International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN: 2347-5552, Volume-12, Issue-6, November 2024
https://doi.org/10.55524/ijircst.2024.12.6.1
Article ID IRP-1566, Pages 1-6
www.ijircst.org

New Strategies for Boosting Localization Accuracy in Wireless Sensor Nodes

Mohankumar T P[1], and D. Ramesh[2]

[1] Research Scholar, Department of Computer Applications, Sri Siddhartha Academy of Higher Education, Tumakuru, India
[2] Professor, Department of Computer Applications, Sri Siddhartha Academy of Higher Education, Tumakuru, India

Correspondence should be addressed to Mohankumar T P; mohankumartp@ssit.edu.in

Received 12 September 2024; Revised 26 September 2024; Accepted 11 October 2024

ABSTRACT - Wireless Sensor Networks (WSNs), accurate and energy-efficient localization of sensor nodes remains a challenging task despite significant advancements. Current geolocation algorithms often struggle with scalability, adaptability, and energy efficiency, particularly in large-scale, dynamic environments where node failures or random shifts occur. This paper proposes a novel Secure Node Localization (SABWP-NL) approach, combining Self-Adaptive Binary Waterwheel Plant Optimization (SABWP) and Bayesian optimization to enhance localization accuracy, scalability, energy efficiency, and robustness. The method evaluates node trust using Dempster-Shafer Evidence Theory to secure localization against rogue nodes and optimizes the localization process through trilateral and multilateration systems. The SABWP-NL approach demonstrates superior performance in terms of localized nodes and localization error compared to existing techniques like BWP, ROA, and AO. Results show that SABWP-NL achieves the highest number of localized nodes and the lowest localization error, making it a promising solution for efficient and secure node localization in WSNs.

KEYWORDS- Wireless Sensor Networks, Secure Node Localization (SABWP-NL) Approach, Bayesian optimization, Dempster-Shafer Evidence Theory.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have gained significant attention in recent years due to their wide range of applications, including environmental monitoring, healthcare, industrial automation, and military surveillance. One of the critical challenges in WSNs is the accurate localization of sensor nodes, as the functionality and effectiveness of these networks heavily depend on knowing the precise positions of nodes. Despite advancements in geolocation techniques, existing algorithms often face limitations in terms of energy consumption, scalability, adaptability, and accuracy. These challenges become more pronounced in large-scale and dynamic environments where sensor nodes may fail, shift randomly, or be subject to security threats like rogue nodes. Localization accuracy is often compromised by the trade-off between energy efficiency and precision, which is especially problematic in resource-constrained WSNs [1-5]. Additionally, many existing approaches lack robustness, making them less suitable for real-world deployment where scalability and reliability are essential. Applications such as target tracking and data source location are made possible by the location information in WSNs, which also allows for effective routing and power savings [6]. For a large-scale network with movable nodes, manual location setup is not possible. Since global positioning systems (GPS) are expensive in terms of both cost and energy consumption, it is not a practical option to equip every node with GPS hardware for localization [7]. High-resolution time synchronization with satellites is often achieved using complex hardware, such as an onboard GPS, which is a typical high-end solution [8]. This approach is not feasible due to the power and cost limitations of small sensor nodes. Alternative approaches need individual node devices capable of varying across adjacent nodes. This is most crucial topics, since location data is frequently needed for coverage, location services, deployment, target tracking, routing, and rescue [9-14]. However, conventional localization solutions sometimes encounter difficulties due to things like challenging deployment conditions, scarce resources, and possible security risks. Incorrect node localization can cause data integrity issues, and ineffective routing, and eventually make it more difficult for the network to achieve its monitoring targets. Moreover, effective data transfer is critical to prolonging WSNs' operating life. Since sensor nodes are frequently placed in remote areas and run on batteries, it is essential to minimize energy usage when transmitting data. Existing routing techniques may not always emphasize energy efficiency, which could result in early node resource depletion and shorter network lifetime [15-18].

To address these challenges, Present research paper introduces a novel approach called Self-Adaptive Binary Waterwheel Plant Optimization (SABWP-NL), which integrates advanced optimization techniques with secure trust-based localization methods. By evaluating node trust using Dempster-Shafer Evidence Theory and employing SABWP for optimal node localization, the proposed method significantly improves localization accuracy, energy efficiency, and robustness. The approach is particularly effective in mitigating the effects of rogue nodes and ensuring secure localization, making it a promising solution for enhancing WSN deployment in real-world applications.

