Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 8, S. 60-75, 5, 2024

Araştırma Makalesi

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 8, pp. 60-75, 5, 2024

Research Article

https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

A Review of AI-Based Approaches against Wormhole and Blackhole Attacks in AODV Protocol

Zainab Bashar Ibrahim[*], Mayada Faris Ghanim[2]

[1] *Computer Engineering Department/Network Security, University of Mosul, Iraq*

[2] *Computer Engineering Department/Network Security, University of Mosul, Iraq*

[*]*Zainab.en1384@student.uomosul.edu.iq*

(Received: 13 June 2024, Accepted: 25 June 2024)

(3rd International Conference on Frontiers in Academic Research ICFAR 2024, June 15-16, 2024)

ATIF/REFERENCE: Ibrahim, Z. B. & Ghanim, M. F. (2024). A Review of AI-Based Approaches against Wormhole and Blackhole Attacks in AODV Protocol. *International Journal of Advanced Natural Sciences and Engineering Researches*, 8(5), 60-75.

Abstract – A Mobile ad-hoc networks (MANET) is a wirelessly linked network of one or more devices that can configure itself. In a MANET, nodes can exchange data with one another directly or indirectly (via intermediary nodes). Because of the lack of central administration, open media, and several other reasons that make this type of network more vulnerable to security assaults, some researchers are utilizing artificial intelligence approaches in MANET routing to offer security. Several network layer attacks, including the black hole, and wormhole assaults, are covered in this essay. The detection of collaborative network assaults is examined, and frequent multiple network attacks are noted. A few of these assaults' symptoms will be emphasized. A network might exhibit a number of signs and observations that indicate the existence of an attack. The review calls for continued research to refine and deploy AI-based security mechanisms in real-world scenarios, addressing scalability concerns and advancing the vision of self-defending MANETs and wireless sensor networks (WSNs). The review serves as a resource for researchers, practitioners, and policymakers interested in fortifying the security of dynamic wireless networks.

Keywords – MANET, AODV, AI, Blackhole, Wormhole

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are wireless networks without fixed infrastructure, allowing for spontaneous setup and instant data access, analysis, and transportation. These networks are capable of autonomous communication and packet sending/receiving, making them beneficial for large-scale infrastructure due to their lack of permanent infrastructure and ease of neighbor communication. Despite consuming battery power, MANETs enable nodes to connect with other network nodes and intermediary nodes, maintaining their network without fixed points [1] [2]. Due to its adaptability and suitability for scenarios where stable infrastructure is unavailable, MANET is widely used in military operations, disaster relief, business meetings, and mine site operations. Its features include dynamic topology, bandwidth-limited connections, energy constraints, and physical protection [3]. Meanwhile, team assaults, wormholes, jellyfish, black holes, and grey holes can all attack the MANET [4], [5]. Vehicle Ad hoc Networks

(VANETs) is a subclass of Mobile Ad hoc Networks (MANETs), and represent a promising way to implement Intelligent Transportation Systems (ITS). In actuality, ITSs are more well-known for raising traffic safety. Traffic control and safety have a direct impact on the lives of those who use roadways [6]-[8]. Security requirements: The following are some fundamental security prerequisites for safe communication [9]:

- **Confidentiality:** ensures that the communication remains private and is not intercepted by unauthorized parties [10]. That means it exudes confidence. It guarantees that information can only be accessed by a specific entity. Confidentiality is broken if the message is seen by an unauthorized party [9].
- **Authentication:** This means that a message from a reliable source is on its way and is intended for the designated claimed destination node [9].
- **Integrity:** When a communication is comprehensive, whole, and free of corruption, it has integrity. It denotes that an unauthorized entity may never alter a message that has been conveyed [9].

Three classifications are used to classify topology-based routing.

- Proactive (table-driven) routing protocols.
- Reactive (on-demand) routing protocols.
- Hybrid routing protocols (for both types).

A. Ad hoc On-Demand Distance Vector (AODV) Routing protocol

A part of the mobile network's Bellman-Ford remote vector protocol is AODV. It searches routes only when data packets are required, making it reactive and on-demand. Because of its minimal network overhead and loop-free paths, it's an affordable option [11].

- It broadcasts Route Request Packet (RREQ) to all neighbour nodes.
- It is important to remember that RREQ includes the following fields in addition to other pre-defined ones: hop count, source and destination sequence numbers, destination and source addresses, and RREQ ID.
- An intermediate node receives an RREQ, searches its routing table for a path to the destination, and unicasts a route reply (RREP) to the source if it finds one.
- If not, it adds its ID to the RREQ, increases the hop count by one, and then rebroadcasts the RREQ to its neighbour's.
- This process is repeated until the RREQ reaches its destination
- Following many RREPs, the source chooses the route with the greatest sequence number and fewest hops, creates the route, and begins transmitting packets [12].

- creates the route, and begins transmitting packets [12].

