IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Survey of Various Black hole Attack Detection Techniques in MANET

Gaurav Mehta
Assistant Professor
CSE Deptt, UIE
Chandigarh University
Mohali,India

Abstract : A blackhole attack in Mobile Ad Hoc Networks (MANETs) represents a significant security threat, exploiting the network's routing protocol to intercept and discard data packets. In such an attack, a malicious node advertises itself as having the shortest path to the destination node, thereby attracting all the surrounding nodes' traffic. Once the data packets are rerouted through the blackhole node, it can drop the packets or misuse the information. This attack severely compromises the network's integrity, confidentiality, and availability. MANETs, characterized by their dynamic topology, decentralized nature, and lack of a fixed infrastructure, are particularly vulnerable to such attacks. Detection and prevention of blackhole attacks are challenging due to the network's inherent properties. Various defense mechanisms have been proposed, including trust-based methods, anomaly detection systems, and secure routing protocols.

Keywords

MANET, Black Hole, Malicious, Trust Based Mechanism

1. Introduction

A self-configuring network which is made up of several mobile user devices is called MANET (Mobile adhoc network). In addition to communicating with one another without the need for infrastructure, all of the transmission links are located by using the wireless medium. MANET is extensively used in military purpose, disaster area, personal area network and so on according the communication node mentioned earlier. Still there are many unresolved problems about MANETs which caused processing capabilities [1][2], such as security problem, finite transmission bandwidth, abusive broadcasting messages, reliable data delivery, dynamic link establishment and restricted hardware. In wired and wireless networks, the security threats have been extensively examined and addressed and because of intrinsic design flaws, the similarly perplexing situation has also arisen in MANET. Recently, a lot of issues related to security have been studied. Examples include snooping attacks, wormhole attacks, black hole attacks, routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, et cetera. Particularly, one of the most serious attacks faced by the adhoc networks is the Blackhole (BH) attack [3][4]. An attacking node target data packets to itself in BH attacks and intercepts or discards them. It is important to make sure that the security is trustworthy when designing an adhoc network.

A denial of service (DoS) attack, known as a blackhole attack, involves intercepting or discarding data packets as they travel from a source node to a destination node. The blackhole (BH) node achieves this by capturing a Route Request (RREQ) and responding with a counterfeit Route Reply (RREP) containing a bogus sequence number [5][6]. This deceives the source node into routing packets through the BH node, which then consumes the packets, causing a significant decline in throughput and packet delivery rate. The blackhole node's use of fake RREPs to divert data packets to itself is

illustrated in Figure 1, where B represents the malicious node.

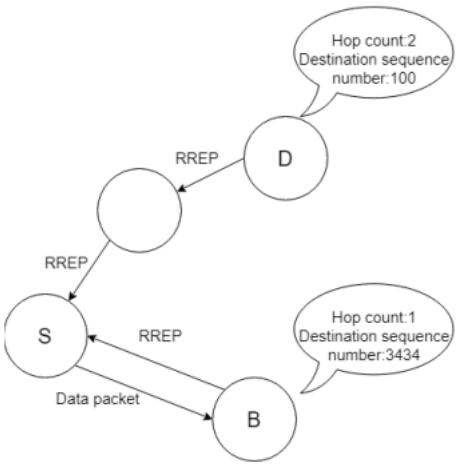

Fig. 1 Blackhole attack

Step1: Transmission of a spoofed RREP: Upon receiving a Route Request (RREQ), the blackhole (BH) node sends a counterfeit Route Reply (RREP). This fake RREP contains a sequence number higher than the actual one and lists a minimal number of hops. The recent and most stable route in AODV is thought to be the one with the maximum sequence number [7][8]. By exploiting this vulnerability and assigning a high sequence number, standard blackhole (BH) attacks ensure that the route incorporating the BH node is perceived by the surrounding nodes as the most recent and reliable path.

Step 2: Data packet routing: The BH node sends the forged RREP to the source node. Upon receiving this information, the source node presumes that the path that contains the malicious node is the most recent path with the fewest hops. Consequently, data packets are sent to the malevolent node by the source node [9][10].

