International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Protocols to Mitigate Blackhole Attack in Wireless Networks - A Survey

B. Sandhya Rani[1], Kattula Shyamala[2]

[1]Degree Lecturer in Computer Science, Telangana Social Welfare Residential Degree College for Women - Jagathgirigutta, Hyderabad, Telangana, India
sandhya.cse.nalgonda[at]gmail.com

[2]Professor, Department of Computer Science and Engineering, UCE-OU(A), Osmania University, Hyderabad, Telangana, India
prkshyamala[at]gmail.com

Abstract: ***Wireless networks have become an integral part of modern communication systems, enabling seamless connectivity across various devices and applications. They are fundamental to both everyday consumer use and functioning of critical systems in industries ranging from healthcare to transportation, finance, and entertainment. Unlike traditional wired networks, wireless networks use electromagnetic waves for data transmission, offering mobility, scalability, and flexibility in design for a wide range of applications. Wireless networks have come with a number of challenges that can impact performance, reliability, security, dynamic topology, limited resources, energy efficiency, data aggregation, and fault tolerance. These networks are vulnerable to various attacks like blackhole, grey hole, sinkhole etc. The paper presents the literature survey on various trust-based approaches based on trust values, fuzzy logic, machine learning approaches and QoS calculations to mitigate blackhole attack in wireless networks.***

Keywords: Blackhole attack, MANETs, mitigate blackhole attack, trust-based protocols, security issues in wireless networks, wireless sensor networks

1. Introduction

Wireless networks are critical in applications like emergency response, environmental monitoring, and military operations. However, the inherent characteristics of these networks, such as dynamic topology, lack of centralized management, limited resources, and reliance on wireless communication, make them highly vulnerable to various security attacks [1]. The security threats compromise confidentiality, integrity, availability, and reliability of the network, leading to service degradation, loss of data, and network failure. The attacks are categorized as passive attacks and active attacks. Passive attacks involve eavesdropping on network traffic without modifying the data and active attacks aim at fabricating or modifying the data [2]. The paper presents the details about the blockhole attack, detection techniques, consequences and prevention of blackhole attack in section II, section III trust-based routing, section IV literature survey and conclusion.

2. Blackhole Attack

2.1 Blackhole Attack

A blackhole attack is a Denial of Service (DOS) attack. When a route discovery process is initiated by broadcasting a Route Request (RREQ), the malicious node advertises itself as having a fresh route to the destination by sending Route Reply (RREP) to a node that has sent RREQ. Therefore, all the packets are routed through the malicious node, which instead of forwarding the packets drops them. Figure 1 shows the working of a blackhole attack. Node A is a source, Node M is a malicious node, and node F is the destination node. Node A initiates the route discovery process and broadcasts RREQ, malicious node M also receives the RREQ and without referring routing table sends RREP to node A and claims that it is a fresh route to the destination. Node A trusts this information and routes all the packets through the M, which in turn drops all the packets. As a result, the data sent through this route is lost, leading to a denial of service and network performance degradation as shown in Figure 1. A compromised node in the attack may lead to other attacks such as Replay attack, Man-in-the- Middle attack, and Selective forwarding attack [3].

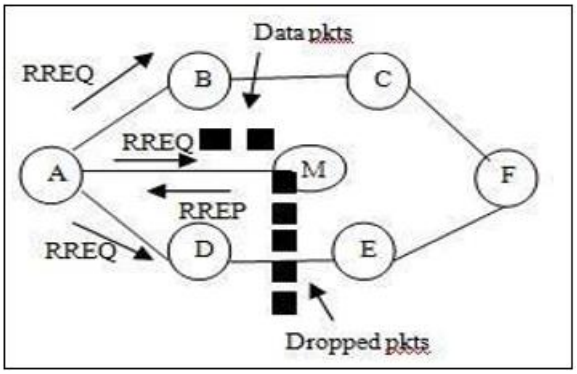

Figure 1: Black Hole Attack

The detection and avoidance of such attacks include secure routing protocols based on trust, cryptographic methods, and intrusion detection systems. Blackhole nodes detection and prevention techniques are presented in [4].

2.2 Blackhole Detection Techniques

Anomaly Detection: If a node suddenly starts dropping packets or behaving erratically, it can be flagged as a potential blackhole attacker. The system can track the number of dropped packets or routing inconsistencies over a time to detect suspicious behavior.

