iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** VII **Month of publication:** July 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.73302

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue VII July 2025- Available at www.ijraset.com*

# AI- Based UAV with Fuzzy Logic Algorithm using Wormhole Attack Detection in Wireless Sensor Networks

J. Saranya[1], Dr. P. Bharathisindhu [2]
[1]*Ph.D Research Scholar, Department of Computer Science, Vellalar College for Women Thindal, Erode*
[1]*Assistant Professor, Department of Information Technology, Hindusthan College of Arts & Science, Coimbatore*
[2]*Assistant Professor, Department of Computer Science, Vellalar College for Women Thindal, Erode*

***Abstract:*** ***Wireless Sensor Networks (WSNs) play a vital role in modern communication systems but remain highly vulnerable to sophisticated security threats—particularly wormhole attacks. These attacks exploit low-latency links between compromised nodes, disrupting routing protocols and often bypassing conventional cryptographic defenses. To address this challenge, this study proposes an AI-based Unmanned Aerial Vehicle (UAV) system integrated with a fuzzy logic algorithm to enhance the detection and mitigation of wormhole attacks in WSNs. The UAV acts as a mobile monitoring agent, dynamically analyzing communication patterns and network behaviors. Fuzzy logic enables the system to make intelligent decisions based on uncertain or imprecise inputs such as signal strength, hop count deviation, and packet delay. By incorporating energy-aware fuzzy clustering, the UAV optimizes its flight and monitoring tasks, extending network lifetime and improving detection accuracy. This research not only compares existing wormhole detection techniques but also introduces a novel, adaptive, and energy-efficient approach using AI and UAV technology to safeguard WSNs from one of their most dangerous attack vectors.***
***Keywords: Unmanned Aerial Vehicle (UAV), Wormhole Attacks, AI and ML; Detection Techniques, Fuzzy logic, Clustering, Wireless Sensor Networks.***

## I. INTRODUCTION

Wireless sensor networks (WSNs) are increasingly targeted by various types of distributed denial-of-service (DDoS) attacks [1]. Notable examples include sinkhole, black hole, grey hole, wormhole, Sybil, and clone attacks [2]. Among these, wormhole attacks involve multiple malicious nodes that establish a covert communication path between distant points, thereby compromising the routing mechanism [3]. These attacks are generally classified into three categories: open, half-open, and closed wormholes [4].

The ongoing advancements in wireless communication have accelerated the adoption of WSNs [5]. These networks are self-organizing systems composed of sensor nodes—devices that are both cost-effective and energy-efficient [6]. Sensor nodes are capable of collecting and preprocessing data, as well as transmitting it across the network. They often serve as routers, relaying information from neighboring nodes to a base station, which then forwards the data to remote servers. Thanks to their flexible architecture and reliable data transmission, WSNs are used in a variety of fields, including environmental monitoring, smart homes, and healthcare. Their applications also extend to military, urban, and industrial domains. In the military, for instance, WSNs [7] support surveillance, battlefield monitoring, and intruder detection, while in healthcare, they enable patient monitoring and home assistance systems. Environmental uses include air and water quality monitoring and emergency alert systems.

Despite their benefits, WSNs face significant security challenges due to their dynamic topology and resource constraints. Their low-cost, low-power design makes them susceptible to DDoS attacks, which are increasingly common [8]. These attacks disrupt network functionality by altering data, leaking sensitive information, granting unauthorized access, or allowing intruders to infiltrate the system. Common forms include wormhole [9], black hole, jamming, and clone attacks. Of these, wormhole attacks [10] are considered the most dangerous. They allow attackers to manipulate network communication without altering its visible structure, making detection [11] especially difficult. By creating a hidden tunnel between two malicious nodes, attackers can intercept, alter, and reroute data while masquerading as legitimate participants. Due to the stealthy and complex nature of wormhole attacks [12], detecting and preventing them remains a major research focus in securing WSNs.

Wormhole nodes create a deceptive shortcut in the network that appears shorter than the actual route. This false path disrupts the routing [13] topology, which typically relies on the physical distance between nodes.

A wormhole tunnel is established between two malicious nodes: the first node captures data packets [14] from one part of the network and transmits them through the tunnel to the second node, located far away. The second node then re-injects the packets into the network as if they originated locally [15]. What makes this attack particularly dangerous is that it can be launched without any prior knowledge of the network's structure and without interfering directly with legitimate nodes[16]. As a result, wormhole attacks are considered highly severe. They can be executed in several different forms. Figure 1 illustrates the various types of wormhole attacks [17].

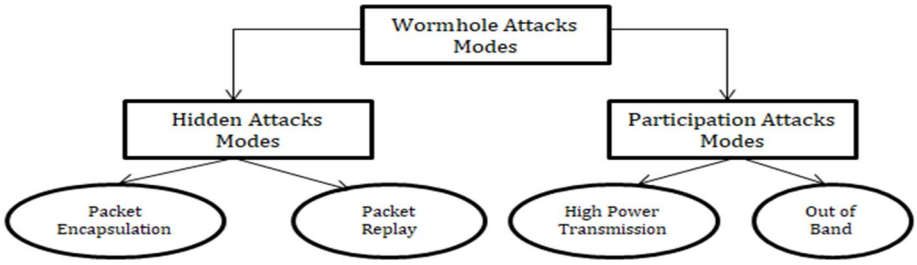



Figure 1: Wormhole attack classification according to participating and hidden nodes.

