International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi :https://doi.org/10.32628/CSEIT2390395

Mitigation of Black Hole and Selective Forwarding Attacks through Active Trust Mechanisms in Wireless Sensor Networks

Mohammad Sirajuddin*[1], Dr. B. Sateesh Kumar[2]
*[1]Research Scholar, Department of Computer Science & Engineering, JNTU, Hyderabad, Telangana, India
[2]Professor, Department of Computer Science & Engineering, JNTUH-College of Engineering, Jagitial, Telangana, India

ARTICLEINFO

Article History:

Accepted: 01 May 2023
Published: 20 May 2023

Publication Issue
Volume 9, Issue 3
May-June-2023

Page Number
329-337

ABSTRACT

In modern times, security remains a significant concern in wireless networks. Wireless sensor networks are widely employed in different practical situations. WSNs struggle with numerous internal and external threats, and detecting and defending against insider attacks is difficult. Insider attacks, in which intruders discard received data packets selectively, pose a significant risk to WSNs. The presence of black hole nodes within the network causes this issue. This research paper presents a secure and reliable route management methodology for WSNs that selects nodes and routing paths based on trust metrics. The proposed mechanism employs intelligent routing and node selection to defend against various types of assaults encountered during the routing process, including selective forwarding and black hole attacks. As a result, the paper identifies secure routes and establishes secure network routing. This scheme uses throughput, latency, and packet drop ratio as performance metrics. Experimentation demonstrates that the proposed system effectively increases the probability of secure network routing paths while extending the network lifecycle.

Keywords : Black-Hole Attacks, Dos Attacks, WSN Security, Trust Metrics

I. INTRODUCTION

A sensor network is an amalgamation of sensing, processing, and communication capabilities designed to observe and react to environmental events. Wireless sensor networks (WSNs) typically comprise many nodes, often numbering thousands. These nodes collaborate to collect, process, and transmit information to a central location. The utilization of WSN technology presents numerous advantages compared to traditional networking solutions. These benefits encompass cost savings, reliability, scalability, flexibility, precision, and ease of deployment. With rapid technological advancements, sensors are becoming smaller and more affordable, deploying billions of sensors across various applications. Promising application domains for WSNs include the military, environmental monitoring, healthcare, and security[1].

When designing a WSN, several factors come into play, such as production costs, operating environment, sensor network topology, hardware limitations, transmission media, and power consumption. These factors serve as crucial considerations in shaping the design of protocols and algorithms to construct an efficient sensor network[2].

Moreover, ensuring security in WSNs poses a significant challenge, mainly when entrusted with critical tasks. When sensor networks interact directly with the environment, individuals, and other objects, their vulnerability to security threats increases. The primary objective of security measures in WSNs is to safeguard data and resources against attacks and malicious activities. Various forms of assaults can jeopardize the reliability and functionality of a WSN, particularly at the network layer. Special network layer attacks garnered recent attention, including wormhole attacks, sinkhole attacks, selective forwarding attacks, greeting flood attacks, false routing attacks, and acknowledgment flooding. Among these, the black hole attack is one of the most severe threats to WSNs[3].

A. Black-hole Attacks

Black hole attacks in wireless sensor networks refer to a type of security threat where a malicious node, known as a black hole, selectively drops or absorbs all the data packets it receives, effectively making the data disappear. This attack can severely disrupt the normal functioning of the network and compromise its integrity. In a wireless sensor network (WSN), sensor nodes collaborate to collect and transmit data to a central base station or a sink node. Each sensor node typically has limited resources such as power, memory, and processing capabilities. To achieve its objectives, the network relies on cooperation and information sharing among nodes[2]. In a black hole attack scenario, one or more nodes in the network behave maliciously and falsely advertise themselves as having the shortest or most optimal path to the sink node. Unaware of the malicious node's intentions, other legitimate nodes may route their data through the malicious node, believing it to be a reliable path. However, instead of forwarding the data packets as expected, the black hole node drops or absorbs all the packets, preventing them from reaching their intended destination. This leads to data loss and disrupts the normal functioning of the network. Since the black hole node does not participate in the network's routing protocols and data forwarding mechanisms, it can go undetected for an extended period. Black hole attacks can have severe consequences in wireless sensor networks, such as:

Data loss: The network loses valuable data due to the malicious node intercepting and discarding packets.

