Transactions on Engineering and Computing Sciences - Vol. 12, No. 4
Publication Date: August 25, 2024
DOI:10.14738/tecs.124.17242.
Seidu, R., Salifu, A.-M. S., & Ansuura, J. A. K. (2024). A Genetic Algorithm with a Trust Model Function for Detecting Sinkhole and Wormhole Nodes in Wireless Sensor Networks. Transactions on Engineering and Computing Sciences, 12(4). 30-44.
SERVICES FOR SCIENCE AND EDUCATION

A Genetic Algorithm with a Trust Model Function for Detecting Sinkhole and Wormhole Nodes in Wireless Sensor Networks

Rafiw Seidu
C. K. Tedam University of Technology and Applied Sciences,
School of Computing and Information Sciences, Department of
Information Systems and Technology, Upper East Region, Navrongo, Ghana

Abdul-Mumin Selanwiah Salifu
C. K. Tedam University of Technology and Applied Sciences,
School of Computing and Information Sciences, Department of
Information Systems and Technology, Upper East Region, Navrongo, Ghana

Johnbosco A. K. Ansuura
C. K. Tedam University of Technology and Applied Sciences,
School of Computing and Information Sciences, Department of
Information Systems and Technology, Upper East Region, Navrongo, Ghana

ABSTRACT

This study delved into wireless sensor networks, comprising numerous nodes with limited energy, computation, and transmission capabilities. Wireless sensor networks face security challenges due to their vulnerability to capture and compromise in insecure environments. Malicious nodes exploit communication's wireless nature, engaging in sinkhole and wormhole attacks. To address this, we propose a genetic strategy utilising a trust-based formula as a fitness function to evaluate sensor node reliability. Nodes progressing beyond a trust threshold criterion are identified, isolating malicious nodes responsible for attacks. Implemented in MATLAB 2018a, our approach effectively identifies and isolates such nodes, as demonstrated by the results.

Keywords: Genetic algorithm, Trust model, Sinkhole node, Wormhole node.

INTRODUCTION

Wireless sensor technology serves diverse purposes, from military surveillance and environmental monitoring (e.g., fire detection) to healthcare applications like heart condition monitoring [1]. Often deployed in open and challenging environments, many wireless sensor networks (WSNs) operate in unmonitored conditions [2]. Most WSN routing protocols neglect security, given sensors' limited resources like low processing power, restricted memory, and constrained communication range. This vulnerability exposes them to internal and external routing attacks [3], [4].

External attacks come from outside nodes disrupting the network, while internal attacks involve insiders with valid identities causing disruption [5]. In cybersecurity, internal attacks,

like sinkhole and wormhole attacks in WSNs, are challenging to manage and defend against, posing serious threats and potential network disruption [6], [7]. A sinkhole attack manipulates the routing algorithm to divert traffic through a compromised node, tricking victim nodes into thinking it's the shortest path to the base station [8]. The malicious node, now between the base station and sensor node, can tamper with or drop packets. In a wormhole attack, multiple hostile nodes collaborate to disrupt routing without needing a cryptographic breach. A high-speed tunnel connects malicious nodes, allowing intercepted traffic in one location to be replayed by another node elsewhere [9], [10].

Adversaries can seize control of a wireless sensor network by launching combined sinkhole and wormhole attacks. Existing research addresses these threats individually, utilizing cryptographic, rule-based, probability-based, neighbour discovery, hop count, weight-based, and path selection methods. However, integrated solutions are essential to safeguarding the reliability and longevity of wireless sensor networks. Traditional methods fall short in identifying sinkhole and wormhole attack nodes in combined attacks. Exploring alternative techniques is crucial for effective detection and isolation of WSNs.

This study presents a genetic and trust-based approach to detecting combined sinkhole and wormhole attack nodes in WSNs, offering a robust solution to the challenge.

RELATED WORKS

This section thoroughly reviews the literature on methods in wireless sensor networks, including rule-based, trust-based, probability-based and cryptographic techniques. It also covers the types of attacks these methods aim to identify and prevent.

Cryptographic Based Works

[11] propose HKP HD, a hybrid key predistribution scheme for wireless sensor networks, bolstering resistance to node capture attacks. The scheme combines q-composite and threshold-resistant polynomial schemes to reduce key compromise probability and communication overhead. Strengths include considering adversary behaviour and using unbalanced key predistribution for reduced storage overhead. Vulnerabilities arise from assumptions about an intelligent adversary, posing scalability and energy consumption challenges. Research gaps include the need for real-world evaluation, optimal value determination, and solutions for isolating vulnerable nodes and reducing energy consumption. [12] introduce a lightweight and energy-efficient methodology for secure sinkhole detection in wireless sensor networks, using homomorphic encryption and watermarking techniques. The approach excels in terms of delay, packet delivery ratio, throughput, and energy consumption. However, it solely addresses sinkhole attacks, leaving a gap in real-world experimentation validation and scalability assessment for large-scale networks. Additional measures are therefore required for overall network security against various attacks.

Rule-Based Works

[13] introduced the Warning Message Counter (WMC) to detect packet-dropping attacks in wireless sensor networks using network-layer acknowledgements. While effective against various attacks, WMC exclusively focuses on packet-dropping incidents, lacks evaluation in

large-scale networks, and offers no specifics on extending the algorithm for cooperative attack detection.