Behavioral Pattern Analysis: By analyzing node's historical behavior, the system can recognize patterns indicative of malicious actions. Nodes that consistently fail to forward packets or deviate from normal routing protocols can be identified as blackhole attackers.

Neighboring Node Feedback: Each node can collect feedback from its neighbors. If several neighboring nodes report a node as untrustworthy or behaving maliciously, the suspicious node can be flagged as a blackhole attacker.

Route Monitoring: The path taken by data packets can be monitored. If a node along the path consistently receives data but does not forward it or drops packets, it is flagged as a blackhole node.

2.3 Consequences of Blackhole Attack

- **Packet Loss:** The malicious node intercepts and discards packets, preventing them from reaching the destination.
- **Network Instability:** As legitimate routes are compromised; network performance degrades and leads to data loss and delays.
- **Resource Wastage:** Energy and bandwidth get wasted, as data packets are forwarded to malicious nodes instead of legitimate ones.
-

2.4 Prevention of Blackhole Attacks

Route Discovery and Validation
Secure Route Discovery: During the route discovery phase, nodes can validate the authenticity of the advertised routes before accepting them. For example, instead of relying on a single route advertisement, multiple nodes can be queried to verify the integrity of the route.

Route Validation: If a node claims to have the best route but has a low trust score or a history of malicious behavior, its route is not accepted, and the node is excluded from the route discovery process.

Trust-Based Path Selection
Trust-Aware Routing: A path with the highest overall trust score is selected. If a node along the path is flagged as unreliable or malicious, the system reroutes traffic to bypass the compromised node.

Path Diversity: Instead of relying on a single route, the protocol can utilize multiple paths to ensure that if one path is compromised by a blackhole attack, the data can still reach its destination through an alternative route.

Collaborative Detection
Collaborative Trust Assessment: Nodes can share their trust scores with neighbors, allowing them to collectively detect blackhole attacks. For example, if a node notices that several neighboring nodes have flagged a particular node as malicious, it will avoid routing through that node.

Multi-Hop Route Validation
Rather than accepting a route based solely on a node's claims, the protocol can validate routes by checking whether intermediate nodes along the route consistently forward data.

Encryption and Authentication
Data Integrity: Encryption can be applied to ensure that data transmitted through the network cannot be altered by malicious nodes. Digital signatures and Message Authentication Codes (MACs) can be used to verify the authenticity of routing messages.

Authentication of Nodes: Before nodes participate in routing, they can be authenticated using techniques such as Public Key Infrastructure (PKI) or shared keys to prevent the inclusion of malicious nodes.

Detection and Exclusion of Malicious Nodes
Exclusion from Routing: A node that has been identified as malicious is removed from the routing process and is blocked to avoid further participation in the routing process. The rest of the network is informed about the compromised node.

Reputation System: Nodes that exhibit consistent malicious behavior can have their reputation reduced to the point where they are no longer trusted and excluded from future routing decisions.

3. Trust Based Routing

The behavior of nodes is evaluated based on their previous interactions and is used to make routing decisions. Direct and Indirect trust, reputation-based trust, and aggregated trust score are the trust-based strategies that can be implemented to combat blackhole attacks [5]. Reputation scores are maintained based on feedback from other nodes in the network. A node that consistently forwards packets correctly gains a higher reputation, while a node that drops packets (a blackhole) will have a low reputation score. Direct trust is based on the node's direct performance such as forwarding packets, node's cooperation and behavioral history. Indirect trust refers to feedback received from other nodes about a node's behavior. A combination of direct and indirect trust is used to compute an aggregated trust score. A node is deemed unreliable and removed from routing paths if the score drops below a predetermined level. Trust-Based routing protocols offer improved security, reliability, adaptability, energy efficiency, and data integrity making them to be used in military, disaster recovery networks, healthcare, IoT, autonomous vehicles and smart cities [6]. On the other hand, the protocols suffer from increased overhead, vulnerability to collusion and involve complex trust management operations. A trust-based routing protocol work as follows:

- **Trust Initialization:** Each node initializes with a neutral trust score. As it interacts with its neighbors, it starts evaluating their behavior based on successful packet forwarding, honesty in route advertisements, and other criteria.
- **Route Discovery:** When a node needs to discover a route to a destination, it broadcasts RREQ packets and the nodes exchange trust metrics (e.g., trust scores and reputation).
- **Route Selection:** The node selects routes based on the trust score of the intermediate nodes along the path. Paths with low-trust nodes (suspected of being black holes) are avoided.
- **Continuous Monitoring:** After selecting a route, the node continues to monitor whether packets are being successfully forwarded. If any discrepancy is observed (such as packet drops without forwarding), the trust score of the suspected blackhole node is reduced.
- **Feedback and Isolation:** If malicious activity is detected, the network shares feedback about the compromised node,

and other nodes in the network can update their trust tables. The malicious node is isolated from future routing decisions.