II. PROBLEM STATEMENT

In WSNs, sensor node localization is still a difficult task in spite of great progress made in the area. The energy consumption, accuracy, scalability, and adaptability of current geolocation algorithms are frequently limited. Certain algorithms prioritize accuracy over energy efficiency when it comes to resource conservation in frameworks with limited resources. There are still problems with reliability, and scalability, particularly in large-scale networks and dynamic contexts where nodes may fail or shift randomly. Furthermore, the suggested approaches' evaluations are frequently not thorough enough, with insufficient analyses of their scalability, robustness, and flexibility to different deployment environments. Therefore, a unique localization methodology that combines several goals such as better localization accuracy, scalability, increased energy economy, robustness in dynamic situations, and thorough assessment methodologies is urgently needed. A strategy like this would greatly expand the capabilities of WSNs and make it easier for them to be widely deployed in a variety of real-world applications.

III. PROPOSED METHODOLOGY

The proposed approach SA-BWP is based on secure node localization. In this, the trust of nodes is evaluated and the based on the trust the nodes are arbitrarily positioned in the environment, and their locations are determined accurately using SA-BWP. Then, G-BWP is employed to select optimal routes for data transmission, with potential alterations made based on the presence of multiple sinks. This approach aims to enhance the performance of WSNs by optimizing secure node localization, route selection, and data transmission efficiency. The structure of proposed model is displayed in Figure 1.

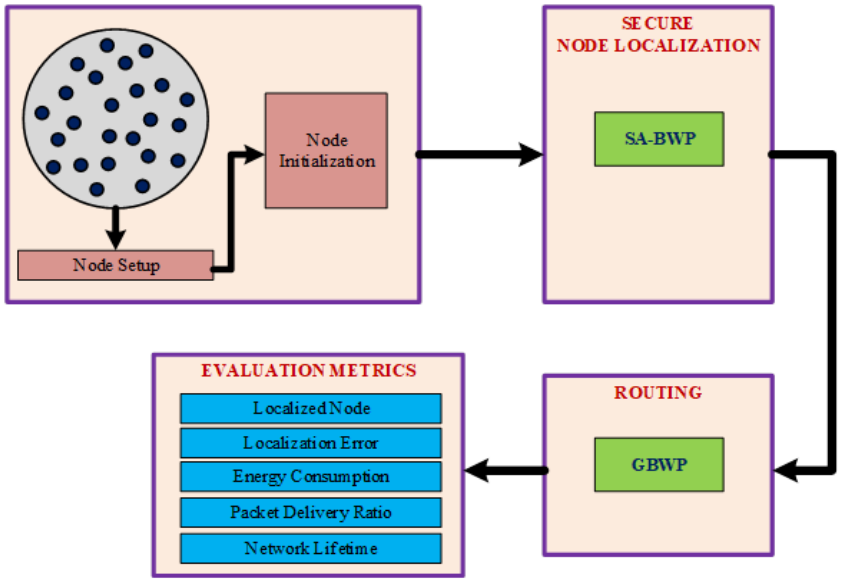

Figure 1: Proposed System Model

A. Secure Node Localization

The first object function is to evaluate the trust of nodes; this is done using Dempster-Shafer Evidence Theory and is divided into three phases: (i) Direct trust assessment; (ii) Indirect trust evaluation; and (iii) A mix of the direct and indirect trust.

Assume a sensor network that consists of both Anchor Node (AN) and Target Nodes (TN). The ANs in a network are presumed to be able to self-place utilizing positioning devices, whereas TNs must localize their position using information from ANs and other nodes. This approach uses the signal attenuation algorithm to estimate the location information first based on the information collected from the AN. Once the AN and TNs have gathered sufficient data, the maximum likelihood estimation approach is employed. The attacker nodes may tamper with the real data gathered by anchor node during this information gathering phase, which results in low localization accuracy. Either an anchor or target node may experience this situation. The Quality of Service (QoS) could be impacted if the malicious target node sends erroneous information to the anchor node. A data aggregation strategy is used when a rogue node transmits duplicate data. A trust evaluation-based model is presented to preserve target and anchor node credibility. According to this model, the target node with the highest trust value is regarded as dependable, and the node with the lowest trust value is eliminated from consideration for the next simulation cycle. Given that anchor node within range of an unknown target node sends a location request signal 'L_{req}' and that node receives an acknowledge packet 'L_{ack}' from the associated node. This incorporates a model of trust computation for both regular and anchor nodes, respectively. At this point, the comprehensive trust values are calculated using the values for direct and indirect trust. The following is an expression of the comprehensive trust's value:

$$T_{Com} = \alpha * T_D + \beta * T_{ID} \quad (1)$$

Where, T_{Com} is value of comprehensive trust; T_D represents value of direct trust; α indicates weight factor of T_D; T_{ID} denotes value of Indirect trust; β specifies weight factor of T_{ID};