Disruption of network operations: The compromised node disrupts the standard data flow, affecting the network's efficiency and reliability[3].

Energy wastage: Legitimate nodes may keep retransmitting data packets, consuming unnecessary energy resources, as they are unaware that their packets are not reaching their destination.

Compromised network integrity: By selectively dropping packets, the black hole node can manipulate the network's behavior, leading to unauthorized access or control over the network.

Several techniques and protocols have been proposed to mitigate black hole attacks and enhance the security of wireless sensor networks[15].

Intrusion detection systems: Implementing algorithms and mechanisms to detect the presence of malicious nodes in the network based on their abnormal behavior.

Secure routing protocols: Designing protocols incorporating security measures, such as authentication and verification, to ensure reliable data transmission.

Trust-based approaches: Introducing trust metrics and reputation systems to evaluate the trustworthiness of nodes and avoid routing through potentially compromised nodes.

Encryption and authentication: Using cryptographic techniques to secure the communication between sensor nodes and the sink node, preventing unauthorized access and tampering.

Researchers and network administrators need to stay updated on the latest security techniques and best practices to protect wireless sensor networks from black hole attacks and other potential security threats.

B. DoS Attacks

DoS (Denial-of-Service) attacks in wireless sensor networks involve malicious attempts to disrupt or disable the normal operation of the network by overwhelming its resources or causing congestion. These attacks aim to render the network unavailable or degrade its performance, making it challenging for legitimate nodes to communicate and fulfill their intended functions[13].

DoS attacks can have severe consequences in wireless sensor networks (WSNs), where nodes have limited resources. Here are a few common types of DoS attacks in WSNs.

Flooding attacks: In a flooding attack, the attacker floods the network with a high volume of packets, consuming the network's bandwidth and overwhelming the resources of the targeted nodes. Legitimate nodes cannot communicate effectively due to the excessive traffic, leading to a denial of service.

Jamming attacks: Jamming attacks involve the deliberate transmission of interference signals on the same frequency used by the wireless sensor network. This disrupts the communication between legitimate nodes, making it difficult or impossible for them to exchange data effectively[4].

Resource depletion attacks: Resource depletion attacks target the limited resources of individual sensor nodes. For example, an attacker may send a large number of resource-intensive requests to a particular node, exhausting its battery power, memory, or processing capacity. Once the resources are depleted, the node becomes unable to function properly or may even shut down, impacting the overall network performance[14].

Selective forwarding attacks: In a selective forwarding attack, the attacker compromises one or more nodes in the network and instructs them to selectively drop or forward packets based on specific criteria. By dropping or blocking specific packets, the attacker can disrupt communication between nodes or manipulate the flow of data in the network[4].

Sinkhole attacks: In a sinkhole attack, the attacker attracts and diverts the network's traffic towards a compromised node that acts as a sinkhole. The compromised node appears to be a reliable and desirable destination for data packets, but instead of forwarding them to the intended destination, it absorbs or drops the packets. This disrupts the normal routing and data transmission in the network.

To mitigate DoS attacks in wireless sensor networks, various security measures can be implemented:

Intrusion detection and prevention systems: Deploying intrusion detection mechanisms to identify and block malicious activities in the network, preventing DoS attacks before they cause significant damage.

Secure communication protocols: Using secure and authenticated communication protocols that protect against packet spoofing and unauthorized access.

Traffic analysis and anomaly detection: Employing techniques to analyze network traffic patterns and detect anomalies caused by DoS attacks, enabling prompt response and mitigation[12].

Collaborative security mechanisms: Implementing collaborative techniques, such as reputation systems and voting-based protocols, to enable nodes to collectively identify and isolate malicious nodes.

Energy-efficient designs: Develop energy-efficient algorithms and protocols that minimize the impact of resource depletion attacks and conserve the energy of sensor nodes.