4. Literature Survey

SAODV protocol in [7] evaluates the behavior of nodes and uses trust metrics to identify malicious behavior, such as selectively dropping packets or misreporting routing information. A source node initiates route discovery process by broadcasting RREQ packets and identifies best route to the destination. Each node in the route will evaluate the trustworthiness of neighboring nodes based on the forwarding data packets. If the packet delivery rate drops significantly, the trust score of the node in question is reduced. Each node sends periodic feedback about its neighbor's behavior. If a node constantly drops packets, the feedback would indicate that it is a potential blackhole attacker. Nodes with trust scores below a certain threshold will be excluded from future routing decisions, effectively isolating blackhole attackers from the network. If a malicious node is identified during communication, the source node rediscovers the route, avoiding the blackhole node. The performance of the protocol is compared with AODV protocol in the presence of blackhole attack. The results show an improvement in throughput, End to End Delay (EED) and Packet Delivery Ratio (PDR), but the energy consumption of SAODV is more compared to AODV.

MT-SMRP [8] incorporates multipath routing and message trust mechanisms in opportunistic networks. The node connectivity in such networks is intermittent and highly dynamic. Trust is established based on message reliability and node's behavior. Each node maintains a trust score for neighboring nodes, which is updated based on their past interactions and the quality of messages they forward. Paths involving high-trust nodes with a history of good behavior are preferred, ensuring secure and efficient data delivery. Multiple paths are identified during route discovery. If one path fails, the system reroutes the message through another path, enhancing reliability. Trust scores are dynamically updated based on the successful delivery of messages, cooperation with neighboring nodes. Finally, Messages are authenticated and encrypted as necessary to ensure data confidentiality and integrity. The results show that the protocol outperforms DMT-SMRP and SHBPR by 18.10%, 7.55%, 3.275% and 21.30%, 7.44%, and 4.85% in terms of delivery probability, messages dropped, and average latency.

ETSP in [9] uses a combination of monitoring, feed- back, and trust evaluation mechanism to detect and identify blackhole nodes.

$$\text{Trust(Ni)for Src} = (\text{R1}) * \gamma * \text{Credits} / m - i + 1$$

Where R1 is the is the social group value of the node, m refers to the number of intermediate nodes, credits refer to how efficiently the messages are transmitted to the nodes. ETSP improves the message drop ratio by about 74.7% over PBH and 36.67% over TSP respectively. PDR is improved by 2.7% compared to PBH and 6% over TSP.

Destination- Oriented Directed Acyclic Graph (DODAG) in [10] is used to identify routes for data transmission. Each node is initialized with a neutral trust score, and periodically, nodes exchange trust information with their neighbors through Trust Request and Trust Response messages. During the DODAG construction phase, each node advertises its trust score along with its rank. Only nodes with trust scores above a certain threshold are considered for the route. As nodes transmit data, they monitor whether the packets are successfully received at the destination. If a packet is not forwarded by a node, its trust score is reduced. Every node sends periodic trust updates to its neighbors. If a node consistently drops packets or misbehaves, its trust score will fall, and is excluded from the network. Testing the protocol with malicious nodes show that the trust embedded protocol outperforms the regular version in terms of energy consumption by 10-40% and PDR by 90%.

BEST protocol in [11] is an improvement of AODV protocol, which has incorporated trust mechanisms based on battery level, energy efficiency and route stability. The protocol not only mitigates blackhole attack, but also improves network performance, energy efficiency, scalability, resistance to collusion-based attacks and adaptability.

To optimize data transmission by integrating Quality of Service (QoS) requirements and trustworthiness of nodes a protocol is proposed in [12]. A trust modelling approach is employed that integrates an authentication technique with a key-based security mechanism to generate trust scores. Additionally, a cluster-based secure routing algorithm is proposed, where the cluster head is selected based on QoS metrics and trust scores to ensure secure routing within each cluster. Trust score is computed as

$$\text{TSG1j} = [\ (\text{ACKP}/\text{RP}) * 100] + f(t1, t2, s)$$

Where, TSG1j is the Trust score of node j when it is group-1, ACKP is the number of acknowledgement packets sent and RP is the count (number) of packets received from the neighbors. f(t1,t2,s) is a function, t1 is the start time, t2 is the end time and s are the time at which score is computed. The final routing path is chosen by considering factors such as path trust, energy consumption, and hop count, optimizing the routing process for efficiency and security. The protocol improves PDR, network lifetime, and security compared to QEER protocol.