The final Direct Trust value can be calculated as following Eqn. (1)

$$T_D = \begin{cases} M_{ab}\{T\} = \alpha_{ab} \\ M_{ab}\{\bar{T}\} = \beta_{ab} \\ M_{ab}\{T, \bar{T}\} = 1 - (\alpha_{ab} + \beta_{ab}) \end{cases} \quad (2)$$

Where, M represents probability of mass function; The sum of the data packet consistency, reception rates, and successful transmission degree is represented by α_{ab}; β_{ab} represents the total degree of transmission discard, reception rates, and packet irregularity.

The trust functions are also computed after the node's trust has been assessed. Then, the indirect trust of nodes x, y is assessed using the data obtained from nearby nodes as indicated by Eqn. (3); in contrast to direct trust, the indirect trust is assessed using the trust data gathered from nodes that are in-between one another rather than by direct interactions.

$$T_{ID} = \begin{cases} M_{ab}\{T\} = \alpha_{a-x-b} \\ M_{ab}\{\bar{T}\} = \beta_{a-x-b} \\ M_{ab}\{T, \bar{T}\} = 1 - (\alpha_{a-x-b} + \beta_{a-x-b}) \end{cases} \quad (3)$$

Where, x is the common neighbor for the nodes "a" and "b" and α_{a-x-b} is the sum of the transmission-reception success probability rate and the consistency between nodes "a" and "x" and the nodes "b" and "x"; The failure probability rate of the aforementioned nodes is totalled as β_{a-x-b}.

Furthermore, Eqn. (4) provides the final probability for the trust evaluation.

$$T_{Eval} = M\{T\} + \left(P\{T\}/P\{T\} + P(\bar{T})\right) * M\{T, \bar{T}\} \quad (4)$$

The following Eqn. (5) provides the average of the trust value along the length L:

$$T_{avg} = \sum_{a=1}^{L} T_{Eval}(t+1)/L \quad (5)$$

Higher trust levels indicate that nodes are more trustworthy. It may be necessary to exclude or give less weight to data from nodes with low trust scores. In the localization process, the distance measurements are determined based on the trust assessments. This study introduces Self-Adaptive Binary Waterwheel Plant Optimization (SABWP) algorithm for localizing nodes after trust evaluation.

B. Processes involved in SABWP

A group of individuals utilize the Waterwheel Plant Optimization (WPO) technique to repeatedly explore the search space for good solution to a problem. The functionality of WPO has been combined with a number of additional operators to create a BWP algorithm that optimizes solutions in a discrete solution space. The binarization of WWPA is a method for solving feature selection issues that gain from formalizing the search space. The BWP Algorithm is a new algorithm that draws inspiration from the way waterwheel plants search and update their positions during the processes of exploration and exploitation. The act of selecting the best features for a classification issue in order to increase the accuracy of the classification is called feature selection, and it is accomplished using the BWP algorithm. The first stage, which defines transformation functions, can change the representation of the solution and optimization process from a continuous to a discrete form. It is imperative to address feature selection-specific issues using the innovative technique. The second modelled method for reaching BWP variant is to modify fitness function. It is necessary to calculate the fitness of every potential solution in order to determine overall best solution. It offers a specification of the fitness function in order to handle the particulars of the current circumstance. The best continuous solution obtained by the continuous WWPA is denoted as S_{best}, and the continuous solution obtained by the WWPA algorithm is transformed to binary using the following sigmoid function.