Probability-Based Works

[14] suggest a technique that uses an artificial neural network to detect wormhole attacks in wireless sensor networks based on connectivity information between any two sensor nodes. The proposed technique is implemented under different probability distributions and does not require additional hardware resources. Its strength is achieving high detection accuracy for WSN configurations of 100-500 nodes. However, its weakness is relying solely on connectivity information and not evaluating performance for larger WSNs or sophisticated attacks. [15] introduced a distributed adaptive algorithm using subjective logic and a probabilistic extension of timed automata to detect sinkhole attacks in WSNs. The algorithm adjusts probabilities in the AODVv2-12 routing protocol, prioritizing reliable nodes. It effectively prevents sinkhole attacks, is resilient to malicious nodes, and adapts to environmental changes. However, it incurs additional overhead and exclusively addresses sinkhole attacks, overlooking other potential threats to Wireless sensor networks. [16] suggests a novel approach for detecting wormhole attacks in wireless sensor networks. The approach uses only the network's connectivity information and does not require any special hardware or prior knowledge of the network. The proposed algorithm is simple, efficient, and effective and is designed to run in a distributed manner with low communication costs. The main strength of the paper is the simplicity and efficiency of the proposed approach. However, the paper lacks a comparison with other existing approaches for detecting wormhole attacks, which limits its evaluation and applicability in different scenarios. The research gap in the paper is the need for future research to compare the proposed approach with other methods and identify potential limitations or weaknesses to improve its applicability in real-world applications.

Trust-Base Works

[17] present TBSEER, a Trust-Based Energy Efficient Secure Routing protocol for Wireless Sensor Networks, effective against Wormhole attacks. Simulations using TRMSim-WSN show TBSEER outperforming other models in energy consumption, path length, and accuracy. Despite its dynamic adaptability and minimal sensor resource burden, the protocol's evaluation is limited to a specific simulation environment, necessitating broader assessments in diverse network conditions. Furthermore, its impact on WSNs' latency and throughput remains unexplored, requiring further investigation. [18] present a novel sinkhole attack detection method for hierarchical wireless sensor networks. The scheme, dividing the network into clusters with high-end sensor nodes, achieves a 95% detection rate and a 1.25% false positive rate, surpassing previous approaches. The algorithm minimizes message exchanges, reducing communication costs, and is well-suited for resource-constrained sensor nodes in critical applications such as military deployments. [19] present a trust-based method for detecting and isolating malicious nodes in a sensor network to prevent sinkhole and wormhole attacks. The approach deviates from traditional cryptography-based solutions and uses trust levels to influence routing decisions. The methodology is practical and suitable for rapidly deployed networks without imposing any prerequisites on the network establishment and operation phase. However, the methodology assumes that nodes will always act altruistically, and the trust levels may be manipulated by malicious nodes, compromising its effectiveness. The paper

does not consider the impact of the scheme on network performance and scalability for larger and more complex sensor networks. Further research is needed to evaluate the applicability of the scheme in real-world scenarios.

The literature reviewed reveals that [19] were the exclusive researchers delving into the subject of our present study, employing a trust-based methodology. Consequently, their methodology stands as the most sophisticated approach for identifying and countering sink and wormhole nodes in the context of a simultaneous sinkhole and wormhole attack on a Wireless Sensor Network (WSN). Our research offers a novel viewpoint on the recognition and mitigation of sinkhole and wormhole nodes in the face of a combined sinkhole and wormhole attack on a wireless sensor network, utilizing Genetic Algorithms (GA) in conjunction with a trust-based model.

METHODOLOGY

The proposed methodology, which combines a genetic algorithm (GA) with a trust model, enables the system to flexibly adjust to new threats, thereby bolstering the network's capability to detect attacks. The trust model aids in evaluating the behaviour of network nodes, while the genetic algorithm optimises the choice of reliable nodes across multiple generations by ensuring that nodes that meet the trust threshold criterion of total trust value Tij (t) ≥ 0.5 are always selected in every generation. This optimization is accomplished by employing genetic operators, including selection, crossover, and mutation. Figure 1 and Figure 2 depict the data routing pathways within the wireless sensor network and the distinct stages of the genetic algorithm process involved in the selection of dependable sensor nodes within those routing paths, respectively.