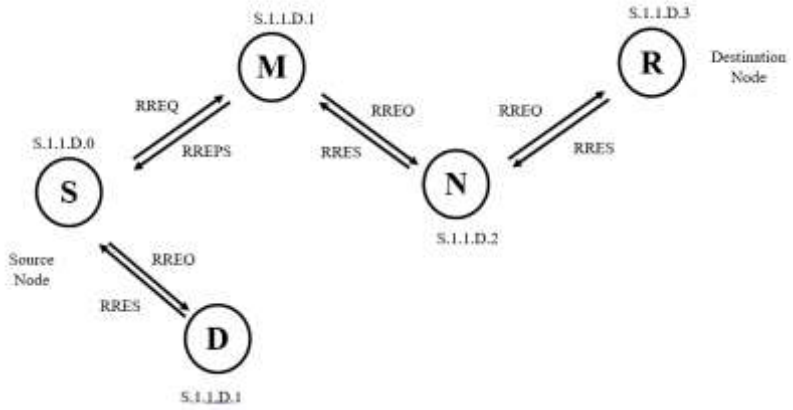

Figure 1: AODV protocol

In RREQ, the use of a sequence number ensures loop freedom. A node looks for an entry to the designated destination in its routing table upon receiving a control message. A new entry is made if none can be found. If the hop count is less than the current hop count, or unknown, but the new sequence number is greater or equal to the destination sequence number, the route is adjusted. To reduce network overhead and prevent RREQ packet flooding, the source employs a Time To Live (TTL) count. Periodically, a HELLO message is broadcast to neighbouring nodes to let them know that you exist. A new RREQ is started when an active node sends an RERR packet to the source node after detecting a route failure [12]. AODV maintains a sequence number and broadcast identity document (ID) for a network consisting of five nodes shown in figure 1. The source node, S, and the destination node, D, are placed at unit distance from each other. Requests are sent from source to destination via route request (RREQ) while answers are sent from destination to source via route response (RRES). The source and destination nodes' IP addresses are known. The following fields serve as the foundation for AODV routing: RREQ (Destination-IP, Destination-Sequence-Number, Source-IP, Source-Sequence-Number, Hop-Count) [13].
Because there is no centralized control, no predetermined boundaries, adversaries within the networks, and limited energy resources, MANET security challenges are extremely difficult to solve. Threats and assaults of many kinds can impact MANETs [14].

II. NETWORK ATTACKS ON MANET

MANETs are susceptible to network layer denial of service (DoS) attacks. These attacks may be divided into two groups: resource use attacks and forwarding interruption and routing disruption attacks. There are two categories of risks to network security: active and passive assaults. While passive attacks track and examine traffic, active attacks circumvent security protocols to get access to data or nodes. Nevertheless, these findings may be utilized to carry out significant network assaults, emphasizing the significance of strong defenses in network security. Attacks from wormholes and black holes are the causes of route disruption. Additionally, forward disruption attacks like jellyfish and directed antenna misuse are included in the category of resource consumption attacks, which also includes control packet flooding and packet injection [15] - [17].

A. Blackhole Attack

Black hole attacks exploit the AODV route discovery process by allowing a malicious node to promote false paths to the source node as feasible routes. The malicious node sends an RREP with a destination sequence number larger than the RREQ message, signaling a new route to the target. This attack dumps the packet without sending it to the destination, imitating the RREQ sent by the source node with a

higher sequence number and shortest path [18] [19]. After the source node chooses this path, the malicious node breaks into the network by intercepting every data sent across it. The communication is entirely discarded by the rogue node [20].

Figure 2 shows a black hole attack scenario, malicious node R responds to source node S with a false RREP message, indicating it has the maximum sequence number of destination node D. Initially, source node S broadcasts the RREQ message for destination node D, rejecting recent packets from intermediate nodes N or M. The malicious node R is targeted by source node S, which assumes the packets will reach destination node D. However, in reality, malicious node R will drop packets and cease forwarding any packets to any further nodes. As a result, the network operation is severely disrupted, as black hole malevolent node B consumes all of the packets [14].

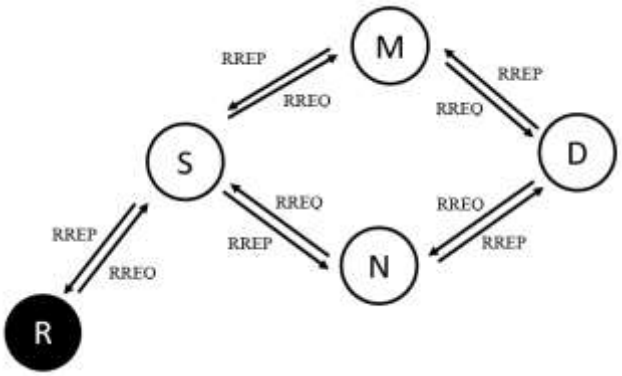

Figure 2: Blackhole Attack

B. Wormhole Attack

Wormhole attacks are highly dangerous network layer attacks where attacker nodes record information and tunnel it to another point, causing damage without network knowledge [21]. The attackers create a tunnel between them, using other network nodes to create an out-of-band or in-band channel. They trick the target node into choosing the route promoted by the attacker, often promoting the tunnel as the preferred route. This method can be used by at least two conspiratorial assailants [22].

An illustration of a common wormhole attack on an ad hoc network is presented in Figure 3 [23]. Attacker D conspires with attacker R to include both D and R as the most effective way towards the route, misleading the destination of a packet about the route. The route between D and R may be selected as the communication path from source to destination as the majority of ad hoc network routing methods choose the most economical way [24].

Node S sends packets to destination node M via normal route and wormhole route. Normal route packets reach destination node M later than wormhole packets, dropping them. Wormhole nodes attract packets by creating false routing between source and destination. Tunneled packets can be dropped, modified, or sent to third parties for malicious purposes. Wormholes are hard to detect and can significantly impact network services like localization, data fusion, and time synchronization. They pose a serious threat in wireless networks, especially against routing protocols [23].

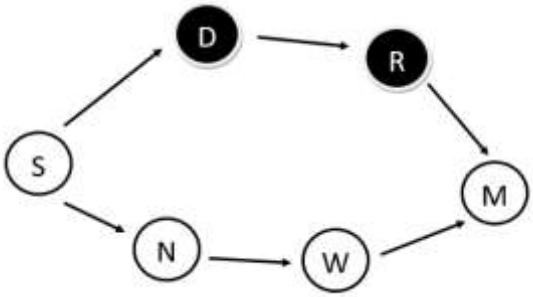

Figure 3: Wormhole Attack

III. Comprehensive Literature

The main aim of all research was to use AI and the AODV protocol to improve network security.

A. *MANET*

An artificial immune system with fuzzy logic was provided in the study of S. J. R. Fotohi et al. [25] study to mitigate wormhole assaults with high FPR and PDR and low PLR. Fuzzy logic was used in the AODV protocol changes to create the system, which developed an immune system. The NS2 simulator was used to model the outcomes. As the number of connections increases, the AODV protocols' delivery ratio falls. Network traffic may cause the shortest path to be lost during the pathfinding process.