1.1 Existent Defence methods and smart BH attacks

In MANETs, BH assaults pose a serious concern, often leading to severe performance degradation and, in extreme cases, network failure. Present-day networks can use an authentication control header to restrict anonymous node membership in a MANET. The aim of this approach is to efficiently prevent malevolent nodes from entering and damaging the network. Nevertheless, in energy-sensitive networks like wireless sensor networks, repeated security key trade-off can greatly reduce performance. Therefore, some networks might decide against using these security measures [11][12].

Employing a blackhole (BH) detection method can often lead to reduced overhead compared to using security authentication techniques. Some defence strategies identify the presence of BH nodes by utilizing a fake RREQ. This method operates on the principle that a BH node will immediately respond to an RREQ with a RREP. Nodes that respond to a fake RREQ with an illusionary address are then identified as BH nodes. However, smart BH nodes can partially infer the existence of the destination address and easily bypass this defence strategy. Other existing protection strategies against blockhole assaults primarily include thresholding sequence numbers. RREP signals with a significant sequence number value are produced by typical BH attacks [13][14]. Thus, merely restricting the sequence numbers can aid in thwarting these attacks. Figure 2 illustrates this kind of defence strategy, which is referred to as threshold-based defence.

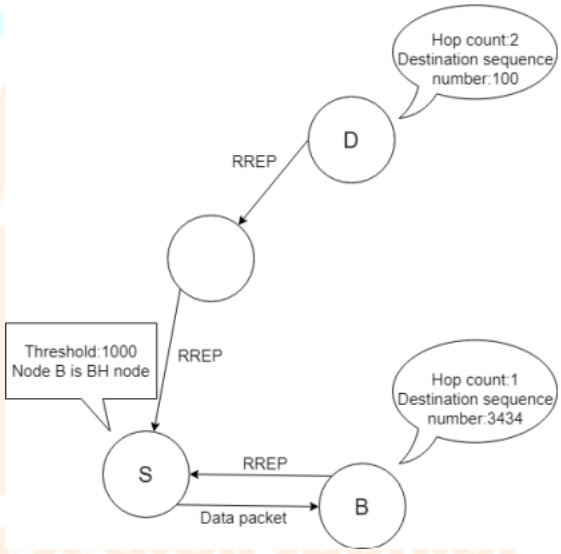

Fig. 2 Threshold defence method

In this scenario, node S sets a threshold for sequence numbers at 1000. Node D is recognized as secure by nose S because the sequence number of RREP generated by this node is 100, which is below the threshold. Node S identifies node B as a blackhole (BH) node and discards its next RREPs because node B's RREP has a sequence number of 3434, which exceeds the threshold. Nevertheless, this security strategy overlooks the possibility that a BH node could conduct a smart attack by wisely setting its sequence numbers to avoid detection. Smart blackhole (BH) assaults can circumvent threshold-based defense methods by observing the sequence numbers in received RREQs and making predictions about the real sequence number values partially. This is achieved using methods like the least-squares technique also known as dynamic threshold attack [15][16]. It is plausible to believe that many defence strategies resembling threshold-based defences can be circumvented by smart blackhole (BH) attacks.

Several studies have demonstrated ineffectiveness against advanced BH attacks while being successful against standard BH attacks. WSN security is essential, and defence strategies need to be able to identify and stop BH attacks even in cases when the attackers may anticipate sequence numbers.

2. Literature review

J. Vinayagam, et al. (2019) introduced the Integrated Cross Interior (ICI) structure for Intrusion Detection System (IDS), specifically ICIs for IDS, to enhance the accuracy of detecting black hole attacks [17]. The ICIs for IDS handled the routing of mobile nodes, ensuring secure communication and distributing packets among destinations on the basis of priority. This method was developed from the suggested ICIs for IDS, which improved the Intrusion Detection System (IDS). To protect the network from black hole attacks, this study introduced a novel Integrated Cross Interior structure for Intrusion Detection System (ICIS for IDS). The approach was introduced for node routing and safety, achieving a minimal routing cost, 6.3 ms of response time and a maximal throughput of 83.5%. Testing results demonstrated that compared to other current approaches like IDS with AODV, security policies leveraging ICIs for IDS significantly reduced response times and mobile routing costs. This work used Network Simulator-2 to evaluate the suggested algorithm, showing superior performance over traditional algorithms such as IDS with AODV.