Joint Trust in [13] involves a combined trust evaluation approach, where multiple parameters like data reliability, energy efficiency, and behavior consistency are assessed to determine the trustworthiness of each node. The Joint Trust combines both direct and indirect trust making the network less susceptible to attacks. Energy efficiency, data accuracy and communication consistency are considered to calculate trust value. Rather than routing data along only on one path, data can pass through multiple paths to balance the load across nodes, prolonging the network's lifespan and enhancing security. The approach minimizes the risk of malicious activity, supports energy efficiency, and ensures data accuracy, making it well-suited for applications where secure, reliable, and efficient data flow is essential. The maximal PDR, throughput, and minimal delay of the protocol is 44%, 52.8%, and 0.344 s

A hybrid optimization algorithm, Monarch-Cat Swarm Optimization (M-CSO) based on Monarch Butterfly Optimization in Cat Swarm Optimization is proposed in [14]. The framework operates in two aspects: select the secure nodes and the other is to choose opportunistic nodes among selected secure nodes. The selection of secure nodes is based on the parameters of trust, connectivity, and QoS. Secondly, opportunistic nodes are optimally chosen through proposed M-CSO, based on the fitness parameters like trust, distance, delay, and connectivity. At the end of 100 rounds, the throughput of the routing protocols TARF, SOAR, ACOSR, and M-CSO are 52.81, 58.31, 62.83 and 65.24. The proposed protocol detection rate, delay, throughput and distance of the M-CSO protocol is 57.8, 162.8s, 13 , 65.2 respectively.

The protocols in [15]-[16] continuously assesses each node's behavior by analyzing packet forwarding success rate, response consistency, and other network activities to compute direct trust and uses recommendations from neighboring nodes to compute indirect trust. By aggregating trust information from multiple sources, active trust reduces the risk of falsely identifying honest nodes as malicious. A trust threshold is set, and nodes whose trust scores fall below this threshold are considered suspicious and isolated from routing activities. The isolation of malicious node prevents data loss due to packet drops. To prevent unauthorized nodes from joining the network and falsely boosting trust scores, cryptographic methods like digital signatures are used to verify node's identity before establishing trust relationship.

A novel indirect trust mechanism, ITAODV proposed in [17] uses packet forwarding success rate, packet drop rate, route consistency and neighbor feedback to compute trust as shown below.

$$Ttotal=w1 * Tforward + w2 * Tdrop + w3 * Tconsistency + w4 * Tfeedback$$

Where Tforward is the packet forwarding trust, Tdrop is the packet drop rate trust, Tconsistency is the route consistency trust,

Tfeedback is the aggregated feedback from neighbors. w1,w2,w3,w4 are weight factors. Results of ITAODV are compared with standard AODV protocol and the results show an improvement in PDR and EED.

A fuzzy-based reliability prediction model combined with Genetic Algorithms (GA) and Teaching-Learning Based Optimization (TLBO) in [18] enhances the security and efficiency of routing protocol. The proposed approach leverages fuzzy logic for predicting node reliability, while GA and TLBO optimize the routing paths to mitigate blackhole attack and improves overall network performance. A message is passed through all the nodes to check if it received by the destination. If a destination receives a message, all the paths along which message is received is assigned 1 and others are assigned with 0. These paths are multiplied with the corresponding value and the results are added to find out a node whose value is zero and is marked as malicious node. Once candidate routes are generated using GA, TLBO is used to refine these solutions by adjusting the routes further based on feedback from neighboring nodes. TLBO adjusts the paths based on the best-known solution and iteratively refines it to ensure that the route is energy-efficient, secure, and reliable. The protocol is compared using TS and GA protocols. The response time of TS is 84 , GA is 51.2 and TLBO is 33.7 and average energy consumption is 13.7J, 10.3 J and 7.1 J respectively.

