**Library Progress International**
*Vol.44 No. 3, Jul-Dec 2024: P.1587-1600*

*Print version ISSN 0970 1052*
*Online version ISSN 2320 317X*

*Original Article*

*Available online at www.bpasjournals.com*

# Detection and Mitigation of Black Hole Attack Using Fuzzy Heuristics in Mobile AdHoc Network (MANET)

**Mr. K. Mohanraj[1], Dr. B.Arivazhagan[2]**

[1] Research Scholar1, Assistant Professor2
Department of Computer Science1, 2
VET Institution of Arts & Science (Co- Ed) College, Erode1, 2
kmohamca@gmail.com, arivazhaganpsgcas92@gmail.com

**How to cite this article:** K. Mohanraj, B.Arivazhagan. (2024) Detection and Mitigation of Black Hole Attack Using Fuzzy Heuristics in Mobile AdHoc Network (MANET) , 44(3), 1587-1600

**Abstract**:
Detection of attacks in Ad Hoc Networks for Mobile(MANETs) employs anomaly and intrusion activity detection, intrusion detection systems (IDS), trust-based approaches, collaborative detection, and game-theoretic methods. These techniques monitor network behavior, identify malicious nodes, detect known attack signatures, assess node trustworthiness, promote cooperative detection, and model node interactions. By integrating diverse detection mechanisms, MANETs can effectively identify and mitigate security threats, ensuring reliable communication in dynamic environments. This study aims to develop a system for detecting and preventing black hole attacks in wireless ad hoc networks using fuzzy heuristics. The approach involves defining fuzzy logic rules and heuristics to identify abnormal activity indicative of black hole attacks in network traffic. Algorithms are designed to analyse network parameters such as packet routing, signal strength, and node behaviour using fuzzy logic techniques. Attack detection mechanisms are implemented to dynamically adjust network parameters based on fuzzy inference to mitigate the impact of black hole attacks. Anomaly detection and prevention modules are integrated into existing network protocols to enhance security against black hole attacks. The effectiveness of the fuzzy heuristic-based approach is evaluated through simulation and real-world experimentation, considering factors such as detection accuracy, false positive rate, and network performance.

**Keywords:** Attack detection, black hole, fuzzy heuristics, MANET, routing, mitigation, and network traffic.

## INTRODUCTION

Ad hoc Mobile Network(MANET) is a cooperative base a mobile node network where the network does not require an infrastructure[1]. Generally, MANETs are characterized by the following characteristics: node mobility scalability, high mobility of users, high user density, shared wired-media, no central hub, multi-hop routing, low security and flexibility in the design of the network. However, as we will see, MANET is made up of wireless devices that may exchange information as and when required with the other devices. Since it is an infrastructure network, the nodes are able to roam about and thus the network design changes with the growth of the network. In this network, the nodes are more susceptible to attack as compared to the normal networks because they are not well protected[2].

MANETs also offer another type of competence because of their difficult applications in civil and military applications, environmental and infrastructural projects[3]. They have limited chances to stand up against various kinds of malicious attacks in addition to their effectiveness. Nonetheless, some security attacks arise because of such specific characteristics of MANETs. An example of a MANET in action may be seen in the FIG 1. Mobile ad hoc networks are comparatively prone to security threats as compared to wired networks. In fact, the geometry

of a mobile ad-hoc network is not well-defined and hence cannot be enclosed. In nomadic environment, it is also possible for nodes to come and go as they wish in a wireless network[4].

Once an enemy comes within its radio range, it will be in a position to link up with a node. Mobile nodes of the MANET can be incorporated in the network at any time as well as can be disconnected at any time. A node in the network can be inclined to display malicious behaviour; it may be hard to determine whether a node is malicious or not[5]. A more dangerous attack for the firm than external one[6]. Due to the malware infection these nodes have been referred to as "compromised" nodes. Some of the security problems that may prevail are as follows since MANETs have no form of centralized control facility. Therefore, it becomes almost impossible to note any attacks that may be experienced[7].

It is impossible to monitor traffic from one node to another from a centralised point. If the adviser has changed the attack pattern and also the target of the attack, it becomes easier not to detect an attack[8]. Perhaps the node is broken by an adversary or a network fault. There is no security association and this means that the nodes cannot be categorized as trusted or untrusted. A Mobile Ad hoc Network is solely dependent on battery power to run all the nodes and no other source of power is conceivable. The enemy can generate a lot of traffic to the target. The battery power of the target node may be drained because of handling these packets on a regular basis. Thus, the node will not be in a position to offer network services to the rest of the networks[9].

Sometimes the attackers will request the nodes to perform a meaningless computation, which consumes time and batteries. There are nodes which can be or are possibly malicious. In a situation where all the nodes are running a shared algorithm, a selfish node does not contribute[10]. For instance, a cluster-based intrusion detection system employs a set of nodes in detecting intrusions. In the monitor selection technique, a node is chosen that wants to become a monitor. This way, a malicious act does not becomes the monitor by not participating in it. Due to selfishness the entire system will collapse[11]. The scalability of Mobile Ad hoc Networks is not constant but rather has a tendency of being dynamic. There is no definite forecast of the number of nodes in Future mobile ad-hoc networks. MANET protocols and services must be adopted to this larger scale.

