IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Detection of Black Hole Attack in Wireless Sensor Network Using Enhanced Check Agent

S Rajesh[1], S Ahamed Thouban Asat[2], S Badhri[3], S R Mani Bharathi[4]

[1]Assistant Professor (Sl, Gr), Dept of CSE

[2, 3, 4]Dept of CSE

[1, 2, 3, 4] Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nādu, India

Abstract: *Wireless Sensor Networks (WSNs) are increasingly utilized in critical applications, making them vulnerable to various security threats, particularly black hole attacks. These attacks significantly degrade network performance by maliciously dropping all received packets. This research proposes an Enhanced Check Agent (ECA) mechanism designed to detect and mitigate black hole attacks in WSNs. The proposed method continuously monitors node behavior, verifies data forwarding integrity, and identifies anomalies in routing patterns. Through simulation and performance evaluation, the ECA demonstrates improved detection accuracy and reduced packet loss compared to traditional techniques. The approach enhances the overall reliability and security of data transmission in WSN environments.*

Keyword Index: Black Hole Attack, Network Security, Enhanced Check Agent (ECA), Intrusion Detection, Secure Routing, Packet Dropping Attack, Node Behavior Monitoring, Data Integrity, Trust-based Detection

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a vital technology in various domains such as environmental monitoring, military surveillance, healthcare, and industrial automation. These networks consist of lightweight, low-power sensor nodes that collaborate to collect and transmit data across the network. Due to their deployment in open and often unattended environments, WSNs are highly susceptible to various security threats, with black hole attacks being among the most severe. Such vulnerabilities not only compromise data integrity but also affect the overall performance and reliability of the network.

A black hole attack occurs when a malicious node falsely advertises the shortest path to the destination node, thereby attracting all the data packets. Once the packets are received, the malicious node drops them instead of forwarding, causing a significant loss of critical information. Traditional routing protocols in WSNs are not equipped with adequate mechanisms to detect and prevent such deceptive behavior. This makes the detection of black hole attacks a crucial challenge in ensuring secure communication within WSNs.

Several detection techniques have been proposed in the past, ranging from trust-based systems to anomaly detection methods. However, many of these approaches suffer from limitations such as high energy consumption, increased computational complexity, or inability to detect sophisticated attacks. There is a growing need for lightweight, accurate, and energy-efficient mechanisms that can promptly identify malicious activity without degrading network performance. The focus should be on maintaining a balance between security and the limited resources of sensor nodes.

This research introduces an Enhanced Check Agent (ECA) designed to effectively detect black hole attacks in WSNs. The ECA operates by monitoring the behavior of nodes in real time, analyzing their packet forwarding patterns, and comparing them with expected behavior metrics. By identifying inconsistencies and sudden changes in routing patterns, the system can accurately isolate the malicious nodes involved in black hole activities. The proposed method aims to reduce false positives and maintain high detection accuracy with minimal impact on node resources.

In conclusion, the Enhanced Check Agent provides a promising solution to the ongoing challenge of black hole attack detection in WSNs. By integrating behavioral monitoring with intelligent detection mechanisms, the approach strengthens the network's defense while preserving its efficiency. This work not only contributes to the field of wireless network security but also lays the foundation for future enhancements in intrusion detection for resource-constrained environments.

II. RELATED WORK

Over the years, researchers have proposed various techniques to combat black hole attacks in Wireless Sensor Networks (WSNs). Many early approaches focused on modifying routing protocols such as AODV (Ad hoc On-Demand Distance Vector) to include mechanisms that detect packet dropping. These modified protocols typically rely on the exchange of routing information and the verification of route authenticity. Although effective in some cases, these methods often introduce additional routing overhead and are limited in detecting collaborative black hole attacks, where multiple nodes act maliciously.

Trust-based models have also been extensively explored for black hole detection. In these approaches, each node assigns trust scores to its neighbors based on their behavior, particularly in forwarding packets. Nodes that consistently fail to forward packets see a reduction in trust levels and are eventually isolated. While this method enhances the network's resilience to attack, it can be susceptible to false positives, particularly in dynamic environments where nodes may drop packets due to network congestion or battery depletion rather than malicious intent.

Another significant category of detection techniques involves watchdog and path rater mechanisms. The watchdog monitors the forwarding behavior of neighboring nodes, while the path rater evaluates the reliability of different routes based on observed behavior. Though this technique provides a proactive solution, it often struggles in environments with high mobility or limited line-of-sight communication, where direct monitoring becomes challenging. Additionally, watchdog-based methods may consume considerable energy due to continuous monitoring, which is not ideal for resource-constrained WSNs.

Machine learning and anomaly detection techniques have also been proposed to identify black hole attacks by learning normal network behavior and flagging deviations. These solutions demonstrate high accuracy but require significant training data and computational resources. The limitations of energy and processing power in WSN nodes make such approaches less feasible for real-time deployment. Furthermore, the adaptability of machine learning models to new or evolving attack strategies remains a topic of ongoing research.

