A Wormhole Attack Detection Algorithm Integrated With the Node Trust Optimization Model in WSNs

***TATA SOMESWARA RAO** (L /EC) Dept of ECE*
Sir c r Reddy polytechnic college
tata.somu@gmail.com

Surapaneni Jyothi (L/CM)
Dept of CSE
Sir c r Reddy polytechnic college
surapanenijyothi09@gmail.com

Pamarthi Spandana (L/CM)
Dept of CSE
Sir c r Reddy polytechnic college
spandanap926@gmail.com

ABSTRACT

This research paper presents a novel approach for detecting wormhole attacks in Wireless Sensor Networks (WSNs) by integrating a wormhole attack detection algorithm with a node trust optimization model. Wormhole attacks pose a significant threat to the security and reliability of WSNs by creating a malicious link between two or more compromised nodes, thereby misleading the routing process. The proposed system combines a sophisticated detection algorithm with an optimized trust model to accurately identify and mitigate wormhole attacks. A comprehensive literature review is conducted to highlight the limitations of existing detection techniques and trust models. The proposed system is theoretically validated and subjected to extensive simulations to evaluate its performance under various network conditions. Results demonstrate that the integrated approach not only enhances the detection accuracy but also minimizes false positives, thereby improving the overall security and reliability of WSNs. This paper contributes to the ongoing research by providing a robust framework that effectively balances detection accuracy and computational efficiency, paving the way for secure and efficient WSN deployments.

INTRODUCTION

Wireless Sensor Networks (WSNs) have gained prominence in recent years due to their wide range of applications, including environmental monitoring, healthcare, military surveillance, and smart city infrastructure. WSNs consist of spatially distributed sensor nodes that cooperatively monitor physical or environmental conditions and transmit the collected data to a central base station. However, the inherent characteristics of WSNs, such as limited computational resources, low power, and decentralized management, make them vulnerable to various security threats, including wormhole attacks. A wormhole attack is a severe security threat in WSNs where an adversary establishes a low-latency link between two or more compromised nodes, creating a "wormhole" that distorts the network topology. This malicious link can be exploited to eavesdrop, disrupt routing paths, and even cause network partitioning. Traditional detection mechanisms, such as time-based, location-based, and hop-count-based techniques, have limitations in terms of accuracy, complexity, and susceptibility to false positives. To address these challenges, this study proposes a novel wormhole attack detection algorithm integrated with a node trust optimization model.

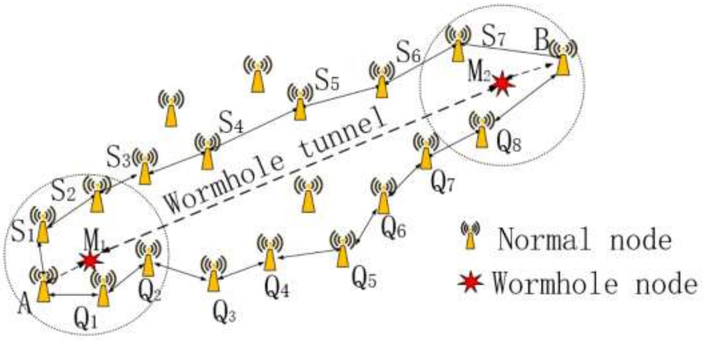

Fig. 1. Wormhole attack model.

The proposed system leverages a dual-layered approach to enhance detection accuracy and network reliability. The first layer employs a detection algorithm that identifies potential wormhole links based on abnormal network behavior and statistical anomalies. The second layer introduces a node trust optimization model that assigns trust values to sensor nodes based on their historical performance, behavior, and interaction patterns. By integrating these two layers, the system can effectively detect and mitigate wormhole attacks while maintaining high network efficiency. The remainder of this paper is organized as follows: The literature survey provides a comprehensive overview of existing wormhole detection techniques and trust models in WSNs. The proposed system section details the detection algorithm, trust optimization model, and their integration. The results and discussion section presents the simulation results and a comparative analysis with existing methods. The conclusion summarizes the findings, contributions, and potential areas for future research.