A. K. M.S et al. [26] Using the information gathered by the routing protocol and reinforcement learning, this optimization determines the best route from source to destination. During the recognition phase, round trip time and packet delivery rate are important factors to take into account. This setting determines the cutoff point for identifying normal nodes from suspicious ones. The node will either be destroyed or recovered if it turns out to be a malicious node, depending on the type of infiltration. The performance measures that yield the best results among the current approaches are studied and include the percentage of delivered packets (98%), average E2E delay, energy utilization (57J), packet loss (4.75%), end-to-end latency (23.91 sec), and throughput (408/sec). via accounting for the nodes' mobility. Only the proposed work has the ability to recognize wormholes.

The research of A. R. Y. Khalil et al. [27] presented an adding the A* search algorithm to the AODV routing process, the suggested EAODV improves the routing process while making modifications to the regular AODV. The estimate time and hop count value are inputs into the A* algorithm. To safeguard the hop count value, a one-way hash algorithm is employed. The outcomes of the experiment demonstrated that EAODV may protect the network from black hole attacks while simultaneously enhancing network performance.

Fatima-tuz Zahra et al. [28] suggested a hybrid RPL protocol for countering wormhole attacks with high DA while requiring minimal computing power. It detects intruders using a support vector machine, which is a supervised machine learning technique. RPL is a complicated protocol that increases the number of control packets on the network, resulting in higher overhead and energy consumption.

S. A. H. S. Masoud Abdan et al. [29] proposed an approach for mitigating wormholes in MANETs that is based on machine learning. It classifies harmful nodes using KNN, SVM, DT, LDA, NB, and CNN based on attributes that are taken from the nodes' gathered data. All of the approaches' simulations were carried out using MATLAB 2019b. The outcomes demonstrated the excellent detection accuracy—up to 98.9%—that the decision tree (DT) offers.

In the study of M. K. Alaa Althalji et al. [30] suggested technique fends off attacks from black holes and gray holes using fake immunity. Three factors are used by the V-detector method to identify fraudulent RREPs: the number of hops delivered by the malicious node, the life-time parameter, and the discrepancy between the RREP's sequence number and the routing table's sequence number. The packet drop ratio of the suggested protocol, which is 2.683 in big networks and 0.243 in small networks, reduces the impact of the assault. The study comes to the conclusion that the suggested protocol, DAODV, is capable of withstanding assaults, shielding the routing table from inaccurate information updates, and preventing the deletion of data by intruding nodes. On the other hand, the attack-free performance of DAODV is the same as that of AODV.

In research of Zulfiqar Ali Zardari et al. [31], a lightweight strategy for mitigating wormholes in MANETs was described. To identify intruders, the sender nodes gather all reply packets and their sequence numbers, comparing them to the computed average sequence number. In the NS2 Simulator, this lightweight scheme is contrasted with the AODV. The suggested technique offers high throughput, high PDR, low routing overhead, and average latency, according to the results.

D. R. P. Rubi et al. [32] A machine learning technique using SVM-GA classifier is proposed to predict malicious nodes and attacks on MANETs. By identifying healthy and destructive nodes, the technique can predict

attacks on the path, allowing for the creation of protected and sheltered routes. Simulation results show high accuracy of about 85% in ordering and predicting harmful nodes, similar to previous methods for predicting malicious nodes and system invasion.

The research of U. S. Mukul Shukla et al. [33] suggested a wormhole mitigation strategy using elliptic curve encryption. The AODV protocol is employed. In the NS2 simulator, 250 nodes were used for the simulations. The outcomes shown that the proposed crypto method offers low routing overhead, high PDR, low E2E latency, and high throughput.

The AODV protocol was modified by Md Ibrahim Talukdar et al. [14] along with the trust value of the nodes, the IDS-performed detection that needs a time stamp, and the encryption method that uses a digital signature. When changing the number of nodes, packet size, and simulation periods, the analysis is done in terms of PDR, average delay, and overhead ratio. The study found that by increasing the overhead ratio and reducing the delivery ratio, BH-AODV routing significantly reduces AODV performance over a range of factors, such as node count, packet size, and simulation durations. The D-BH-AODV offers more delivery and less overhead than the BH-AODV. The D-BH-AODV routing also shows a lower average latency than the original AODV routing for IDS and digital signatures. This suggests that while the BH-AODV considerably reduces performance, the D-BH-AODV enhances network performance.

The research of M. Al-Shabi et al. [34] presented IDSAODV protocol, that While throughput and average throughput may increase using the IDSAODV protocol, its effectiveness declines as the number of attackers increases. When the attacker node is nearer the source, the performance of the IDSAUDV protocol can be enhanced. Better results are provided by the IDSAODV protocol, although it has a higher routing burden.

This research of Pooja Rani et al. [35] uses an updated AODV routing protocol with SVM and ANN to discover black holes in IoT-MANET pathways and channel them through protected nodes. Enhancing data packet transmission efficiency based on node location, energy consumption, and data transmission latency is the main goal of the research. With an average of PDR, throughput, and latency of 97.96%, 92.78% Kbps, and 0.04 s, respectively, the AODV with ABC, ANN, and SVM method worked well.

For the purpose of identifying floods and blackhole attacks in MANETs, the study of S. V. Shaik Shafi et al. [36] suggests an Effective Machine Learning-Based Secure AODV routing system (ML-AODV). By employing an ANN with SVM classifier to increase intrusion detection accuracy and throughput, the approach enhances secure communication. Because of its dynamic node density and speeds, the ML-AODV is appropriate for information sharing in semi-urban regions but not in fully urban ones. The effectiveness is evaluated in comparison to current trust-based and standard AODV procedures.

Ashutosh Vashist et al. [37] uses AODV and neural networks to identify and stop malicious attacks in mobile ad hoc networks (MANETs). Enhancing the security and dependability of mobile ad hoc networks is the goal of this field of research. The results offer important new information about the efficacy and precision of the Neural Network and AODV combination in identifying and stopping malicious attacks, which will help shape the creation of better security protocols and procedures.