II. LITERATURE REVIEW

The paper [5] presents a concise method for detecting black hole attacks with efficiency. As a result of a black hole attack, network parameters such as TH, TND, NRL, PDR, and PLR significantly improve. The proposed method computes trust levels using the KNN algorithm for clustering, beta distribution, Josang mental logic, and fuzzy inference. The reputation of nodes is then determined by the trust server. Ultimately, based on the reputation table, the cluster master periodically distributes a list of defective cluster nodes.

The paper [6] presents a Hidden Markov Model-based solution for detecting malicious nodes and preventing black hole attacks in wireless sensor networks. The proposed method implements a novel routing algorithm that analyses the shortest path to avoid malevolent node paths. The obtained results demonstrate the efficacy and effectiveness of the proposed routing algorithm in preventing black hole attacks.

The paper [7] examines black hole denial-of-service attacks against the general-purpose ad hoc on-demand distance vector (AODV) protocol. Normal AODV, BH_AODV, and D_BH_AODV were tested. Black hole attacks slowed networks. IDS and digital signatures were used to prevent black hole attacks. QoS measures, including packet delivery ratio (PDR), delay, and overhead were used to compare the conventional AODV, BH_AODV, and D_BH_AODV protocols. Nodes, packet sizes, and simulation timeframes were evaluated. NS2 was used to imitate malicious protocols with a bespoke D_BH_AODV routing protocol. The D_BH_AODV technique improves PDR by 40% to 50% for different nodes and packets. With more nodes and packets, the delay drops from 300 to 100 and 150 to 50 ms. Node and packet values affect overhead from 1 to 3. The research shows that black hole attacks hurt network performance, but the D_BH_AODV strategy improves QoS by recognizing and avoiding black hole nodes during communication.

The article [8] presents a novel Strategic Security System (SSS) comprising three essential operations: replicator prediction, detection, and isolation. The system provides numerous benefits, such as the absence of SS-Manager nodes and minimal additional resource utilization for any security system. It accommodates hierarchical topologies. Simulation results indicate that this method is one of the most efficient strategies for removing replicators from a network.

The research [9] concentrates on conducting a forensic analysis of ad hoc IoT networks utilizing the ad hoc on-demand distance vector (AODV) routing protocol in the presence of black hole attacks, a type of denial-of-service attack that poses a serious threat to IoT networks. The investigation also analyses network traffic patterns and nodes to determine the extent of attack damage. In order to facilitate digital forensic (DF) investigations, a protocol's vulnerabilities are analysed. In addition, the research entails reconstructing the networks under various modes and parameters to validate the analysis and provide suggestions for designing robust routing protocols. The objective is to increase knowledge of IoT network performance in the face of black hole attacks and contribute to developing more secure and resilient routing protocols.

In the study [10], researchers introduce a remarkable solution for combating black hole attacks in AODV routing protocols. Departing from the conventional approach, they present a secure and innovative AODV routing protocol that addresses this pressing issue. The proposed method introduces significant modifications to the original AODV routing protocol, with particular emphasis on the reinforcement of RREQ and RREP packet protocols. These enhancements pave the way for a more robust and secure network infrastructure. One of the notable features is the integration of a cryptography-based encryption and decryption function, which plays a crucial role in verifying the authenticity of both source and destination nodes. By leveraging this mechanism, the protocol fortifies the security measures, ensuring heightened protection against potential threats. To evaluate the effectiveness of their solution, the researchers utilize the powerful NS-2.33 simulator, considering a diverse range of network parameters. The evaluation encompasses metrics such as dropped packets, end-to-end latency, packet delivery ratio (PDR), and routing request overhead. These measures provide a comprehensive understanding of the protocol's performance in the face of black hole assaults. The results of the evaluation showcase the superiority of the proposed method over the existing AODV routing protocol when confronted with black hole attacks. This improvement translates into enhanced network performance on the whole, promising a more secure and reliable environment for data transmission. The findings of this study mark a significant milestone in the field, offering a substantial contribution to the advancement of secure AODV routing protocols.

