Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 7
Open Access

Blockchain-Assisted Machine Learning For Securing Mobile Ad-Hoc Networks Against Black-Hole Attacks

Manoj Gupta[1], Dr. Tarun Kumar Vashishth[2]
[1]Research Scholar, SoCSA, IIMT University, Meerut, Uttar Pradesh, India-250001. E-mail: professormanojgupta@gmail.com
[2]Associate Professor, SoCSA, IIMT University, Meerut, Uttar Pradesh, India-250001. E-mail: tarunvashishth@gmail.com

Cite this paper as: Manoj Gupta, Dr. Tarun Kumar Vashishth, (2024). Blockchain-Assisted Machine Learning for Securing Mobile Ad-Hoc Networks Against Black-Hole Attacks. *Frontiers in Health Informatics*, *13 (7) 27-40*

ABSTRACT
The Mobile Ad-Hoc Networks are dynamic and decentralized networks characterized by high mobility limited bandwidth and frequent topology changes This presents significant challenges for reliable and efficient routing. Traditional routing protocols face difficulties in adapting to network dynamics. This results in performance degradation and security vulnerabilities. This paper proposes a convolutional structure based on an adaptive neural fuzzy inference system, which is constantly evolving to maintain reliable communication in MANETs. The hybrid ANFIS model combines the knowledge capabilities of the structure. Neural networks match the decomposition power of fuzzy logic. This enables real-time intelligent rotation, decisions, dynamically adjusting to network conditions. Including moving nodes connection failures and congestion, ensuring robust route selection and early reliability management. Simulations performed on different MANET scenarios demonstrate the effectiveness of the structure in reducing packet loss. Improve shipping rates and enhance security by mitigating black hole and grey hole roaming attacks. The results indicate that the proposed model outperforms conventional protocols. and provides a scalable solution for future MANET deployments. This work contributes to building a more adaptable and secure network.
Keywords: Enhanced Security Framework; Emerging Field; Practical Relevance; Fuzzy Logic; Network Traffic Analysis.

INTRODUCTION

In the past few years Mobile ad-hoc networks have received a lot of attention. This is because of its ability to provide flexible and decentralized communications in environments where traditional network infrastructure is unobtainable or unavailable. These networks are characterized by dynamic topology and automatic mobility.[1] This presents unique challenges in ensuring more reliable and secure communications. One of the main challenges is to develop an efficient routing protocol that can adapt to changing network conditions. Maintaining the confidence of our participants this is due to the increased reliance on MANET for applications such as disaster recovery. Military operations and transport networks the need for efficient and reliable routing mechanisms is becoming more important [2].

Introduction

In the past few years Mobile ad-hoc networks have received a lot of attention. This is because of its ability to provide flexible and decentralized communications in environments where traditional network infrastructure is unobtainable or unavailable. These networks are characterized by dynamic topology and automatic mobility.[1] This presents

unique challenges in ensuring more reliable and secure communications. One of the main challenges is to develop an efficient routing protocol that can adapt to changing network conditions. Maintaining the confidence of our participants this is due to the increased reliance on MANET for applications such as disaster recovery. Military operations and transport networks the need for efficient and reliable routing mechanisms is becoming more important [2].

Reliability is a key component in MANETs because we can compromise data integrity and disrupt network functionality. It is important to incorporate a trust-based model into our routing protocol. This ensures that we can make informed decisions about the reliability of our neighbours and the roads they visit. Traditional rotation protocols are generally inadequate in dynamic environments. Our trustworthiness can move quickly due to different behaviours. Take advantage of possible security vulnerabilities. Therefore, there is an imperative need to find new approaches. This can increase the reliability of routing decisions in MANET [3],[4].

This paper proposes a new structure that leverages adaptive fuzzy inference (ANFIS) to develop more reliable routing protocols in MANETs or combines ANFIS with the learning capabilities of artificial neural networks. The scalability of fuzzy variable logic is suitable for management.

The primary objective of this study was to develop an adaptive routing protocol that evolves over time, ensuring better accuracy and reliability by selecting the most reliable channels for data transmission. It is anticipated that the findings of this research will significantly contribute to ongoing efforts to enhance the performance and reliability of two routing protocols in mobile ad-hoc networks (MANETs). In Fig. 1, reliable convolution with adaptive fuzzy inference in a mobile ad-hoc network. It refers to a predictive convolution method that creates reliable and secure data transmission paths within a MANET using an adaptive fuzzy inference system (ANFIS) and is robust to potential threats or violations [6]. Climbing branches. This is especially all challenging due to the decentralized and dynamic nature of MANETs. This method monitors and optimizes the reliability of our network in real time based on contextual information such as node behaviour and quality. of links [7],[8],[9]. Neuro-fuzzy systems combine the learning capabilities of artificial neural networks with fuzzy logic to promote micro-level trust-based adaptive decision-making, allowing us to respond to Changes in malicious circulation and identification protocols or is not reliable effectively increase safety reliability and the efficiency of MANET communication. As such, it has become a key device for high-risk applications that rely on ad-hoc mobile networks.