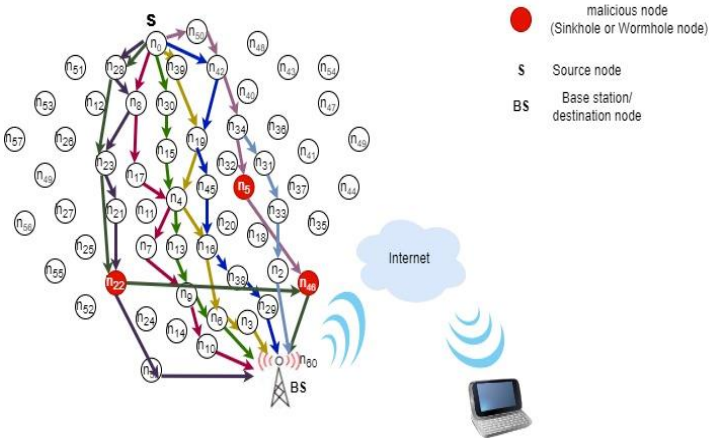


Figure 1: Selected nodes (chromosomes) in routing paths in a WSN

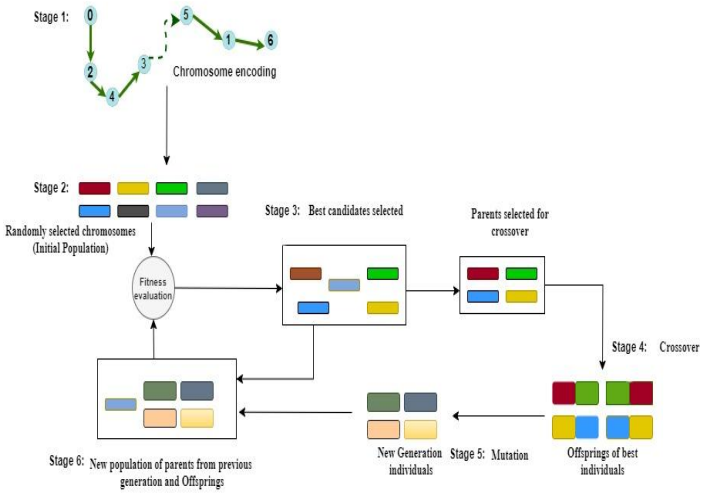


Figure 2: Stages of the GA process

Stage 1: Chromosome Encoding

The data routing chain is represented by a chromosome in the genetic algorithm, where genes denote specific configurations of Sensor Nodes (SNs). Each gene's index indicates the node's position, while the value provides its ID. The chromosome, an integer string of unique values from 1 to N, embodies an ordered sequence of nodes. After encoding, the genetic algorithm identifies an initial population of potential solutions by establishing feasible routes that avoid malicious nodes, a phase referred to as population initialization.

Stage 2: Initial Population

An initial population was formed through a basic random number generation algorithm, creating q chromosomes for optimization. The higher q enhances the likelihood of improved solutions. Chromosomes are generated with constraints on distances between consecutive nodes (gene values do not exceed the wireless range of communication).

Stage3: Selection Scheme

This study utilised the 'Roulette wheel selection' method for optimal selection in the proposed Genetic Algorithm (GA). This method ensures the inclusion of all chromosomes in the population, maintaining demographic diversity. Two parent chromosomes are selected based on fitness values and subjected to crossover and mutation in the next stage.

Stage 4: Crossover

Crossover is a key step in genetic algorithms, merging two-parent routes to create a new path through genetic recombination. In our implementation, we use a simple single-point crossover with a user-defined probability (P_{cr}) of 0.8. The crossover point is chosen based on the trust value of nodes exceeding a threshold of 0.5. Higher P_{cr} in early stages aids exploration, while lowering it later prevents trait loss, accelerating convergence. The process modifies existing solutions, revealing improved alternatives [20]. To assess effectiveness, we employ Equation 3.6 [21] for average crossover performance during a generation run.

Stage 5: Mutation

In the mutation process, newly formed strings undergo random alterations, fostering population diversity. Higher mutation probabilities lead to more new individuals, dispersing across the search area and reducing the proportion of fit individuals. This increased mutation likelihood delays algorithm convergence, impacting dominant individuals in later stages [22]. Mutation probability values (P_{mt}) typically range from 0.001 to 0.05 [21]. This study starts with a high P_{mt} of 0.05 (Table 2) and gradually reduces it for convergence. Figure 3.8 illustrates the mutation type. Average mutation progress for a generation with nm mutation operations is calculated using Equation 3.8, akin to the crossover process.

Stage 6: Fitness Function

The fitness function, utilizing the trust Equation 3.3, assesses how well a solution aligns with the ideal one in the Genetic Algorithm (GA) process [20], [23]. Chromosomes meeting the fitness test are selected as optimal routes, free from malicious nodes. These chosen chromosomes and their nodes advance to the next GA stage, with the fitness function explicitly defined as:

$$f(t) = \lambda DT_{ix}(j) + \mu IT_i^k(j) \quad (1)$$

$$\mathrm{DT_{ix}(j)} = \frac{P_f}{P_f + P_d} \quad (2)$$

$$IT_i^k(j) = \frac{\sum_{x=1,2,\ldots,k} T_i(j)}{k} \quad (3)$$

Equation 1 defines $DT_{ix}(j)$ as the direct trust degree of node i in node j, used to detect sinkholes and authenticate packets. Equation 2 introduces P_r, P_f and P_d as counts of received, forwarded and dropped packets by node j. In Equation 3, $IT_i^k(j)$ represents node $i's$ average indirect trust gained through recommendations from neighbours denoted by k for node j.

The weight factors λ and μ in Equation 3, where $\lambda + \mu = 1$ and $0 \leq \lambda \leq 1$, $0 \leq \mu \leq 1$, determine the influence of direct and indirect trust [24]. We assigned 0.7 to λ and 0.3 to μ, prioritizing the accuracy of direct interactions. This decision acknowledges the significance of indirect trust, especially for new nodes with limited experience in assessing neighbours' cooperation tendencies [25].