T. Terai, et al. (2020) utilized an extremely destructive BH attack capable of predicting sequence numbers, which surpassed conventional detection strategies, relying on setting sequence number thresholds [18]. This work presented a detection and prevention approach that leveraged local data exchanged with nearby nodes to counter this type of BH attack. The experimentation verified that this method effectively detected and mitigated even sophisticated BH threats, resulting in a decrease in attack success rates. The future goals for this work will include refining the devised approach to reduce the Fault Detection Rate (FDR) and developing an adaptive approach capable of adjusting dynamically to various situations.

E. Elmahdi, et al. (2020) introduced a novel solution to enhance the reliability and security of data transmitted in Mobile Ad-hoc Networks (MANETs), particularly under potential blackhole attacks. For this purpose, this work used an advanced version of the ad-hoc on-demand multipath distance vector (AOMDV) protocol [19]. Their approach involved dividing messages into manifold routes towards the destination and employing a cryptography approach based on homomorphic encryption. The efficacy of the introduced approach demonstrated a steady and significantly high PDR (packet delivery ratio), whereas the original AOMDV was discovered to be susceptible to attack by spiteful nodes in the network. Simulation outcomes indicated a considerable improvement in PDR and network throughput by the presented approach in comparison to the standard AOMDV approach even when malevolent nodes were present. Future research will concentrate on minimizing end-to-end delay to implement this approach effectively in critical applications in MANETs.

P. R. B, et.al (2021) recommended protocol integration for OSPFV (for wireless LANs) with integral security, using threshold evaluation and cryptographic verification [20]. This paper simulated two protocols, the blackhole attack and the proposed AODV-BS protocols, on various MANET models. Two network metrics, namely Network Packet Delivery Ratio and normalized Out of Routing Overhead Utilization and Network Delay, were computed, and their performance was analyzed to determine the outcome. The focus of this study was on countering internal attacks only. Future research can extend this work by incorporating a cryptography-based security framework to defend against external attacks.

E. Lema, et al. (2022) suggested a trust-based technique to shield the network from blackhole attacks [21]. The behaviour of a blackhole node and a trust-based security method were presented in this research. Additional suggested technique was investigated and assessed in relation to several assessment metrics, such as attack %, PDR, throughput, and end-to-end delay. Three distinct scenarios, including attack, watchdog, and intrusion detection system scenarios, were evaluated with the suggested security approach utilizing the evaluation criteria mentioned above. The comparison showed that the recommended trust-based security guaranteed real-time data transfer as well as identification and prevention against blackhole nodes during route discovery.

R. Gotti, et al. (2023) outlined MANETs as providing wireless connectivity between devices independent of centralized management or stationary infrastructure [22]. Due to the ease with which intruders might access MANETs, security is a major concern. An efficient intrusion detection system (IDS) is necessary for identifying and detecting breaches, such as blackhole assaults, in order to address this problem. This study presented a novel method that simulates a network of 25 nodes connected by TCP and UDP and gathers various

statistics from trace files. Several machine learning methods were then used to assess these features.

S. Shafi, et al. (2023) presented a Machine Learning and Trust-Based AODV Routing Protocol (ML-AODV) aimed at mitigating Flooding and Blackhole Attacks in MANETs [23]. The protocol selected cooperative intermediate nodes in the network by estimating trust level at each node to prevent redundant transfer of routing packets (flooding attack) to illusionary endpoints. To identify the finest routes with the lowest PDR, the protocol selected nodes with the maximum trust values as trusted relay senders to combat Blackhole attacks. Additionally, it utilized a machine learning-reliant approach, combining Artificial Neural Network (ANN) and Support Vector Machine (SVM) classifiers, to determine the best path that minimized energy disproportion and packet transfer delay. To enhance productivity and accuracy in intrusion detection, SVM was employed to identify intruders along the chosen route. This work used NS-2 to examined the efficacy of the presented ML-AODV and compared it with other vulnerable routing systems. Simulation results indicated that the proposed approach demonstrated boosted reliability by 44% and throughput by 4% compared to previous methods. Additionally, reductions in delay, routing overhead, and packet loss ratio by 12%, 15%, and 10%, respectively, were achieved.