This research [11] detects and prevents WSN black hole and selective forwarding attacks. Two security mechanisms—two-stage and dual assurance—are offered. Trust and CS algorithms in clustered sensor networks identify untrusted links and provide secure routing for data packets. This energy-efficient device detects malicious nodes. Secure routing avoids black holes and selective forwarding attacks, maximising packet delivery ratio. The suggested system is accurate, energy-efficient, user-friendly, private, and reliable for real-time WSN applications. These features aid risk management, system assessment, secure data packet transmission, and routing path construction. Experimental results show that the proposed system outperforms existing systems in energy consumption, latency, path length, network lifetime in heterogeneous and homogeneous networks, throughput, and packet drop ratio. The proposed system achieves 85% throughput with maximum network size and 20,000ms delay.

III.METHODOLOGY

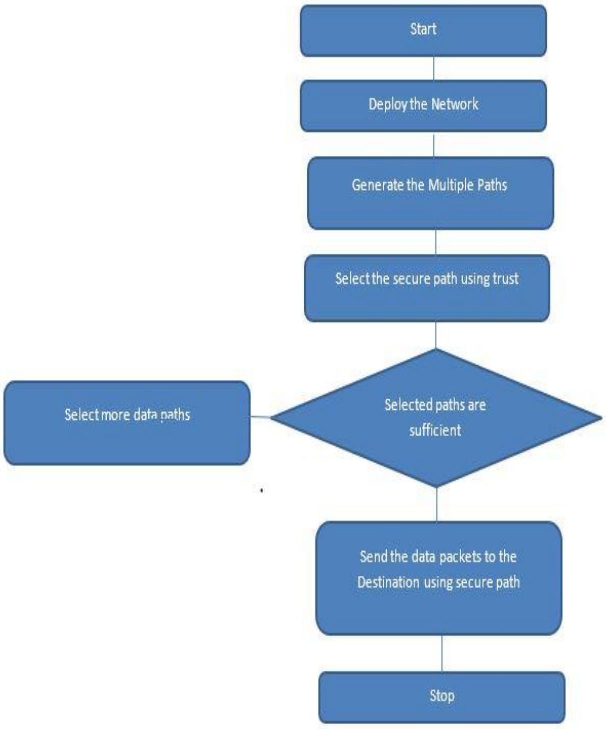
Start
Deploy the Network
Generate the Multiple Paths
Select the secure path using trust
Select more data paths
Selected paths are sufficient
Send the data packets to the Destination using secure path
Stop

Figure 1. Architecture of proposed scheme

This paper develops a safe and secure path selection mechanism for Wireless Sensor Networks (WSNs). The goal is to prevent routing nodes from being compromised or malicious by proactively detecting Black hole attacks. By optimising the distribution of data packets along more efficient route paths, the primary objective of this study is to extend the lifetime of sensor nodes within Wireless Sensor Networks (WSNs). To attain this objective, a trust-based route selection mechanism is proposed. This mechanism identifies reliable paths from the source to the destination within WSNs, thereby ensuring the integrity of data transmission. The procedure entails generating a source node and facilitating the transmission of data from the source to the intended destination. A malicious node is detected by trust value. The minimum threshold value establishes a secure routing path for the entire transmission path upon effective detection of a malicious node. During transmission, the trust-based path selection technique is utilised to identify a secure routing path. This strategy protects the network from black hole and selective forwarding assaults, ensuring its security and integrity. This mechanism illustrates the trust system through a variety of facets. These include assuring the routing path's security and determining the optimal threshold value based on trust considerations. These factors have two major effects: first, they affect the performance of the trust system, and second, they affect the threshold-based trust factors. In order to accomplish these objectives, the mechanism computes a threshold value for each path. The calculation seeks to identify the path with the lowest threshold value, which represents the most secure data routing path. Consequently, during the routing of detection and data packets, each sensor node can estimate its level of trust to avoid potential issues such as black hole attacks and selective forwarding attacks.