Node Evaluation Algorithm:

1. Begin
2. Check if *i* has any past interaction with *j*
3. If yes and $DT_{ix}(j) \geq \tau$
4. i and j may interact
5. Otherwise
6. $DT_{ix}(j) < \tau$ and no history of past interactions
7. i check for trust recommendations from one-hop neighbours using $IT_i^k(j)$
8. If $Ti\ j(t) > \tau$ then

9. *i* and *j* may interact
10. Otherwise
11. $IT_i^k(j) < \tau$ no recommendations from one-hop neighbours
12. i check for any risk to be taken *R*.
13. if there is a risk, then
14. Assess if $R \geq 0$ then interact.
15. Otherwise
16. Decline interaction node associated with a distrust value
17. end.

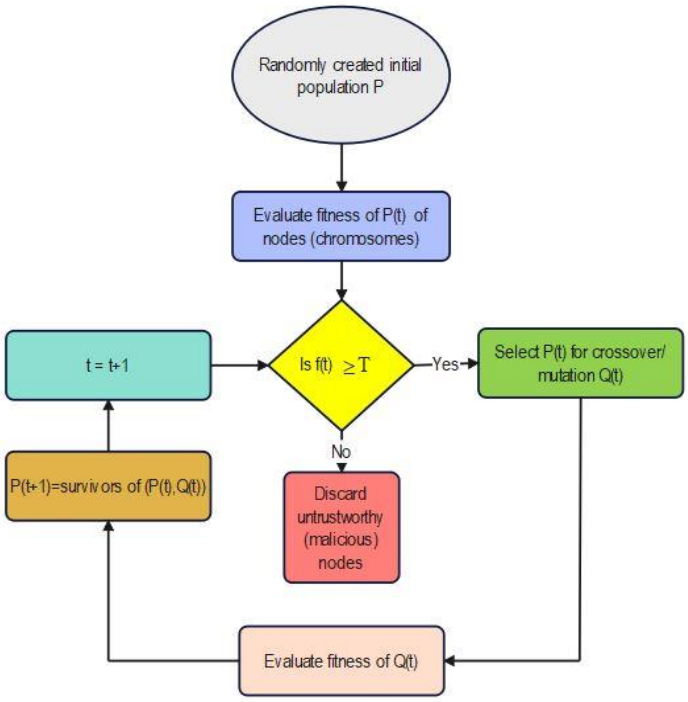


Figure 3: Flowchart of the genetic algorithm process

Simulation Parameters

The parameters for the genetic algorithm (GA) employed to simulate the environment and the parameters controlling network construction in this study are outlined in Table 1 and Table 2, respectively. These parameter configurations are mainly derived from the research conducted by [26], with slight modifications made to certain values.

Table 1 - parameter values for GA

Parameter	Value
Chromosome length	100
Selection type	Roulette wheel
Crossover probability	0.8
Crossover type	Single point
Mutation rate	0.05
Number of iterations	50

Table 2 - Network simulation parameters

Parameter	Value
Network size	500 x 500
Number of nodes	100
Number of sinkhole nodes	3
Number of wormhole nodes	2
Initial energy of node	100 J
Simulation time	300 s
Channel type	Wireless
Transmission range	200 m
Packet type	200 bites

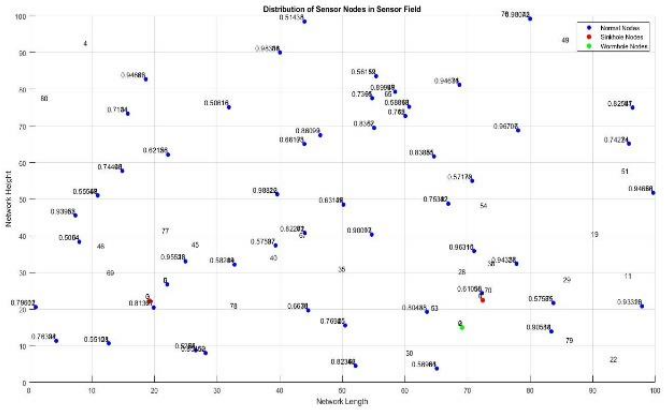


Figure 4: Simulated wireless sensor field

RESULTS

This section outlines our simulation studies using a genetic algorithm (GA) to enhance the resilience of wireless sensor networks (WSNs) against security vulnerabilities, particularly sinkhole and wormhole nodes. The GA, known for optimal solutions in complex environments, evolved 100 nodes over 50 generations. Fitness ratings were assigned based on a trust equation considering direct trust (DT) and indirect trust (IT). Results, presented in tables and visuals, show improvements in algorithm efficacy over time. The simulation focused on detecting sinkhole and wormhole nodes, with direct trust emphasizing packet transmission behaviour (0.7 weight) over indirect trust (0.3 weight).

Peak Fitness Value Across Generations

The Genetic Algorithm (GA) began with random nodes, evolving through generations by selecting high-fitness nodes for reproduction, crossover, and introducing mutations. Figure 5 shows a consistent rise in peak fitness, indicating the GA's effectiveness. It improved in detecting malicious nodes, with fluctuations suggesting ongoing learning. While proficient in identifying sinkhole and wormhole nodes, a plateau suggests potential for enhancement through parameter adjustments or diverse initial populations.