A hybrid approach combining K-Nearest Neighbor (K-NN) algorithm and reputation calculation in [19] is used to calculate trust. K-NN algorithm is used for classification and identifying malicious nodes based on their behavior, while reputation calculation helps assess the trustworthiness of nodes based on historical interactions and data forwarding. Using KNN algorithm node's behavior is monitored, and features are extracted based on packet forwarding rate, route request handling, packet drop rate. Next the data training takes place, where a set of labelled nodes (trusted or malicious) are used to train the K-NN model based on historical data. When a node's behavior needs to be evaluated, the K-NN algorithm compares it to the behavior of its K nearest neighbors (i.e., nodes that are most similar in terms of their packet forwarding behaviors). If the majority of the neighbors claim the node as trustworthy, it is classified as trustworthy. If the majority of neighbors claim malicious behavior, the node is flagged as malicious. The results are compared with the three-layered ANN for classification and SVM as the supervised learning model, Neurofuzzy Inference System (ANFIS), Particle Swarm Optimization (PSO) and fuzzy trust approach to detect black hole attack. An improvement in throughput, packet loss ratio, total network delay, normalized working load is observed.

TBSEER in [20] combines trust mechanisms with energy optimization techniques to create a network that is both resilient to attacks and energy efficient. Compared with TSSRM and TESRP, the performance of TBSEER against blackhole attack is increased by 37.5% and 62.5%, selective forwarding attacks increased by 15.38% and 30.77%. The average identification speed of TBSEER is 6.97% and 18.1% faster than TSSRM and TESRP, respectively. TBSEER has lower latency than TSSRM and TESRP, and the average latency is reduced by 6.74% and 18.31% , respectively.

The Machine Learning-Based Trust Model in [21] integrates machine learning algorithms with the traditional trust evaluation framework to improve the detection of blackhole attacks. Data about node behavior is collected, including the number of successful packet forwards, routing requests, acknowledgement's, and any packet drops or errors. Feedback from neighboring nodes about their interactions with each node is also collected to build an accurate picture of each node's behavior. The raw data is processed to extract relevant features that can be used to evaluate trustworthiness by considering packet forwarding rate, route consistency, response time and reputation score. A machine learning model is trained using labelled data (for supervised learning) or behavior patterns (for unsupervised learning). The model learns to classify nodes as trustworthy or malicious based on the collected features. After the model is trained, it is used to predict the trustworthiness of nodes in real-time. The trust value is calculated based on its behavior and the learned patterns. Nodes that exhibit anomalous behavior, such as consistently dropping packets or advertising invalid routes,

will be flagged as malicious. When selecting routes, a path with the highest trust score is selected, ensuring that data is routed through reliable and secure nodes. As the network evolves and new attacks are introduced, the machine learning model continues to learn from new data, improving its detection accuracy and adapting to changing attack patterns. By leveraging machine learning techniques, the system can intelligently detect malicious nodes, adapt to evolving network conditions, and make informed routing decisions that enhance network security and reliability.

To overcome the limitations of rank and blackhole attack, a trust-based IDS in [22] evaluates the behavior of nodes in the network. The trust metrics are based on the reliability and QoS of the node's routing decisions. Trust values are updated based on the node behavior and neighbor information and on the historical data. The protocol incorporates a feedback loop to isolate malicious nodes and protect the network from their harmful effects. The proposed IDS is tested through simulations in a variety of network scenarios. The protocol exhibits high detection rate for both rank and blackhole attacks, minimizes false alarms, ensures that legitimate nodes are not incorrectly flagged as malicious and low overhead, making the system suitable for resource-constrained environments like IoT.

The Secure EELB-AOMDV protocol [23] is an enhancement of AOMDV to improve both security and energy efficiency. The protocol introduces an energy-efficient load balancing mechanism that distributes traffic across multiple paths to prevent overburdening a single route and to conserve energy across the network. Nodes with higher residual energy are preferred, helping to ensure that routes remain viable over a longer period and do not quickly deplete node's battery. Load balancing ensures that no single node or link is overwhelmed, which helps in prolonging the lifetime of the network and reduces the chances of network failure due to energy exhaustion. An authentication mechanism where nodes authenticate each other's digital signatures and ensures that only authorized and legitimate nodes participate in the network. A reputation-based trust management is implemented, where each node maintains a reputation score based on the behavior of neighboring nodes. Trust scores are updated based on metrics such as successful packet forwarding, compliance with the expected route behaviors, and energy efficiency. Nodes with poor reputations are excluded from the routing process. When a node suspects that another node is behaving maliciously, it performs additional security checks such as crosschecking route replies from multiple nodes. If a black hole node is detected, it is isolated from the network, and other nodes are informed about the malicious behavior. This helps in preventing further damage and ensures the reliability of the network.

