$, $b$ are parameters defining the fuzzy interval for "Low". If Energy = High and Throughput = Low, Trust = Low

$$\text{Trust} = \frac{\int_{\alpha}^{\beta} \mu(x) \cdot x \, dx}{\int_{\alpha}^{\beta} \mu(x) \, dx} \quad (2)$$

Equation 2 illustrates the Final Trust Score (Defuzzification using Centroid Method) where $\mu(x)$ is the aggregated membership function, and $\alpha$, $\beta$ represent the domain limits of trust value (usually 0 to 1)

The system bases its choices on combining trust score data with classifier output information. When both metrics show high threat indicators, the system activates strong blocking actions (blacklisting and alert broadcast). The system performs rate limiting and sandboxing operations when the classifier indicates an attack while trust remains at a moderate level. A system initiates soft challenges or monitoring procedures when the trust score decreases without receiving a classifier alert. Normal operations continue when both metrics show benign indicators. Each node maintains its response policies through independent decision-making while having the capability to share alerts for collective mitigation actions. The mitigation module adjusts its thresholds for recent events to improve its performance. The audit logging system stores a chronological record of responses, which can be used to enhance future model development or support forensic investigations. The system design functions like an immune system through X-SPCNN detection, FES adaptive components, and mitigation as the effectors.

The combined BM-HHO, X-SPCNN, and FES system creates an accurate detection system that produces fast responses and minimizes errors in MANET networks. The combination of learning components with reasoning and optimization techniques demonstrates a state-of-the-art response approach for defending distributed mobile networks against sophisticated threats.

## 4. Results and Discussion

The proposed hybrid detection framework needed evaluation by creating an original dataset that mirrored actual traffic conditions found in Mobile Ad hoc Networks (MANETs). The absence of appropriate public datasets that focus on application-layer DDoS attacks in MANETs led to the creation of synthetic data through NS-3 simulations. The simulation included 50 mobile nodes that operated HTTP file transfers, VoIP sessions, and ICMP pings in a 1000m × 1000m space with the Random Waypoint mobility model. The first half of the simulation period ran without attacks to gather normal operational data. The simulation introduced an application-layer DDoS attack at 300 seconds when five attacker nodes launched HTTP GET floods against the web service-hosting node.

The attack duplicated DDoS strategies through rapid bursts of traffic and continuous low-rate requests to create an aggressive and stealthy attack profile. The experiment incorporated background noise from darknet traffic through scan attempts and malformed packets to enhance detection complexity. The system captured network data in 1-second intervals to obtain performance metrics consisting of TCP connection attempts, request rates, inter-arrival times, throughput and latency measurements. This data is mixed with Darknet CIC 2020 data, which contains real-world attack signatures.

Each node interval tuple received a label indicating its position during the attack period. A Brownian Motion-enhanced Harris Hawks Optimization (BM-HHO) was applied for feature selection to optimize subsets through shallow neural network evaluation, which produced the most informative features from an initial 20. The selected features numbered 10 after evaluation.

An X-SPCNN attack classifier received training with the chosen features. The fundamental structure consisted of a single convolutional layer with temporal filters, leading to an output layer activated by sigmoid functions. Adam optimization led to training convergence during ten epochs. A Fuzzy Extrapolation System (FES) analyzed throughput drop, energy consumption, and classifier alert frequency to generate a dynamic trust score in parallel.

The testing on a mid-range CPU resulted in real-time performance, with each node's evaluation taking less than 3 milliseconds. The framework operates with a compact model and rule base, which makes it suitable for real-time intrusion detection within the limited resources of MANET environments. Table 1 shows the Synthetic Feature and its Real-World Name. Table 2 highlights the top 10 features calculated by FES analysis.