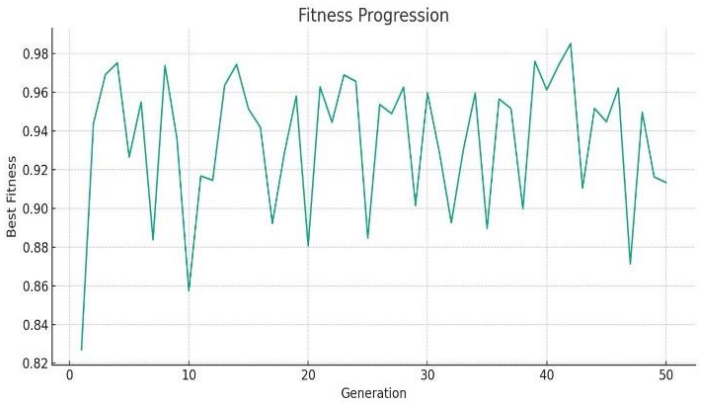


Figure 5: Fitness Progression

Detection of Sinkhole and Wormhole Nodes

Figure 6 shows varying counts of sinkhole and wormhole nodes across generations, reflecting the genetic algorithm's dynamic exploration in WSN security. Detection rates for both types increased over generations, indicating GA's success in evolving better solutions. Towards later generations, detection rates plateaued, suggesting convergence to optimal or near-optimal solutions given the parameters.

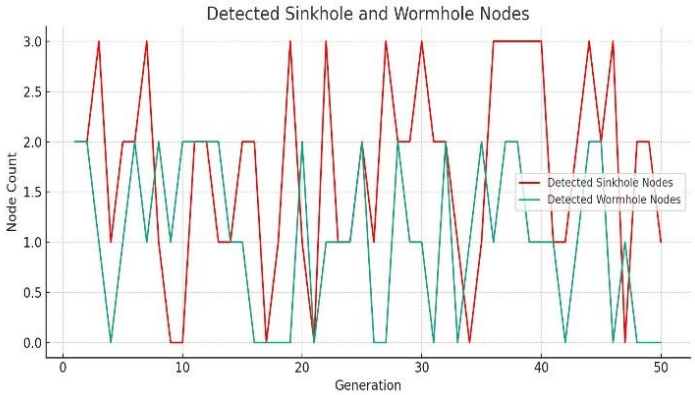


Figure 6: detected sinkhole and wormhole nodes

Performance of the GA and Data Distribution

The evaluation of the genetic algorithm's performance involved the utilization of histograms to illustrate the distribution of optimal fitness values across generations. These visual aids segment data into bins, where each bar corresponds to the number of data points within a bin.

In Figure 7, the algorithm's proficiency in consistently identifying solutions with high fitness is emphasized, showcasing the pattern of frequency and range in fitness scores.

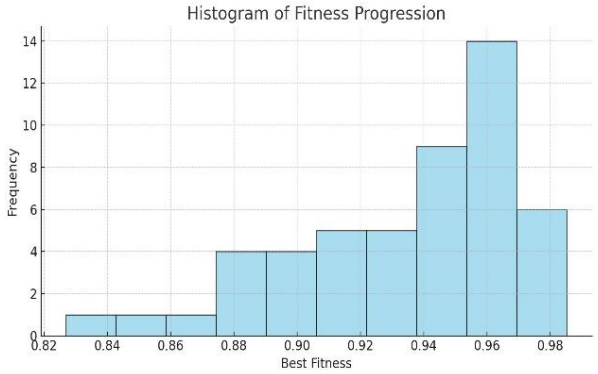


Figure 7: Histogram showing fitness progression

Distribution of Node Type Identified

Figure 8 and Figure 9 graphically depict the prevalence of node types, showcasing the algorithm's consistent identification of security threats.

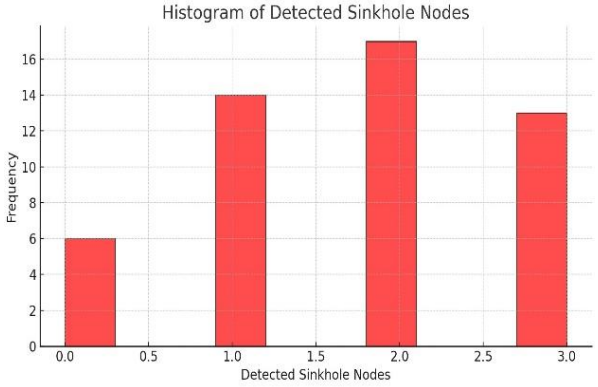


Figure 8: Detected sinkhole nodes histogram

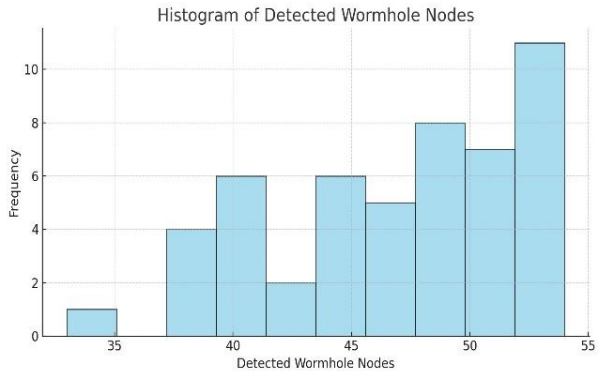


Figure 9: Detected wormhole nodes histogram

Error Analysis

The reliability and consistency of the simulation outcomes were evaluated by conducting an error analysis (refer to Figure 10) across multiple simulation iterations. The plots presented

showcase the mean values for each generation, with error bars representing the corresponding standard deviations. Specifically, in the graph labelled "Average Best Fitness over Multiple Runs," we depict the mean of the top fitness values for each generation across all runs. The accompanying error bars convey the standard deviation, offering insight into the variation in top fitness values across different simulation runs.