Considering these limitations, the development of lightweight, efficient, and accurate detection methods is essential. The Enhanced Check Agent (ECA) proposed in this study addresses these challenges by combining behavioral analysis with an intelligent decision-making process to identify malicious nodes. Unlike traditional methods, the ECA minimizes resource consumption while maintaining high detection accuracy, making it a practical solution for real-world WSN applications. By learning from the strengths and weaknesses of existing approaches, the ECA aims to provide a balanced and robust defense against black hole attacks.

III. PROBLEM STATEMENT

Wireless Sensor Networks (WSNs) are highly vulnerable to security threats due to their decentralized nature, limited computational resources, and deployment in open environments. Among these threats, black hole attacks pose a significant risk by causing malicious nodes to falsely claim optimal routes and then drop all intercepted data packets. This leads to severe data loss, network performance degradation, and compromised system reliability.

Traditional detection mechanisms often suffer from high energy consumption, low detection accuracy, and an inability to adapt to dynamic attack patterns. Furthermore, many existing solutions lack the efficiency to differentiate between malicious packet drops and those caused by network conditions such as congestion or node failure. Therefore, there is a critical need for a lightweight, accurate, and energy-efficient mechanism capable of identifying black hole attacks in real-time without imposing significant overhead. This research aims to address these challenges by introducing an Enhanced Check Agent (ECA) to monitor node behavior and detect anomalies effectively, ensuring secure and reliable data transmission in WSNs.

IV. EXISTING SYSTEM

While the Enhanced Check Agent (ECA) provides an efficient mechanism for detecting black hole attacks in Wireless Sensor Networks (WSNs), certain limitations still persist.

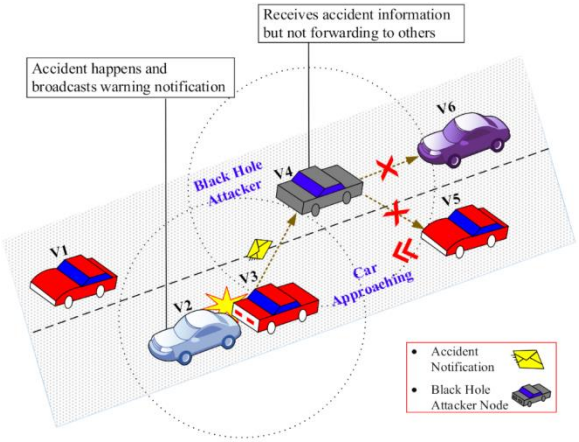

Figure 1: Prevention of Black Hole Attack in VANETs

One notable disadvantage is the potential increase in processing load due to continuous behavior monitoring, which can impact the lifetime of energy-constrained sensor nodes. Additionally, in dense network environments, the overhead generated by check agents communicating and verifying multiple nodes might lead to congestion or delayed data transmission. The accuracy of detection could also be affected in scenarios involving multiple coordinated attackers, making it difficult to distinguish between genuine packet loss and malicious activity. Moreover, the system may require periodic updates or reconfiguration to remain effective against evolving attack strategies, which can be resource-intensive. Despite these challenges, the ECA remains a promising approach, but further optimization is needed to balance security with energy efficiency and network scalability.

V. PROPOSED SYSTEM

The proposed system introduces an Enhanced Check Agent (ECA) framework to effectively detect and isolate black hole attacks in Wireless Sensor Networks (WSNs). This approach focuses on real-time monitoring of node behavior by embedding intelligent agents within selected sensor nodes. These agents actively track data forwarding activities, analyze routing patterns, and identify discrepancies that indicate potential malicious behavior. The ECA uses lightweight algorithms to ensure minimal energy consumption while maintaining high detection accuracy. When a node is suspected of being malicious, the agent flags it and informs neighboring nodes to avoid routing through it. By integrating behavioral analysis and trust evaluation, the system enhances network security without compromising performance or resource efficiency. The proposed method is scalable, adaptable to dynamic network conditions, and aims to ensure secure and reliable data transmission within WSNs.

VI. SYSTEM MODEL

The proposed system model for detecting black hole attacks in Wireless Sensor Networks (WSNs) using an Enhanced Check Agent (ECA) consists of several interconnected components designed to work in a systematic and efficient manner. Initially, the WSN is deployed with multiple sensor nodes distributed across a geographical area, where each node is responsible for sensing, processing, and forwarding data. These nodes communicate using a routing protocol such as AODV or DSR.

Enhanced Check Agent is embedded in selected nodes, known as monitoring nodes, which are strategically placed to observe the behavior of neighboring nodes.

VII. SIMULATION RESULTS

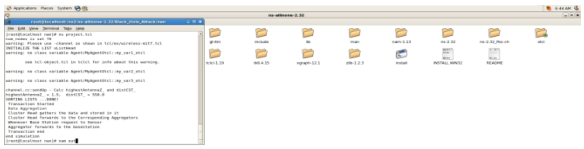

Figure 2: Simulation Command

The second step involves the ECA continuously monitoring the packet forwarding behavior of nearby nodes, recording metrics such as packet delivery rate, forwarding history, and routing requests.

Figure 3: Block Hole attacks in Wireless Sensor Networks (WSNs)

Last but not least, I am deeply grateful to my family for their unwavering support and encouragement, without which this research would not have been possible.