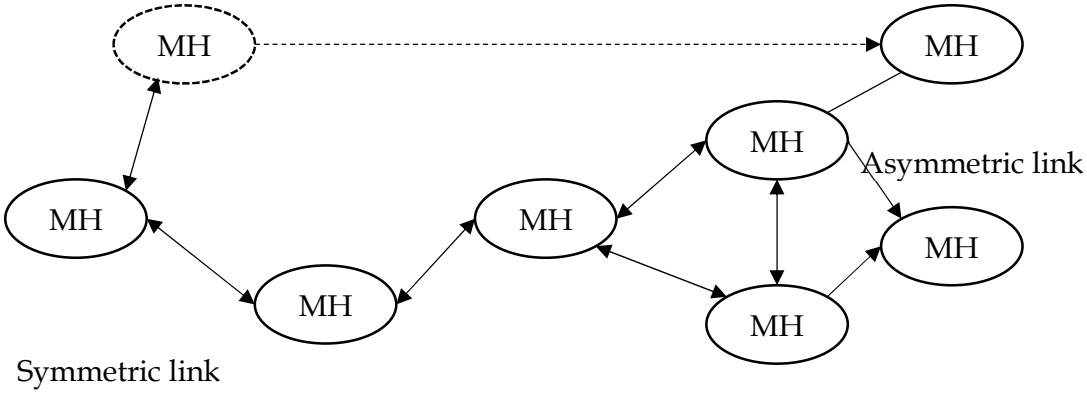


Figure 1.Mobile Ad hoc Network

The nodes that are in the MANET can move in any manner and orientation and they can also switch between the connection with other devices[12]. The nodes are all self-organizing and it is the duty of every node to find other nodes and they are all able to speak to one another, that is, to use language. The nodes do not interconnect without restrictions because the transmission range is very small in most of the nodes[13]. Among the responsibilities of a router, a node is always forced to forward traffic that is not of any use to it. Normally, MANETs may have several hops, and this implies that there are other nodes through which the source node helps to transfer data from the source to the destination node[14].

In MANETs, black hole attack is when an unauthorized node asserts that it has the quickest route to any other node and hence all the packets are routed to it and they are either dropped or not forwarded causing a disruption in the transmission. Prevention of black hole attack using Fuzzy Heuristics involves the formulation of fuzzy rules that detect the irregular behavior in the traffic of the network such as a sharp decrease in forwarding of packets or a large departure from the normal routing tables. Using fuzzy logic techniques on network parameters such as packet routing, signal strength and node behaviour, patterns that represent black hole attacks can be detected. Mitigation is achieved through changing the network parameters using fuzzy inference to avoid the traffic going

through the suspicious nodes and to ensure that the communication is not interrupted. The inclusion of anomaly detection as well as prevention modules in the currently used network protocols enhances security against black hole attacks in MANETs[15].

**Related works**

Black hole attacks are highly damaging to MANETs and WSNs in terms of performance. These problems are solved with the help of trust-based routing (AODV), HPAS-LSTM, DT-AODV, FIDS-HMM, and with the help of Kolmogorov–Smirnov methods improving the detection and prevention approaches. But they are accompanied with certain disadvantages in terms of implementation and computational cost.

| | **Inference** | **Outcome** | **Technique used** | **Significance** | **Drawback** |
|---|---|---|---|---|---|
| [16] | AODV protocol in MANETs is susceptible to black-hole attacks due to its reactive nature. | Introduction of a route development and data retrieval phases of a trust-based routing strategy. | Trust-based routing scheme | Enhances security in data transmission by predicting a safe path. | Complexity in implementation and may require significant overhead in trust management. |
| [17] | MANETs face threats fromattacks known as "black holes," which can significantly impair network performance. | HPAS-LSTM combines honeypots with LSTM for improved detection of black hole attacks. | HPAS-LSTM (Detection using honeypot agents and long-short-term memory) | surpasses current techniques in relation to throughput, packet loss rate, packet delivery ratio, and network delay. | May involve high computational costs due to advanced detection mechanisms. |

| | | | | | |
|---|---|---|---|---|---|
| [18] | Traditional AODV protocols are vulnerable to black hole attacks which affect network performance. | DT-AODV protocol, which uses a dynamic threshold to handle black hole attacks more effectively. | Dynamic Threshold-AODV (DT-AODV) | demonstrates notable increases in the packet delivery rate and throughput compared to traditional methods. | Threshold setting may be complex and impact performance if not optimized correctly. |
| [19] | WSNs are vulnerable to black hole attacks among other security threats. | Fuzzy Logic-based Intrusion Detection System with Hidden Markov Model (FIDS-HMM) for identifying malicious nodes. | FIDS-HMM (Fuzzy Logic and Hidden Markov Model) | Provides effective detection and mitigation of black hole attacks, improving QoS parameters. | May have high computational overhead due to the complexity of Fuzzy Logic and HMM. |

| | | | | | |
|---|---|---|---|---|---|
| [20] | Black hole attacks and other security flaws found in MANETs are carried over to vehicular ad hoc networks. | A detection system that detects communication disturbances by applying the Kolmogorov-Smirnov statistical approach. | Kolmogorov-Smirnov statistical method | Can detect black hole attacks by monitoring network activity without modifying the routing protocol. | Effectiveness might be limited if the statistical method cannot capture all attack patterns accurately. |

