International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 13, Issue 01, January 2024)

Review of Blackhole Attack in Wireless Sensor Networks

Hemant Dhoot[1], Prof. Suresh S. Gawande[2]

[1]*Research Scholar,* [2]*Head of Department, Dept. of Electronics & Communication Eng., Bhabha Engineering Reasearch Institute, Bhopal, India*

***Abstract*— Wireless Sensor Networks (WSNs) have gained prominence in various applications, ranging from environmental monitoring to industrial automation. However, the distributed and resource-constrained nature of WSNs makes them susceptible to security threats, such as the Blackhole attack. The Blackhole attack involves malicious nodes diverting or dropping data packets, disrupting communication and potentially compromising the network's integrity. This paper provides a comprehensive review of the Blackhole attack in WSNs, encompassing its impact, detection, prevention, and mitigation strategies. Various techniques, including cryptographic protocols, intrusion detection systems, trust-based mechanisms, and energy-efficient routing, are examined in the context of addressing this threat.**

***Keywords*— WSN, Black hole attack, Detection, Routing.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a transformative technology, enabling real-time data collection, monitoring, and analysis across diverse domains. These networks consist of a multitude of small, low-cost sensor nodes with limited computational capabilities, memory, and energy resources. While WSNs offer unprecedented advantages, their inherent vulnerabilities render them susceptible to a range of security threats. One such formidable threat is the Blackhole attack, which exploits the decentralized nature of WSNs to disrupt communication and compromise data integrity.

The Blackhole attack represents a malicious activity where a compromised or rogue node, referred to as a "Blackhole" node, selectively drops or diverts incoming data packets. This insidious behavior disrupts the intended flow of information, potentially leading to data loss, network congestion, and a degradation of overall network performance. The consequences of Blackhole attacks can be dire, particularly in applications where timely and accurate data transmission is critical, such as environmental monitoring, disaster response, and industrial automation.

This study delves into a comprehensive exploration of the Blackhole attack in Wireless Sensor Networks. We examine the attack's operational mechanisms, potential impact on network performance, and the challenges it poses to ensuring reliable and secure data communication. Moreover, we discuss various strategies for detecting, preventing, and mitigating Blackhole attacks, shedding light on the innovative approaches that researchers have developed to safeguard WSNs against this menacing threat.

This study not only contributes to a deeper understanding of the intricacies surrounding Blackhole attacks but also provides a valuable resource for network administrators, researchers, and stakeholders seeking effective measures to fortify the security of Wireless Sensor Networks. By comprehending the nuances of this threat and implementing robust countermeasures, we can bolster the resilience of WSNs and promote their continued adoption across diverse and critical applications.

The development of Wireless Sensor Networks (WSNs) in real-time applications is being driven by healthcare services and people's position/status being continually tracked in progressive mode. The security gap between existing WSN plans and daily application requirements remains unknown, despite the expanded scope of potential application systems, which now includes in-hospital, home monitoring, pre-hospital facility, and mobile, as well as long-term database gathering for longitudinal pattern investigation. In terms of communication, energy management, and processing, WSN devices are, for the most part, severely constrained [1].

The rising use of portable devices with advanced wireless communication gives Mobile ad-hoc networks more significance with the expanding number of widespread applications. This infrastructure uses a link-to-link wireless connection to transfer the data called route, which uses a routing protocol. AODV is a reactive protocol that uses control packets to discover a route toward the destination node in the network. Since MANET is an open infrastructure without a centralized controller, it is at risk of security assaults that are generated through the malicious node at the time of route discovery and data transmission.

For example, the Blackhole attack in which the offender node retains and drops few or all data/control packets by using vulnerabilities of the on-demand routing protocols [2].

Blackhole attack is one of the major security concerns in mobile ad-hoc networks that are hard to detect. In this type of attack, the malicious node attracts message packets by advertising itself as a cooperating node but eventually drops them, thus heavily degrading the network performance. This attack becomes a more serious threat in Opportunistic Networks due to the absence of any predefined path of trustworthy nodes between source and destination.

II. Literature Survey

A. Revathi et al.,[1] presented the Blackhole attack Detection based on Trust Calculation (BDTC) Mechanism for the identification of malicious node in the WSN. Black hole attack identification mechanism for the detection of malicious node has introduced. This approach is extended to develop the communication type of attack in the network. This approach executes the novel Weighted Clustering and Security Algorithm (WCSA) to choose Cluster Heads procuring into consideration the mobile nodes battery power, mobility, ideal degree (number of neighbors), and transmission power.

