https://doi.org/10.48047/AFJBS.6.13.2024.4813-4821

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

A COMPREHENSIVE ANALYSIS OF SINKHOLE ATTACK DETECTION AND PREDICTION IN WIRELESS SENSOR NETWORKS

Mrs.J.Gnana Mano Sheebha,
Research Scholar,
sheebhabovas@gmail.com,
RVS College of Arts and Science(Autonomous),Sulur,
Coimbatore, Tamil Nadu, India

Dr.D.Maheswari,
Head & Research Coordinator
School of Computer Studies-PG
maheswari@rvsgroup.com
RVS College of Arts and Science (Autonomous),Sulur,
Tamil Nadu, India

Article History
Volume 6, Issue 13, July 2024
Received: 04 June 2024
Accepted: 05 July 2024
doi:
10.48047/AFJBS.6.13.2024.4813-4821

Abstract

Sinkhole attacks represent a significant security threat in Wireless Sensor Networks (WSNs) and the Internet of Things (IoT), where compromised nodes deceitfully attract network traffic to disrupt normal operations. This survey paper comprehensively reviews contemporary techniques developed to detect and mitigate sinkhole attacks, comparing their methodologies, strengths, and limitations. Various approaches are explored, including knowledge-based rules, cross-layer integrations, Machine learning models, trust-based protocols, and algorithmic detection methods. Each technique is assessed based on its detection accuracy, implementation complexity, resource requirements, and adaptability to evolving threats. The comparative analysis aims to provide insights into the effectiveness of these methods under different network conditions and attack scenarios. By highlighting the advantages and disadvantages of each approach, this survey has taken several research papers to analyze the resilience of WSNs and IoT networks against sinkhole attacks. Through this detailed examination, the paper underscores the necessity for integrated and adaptive solutions that balance security, efficiency, and scalability to safeguard the growing landscape of interconnected devices.

Keywords: Attack Detection, Sinkhole, Sensor Node, IoT, WSN

I INTRODUCTION

The proliferation of Wireless Sensor Networks (WSNs) and the Internet of Things (IoT) has revolutionized numerous sectors, including healthcare, smart cities, and industrial

automation. These technologies rely on a network of interconnected devices to collect and exchange data, providing critical insights and enabling automated control. However, the inherent openness and resource constraints of these networks make them vulnerable to various security threats, notably sinkhole attacks. In a sinkhole attack, a malicious node attracts a significant portion of the network traffic by falsely advertising an optimal path to the base station, thereby disrupting the network's normal functioning and enabling further malicious activities such as data interception or selective forwarding.The detection and prevention of sinkhole attacks have been the focus of extensive research, leading to the development of various techniques. An and Cho (2022) introduced a knowledge-based specification rule that leverages predefined rules and an understanding of network behavior to identify anomalies indicative of sinkhole attacks. Aryai and Binu (2017) proposed a cross-layer approach utilizing mobile agents to integrate information from multiple layers of the network protocol stack, enhancing detection accuracy.