Hidden modes include packet encapsulation and packet relay. In packet encapsulation, data packets are transmitted only through legitimate routes [18]. When a wormhole node receives a data packet, it encapsulates the packet to prevent the hop count from increasing. The packet remains essentially unchanged due to the involvement of the second node [19] in the wormhole tunnel. Packet relay mode allows a wormhole attack to be executed using a single node. These malicious node forwards packets from distant nodes, making them appear as neighbors [20]. As a result, other nodes treat it as a neighbor and send data packets through it. Participation modes include high-power transmission and out-of-band communication. In high-power transmission, one malicious node with strong transmission power attracts data packets to route through it [21]. In the out-of-band mode, two malicious nodes establish a high-bandwidth out-of-band channel to form a wormhole [22] tunnel. Figure 2 illustrates the wormhole attack in wireless sensor networks (WSN).

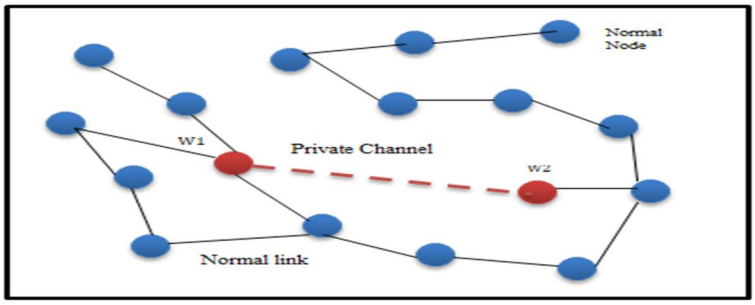



Figure 2. Wormhole attack from the outside with high power transfer.

Various techniques have been examined for detecting wormhole attacks, which pose a serious threat to network operations [23]. Particular attention has been given to wormhole detection methods in Wireless Sensor Networks (WSNs), especially in terms of their impact on energy efficiency. Additionally, several approaches have been analyzed for identifying wormhole attacks within Internet of Things (IoT) environments [24]. A comprehensive review has also been conducted on multiple strategies aimed at both detecting and preventing wormhole attacks in WSNs [25].

## II. LITERATURE REVIEW

### A. *Artificial Protective Systems and Systems Based on Machine Learning*

Murty, M. V. D. S. K et.al (2023) proposed an artificial immune system integrated with fuzzy logic to mitigate wormhole attacks, demonstrating high false positive rate (FPR) and packet delivery ratio (PDR), along with low packet loss ratio (PLR). This system was built by modifying the AODV protocol using fuzzy logic to simulate an immune-like defense mechanism. Simulations were carried out using the NS2 simulator. However, the delivery ratio of AODV decreased significantly with an increasing number of connections, and due to network congestion, the optimal path may be overlooked. Zalak L. Thakker et.al (2024) introduced a hybrid RPL protocol aimed at wormhole attack mitigation, emphasizing high detection accuracy (DA) while minimizing computational

overhead. The system utilized a support vector machine (SVM), a supervised learning algorithm, for identifying intrusions. However, the complexity of the RPL protocol led to increased control packet generation, resulting in overhead and higher energy consumption. Numan, M.; Subhan, F.et.al (2020) presented an artificial neural network (ANN)-based approach for wormhole attack detection, leveraging node connectivity information as a distance metric via hop counts. The method was tested on a 500-node network using MATLAB. The training and testing phases of the ANN revealed a detection accuracy of up to 97% without requiring any additional hardware. Manar J. et.al (2022) proposed a deep learning approach using round-trip time (RTT) and long short-term memory (LSTM) networks for wormhole detection. The Whale Optimization Algorithm, enhanced with fitness rate adjustment, was employed to determine the optimal routing path. Implemented in Python, the method demonstrated high detection accuracy, increased PDR, reduced energy consumption, and minimized end-to-end delay. J. P. Ntayagabiri, Y. et.al (2025) introduced the Delta Rule First Order Iteration Deep Neural Learning Intrusion Detection (DRFOIDL-ID) approach for wormhole mitigation. This deep neural network-based technique identifies and isolates intruders. When compared with the Energy Trust System (ETS) and RPL-based systems, DRFOIDL-ID achieved higher detection accuracy, lower FPR, and reduced PLR. Zalak L.et.al (2024) focused on wormhole mitigation in mobile ad hoc networks (MANETs) using a machine learning-based method. Algorithms including KNN, SVM, decision tree (DT), linear discriminant analysis (LDA), naïve Bayes (NB), and convolutional neural networks (CNN) were employed to classify malicious nodes based on extracted features. Simulations in MATLAB 2019b revealed that the decision tree classifier attained the highest detection accuracy at 98.9%.

## III. WORMHOLE ATTACK

A wormhole attack involves one or more malicious nodes connected through a tunnel. These nodes intercept packets at one location and forward them to a distant node, which then re-broadcasts them locally. The tunnel between these nodes can be established through various means, such as in-band or out-of-band channels. As a result, tunneled packets may appear to arrive faster or traverse fewer hops than those following standard multi-hop routes. This behavior can mislead routing protocols that rely on hop count or distance metrics, as the malicious nodes falsely present a shorter path within the network. Once this false route is established, attackers can launch various types of disruptions, including selective packet dropping, eavesdropping, and replay attacks. Wormholes can be formed using an in-band channel, where packets are encapsulated and forwarded from one malicious node (e.g., m1) to another (e.g., m2), making intermediate nodes between them unaware of their presence. Alternatively, a physical connection such as a dedicated wired link or a long-range wireless link can be used to create the tunnel, as illustrated in Fig. 3. Depending on their strategy, malicious nodes may either reveal themselves within the routing path (known as an open or exposed wormhole attack) or remain hidden (a closed or hidden wormhole attack).