The table provides an overview of various strategies to combat black hole attacks across different network types, each employing unique techniques to increase security and performance. In ad hoc mobile networks (MANETs), the routing scheme and the HPAS-LSTM detection system are notable for their innovative approaches. The trust-based scheme, by introducing stages for data retrieval and route development, improves secure routing but may face challenges related to trust management complexity. In contrast, the HPAS-LSTM technique combines honeypots with Long-Short Term Memory networks to effectively detect and mitigate attacks, though it may involve high computational costs. The Dynamic Threshold-AODV (DT-AODV) protocol enhances traditional AODV routing by using dynamic thresholds to better manage black hole attacks, improving packet delivery rates but potentially complicating threshold management. For wireless sensor networks (WSNs), the FIDS-HMM protocol integrates Fuzzy Logic with a Hidden Markov Model to detect malicious nodes and improve Quality of Service (QoS) parameters, although it can be computationally intensive. Lastly, the Kolmogorov-Smirnov statistical method provides a non-intrusive way to detect black hole attacks in vehicular networks, monitoring activity without modifying routing protocols, but it may not fully capture all attack patterns. Each method offers distinct advantages and limitations, reflecting the ongoing efforts to secure networks against sophisticated attacks.

**Proposed methodology**

MANET is a computing node set at which there is no support on the fixed infrastructure. In the network each node in turn communicates with one another using wireless links and the architecture used in the network is illustrated in the following figure. Besides, the dynamic topology of nodes in the MANET is challenging their role essentially for providing the network security. The network security is made by the help of the black hole attack prediction and detection.This method for detecting black hole attacks a new system of fuzzy inference is developed with reference to the certificate authority, trust valve, energy level, message integrity, and node authentication. The primary focus of the proposed effort is node authentication. In MANET before the process of route discovery initiation, the simulation is done with the help of NS2 network simulator in which the system of fuzzy inference design provide better features in offering the certificates to the trusted nodes only. This in turn helps to identify and avoid the black hole attack on malicious nodes as well. Better performance outcomes lead to an increase in throughput and a decrease in End to End Delay when the packet delivery ratio improves. This indicates clearly that the system is more recovered and reliable for their military application.

This work targets on node authentication in MANETs prior to the route discovery procedure and for the use of a fuzzy inference method to detect black hole attacks based on criteria such as energy level, message integrity, trust values, and certificate authority.By achieving better performance due to fuzzy rules the system guarantees that certificates are issued only to the trusted nodes thus assisting in the identification of the In the present scenario, they are malicious nodes and black hole attack. The architecture comprises four phases: Trust Manager, Certificate

Authority, Node Authentication and Fuzzy Inference System. The Trust Manager computes trust values as per what the Trust Manager can perceive and other aspects such as the number of packets sent. The Certificate Authority provides certificates based on fuzzy analysis, classifying nodes as 'Normal' and 'Malicious.' The former is granted certificates for routing while the latter raises alarms to other network nodes to prevent black hole interception. This integrated approach also provides a mechanism to detect and isolate malicious nodes thus improving the security of the network.

First, the trust manager assesses each node's degree of trust based on direct monitoring of the neighboring nodes. This evaluation is premised on the number of packets that have been transmitted and received by the various nodes. Every node also stores the list of its neighbors and their trust values as per the trust value table illustrated in figure 3 (a). The trust value is determined by the packet transmission interactions of the nodes only as shown in Figure 3 (b). For example, Equation (1).

$$Trust_{AB} = \frac{(P_s)_A}{(P_r)_B}$$

In this context, the variable TAB refers to the calculate trust value of node A with respect to node B, where (Ps)In order to build a packet transmission format as illustrated in Figure 3(b), A is the number of packets sent from node A and (Pr)B is the total number of packets received by node B. The format has a source node list (SL) that indicates the node that sent the packet to be forwarded. Also, the term 'Forwarded Packet' (F) shows the total number of data packets that have been sent to other network nodes that are trustworthy. Last, when node A comes to know that node B has acknowledged that it has received a forwarded packet, then the "To Forward" (TF) of node B is incremented by 1. The packet transmission algorithm is presented in the following algorithm 1.

**Algorithm 1: Packet Transmission**

**Input**:List of Source Nodes, Trust Value of Nodes, $(P_s)_{A,}$ $(P_r)_B$

**Output**: Malevolent Node with a Trust Value

**Step 1:** If $(F)_{node\ B}$ and SL)]

**Step 2**:(F) node $B^{++}$;

**Step 3**:(TF) node $B^{++}$;

**Step 4**:$(F)_{node\ B} \geq$ Threshold Limit.

**Step 5**: Else calculate

$Trust_{AB} = (\frac{(P_s)_A}{(P_r)_B}//$

**Step 6**: Declare Malicious Node.

Malicious nodes that pretend to provide authentic routes from source to destination without really forwarding packets modify routing paths in a black hole attack, producing inaccurate data. The suggested technique and packet transmission format are essential for identifying the false information generated by these hostile nodes.

Because resources are scarce in wireless ad hoc networks, energy resources are essential to the behavior of healthy nodes. Network operations can be affected by selfish conduct, such as avoiding forwarding packets and preserving battery life. As nodes send and receive data, their energy levels are periodically checked, which has an impact on each node's trust values (shown as Energy(node)). In addition, the watch dog technique is used, in which every node observes how its neighbors behave in order to identify irregularities such packet drops or non-forwarding actions. In order to detect network anomalies like packet losses and forwarding delays, the trust manager helps nodes communicate with one another.

Network nodes protect the integrity of packets by detecting any neighbor node attempting to change the content of a message. If this happens, the tampered packet is immediately discarded to preserve packet integrity. Every node starts off with a positive Data Integrity Value (MIV(node)), which drops off if any nodes try to change the content of a packet. Nodes verify authenticity by digitally signing data packets with unique keys and hop count fields. In order to lessen harmful network activity, nodes also lower hop count measurements. Nodes monitor digital signature material and decrypt the public key used by the originating node to confirm authenticity after receiving information, making sure that the received packet fields match. A node reduces its MIV(node) and discards the packet if it finds evidence of content change. Using the MD4 method to hash packets reduces energy consumption.