$$binary = \begin{cases} 1 & if\ sigmoid\ (S_{best}) \geq 0.5 \\ 0 & otherwise \end{cases} \quad (6)$$

$$sigmoid\ (S_{best}) = \frac{1}{1+e^{-10(S_{best}-0.5)}} \quad (7)$$

The main limitations of BWP are the performance is heavily reliant on the control parameters and fitness function selection, and the algorithm may become trapped in local optima, which might result in less-than-ideal answers. To overcome these drawbacks, the self-adaptive Bayesian inspired BWP is introduced in this phase to improve the performance. For this vector optimal solution is introduced using Bayesian optimization method in above function and it can be rewrite as:

$$sigmoid\ (S_{best}) = \hat{\eta}\ \left(\frac{1}{1+e^{-10(S_{best}-0.5)}}\right) \quad (8)$$

Where, $\hat{\eta}$ denotes vector optimal solution and it can be expresses as:

$$\hat{\eta} = \underset{\eta}{\operatorname{argmax}}\, P(f(x_{1:n})|\,\eta) \quad (9)$$

Finding a maximum likelihood estimate is the first step. By using this method, the probability of observations $(x_{1:n})$ is obtained under the prior, $(f(x_{1:n})|\,\eta)$, and the notation can be change to show its reliance on the η. This is a multivariate normal density for likelihood. Then, set η to the value that maximizes this likelihood in estimation process. The η value is set in the ranges between 0 and 1. It is especially helpful when minimizing an objective function that is difficult to analyze. The primary benefit of using Bayesian optimization is its ability to locate global optima in an acceptable period, even in hyperparameter spaces that are noisy or irregular. Bayesian optimization has been applied to improve continuous system performance and to adjust the optimal solution.

C. SABWP-NL Based Localization Process

The sensor's coordinate point is initiate by employing SABWP-NL localization approach. The goal of study is to reduce the objective function in order to measure the coordinate points of chosen node. WSN localization issues were taken into consideration as optimization issues were created using a variety of metaheuristic techniques. The following procedures are involved in the SABWP-NL model for localizing the sensor nodes in WSN:

- Arrange 'X' Target Node (TN) and 'Y' Anchor Node (AN) in any way within the sensor zone. Every AN is composed of location awareness to determine the location. Every TN and AN cover the signal range R.
- Additive Gaussian noise is used to measure and modify the distances between TN and AN. The target node specifies the distance as $\widehat{D_r} = D_r + N_r$, where, where D_r signifies the actual distance that is calculated using Eqn. () between TN's position (a, b) and AN's location $(a_i,\ b_i)$.

  $$D_r = \sqrt{(a-a_i)^2 + (b-b_i)^2} \quad (10)$$

  Where, N_r represents the noise that affects the expected distance from $D_r \pm D_r\left(\frac{S_n}{100}\right)$, while S_n stands for the

noise ratio in the distance that is evaluated.

- If there are three anchor nodes inside the TN's communication radius, the desired node is considered localizable. Next, the distance between TN and three ANs is recognized, along with the explanation based on trilateral positioning system and coordinates of three anchor nodes $A(a_1,\ b_1)$, $B(a_2,\ b_2)$, and $C(a_3,\ b_3)$. Similarly, the coordinates of TNs are defined by using sine or cosine trigonometric formulas. The distance metrics of massive ANs are applied in the multilateration TN evaluation model concurrently to reduce errors from the original and predicted distance.
- The location of TN can be determined autonomously for the localizable node using SABWP-NL technique. The given task enforces the coyotes inside the transmission radius of the ACN centroid:

$$(a_m, b_m) = \left(\frac{1}{L}\sum_{i=1}^{L} a_i\ , \frac{1}{L}\sum_{i=1}^{L} b_i\right) \quad (11)$$

Where, L indicates total number of ANs within the localization TN's communication range.

- The coordinates (a, b) that lessen error localization are appropriate to be recognized as the TN using SABWP-NL method. The primitives used in localized problem are a mean square distance between TN and ANs, which is reduced by using following Eqn. (12):

$$f(a,b) = \frac{1}{L}\left(\sum_{i=1}^{L}\sqrt{(a-a_i)^2 + (b-b_i)^2} - \widehat{D_r}\right)^2 \quad (12)$$

Where, the quantity of AN within a TN transmission radius is indicated by $L \geq 3$.