Ramesh Vatambeti, et al. (2024) introduced a novel framework for detecting and preventing intrusionsin MANET. This framework leveraged machine learning techniques for the detection and prevention of blackhole intrusions [24]. This study developed a context-based node acceptance system named NA-DE, inspired by the Dolphin Echolocation model, to establish appropriate security protocols and automate defence operations in comprehensive MANETs. This method attempted to accomplish early and quick detection of black hole attacks without sacrificing network performance by automatically detecting spiteful nodes. In addition, traffic was always redirected via healthy nodes while damaged nodes were segregated from the rest of the network. The routing protocol was Ad-hoc On-Demand Distance Vector Routing (AODV). The effectiveness of the method proposed in the study was evaluated using a number of criteria. It was feasible to determine that the recommended methodology outperforms another cutting-edge routing protocol by contrasting its performance measures with those of the latter. When there were 250 nodes in the experiment, it was evident from the findings that the NA-DE technique performed better at identifying black hole nodes and made it possible to transmit safe data while using less energy.

M. S. Sheela et al. (2024) aimed to develop a smart IDS system to significantly enhance MANET security using deep learning models [25]. The study pre-processed cyber-attack datasets by applying the minmax normalization model, normalizing attributes or fields to improve the classifier's overall efficacy in detecting intrusions. Subsequently, they implemented a novel Adaptive Marine Predator Optimization Algorithm (AOMA) to select best features, enhancing both the speed and intrusion detection efficacy of the classification model. Additionally, this work adopted an approach named DSLC (Deep Supervise Learning Classification) for predicting and categorizing intrusion types leveraging effective learning and training processes. Performance indicators and benchmark datasets were used to assess and validate the efficacy and outcomes of the suggested IDS based on AOMA-DSLC technique.

2.1 Comparison Table

Author & Year	Technique Used	Simulation tool	Performance Metrics	Findings	Limitations
J. Vinayagam et al. (2019)	Integrated Cross Interior (ICI) structure for IDS	Network Simulator-2 (NS-2)	Routing cost, response time, throughput	Reduced response time (6.3 ms), high throughput (83.5%), minimal routing cost	One drawback of this approach is that it does not parallelize the various stages of the proposed routing models, which leads to decreased performance.
T. Terai et al. (2020)	Local data exchange for BH attack detection	Network Simulator-2 (NS-2)	Attack success rates	Effective in detecting and mitigating sophisticated BH threats	The proposed approach has low false detection rate.

E. Elmahdi et al. (2020)	Advanced AOMDV protocol, homomorphic encryption	Network simulator (NS-2)	Packet delivery ratio (PDR), network throughput	Improved PDR and network throughput, effective against blackhole attacks	This approach exhibits high end-to-end delay, making it unsuitable for emergency applications in MANETs.
P. R. B et al. (2021)	OSPFV integration, threshold evaluation, cryptographic verification	Network simulator (NS-2)	PDR, routing overhead, network delay	Effective in countering internal attacks	A limitation of this work is that it relies exclusively on simulations using the random mobility model.
E. Lema et al. (2022)	Trust Embedded AODV	Network simulator (NS-2)	Attack percentage, PDR, throughput, end-to-end delay	Ensured real-time data transfer, detection, and prevention of blackhole nodes	In scenarios of link failure, a significant number of control packets are generated, which consumes network bandwidth and reduces the Quality of Service (QoS) as the network density increases
R. Gotti et al. (2023)	Machine learning methods	Network simulator (NS-2)	PDR, throughput	Effective in detecting blackhole attacks using ML methods	This method fails to differentiate hostile activity from typical network fluctuations, particularly in dynamic and unpredictable mobile situations.
S. Shafi et al. (2023)	ML-AODV, ANN, SVM	Network simulator (NS-2)	Reliability, throughput, delay, routing overhead, packet loss ratio	Improved reliability (44%), throughput (4%), reduced delay (12%), routing overhead (15%), packet loss (10%)	ML-AODV may be less suitable for fully urban scenarios due to the highly dynamic nature of node density and speeds, which can affect its performance in information exchange.
Ramesh Vatambeti et al. (2024)	NA-DE inspired by Dolphin Echolocation, AODV	NSv2.34	Reliability, PDR, throughput	Early and quick detection of blackhole attacks, secure data transmission, reduced energy usage	The main drawback of the suggested method is its reliance on the accuracy and availability of sensory data,