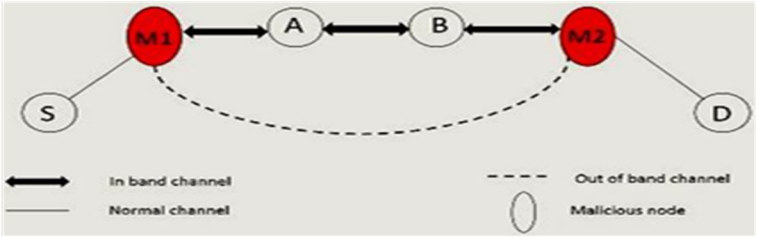



Fig 3 Wormhole Attack

In Fig. 3, under a hidden wormhole attack, the destination node D perceives that the packet from the source node S has been routed through nodes A and B. However, in the case of an exposed wormhole attack, it correctly identifies the packet path as passing through nodes A, m1, m2, and B.

## IV. PROPOSED WORK

To establish multiple paths between the source and destination during each route discovery phase, an AI-enabled Unmanned Aerial Vehicle (UAV) network is employed—an extension of the AODV protocol. In this AI-enhanced UAV routing protocol, the source node first checks its routing table for an existing route between any two nodes. If a route exists, the corresponding routing information is used. Otherwise, the node broadcasts a Route Request (RREQ) packet to its neighbors, which then check for a valid route to the destination.

Upon receiving an RREQ, the destination node responds with a Route Reply (RREP) along the same path that the RREQ arrived. For each RREQ received via alternative routes, an RREP is sent back through the respective paths. All discovered paths are then stored in the source node's routing table. This approach allows the protocol to maintain multiple paths for improved reliability.

The key concept of the AI-enabled UAV protocol is to compute multiple routes during the route discovery process in order to mitigate link failures. Among the established paths, the primary route is selected based on the earliest route establishment time. Alternate routes are only utilized if the primary route fails, and the earliest available alternative is prioritized.

This paper proposes a wormhole detection and prevention technique based on the AI-enabled UAV protocol. The algorithm works as follows: when the source node broadcasts an RREQ, it records the time 1. Upon receiving an RREP, the arrival time is noted. If multiple RREP packets are received, indicating multiple available paths to the destination, the respective arrival times $t2\_i$ are recorded. Using these timestamps, the round-trip time (RTT) $t3\_i$ for each route is calculated. Next, the RTT for each route $t3\_i$ is divided by its corresponding hop count to derive the average RTT per hop. These values are then used to calculate a threshold RTT $h$. Each route's average RTT $ts\_i$ is then compared to $h$. If the RTT $ts\_i$ of a given route is significantly lower than the threshold and its hop count is exactly two, it is indicative of a potential wormhole link. Upon detecting such a condition, the source node identifies its first-hop neighbor $m1$ on the suspicious route as a wormhole node and sends a dummy RREQ through that route. When the destination receives the dummy RREQ via its neighbor 2, it also flags $m2$ as a wormhole node. Both $m1$ *and* $m2$ are then blacklisted: their routing entries are deleted from the source's table and broadcast to the rest of the network. This ensures that the compromised path is effectively blocked from future use. From that point onward, whenever the source requires a route to the same destination, it checks the routing table during the route establishment phase. If the identified route includes a known wormhole link, it is discarded in favor of an alternative secure path, if available. The advantage of employing the AI-enabled UAV protocol in this proposed method lies in its reduced overhead and minimized end-to-end delay. The detailed process is illustrated in the flowchart shown in Fig. 4. AI-based Unmanned Aerial Vehicle (UAV) system integrated with a fuzzy logic algorithm to enhance the detection and prevention of wormhole attacks in WSNs. The UAV acts as a mobile monitoring node, dynamically scanning and analyzing communication patterns within the network. The fuzzy logic clustering based on energy management model processes uncertain or imprecise information—such as packet delay, hop count variation, and signal strength—to accurately identify anomalies associated with wormhole behavior. By leveraging artificial intelligence and mobility, the system significantly improves detection accuracy, reduces false positives, and enhances network resilience.