The study of Xuetao Jia et al. [38] presents the use of machine learning models based on Multi-Tier honey pot analysis with stacked reinforcement learning (MHSRL) and linear gradient Distance Vector dynamic Mamdani routing system (LGDVDMR), the research offers a novel method for MANET routing and security analysis. With up to 39 hidden nodes and a learning rate of 0.001, the results demonstrate promising outcomes when utilizing deep learning neural networks. The research intends to keep enhancing the suggested IDS in order to identify additional attacks in MANETs via the DL technique and deal with problems related to zero-day attack detection.

By utilizing an accurate map, Shahjahan Ali et al. [39] presented a supervised machine learning technique for highly accurate wormhole attack detection in VANETs. By employing K-nearest neighbor and random forest classifiers, the system effectively detected malicious nodes. In order to counteract wormhole assaults, the paper also presents a method that combines packet leash with cryptographic concepts. Simulation findings showed that the developed detection strategy may achieve up to 99.1% detection accuracy.

Using machine learning approaches, the research of ALMAMOORI et al. [40] investigates embedded network use and evaluates findings. The accuracy of the suggested methods was 74% in 27 seconds for CBPNN, 82% in 18 seconds for FFNN, and 85% in 17 seconds for CNN. The CNN algorithm produced the greatest results, which improved the end-to-end decrease and average receiving packet. When comparing the model to another research, the CNN algorithm outperformed the earlier CNN implementation, achieving 82% accuracy and 99% detection rate. Moreover, the BLSTM and DBM algorithms yield 75% and 66% accuracy and detection rate (67% and 54% DR). Last but not least, another author employed the same model (CNN) and reported 80% DR and 77% accuracy.

According to the research of V Harsha Shastri et al. [41] nearly all researchers employ fuzzy logic as a classification method, which results in strong measurement. ANN addresses these problems and offers a stable black hole attack; ANN modeling was investigated for the purpose of detecting black hole assaults. Input data for neural network training was obtained by utilizing end-to-end latency, packet distribution ratio, and throughput.

Marjan Kuchaki Rafsanjan et al. [42] proposes a novel routing protocol called VRU, which supports ad hoc routing between vehicles and UAVs and between UAVs themselves. It consists of two protocols: VRU-vu for communication between vehicles and UAVs and VRU-u for communication between UAVs. The protocol uses UAVs to appraise vehicle density, detect malicious vehicles, select appropriate routes for data transmission, and apply UAVs to route packets when vehicle density is insufficient. Simulation results show VRU is suitable for urban scenarios, improving packet delivery ratio by 16%, reducing

overhead by 40%, and reducing end-to-end delay by an average of 13%. However, VRU is only suitable for urban scenarios and is vulnerable to malicious UAV intrusion.

Table 1: Summary of Analysis

Ref.	Year	Technique	Improvement
[25]	2016	artificial immune system with fuzzy logic	FRR and PDR and PLR
[26]	2023	Quantum walk and reinforcement learning	delivered packets (98%), end-to-end latency (23.91 sec), packet loss (4.75%), energy use (57J), throughput (408/sec)
[27]	2013	A* algorithm	Minimize the Average End-to-End Delay about 8% and PDR about 33% packets.
[28]	2020	SVM	control packets and energy consumption
[29]	2021	ML, KNN, SVM, DT, LDA, NB and CNN	accuracy for KNN = 97.1%, SVM = 98.2%, DT = 98.9%, LDA = 95.2%, NB = 94.7%, and CNN = 96.4%
[30]	2019	V-detector method	PDR = 97.134% it was 27.511%, Packet Drop Ratio = 0.243% it was 65.864%, throughput = 287.738% it was 81.495%, PLR = 2.612% it was 6.620%, Delay = 0.168% it was 0.518%
[31]	2020	Lightweight technique	throughput increased = 83\%, PDR, routing overhead, and average latency
[32]	2020	SVM-GA classifier	high accuracy about 85%
[33]	2021	Elliptic curve cryptography scheme	throughput enhancement of 188.39 kbps, high PDR, less E2E delay about 325.55ms, and routing overhead = 69.26%, Energy consumption is around 72.46%
[14]	2021	IDS and the encryption method that uses a digital signature	PDR, delay, overhead ratio
[34]	2022	IDS	PDR improved to 68%
[35]	2022	SVM and ANN	average of PDR, throughput, and latency of 97.96\%, 92.78\% Kbps, and 0.04 s, respectively the AODV with ABC, ANN, and SVM method worked well.
[36]	2023	ANN with SVM classifier	10% less packet loss, throughput is 3%, 4% higher, 12%, 15% less delay, reliability is 44% higher.
[37]	2023	Nural network	Throughput achieving over 99.9% success rate, PDR above 99.8%, E2Edelay ranging from 0.1- 0.2 seconds,
[38]	2023	machine	throughput 96%, trust analysis 98%, end-end delay 59%, PDR

		learning models based on Multi-Tier honey pot analysis with MHSRL and LGDVDMR	79%.
[39]	2022	Random forest and K-nearest neighbor classifiers	accuracy of up to 99.1%
[40]	2023	machine learning (FFNN, CBPNN, CNN, BLSTM, DBM and DR)	The accuracy of CBPNN = 74% in 27 seconds, FFNN = 82% in 18 seconds, CNN = 85% in 17 seconds, the BLSTM = 75% and DBM algorithm = 66% and detection rate DR = 67% and 54%.
[41]	2021	fuzzy logic, and ANN	throughput increases with ANN about 11.12%, PDR = 4.68%
[42]	2021	Unmanned Aerial Vehicles (UAVs)	Improves the PDR by 16% and decrease the overhead by 40%, end-to-end delay by an average of 13% and detection ratio by 7%.