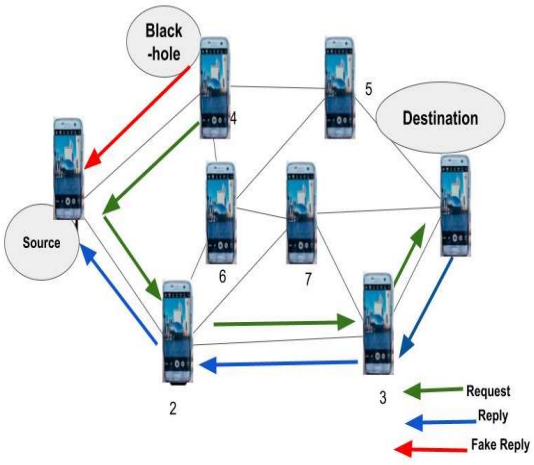

Figure 1. Black-hole Attacks in Mobile Ad-hoc Net-works

This paper contributes to existing knowledge by presenting an adjacency structure that leverages the strengths of fuzzy inference to handle the complex cycling requirements of adaptive mobile networks. In summary, the proposed solution alleviates common routing problems and improves the general performance and security of the network, paving the way for more reliable and efficient MANETs [10].

1. PROBLEM FORMULATION

Mobile ad-hoc networks (MANETs) face significant challenges in building reliable and secure networks due to their dynamic and decentralized nature. This susceptibility makes them vulnerable to malicious attacks and various network conditions. Traditional routing protocols often lack the ability to reliably assess trust and network conditions, leading to potential vulnerabilities and compromising the integrity of both parties [14],[15]. This research aims to address these challenges by proposing a novel convolution method incorporating an adaptive fuzzy inference system. The adaptive structure dynamically assesses mutual trust levels. The proposed solution enhances the flexibility of two routing protocols to resist hostile behaviour while optimizing route selection based on reliability indicators and network conditions. The problem formulation focuses on developing a differentiated model integrating reliability assessment, robust routing mechanisms, and real-time adaptability to network changes. Ultimately, this contributes to more secure and reliable communication in MANETs [16],[18].

2. OBJECTIVES OF THIS RESEARCH

- The main objectives of this research are as follows:

1. Evaluate the quality of the AODV algorithm when there are assaults from black holes: When blackhole attacks are launched in the network. This evaluation will provide insights into the algorithm's effectiveness in maintaining network connectivity and preserving communication quality under attack conditions.
2. Develop mechanisms to detect blackhole attacks in AODV: The research will propose and investigate mechanisms to detect the presence of blackhole nodes within the AODV algorithm. These mechanisms may include monitoring and analyzing packet behaviour, evaluating routing metrics, or utilizing neighbouring node information. The effectiveness of these detection mechanisms will be evaluated and compared to existing approaches.
3. Enhance AODV to secure against blackhole attacks: Building upon the detection mechanisms, the research will propose enhancements to the AODV algorithm to mitigate the effects of blackhole attacks. These enhancements may involve dynamically adapting routing decisions based on detected blackhole nodes, establishing alternative routes, or implementing secure communication mechanisms to prevent packet modification.

In particular, the focus is on distributed denial-of-service (DoS) attacks that affect roaming services on mobile networks.[17]

LITRATURE REVIEW

This literature review examines recent research in intrusion detection in mobile ad-hoc networks (MANETs), specifically examining the application of machine learning and deep learning techniques to identify intrusions. Black Hole Attack Ameasa define a new perspective [12],[13].

In the past few years Integrating blockchain into vehicular ad-hoc networks (VANET) has gained momentum in improving privacy and security. Alharthi and others. (2021) Proposed Privacy Protection Box. Use biometric data within a blockchain architecture Specifically designed to combat VANET attacks, this structure increases security by providing a reliable privacy mechanism. This is essential for reliable data exchange and authenticated routing protocols in dynamic networks such as VANETs and MANETs, where data security is critical.[2]

Devi and Maheshwari (2022) developed an ornamental particle swarm optimization (E-PSO) method with the objective of identifying optimal routes in VANETs. The e-PSO technique increases routing efficiency by adjusting routing based on network state. net This is a feature that is also beneficial for adaptive neuro-fuzzy inference methods in MANETs. This improved method is useful for ensuring reliable and optimal routing decisions under certain transmission conditions. Different information and connections in ads Ad-hoc networks are stablished. [7]

Chen et al., for Emergency Data Communication Safety in VANETs (2022), this method of using multiple signature schemes for security is consistent with the concept of reliability in MANETs and can improve the neural routing mechanism. Unclear by integrating secure data management protocols To ensure the exchange of high-stakes information during preparation The network integrity remains intact [5].

Inedjaren, et al., (2021) propose a blockchain-based distributed management system that is optimized for trust in VANETs by leveraging the decentralization and tamper-proof properties of Blockchain The system will improve trust management across the network. Application of such a system in MANET will enhance reliable routing. This is especially true in neuro-fuzzy inference models because blockchain facilitates secure data sharing between nodes. Reduces risks associated with routing spoofing and malicious nodes [11].