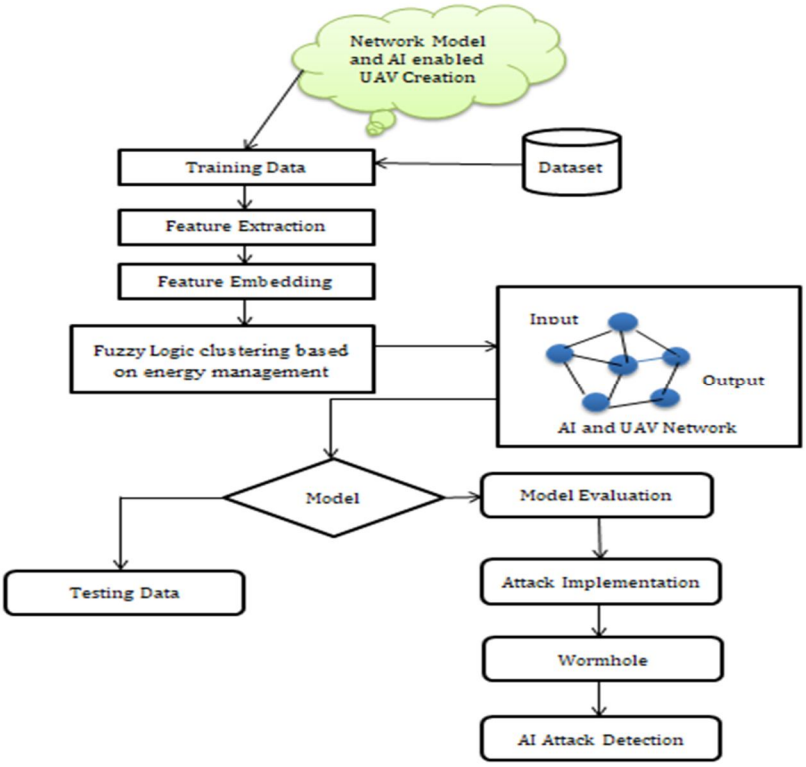



Figure 4: Overall architecture in AI based wormhole attack detection

Simulation results demonstrate the effectiveness of the proposed approach in terms of detection rate, energy efficiency, and response time, offering a robust solution for securing WSNs against advanced cyber threats.

Algorithm:

1. When sender broadcast route request packet it will note the time $t_1$.
2. For each route reply received by the sender node, sender node notes time $t_{2-i}$.
3. Sender node calculates the round trip time for all routes using a formula

   $t_{3-i} = t_{2-i} - t_1$.
4. Calculate the threshold round trip time by using this formula
   a. $\frac{t_{3-i}}{hop\,count_i} = t_{S1}$
5. Take average of $t_{S-i}$ for i number of paths from step 4.
6. Note this time as threshold round trip time $t_{th}$ for each route. Just to understand assume
7. i=3 i.e. total three paths to the destination. Then according to step 4

   $\frac{t_{3-1}}{hop\,count_i} = t_{S1}$ $\frac{t_{3-2}}{hop\,count_i} = t_{S2}$ $\frac{t_{3-3}}{hop\,count_i} = t_{S3}$
8. Step 5 will give the average of above values $\frac{t\_(s-1)+t\_(s-2)+t\_(s-3)}{3} = t_{th}$ which is threshold round trip time
9. If ($ts\_i$ is less than $tth$ and hop count on route i is equals to 2 == true) then

{

   a. Detect route i as a wormhole link
   b. Sender detects first neighbour node $m_1$ as wormhole node
   c. Sender sends dummy RREQ through route i and neighbour $m_1$
   d. Receiver receives dummy RREQ from its neighbour $m2$
   e. Receiver detects its neighbour $m_2$ as wormhole node
   f. Routing table entries for $m_1$ and $m_2$ are removed and also broadcasted to other nodes

}

Else

{

End If

There is no threat of wormhole attack and it is not detected

}

## V. RESULT ANALYSIS

Simulation results were obtained by evaluating parameters such as packet delivery rate, average end-to-end delay, and average throughput at the destination. These metrics were compared across three scenarios: the standard AI-enabled UAV protocol, the wormhole-affected AI-enabled UAV protocol, and the proposed AI-enabled UAV protocol with wormhole mitigation.

Initially, performance measurements were recorded for the standard AI-enabled UAV protocol under normal operating conditions. Subsequently, wormhole nodes were introduced into the same environment, and the metrics were re-evaluated to assess the impact of the attack. Finally, the proposed detection and prevention mechanism was applied to the compromised network, and its performance was compared against the other two scenarios.

The simulation was conducted in a wireless sensor network environment using Network Simulator 2.34 (NS-2.34). The simulation parameters used in the study are listed in the following table.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue VII July 2025- Available at www.ijraset.com*

Table 1 Simulation Parameters

| | |
|---|---|
| Simulation area | 1000m x 1000m |
| Network Simulation | NS22.34 |
| Channel Type | Wireless |
| Routing protocol | AODV |
| Total Energy | 150J |
| Number of nodes | 100 |
| Simulation time | 60 sec |

The y-axis indicates the various routing protocols, while the x-axis shows the network parameters in each of the diagrams below. Under various network densities (i.e., node counts), Figure 5 shows the average throughput values plotted against the three routing techniques. The throughput difference between the proposed AI-enabled UAV protocol and the wormhole-affected AI-enabled UAV protocol grows more noticeable as network density rises for CBDT-IMA (82.43%), ENS-WHA (89.87%), and AI-UAV (98.23%). This shows that the suggested approach outperforms the Eq. (1) technique in terms of throughput, especially in crowded network situations.

Throughput

$$Average\ Throughput\ Nodes\ = \frac{Total\ Data\ Transferred\ Packet\ Size}{Total\ Time\ (T_{iEnd} - T_{iStart})} \qquad (1)$$