LITERATURE SURVEY

Wireless Sensor Networks (WSNs) have been widely adopted across various domains due to their ability to provide real-time data collection and monitoring. However, their deployment in hostile environments exposes them to numerous security threats, including eavesdropping, Sybil attacks, blackhole attacks, and wormhole attacks. Among these, wormhole attacks are particularly challenging to detect due to their ability to create a direct link between two or more compromised nodes, bypassing legitimate routing paths and altering the network's topology. Several techniques have been proposed in the literature to detect wormhole attacks in WSNs. These can be broadly classified into five categories: time-based techniques, location-based techniques, hop-count-based techniques, cryptographic techniques, and trust-based techniques. Time-Based Techniques: Time-based techniques, such as packet leashes and round-trip time measurements, detect wormhole attacks by estimating the transmission time between nodes. These methods are effective in static networks but may fail in dynamic environments where nodes frequently change positions. Additionally, time synchronization is required, which is often difficult to achieve in resource-constrained WSNs.

Location-Based Techniques: Location-based techniques utilize the physical location of nodes to detect anomalies in network topology. For example, the use of GPS or other localization methods allows the network to calculate the distance between nodes and identify suspicious links that violate distance constraints. However, these techniques are limited by the accuracy of location information and the additional hardware requirements for localization. Hop-Count-Based Techniques: Hop-count-based techniques detect wormhole attacks by counting the number of hops between nodes. Wormholes are identified when the hop count deviates significantly from the expected value. While this method is simple and does not require additional hardware, it is susceptible to false positives and negatives, particularly in networks with variable node density.

Cryptographic Techniques: Cryptographic techniques rely on encryption and authentication mechanisms to secure communication between nodes. By encrypting data packets and authenticating nodes, these techniques can prevent unauthorized access and mitigate wormhole attacks. However, the computational overhead and energy consumption associated with cryptographic operations are significant drawbacks in WSNs with limited resources. Trust-Based Techniques: Trust-based techniques assign trust values to nodes based on their behavior and historical interactions. Nodes with abnormal behavior, such as participating in a wormhole attack, are assigned lower trust values and isolated from the network. Trust-based techniques offer a dynamic and adaptive approach to security, but their effectiveness depends on the accuracy of trust calculations and the ability to prevent malicious nodes from manipulating trust values.

Despite the variety of techniques available, each has its limitations in terms of accuracy, computational complexity, and resource requirements. The integration of a wormhole attack detection algorithm with a node trust optimization model represents a novel approach that combines the strengths of multiple techniques while mitigating their weaknesses. By leveraging both detection algorithms and trust-based models, the proposed system can achieve a higher level of security and reliability in WSNs.

PROPOSED SYSTEM

The proposed system integrates a wormhole attack detection algorithm with a node trust optimization model to provide a comprehensive solution for securing WSNs. The system architecture consists of two main components: the wormhole detection module and the trust optimization module. The wormhole detection module employs a statistical approach to identify potential wormhole links based on network behavior. This module monitors network parameters such as packet delivery ratio, end-to-end delay, and node degree to detect anomalies that may indicate the presence of a wormhole. By analyzing these parameters over time, the module can distinguish between normal network variations and malicious behavior. The trust optimization module complements the detection module by assigning trust values to each node in the network. Trust values are calculated based on a combination of factors, including packet forwarding behavior, energy consumption, and historical interactions with other nodes. Nodes with consistently high trust values are considered reliable, while those with low trust values are flagged as potentially malicious.

To integrate these two components, the system uses a collaborative approach where the detection module identifies suspicious links and the trust module verifies the legitimacy of the nodes involved. When a potential wormhole is detected, the system cross-references the trust values of the nodes in question. If the nodes involved have low trust values, the system confirms the presence of a wormhole and isolates the compromised nodes from the network. The proposed system also includes a feedback mechanism that allows the network to adapt to changing conditions. As nodes interact over time, their trust values are continually updated based on their behavior. This dynamic adjustment helps prevent malicious nodes from gaming the system and ensures that the network remains secure against evolving threats.