The trust-based threshold value is computed with the following equation

$$\text{Trust Treshold of a Node} = \frac{\text{Node Trust}}{\text{Dastance}}$$

To calculate the threshold values for a node, a division operation is performed by dividing the trust values by the corresponding distance values. Once these trust-based threshold values are computed for a sensor node, the next step involves calculating the threshold value for each path within the node. This calculation is carried out using the following equation.

$$Trust\ Treshold\ of\ a\ Path = \sum_{k=0}^{n} Trust\ Threshold\ of\ a\ Node$$

Henceforth, this equation serves as a representation of the cumulative threshold values encompassing every node along various paths. Within this framework, the path yielding the minimum computed threshold value emerges as the most reliable and secure route for data routing. Once the network is deployed, the initial step involves selecting a trusted path originating from the source node and extending to the destination node. This selection process relies on identifying the minimum threshold value. With trust established, the subsequent objective entails identifying potential paths connecting the source and destination nodes[13]. The subsequent focus shifts towards discerning secure routing paths amidst the multitude of estimated options, utilizing trust as a guiding factor in enhancing security. If a trusted path is deemed satisfactory, the data packet traverses that route. However, in cases where the trusted path falls short, alternative trusted paths within the network are explored and considered. To prevent potential issues, packets exceeding the anticipated size are rejected. Conversely, when the packet size falls within acceptable parameters, the sensor node proceeds to transmit the data directly from the previous node to the subsequent node, terminating the process. After transmitting the data, if the previous node lies beyond the range of the subsequent node, a common neighbor node is sought, and the data is relayed to that intermediary. On the other hand, if the previous node is within range, the data is dispatched directly to the intended node, culminating the procedure. By adhering to this mechanism, an improved routing path is achieved, taking into account enhanced security considerations.

IV.RESULTS AND DISCUSSION

This section provides an overview of the proposed approach and presents relevant data to support it. It is advisable to have a contingency plan as a precautionary measure. To conduct the simulation, we employed Network Simulator 2 (NS-2) to replicate the wireless sensor network, utilizing the Ad hoc On-Demand Distance Vector (AODV) protocol. Table 1 enumerates the necessary components for the simulation. Our analysis encompassed various quantitative aspects, including network packet overhead, throughput, delay, and resource utilization.

TABLE I SIMULATION PARAMETERS

Parameter	Quantity
Protocol	AODV
Simulator	NS-2
Simulation Area	500 * 500

Number of Nodes	20
Packets	TCP Packets
Transmission Range	200m
Transmission Time	100sec

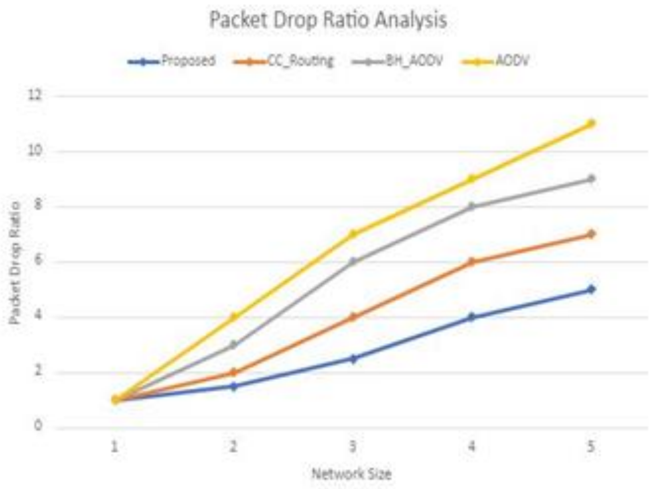

Figure 2. Packet Drop Ratio Analysis

The efficiency of a routing scheme can be determined by evaluating the packet drop ratio. In the case of the proposed technique, a comparison was made with existing methodologies, revealing that the packet drop ratio of the proposed methodology surpasses that of the existing methodologies. These results clearly demonstrate the proposed methodology's superior performance in minimizing packet drops.