Information integrity values, trust values, and energy level of the target node are taken into account by the ultimate trust manager when assessing its trustworthiness. The ultimate trust value and timeout value are established based on these variables. Below equation is used to determine the total final trust value.

$$Trust_{(new)} = Energy_{(node)} + Trust\ value\ _{(old)} + MIV_{(node)}$$

Where

$$Energy_{(node)} = \frac{\sum(PR + PF + BP))}{node_{ito\ n}}$$

In this case, the network nodes range from i to n, and PR, PF, and BP stand for packet received, packet forwarded, and battery power, respectively. It updates the $Trust_{(new)}$ to the Certificate Authority (CA) and recalculates the trust value upon receiving a request for the final trust manager. To choose the node with the highest trust value to serve as the Certificate Authority, the CA uses an election algorithm. Through the use of trust value certificates, the CA node allows other nodes in the network to obtain certificates for data exchange, guaranteeing private and secure communication by limiting access to trusted nodes exclusively. Algorithm 2 presents the certificate authority authentication algorithm.

**Algorithm2**: Election of Certificate Authority

**Input**: Route discovery node

**Output:** Nodes for transmission

**Step 1**: Initially generate the shared keys of the node $(S.Key)_s$

**Step 2**: Source node initiates the communication and request CA toprovide

[S.Req ($S_{ID}$, $D_{ID}$. $Trust_{(new)}$]$_{(s.key)s}$

**Step 3**: CA decrypts S. Req and obtains the $S_{ID}$ in the ID Repository

**Step 4**: CA checks if($S_{ID}$ == ID repository) Then CA checks $D_{ID}$ is in its range

**Step 5**:lf ($D_{ID} == range$)

Go to step 7

**Step 6**: Else

Initiate communication again

**Step 7**: Generate $(P.Key)_S$ (Pr. Key $)_s$, $(P.Key)_d$. (Pr. Key $)_d$ .$(S.Key)_d$

**Step 8**: The certificate authority therefore provides certificate as, Certificate A [Sin. (P.Key)., (Pr.Key),$Trust_{AB} Trust_{(new)}$]

**Step 9**: CA sends E [(Certificate A) S.$Key_s$, to source node

**Step 10**: CA sends E [(Certificate B) S. $Key_d$] to destination node

**Step 11**: Else Quit or Stop.

In this case, packet reception, packet forwarding, and battery power are denoted by PR, PF, and BP, respectively. There are nodes in the network that range from i to n. The trust value is recalculated and $Trust_{(new)}$ to be sent to the CA is updated each time the certificate authority asks the final trust manager for assistance.