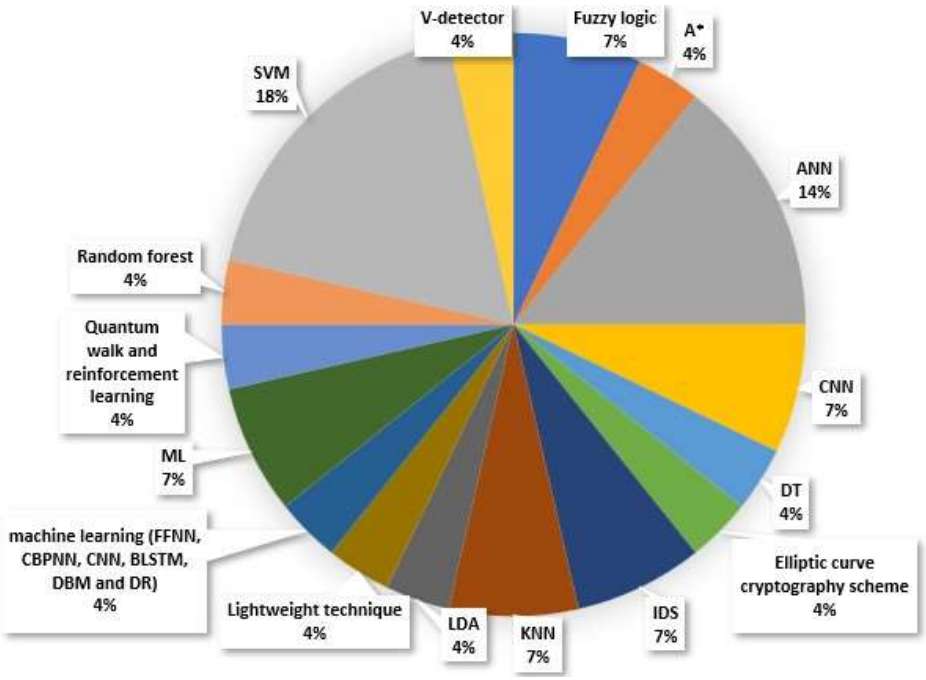

Figure 4: Statistics of AI techniques at MANET

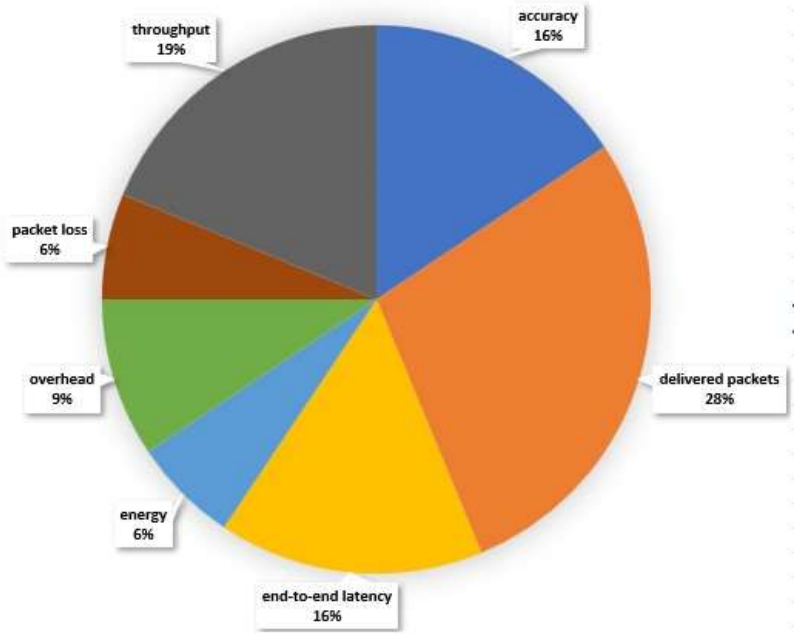

Figure 5: Parameters Statistics

Advantages and Disadvantages

1) *Fuzzy Logic:*

- **Advantage**: is a useful tool for detecting attacks in MANET due to its ability to model complex relationships between variables and handle imprecise information. Systems like the Mamdani fuzzy-based inference system (MFIS) [43] estimate trust values and classify attacks based on multiple QoS parameters [44]. Fuzzy logic can be combined with other machine learning techniques like Principal Component Analysis (PCA) and Fuzzy Extreme Learning Machine (FELM) to improve accuracy and performance in detecting attacks [45] [46].

- **Disadvantage:** Fuzzy logic's effectiveness in detecting MANET attacks is limited due to its inability to identify gray hole attacks [44], causing packet drop rates and network performance issues. To address this, additional QoS metrics and the Kullback-Leibler divergence method are used [45], preventing both black hole and gray hole attacks simultaneously, improving network security [46].

2) Support Vector Machine (SVM):

- **Advantage:** For highly accurate intrusion detection in a network, the SVM is the best option, SVM is used to identify trespassers who cross the route [36]. May be used to do regression and classification [47], the thorough analyses of the literature that are provided make it abundantly evident that the SVM-based SRA is receiving a lot of attention because to its exceptional capacity to handle high dimensional issues with fewer samples [48].

3) Artificial Neural Networks (ANNs):

- **Advantage:** Mobile Ad hoc Networks (MANETs) employ Artificial Neural Networks (ANNs) for security. ANNs are a kind of deep learning method that has the ability to recognize and anticipate intrusion attempts in MANETs.
  They can offer a greater level of protection and are efficient in spotting unusual invasive activity [49]. ANNs are used to build a system for categorizing and forecasting cyberattacks in MANETs and to optimize pre-processed data. They are capable of efficiently identifying and categorizing intrusions, ensuring safe data transfer, and stopping hacker assaults [50].
- **Disadvantage:** Employing ANNs for security in MANETs has several drawbacks. One drawback is that MANET hardware resources are limited, which may have an impact on ANN performance. Furthermore, because ANNs rely on training data and may find it difficult to recognize unusual intrusive behaviour, they may not be able to detect assaults in MANETs that have not yet been seen or identified [49]. Consequently, even though ANNs have demonstrated promise in raising the overall security level of MANETs, their efficiency may be constrained by hardware limitations and their limited capacity to identify undiscovered threats.