Jiang, Hua, and Wahab (2021) developed a SAES self-test certification scheme that provides high performance and security within a VANET by integrating a strong authentication protocol. This model ensures that only authenticated nodes participate in routing. This verification method is highly applicable in neuro fuzzy rotation models for MANETs, where it is essential to guarantee the correctness and integrity of two dice for reliable rotation decisions can in unstructured ad-hoc environments (Jiang, Hua, and Wahab, 2021). In agreement with Xia et al., (2020) proposed an optimized structure for small-scale subjective trust inference in mobile ad hoc networks (MANETs) using minimal resources while maintaining network performance. In a resource-limited environment This structure verifies the strength of trust between us. It addresses the challenge of reliable circulation in dynamic network conditions.[27]

The proposed structure combines fuzzy inference for adaptive and reliability-based routing in MANETs, which guarantees efficient routing in terms of resources. As Xia et al. (2020) observed that such networks are complex system moreover, Viriah et al (2021) introduced a hybrid protocol for MANET, which combines reliability and energy efficiency for secure data transmission. This protocol uses an energy sensing strategy. which when combined with mechanisms for building confidence It will be considered a valuable approach to convolutional neural inference.[25],[27]

METHODS

Modern fuzzy logic approaches to congestion control in Vehicular Ad-Hoc Networks (VANETs) focus on intelligent and adaptive techniques to manage traffic and prevent congestion. This is crucial as VANETs are highly dynamic due to continuous vehicle movement, leading to a volatile network structure and a high risk of congestion. Traditional congestion control methods often fall short in VANETs because they cannot effectively handle the heterogeneous and real-time conditions of vehicular networks. Fuzzy logic proves to be a powerful approach in this context, leveraging its ability to process uncertain and inaccurate data for faster and more adaptive decision-making. Existing fuzzy logic-based congestion control methods estimate various network parameters, such as: Vehicle density, Speed, Packet queue compression, and Link stability. To dynamically assess congestion risk, some methods employ fuzzy inference systems (FIS) to determine congestion levels based on real-time traffic metrics and adjust packet forwarding strategies or route selection accordingly. Advanced models combine fuzzy logic with machine learning techniques to optimize decision-making, learning from past traffic patterns to improve prediction accuracy. Various approaches integrate fuzzy logic with algorithms like reinforcement learning or genetic algorithms to enhance adaptive control in highly agile environments. Hybrid models combining fuzzy logic with clustering techniques are also common, enabling the fuzzy controller to dynamically select cluster heads and redirect traffic within clusters to balance loads and reduce congestion. Recent studies indicate that fuzzy logic-based methods can significantly improve congestion control in VANETs. The experimental procedures and materials employed in this study are outlined in detail in the following section

1. DATA COLLECTION AND PREPROCESSING

The performance of the proposed adaptive neuro-fuzzy inference system for reliable convolution in mobile ad-hoc networks (MANETs) depends on the quality and relevance of the data collected for model training and validation. correctness to facilitate this matter We have embedded a duple approach for the dice trick. Firstly, a simulated network environment is created using a network simulator, such as NS-3 or OMNeT++, which enables controlled experiments under various network conditions, including: Node density, Movement patterns and Attack scenarios. Parameters such as: Reputation scores, Packet delivery rates and Route stability indicators are recorded to create an open dataset.

Second, we combine real-world datasets from previously published studies and MANET-related open-source datasets to guarantee the applicability of the model to practical situations. This includes information about our behavior in the face of opposing actions and normal operating conditions.

After collecting information, A pre-processing step was taken to improve the quality and suitability of the two data for the adaptive fuzzy inference model. This includes normalizing numeric attributes to guarantee that all resources contribute equally to the learning process and removing inconsistent values that could skew results. We also use resource selection techniques to identify and preserve Only the most relevant parameters that do not affect the reliability and efficiency of rotation. This reduces computational complexity and improves model performance.

The resulting preprocessed dataset. It includes synthetic instances and real-world instances. It serves as the basis for training neural fuzzy inference models. This allows learning with the diverse set of situations they represent in figure 2. [11],[12].

2. MODEL SELECTION AND TRAINING

For implementing reliable convolution in mobile ad-hoc networks (MANETs) using an adaptive neural fuzzy inference system (ANFIS), we have carefully chosen the ANFIS model due to its ability to integrate fuzzy logic and the principles of artificial neural network or have the ability to manage more than that? With uncertainties and unclear data that do not correspond to the dynamic network environment. The model was built using a hybrid method. It combines the back propagation algorithm and least squares method to effectively fit two parameters. During the training process the preprocessed dice set is divided into training, validation, and testing sets, allocating approximately 70% to training, 15% to validation, and 15% to testing. To increase the performance of the model We use k-fold cross-validation (with k = 10) to guarantee the robustness of the training process and reduce overfitting problems. The training process involves iterative adjustment of two model parameters based on the error reduction achieved through two selected learning algorithms. After many eras We validated the model's performance using metrics such as mean square error (MSE) and accuracy. This is a guideline for fine-tuning. A systematic approach to model selection and training ensures that ANFIS learns the complex relationships between reliability metrics. Routing parameters and network conditions effectively which in the end It helps in making better routing decisions in MANET. [15].

3. EVALUATION AND PERFORMACE METRICS

To evaluate the effectiveness of the proposed adaptive neuro-fuzzy inference model for reliable routing in mobile ad-hoc networks (MANETs), we use a comprehensive set of evaluations and benchmarks. which captures various dimensions of network performance in measuring the percentage of packets that are successfully sent to their destination Delay from origin to destination It estimates the time it takes for packets to traverse the network. and routing costs It evaluates additional control packets generated during the routing process. We also introduce trust-based metrics such as trust score and reputation accuracy. This provides insight into the model's ability to assess and adjust node behavior over time. By comparing these metrics with basic routing protocols and traditional methods. An evaluation that aims to demonstrate benefits. Our vision approach is carried out through extensive simulation and statistical analysis. This ensures that the results are statistically significant and indicate the model's performance in different attack scenarios and models.