Comprehensive Trust-Based Routing in [24] uses a weighted combination of direct and indirect trust which uses packet forwarding ratio and recommendations from neighboring nodes to calculate trust score. Trust values are calculated through various parameters, such as packet forwarding reliability, energy consumption, and packet loss. The protocol offered higher packet delivery due to the filtering of malicious nodes, longer network lifetime by prioritizing energy-efficient, trustworthy nodes. An improvement in EED and throughput is achieved compared to other protocols.

TBSRS in [25] uses a trust-based relay selection mechanism to ensure selecting the safest relay nodes for data transmission based on trust evaluations. Each node monitors its neighboring nodes, evaluating their behavior to compute a trust score based on packet forwarding ratio, transmission delay and behavior consistency. Based on these metrics, a dynamic trust score is assigned to each node, which is periodically updated. Nodes use a threshold-based approach to filter out potential blackhole nodes. The protocol improves the detection rate, PDR, data integrity, network reliability, and energy efficiency, but the routing overhead is increased.

TAODV in [26] operates in three main stages: trust establishment, route discovery, and trust evaluation. When a node joins the network, it starts with an initial neutral trust value. Trust is established through packet-forwarding interactions with neighboring nodes, which gradually increases or decreases based on behavior. Source discovers route by sending a RREQ message. Intermediate nodes forward RREQs, considering both the shortest path and the trustworthiness of routes. If an intermediate node's trust score is below a set threshold, the node is excluded from the routing process. Nodes continuously monitor packet forwarding behavior. If a node consistently drops packets or behaves maliciously, its trust score is lowered. Nodes share trust information, so that trust scores are collaboratively maintained across the network. Security and reliability of data transmission is achieved by identifying and isolating black hole nodes, though it introduces some trade-offs in terms of processing overhead and complexity.

Authors in [27], proposed a methodology using mobile agents with authentication of nodes and trust values to detect blackhole nodes, which increases energy consumption and hence network lifetime, while reducing the PDR. The protocol is tested using different evaluation measures and the results show that the PDR is increased by 19.51%, the energy consumption is reduced by 53.3%, and network life is increased by 43.3%.

The Fuzzy Heuristics-Based Detection and Mitigation in [28]-[29] offers fuzzy logic to evaluate the behavior of nodes, based on PDR, latency, and routing behavior. The trust score reflects how likely the node is to be involved in malicious behavior, based on its past interactions and network performance. It adjusts to varying levels of network congestion, node density, and topology changes, which helps to maintain the robustness of the network against attacks. The fuzzy-based approach can be energy-efficient since it doesn't require heavy computational resources or continuous resource intensive monitoring. By using fuzzy inference systems, the detection and mitigation of attacks can be done with minimal overhead. The system focuses on evaluating key metrics rather than performing exhaustive checks across all network traffic, making it suitable for the resource-constrained networks. The performance of the protocol is measured in terms of detection rate, false positive/negative rate, energy consumption and network throughput.

In [30] a secure routing protocol which combines the Coot Chimp Optimization Algorithm (CCOA) and a Deep Q

Network (DQN) to enhance security and routing efficiency is proposed. The CCOA is a nature-inspired optimization algorithm based on the behaviors of two animals: The Coot and the Chimpanzee. The system optimizes routing decisions using the CCOA, which takes into account energy efficiency, link quality, and path reliability to select secure routes. Blackhole attack is detected through the Deep Q Network. It continuously monitors the network for any deviation in packet forwarding behavior. Nodes that consistently drop packets instead of forwarding them are identified as potential blackhole attackers. Q-values are adjusted based on the node's packet forwarding behavior, and malicious nodes are flagged if their Q-values indicate abnormal activity. This approach allows the system to adaptively learn and identify new patterns of blackhole attacks. The DQN-based system can identify attacks in real-time by continuously analyzing packet forwarding behavior and routing patterns. The combination of CCOA and DQN allows for both efficient routing and effective attack detection. CCOA optimizes the routing paths, while the DQN provides intelligent and adaptive learning for attack detection. This hybrid approach improves the overall security, efficiency, and robustness of the network, as it can handle the challenges posed by both dynamic routing conditions and evolving attack strategies. The protocol evaluated using detection accuracy, routing efficiency, network throughput, energy consumption and Latency.