B. *WSN*

An ANN method for mitigating wormholes was presented by Moirangthem Marjit Singh et al. [51]. Hop counts are calculated using the connection data of sensor nodes as a distance metric. MATLAB was used to run the suggested approach's simulations on 500 nodes. The training and testing results of the ANN demonstrate that this method can detect wormholes without the need for extra hardware and with a high detection accuracy of up to 97%.

Fuzzy logic combined with a feed-forward neural network is a unique intrusion detection system that was presented by Ezhilarasi et al.'s research [52]. The neural network is trained using fuzzy rules, and simulation was performed to assess the neural network's performance. When the outcomes were compared to basic machine learning methods, it became clear that this innovative strategy offers a detection accuracy of up to 98.8%.

The research of Lakshmi Narayanan et al. [53] proposed a supervised machine learning-based technique for detecting malicious nodes that combines the improved code-based round trip time (EC-BRTT) with a naïve Bayes classifier. Effective outcomes in terms of data latency, attack detection, and communication overhead were demonstrated by the simulation of the method that was provided.

Five scenarios totalling 25 nodes were simulated by Sana AKOURMIS et al. [54], and one to five malicious nodes were added to each scenario. The findings shown that important packets are rejected and packet latency becomes intolerable in the event of a black hole assault. To lessen the consequences of black holes, the authors investigated an IDS solution in a WSN model. The findings shown that while throughput rises, the introduction of rogue nodes reduces the routing protocol's (AODV) performance under black hole attacks. In the sensor network, the IDSHNAODV solution dramatically lowers packet loss and the effects of black hole assaults.

Pratik Gite et al. [55] proposed a machine learning technique for intrusion detection that is supervised. To find network patterns, it employs decision tree techniques called C4.5 and CART. A comparison was made between the suggested approach's outcomes and several network metrics, including accuracy, node count, training sample count, and attacker count. As a consequence, C4.5 outperformed the CART classifier in accuracy, achieving a 70% rating.

The study of Xiao Luo et al. [56] suggested a method that used less energy, required no extra hardware, and had a greater detection accuracy. It is suggested to use the localized Credible Discovery Networking Protocol (CREDND). It is capable of identifying wormholes both within and outside the network. The accuracy of the previously developed SECUND and SEINE techniques—which also

make use of hop difference and local monitoring—was contrasted with that of the proposed approach, CREDND. When nodes' communication ranges changed dynamically, CREDND could not function properly.

Amit Kumar Roy et al. [57] suggested a new technique that offers good detection rates for wormhole attack detection in wireless mesh networks. The propagation time and the round-trip time (RTT) approach were combined in the proposed protocol. To evaluate the efficacy of the suggested methodology, four distinct scenarios with varying numbers of nodes were simulated using NS3 simulators. Network traffic was preventing the RTT from proceeding. The efficiency of the RTT is impacted and the RTT is increased when a server requests an increase. When network traffic causes a node to become congested, the RTT also rises as a result of the connection being slower. The RTT rises with the distance between nodes.

Table 2: Summary of Analysis

Ref.	**Year**	**Technique**	**Improvement**
[51]	2021	ANN	Accuracy up to 97\%
[52]	2023	fuzzy logic with a feed-forward neural network	Accuracy up to 98.8%
[53]	2022	naıve Bayes classifier with EC-BRTT (enhanced code-based round trip time for detection	communication overhead, data delay, and attack detection.
[54]	2023	IDS	End-to-End Delay, Throughput, Energy, Packet loss
[55]	2023	Decision tree algorithms named C4.5 and CAR	C4.5 attained a higher accuracy (70%) than the CART classifier and CNN = 96.4%
[56]	2020	CREDND protocol	
[57]	2020	Round-trip time (RTT) method	C4.5 attained a higher accuracy (70\%) than the CART classifier.