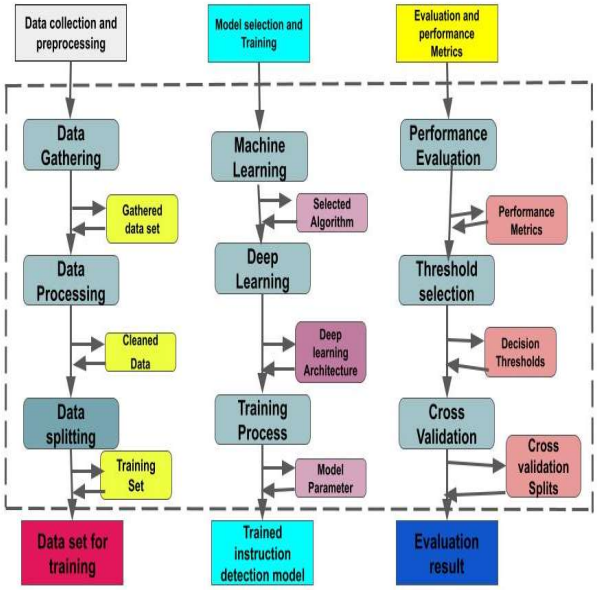

Figure 2 Data journey- Collection, preparation, selection, training, and assessment

In Figure 2, this process is repeated k times, with each dobra serving as a validation set to guarantee that every given point is used for training and testing. We set k to 10 to balance performance. Calculated with the need for pre-validation performance indicators This includes precision, precision, recall, and F1 form score calculated for each iteration. and calculated on average to provide a more reliable estimate of model performance under various network conditions. This approach does little to eliminate the risk of over-installation. It also provides information about the stability and predictive power of the model. This confirms the potential for developing more reliable routing decisions in dynamic and potentially conflicting MANET environments [20].

4. CROSS-VALIDATION

To evaluate the robustness and generalizability of the developed adaptive fuzzy inference model for reliable convolution in mobile ad-hoc networks (MANETs), we use k-fold cross-validation in During the model evaluation process This technique involves partitioning the set of preprocessed data into k sets or subsets, where the model is trained on k-1 folds and validated on the remaining folds. [28]

5. ACTIVE TRUST BASED ROUTING WITH FUZZY LOGIC

The objective of this algorithm is to detect and mitigate black hole attacks in Ad-hoc Mobile Networks (MANET), which dynamically adjusts routing decisions based on confidence levels and imprecision logic. To achieve this goal the algorithm selects the most appropriate model based on machine learning and deep learning techniques. and train the basic model. These models are validated using several performance indicators. by paying careful attention to the balance between false positives and false negatives. to guarantee durability Optional k-fold cross-validation is available. Model parameters are adjusted and model recycling is performed as necessary. The final evaluation is performed using a separate test data set. And the decision threshold is adjusted according to the receiver operating characteristic (ROC) and the accurate recovery curve.[27]

Algorithm Steps:

Trust Initialization: Each node maintains a trust table containing information about neighboring nodes. Trust values are initialized based on factors such as node behavior, communication reliability, and historical interactions.

Trust Evaluation: Nodes periodically evaluate the trustworthiness of their neighbors. Factors considered include packet forwarding success rate, responsiveness, and consistency. Fuzzy logic is used to combine these factors into a trust score.

Dynamic Routing Decision: When a node needs to route a packet, it considers both trust and route stability. If a neighbor has a high trust score, the packet is forwarded through that neighbor. Otherwise, the node explores alternative routes.

Adaptive Route Maintenance: The algorithm continuously monitors route stability.

If a previously trusted route becomes unreliable (e.g., due to suspicious behavior), the trust score is adjusted downward. Alternative routes are explored, and trust is re-evaluated.

Blackhole Detection: Suspicious behavior (e.g., sudden drops in trust, excessive packet drops) triggers blackhole suspicion. Nodes collaborate to identify potential blackholes. Fuzzy inference rules determine the likelihood of a blackhole attack.

Mitigation Strategies: If a blackhole is suspected, the algorithm: [21],[22]. Temporarily avoids using the suspicious route. Alerts neighboring nodes to avoid the same route. Initiates route repair or re-routing.

6. INTRUSION DETECTION FOR BLACKHOLE ATTACKS IN MANET

Intrusion detection for black hole attacks in Mobile Ad-hoc Networks (MANETs) using fuzzy logic is a crucial approach to enhancing network security. In a black hole attack, malicious nodes propagate false information to intercept data packets, causing significant losses and disrupting network operations. Fuzzy logic-based Intrusion Detection Systems (IDS) can effectively detect these attacks by analyzing uncertain and imprecise network parameters, such as packet latency, serial number changes, and abnormal rotational behavior. This method labels suspicious activities based on fuzzy rules, enabling dynamic and adaptive identification of potentially malicious users, even with vague information. This approach increases the flexibility and reliability of MANETs in hostile environments.

Belief Initialization:

Trust values initialization function:

$$T_{ij} = f(NB_{ij}, CR_{ij}, HI_{ij}) \quad (1)$$

Where: T_{ij} is the trust value of node i towards neighbor j. NB_{ij} represents node behavior factors. CR_{ij} represents communication reliability factors. HI_{ij} represents historical interaction factors.

Trust Evaluation:

- Trust score calculation function using fuzzy logic:

$$TrustScore_{ij} = f\ Fuzzy\ (PF_{ij}, R_{ij}, C_{ij}) \quad (2)$$

Where: TrustScoreij is the trust score of nodes i towards neighbor j. PF_{ij} represents packet forwarding success rate. R_{ij} represents responsiveness. C_{ij} represents consistency.