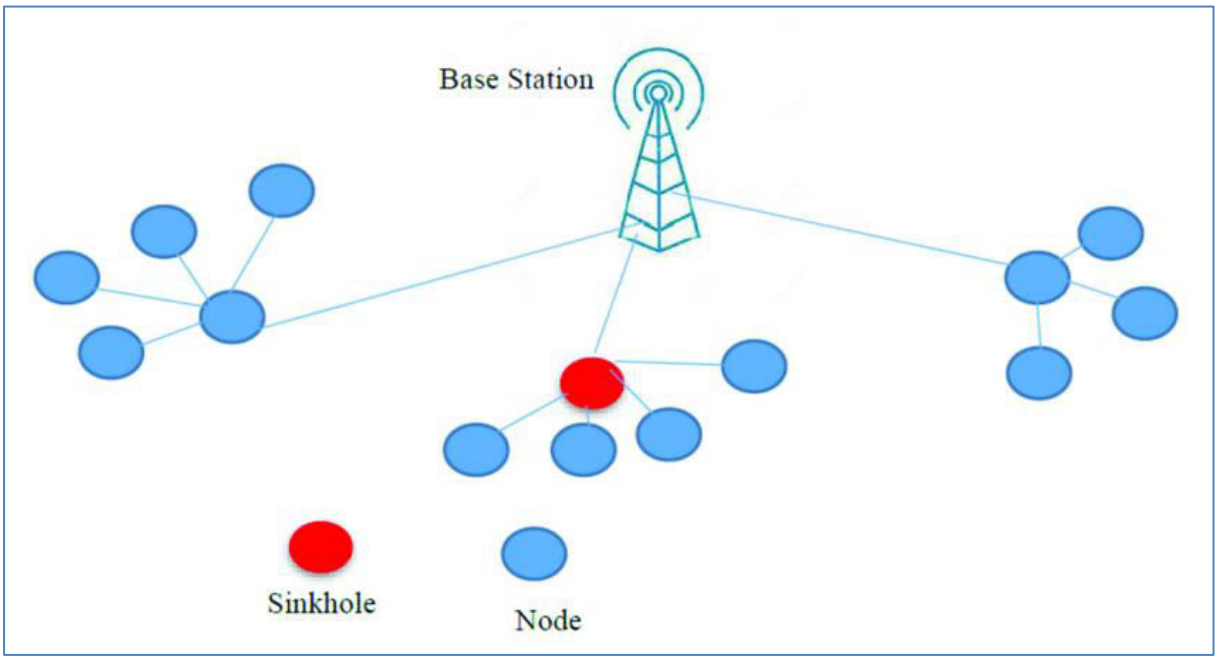

Figure 1: Sinkhole Attack Detection
https://www.researchgate.net/figure/Sinkhole-attack-35_fig3_343752891

A sinkhole attack occurs when an attacker node in a wireless sensor network disguises itself as the legitimate node closest to the base stationin order to have all data pass through, hence having the opportunity to modify, drop or delay data going to the base station.

Giri et al. (2023) employed machine learning models to analyze network traffic patterns, providing predictive capabilities for low-power and lossy IoT networks.Neighbor information has also been a key focus, as highlighted by Han et al. (2015), who developed an intrusion detection algorithm relying on consistency checks among neighboring nodes. Similarly, Lee and Cho (2016) used neighbor information in LEAP-based WSNs to enhance detection capabilities. Trust-based methods have been explored by Hu et al. (2022) and Prathapchandran and Janani (2021), who incorporated trust metrics and machine learning, respectively, to improve detection accuracy and adapt to network changes.Techniques such as redundancy mechanisms (Zhang et al., 2014) and distance-based detection (Mondal et al., 2022) have also been proposed to verify

the legitimacy of reported paths and identify anomalies. Mohammed et al. (2024) enhanced reputation-based intrusion detection systems, continuously evaluating node behavior to identify malicious nodes dynamically.

Additionally, secure routing protocols (Salve et al., 2015) and combined detection techniques (Stephen and Arockiam, 2017) offer comprehensive solutions to mitigate sinkhole attacks.This survey paper aims to provide a detailed comparative analysis of these diverse methodologies, assessing their strengths, limitations, and applicability in different network environments. By synthesizing insights from various studies, this paper seeks to guide future research and practical implementations, ultimately enhancing the security and resilience of WSNs and IoT networks against sinkhole attacks.

II LITERATURE REVIEW

An and Cho (2022) proposed a knowledge-based specification rule to enhance sinkhole attack detection in IoT environments. Their technique leverages predefined rules and an understanding of normal network behavior to identify anomalies that indicate potential sinkhole attacks. This approach is particularly effective in distinguishing between legitimate and malicious nodes based on their behavior patterns.

Aryai and Binu (2017) introduced a cross-layer approach using mobile agents to detect and prevent sinkhole attacks. Their method integrates information from multiple layers of the network protocol stack, enhancing the accuracy of detection by considering diverse data points such as packet routing paths, node behavior, and traffic patterns. This comprehensive approach helps in the early detection and prevention of sinkhole attacks.

Giri et al. (2023) focused on identifying and predicting sinkhole attacks in low-power and lossy IoT networks using machine learning models. These models analyze network traffic patterns and node behaviors to predict potential sinkhole attacks before they cause significant damage. By employing advanced predictive analytics, their approach aims to improve proactive defense mechanisms in IoT networks.

Han et al. (2015) developed an intrusion detection algorithm based on neighbor information to counter sinkhole attacks in WSNs. This method relies on the consistency of routing information among neighboring nodes to detect anomalies. If a node reports significantly different routing information compared to its neighbors, it is flagged as potentially compromised, thereby enabling the network to isolate and mitigate the attack.

Hu et al. (2022) presented a trust-based, secure and energy-efficient routing protocol for WSNs. In their approach, trust metrics are used to evaluate and identify malicious nodes. By incorporating trust evaluation into routing decisions, their protocol not only enhances security but also ensures energy efficiency, making it suitable for resource-constrained WSN environments.

Karthigadevi et al. (2019) proposed a neighbor density estimation technique to improve the quality of service and detect sinkhole attacks. This approach involves estimating the density of nodes in a given area to identify abnormal concentrations, which may indicate the presence of a sinkhole attack. By monitoring changes in node density, their technique provides a reliable means of detecting malicious activities.