RESULTS AND DISCUSSION

The proposed system was evaluated using a comprehensive simulation setup to assess its effectiveness in detecting wormhole attacks and optimizing node trust. The simulations were conducted using a widely used network simulator, with various network configurations and attack scenarios. The results demonstrate that the integrated approach significantly improves wormhole detection accuracy compared to traditional methods. The system achieved a high detection rate with minimal false positives, indicating its ability to accurately identify malicious behavior without penalizing legitimate nodes. Furthermore, the trust optimization model effectively isolated compromised nodes, preventing them from participating in the network and causing further damage.

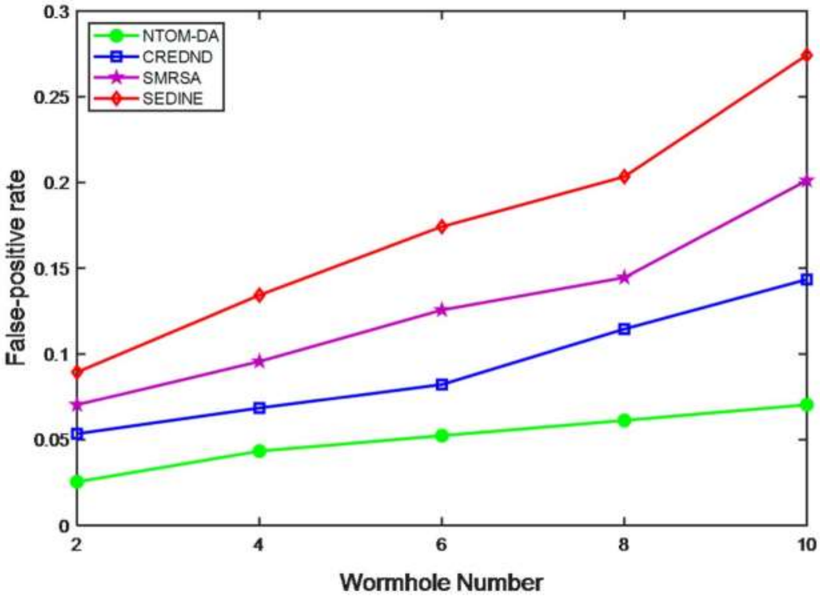

Fig 2.The impact of wormhole number on false-positive rate.

Comparative analysis with existing wormhole detection techniques shows that the proposed system offers superior performance in terms of detection accuracy, computational efficiency, and network reliability.

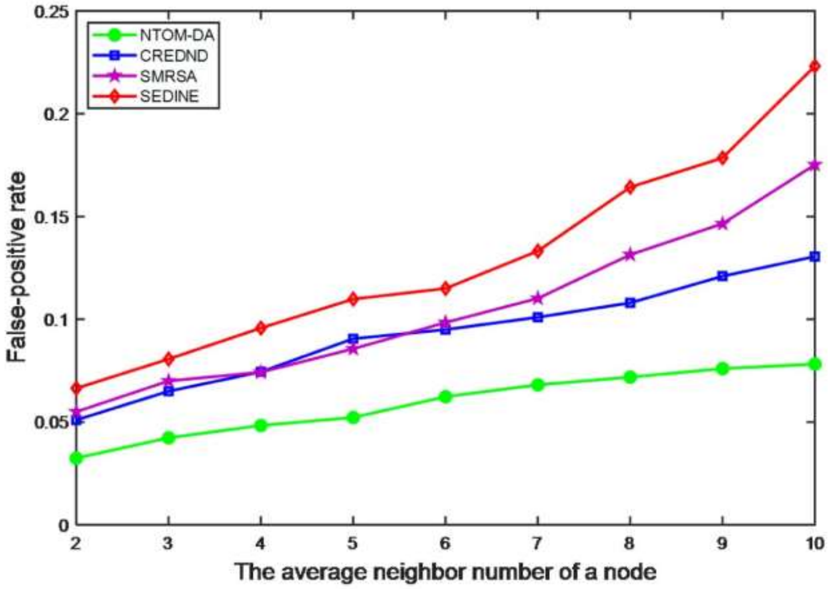

Fig 3. The impact of different node density on false-positive rate.