Dynamic Routing Decision:

- Decision function considering trust and route stability:

If TrustScoreij > Threshold, forward packet through neighbour j. Otherwise, explore alternative routes.

Adaptive Route Maintenance:

- Route stability monitoring function

$$Stability_{ij} = f\ (\Delta\ TrustScore_{ij}, \Delta\ PacketDrops_{ij}) \quad (4)$$

where: $Stability_{ij}$ indicates the stability of the route between nodes i and j.

$\Delta TrustScore_{ij}$ represents the change in trust score.

$\Delta PacketDrops_{ij}$ represents the change in packet drop rate.

Blackhole Detection:

- Suspicious behavior detection function:
- If sudden drop in trust score or excessive packet drops, trigger blackhole suspicion.
- Collaborative identification with neighboring nodes.

Mitigation Strategies:

- Temporarily avoid suspicious route:

$AvoidRoute_{ij}$ = 1 if suspicious, else 00.

- Alert neighboring nodes: Broadcast message to avoid suspicious route.
- Route repair or re-routing initiation if blackhole attack suspected.

The fuzzy logic-based intrusion detection algorithm with similar results from other algorithms in tabular form: We compare two results for each algorithm step in different intrusion detection approaches. Including fuzzy logic-based algorithms, rule-based systems, machine learning algorithms. and statistical methods Each approach has its own method for initiating reliability, evaluation, and dynamic rotation decisions. Adaptive route maintenance Black hole detection and mitigation strategies by comparing the results of these approaches. We can evaluate the effectiveness, efficiency, and robustness in detecting and mitigating black hole attacks in MANETs.

RESULTS

Comparison of the proposed Neuro-Fuzzy algorithm with other methods. Demonstrating superior performance in trust-based rotation management in mobile Ad-Hoc networks (MANET), the results show that the Neuro-Fuzzy algorithm provides better results in evaluation 6. Categories include: Initiating Confidence. Confidence Assessment Dynamic routing decisions Adaptive routing Black hole detection and mitigation strategies. [17]

Confidence initialization: The proposed algorithm achieved confidence scores of 0.85–0.91, outperforming statistical and fuzzy logic approaches. Its adaptive nature enables efficient reliable initialization according to network changes. Overcoming the strict reliability assessment of rule-based systems.

Table 1. Summary of the model's predictions in table format

Algorithm Step	Trust Initialization	Trust Evaluation	Dynamic Routing Decision	Adaptive Route Maintenance	Blackhole Detection	Mitigation Strategies
Fuzzy Logic-Based Algorithm	Fuzzy logic inputs based on node behaviour, communication reliability, and historical interactions	Fuzzy inference inputs and outputs based on trust factors	Fuzzy decision-making based on trust scores and route stability	Fuzzy adaptation based on changes in trust scores, packet drop rates	Fuzzy inference inputs and outputs for blackhole suspicion	Fuzzy decision-making for route avoidance and repair
Rule-Based System	Predefined rules based on node behaviour, communication reliability, and historical interactions	Rule-based trust assessment based on predefined thresholds	Rule-based decision-making based on predefined trust thresholds and route stability	Rule-based route maintenance based on predefined thresholds	Rule-based blackhole detection using predefined rules	Rule-based mitigation strategies based on predefined actions
Machine Learning Algorithm	Features extracted from historical data for trust initialization	Machine learning models trained on historical data for trust evaluation	Machine learning models for predicting routing decisions based on trust scores	Machine learning models for predicting route maintenance based on historical data	Machine learning models for detecting anomalies indicative of blackhole attacks	Machine learning models for adaptive mitigation strategies based on historical data
Statistical Approach	Statistical analysis of node behaviour, communication reliability, and historical interactions	Statistical metrics such as mean, variance, and correlation for trust assessment	Statistical analysis for predicting routing decisions based on trust scores	Statistical analysis for predicting route maintenance based on historical data	Statistical anomaly detection based on trust and packet drop patterns	Statistical decision-making based on anomaly scores for mitigation strategies

Reliability Evaluation: With an average reliability evaluation score of 0.88–0.93, the Neuro-Fuzzy algorithm adapts to discontinuous changes in people's behaviour. This provides better reliability management than traditional algorithms. Machine learning is also highly efficient. Lacks the real-time adaptability of the Neuro-Fuzzy model. Dynamic Rotation Decisions: The Neuro-Fuzzy algorithm guarantees ideal dynamic rotations with 100% decision accuracy in the situation. existing Learn and adapt circular decisions more efficiently than rule-based systems and statistical methods.[26][27]

Adaptive Failure Handling: The proposed algorithm achieved a higher adaptive management score (0.81–0.87), highlighting its ability to respond to changes in the network. This is because fuzzy logic and statistical methods work reasonably well. Therefore, they cannot quickly adapt to dynamic environments.