E. Lema et al.,[2]presented a trust-based method to prevent the network against blackhole attack. This paper modeled the behavior of blackhole node and proposes a trust-based security technique. Further suggested technique is analyzed and evaluated against various evaluation metrics like PDR, throughput, end-to-end delay, attack percentage, etc. The proposed security technique is also compared with three different scenarios, namely attack, watchdog, and IDS scenarios, using the above evaluation metrics.

A. V. Jatti et al.,[3] presented the denial of service (DoS) attack namely black hole attacks in ad hoc on-demand distance vector (AODV) routing protocol. In this study three methods are considered viz, normal AODV, black hole AODV (BH_AODV), and black hole mitigation AODV (M_BH_AODV). Black hole mitigation that is detection and prevention is done as per trust based scheme. Three methods that is normal AODV, BH_AODV, and M_BH_AODV protocols are examined for different quality of service (QoS) parameters, i.e., packet delivery ratio (PDR), end-to-end delay, and overhead with varying the number of nodes. To simulate the network topologies network simulation software NS-2.35 was employed. The software does not have in built mechanism to simulate rouge node protocols.

W. Choukri et al.,[4] The routing protocol for low-power and lossy networks (RPL) was developed specifically for constrained communication. Considering its constrained nature, RPL-based Networks can be accessible by trusted and untrusted global users via the Internet and can be subject to serious attacks. Routing attacks are especially difficult to be identified when they occur. However, Deep Learning techniques can be leveraged in detecting network intrusions. This work comes up with a new deep learning-based framework for routing attack detection in unsecured RPL networks. It allows analyzing and processing the network traffic, extracting features, and defining target-based intrusion thresholds, which leads to the detection of routing attacks.

P. P. Ioulianou et al.,[5] Although IoT security is a field studied extensively, recent attacks such as BotenaGo show that current security solutions cannot effectively stop the spread of IoT attacks. Machine Learning (ML) techniques are promising in improving protection against such attacks. In this work, three supervised ML algorithms are trained and evaluated for detecting rank and blackhole attacks in RPL-based IoT networks. Extensive simulations of the attacks are implemented to create a dataset and appropriate fields are identified for training the ML model. We use Google AutoML and Microsoft Azure ML platforms to train our model. Our evaluation results show that ML techniques can be effective in detecting rank and blackhole attacks, achieving a precision of 93.3%.

S. Barai et al.,[6] presented a technique to identify the potential Blackhole nodes present in the network. With the knowledge of such a list and minor modification of the traditional Spray-and-Wait Routing protocol, we were able to mitigate the effect of Blackhole attack on the network performance. Simulation results show improvement in the network performance in terms of delivery ratio and the number of dropped messages, even in the presence of Blackhole nodes. It has also been observed that traditional routing protocols like Epidemic, Prophet and Spray-and-Wait routing, perform better if the paths containing the suspected nodes detected by our proposed method are avoided.

A. U. Khan et al.,[7] There is one malicious node in a single black-hole attack that can act as the node with the highest sequence number. The node source would follow the direction of the malicious node by taking the right direction. There is more than one malicious node in the collaborative black-hole attack. One node receives a packet and sends it to another malicious node in this attack. It is very difficult to detect and avoid black-hole attacks. Many researchers have invented black-hole attack detection and prevention systems. In this paper, find a problem in the existing solution, in which validity bit is used.

This work also provides a comparative study of many scholars. The source node is used to detect and prevent black hole attacks by using a binary partition clustering based algorithm.

T. Terai et al.,[8] Blackhole (BH) attacks are one of the most serious threats in mobile ad-hoc networks. A BH is a security attack in which a malicious node absorbs data packets and sends fake routing information to neighboring nodes. BH attacks are widely studied. However, existing defense methods wrongfully assume that BH attacks cannot overcome the most common defense approaches. A new wave of BH attacks is known as smart BH attacks. In this study, we used a highly aggressive type of BH attack that can predict sequence numbers to overcome traditional detection methods that set a threshold to sequence numbers. To protect the network from this type of BH attack, we propose a detection-and-prevention method that uses local information shared with neighboring nodes.