The protocol in [31] focuses on identifying deviations from normal network behavior, such as irregular routing patterns or unusual delays. Nodes within the network continuously monitor routing behaviors and detect inconsistencies or irregularities in packet forwarding. When an anomaly is detected, such as a sudden drop in packet delivery or an increase in traffic to an unusually high number of nodes, the nodes generate anomaly reports. Cycling Anomaly Reports are circulated within the network to other nodes to ensure that anomalies are not isolated but instead acknowledged by multiple nodes. This helps to validate the existence of an attack and provides a distributed method of detection. The "cycling" refers to the repeated sharing of reports, ensuring that data about potential attacks is propagated and cross-checked throughout the network. Once an anomaly is confirmed, nodes can take measures such as avoiding routes through the suspected black hole, re-routing traffic, or using alternative routing protocols that are more resilient to attacks. As nodes continue to monitor and validate reported anomalies, they refine the network's understanding of attack patterns and improve their defenses over time. The feedback loop helps to adapt to evolving attack strategies. This approach enhances the resilience of wireless sensor networks by combining anomaly detection, collaborative defense, and dynamic response to attacks. It ensures that blackhole attacks are detected and mitigated swiftly, improving the overall reliability and security of the network.

5. Conclusion

In this survey, we have explored various protocols and strategies aimed at mitigating blackhole attacks in wireless networks. In blackhole attack, malicious nodes deceive the network into routing traffic through them, pose a significant threat to the reliability, security, and performance of the network. The paper highlights the importance of developing robust detection and prevention mechanisms to address these vulnerabilities. Through a comprehensive review of existing literature, we identified several techniques, such as secure routing protocols, anomaly detection methods, trust-based approaches, and cryptographic solutions, that have been proposed to combat blackhole attacks. While many of these solutions offer promising results, challenges remain in terms of scalability, energy efficiency, and the adaptability of protocols to dynamic network conditions. Further research is required to develop more effective, scalable, and lightweight solutions, focusing on integrating multiple defense mechanisms to enhance the robustness of WSNs.

References

[1] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," in IEEE International Conference on Machine Intelligence and Research Advancement, 2013, pp. 58–62.
[2] Riaz, Muhammad Noman, Attaullah Buriro, and Athar Mahboob. "Classification of attacks on wireless sensor networks: A survey." International Journal of Wireless and Microwave Technologies 8.6 (2018): 15-39.
[3] M. Shinde and D. Mehetre, "Black hole and selective forwarding attack detection and prevention in wsn," in IEEE International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2017, pp. 1–6.
[4] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik and A. ur Rehman, "Detection and prevention of Black Hole Attacks in IOT & WSN," 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 2018, pp. 217-226, doi: 10.1109/FMEC.2018.8364068.
[5] S. Naveena, C. Senthilkumar, and T. Manikandan, "Analysis and countermeasures of black-hole attack in manet by employing trust-based routing," in IEEE 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 1222–1227.
[6] Khan, Tayyab, and Karan Singh. "TASRP: a trust aware secure routing protocol for wireless sensor networks." International Journal of Innovative Computing and Applications 12.2-3 (2021): 108-122.
[7] M. Goswami, P. Sharma, and A. Bhargava, "Black hole attack detection in Manets using trust-based technique," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 4, pp. 1446–1451, 2020.
[8] S. K. Dhurandher, J. Singh, I. Woungang, R. Kumar, and G. Gupta, "Message trust-based secure multipath routing proto- col for opportunistic networks," International Journal of Communication Systems, vol. 33, no. 8, p. e4364, 2020.
[9] D. K. Sharma, S. Agarwal, S. Pasrija, and S. Kumar, "Etsp: Enhanced trust-based security protocol to handle blackhole attacks in opportunistic networks," in Advances in Data Sciences, Security and Applications: Proceedings of ICDSSA 2019. Springer, 2020, pp. 327–340.
[10] N. Bhalaji, K. Hariharasudan, and K. Aashika, "A trust-based mechanism to combat blackhole attack in rpl protocol," in System Reliability, Quality Control,