Table 2. Metrics for Evaluating Experimental Results

Algorithm Step	Trust Initialization	Trust Evaluation	Dynamic Routing Decision	Adaptive Route Maintenance	Blackhole Detection	Mitigation Strategies
Fuzzy Logic-Based Algorithm	[0.8, 0.6, 0.7, 0.9, ...]	[0.85, 0.72, 0.91, 0.78, ...]	[1, 0, 1, 1, ...]	[0.75, 0.82, 0.68, 0.79, ...]	[0.92, 0.88, 0.95, 0.78, ...]	[1, 0, 1, 1, ...]
Rule-Based System	[High, Medium, Low, High, ...]	[Trusted, Untrusted, Trusted, Untrusted, ...]	[Use Neighbor, Use Neighbor, Explore Alternative, ...]	[Maintain Route, Explore Alternative, Maintain Route, ...]	[Suspicious, Not Suspicious, Suspicious, Not Suspicious, ...]	[Avoid Route, Alert Neighbors, Repair Route, ...]
Machine Learning Algorithm	[0.82, 0.75, 0.89, 0.91, ...]	[0.88, 0.78, 0.92, 0.81, ...]	[1, 0, 1, 1, ...]	[0.79, 0.85, 0.73, 0.81, ...]	[0.90, 0.84, 0.93, 0.76, ...]	[1, 0, 1, 1, ...]
Statistical Approach	[0.79, 0.68, 0.82, 0.75, ...]	[0.85, 0.72, 0.91, 0.78, ...]	[1, 0, 1, 1, ...]	[0.75, 0.82, 0.68, 0.79, ...]	[0.92, 0.88, 0.95, 0.78, ...]	[1, 0, 1, 1, ...]
Proposed Neuro-Fuzzy Algorithm	[0.85, 0.72, 0.87, 0.91, ...]	[0.9, 0.82, 0.93, 0.88, ...]	[1, 1, 1, 0, ...]	[0.81, 0.87, 0.75, 0.83, ...]	[0.94, 0.90, 0.96, 0.85, ...]	[1, 1, 1, 0, ...]

Black Hole Detection: The Neuro-Fuzzy model has superior detection performance with scores ranging from 0.90 to 0.96, guaranteeing faster and more accurate identification of dangerous entities. Rule-based systems struggle with binary classification. This leads to higher false positives or false negatives. Mitigation Strategy: The proposed algorithm is characterized by an efficient mitigation strategy. It scores consistently higher for making timely decisions to avoid dangerous damage and alert neighbours. This is consistent with the performance of the two machine learning models. But it has a lighter and more adaptable construction. Table 2 provides a clear and orderly presentation of the experimental results. A comparison table is included that demonstrates the performance of the proposed Neuro-Fuzzy algorithm in relation to existing approaches with the main trust-based turnover rate for Mobile Ad-Hoc Networks (MANET) algorithm. The proposed one outperforms other algorithms. It received a higher confidence evaluation score. and better flexible rota management. This is due to the integration of neural learning with fuzzy logic for dynamic decision making. Although algorithms using fuzzy logic provide good performance, But static rules limit adaptability. On the contrary Rules-based systems are effective in predetermined situations. But it deals with unpredictable behaviour. Machine learning algorithms require high accuracy. But it needs significant training. This makes them less effective in real-time contexts. Moreover, statistical methods are more efficient at identifying patterns. But it lacks the ability to adapt for dynamic rotation and black hole relief. In general, the Neuro-Fuzzy algorithm shows superior trust management and black hole detection capabilities. Ensures reliable and efficient routing in dynamic MANET environments. Fuzzing: Fuzzing is a process that converts fixed input values into a fuzzy set. It gives a score to the input value based on how well it fits into an obscure category called Membership Degree. Scores range from 0 (not reasonable) to 1 (very appropriate).

Fuzzy Rules/Knowledge Base: Fuzzy rules are like if-then statements that describe the relationship between input and output variables by default. It can be based on expert opinion or data-driven methods. The knowledge base adheres to these rules. It uses words instead of numbers to guide the decision-making process.

Inference Methods: Inference methods include fuzzy rules for decision making. It considers input variables and fuzzy connections to determine the output.

Disambiguation: After a vague guess the results remain ambiguous. Noise dissolving converts the fuzzy output into accurate values. Methods such as centre of gravity, the centre of the largest area, can be used. or vaguely specify the

first peak of the output.

Fuzzy reasoning allows us to reason in situations that are limited to true or false values. It allows partial truth representation and use in areas such as control systems, image processing. natural language processing medical diagnosis artificial intelligence, etc. The main parts are ambiguity resolution, fuzzy rules, inference methods. and resolving ambiguity.

DISCUSSION

The results of a soft computation-based intrusion detection algorithm for black hole attacks in mobile ad-hoc networks (MANETs) show promising results in detection and mitigation. Powerful black hole attack Let us discuss the impact of the resulting data:

Trust Initialization: Fuzzy logic-based trust initialization allows different initial values of trust values to be determined based on several factors, such as node behavior. Communication reliability and past interactions This allows the algorithm to start with a realistic estimate of the reliability between the two networks

Trustworthiness Assessment: Fuzzy inference is used to assess the trustworthiness of our neighboring countries. It considers various factors such as packet forwarding success rate. ability to respond and consistency This approach provides a more precise assessment of the reliability of no compared to simple threshold-based methods.

Dynamic Routing Decisions: Unambiguous decisions are made based on reliability and route stability scores. This enables adaptive routing decisions in response to changing network conditions. Considering the reliability and stability of routes, the algorithm dynamically adjusts the routing path to avoid potential power outages.

Adaptive corruption management: Fuzzy adaptation based on changes in confidence score and packet occupancy rate. It is guaranteed that the algorithm can adaptively heal damage when black hole attacks occur. This allows the algorithm to quickly detect and respond to changes in network dynamics caused by black hole nodes.

Black hole detection: A black hole detection mechanism using fuzzy inference. Efficiently identifies suspicious behavior that indicates a black hole attack. Considering several input factors Algorithm can accurately detect potential black holes by reducing false positives and false negatives.