R. Saputra et al.,[9] Wireless Sensor Network (WSN) is a heterogeneous type of network consisting of scattered sensor nodes and working together for data collection, processing, and transmission functions. Because WSN is widely used in vital matters, aspects of its security must also be considered. There are many types of attacks that might be carried out to disrupt WSN networks. The methods of attack that exist in WSN include jamming attack, tampering, Sybil attack, wormhole attack, hello flood attack, and, blackhole attack. Blackhole attacks are one of the most dangerous attacks on WSN networks. Enhanced Check Agent method is designed to detect black hole attacks by sending a checking agent to record nodes that are considered black okay.

F. Taranum et al.,[10] Mobile Adhoc networks (MANETs) comprises of mobile devices or nodes that are connected wirelessly and have no infrastructure. Detecting malicious activities in MANETs is a challenging task as they are vulnerable to attacks where the performance of the entire network degrades. Hence it is necessary to provide security to the network so that the nodes are prone to attack. Selecting a good routing protocol in MANET is also important as frequent change of topology causes the route reply to not arrive at the source node.

III. Challenges

The detection and mitigation of Blackhole attacks in Wireless Sensor Networks (WSNs) pose a series of intricate challenges, stemming from the unique characteristics of WSNs and the sophisticated nature of the attack itself.

Addressing these challenges is essential to ensure the security and reliability of WSNs in the face of evolving cyber threats. The following are some of the key challenges associated with detecting and mitigating Blackhole attacks:

- *Limited Resources:* Sensor nodes in WSNs operate with constrained computational power, memory, and energy resources. Implementing sophisticated intrusion detection and prevention mechanisms must strike a delicate balance between accuracy and resource efficiency, as resource-intensive approaches can potentially lead to network performance degradation.
- *Dynamic Network Topology:* WSNs often operate in dynamic and ad hoc environments, where nodes may join, leave, or change their positions frequently. This dynamic topology complicates the establishment of secure and trusted communication paths, making it challenging to differentiate between legitimate route changes and those induced by Blackhole attacks.
- *Asymmetric Communication:* In many WSNs, communication patterns are asymmetric, with nodes having different roles and responsibilities. The malicious insertion of Blackhole nodes into the network can exploit these asymmetries to divert traffic, making it difficult to discern abnormal behavior solely based on traffic patterns.
- *Cooperative Detection:* Collaborative detection mechanisms that rely on nodes sharing information about detected anomalies may be vulnerable to attacks where malicious nodes intentionally provide false information to mislead the detection process.
- *False Positives and Negatives:* Intrusion detection systems aimed at identifying Blackhole attacks can generate false positives (identifying normal nodes as attackers) or false negatives (failing to detect actual Blackhole nodes). Balancing sensitivity and specificity in detection algorithms is essential to minimize these errors.
- *Secure Routing Protocols:* Many existing secure routing protocols for WSNs are computationally intensive and may lead to increased energy consumption. Developing lightweight yet effective secure routing protocols that can withstand Blackhole attacks without exhausting node resources is a significant challenge.
- *Trust Establishment:* Building and maintaining trust among nodes in a decentralized WSN environment is complex. Determining which nodes are reliable and trustworthy, especially when nodes may exhibit varying levels of trustworthiness over time, poses a challenge.

IV. Detection And Prevention

Detecting and preventing Blackhole attacks in Wireless Sensor Networks (WSNs) is a complex endeavor that requires a combination of innovative techniques and strategies. This section explores various approaches designed to identify and mitigate the risks posed by Blackhole attacks, ensuring the secure operation of WSNs.

A. *Cryptographic Solutions:* Cryptographic techniques provide a foundation for securing WSNs against Blackhole attacks. Digital signatures, certificates, and encryption can authenticate the identity of nodes and protect the integrity of data transmissions. By ensuring that routing information is genuine and untampered, cryptographic methods hinder attackers from manipulating network routing paths.

B. *Intrusion Detection Systems (IDS):* Intrusion Detection Systems monitor network traffic and behavior patterns to identify abnormal activities indicative of Blackhole attacks. Anomaly-based IDS algorithms compare current behavior against established baselines, while signature-based methods rely on predefined patterns of attack. Balancing detection accuracy with minimal resource consumption is crucial to ensure that IDS mechanisms do not overly burden the constrained resources of sensor nodes.