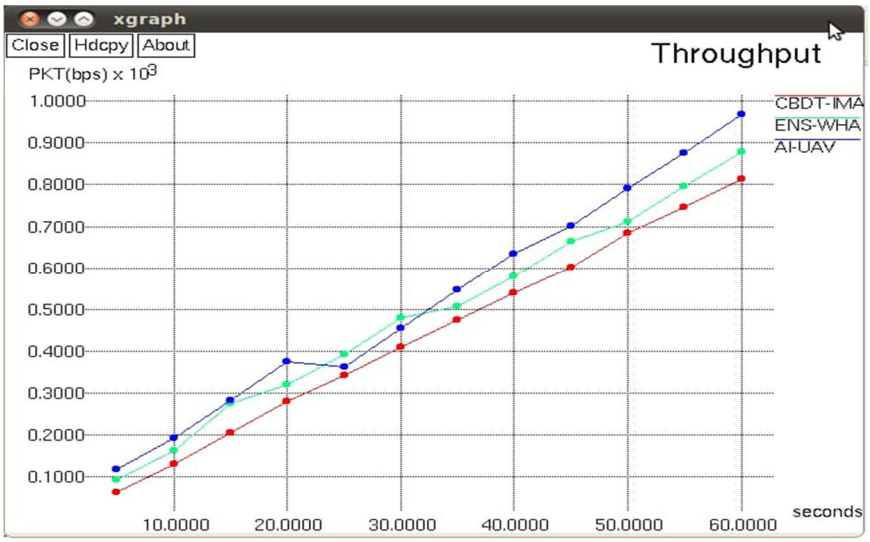



Fig 5 Average throughput for nodes

The average end-to-end delay in Eq. (2) increases when wormhole nodes are added to the conventional AI-enabled UAV protocol, as seen in Figure 6. But when the suggested algorithm is used in this setting, the delay times for CBDT-IMA 25.50%, ENS-WHA 21.23%, and AI-UAV 18.12% drop noticeably. It is noteworthy that the delay values obtained with the suggested AI-enabled UAV protocol are significantly lower than those observed in non-attack scenarios. These findings, which are displayed in Figure 6, show that the suggested approach improves end-to-end delay performance, especially in situations involving high-density networks.

$$T_{E2E} = T_{iEnd} - T_{iStart}$$

The average end-to-end (E2E) delay is the sum of all end-to-end delays divided by the total number of flows $N_F$

$$Average(T_{E2E})\ nodes\ = \frac{\sum_{i=1}^{N}(T_{E2E_i})}{N_F} \qquad (2)$$

End to End Delay

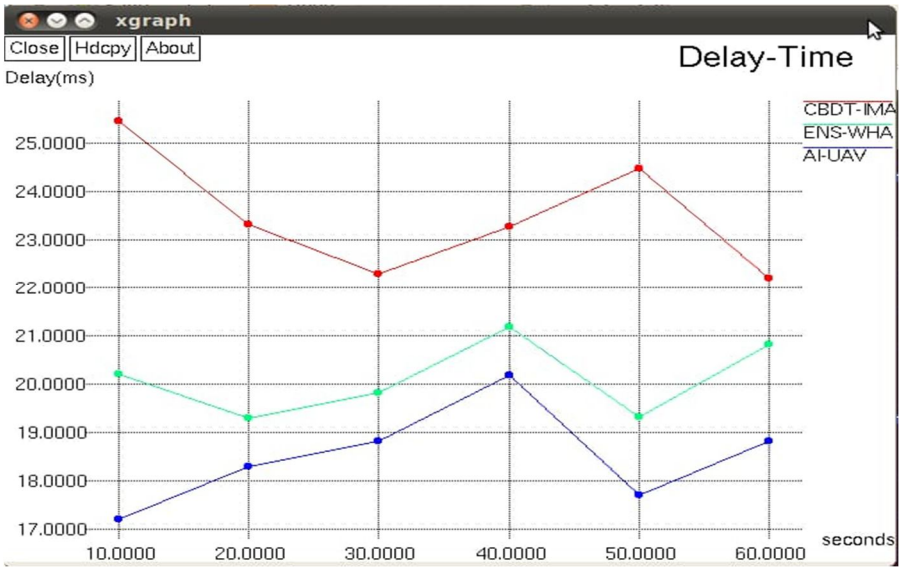



Fig 6 Average End to End Delay for Nodes

The findings for the packet delivery fraction at various network densities are shown in Figure 7. Although there are some differences, the overall packet delivery fraction node (PDFN) for CBDT-IMA IN 94.67%, ENS-WHA IN 97.78%, and AI-UAV IN 99.58% improves with increasing density. The success of the suggested strategy, which adheres to Eqs. (3) and (4), is demonstrated by the difference in delivery rates between the performance of the wormhole-affected AI-enabled UAV protocol and the proposed AI-enabled UAV protocol.

$$PDFN = \frac{\sum Number\ of\ Packets\ Received\ to\ Legitimate\ Nodes}{\sum Number\ of\ Packets\ Send\ \ to\ Legitimate\ Nodes} \times 100\% \qquad (3)$$

$$Since\ PDFN = \frac{\sum_{k=1}^{n} X\,K\alpha}{\sum_{k=1}^{n} Y\,K\alpha} \times 100\% \qquad (4)$$

XKα It specify for number of packets received to the legitimate nodes

*Y*Kα It specify for number of packets send to the legitimate nodes

*Kα* It specify for methods that can possibly detect wormholes: Negative Temperature, Hawking/ Phantom Radiation, and Kα iron emission lines