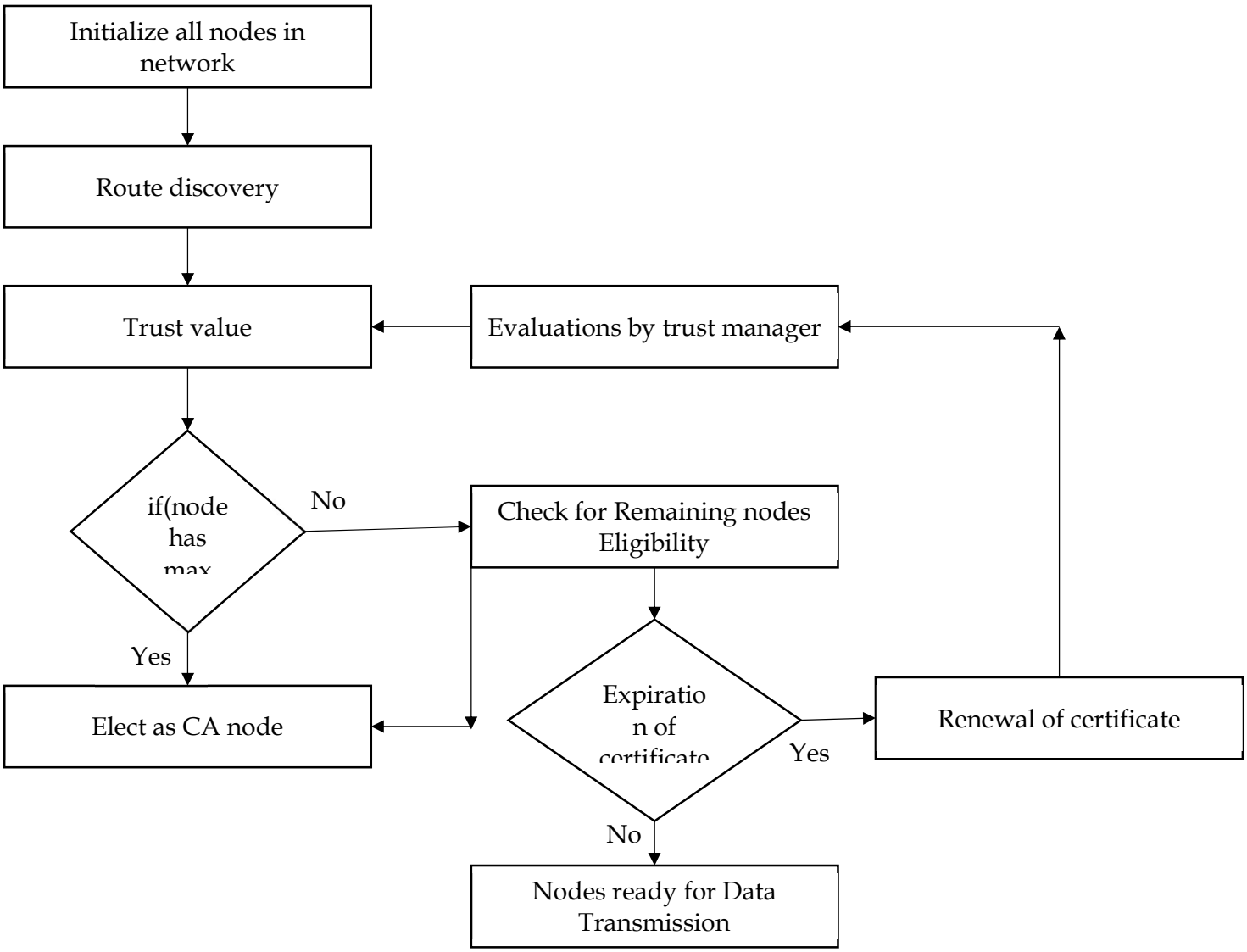


Figure 2.Electron of certificate authority

The suggested system uses fuzzy logic and Pareto optimization to improve node dependability. Trust values, on the other hand, represent both optimistic and pessimistic situations and range from 0 to 1. The fuzzy method structure is represented by Figure 5 and consists of one output (Node Type) and four inputs (Direct Trust of node u, Node Energy Value u, Node Trust Value u, and Message Integrity Value of node u). Fuzzification is the process by which crisp inputs are converted into fuzzy trust values. The inference engine processes the inputs by applying pre-established rules that are kept in the rule base. Higher f(u) values are used by the rule base to select trustworthy nodes that the Certificate Authority can issue certificates to The chosen node then goes on to become the next forwarder to arrive at the destination. The output N(u) is facilitated by membership functions, which are divided into Very Low, Low, Medium, High, and Very High categories. IF-THEN statements are utilized in fuzzy rule base formulation to create judgments based on fuzzy values EV(u), TV(u), and MIV(u). The inference engine maps these rules in a nonlinear fashion, producing fuzzy outputs that are consistent with the given if-then rules and guaranteeing comparable outcomes. Making decisions is made easier by the way the intermediate metrics and rule creation work with AND operations.

$$IF(u)\ is\ VH\ AND\ TV\ (u)\ is\ VH\ AND\ MIV\ (u) VH\ THEN\ N(u)\ is\ VH$$

$$IF(u)\ is\ VL\ AND\ TV\ (u)\ is\ VL\ AND\ MIV\ (u) VL\ THEN\ N(u)\ is\ VL$$
$$IF(u)\ is\ L\ AND\ TV\ (u)\ is\ L\ AND\ MIV\ (u) L\ THEN\ N(u)\ is\ L$$

The sample fuzzy rule shown above is the same as the set of 136 rules that was utilized to determine the fuzzy outputs. The output of the inference engine, which generated fuzzy results by mapping utilizing fuzzy rules, was fed fuzzified values. For instance, the inference engine discovers from Table 1 that if there is an increase in EV(u), TV(u), and MIV(u). The extremely reliable node known as "Trusted Node" came next. While there are several defuzzification techniques available, center of gravity is a common and useful one. Nevertheless, the center of gravity's defuzzification, which is described as,

$$N(u) = \frac{\sum_{i=1}^{n} u_i * c}{\sum_{i=1}^{n} c_i}$$

where, $ui$ is the rule base output i $ci$ is the centre of the membership function output.

Table 1.Discrimination in Fuzzy

| **Fuzzy level** | **Trust value** | **Output Normal (trusted)\ Malicious** |
|---|---|---|
| Very low | 0 to 0.2 | Malicious |
| Low | 0.2 to 0.4 | Malicious |
| Medium | 0.4 to 0.6 | Trusted |
| High | 0.6 to 0.8 | Trusted |
| Very high | 0.8 to 1 | Trusted |

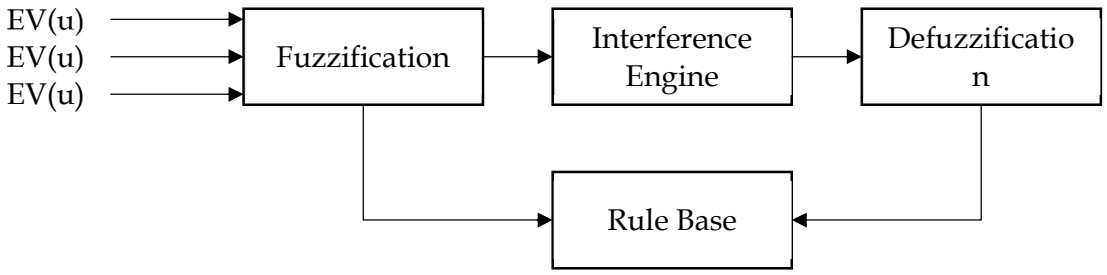


Figure 3.Fuzzy design approach

**Result and Discussion**

The NS-2 is used for simulation, with varying network speeds. The network scenario for simulation is presented in Table 2.The performance analysis of Certificate Authority with Fuzzy Approach is done on the basis of Packet Delivery Ratio, throughput, End-to-End Delay with AODV with Black Hole Attack and Normal AODV, and Detection Ratio of Malicious Node. Twenty, thirty, forty, fifty, and sixty nodes were clustered in the performance analysis. while the malicious nodes were 50, 100, 150, 200, and 250.