Krontiris et al. (2008) examined algorithmic methods for detecting sinkhole attacks in WSNs. Their research focused on developing algorithms that identify abnormal routing behaviors, such as sudden changes in route paths or the appearance of new, unexplained nodes in the network. These algorithmic checks help in the early detection and mitigation of sinkhole attacks.

Lee and Cho (2016) utilized neighbors' information in LEAP-based WSNs to enhance detection capabilities. Their approach leverages the consistency of routing information among neighboring nodes to identify potential sinkhole attacks. By comparing routing data from multiple nodes, they can detect discrepancies that indicate malicious activity.

Mondal et al. (2022) developed a method for detecting sinkhole attacks in IoT-based WSNs using the distance from the base station. This technique involves calculating the expected distance of nodes from the base station and identifying inconsistencies in reported distances. Nodes that report abnormal distances are flagged for further investigation, helping to isolate and mitigate sinkhole attacks.

Mohammed et al. (2024) proposed an enhanced reputation-based intrusion detection system that improves detection accuracy by evaluating the reputation of nodes over time. This system continuously monitors node behavior and updates their reputation scores, allowing for the dynamic identification of malicious nodes. By maintaining an up-to-date reputation database, their approach enhances the network's resilience to sinkhole attacks.

Ngai et al. (2006) examined intruder detection methods for sinkhole attacks in WSNs. Their study focused on identifying abnormal routing behaviors, such as unexpected changes in traffic patterns or the appearance of suspicious routes. By analyzing these anomalies, their method provides an effective means of detecting and mitigating sinkhole attacks.

Prathapchandran and Janani (2021) introduced RFTRUST, a trust-aware security mechanism using random forest algorithms to detect sinkhole attacks in RPL-based IoT environments. Their approach combines trust evaluation with machine learning to enhance the accuracy and reliability of sinkhole attack detection. By leveraging random forest algorithms, they can analyze complex patterns in network behavior to identify malicious nodes.

Table 1: Comparative table for advantages and limitations

Author(s) and Year	**Approach**	**Key Techniques**	**Advantages**	**Disadvantages**
An and Cho (2022)	Knowledge-based specification rule	Predefined rules, network behavior analysis	High detection accuracy, specific to known behaviors	Limited to predefined rules, may miss novel attacks
Aryai and Binu (2017)	Cross-layer approach using mobile agents	Cross-layer integration, mobile agents	Comprehensive detection, early prevention	Complex implementation, higher resource consumption
Giri et al. (2023)	Machine learning for low-power IoT networks	Traffic pattern analysis, predictive analytics	Proactive defense adapts to evolving threats	Requires training data, computationally intensive

Han et al. (2015)	Neighbor information-based detection	Consistency checks among neighbors	Simple implementation, effective for local anomalies	Limited scalability, may not detect sophisticated attacks
Hu et al. (2022)	Trust-based secure and energy-efficient routing	Trust metrics, energy efficiency considerations	Enhances security and energy efficiency simultaneously	Attackers may manipulate trust evaluation
Karthigadevi et al. (2019)	Neighbor density estimation	Node density estimation	Effective for detecting abnormal node concentrations	Less effective in highly dynamic networks
Krontiris et al. (2008)	Algorithmic detection methods	Algorithmic checks, routing behavior analysis	Early detection of routing anomalies	Generate false positives, depending on algorithm quality
Lee and Cho (2016)	Neighbor information for LEAP-based WSNs	Consistency checks among neighbors	Enhances detection in LEAP-based networks	May not be applicable to all network types
Mondal et al. (2022)	Distance from base station	Distance consistency checks	Simple and effective for distance anomalies	Limited to distance-based anomalies
Mohammed et al. (2024)	Enhanced reputation-based intrusion detection	Reputation scores, continuous monitoring	Dynamic and adaptive, it improves over time	Requires ongoing monitoring, may have initial inaccuracy
Ngai et al. (2006)	Intruder detection for routing anomalies	Traffic pattern and routing behavior analysis	Effective for early anomaly detection	Depends on accurate traffic pattern analysis
Prathapchandran and Janani (2021)	Random forest-based trust mechanism	Machine learning (random forest), trust metrics	High accuracy, adapts to network changes	Computationally intensive, requires training data

Ramachandran et al. (2023) explored watermarking for sinkhole detection and prediction. This method involves embedding identifiable marks within the network traffic, enabling the detection of altered routes indicative of a sinkhole attack. By monitoring these watermarks, their technique provides a robust means of detecting and predicting sinkhole attacks.