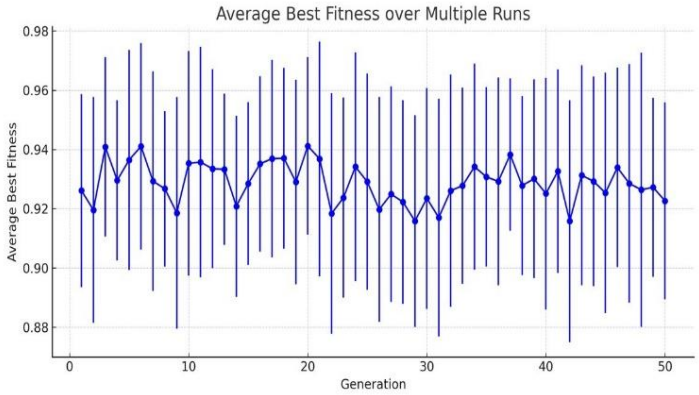


Figure 10: Average Best Fitness over Multiple Runs

The next plot (Figure 11), "Average Detected Sinkhole Nodes Over Multiple Runs," reveals the mean number of identified sinkhole nodes per generation. The error bars in this plot represent the standard deviation, showcasing the variability in the count of identified sinkhole nodes across disparate runs.

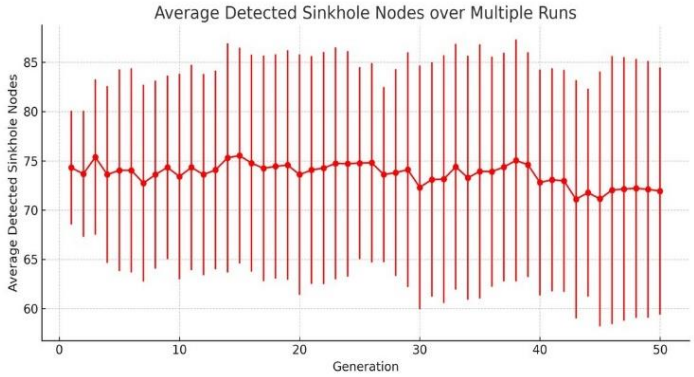


Figure 11: Average Detected Sinkhole nodes over Multiple runs

Similarly, the final plot (Figure 12), "Average Detected Wormhole Nodes Over Multiple Runs," shows the average count of identified wormhole nodes for each generation, with the standard deviation depicted as error bars. This offers an understanding of the range in the count of detected wormhole nodes across distinct runs.

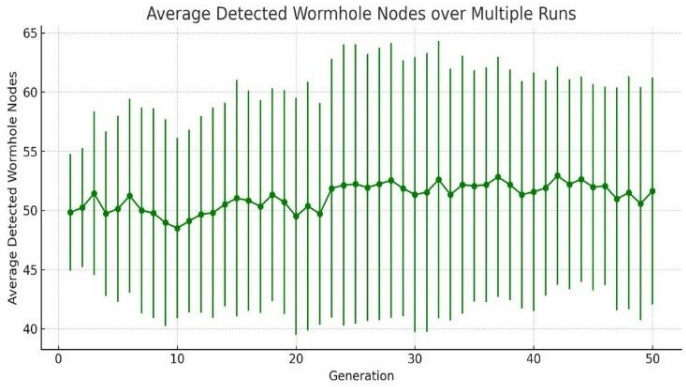


Figure 12: Average Detected Sinkhole nodes over Multiple runs

By performing this error analysis, we derive valuable conclusions about the stability and consistency of the simulation results when repeated multiple times.

Sensitivity Analysis

The sensitivity analysis results are depicted in the three plots. The first plot (Figure 13), titled "Sensitivity of Average Best Fitness," demonstrates how the average best fitness evolves when varying the crossover probability and mutation rate parameters. The colour represents the average best fitness, with lighter colours indicating higher fitness. This heat map provides an intuitive way to understand how these two key parameters impact the overall performance of the genetic algorithm. The second plot (Figure 14), "Sensitivity of Average Detected Sinkhole Nodes," illustrates how the average number of detected sinkhole nodes changes when adjusting the crossover probability and mutation rate parameters. The colour signifies the average number of detected sinkhole nodes, with lighter colours indicating a higher number. This visualization is valuable for understanding the relationship between these parameters and the effectiveness of the algorithm at detecting sinkhole nodes. The final plot (Figure 15), "Sensitivity of Average Detected Wormhole Nodes," displays the influence of varying crossover probability and mutation rate on the average number of detected wormhole nodes. Here again, lighter colours represent a higher average number of detected wormhole nodes. Through this sensitivity analysis, we can observe how small changes in key parameters can have a substantial effect on the outcome of the genetic algorithm. These insights can be useful for fine-tuning the parameters to achieve optimal results.