- The SABWP-NL technique is then used to identify the ideal position coordination (a, b) once the maximum number of iterations has been reached.
- After assessing the localization target node NL, the whole localization error is defined. The distance between defined node coordinates $(A_i,\ B_i)$ and actual node coordinates $(a_i,\ b_i)$ is measured as the mean square, and it can be represented as following Eqn. (13):

$$LE_1 = \frac{1}{L_1}\sum_{i=1}^{L}\sqrt{(a-a_i)^2 + (b-b_i)^2} \quad (13)$$

- The TN is localized by repeating steps two through six in this process. The localization module is defined by the maximum error localization LE_1 and the number of unlocalized nodes U_{N_L} in the $U_{N_L} = M - N_L$ application. An efficient localization is enhanced by the minimal score of LE_1 and U_{N_L} combined.

A higher iteration count results in a higher number of localized nodes. As the measured position of TN performs an AN in the subsequent iteration, it also leads to an increase in the number of AN in the transmission radius of localizable TN. It can be applied to limit the flip uncertainty problem that leads to higher error localization. Therefore, increasing the iteration improves the processing time for localized data of the TN. The working process of SABWP-NL is illustrated in Figure 2.

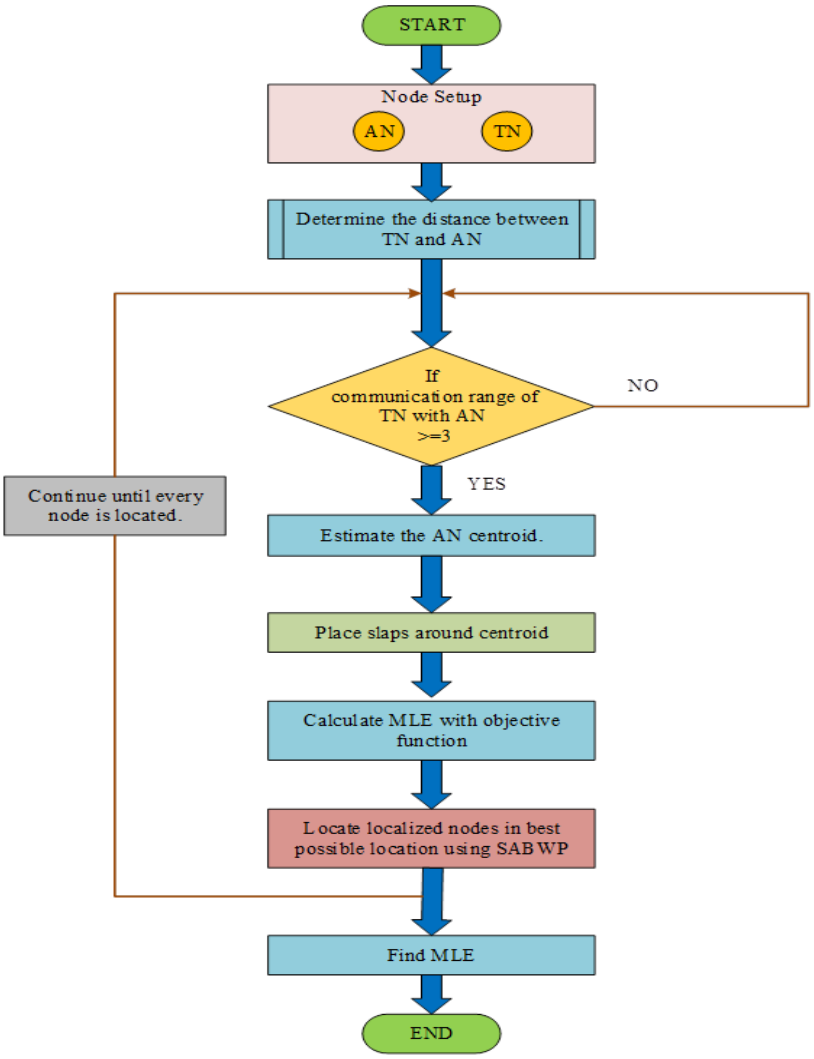

Figure 2: Flowchart of SABWP based Node Localization

IV. PERFORMANCE EVALUATION OF NODE LOCALIZATION

This section presents the analysis of Localized Node (LN) and LE of the SA-BWP based NL methodology with other existing techniques such as BWP, ROA, and AO. Table 1 validate the localization performance of proposed technique with current models in terms of localized node.