					which can be impacted by node actions and ambient factors not included in the model.
M. S. Sheela et al. (2024)	Deep learning models, AOMA-DSLC	Not specified	detection rate, accuracy, and false positive rates	Improved classifier efficacy, effective intrusion detection	The main drawback of the proposed approach is its reliance on the availability and quality of training data.

Conclusion

In conclusion, blackhole attacks pose a severe risk to the security and functionality of Mobile Ad Hoc Networks. The dynamic and decentralized nature of MANETs, while providing flexibility and ease of deployment, also introduces vulnerabilities that can be exploited by malicious entities. Effective detection and prevention strategies are crucial to safeguard the network against these attacks. Although numerous approaches, such as trust-based systems and anomaly detection, have been developed, they often face challenges in maintaining a balance between security and network performance. Ongoing research and development are necessary to refine these methods and develop new solutions that can provide robust security without degrading network efficiency. Ensuring the protection of MANETs against blackhole attacks will enhance their reliability and trustworthiness, paving the way for their broader adoption in various critical applications.

References

[1] I. Nausheen and A. Upadhyay, "ETSAODV: An Efficient and Trusted Secure AODV with Performance Analysis for MANETS suffering Blackhole Attack," 2023 Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2023, pp. 1-6, doi: 10.1109/ICAECT57570.2023.10118159.

[2] N. G. Wakode, "Defending blackhole attack by using acknowledge based approach in MANETs," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, India, 2017, pp. 1-6, doi: 10.1109/ICIOTA.2017.8073611.

[3] P. R. Dumne and A. Manjaramkar, "Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2016, pp. 486-490, doi: 10.1109/ICRITO.2016.7785004.

[4] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 28-33, doi: 10.1109/JEEIT.2019.8717449

[5] M. Bharti, S. Rani and P. Singh, "Security Attacks in MANET: A Complete Analysis," 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 2022, pp. 384-387, doi: 10.1109/ICDCS54290.2022.9780760.

[6] P. Satyanarayana, G. V. S. P. Rao, S. Dasam, A. M, D. Kalpana and V. G. Krishnan, "Enhancement of Network Security in MANETs Using Improved Averaging Self-Optimization Algorithm (IASOA) for IoT Applications," 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, India, 2023, pp. 1-5, doi: 10.1109/ICMNWC60182.2023.10435907.

[7] Y. Fu, G. Li, A. Mohammed, Z. Yan, J. Cao and H. Li, "A Study and Enhancement to the Security of MANET AODV Protocol Against Black Hole Attacks," 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing,

Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 2019, pp. 1431-1436, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00259.

[8] R. Agrawal, R. Tripathi and S. Tiwari, "Cluster Based MANET Security with N-TH Degree Truncated Polynomial Ring (NTRU) Public Key Cryptosystem," 2023 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2023, pp. 126-133, doi: 10.1109/ICCIKE58312.2023.10131714.

[9] B. Banerjee and S. Neogy, "A brief overview of security attacks and protocols in MANET," 2021 IEEE 18th India Council International Conference (INDICON), Guwahati, India, 2021, pp. 1-6, doi: 10.1109/INDICON52576.2021.9691554.