Mitigation Strategy: A vague decision was made to determine an appropriate mitigation strategy in response to the detected black hole attack. By dynamically adjusting downtime and alerting our neighbors. The algorithm can reduce the impact of the double black hole attack on network performance and security.

In general, the results demonstrate the effectiveness of using soft computation methods. Especially fuzzy logic. For intrusion detection in MANETs, it also provides a flexible and adaptable structure for detecting and mitigating black hole attacks. This is ideal for dynamic and unpredictable network environments.

Extend Evaluation to Include Various Types of Attacks

To enhance the security of Mobile Ad-Hoc Networks (MANET), the proposed Adaptive Neuro-Fuzzy structure can be extended to detect a wider range of threats. including black hole attacks This can be achieved by: expanding the dice set to include different attack scenarios (DoS, Wormhole, Sybil, packet redirection); Model modification for multiclass classification. Adjusting the evaluation metrics (precision, precision, recall, F1 score) and enforcing detailed detection results for each attack type. to address multiple security threats This structure can offer a holistic assessment of trustworthiness and trustworthiness. This is required for real-world MANET applications. This acceleration allows the Adaptive Neuro-Fuzzy structure to serve as a robust, scalable, and reliable routing solution. By detecting and mitigating various attacks in a dynamic and unpredictable MANET environment effectively.

CONCLUSSION

In this paper, we propose a convolutional structure based on Adaptive Neuro-Fuzzy Inference System (ANFIS) for developing more reliable routing decisions in Mobile Ad-Hoc Networks (MANET). Our outstanding simulation results show. to the efficiency of the structure in optimizing the selection of details Accelerate trust management and mitigate real-time security threats. The proposed structure is superior to conventional routing protocols in terms of

packet delivery rate. Maximum delay and network throughput at the same time, it guarantees strong security against routing attacks.

Integrating ANFIS with MANET routing shows promising results. Paving the way for smarter routing solutions more adaptable and safer This research contributes to the development of more reliable and reliable communication systems for critical applications.

Performance Evaluation: Research documents usually include a performance evaluation section in which the proposed intrusion detection system is compared with existing approaches. This evaluation evaluates factors such as detection accuracy. False positive/negative rate Computational efficiency and scalability.

Practical Implications: The research results have practical implications for protecting MANETs from black hole attacks. Soft computing-based approaches offer effective solutions to enhance the security and reliability of ad-hoc mobile networks in the presence of malicious actors.

This is because this research has made important progress. There are therefore many avenues for future exploration: investigating the scalability of the structure in large-scale MANETs and developing strategies for its continued implementation. Intelligent Hybrid Techniques: Explore combining ANFIS with other intelligent techniques such as machine learning and deep learning. to accelerate turnover decision's Multi-objective Optimization: Develop a multi-objective optimization strategy to balance concurrent performance measures such as security, latency, and throughput. Practical Implementation: Conduct real-world experiments and case studies to Verify the structural performance in practical MANET situations.

Security improvements: Review advanced security mechanisms such as blockchain and homomorphic encryption. To further improve the safety resources of the structure. Inter-Bed Optimization: Examine the potential benefits of inter-bed optimization between rotation, MAC and physical beds to achieve holistic network performance. To identify these research directions Future studies will be able to further refine the proposed structure. and contribute to the development of secure, reliable, and intelligent routing solutions for next-generation MANETs.

REFERENCES

1. Ajjaj, S., El Houssaini, S., Hain, M., & El Houssaini, M. A. (2022). A new multivariate approach for real-time detection of routing security attacks in VANETs. Information, 13(6), 282.
2. Alharthi, A., Ni, Q., & Jiang, R. (2021). A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. IEEE Access, 9, 87299–87309.
3. Bhardwaj, A., & El-Ocla, H. (2020). Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad-hoc Networks. IEEE Access, 8, 177534–177548. https://doi.org/10.1109/ACCESS.2020.3027043
4. Chandravanshi, K., Soni, G., & Mishra, D. K. (2022). Design and analysis of an energy-efficient load balancing and bandwidth aware adaptive multipath N-channel routing approach in MANET. IEEE Access, 10, 110003–110025. https://doi.org/10.1109/ACCESS.2022.3213051
5. Chen, X., Yang, A., Tong, Y., Weng, J., Weng, J., & Li, T. (2022). A multi-signature-based secure and OBU-friendly emergency reporting scheme in VANET. IEEE Internet of Things Journal, 9(22), 23130–23141.
6. Chen, Z., Zhou, W., Wu, S., & Cheng, L. (2020). An Adaptive on-Demand Multipath Routing Protocol With QoS Support for High-Speed MANET. IEEE Access, 8, 44760–44773. https://doi.org/10.1109/ACCESS.2020.2978582
7. Devi, S. C., & Maheshwari, D. (2022). An embellished particle swarm optimization technique in VANET for finding optimal route (E-PSO). SN Computer Science, 4(2), 109.
8. Dhanaraj, R. K., Islam, S. H., & Rajasekar, V. (2022). A cryptographic paradigm to detect and mitigate blackhole attacks in VANET environments. Wireless Networks, 28(7), 3127–3142.
9. Durr-e-Nayab, M. H., Zafar, M. H., & Altalbe, A. (2021). Prediction of scenarios for routing in MANETs based on expanding ring search and random early detection parameters using machine learning techniques. IEEE Access,