Table 1: Evaluation of LN using AN

Methods	No. of Anchor Nodes				
	10	20	30	40	50
Proposed SA-BWP	149	153	179	192	203
BWP	129	137	151	168	183
ROA	103	136	147	151	163
AO	114	111	121	134	143

According to results, the proposed SA-BWP based NL approach produced better results with the highest LN. For illustration, the proposed method has a maximum number of LN of 149 with 10 anchors, whereas the minimum LNs acquired by the BWP, ROA, and AO systems are 129, 103, and 114 respectively. The proposed model achieves 153, 179, and 192 LN for 20, 30, and 40 anchors respectively and these LNs of proposed strategy is highest when compared to other existing methods. The proposed model eventually achieved a maximum number of LN of 203 with 50 anchors, whereas the AO, ROA, and BWP approaches obtained lowest NLNs of 143, 163, and 183 respectively. The analysis result is displayed in Figure 3.

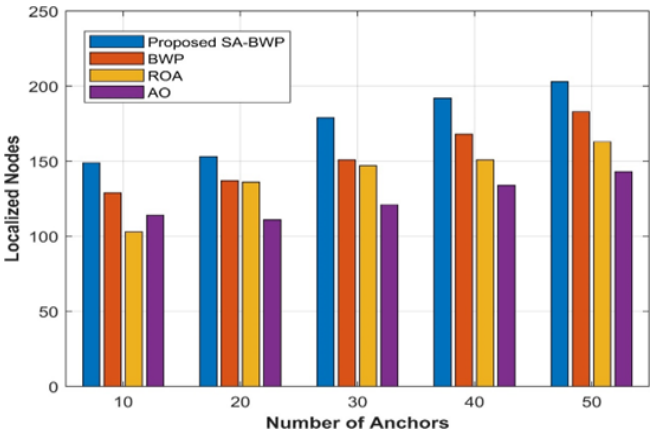

Figure 3: Analysis of NL for proposed and existing approaches

A brief LE analysis of proposed SA-BWP based NL method is conducted with different anchors. Table 2 depicts the evaluation findings of LE for proposed and various present approaches.

Table 2: Evaluation of LE using various number of AN

Methods	No. of Anchor Nodes				
	10	20	30	40	50
Proposed SA-BWP	0.27	0.25	0.15	0.07	0.06
BWP	0.35	0.27	0.26	0.28	0.19
ROA	0.4	0.35	0.35	0.29	0.26
AO	0.57	0.62	0.4	0.37	0.34

The forementioned LE analysis demonstrates that the proposed approach produced the lowest LE of 0.27 under 10 anchors, but ROA, BWP, and AO algorithms produced higher LEs of 0.4, 0.35, and 0.57, respectively. Furthermore, the SA-BWP methodology yielded a minimum LE of 0.15 under 30 anchors, but the AO, BWP, and ROA methods achieved higher LEs of 0.4, 0.26, and 0.35, respectively. Similarly, the BWP, AO, and ROA techniques have obtained a maximum LE of 0.19, 0.34, and 0.26 respectively under 50 anchors, whereas the proposed approach has produced a minimum LE of 0.06. Figure 4 demonstrates how the SA-BWP technique has produced better results with the least amount of LE.

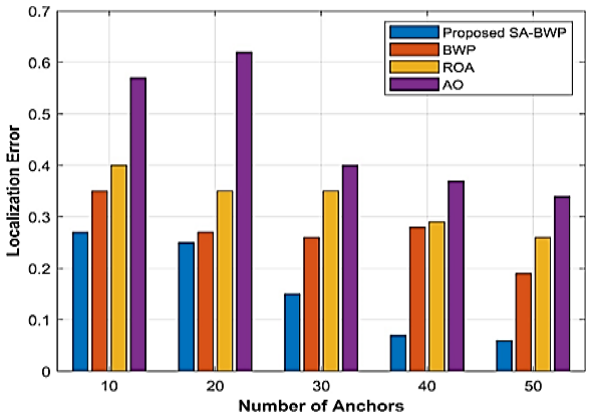

Figure 4: Analysis of LE

V. CONCLUSION

This study focused on secure node localization presenting a novel strategy to improve WSN performance. The crucial issue of resource limitations and security flaws in WSNs is addressed by the suggested method. The study introduced Self Adaptive Binary Waterwheel Plant Optimization method to locate secure nodes. The purpose of this stage is to reduce security risks from the initial deployment phase by including trust evaluation. The position of sensor nodes is efficiently and accurately determined by SA-BWP algorithm. The performance of proposed method is evaluated and compared with various existing algorithms such as BWP, GOA, ROA, and AO. The proposed method performs better in NL than other existing models. This study addresses significant issues of security, efficiency, and performance optimization while contributing innovative methods to WSN. Investigating the use of the suggested method in various WSN deployment circumstances may be one of the future research paths.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] A. Karthikeyan and G. Aghila, "Survey on localization in wireless sensor networks: An emerging research area," *International Journal of Computer Networks & Communications*, vol. 10, no. 1, pp. 75–98, 2018.