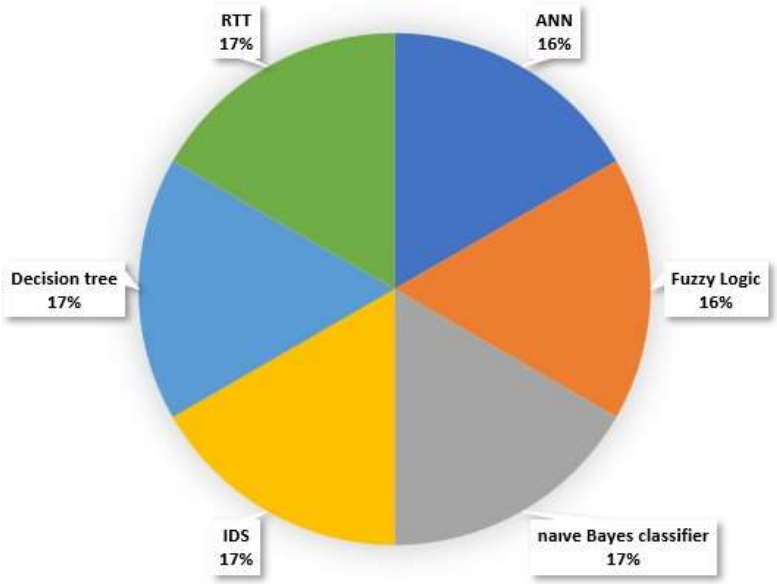

Figure 6: Statistics of AI techniques at WSN

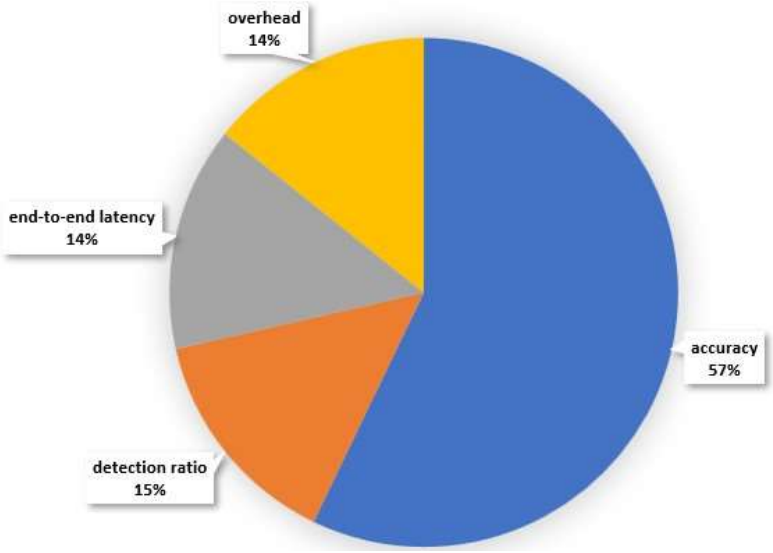

Figure 7: Parameters Statistics

IV. CONCLUSION

This review paper explores the security challenges of Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs), focusing on the prevalence of malicious attacks like wormhole and blackhole attacks. The Ad Hoc On-Demand Distance Vector (AODV) protocol provides insights into its strengths and vulnerabilities. The evolving wireless communication landscape demands robust security mechanisms to ensure data transmission integrity and confidentiality. The identified threats, such as wormhole and blackhole attacks, can compromise the performance and reliability of MANETs and WSNs. The integration of Artificial Intelligence (AI) techniques is seen as a promising avenue for enhancing the security posture of these networks. AI algorithms offer a proactive approach to detect and mitigate security threats, and leveraging AI in conjunction with traditional security measures can fortify the resilience of MANETs and WSNs against emerging and sophisticated attacks. Future research should focus on refining

AI-based security mechanisms. These articles provide valuable insights on how to use AI and the AODV protocol for network security.

REFERENCES

[1] M. M. K. K. Amarjeet Singh, Tripatdeep Singh, "Performance improvement in aodv routing protocol with artificial intelligence" Research gate, p. 5, 2016.

[2] S. G. VIVEK MANKOTIA, RAMESH KUMAR SUNKARIA, "Dt- aodv: a dynamic threshold protocol against black-hole attack in manet," Indian Academy of Sciences, p. 14, 2023.

[3] N. V. K. RAJYALAXMI, M. ANUSHA, "Survey of ai techniques in manet routing," INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY, p. 6, 2022.

[4] S. Z. D. S. Fasunlade, Olufemi, "Comprehensive review of collaborative network attacks in manet," pp. 1542–1545, 2020.

[5] M. O. N. D. A. T. Hammamouche, Assia, "Lightweight reputation-based approach against simple and cooperative black-hole attacks for manet," Journal of information security and applications, pp. 12–20, 2018.

[6] A. H. A.-B. H. Z. Saif Al-Sultan, Moath M. Al-Doori, "A comprehensive survey on vehicular ad hoc network," p. 37, 2014.

[7] C. B. c. A. L. Hamssa Hasrouny a b, Abed Ellatif Samhat b, "Misbehavior detection and efficient revocation within vanet," p. 46, 2019.

[8] M. K. R. Hamideh Fatemidokht, "F-ant: An effective routing protocol for ant colony optimization based on fuzzy logic in vehicular ad hoc networks," p. 29, 2018.

[9] A. M. T. V. Y. A. K. R. U. K. M. R. Vimal Kumar, Mahima Shanker, "Prevention of blackhole attack in manet using certificateless signature scheme," 2021.

[10] M. v. S. Andrew S. Tanenbaum, Distributed Systems: Principles and Paradigms, 2nd ed., 2007.

[11] A. J. A. K. Namit Gupta1, Kunwar Singh Vaisla and R. Kumar, "Performance evaluation of aodv routing protocol in vanet with ns2," International Journal of Interactive Multimedia and Artificial Intelligence, p. 5, 2017.

[12] Y. H. Jazyah, "Enhancing the performance of wireless routing protocols of manet using ai," Journal of Computer Science, p. 8, 2021.

[13] A. J. A. K. R. K. Namit Gupta, Kunwar Singh Vaisla, "Performance analysis of aodv routing for wireless sensor network in fpga hardware," p. 13, 2021.

[14] M. S. H. K. A. F. Q. a. A. S. A. Md Ibrahim Talukdar, Rosilah Hassan, "Performance improvements of aodv by black hole attack detection using ids and digital signature," Wireless Communications and Mobile Computing, p. 13, 2021.

[15] S. K. K. Raj Kamal Kapur, "Analysis of attacks on routing protocols in manets," p. 5, 2015.

[16] K. M. Nidhi Purohit, Richa Sinha, "Simulation study of black hole and jellyfish attack on manet using ns3," p. 14, 2011.

[17] M. R. Manmohan Sharma, "Security attacks in manet – a comprehensive study," p. 6, 2020.

[18] N. M. O. H. M. Ibrahim and E. K. William, "Detection and removal of gray, black and cooperative black hole attacks in aodv technique," p. 6, 2015.

[19] N. A. O. M. Olanrewaju, A. A. Abdulwasiu, "Enhanced on-demand distance vector routing protocol to prevent blackhole attack in manet," INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING COMPUTER SYSTEMS (IJSECS), p. 8, 2023.

[20] T. Kaur, "Mitigation of blackhole attacks and wormhole attacks in wireless sensor networks using aodv protocol," Conf. Smart Energy Grid Eng, 2018.

[21] D. G. R. C. P. Sandeep Kumar, Monika Goyal, "Routing protocols and security issues in manet," International Conference on Infocom Technologies and Unmanned Systems, p. 7, 2017.

[22] P. V. T Divya Sai Keerthi, "Confirmation of wormhole attack in manets using honeypot," p. 30, 2018.

[23] S. P. Jegan Govindasamy, "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack," Electrical Systems and Information Technology, p. 10, 2018.

[24] D. S. Juhi Biswas, Ajay Gupta, "Wadp: A wormhole attack detection and prevention technique in manet using modified aodv routing protocol," p. 6, 2014.

[25] S. J. R. Fotohi, "Defending against wormhole attack in manet using an artificial immune system," New Review of Information Networking, p. 21, 2016.