**Table 1. Top 20 features of synthetic dataset**

| | |
|---|---|
| Feature1 | Flow Duration |
| Feature2 | Total Fwd Packets |
| Feature3 | Total Backwards Packets |
| Feature 4 | Packet Length Mean |
| Feature5 | Packet Length Std |
| Feature6 | Flow Bytes/s |
| Feature7 | Flow Packets/s |
| Feature8 | Fwd Packet Length Max |
| Feature 9 | Bwd Packet Length Mean |
| Feature 10 | Flow IAT Mean |
| Feature11 | Flow IAT Std |
| Feature12 | Fwd IAT Mean |
| Feature13 | Bwd IAT Std |
| Feature 14 | Destination Port |
| Feature15 | Protocol (e.g., TCP=6, UDP=17) |
| Feature16 | Source IP ID (encoded) |
| Feature17 | Destination IP ID (encoded) |
| Feature 18 | Packet Interarrival Time |
| Feature19 | URG Flag Count |
| Feature 20 | Down/Up Ratio |

**Table 2. Top 10 features by FES**

| | | |
|---|---|---|
| 1 | Feature4: | 0.1857 |
| 2 | Feature9: | 0.1826 |
| 3 | Feature14: | 0.1069 |
| 4 | Feature20: | 0.1039 |
| 5 | Feature17: | 0.1017 |
| 6 | Feature19: | 0.0773 |
| 7 | Feature6: | 0.0537 |
| 8 | Feature16: | 0.0159 |
| 9 | Feature15: | 0.0157 |
| 10 | Feature7: | 0.0148 |