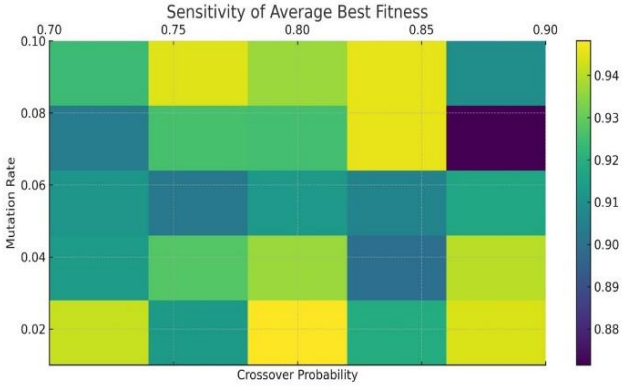


Figure 13: Sensitivity analysis - Average Best Fitness

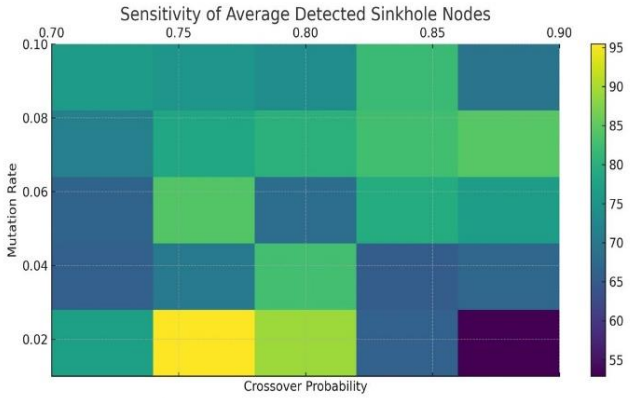


Figure 14: Sensitivity analysis - Average Detected Sinkhole nodes

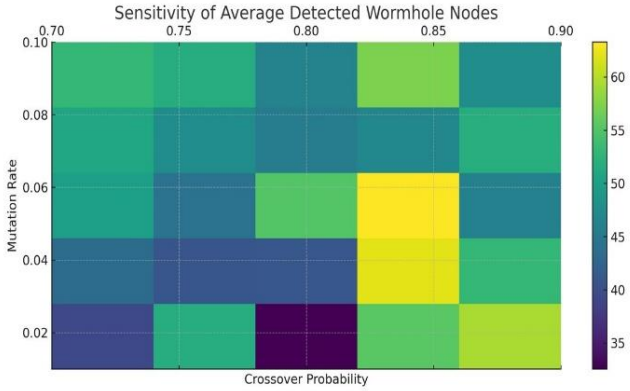


Figure 15: Sensitivity analysis - Average Detected Wormhole nodes

CONCLUSION

The deployment of wireless sensor networks faces numerous vulnerabilities, making them susceptible to various types of attacks. Among these attacks, sinkholes and wormholes are particularly prominent, aiming to disrupt the network's proper functioning. Detecting and countering such attacks nodes in wireless sensor networks pose significant challenges in the research field. This study presents an innovative approach that combines genetic and trust-based methods to address the complex scenario of a combined sinkhole-wormhole attack on a wireless sensor network. Unlike commonly used cryptographic-based, rule-based, probability-based, and neighbour discovery-based systems, the proposed scheme put forward by this study focuses on establishing trust levels among neighbouring nodes based on their packet forwarding and packet address modification behaviours.

To achieve this, a trust equation is utilized as the fitness function of the genetic algorithm. This allows the genetic algorithm to search through the search space by evaluating each sensor node within selected chromosomes of sensor nodes to identify potential malicious sinkhole and/or wormhole nodes based on their trustworthiness, determined by their packet forwarding behaviour and packet address modification metrics. By finding optimal routes that prioritize more trustworthy nodes, the proposed scheme aims to reduce packet loss and improve throughput during node connectivity in the network.

The proposed scheme is especially well-suited for sensor networks requiring rapid deployment, as it imposes no prerequisites on network establishment and operation phases. Through the study's results and analysis, the efficacy of the genetic algorithm has been confirmed in conjunction with the trust model for detecting malicious sinkhole and wormhole nodes in the wireless sensor network. And the research objectives set out in this study have been achieved.

References

[1] M. K. Prasannadevi, P. Karthikeyan, and M. A. Swathy, "A Research of Dealing with Sinkhole Attacks To Prevent Security in WSN."

[2] Dr. A. A. Waoo and Mr. V. Tiwari, "Challenges in Sinkhole Attack Detection in Wireless Sensor Network," *Indian Journal of Data Communication and Networking*, vol. 1, no. 4, pp. 1–7, Aug. 2021, doi: 10.54105/ijdcn.C5016.081421.

[3] D. Martins and H. Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms-A short survey." [Online]. Available: https://hal.science/hal-00661831

[4] IEEE Staff and IEEE Staff, *2010 IEEE International Conference on Wireless Communications, Networking and Information Security.*

[5] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, vol. 26, no. 5, pp. 3169–3182, Jul. 2020, doi: 10.1007/s11276-019-02129-w.