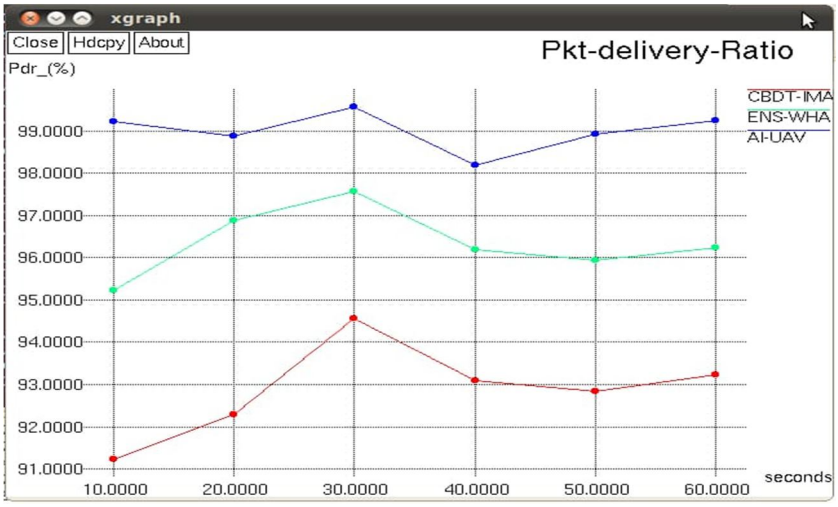



Fig 7 Packet Delivery Fraction for Nodes

### *A. State of the Art Method*

The time needed to transport the entire message is the delay value, and since hostile sensors drop packets, it will never be delivered in its entirety. Since the attack case will never deliver the message, an infinity value is chosen. It is evident that the suggested secure approach has a negligible increase in the delay value that is difficult to identify. In a network with 50 nodes, the detection method's increased delay is 1.6 seconds. Furthermore, the additional transmission latency in a network with 75 nodes is 0.3 seconds. Additionally, an extra one second is used for detection in the 100-node network size. The length of the wormhole tunnel and the size of the neighbourhood lists are positively connected with the amount of time needed to execute the suggested security solution. For a network size of 100 nodes, the end-to-end delay has the highest values.

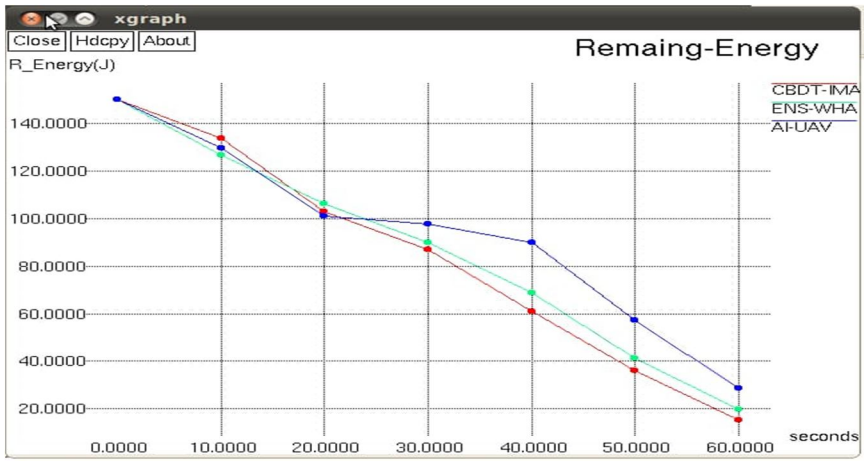



Figure 8: Energy Consumption for Nodes

Table 2: Overall Comparison Result Analysis

| State of the Art Method | CBDT-IMA | ENS-WHA | AI- Based UAV with Fuzzy Logic Algorithm |
|---|---|---|---|
| Packet Ratio (%) | 91.35 | 95.43 | 99.47 |
| Delay Time (Sec) | 25.67 | 20.12 | 17.34 |
| Remaining Energy (J) | 18.56 | 20.12 | 30.65 |
| Throughput (Transmission Sec) | 0.83 | 0.89 | 0.98 |
| Overall Result Analysis (100 nodes) | 90.01% | 95.23% | 99.45% |

Approaches based on artificial intelligence (AI) and machine learning (ML) provide efficient answers to the most recent problems. Neighbor-based discovery strategies are one of the main problems, as Table 2 illustrates. These techniques are frequently inefficient in terms of energy for CBDT-IMA in 18.56 and ENS-WHA in 20.12 and AI- Based UAV with Fuzzy Logic Algorithm 30.65 and may not be able to detect short tunnel wormholes, even if they can attain detection accuracy of overall result analysis for (show in Figure 8) AI- Based UAV with Fuzzy Logic Algorithm up to 99.45%. A weighted clustering technique has been incorporated into an unsupervised learning-based strategy to overcome these drawbacks. This technique keeps the detection accuracy at 99.45% while drastically lowering energy usage. Further enhancements in throughput CBDT-IMA 0.83 and ENS-WHA for 0.89 and AI-Based UAV with Fuzzy Logic Algorithm 0.98 and packet delivery ratio CBDT-IMA 91.35% and ENS-WHA for 95.43% and AI-Based UAV with Fuzzy Logic Algorithm 99.47%.

## VI. OPTIMAL SOLUTIONS

The previous section highlights several state-of-the-art challenges, including a lack of scalability, inadequate load balancing, poor congestion control, excessive communication overhead, data integrity concerns, high energy consumption, increased time delays, suboptimal average packet delivery ratio (PDR) and packet loss ratio (PLR), low false positive rate (FPR), reduced transmission rates, and insufficient detection accuracy.

### *A. Schemes Based on AI and ML as the Best Answers to Cutting-Edge Issues*

Artificial intelligence (AI) and machine learning (ML)-based approaches offer effective solutions to the state-of-the-art challenges. As outlined in Table 3, one of the primary issues lies in neighbor-based discovery schemes. While these methods can achieve detection accuracies of up to 90%, they are often not energy-efficient and may fail to identify short tunnel wormholes. To address these limitations, an unsupervised learning-based approach incorporating a weighted clustering algorithm has been proposed. This method significantly reduces energy consumption while maintaining a 90% detection accuracy. Additionally, by integrating support vector machines (SVM) and multilayer perceptron's (MLP), the scheme demonstrates further improvements in throughput and packet delivery ratio.