Table 2. Simulation Setup

| **Parameters** | **Value** |
|---|---|
| Area | 1000 $m^2$ |

| | |
|---|---|
| Routing Protocol | AODC |
| Data rate | 5 pks\s |
| Packet size | 64 bytes |
| Number of nodes | 50, 100, 150, 200, and 250 |
| Simulation time | 600ms |
| Traffic model | CBR |
| Transmission range | 250m |
| Node speed | 2 ms |
| Pause time | 10s |

Throughput: Throughput is described as the volume of data that can go a certain distance of time over a certain network from a source to a destination. Bits per second or packets per second are common ways to represent it abbreviated as bps or pps respectively. Throughput in the context of wireless networks particularly MANETs is a measurement of the amount of data that can be successfully transmitted in a specific amount of time. Throughput thus refers to the network's capacity to transfer data and is an essential measure of network performance.

$$T_h = \frac{\sum_{i=1}^{n} N^T}{\sum_{t-1}^{n} N^S} \times 100$$

where, N T is average number of receiving node, NS is average number of sending node and n is number of node.

Table 3. Comparison of Throughput

| No of Nodes | HPAS-LSTM | DT-AODV | FIDS-HMM | Fuzzy Heuristics inMANET |
|---|---|---|---|---|
| 50 | 3.34 | 4.23 | 5.23 | 7.12 |
| 100 | 3.56 | 4.34 | 5.45 | 7.23 |
| 150 | 3.86 | 4.56 | 5.87 | 7.34 |
| 200 | 4.89 | 4.89 | 5.91 | 7.67 |
| 250 | 5.24 | 4.9 | 6.34 | 8.23 |

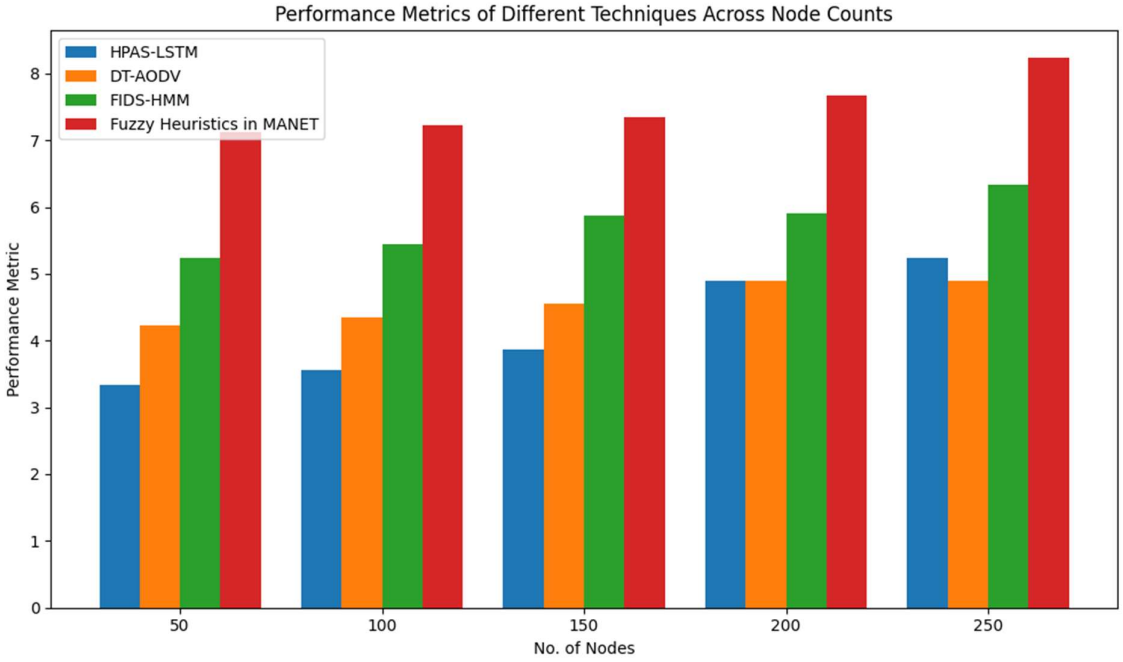


Figure 4. Comparison of Throughput

Final Delay: Final to Final The delay is the amount of time a data packet takes to get to its intended node in a network and is also referred to as latency. It encompasses all delays that may occur at the transmission path, including delays in processing, queuing, transmission, and propagation. Completely Postponement is crucial in real-time applications, where low latency is essential for ensuring timely delivery of data packets. In MANETs, minimizing End-to-End Delay helps improve overall network responsiveness and user experience.

$$D_t = \frac{\sum_{i=1}^{n} d_i}{n}$$

where n is the number of nodes and di is the average end-to-end latency.