[6] R. Zeng, "Applied technology for typical attacks and security mechanisms in wireless sensor networks," in *Advanced Materials Research*, Trans Tech Publications Ltd, 2014, pp. 484–490. doi: 10.4028/www.scientific.net/AMR.977.484.

[7] D. Padmapriya, S. Sathya, S. Jeyalaksshmi, and S. Kamalakkannan, "A Survey: Techniques and Challenges to Detect Wormhole Attack in Wireless Sensor Network."

[8] R. Waseem Anwar, M. Bakhtiari, A. Zainal, K. Naseer Qureshi, and J. Bahru, "WIRELESS SENSOR NETWORK PERFORMANCE ANALYSIS AND EFFECT OF BLACKHOLE AND SINKHOLE ATTACKS," 2016. [Online]. Available: www.jurnalteknologi.utm.my

[9] M. Patel, A. Aggarwal, and N. Chaubey, "Detection of wormhole attack in static wireless sensor networks," in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2019, pp. 463–471. doi: 10.1007/978-981-13-0344-9_39.

[10] A. Abduvaliyev, A.-S. Khan Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks."

[11] P. Ahlawat and M. Dave, "An attack resistant key predistribution scheme for wireless sensor networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 3, pp. 268–280, Mar. 2021, doi: 10.1016/j.jksuci.2018.03.002.

[12] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking," *IEEE Access*, vol. 8, pp. 92098–92109, 2020, doi: 10.1109/ACCESS.2020.2994587.

[13] J. S. Terence and G. Purushothaman, "A novel technique to detect malicious packet dropping attacks in wireless sensor networks," *Journal of Information Processing Systems*, vol. 15, no. 1, pp. 203–216, 2019, doi: 10.3745/JIPS.03.0110.

[14] M. M. Singh, N. Dutta, T. R. Singh, and U. Nandi, "A technique to detect wormhole attack in wireless sensor network using artificial neural network," in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 53, Springer Science and Business Media Deutschland GmbH, 2021, pp. 297–307. doi: 10.1007/978-981-15-5258-8_29.

[15] G. Jahandoust and F. Ghassemi, "An adaptive sinkhole aware algorithm in wireless sensor networks," *Ad Hoc Networks*, vol. 59, pp. 24–34, May 2017, doi: 10.1016/j.adhoc.2017.01.002.

[16] K. Harsanyi, A. Kiss, and T. Sziranyi, "Wormhole detection in wireless sensor networks using spanning trees," in *2018 IEEE International Conference on Future IoT Technologies, Future IoT 2018*, Institute of Electrical and Electronics Engineers Inc., Mar. 2018, pp. 1–6. doi: 10.1109/FIOT.2018.8325596.

[17] S. Al-Ahmadi, "A Novel Energy-efficient Wormhole Attack Prevention Protocol for WSN based on Trust and Reputation Factors," Scitepress, Feb. 2022, pp. 191–201. doi: 10.5220/0010951400003118.

[18] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4596–4614, Nov. 2016, doi: 10.1002/sec.1652.

[19] A. Pirzada, C. Mcdonald, and A. A. Pirzada, "Circumventing Sinkholes and Wormholes in Wireless Sensor Networks," 2005. [Online]. Available: https://www.researchgate.net/publication/250774526

[20] R. Okoro, O. C. Ubadike, A. J. Onumanyi, and A. M. Aibinu, "Routing optimization in a wireless network using genetic algorithm and ILA routing metric," *Nigerian Journal of Technology*, vol. 40, no. 5, pp. 938–946, May 2022, doi: 10.4314/njt. v40i5.19.

[21] W. Lin, W. Lee, and T. Hong, "Adapting Crossover and Mutation Rates * in Genetic Algorithms," 2003.

[22] S. Kannimuthu and K. Premalatha, "Discovery of high utility itemsets using genetic algorithm with ranked mutation," *Applied Artificial Intelligence*, vol. 28, no. 4, pp. 337–359, Apr. 2014, doi: 10.1080/08839514.2014.891839.

[23] S. Aliabadi and M. A. Saram, "An Approach to DSRRouting QOS by Fuzzy-Genetic Algorithms [," *International Journal of Wireless & Mobile Networks*, vol. 6, no. 2, pp. 89–100, Apr. 2014, doi: 10.5121/ijwmn.2014.6208.

[24] R. Waseem Anwar, M. Bakhtiari, A. Zainal, and K. Naseer Qureshi, "Malicious Node Detection Through Trust Aware Routing in Wireless Sensor Networks," *J Theor Appl Inf Technol*, vol. 10, no. 1, 2015, [Online]. Available: www.jatit.org

[25] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, "Mobile networks: Trust management in wireless sensor networks," *European Transactions on Telecommunications*, vol. 21, no. 4, pp. 386–395, Jun. 2010, doi: 10.1002/ett.1413.

[26] A. Norouzi and A. H. Zaim, "Genetic algorithm application in optimization of wireless sensor networks," *The Scientific World Journal*, vol. 2014, 2014, doi: 10.1155/2014/286575.