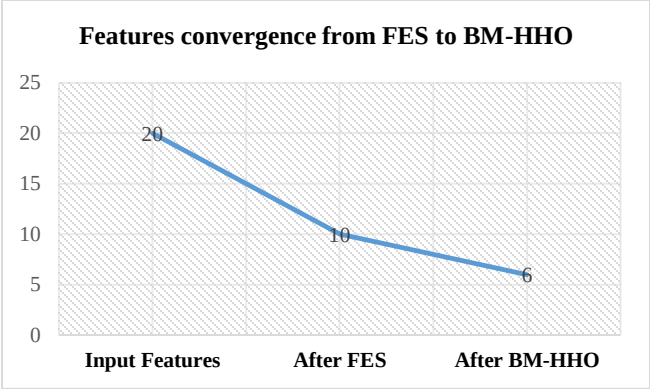


**Fig. 2 Features convergence process**

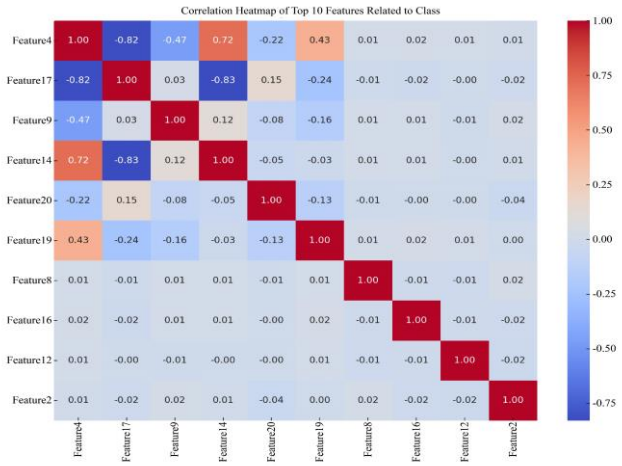


**Fig. 3 Correlation heatmap of top 10 features**

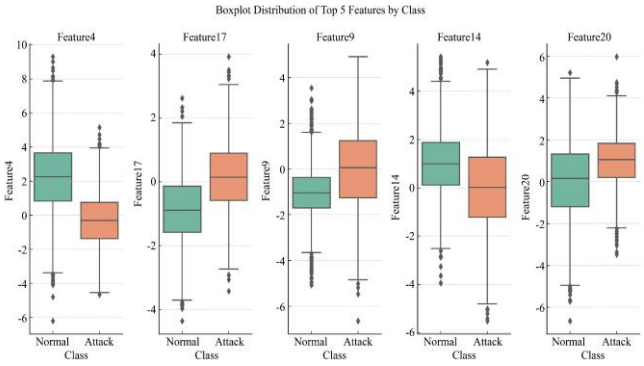


**Fig. 4 Box-plot distribution of top 5 features**

Figure 2 highlights the Features Convergence Process from extraction to BM-HHO. Figure 3 explicates the correlation heatmap of the top 10 Features, with strong correlations marked in dark colour. Figure 4 shows the box-plot distribution of the Top 5 Features by BM-HHO, which is inspired by the hunting nature of hawks. Figure 5 explains the scatter matrix of the top 5 features, highlighting strong correlation in terms of application layer DDoS Attack Detection.

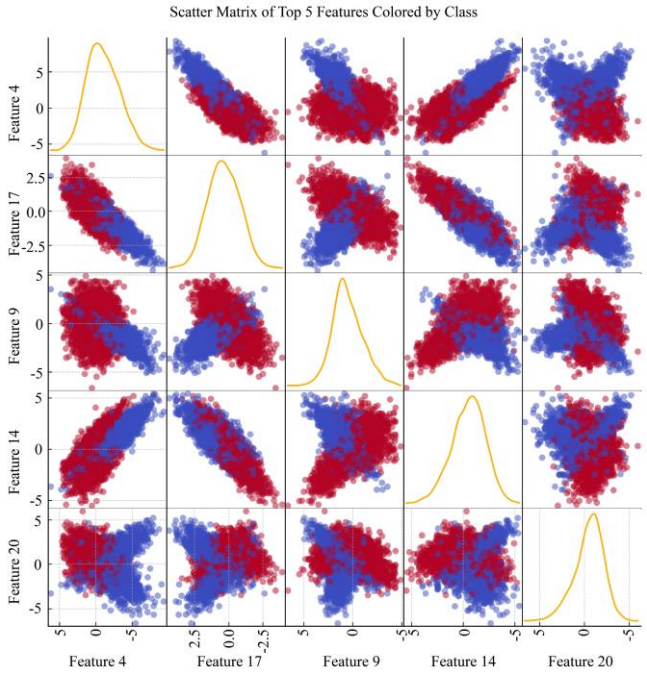


**Fig. 5 Scatter matrix of top 5 features**

The assessment of the proposed hybrid system utilized the synthetic MANET+DDoS dataset. The evaluation examined detection accuracy together with precision and recall (detection rate), as well as false positive rate. The system's reaction time and its ability to handle different attack strength levels were evaluated to determine its readiness for live MANET operations.

The research compared four detection systems, which included (i) the complete hybrid system that combined FES with BM-HHO and X-SPCNN and (ii) an ML-only system using BM-HHO and X-SPCNN without fuzzy logic, (iii) a fuzzy-only system that lacked ML support, and (iv) a conventional SVM classifier that used all features but no optimization techniques. Each model received the same dataset partitions for training and testing purposes to establish a proper evaluation framework.

The hybrid detection system achieved the highest detection accuracy at 99.2%, which outperformed the ML-only detection system, which reached 97.8%. The hybrid model achieved the lowest false positive rate (1.5%), which helps maintain genuine network activity in MANET settings. The recall score reached 99.6%, meaning nearly all attack events were detected. The X-SPCNN failed to identify certain cases, but the FES system detected them by monitoring slight yet persistent degradation in node trust metrics. The ML-only version achieved high recall at 98.1% but it incorrectly identified normal bursts as attacks because it lacked contextual understanding. The fuzzy-only system achieved a 90.7% accuracy rate but performed poorly during the stealthy attack phase because the traffic patterns remained normal and did not activate fuzzy rules quickly.