Table 4. Comparison of End to End Delay

| No of Nodes | HPAS-LSTM | DT-AODV | FIDS-HMM | Fuzzy Heuristics in MANET |
|---|---|---|---|---|
| 50 | 345 | 431 | 545 | 291 |
| 100 | 364 | 454 | 567 | 301 |
| 150 | 379 | 486 | 586 | 321 |
| 200 | 398 | 495 | 591 | 331 |
| 250 | 423 | 523 | 602 | 341 |

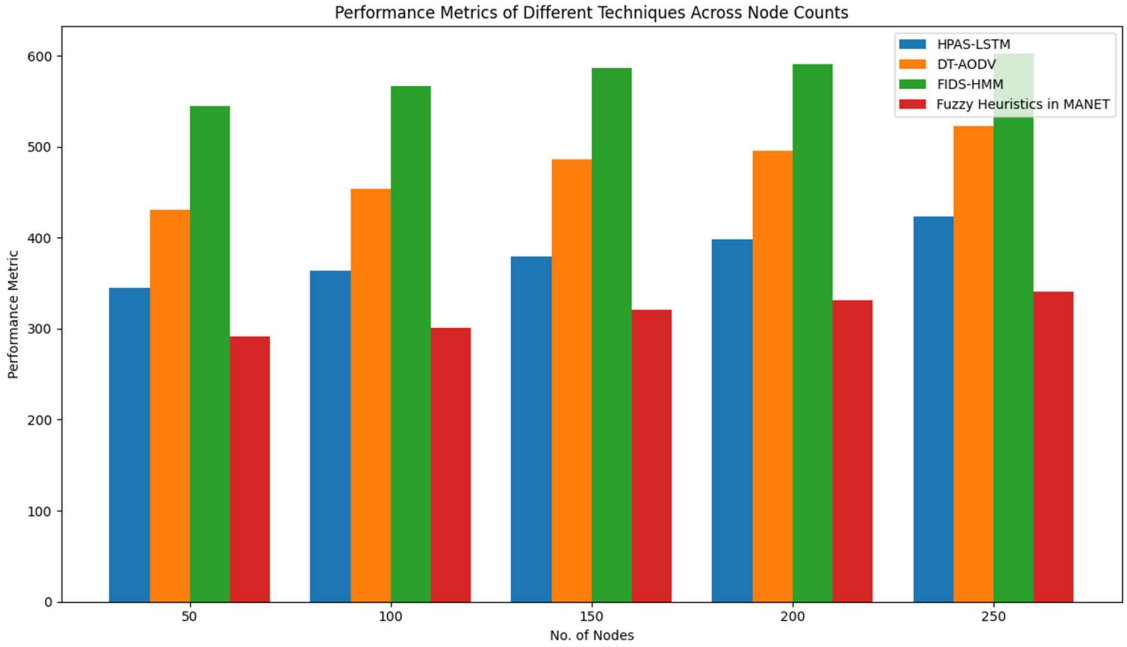


Figure 5. Comparison of End to End Delay

The packet delivery ratio is the ratio of the total number of packets received by the destination to the total number of packets, or PDR transmitted by source node.It shows how well the network works at getting data packets to where they're supposed to go. A healthy network is indicated by a high packet delivery ratio. performance, indicating minimal packet loss or transmission errors. In MANETs, maintaining a high Packet Delivery Ratio is essential for ensuring reliable communication and efficient data transfer.

$$PD_R = \frac{\sum_{i=1}^{n}(N_i^s - N_i^T)}{\sum_{i=1}^{n} N_i^s} \times 100$$

where, PDR is average packet delivery NS is the node delivered by the sender, NT is the node received by the recipient, and ratio and n are the number of nodes.

Table 5. Comparison of Detection Ratio

| No of Nodes | HPAS-LSTM | DT-AODV | FIDS-HMM | Fuzzy Heuristics in MANET |
|---|---|---|---|---|
| 50 | 76 | 80.23 | 81.23 | 90.12 |
| 100 | 77.34 | 81.34 | 81.89 | 91.23 |
| 150 | 78.23 | 82.54 | 82.43 | 91.56 |
| 200 | 78.92 | 83.45 | 83.23 | 91.78 |
| 250 | 79.45 | 85.34 | 84.23 | 92.43 |