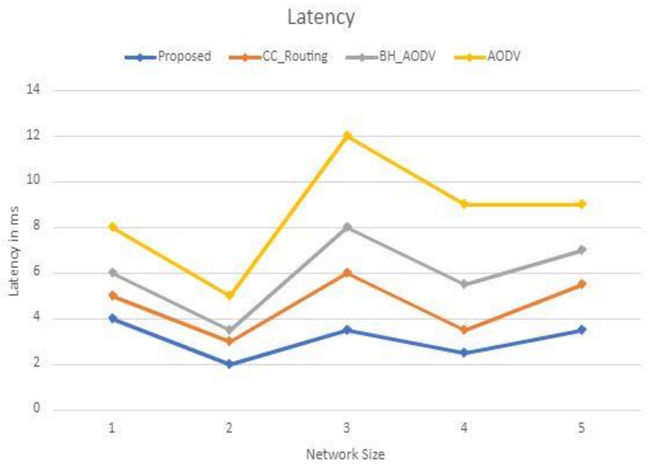

Figure 3. Latency Analysis

A meticulous comparison of latency between the proposed method and existing methodologies indicates that the proposed scheme exhibits a notably reduced latency in contrast to alternative routing methodologies.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left justified and right-justified.

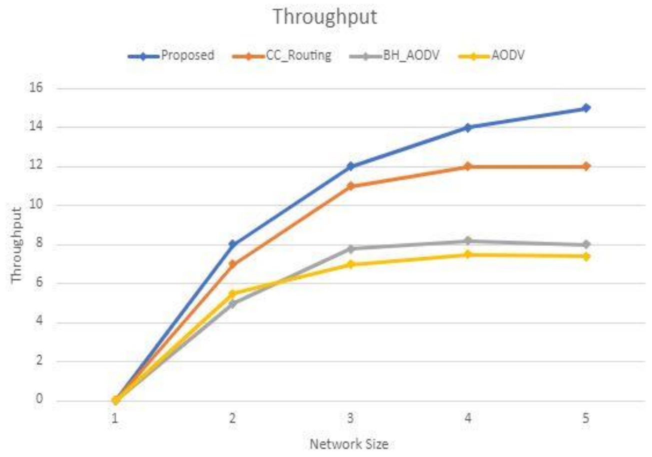

Figure 4. Throughput Analysis

The efficacy of the suggested scheme's throughput is appraised by scrutinizing the quantity of packets successfully received in proportion to the number of packets smoothly transferred. Upon thorough analysis, it becomes evident that the proposed methodology exhibits a moderately superior throughput value compared to the prevailing routing schemes.

V. CONCLUSION

The increasing need for security in modern times, particularly sensor networks, cannot be understated. Wireless sensor networks (WSNs) are extensively utilized in various practical applications, but they face numerous internal and external threats, making detection and defense against insider attacks challenging. Insider attacks, which involve selectively discarding received data packets, pose a significant risk to WSNs, especially in unattended clustered environments. This research paper addresses these challenges by presenting a reliable and secure routing scheme for WSNs that focuses on selecting nodes and routing paths based on trust metrics. The proposed mechanism utilizes intelligent routing and node selection to effectively defend against various types of assaults encountered during the routing process, such as black hole attacks and selective forwarding attacks. By identifying secure routes and establishing secure network routing, the proposed scheme enhances the probability of secure network routing paths while extending the network's lifespan. The performance of the proposed system is evaluated using latency, packet drop ratio, and throughput as metrics. Through experimentation, it is demonstrated that the proposed scheme significantly improves the probability of secure network routing paths while extending the network's lifespan. Thus, this research contributes to enhancing the security and reliability of wireless sensor networks in the face of evolving threats.

VI. REFERENCES

[1]. Khattak, Hasan Ali Fang, Weidong Zhang, Wuxiong Chen, Wei Pan, Tao Ni, Yepeng Yang, Yinxuan 2020 Trust-Based Attack and Defense in Wireless Sensor Networks:ASurvey ISSN: 1530-866 https://doi.org/10.1155/2020/2643546.

[2]. Hasan, A.; Khan, M.A.; Shabir, B.; Munir, A.; Malik, A.W.; Anwar, Z.; Ahmad, J. Forensic Analysis of Black-hole Attack in Wireless Sensor Networks/Internet of Things. Appl. Sci. 2021, 12, 11442. https://doi.org/10.3390/app122211442.