The SVM-based approach delivered 95.4% accuracy, yet needed additional computation power and exhibited delayed responses because it processed an extensive feature set. The optimization of BM-HHO led to an improvement in X-SPCNN's performance from 96.8% to 97.8% through the selection of a 10-feature subset from its 20 available features, which simultaneously decreased complexity and training duration. Expert heuristics-based manual feature selection proved less effective than BM-HHO, which demonstrated its superiority through metaheuristic optimization.

The FES module in the system proved effective at correcting ML model errors by both eliminating false positives and identifying undetected attacks. The FES module detected 3 attack instances, which ML failed to detect, while suppressing 10 incorrect alerts from normal nodes, thereby enhancing both precision and recall rates. The X-SPCNN system detected high-rate attacks in 1 second, yet the FES system identified stealthy behaviors between 5-6 seconds. The system responded within six seconds throughout its worst-case scenarios. Standard hardware execution of the solution performed well since X-SPCNN Extrapolation needed 2 milliseconds per sample, and FES computations required almost no time.

The hybrid design on the hybrid dataset (Darknet + NS3 simulations) demonstrated robustness against deceptive traffic scenarios through stress testing with flash crowds and slow ramp-up attacks. The FES system protected against ML classifier misclassifications by analyzing the complete behavioral patterns of network activity. The experimental findings confirm that integrating BM-HHO optimization with X-SPCNN classification and fuzzy trust evaluation creates a strong, scalable system for detecting and mitigating application-layer DDoS attacks in MANETs. Table 3 compares different implemented approaches on acclaimed performance metrics.

The proposed hybrid framework presents a new approach that combines Brownian Motion-enhanced Harris Hawks Optimization (BM-HHO) with Extended Simplified Pulse-Coupled Neural Network (X-SPCNN) and Fuzzy Extrapolation System (FES) for application-layer DDoS detection in MANETs. Our system stands apart from previous models because it unites metaheuristic feature selection with biologically inspired lightweight classification and context-aware trust analysis. The existing methods, including GA-SVM and PSO-based classifiers and standalone PCNNs, either fail to interpret context or require excessive computational resources that exceed MANET node capabilities. The BM-HHO system optimizes feature dimensions while X-SPCNN provides quick and precise

classification, and FES uses network behavior patterns to adapt detection methods. The unified system demonstrates 99.2% detection accuracy and 1.5% false positive rate, and 99.6% recall, surpassing benchmark methods, including SVM and ML-only detectors. The unique system design provides high scalability, real-time performance and robustness against stealthy or mimicry attacks, which makes it an effective deployable solution for decentralized and constrained MANET environments.

Figures 6 and 7 show the confusion matrices of well-known machine learning models and implemented ML models. Figure 8 demonstrates RoC curves of eminent ML Models, which are lagging implemented hybrid models.

**Table 3. Detection results comparison**

| Detection Method | Accuracy | Precision | Recall (Detection Rate) | False Positive Rate |
|---|---|---|---|---|
| Proposed Hybrid | 99.2% | 98.5% | 99.6% | 1.5% |
| ML-only | 97.8% | 96.4% | 98.1% | 3.1% |
| Fuzzy-only | 90.7% | 85.3% | 92.0% | 9.8% |
| SVM | 95.4% | 93.0% | 96.8% | 4.5% |
| Deep CNN | 98.6% | 96.9% | 98.9% | 2.9% |
| Multi-layer PCNN | 97.2% | 94.1% | 96.0% | 5.2% |