Salve et al. (2015) focused on secure routing protocols that inherently mitigate sinkhole attacks. Their protocols ensure that routing decisions are made based on secure and verified information, reducing the likelihood of compromised nodes influencing the network. By incorporating security measures into the routing process, their approach enhances the network's resilience to sinkhole attacks.

Sasirekha and Radha (2017) combined secure routing with attack awareness for mobile ad hoc networks, addressing both wormhole and sinkhole attacks simultaneously. Their approach involves monitoring routing paths and traffic patterns for signs of malicious activity, enabling the network to detect and mitigate multiple types of attacks.

Stephen and Arockiam (2017) enhanced sinkhole detection in IoT by integrating multiple detection techniques. Their method combines anomaly detection, behaviour analysis, and machine learning to provide a comprehensive solution for identifying sinkhole attacks. By leveraging multiple techniques, their approach improves detection accuracy and reliability.

Tahir et al. (2019) developed an intrusion detection system for preventing active sinkhole routing attacks in IoT. This system monitors network traffic for signs of sinkhole attacks and takes preventive measures to isolate and mitigate compromised nodes. By continuously analyzing traffic patterns, their system provides real-time protection against sinkhole attacks.

Yadav and Tak (2018) used the Ad-hoc On-demand Distance Vector (AODV) protocol to detect sinkhole attacks by monitoring routing changes. Their method involves identifying discrepancies in routing information to detect compromised nodes. By ensuring that routing decisions are based on accurate and verified information, their approach enhances the security of WSNs.

Zhang et al. (2014) proposed a redundancy mechanism to detect sinkhole attacks, where redundant routing information is used to verify the legitimacy of reported paths. By cross-checking routing data from multiple sources, their technique helps identify and isolate malicious nodes, ensuring the integrity and reliability of the network.

Table 2: Comparative Analysis ofVarious Protocols

Author(s) and Year	**Approach**	**Key Techniques**	**Advantages**	**Disadvantages**
Ramachandran et al. (2023)	Watermarking for detection and prediction	Traffic watermarking, anomaly detection	Robust against traffic manipulation	Implementation complexity may affect network performance

Salve et al. (2015)	Secure routing protocols	Secure routing algorithms	Inherent security in routing decisions	Implementation complexity may increase routing overhead
Sasirekha and Radha (2017)	Combined secure routing and attack awareness	Multi-attack detection, secure routing	Comprehensive security solution	Increased complexity, resource-intensive
Stephen and Arockiam (2017)	Integrated detection techniques	Anomaly detection, behavior analysis, ML	High detection accuracy, versatile	Complex implementation, resource-intensive
Tahir et al. (2019)	Intrusion detection system	Real-time traffic monitoring	Real-time protection, proactive defense	It may generate false positives, requires constant monitoring
Yadav and Tak (2018)	AODV protocol for routing changes	Routing information consistency checks	Simple implementation, effective for AODV networks	Limited to AODV protocol, may not detect complex attacks
Zhang et al. (2014)	Redundancy mechanism	Redundant routing information verification	Ensures routing integrity, effective anomaly detection	May increase routing overhead, complexity in redundancy

III CONCLUSION

In Conclusion, this survey has reviewed 19 research papers studied with its strengths and limitations, and no single technique is universally applicable. The most effective strategy involves a combination of methods that address different aspects of sinkhole attacks, balancing detection accuracy, implementation complexity, and resource efficiency. Machine learning models offer advanced predictive capabilities, analyzing network traffic patterns to identify potential attacks before they occur. These techniques can significantly improve proactive defense but depend on the availability of quality training data and are computationally intensive. Trust-based and reputation-based systems enhance detection by evaluating node behavior over time, providing dynamic adaptability to changing network conditions. However, these systems can be

susceptible to manipulation by malicious nodes. Future research should focus on developing integrated solutions that leverage the strengths of multiple techniques while addressing their weaknesses. By doing so, we can enhance the security and resilience of WSNs and IoT networks, ensuring their robustness in the face of sophisticated and evolving threats.