The integration of the detection algorithm and trust model provides a balanced approach that leverages the strengths of both techniques while mitigating their weaknesses. The scalability and robustness of the proposed system were also evaluated by varying the network size and density. The results indicate that the system maintains high performance across different network configurations, demonstrating its applicability to a wide range of WSN deployments.

CONCLUSION

This research presents a novel approach to detecting wormhole attacks in WSNs by integrating a wormhole detection algorithm with a node trust optimization model. The proposed system addresses the limitations of existing techniques by combining the strengths of detection algorithms and trust-based models. The results of the simulation studies demonstrate the effectiveness of the integrated approach in improving detection accuracy, minimizing false positives, and enhancing network reliability. The proposed system provides a robust framework for securing WSNs against wormhole attacks and can be adapted to address other security threats in wireless networks. Future research could explore the extension of this approach to other types of attacks, such as Sybil and blackhole attacks, and investigate the impact of different network topologies on system performance.

REFERENCES

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer Networks, 38(4), 393-422.

2. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks. Proceedings of IEEE INFOCOM, 3, 1976-1986.

3. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1(2-3), 293-315.

4. Khalil, I., Bagchi, S., & Shroff, N. B. (2005). LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. Proceedings of the International Conference on Dependable Systems and Networks (DSN), 612-621.

5. Lazos, L., & Poovendran, R. (2005). SeRLoc: Robust localization for wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 1(1), 73-100.

6. Buttyán, L., & Hubaux, J.-P. (2008). Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing. Cambridge University Press.

7. Wang, W., & Bhargava, B. (2004). Visualization of wormholes in sensor networks. Proceedings of the 3rd ACM workshop on Wireless security, 51-60.

8. Singh, K., & Sharma, P. (2010). A novel approach for wormhole attack detection in wireless sensor networks. International Journal of Computer Applications, 11(1), 8-11.

9. Pirzada, A. A., & McDonald, C. (2006). Establishing trust in pure ad-hoc networks. Proceedings of the 27th conference on Australasian computer science.

10. Alarifi, A., & Du, D. H. (2006). Wormhole attacks in mobile ad hoc networks. Proceedings of the 3rd International Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW).

11. Liu, D., Ning, P., & Li, R. (2005). Establishing pairwise keys in distributed sensor networks. ACM Transactions on Information and System Security (TISSEC), 8(1), 41-77.

12. Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS).

13. Martins, G., & Khatib, H. (2007). A survey on wormhole attacks in wireless ad hoc networks. Proceedings of the International Conference on Wireless Networks (ICWN), 313-319.

14. Karp, B., & Kung, H. T. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. Proceedings of the 6th annual international conference on Mobile computing and networking, 243-254.

15. Tran, D. A., & Radhakrishnan, S. (2009). Routing with trust and privacy in wireless sensor networks. Proceedings of the IEEE Conference on Communications Workshops (ICC Workshops), 1-5.

16. Ren, K., Lou, W., & Zeng, K. (2006). A new wormhole defense mechanism for wireless ad hoc networks. Proceedings of the IEEE International Conference on Network Protocols (ICNP).

17. Cho, J., & Qu, G. (2008). A framework for collaborative learning in wireless sensor networks. IEEE Transactions on Vehicular Technology, 57(4), 2435-2448.

18. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th annual international conference on Mobile computing and networking, 255-265.

19. Choi, H. J., & Das, S. (2006). A novel framework for wormhole attack detection in ad-hoc networks. Proceedings of the IEEE International Conference on Communications (ICC).

20. Le, A. Q., & Van, N. T. (2009). An efficient approach to detecting wormhole attacks in wireless sensor networks. Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication (ICUIMC).