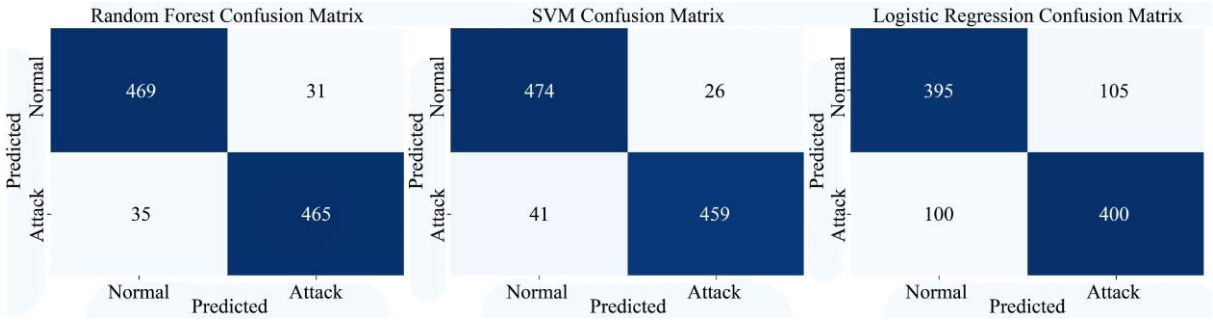


**Fig. 6 Confusion matrix of well-known Ml models**

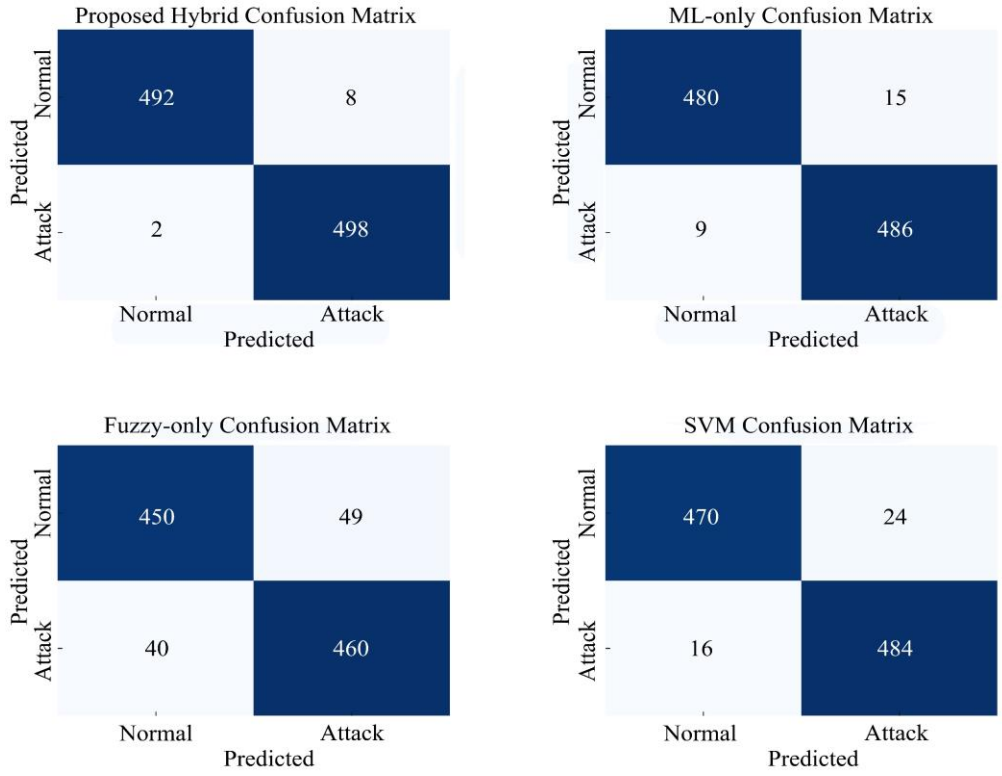


**Fig. 7 Confusion matrix of implemented ML models**

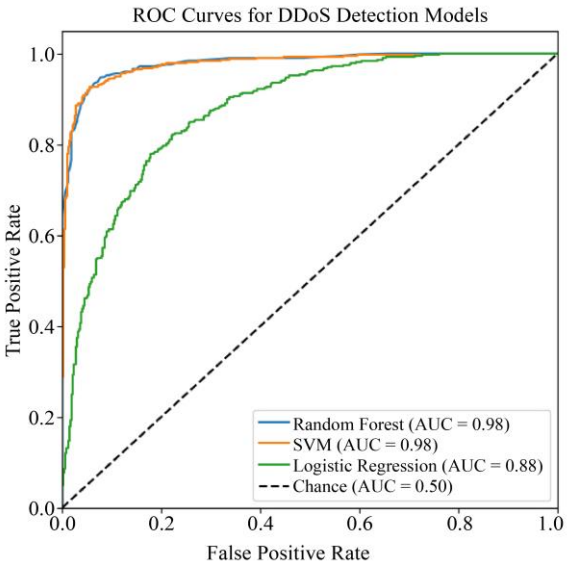


**Fig. 8 RoC curves of eminent ML models**

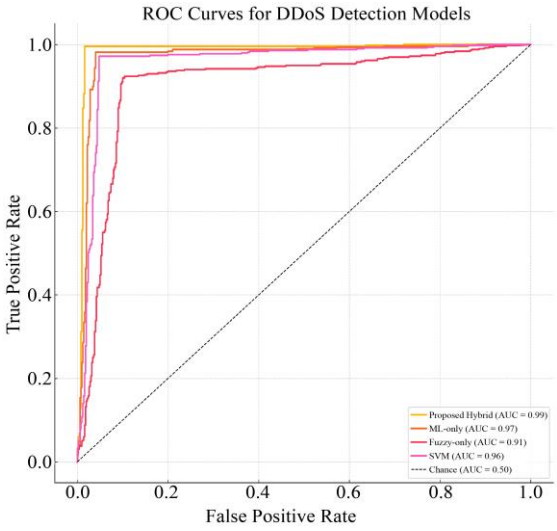


**Fig. 9 RoC curves of implemented ML models**

The proposed hybrid system shows better performance than baseline models, including traditional PCNN and deep CNN architectures. The proposed solution provides higher detection accuracy (99.2%), faster response times, and lower false positives, making it more appropriate for resource-constrained, decentralized MANET environments.

## 5. Conclusion

The research developed a new hybrid defense system to protect MANETs from application-layer DDoS attacks through the integration of fuzzy logic with swarm intelligence and neural network classification methods. The system combines FES for contextual trust evaluation with BM-HHO for effective feature selection and X-SPCNN for lightweight traffic classification. The proposed framework achieves a detection accuracy of 99.2% with minimal false positives, which demonstrates its real-time suitability for resource-limited MANET nodes. The combination of feature dimensionality reduction with adaptive classification enables the system to scale up when network sizes and traffic volumes increase. The fuzzy module is a key component because it identifies threats from benign anomalies through behavioral context analysis of nodes. The architecture and techniques developed here can be adapted to protect decentralized and dynamic networks, including VANETs and IoT-based networks. Future research will concentrate on developing the framework to detect various attack types while adding online learning features to the X-SPCNN for pattern evolution and improving inter-node collaboration through consensus-based alert validation and trust dissemination. The research will investigate ways to enhance ML decision Explainability through the integration of interpretability tools such as SHAP or rule extraction from the classifier. The system will be tested on real MANET testbeds using Raspberry Pi-based nodes to evaluate actual performance while addressing deployment obstacles. The proposed hybrid system provides a scalable, intelligent, resilient solution to protect MANETs from advanced DDoS threats.