[26] A. K. M.S, "An adaptive technique for wormhole attack detection in manet using quantized ad-hoc on-demand multipath distance vector routing protocol," SPIE, p. 23, 2023.
[27] A. R. Y. Khalil I. Ghathwan and R. Budiarto, "Eaodv: A*-based enhancement ad-hoc on demand vector protocol to prevent black hole attacks," p. 7, 2013.
[28] S. N. B. N. A. M. M. H. Fatima-tuz Zahra, NZ Jhanjhi, "Proposing a hybrid rpl protocol for rank and wormhole attack mitigation using machine learning," International Conference on Computer and Information Sciences (ICCIS), p. 6, 2020.
[29] S. A. H. S. Masoud Abdan, "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (manet)", Wireless Communications and Mobile Computing, p. 12, 2021.
[30] M. K. Alaa Althalji, Souheil Khawatmi, "Improving the security of aodv protocol using v-detector algorithm," p. 8, 2019.
[31] R. A. S. S. D. I. A. Zulfiqar Ali Zardari, Kamran Ali Memon, "A lightweight technique for detection and prevention of wormhole attacks in manet," p. 6, 2021.
[32] D. R. P. Rubi, "A wormhole attack detection in mobile ad-hoc network using ga and svm", p. 7, 2020.
[33] U. S. Mukul Shukla, Brijendra Kumar Joshi, "Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in manet", Wireless Personal Communications, p. 24, 2021.
[34] M. Al-Shabi, "Performance ameliorations of aodv by black hole attack detection utilizing idsaodv as well as reverse aodv", International Journal of Communication Networks and Information Security, p. 12, 2022.
[35] S. V. N. K. M. W. J. S. M. F. I. Pooja Rani, Kavita, "Robust and secure data transmission using artificial intelligence techniques in ad-hoc networks," Sensors, p. 22, 2022.
[36] S. V. Shaik Shafi, S Mounika, "Machine learning and trust based aodv routing protocol to mitigate flooding and blackhole attacks in manet", p. 10, 2023.
[37] D. R. S. S. Ashutosh Vashist, "A techniques for security in manet: A combined approach of neural network and aodv for malicious attack detection and prevention," Industrial Engineering Journal, p. 13, 2023.
[38] N. Q. Xuetao Jia, Donggui Huang, "Ai-enhanced security demand and routing management for manets with optical technologies," p. 19, 2023.
[39] S. T. Shahjahan Ali, Parma Nand., "Detection of wormhole attack in vehicular ad-hoc network over real map using machine learning approach with preventive scheme", p. 20, 2022.
[40] Z. A. A. ALMAMOORI, "Embedding intrusion detection in distributed computing artificial intelligence-based routing in ad hoc networks," p. 108, 2023.
[41] V. K. N. G. S. P. K Srinivas, V Harsha Shastri and P. R. Kumar, "Discernment and diminution of black hole attack in mobile ad-hoc network using artificial intelligence," Journal of Physics: Conference Series, p. 18, 2021.
[42] B. B. G. C.-H. H. Hamideh Fatemidokht, Marjan Kuchaki Rafsanjan, "Efficient and secure routing protocol based on artificial intelligence algorithms with uav-assisted for vehicular ad hoc networks in intelligent transportation systems," p. 22, 2021.
[43] A. J. J. Arthi and B. S. Brett Beno, "Fuzzy based inference system with ensemble classification based intrusion detection system in manet", Journal of Intelligent and Fuzzy Systems, pp. 1–8, 2023.
[44] K. O. Murray, "Fuzzy based intrusion detection system in manet", Measurement: Sensors, p. 26, 2023.
[45] S. Maheswari and R. Vijayabhasker, "Fuzzy reputation-based trust mechanism for mitigating attacks in manet," Intelligent Automation Soft Computing, p. 35, 2023.
[46] K. E. S. S. K Bala, J Paramesh, "An intrusion detection system for manet to detect gray hole attack using fuzzy logic system," IEEE, 2023.
[47] A. S. S. K. G.-S. H. A. A. S. Subhankar Ghosh, Anuradha Banerjee, "Efficient selfish node detection using svm in iot-manet environment", WILEY, p. 25, 2022.
[48] S. C. Atin Roy, "Support vector machine in structural reliability analysis: A review," ELSEVIER, 2023.
[49] M. A. K. Mohamad T Sultan, Hesham El Sayed, "An intrusion detection mechanism for manets based on deep learning artificial neural networks (anns)," International Journal of Computer Networks Communications (IJCNC), p. 15, 2023.
[50] M. O. Wafa Bouassaba, Abdellah Nabou, "Review on machine learning based intrusion detection for manet security," IEEE, 2022.

[51] T. R. S. U. N. Moirangthem Marjit Singh, Nishigandha Dutta, "A technique to detect wormhole attack in wireless sensor network using artificial neural network," p. 10, 2021.
[52] A. K. M. S. M. Ezhilarasi, L. Gnanaprasanambikai, "A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks," p. 9, 2023, https://doi.org/10.1007/s00500-022-06915-1.
[53] E. G. J. Y. H. R. . V. S. K. Lakshmi Narayanan, R. Santhana Krishnan, "Machine learning based detection and a novel ec-brtt algorithm based prevention of dos attacks in wireless sensor networks," p. 24, 2022.
[54] M. D. R. Sana AKOURMIS, Youssef Fakhri, "Protecting aodv protocol from black hole attack in wsn," p. 21, 2023.
[55] K. M. K. C. K. N. M. S. A. S. Pratik Gite, Kuldeep Chouhan, "ML based intrusion detection scheme for various types of attacks in a wsn using c4.5 and cart classifiers," p. 7, 2023.
[56] Q. L. K. X. S. L. L. C. Xiao Luo, Yanru Chen; Miao Li, "Crednd: A novel secure neighbor discovery algorithm for wormhole attack," 2020.
[57] A. K. K. Amit Kumar Roy, "Rtt based wormhole detection for wireless mesh networks," p. 7, 2020.