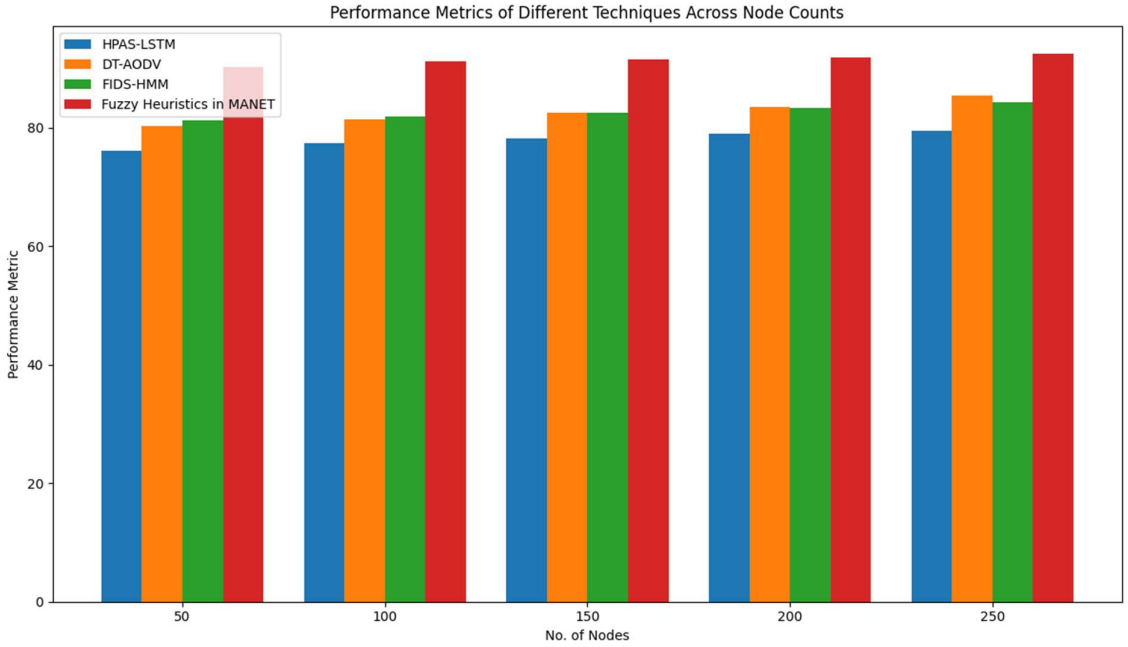


Figure 6. Comparison of Detection Ratio

**Conclusion**

The effectiveness of the proposed fuzzy inference method in mobile ad hoc networks for identifying black hole attacks(MANETs) through node authentication, Certificate Authority, analysis of trust values, energy level, and message integrity. Emphasizing on node authentication as a crucial step before route discovery, the system ensures that certificates are issued only to trusted nodes, resulting in improved performance metrics such as End-to-End Latency, throughput, malicious node detection ratio, and packet delivery ratio in comparison to conventional techniques like AODV. The CA with Fuzzy Approach outperformed AODV and modified AODV algorithms, especially with more than 60 nodes, where it detected and isolated black hole attacks effectively. While existing mechanisms showed promising results, the proposed approach demonstrated even better performance, with a 20% improvement in malicious node identification. Overall, the CA-enabled fuzzy methodology exhibited superior throughput, latency, packet delivery ratio, and malicious node detection compared to current approaches, showcasing its increasing MANET security.

**Reference**


1. Ramphull, D., Mungur, A., Armoogum, S., & Pudaruth, S. (2021, May). A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In *2021 5th international conference on intelligent computing and control systems (ICICCS)* (pp. 204-211). IEEE.
2. Eltahlawy, A. M., Aslan, H. K., Abdallah, E. G., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A survey on parameters affecting Manet Performance. *Electronics*, *12*(9), 1956.
3. 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.
4. 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.
5. Sivapriya, N., & Mohandas, R. (2022). Analysis on essential challenges and attacks on MANET security appraisal. *Journal of Algebraic Statistics*, *13*(3), 2578-2589.
6. Eltahlawy, A. M., Aslan, H. K., Abdallah, E. G., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A survey on parameters affecting Manet Performance. *Electronics*, *12*(9), 1956.
7. Sankar, S. M., Dhinakaran, D., Deboral, C. C., & Ramakrishnan, M. (2023). Safe routing approach by identifying and subsequently eliminating the attacks in MANET. *arXiv preprint arXiv:2304.10838*.
8. Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Ghafoor, M. I., & Sakr, H. A. (2023, January). In MANET: An improved hybrid routing approach for disaster management. In *2023 IEEE*

*International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T)* (pp. 1-6). IEEE.

9. Saravanan, Thangavel, and S. Saravanakumar. "Energy efficient optimization algorithms for MANET." In *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing*, pp. 572-579. 2023.
10. Reka, R., Karthick, R., Ram, R. S., & Singh, G. (2024). Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET. *Computers & Security*, *136*, 103526.
11. Reka, R., Karthick, R., Ram, R. S., & Singh, G. (2024). Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET. *Computers & Security*, *136*, 103526.
12. Srinivasan, V., Raj, V. H., Thirumalraj, A., & Nagarathinam, K. (2024). Original Research Article Detection of Data imbalance in MANET network based on ADSY-AEAMBi-LSTM with DBO Feature selection. *Journal of Autonomous Intelligence*, *7*(4), 1094.
13. Anand, R. P., Senthilkumar, V., Kumar, G., Rajendran, A., & Rajaram, A. (2024). Dynamic link utilization empowered by reinforcement learning for adaptive storage allocation in MANET. *Soft Computing*, *28*(6), 5275-5285.
14. Pushpalatha, K., Sherubha, P., Sasirekha, S. P., & Anguraj, D. K. (2024). A constructive delay-aware model for opportunistic routing protocol in MANET. *Expert Systems with Applications*, 124527.
15. Gopalan, S. H., Vignesh, V., Rajkumar, D. U. S., Velmurugan, A. K., Deepa, D., & Dhanapal, R. (2024). Fuzzified swarm intelligence framework using FPSOR algorithm for high-speed MANET-Internet of Things (IoT). *Measurement: Sensors*, *31*, 101000.
16. Naveena, S., Senthilkumar, C., & Manikandan, T. (2020, March). Analysis and countermeasures of black-hole attack in manet by employing trust-based routing. In *2020 6th international conference on advanced computing and communication systems (ICACCS)* (pp. 1222-1227). IEEE.
17. Srinivasan, V. (2021). Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET. *Ingénierie des Systèmes d Inf.*, *26*(6), 549-557.
18. Mankotia, V., Sunkaria, R. K., & Gurung, S. (2023). DT-AODV: A dynamic threshold protocol against black-hole attack in MANET. *Sādhanā*, *48*(4), 190.
19. Ravindran, S. (2024). Intelligent fuzzy logic based intrusion detection system for effective detection of black hole attack in wsn. *Peer-to-Peer Networking and Applications*, 1-17.
20. Cherkaoui, B., El Houssaini, M. A., Kasri, M., Beni-Hssane, A., & Erritali, M. (2024). Kolmogorov-Smirnov based method for detecting black hole attack in vehicular ad-hoc networks. *Procedia Computer Science*, *236*, 177-184.