IV REFERENCES

1. An, G. H., & Cho, T. H. (2022). Improving sinkhole attack detection rate through knowledge-based specification rule for a sinkhole attack intrusion detection technique of IoT. *International Journal of Computer Networks and Applications (IJCNA), 9*(2), 169-178. https://doi.org/10.22247/ijcna/2022/212333
2. Aryai, S., & Binu, G. S. (2017). Cross layer approach for detection and prevention of sinkhole attack using a mobile agent. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 359-365). IEEE. https://doi.org/10.1109/CESYS.2017.8321299
3. Giri, A., Goyal, A., Kogta, A., Jain, P., & Verma, P. (2023). Identifying and predicting sinkhole attacks for low-power and lossy IoT networks. In G. Rajakumar, K. L. Du, & Á. Rocha (Eds.), *Intelligent Communication Technologies and Virtual Mobile Networks. ICICV 2023. Lecture Notes on Data Engineering and Communications Technologies* (Vol. 171). Springer, Singapore. https://doi.org/10.1007/978-981-99-1767-9_24
4. Han, G., Li, X., Jiang, J., Shu, L., & Lloret, J. (2015). Intrusion detection algorithm based on neighbor information against sinkhole attack in wireless sensor networks. *The Computer Journal, 58*(6), 1280-1292. https://doi.org/10.1093/comjnl/bxu036
5. Hu, H., Han, Y., Yao, M., & Song, X. (2022). Trust-based secure and energy-efficient routing protocol for wireless sensor networks. *IEEE Access, 10*, 10585-10596. https://doi.org/10.1109/ACCESS.2021.3075959
6. Karthigadevi, K., Balamurali, S., & Venkatesulu, M. (2019). Based on neighbor density estimation technique to improve the quality of service and to detect and prevent the sinkhole attack in wireless sensor network. In *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)* (pp. 1-4). IEEE. https://doi.org/10.1109/INCOS45849.2019.8951406
7. Krontiris, I., Dimitriou, T., Giannetsos, T., &Mpasoukos, M. (2008). Intrusion detection of sinkhole attacks in wireless sensor networks. In M. Kutyłowski, J. Cichoń, & P. Kubiak (Eds.), *Algorithmic Aspects of Wireless Sensor Networks. ALGOSENSORS 2007. Lecture Notes in Computer Science* (Vol. 4837). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77871-4_14
8. Lee, J. J., & Cho, T. H. (2016). Sinkhole attack detection scheme using neighbors' information for LEAP-based wireless sensor networks. *International Journal of Computer Applications, 141*(13), 1-7. https://doi.org/10.5120/ijca2016908375
9. Mondal, K., Yadav, S. S., Pal, V., Singh, A. P., Yogita, Y., & Singh, M. (2022). Detecting sinkhole attacks in IoT-based wireless sensor networks using distance from base station. *International Journal of Information System Modeling and Design (IJISMD), 13*(6), 1-18. https://doi.org/10.4018/IJISMD.297628
10. Mohammed, F. A.-B. A., Mekky, N. E., Soliman, H., &Hikal, N. A. (2024). Sinkhole attack detection by enhanced reputation-based intrusion detection system. *IEEE Access, 12*, 86985-86996. https://doi.org/10.1109/ACCESS.2024.3416270

11. Ngai, E. C. H., Liu, J., & Lyu, M. R. (2006). On the intruder detection for sinkhole attack in wireless sensor networks. In *2006 IEEE International Conference on Communications* (pp. 3383-3389). IEEE. https://doi.org/10.1109/ICC.2006.255595
12. Prathapchandran, K., & Janani, T. (2021). A trust-aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST. *Computer Networks, 198*, 108413. https://doi.org/10.1016/j.comnet.2021.108413
13. Ramachandran, D., Venkatesh, J., Jothilakshmi, R., &Gugapriya, G. (2023). Sinkhole detection and prediction using watermarking (SNDW). *Journal of Intelligent & Fuzzy Systems, 45*(4), 7005-7023. https://doi.org/10.3233/JIFS-224463
14. Salve, V. B., Ragha, L., & Marathe, N. (2015). AODV based secure routing algorithm against sinkhole attack in wirelesses sensor networks. In *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICECCT.2015.7226170
15. Sasirekha, D., & Radha, N. (2017). Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 505-510). IEEE. https://doi.org/10.1109/CESYS.2017.8321128
16. Stephen, R., &Arockiam, L. (2017). An enhanced technique to detect sinkhole attack in Internet of Things. *International Journal of Engineering Research & Technology (IJERT) ICONNECT – 2017 (Volume 5 – Issue 13).*
17. Tahir, S., Bakhsh, S. T., &Alsemmeari, R. A. (2019). An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of things. *International Journal of Distributed Sensor Networks, 15*(11). https://doi.org/10.1177/1550147719889901
18. Yadav, H., & Tak, S. (2018). Detection of sinkhole attack in wireless sensor network using Ad-hoc on-demand distance vector. *International Journal of Engineering Research & Technology (IJERT), 07*(05).
19. Zhang, F. J., Zhai, L. D., Yang, J. C., & Cui, X. (2014). Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. *Procedia Computer Science, 31*, 711-720. https://doi.org/10.1016/j.procs.2014.05.319