[3]. Sirajuddin, M., Sateesh Kumar, B. (2022). Collaborative SecuritySchemes for Wireless Sensor Networks. In: Kumar, A., Mozar, S.(eds) ICCCE 2021. Lecture Notes in Electrical Engineering, vol828, 2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-7985-8_36

[4]. M. Sirajuddin and B. S. Kumar, "Efficient and Secured Route Management Scheme Against Security Attacks in Wireless Sensor Networks," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2021, pp. 1045-1051, doi: 10.1109/ICESC51422.2021.9532779.

[5]. Chaudhry, Shehzad Ashraf Farahani, Gholamreza " Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks"Security and Communication Networks ISSN:8814141-https://doi.org/10.1155/2021/8814141.

[6]. Preventing Black Hole Attack in Wireless Sensor Network Using HMM, Procedia Computer Science, volume 148, pages 552-561, 2019,THE SECOND INTERNATIONAL CONFERENCE ON INTELLIGENT COMPUTING IN DATA SCIENCES, ICDS2018,issn 1877-0509, https://doi.org/10.1016/j.procs.2019.01.028,HananeKalkha and Hassan Satori and Khalid Satori.

[7]. Md Ibrahim Talukdar, Rosilah Hassan, Md Sharif Hossen, Khaleel Ahmad, Faizan Qamar, Amjed Sid Ahmed, "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature", Wireless Communications and Mobile Computing, vol. 2021, Article ID 6693316, 13 pages, 2021. https://doi.org/10.1155/2021/6693316.

[8]. L.Sujihelen, Rajasekhar Boddu, S. Murugaveni, Ms. Arnika, AnandakumarHaldorai, Pundru Chandra Shaker Reddy, Suili Feng, Jiayin Qin, "Node Replication Attack Detection in Distributed Wireless Sensor Networks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 7252791, 11 pages, 2022. https://doi.org/10.1155/2022/7252791.

[9]. Hasan, A.; Khan, M.A.; Shabir, B.; Munir, A.; Malik, A.W.; Anwar, Z.; Ahmad, J. Forensic Analysis of Black-hole Attack in Wireless Sensor Networks/Internet of Things. Appl. Sci. 2021, 12, 11442. https://doi.org/10.3390/ app122211442.

[10]. Ankit Kumar, Vijayakumar Varadarajan, Abhishek Kumar, Pankaj Dadheech, Surendra Singh Choudhary, V.D. Ambeth Kumar, B.K. Panigrahi, Kalyana C. Veluvolu,Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm,Microprocessors and Microsystems, Volume 80,2021, 103352,ISSN 0141-9331,https://doi.org/10.1016/j.micpro.2020.103352.

[11]. Mehetre, D.C., Roslin, S.E. &Wagh, S.J. Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Cluster Comput 22 (Suppl 1), 1313–1328 (2019). https://doi.org/10.1007/s10586-017-1622-9.

[12]. H. Ashraf, F. Khan, U. Ihsan, F. Al-Quayed, N. Z. Jhanjhi and M. Humayun, "MABPD: Mobile Agent-Based Prevention and Black Hole Attack Detection in Wireless Sensor Networks," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-11, doi: 10.1109/ICBATS57792.2023.10111277.

[13]. M. Kumar and J. Ali, "Adaptive Taylor-Sail Fish Optimization based deep Learning for Detection of Black Hole and Sybil Attack in Wireless Sensor Network," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 1237-1244, doi: 10.1109/ICSCDS56580.2023.10104946.

[14]. K.Balasubadra, X. S. A. Shiny, P. P V, P. Solainayagi and S. P. Maniraj, "Hidden Markov Model with Machine Learning-Based Black hole Attack Identification in Wireless Sensor Networks," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 829-833, doi: 10.1109/IITCEE57236.2023.10090993.

[15]. M. A. Goumidi, N. Hadj-Said, A. B. Ali-Pacha and E. Zigh, "Detection of Malicious Nodes in WBAN using a Feed Forward Back Propagation Neural Network," 2022 International Conference of Advanced Technology in Electronic and Electrical Engineering (ICATEEE), M'sila, Algeria, 2022, pp. 1-6, doi: 10.1109/ICATEEE57445.2022.10093101.