[10] I. Nausheen and A. Upadhyay, "Performance Analysis of Efficiently trusted AODV serving Security in MANET under Blackhole Attack Using Genetic Algorithm," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 1127-1131, doi: 10.1109/IITCEE57236.2023.10091046.

[11] R. Ramesh and G. Seshikala, "Link Aware Multipath Routing to Defend Against Black Hole Attacks for MANETs," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-6, doi: 10.1109/CONIT59222.2023.10205694.

[12] B. V. Sherif and P. Salini, "Effective and Prominent Approaches for Malicious Node Detection in MANET," 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA), Nagpur, India, 2021, pp. 1-6, doi: 10.1109/ICCICA52458.2021.9697234.

[13] V. S. Pooja, T. Rohit, N. M. Reddy and S. Sudeshna, "Mobile Ad-hoc Networks Security Aspects in Black Hole Attack," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 26-30, doi: 10.1109/ICECA.2018.8474629.

[15] M. B. M. Kamel, I. Alameri and A. N. Onaizah, "STAODV: A secure and trust-based approach to mitigate blackhole attack on AODV based MANET," 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2017, pp. 1278-1282, doi: 10.1109/IAEAC.2017.8054219.

[16] P. Golchha and H. K. Pati, "A Survey on Black Hole Attack in MANET Using AODV," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2018, pp. 361-365, doi: 10.1109/ICACCCN.2018.8748279.

[17] J. Vinayagam, CH. Balaswamy, and K. Soundararajan, "Certain Investigation on MANET Security with Routing and Blackhole Attacks Detection," Procedia Computer Science, vol. 165, pp. 196–208, 2019, doi: https://doi.org/10.1016/j.procs.2020.01.091.

[18] T. Terai, M. Yoshida, A. G. Ramonet and T. Noguchi, "Blackhole Attack Cooperative Prevention Method in MANETs," 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), Naha, Japan, 2020, pp. 60-66, doi: 10.1109/CANDARW51189.2020.00024.

[19] E. Elmahdi, S.-M. Yoo, and K. Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks," Journal of Information Security and Applications, vol. 51, p. 102425, Apr. 2020, doi: https://doi.org/10.1016/j.jisa.2019.102425.

[20] P. R. B, B. R. B, and D. B, "The AODV routing protocol with built-in security to counter blackhole attack in MANET," Materials Today: Proceedings, Aug. 2021, doi: https://doi.org/10.1016/j.matpr.2021.08.039.

[21] E. Lema, E. G. -M. Desalegn, B. Tiwari and V. Tiwari, "Trust Embedded AODV for securing and Analyzing Blackhole attack in MANET," 2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Naya Raipur, India, 2022, pp. 362-367, doi: 10.1109/WIECON-ECE57977.2022.10150765.

[22] R. Gotti, A. Polagani, G. S. Lakshmi Posina, S. Veerapaneni and T. Prasanth, "Detection and Analysis of Single Blackhole Node with TCP Connection in MANETs using Machine Learning Algorithms," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1704-1710, doi: 10.1109/ICICT57646.2023.10134058.

[23] S. Shafi, S. Mounika, and S. Velliangiri, “Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET,” Procedia Computer Science, vol. 218, pp. 2309–2318, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.206.

[24] Ramesh Vatambeti, Srihari Varma Mantena, K. V. D. Kiran, Srinivasulu Chennupalli, and M Venu Gopalachari, “Black hole attack detection using Dolphin Echo-location-based machine learning model in MANET environment,” Computers & electrical engineering, vol. 114, pp. 109094–109094, Mar. 2024, doi: https://doi.org/10.1016/j.compeleceng.2024.109094

[25] M. S. Sheela et al., "Adaptive Marine Predator Optimization Algorithm (AOMA)-Deep Supervised Learning Classification (DSLC) Based IDS Framework for MANET Security," in Intelligent and Converged Networks, vol. 5, no. 1, pp. 1-18, March 2024, doi: 10.23919/ICN.2024.0001