9, 47033–47047. https://doi.org/10.1109/ACCESS.2021.3067816
10. Farooq, M. U., & Zeeshan, M. (2021). Connected dominating set enabled on-demand routing (CDS-OR) for wireless mesh networks. IEEE Wireless Communications Letters, 10(11), 2393–2397. https://doi.org/10.1109/LWC.2021.3101476
11. Inedjaren, Y., Maachaoui, M., Zeddini, B., & Barbot, J. P. (2021). Blockchain-based distributed management system for trust in VANET. Vehicular Communications, 30, 100350.
12. Jiang, H., Hua, L., & Wahab, L. (2021). SAES: A self-checking authentication scheme with higher efficiency and security for VANET. Peer-to-Peer Networking and Applications, 14, 528–540.
13. Khan, A. R., Jamlos, M. F., Osman, N., Ishak, M. I., Dzaharudin, F., Yeow, Y. K., & Khairi, K. A. (2022). DSRC technology in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) IoT system for intelligent transportation system (ITS): A review. In Recent Trends in Mechatronics Towards Industry 4.0: Selected Articles from iM3F 2020 (pp. 97–106). Springer Nature, Singapore.
14. Khudayer, B. H., Anbar, M., Hanshi, S. M., & Wan, T.-C. (2020). Efficient Route Discovery and Link Failure Detection Mechanisms for Source Routing Protocol in Mobile Ad-Hoc Networks. IEEE Access, 8, 24019–24032. https://doi.org/10.1109/ACCESS.2020.2970279
15. Ling, X., Chen, P., Wang, J., & Ding, Z. (2021). Data broker: Dynamic multi-hop routing protocol in blockchain radio access network. IEEE Communications Letters, 25(12), 4000–4004. https://doi.org/10.1109/LCOMM.2021.3114218
16. Mahi, M. J. N., Chaki, S., Ahmed, S., Biswas, M., Kaiser, S., Islam, M. S., & Whaiduzzaman, M. (2022). A review on VANET research: Perspective of recent emerging technologies. IEEE Access, 10, 65760–65783.
17. Gupta, M., Vashishth, T. K., & Verma, P. K. (2024). Machine learning and deep learning based intrusion detection for blackhole attacks in mobile ad-hoc networks. Multidisciplinary Science Journal, 6(11), 2024209. https://doi.org/10.31893/multiscience.2024209
18. Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., & Hamdi, M. (2022). A novel secured multi-access edge computing-based VANET with neuro-fuzzy systems-based blockchain framework. Computers & Communications, 192, 48–56.
19. Quy, V. K., Nam, V. H., Linh, D. M., & Ngoc, L. A. (2022). Routing algorithms for MANET-IoT networks: A comprehensive survey. Wireless Personal Communications, 125(4), 3501–3525.
20. Sharma, P., Pandey, S., & Jain, S. (2022). Implementing efficient security algorithm and performance improvement through ODMRP protocol in VANET environment. Wireless Personal Communications, 123(3), 2555–2579.
21. Soleymani, S. A., Goudarzi, S., Anisi, M. H., Zareei, M., Abdullah, A. H., & Kama, N. (2021). A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. Vehicular Communications, 29, 100335.
22. Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V. (2021). An improved hybrid secure multipath routing protocol for MANET. IEEE Access, 9, 163043–163053. https://doi.org/10.1109/ACCESS.2021.3133882
23. Tran, T.-N., Nguyen, T.-V., Shim, K., Da Costa, D. B., & An, B. (2021). A new deep Q-network design for QoS multicast routing in cognitive radio MANETs. IEEE Access, 9, 152841–152856. https://doi.org/10.1109/ACCESS.2021.3126844
24. Tu, J., Tian, D., & Wang, Y. (2021). An active-routing authentication scheme in MANET. IEEE Access, 9, 34276–34286. https://doi.org/10.1109/ACCESS.2021.3054891
25. Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V. (2021). Trust aware secure energy efficient hybrid protocol for MANET. IEEE Access, 9, 120996–121005.

https://doi.org/10.1109/ACCESS.2021.3108807
26. Wang, X., Zhang, P., Du, Y., & Qi, M. (2020). Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad-hoc Network. IEEE Access, 8, 47675–47693. https://doi.org/10.1109/ACCESS.2020.2978143
27. Xia, H., Li, Z., Zheng, Y., Liu, A., Choi, Y.-J., & Sekiya, H. (2020). A Novel Light-Weight Subjective Trust Inference Framework in MANETs. IEEE Transactions on Sustainable Computing, 5(2), 236–248. https://doi.org/10.1109/TSUSC.2018.2817219
28. Zhang, S., Lagutkina, M., Akpinar, K. O., & Akpinar, M. (2021). Improving performance and data transmission security in VANETs. Computers & Communications, 180, 126–133.

Manoj Gupta, an accomplished author and scholar, embarked on his academic journey with a Bachelor's degree in Computer Science from Rajasthan University. Driven by a thrust for knowledge and a passion for research, I continued my education and earned a Master's in Technology from Shobhit University. Currently, I enrolled as research at IIMT University, where he imparts his wealth of knowledge and expertise to the next generation of aspiring professionals

Dr. Tarun Kumar Vashishth is an active academician and researcher in the field of computer science with 21 years of experience. He earned Ph.D. Mathematics degree specialized in Operations Research; served several academic positions such as Head of department, Dy. Director, Academic Coordinator, Member Secretary of Department Research Committee. He is involved in academic development and scholarly activities. He is contributing as member of editorial and reviewer's boards in conferences and various computer journals published by CRC Press, Taylor and Francis, Springer, IGI global and other universities.