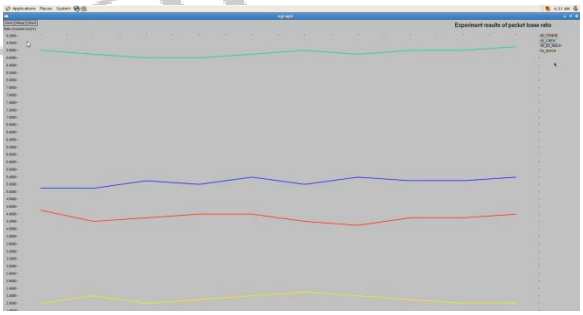

Figure 4: Result Graph

VIII.CONCLUSION

A novel approach using an Enhanced Check Agent (ECA) was proposed to detect and mitigate black hole attacks in Wireless Sensor Networks (WSNs). The method focuses on real-time monitoring and analysis of node behavior to identify malicious activities, particularly packet dropping by compromised nodes. By integrating intelligent decision-making mechanisms and cooperative verification among nodes, the system successfully isolates black hole attackers

without introducing significant energy or computational overhead. This makes it a suitable solution for resource-constrained environments, ensuring secure and reliable data transmission across the network.

The Enhanced Check Agent approach proves to be both effective and efficient in comparison to traditional detection techniques, offering improved detection accuracy and quicker response to threats. It strengthens the overall security of WSNs by proactively identifying attacks and updating routing paths to avoid compromised nodes. Future enhancements may include adapting the system to counter other types of routing attacks and incorporating machine learning for more adaptive threat detection. Overall, the proposed solution contributes to building more resilient and trustworthy wireless sensor networks.

IX.ACKNOWLEDGEMENT

"Detection of Black Hole Attack in Wireless Sensor Network Using Enhanced Check Agent." First and foremost, I would like to thank my supervisor, Dr.S.Rajesh ,Assistant Professor (SL.Gr), for their constant guidance, valuable insights, and unwavering support throughout the course of this study. Their expertise and constructive feedback have been indispensable in shaping this work. I also extend my gratitude to Sri Ramakrishna Institute of Technology, Coimbatore, for providing the resources and facilities that enabled me to carry out my research. Special thanks to my colleagues and friends who offered their encouragement and assistance, particularly during the challenging phases of the project.

REFERENCES

[1] **Bhushan, B., & Saini, R. (2014).** *Black hole attack detection and prevention in wireless sensor networks: A review.* International Journal of Computer Applications, 99(8), 1-6.

[2] **Dhanalakshmi, R., & Tharshini, P. (2016).** *Detection and prevention of black hole attack in wireless sensor networks.* International Journal of Advanced Research in Computer Science, 7(3), 37-40.

[3] **Vijayakumar, V., & Suresh, P. (2013).** *Detection of black hole attacks in wireless sensor networks using trust based model.* Procedia Computer Science, 19, 767-774.

[4] **Singh, A., & Bansal, J. (2016).** *Detection and prevention of black hole attack in wireless sensor networks using AODV protocol.* International Journal of Computer Applications, 139(1), 29-35.

[5] **Chen, X., & Li, H. (2014).** *A review on detection and prevention of black hole attacks in wireless sensor networks.* International Journal of Computer Science and Mobile Computing, 3(4), 18-25.

[6] **Subramanian, V., & Sivakumar, R. (2012).** *Detection of black hole attack using watchdog technique in wireless sensor networks.* Procedia Engineering, 38, 1641-1645.

[7] **Gupta, R., & Kumar, A. (2017).** *Detection and prevention of black hole attacks in wireless sensor networks using hybrid AODV protocol.* International Journal of Computer Applications, 157(6), 32-36.

[8] **Ranjan, P., & Agrawal, D. (2017).** *A review on black hole attack detection and prevention techniques in wireless sensor networks.* International Journal of Computer Science and Information Security, 15(6), 245-249.

[9] **Latha, P., & Chandrasekar, V. (2014).** *Detection and mitigation of black hole attack using improved AODV in wireless sensor networks.* International Journal of Computer Networks & Communications, 6(5), 21-28.

[10] **Rani, R., & Soni, M. (2015).** *Prevention of black hole attack in wireless sensor networks using multi-path routing protocol.* International Journal of Advanced Research in Computer Science, 6(4), 15-18.

[11] **Singh, N., & Gupta, P. (2017).** *Black hole attack detection in wireless sensor networks using threshold-based method.* International Journal of Computer Applications, 169(4), 34-39.

[12] **Patil, S., & Chavan, S. (2018).** *Detection and prevention of black hole attacks in wireless sensor networks using artificial neural networks.* Journal of Electrical Engineering & Technology, 13(1), 323-328.

[13] **Kumar, M., & Singh, A. (2015).** *Black hole attack prevention in wireless sensor networks using cooperative strategies.* International Journal of Computer Applications, 118(20), 39-43.

[14] **Ramani, G., & Srinivasan, S. (2016).** *Detection of black hole attacks in wireless sensor networks using AODV protocol and secure routing algorithm.* Journal of Computer Networks and Communications, 2016, Article ID 7864087.