Safety, Maintenance and Management: Applications to Electrical, Electronics and Computer Science and Engineering. Springer, 2020, pp. 457–464.
[11] N. Khanna and M. Sachdeva, "Best: Battery, efficiency and stability-based trust mechanism using enhanced aodv for mitigation of blackhole attack and its variants in Manets." Adhoc & Sensor Wireless Networks, vol. 46, 2020.
[12] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "Qos aware trust-based routing algorithm for wireless sensor networks," Wireless Personal Communications, vol. 110, pp. 1637–1658, 2020.
[13] P. Rodrigues and J. John, "Joint trust: An approach for trust- aware routing in wsn," Wireless Networks, vol. 26, no. 5, pp. 3553–3568, 2020.
[14] P. A. Patil, R. S. Deshpande, and P. B. Mane, "Trust and opportunity-based routing framework in wireless sensor net- work using hybrid optimization algorithm," Wireless Personal Communications, vol. 115, pp. 415–437, 2020.
[15] J. Ni, W. Huang, and W. Zhang, "Secure routing based on trust management in ad-hoc networks," in LISS2019: Proceedings of the 9th International Conference on Logistics, Informatics and Service Sciences. Springer, 2020, pp. 351–361.
[16] V. A. Kanthuru and K. A. Kumar, "Black hole detection and mitigation using active trust in wireless sensor networks," in Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML 2020. Springer, 2021, pp. 25–34.
[17] H. Jari, A. Alzahrani, and N. Thomas, "A novel indirect trust mechanism for addressing black hole attacks in manet," in Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, 2021, pp. 27–34.
[18] S. Nosratian, M. Moradkhani, and M. B. Tavakoli, "Fuzzy-based reliability prediction model for secure routing protocol using ga and tlbo for implementation of black hole attacks in wsn," Journal of Circuits, Systems and Computers, vol. 30, no. 06, p. 2150098, 2021.
[19] G. Farahani, "Black hole attack detection using k-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks," Security and communication Networks, vol. 2021, no. 1, p. 8814141, 2021.
[20] H. Hu, Y. Han, M. Yao, and X. Song, "Trust based secure and energy efficient routing protocol for wireless sensor networks," IEEE access, vol. 10, pp. 10 585–10 596, 2021.
[21] S. Shanmugam, K. Prathapchandran, T. Janani et al., "Mitigating black hole attacks in routing protocols using a machine learning-based trust model," International Journal of Sociotechnology and Knowledge Development (IJSKD), vol. 14, no. 1, pp.1–23, 2022.
[22] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "A trust-based intrusion detection system for rpl networks: Detect- ing a combination of rank and blackhole attacks," Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 124–153, 2022.
[23] B. S. Rani and K. Shyamala, "Secure eelb-aomdv protocol to mitigate blackhole attack," in IEEE 9th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, 2023, pp. 589–592.
[24] B.Sandhya Rani, "Comprehensive trust-based routing protocol to mitigate black-hole attack in wireless sensor networks," International Journal on Recent and Innovation Trends in Computing and Communication, 2023.
[25] S. Arvind and B. Ajay, "Trust based safe relay selection strategy towards prevention of black hole attack in wireless sensor network," in IEEE 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC), 2023, pp. 1–5.
[26] M. P. S. Chaitanya, B. S. Chowdary, P. L. Prasanna, M. Priyanka, and K. Tejaswi, "Taodv trust based aodv protocol in Manets to mitigate black hole effect," in IEEE International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 2023, pp. 1348–1355.
[27] H. Ashraf, F. Khan, U. Ihsan, F. Al-Quayed, N. Jhanjhi, and M. Humayun, "Mabpd: Mobile agent-based prevention and black hole attack detection in wireless sensor networks," in IEEE International Conference on Business Analytics for Technology and Security (ICBATS), 2023, pp. 1–11.
[28] K. Mohanraj and B. Arivazhagan, "Detection and mitigation of black hole attack using fuzzy heuristics in mobile adhoc network (manet)," Library of Progress-Library Science, Information Technology & Computer, vol. 44, no. 3, 2024.
[29] S. Ravindran, "Intelligent fuzzy logic-based intrusion detection system for effective detection of black hole attack in wsn," Peer- to-Peer Networking and Applications, pp. 1–17, 2024.
[30] D. Sunitha and P. Latha, "A secure routing and black hole attack detection system using coot chimp optimization algorithm-based deep q network in manet," Computers & Security, vol. 148, p. 104166, 2025.
[31] M. A. Vieira and H. Liu, "Defense against black hole attacks in wireless sensor network with anomaly report cycling," in IEEE International Wireless Communications and Mobile Computing (IWCMC), 2024, pp. 1570–1576.