C. *Trust-Based Approaches:* Trust-based mechanisms foster collaboration among nodes by assigning trust levels based on past interactions and behavior. Nodes with higher trust ratings are favored in routing decisions, reducing the chances of malicious nodes being included in communication paths. However, the challenge lies in establishing and updating trust in a dynamic and resource-constrained environment.

D. *Energy-Efficient Routing Protocols:* Energy-efficient routing protocols indirectly mitigate Blackhole attacks by optimizing energy consumption. Such protocols prolong network lifetime by selecting routes that minimize energy expenditure. The additional energy required by malicious nodes to carry out their attacks makes them less attractive choices for routing, thus reducing their impact.

E. *Collaborative Detection:* Collaborative detection involves nodes sharing information about potential attackers or suspicious behavior. By aggregating observations from multiple nodes, the network can collectively identify and isolate Blackhole nodes. However, ensuring the authenticity and reliability of shared information is a challenge, as malicious nodes may attempt to deceive the collaborative process.

F. *Behavioral Analysis:* Behavioral analysis employs machine learning and statistical techniques to discern normal behavior from abnormal patterns associated with Blackhole attacks. By continuously monitoring and analyzing network traffic, behavioral analysis can adapt to evolving attack strategies and provide real-time detection. This approach, however, may require a training period to establish a baseline behavior.

G. *Node Reputation Systems:* Reputation systems assign reputation scores to nodes based on their historical behavior. Nodes with higher reputation scores are considered more trustworthy in routing decisions. This discourages malicious nodes from participating in Blackhole attacks, as their actions would lead to a decline in reputation and subsequent exclusion from routing paths.

V. Conclusion

Blackhole attack stands as a significant and pervasive threat within the realm of Wireless Sensor Networks (WSNs), highlighting the critical importance of robust security measures in ensuring the integrity, reliability, and effectiveness of these networks. As WSNs become increasingly integrated into various applications, from environmental monitoring to healthcare and beyond, the need to safeguard these networks against malicious actors becomes paramount. This paper has delved comprehensively into the intricacies of the Blackhole attack, examining its potential impact on WSNs and presenting various strategies for its detection, prevention, and mitigation.

REFERENCES

[1] A. Revathi and S. G. Santhi, "Blackhole attack Detection based on Trust Calculation Mechanism in Wireless Sensor Networks," 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2022, pp. 1-4, doi: 10.1109/ICAECT54875.2022.9807980.

[2] 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.

[3] A. V. Jatti and V. J. K. Kishor Sonti, "Performance Improvements of Routing Protocol by Blackhole Detection using Trust Based Scheme," 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Amman, Jordan, 2022, pp. 159-164, doi: 10.1109/MENACOMM57252.2022.9998237.

[4] W. Choukri, H. Lamaazi and N. Benamar, "A Novel Deep Learning-based Framework for Blackhole Attack Detection in Unsecured RPL Networks," 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, 2022, pp. 457-462, doi: 10.1109/3ICT56508.2022.9990664.

[5] P. P. Ioulianou, V. G. Vassilakis and S. F. Shahandashti, "ML-based Detection of Rank and Blackhole Attacks in RPL Networks," 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal, 2022, pp. 338-343, doi: 10.1109/CSNDSP54353.2022.9908049.

[6] S. Barai and P. Bhaumik, "Detection and Mitigation of Blackhole Attack Effect in Opportunistic Networks," 2021 19th OITS International Conference on Information Technology (OCIT), Bhubaneswar, India, 2021, pp. 155-160, doi: 10.1109/OCIT53463.2021.00040.

[7] A. U. Khan, R. Puree, B. K. Mohanta and S. Chedup, "Detection and Prevention of Blackhole Attack in AODV of MANET," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2021, pp. 1-7, doi: 10.1109/IEMTRONICS52119.2021.9422643.

[8] 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.

[9] R. Saputra, J. Andika and M. Alaydrus, "Detection of Blackhole Attack in Wireless Sensor Network Using Enhanced Check Agent," 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia, 2020, pp. 1-4, doi: 10.1109/ICIC50835.2020.9288571.

[10] F. Taranum, A. Sarvat, N. Ali and S. Siddiqui, "Detection and Prevention of Blackhole node," 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2020, pp. 1-7, doi: 10.1109/IEMENTech51367.2020.9270072.