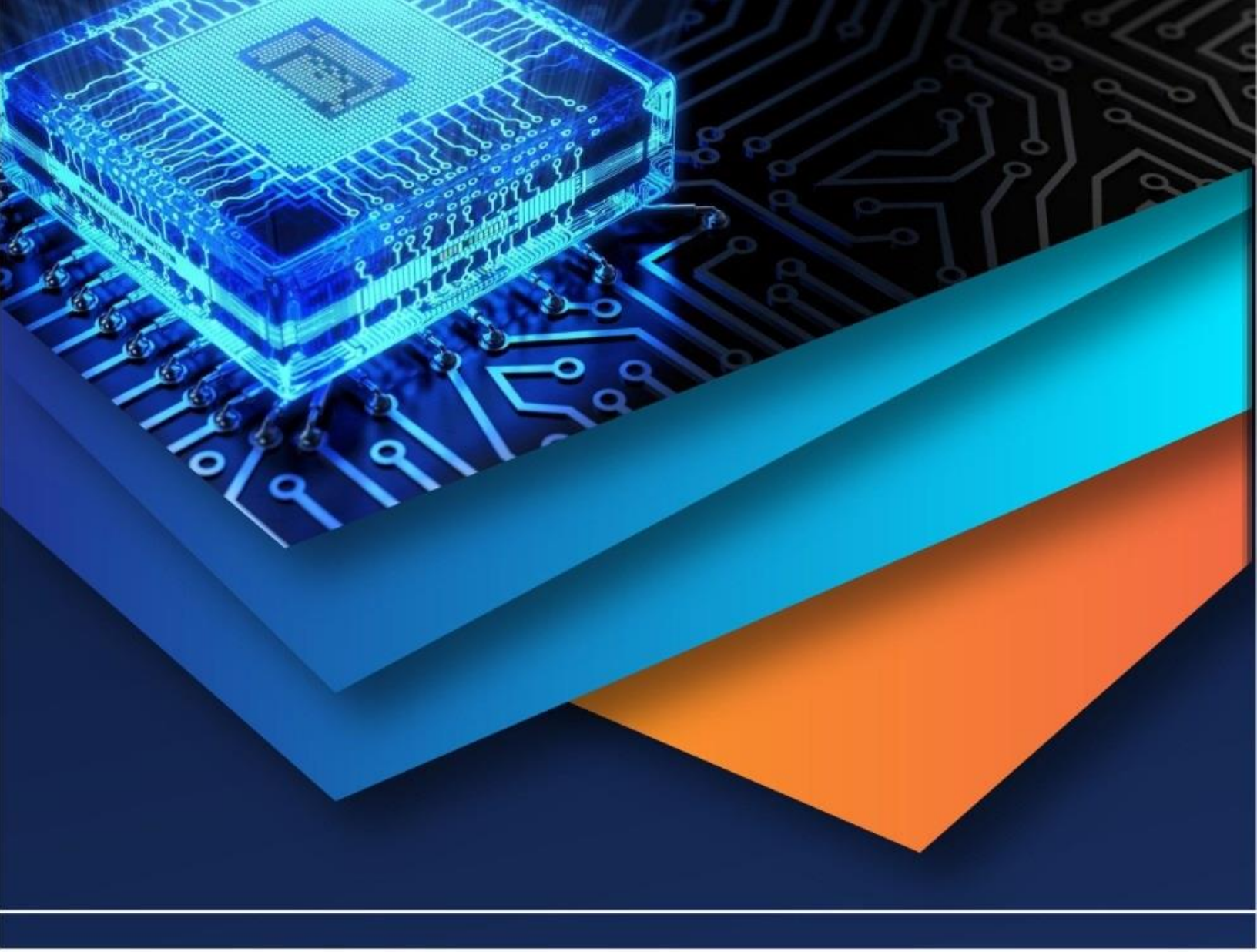
## VII. CONCLUSION

A wide range of existing schemes aimed at both detecting and mitigating wormhole attacks. These include approaches based on artificial intelligence (AI) and machine learning (ML), neighbor discovery and path selection, statistical analysis, AODV protocol, round-trip time (RTT) and hop count, as well as cloud computing and mobile agent-based techniques. A Systematic Literature Review (SLR) has been conducted to critically and comparatively analyze these methods. Each scheme was evaluated across several key performance metrics, including detection accuracy, network lifetime, energy efficiency, algorithmic complexity, packet delivery ratio (PDR), packet loss ratio (PLR), and latency. Through this review, significant gaps in the existing literature were identified, highlighting areas for future research in both the detection and prevention of wormhole attacks. Recent studies demonstrate that AI-based approaches, particularly those leveraging machine learning techniques, have shown notably high detection accuracy, outperforming many traditional methods. The comparative analysis confirms that AI- and ML-driven solutions offer more robust, scalable, and efficient performance compared to conventional state-of-the-art techniques.