[2] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 402–427, 2013. Available From: https://doi.org/10.1109/SURV.2012.031412.00077

[3] H. Yang, X. Wang, L. Zhang, and Y. Jin, "Localization algorithms in wireless sensor networks: A survey," *Wireless Communications and Mobile Computing*, 2015. Available From: https://doi.org/10.1007/s11235-011-9564-7
[4] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero III, R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 54–69, 2005. Available From: https://doi.org/10.1109/MSP.2005.1458287
[5] Z. Yang and Y. Wu, "Localization in wireless sensor networks," *Lecture Notes in Computer Science*, vol. 4487, pp. 276–293, 2007. Available from: https://shorturl.at/KC06D
[6] R. Zhang, P. K. Varshney, and K. R. Pattipati, "A robust sequential localization approach in wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 58, no. 8, pp. 3949–3962, 2010.
[7] A. Kumar and R. K. Jha, "Energy efficient routing schemes in WSN: A survey," *IEEE Access*, vol. 5, pp. 4590–4620, 2017.
[8] L. Wang, G. Chen, and M. Dong, "Trust evaluation based secure localization algorithm for wireless sensor networks," *Journal of Networks*, vol. 8, no. 1, pp. 142–149, 2013.
[9] S. Xiao and S. Liu, "Localization in wireless sensor networks using multi-objective optimization approach," *IEEE Sensors Journal*, vol. 14, no. 9, pp. 2836–2846, 2014.
[10] H. Nguyen and P. Minet, "Analysis of localization accuracy in wireless sensor networks with a mobility model," *Wireless Networks*, vol. 19, no. 6, pp. 1231–1244, 2013.
[11] A. Savvides, C. C. Han, and M. B. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2001, pp. 166–179. Available From: https://doi.org/10.1145/381677.381693
[12] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, vol. 3, 2003, pp. 1976–1986. Available From: https://doi.org/10.1109/INFCOM.2003.1209219
[13] W. Zhang, X. Liu, G. Chen, and W. He, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 6, pp. 1044–1054, 2011. Available From: https://doi.org/10.1109/JSAC.2005.863855
[14] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1067–1080, 2007. Available From: https://doi.org/10.1109/TSMCC.2007.905750
[15] Y. Li, G. Mao, B. Fidan, and B. D. Anderson, "Wireless sensor network localization techniques," *Computer Networks*, vol. 51, no. 10, pp. 2529–2553, 2007. Available From: https://doi.org/10.1016/j.comnet.2006.11.018
[16] T. Alhmiedat, "Fingerprint-based localization approach for WSN using machine learning models," *Applied Sciences*, vol. 13, no. 5, p. 3037, 2023. Available From: https://doi.org/10.3390/app13053037
[17] U. Dampage, L. Bandaranayake, R. Wanasinghe, K. Kottahachchi, and B. Jayasanka, "Forest fire detection system using wireless sensor networks and machine learning," *Scientific Reports*, vol. 12, no. 1, p. 46, 2022. Available From: https://doi.org/10.1038/s41598-021-03882-9
[18] F. Ojeda, D. Mendez, A. Fajardo, and F. Ellinger, "On wireless sensor network models: A cross-layer systematic review," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, p. 50, 2023. Available From: https://doi.org/10.3390/jsan12040050

ABOUT THE AUTHORS

Mohan Kumar T.P, is an Assistant Professor with over 21 years of experience in Software Engineering. He holds an MCA, MPhil, and MTech, and his research work has led to several publications in the field. His expertise extends to guiding research projects in software engineering and technology. As a member of the professional body MISTE, he actively contributes to academic and professional communities.

Dr. D. Ramesh is a Professor and HOD with 32 years of experience in Computer Networks, Software Engineering, and Database Management Systems. He holds a B.E, M.S, and Ph.D., and has authored numerous publications in his areas of expertise. As a member of MISTE and CSI, he actively contributes to professional bodies. His achievements include guiding significant research projects and leading his department's academic growth.