## References

[1] N. Singh, A. Dumka, and R. Sharma, "A Novel Technique to Defend DDOS Attack in Manet," *Journal of Computer Engineering & Information Technology*, vol. 7, no. 5, pp. 1-4, 2018. [Google Scholar] [Publisher Link]

[2] Deepa, Kanwalvir Singh Dhindsa, and Bharat Bhushan, "Clustering-based Technique to Defend DDoS Attacks in Mobile Ad Hoc Networks," *Proceedings of ICETIT 2019: Emerging Trends in Information Technology*, pp. 48-58, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Deepaa, Kanwalvir Singh Dhindsab, and Karanbir Singh, "Entropy-Based DDoS Attack Detection in Cluster-Based Mobile Ad Hoc Networks," *Adhoc & Sensor Wireless Networks*, vol. 49, no. 3-4, pp. 269-288, 2021. [Google Scholar] [Publisher Link]

[4] Munshi Navid Anjum, Chandreyee Chowdhury, and Sarmistha Neogy, "Implementing a Mobile Agent-Based Secure Load Balancing Scheme for MANET," *2019 International Conference on Opto-Electronics and Applied Optics (Optronix)*, Kolkata, India, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] M. Islabudeen, and M.K. Kavitha Devi, "A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks against Security Attacks," *Wireless Personal Communications*, vol. 112, pp. 193-224, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Raj Kumar Batchu, and Hari Seetha, "A Generalized Machine Learning Model for DDoS Attacks Detection using Hybrid Feature Selection and Hyperparameter Tuning," *Computer Networks*, vol. 200, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Hakem Beitollahi, Dyari Mohammed Sharif, and Mahdi Fazeli, "Application Layer DDoS Attack Detection using Cuckoo Search Algorithm-Trained Radial Basis Function," *IEEE Access*, vol. 10, pp. 63844-63854, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] L.V. Legashev et al., "Development of a Model for Detecting Network Traffic Anomalies in Distributed Wireless Ad Hoc Networks," *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, vol. 22, no. 4, pp. 699-707, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sarah Ahmed, and S. M. Nirkhi, "A Fuzzy Rule Based Forensic Analysis of DDoS Attack in MANET," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 6, pp. 1-6, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[10] Sunil Kumar, and Kamlesh Dutta, "Trust based Intrusion Detection Technique to Detect Selfish Nodes in Mobile Ad Hoc Networks," *Wireless Personal Communications*, vol. 101, pp. 2029-2052, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] Wenjuan Li, Weizhi Meng, and Lam For Kwok, "Surveying Trust-Based Collaborative Intrusion Detection: State-of-the-Art, Challenges and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 280-305, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Kazeem B. Adedeji, Adnan M. Abu-Mahfouz, and Anish M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, pp. 1-57, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ranadeep Reddy Palle, and Haritha Yennapusa, "A Hybrid Deep Learning Techniques for DDoS Attacks in Cloud Computing Used in Defense Application," *TIJER - International Research Journal*, vol. 8, no. 1, pp. 44-61, 2021. [Google Scholar] [Publisher Link]

[14] Chour Singh Rajpoot, Amit Kumar Bairwa, and Vijay Kumar Sharma, "Mitigating the Impact of DDoS Attack on Upsurge Network Performance in MANET," *Proceedings of International Conference on Communication and Computational Technologies*, Singapore, pp. 153-164, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sengathir Janakiraman, M. Deva Priya, and A. Christy Jebamalar, "Integrated Context-Based Mitigation Framework for Enforcing Security Against Rendezvous Point Attack in MANETs," *Wireless Personal Communications*, vol. 119, pp. 2147-2163, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Reem Talal Abdulhameed Al-Dulaimi, and Ayça Kurnaz Türkben, "A Hybrid Tree Convolutional Neural Network with Leader-Guided Spiral Optimization for Detecting Symmetric Patterns in Network Anomalies," *Symmetry*, vol. 17, no. 3, pp. 1-37, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Yong Zhang et al., "PCCN: Parallel Cross Convolutional Neural Network for Abnormal Network Traffic Flows Detection in Multi-Class Imbalanced Network Traffic Flows," *IEEE Access*, vol. 7, pp. 119904-119916, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Sumathi Sokkalingam, and Rajesh Ramakrishnan, "An Intelligent Intrusion Detection System for Distributed Denial of Service Attacks: A Support Vector Machine with Hybrid Optimization Algorithm-Based Approach," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 27, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]