## REFERENCES

[1] Murty, M. V. D. S. K., & Rajamani, Dr. L. Neighbour NodeRatio AODV (NNR-AODV) Routing Protocol for Wormhole Attack Detection in MANETs. In International Journal of Emerging Scienceand Engineering, PP: 1-9 | Volume-11 Issue-4, March 2023 | Retrieval Number: 100.1/ijese.D25470311423 | DOI: 10.35940/ijese.D2547.0311423
[2] Luo, X.; Chen, Y.; Li, M.; Luo, Q.; Xue, K.; Liu, S.; Chen, L. CREDND: A novel secure neighbor discovery algorithm for wormhole attack. IEEE Access 2019, 7, 18194–18205. [CrossRef]
[3] Alenezi, F.A.; Song, S.; Choi, B.Y. SWANS: SDN-based Wormhole Analysis using the Neighbor Similarity for a Mobile ad hoc network (MANET). In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 17–21 May 2021; pp. 653–657.
[4] Vo, T.T.; Luong, N.T.; Hoang, D. MLAMAN: A novel multi-level authentication model and protocol for preventing wormhole attacks in mobile ad hoc networks. Wirel. Netw. 2019, 25, 4115–4132. [CrossRef]
[5] Bai, S.; Liu, Y.; Li, Z.; Bai, X. Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures. Comput. Netw. 2019, 150, 190–200. [CrossRef]
[6] Patel, M.; Aggarwal, A.; Chaubey, N. Detection of Wormhole Attack in Static Wireless Sensor Networks. In Advances in Computer Communication and Computational Sciences; Springer: Singapore, 2019; Volume 760, pp. 463–471. [CrossRef]
[7] Aliady, W.A.; Al-Ahmadi, S.A. Energy preserving secure measure against wormhole attack in wireless sensor networks. IEEE Access 2019, 7, 84132–84141. [CrossRef]
[8] Zardari, Z.A.; Memon, K.A.; Shah, R.A.; Dehraj, S.; Ahmed, I. A lightweight technique for detection and prevention of wormhole attacks in MANET. EAI Endorsed Trans. Scalable Inf. Syst. 2021, 8, e2. [CrossRef]
[9] Roy, A.K.; Khan, A.K. RTT-based wormhole detection for wireless mesh networks. Int. J. Inf. Technol. 2020, 12, 1–8. [CrossRef]
[10] Karthigadevi, K.; Balamurali, S.; Venkatesulu, M. Wormhole attack detection and prevention using EIGRP protocol based on round trip time. J. Cyber Secure. Mobil. 2018, 7, 215–228. [CrossRef]
[11] Kori, S.; Krishnamurthy, G.N.; Sidnal, N. Distributed Wormhole Attack Mitigation Technique in WSNs. Int. J. Comput. Netw. Inf. Secure 2019, 11, 20–27. [CrossRef]
[12] Adil, M.; Almaiah, M.A.; Omar Alsayed, A.; Almomani, O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors 2020, 20, 2311. [CrossRef] [PubMed]
[13] Sampoornam, K.P.; Saranya, S.; Mohanapriya, G.K.; Devi, P.S.; Dhaarani, S. Analysis of LEACH Routing Protocol in Wireless Sensor Network with Wormhole Attack. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 147–152.
[14] Numan, M.; Subhan, F.; Khan, W.Z.; Hakak, S.; Haider, S.; Reddy, G.T.; Alazab, M. A systematic review on clone node detection in static wireless sensor networks. IEEE Access 2020, 8, 65450–65461. [CrossRef]
[15] Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of wireless sensor networks: An up-to-date survey. Appl. Syst. Innov. 2020, 3, 14. [CrossRef]
[16] Premkumar, M.; Sundararajan, T.V.P. DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocess. Microsyst. 2020, 79, 103278. [CrossRef]
[17] Yousefpoor, M.S.; Yousefpoor, E.; Barati, H.; Barati, A.; Movaghar, A.; Hosseinzadeh, M. Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. J. Netw. Comput. Appl. 2021, 190, 103118. [CrossRef]

[18] Ahutu, O.R.; El-Ocla, H. Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. IEEE Access 2020, 8, 63270–63282. [CrossRef]
[19] Sankara Narayanan, S.; Murugaboopathi, G. Modified secure AODV protocol to prevent wormhole attacks in MANET. Concurr. Comput. Pract. Exp. 2020, 32, e5017. [CrossRef]
[20] Alenezi, F.A.; Song, S.; Choi, B.Y. WAND: Wormhole Attack Analysis using the Neighbor Discovery for Software-defined Heterogeneous Internet of Things. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
[21] Siddiqui, M.N.; Malik, K.R.; Malik, T.S. Performance Analysis of Blackhole and Wormhole Attack in MANET-Based IoT. In Proceedings of the 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), Islamabad, Pakistan, 20–21 May 2021; pp. 1–8.
[22] J. P. Ntayagabiri, Y. . Bentaleb, J. Ndikumagenge, and H. . El Makhtoum,. A Comparative Analysis of Supervised Machine Learning Algorithms for IoT Attack Detection and Classification. J. Comput. Theor. Appl., vol. 2, no. 3, pp. 395–409, Feb. 2025.
[23] Manar J. Gatea,Sarab M. Hameed. An Internet of Things Botnet Detection Model Using Regression Analysis and Linear Discrimination Analysis", Iraqi Journal of Science, vol. 63, no. 10, pp. 4534–4546, Oct. 2022, doi: 10.24996/ijs.2022.63.10.36.
[24] Zalak L. Thakker, Dr. Sanjay H. Buch. Effect of Feature Scaling Pre-processing Techniques on Machine Learning Algorithms to Predict Particulate Matter Concentration for Gandhinagar, Gujarat, India. International Journal of Scientific Research in Science and Technology(IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011,Volume 11, Issue 1, pp.410-419, January-February-2024. Available at doi : https://doi.org/10.32628/IJSRST52411150



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY