ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 14; Issue 03; 2026; Page No. 47-55

A Novel Harmony Search Framework for Sinkhole Attack Recognition in Wireless Sensor Networks

Avinash chaubey[1], Harish Dutt Sharma[2], Pintu Kumar[2]

[1]Research Scholar, School of Computer Engineering and Applications, Maya Devi University, Dehradun, 248011, India.

[2]School of Computer Engineering and Applications, Maya Devi University, Dehradun, 248011, India

Email-ID: avinashchaubey263@gmail.com

Email-ID: sharma.harish106@gmail.com

Email-ID: pin295kumar@gmail.com

Conflicts of interest: Nil

Corresponding author: Harish Dutt Sharma

Abstract

A Wireless Sensor Network (WSN) is a system of interconnected sensor nodes that can detect and exchange data wirelessly over very small distances. The communication aspect of WSN makes security a major concern. There have been a number of attacks against the sensor nodes. In a sinkhole attack, a node in the WSN falsely claims to be the one with the shortest route to another node, either the sink or the destination. In order to identify the sinkhole attack, researchers put forth several methods. In this research work, Revamped Harmony Search is employed to detect sinkhole nodes in WSN. The proposed model is compared with 4 other existing techniques to prove its significance. The results are interpreted with different level of imposing sinkhole nodes in the network and on different patterns. On an average, the proposed HRS method significantly outperforms the existing methods.

Keywords: WSN, sinkhole attack detection, Revamped Harmony Search.

1. Introduction

A sensor network consists of several small sensor nodes that can perceive their surroundings and communicate with one another using a wireless radio device [5]. The data is collected and sent from the source node to the destination node via numerous hop and it has limited resources like electricity, communication lines, computing power, etc [6]. When it comes to WSN, security is a major concern. Every node is in a dangerous environment, making it susceptible to attacks like sinkholes, wormholes, grey holes, and more [7]. Concerns about energy consumption, data storage capacity, and processing power need safety precautions in sensor networks [8]. Consequently, sensor networks may benefit from using lightweight mechanisms, which are appropriate in terms of computing and energy [9].

When a node in a WSN acts selfishly or with compromised intentions, the result is bad behaviour. Because of the exposed nature WSN are vulnerable to a variety of assaults [10]. Due to their unique communication style, WSN are susceptible to sinkhole attacks [11-13]. Also, it's a self-organising system of interconnected, miniature

sensor nodes that can feel, monitor, and interpret the physical environment via the use of radio transmissions [14].

The objective of a sinkhole attack is to divert almost all traffic into the sinkhole by using a compromised node to falsely pretend to have the best path to the target [15]. It creates significant problems for applications at higher layers because it prevents the base station from obtaining complete and accurate data. We decreased the attack in the wireless sensor network by protecting the compromised node using different settings.

In this research work, Revamped Harmony Search method is used to identify the sinkhole attack. To handle the binary representation of solutions, the Harmony Search method is improvised as Revamped Harmony Search (RHS) to solve sinkhole attack detection. The rest of the paper is organized to hold literature survey in Section 2, problem definition in section 3, proposed method in section 4, experimental analysis in section 5 and conclusion at section 6.

2. RELATED WORK

Due to the critical nature of packet delivery, WSN enables nodes to connect with one another over wireless channels [16]. The issues caused by various attacks are distinct. So, it's important to choose a safe and efficient way to get from the starting point to the final destination. Therefore, the aforementioned study [17] used a Naïve Bayes classifier based on Machine Learning to identify the attack, and an EC-BRTT based method was applied to thwart such noteworthy assaults.

Tabbaa et al. [18] employed both separate and combined ensemble methods in their suggested study. It was thought of as a mixed ensemble strategy, in contrast to the homogeneous ensemble technique proposed. The results of the experiments showed that when it came to detecting and categorising harmful assaults, both heterogeneous and homogeneous methods performed better. In a similar vein, the proposed technique for assessing assaults [19] relied on SINALGO to transport the simulation findings. For WSN attack detection, the proposed research also used SVM classification in conjunction with delay per-hop indication.

The proposed study [20] utilised ML techniques and MLPANN —a model with two critical portions—to identify and localise WSN DoS attacks. The strategy was then applied in a MATLAB simulation [21]. An improved system for safe and reliable data transfer is crucial for MANET applications due to its data-centric nature. To improve the classification process by giving more weight to the retrieved characteristics, the proposed research [22] used the AdaBoost algorithm rather than SVM. This was due to the fact that AdaBoost was deemed more robust.

On the other hand, Evolutionary algorithms have a vast range of applications solved in the domains such as in cloud computing [23, 29], data mining [24, 25], WSN [26-28] image processing [30, 35], cyber security [31-34] and so on. Therefore, we used a different optimization method to address the optimization challenge of detecting sinkhole attacks.

3. PROBLEM DEFINITION

The WSN connects the offline and online worlds and is already finding applications in many different sectors. Modern technology has allowed items to be equipped with processing units and sensors, allowing them to collaborate and communicate in order to accomplish shared goals. It is critical to protect WSN from intrusions because of their numerous uses and the powerful technology they use. Here we outline the specifics of the Internet of Things scenario, including how much power it will need.

A single instance of WSN with built-in sinkhole attack is shown in Figure 1. Nodes are the individual sensors that make up the WSN. Figure 1 shows a network with 10 nodes; node 2 is the sinkhole node, and node SH is the destination node. Additionally, the network has 8 valid nodes. With the circle 'SH' representing compromised nodes, the sinkhole node is responsible for collecting traffic

from these compromised nodes. The affected nodes are called "N4", "N6," and "N7" respectively. It is necessary to calculate the correlation measure for each node in order to locate the objective. The information acquired and delivered by each node all through the operation may be determined using this intrusion measure. Here is the representation of mathematical equation to evaluate the intrusion of a node in WSN:

$$IM_i = \frac{\sum_{j=1}^{N} DIP_{i,j}}{DOP_i} \quad (1)$$

the node that is now being used for the calculation of IM is denoted by i, and the nodes that are sending the packet to the relevant node i are denoted by j.

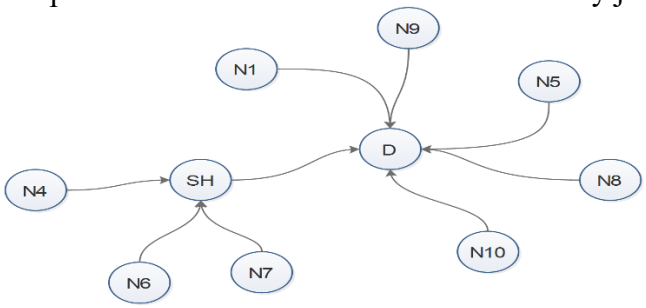

Figure 1: Sample WSN Architecture with Sinkhole node (SH)

Computing this for each node is computationally intensive, and it becomes increasingly so as a network size increases. Optimal node search can be useful in this context to deal with this issue. Anomaly nodes, defined as those with an out-of-the-ordinary IM value and excessive energy utilization are chosen using Harmony search method.

4. REVAMPED HARMONY SEARCH

The method known as the Harmony Search method is revamped in this part so that it can deal with binary representations of solutions.

4.1 Data Encoding

All the nodes in WSN are numbered in sequence from 1 to N where the N^{th} node is the node of Base Station. Hence the N^{th} node is not the part of the CH choosing criteria. The Revamped Harmony Search is used to choose the appropriate CH.

N1	N3	N4	N5	N6	N7	N8	N9	N10
0	0	1	0	1	0	0	1	0

Figure 2: Representation of Solution in binary form

Following the selection of the nodes N4, N6, and N9 from Figure 2, the calculation of IM values will be carried out on these particular nodes of the network. Regarding the optimization procedure, the fitness function that will be taken into consideration is going to be the IM values summation.

4.2 Revamped Harmony Search Algorithm

The Harmony Search (HS) algorithm is an optimisation method specifically designed to draw inspiration from the musical practice of improvisation. The first step involves the creation of a Harmony Memory (HM), which serves as a repository of potential solutions to the optimisation issue. Each instance of "harmony" stored in this memory refers to a possible solution, which is represented by a collection of choice variables. After picking values for each variable, either from the current harmonies in the Harmony Memory (with a probability set by the Harmony Memory Consideration Rate, HMCR) or randomly from the full available range (with a probability of 1-HMCR), the algorithm generates new harmonies. If a value is selected from the HM, it may be gently modified with a probability determined by the Pitch Adjustment Rate (PAR) in order to investigate potential solutions in close proximity.
The following condition will be taken place to improve the solution.

$$X_i = X_i \oplus \alpha \otimes (X_j \ominus X_k)$$

where X refers the solution, $\propto \in \{0,1\}$, $\otimes$ refers the bitwise EXOR, $\oplus$ refers the bitwise addition $\ominus$ refers the bitwise subtraction, i refers the current solution and j, k refers the random solution in the population.

Each freshly produced harmony (solution) is assessed using the objective function, which quantifies its quality, as the algorithm advances. Should the new harmony surpass the worst

harmony in the HM, it will supplant the worst harmony, therefore guaranteeing a progressive improvement in the overall quality of the HM. This iterative process of improvisation, assessment, and updating continues until a predetermined stopping condition is satisfied, usually after a certain number of stages. An optimum or near-optimal solution to the issue is defined as the best harmony in the memory at the conclusion of the procedure. The HS method is very efficient for intricate optimisation issues because of its capacity to strike a balance between exploration (exploring new regions of the solution space) and exploitation (improving existing excellent solutions).

Revamped Harmony Search (**RHS(*f*)**)

1. Initialize the problem and algorithm parameters:
- a. Define the objective function f(x) to be optimized.
- b.Initialize the Harmony Memory (HM) with size HMS (Harmony Memory Size).
- c.Set the Harmony Memory Consideration Rate (HMCR).
- d. Set the Pitch Adjustment Rate (PAR).
- e. Set the maximum number of improvisations (iterations).
- f. Set the number of decision variables (N).
- g. Define the lower and upper bounds for each decision variable.

2. Initialize the Harmony Memory (HM):
- a. For each harmony (solution) in HM:
  - i. For each decision variable:
    - Randomly generate a value within the variable's bounds.
  - ii. Calculate the objective function value for the harmony.
  - iii.Store the harmony and its objective function value in HM.

3. Improvise a new harmony:
- a. For each decision variable:
  - i. With probability HMCR, select a value from the existing harmonies in HM.
  - ii. With probability (1 - HMCR), generate a random value within the variable's bounds.
  - iii. If a value is selected from HM:
    - With probability PAR, adjust the selected value by adding a small random value.
- b. Calculate the objective function value for the new harmony.

4. Update the Harmony Memory:
- a. If the new harmony's objective function value is better than the worst harmony in HM:
  - i. Replace the worst harmony in HM with the new harmony.

5. Repeat steps 3 and 4 until the maximum number of improvisations is reached.

6. Return the best harmony (solution) found in HM.

Algorithm 1 Revamped Harmony Search Method

5. EXPERIMENTAL EVALUATION

In this section, the experimental setup, performance metrics and experimentation evaluation of the proposed RHS is discussed.

5.1 Experimental Setup

A total of four existing methods are used to compare the significance of the proposed RHS method, EM-SD[1], MRH [2], LB-IDS [3] and T-IDS [4]. The implementation is carried out in MATLAB version 9 with the system specification of 3.7zGHz of processor speed with 16GB RAM.

5.2 Performance Metrices

The end-to-end latency and total network lifetime were two performance metrics that were measured in seconds and used in the assessment presented. To test how well the strategy worked, we changed the weightage of malicious nodes in the network and used percentages 15%, 20%, and 25%.

5.2.1 The End-to-end Latency

The total time taken right from the sender sends the packet till the receiver receives it will be the end-to-end latency.

$$Latency = \sum_{i=1,n} Arrival_{i,n} - \frac{Sent}{\sum Connected} \quad (4)$$

5.2.2 Lifetime of the Network

The network time refers to the duration, measured in seconds, during which the network actively manages the communication channel to guarantee the successful delivery of each packet to its intended destination node.

5.3 Experimental results

Table 3 shows the latency achieved in WSN with different number of sensor nodes and with different weightage of sinkhole nodes.

Table 3: Experimental Results of Latency

Sinkhole Nodes	# Nodes	EM-SD	MRH	LB-IDS	T-IDS	RHS
15%	100	2093	1997	1598	1550	1418
	1000	2266	2054	1722	1574	1559
	10000	2379	2111	1828	1649	1608
20%	100	2020	1817	1409	1418	1335
	1000	2077	1975	1537	1496	1383
	10000	2175	2098	1678	1597	1466
25%	100	1906	1779	1346	1280	1275
	1000	1993	1806	1389	1392	1322
	10000	2110	1904	1439	1443	1354

On interpreting the results tabulated from Table 3 and Figure 4, it is evident that the RHS outperforms the current methods for WSN for 100 nodes in latency. To be precise for 15% of sinkhole nodes, RHS outperforms EM-SD with 32.25%, MRH with 29%, LB-IDS with 11.26% and T-IDS with 8.52%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 33.91%, MRH with 26.53%, LB-IDS with 5.25% and T-IDS with 5.85%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 33.11%, MRH with 28.33%, LB-IDS with 5.27% and T-IDS with 0.39%.

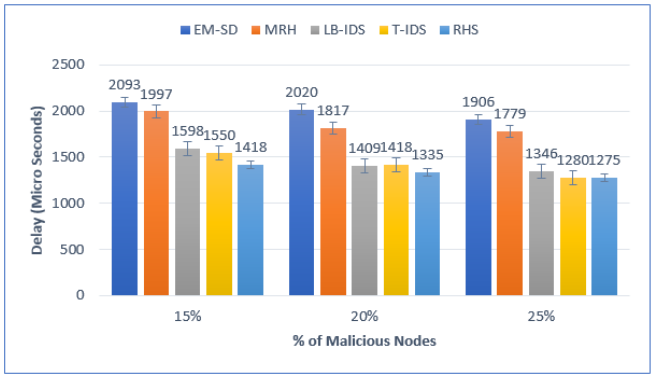

Figure 4: Latency with 100 nodes WSN network

On interpreting the results tabulated from Table 3 and Figure 5, it is evident that the RHS outperforms the current methods for WSN for 1000 nodes in latency. To be precise for 15% of sinkhole nodes, RHS outperforms EM-SD with 31.2%, MRH with 24.1%, LB-IDS with 9.47% and T-IDS with 0.95%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 33.41%, MRH with 29.97%, LB-IDS with 10.02% and T-IDS with 7.55%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 33.67%, MRH with 26.8%, LB-IDS with 4.82% and T-IDS with 5.03%.

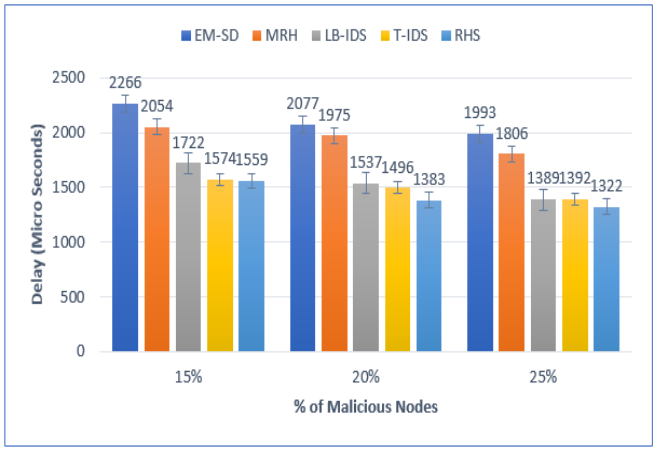

Figure 5: Latency with 1000 nodes WSN network

On interpreting the results tabulated from Table 3 and Figure 6, it is evident that the RHS outperforms the current methods for WSN for 10000 nodes in latency. To be precise for 15% of sinkhole nodes, RHS outperforms EM-SD with 32.41%, MRH with 23.83%, LB-IDS with 12.04% and T-IDS with 2.49%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 32.6%, MRH with

30.12%, LB-IDS with 12.63% and T-IDS with 8.2%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 35.83%, MRH with 28.89%, LB-IDS with 5.91% and T-IDS with 6.17%.

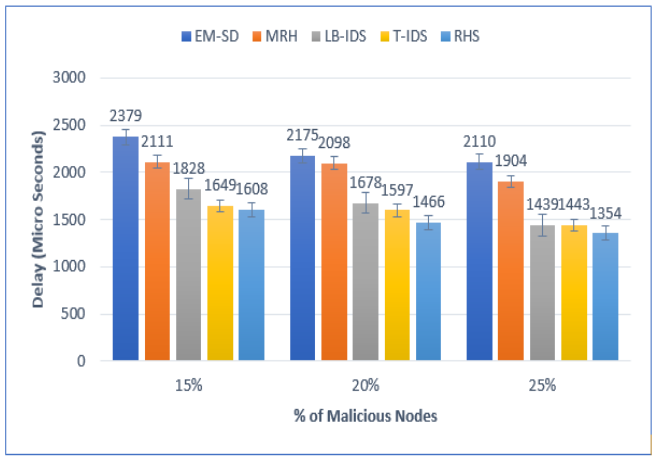

Figure 6: Latency with 10000 nodes WSN network

Table 4: Experimental Results of network lifetime

Sinkhole Nodes	# Nodes	EM-SD	MRH	LB-IDS	T-IDS	RHS
15%	100	168.22	166.41	166.44	171.95	174.98
	1000	140.48	154.82	154.32	164.43	172.83
	10000	125.21	131.68	134.8	149.26	157.52
20%	100	135.22	135.16	136.92	137.82	140.98
	1000	121.52	133.08	139.09	145.55	150.08
	10000	116.57	125.15	129.57	142.07	146.03
25%	100	122.92	124.88	125.16	123.58	129.20
	1000	118.92	122.87	135.33	139.89	143.29
	10000	108.09	115.69	116.25	136.04	139.20

On interpreting the results tabulated from Table 4 and Figure 7, it is evident that the RHS outperforms the current methods for WSN for 100 nodes in network lifetime. To be precise for 15% of sinkhole nodes, RHS outperforms EM-SD with 3.86%, MRH with 4.9%, LB-IDS with 4.88% and T-IDS with 1.73%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 4.09%, MRH with 4.13%, LB-IDS with 2.88% and T-IDS with 2.24%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 4.86%, MRH with 3.34%, LB-IDS with 3.12% and T-IDS with 4.35%.

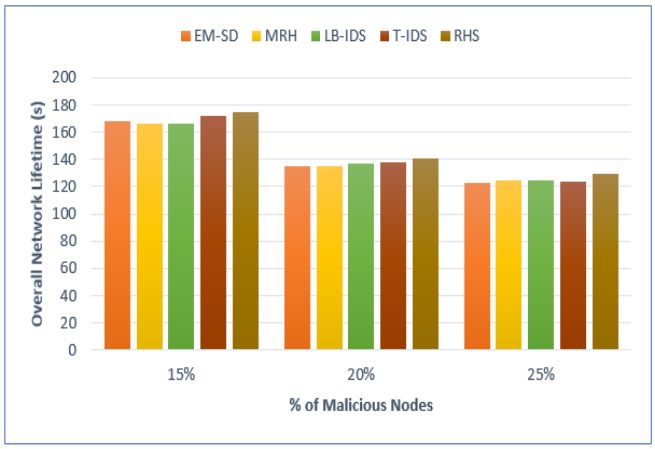

Figure 7: Lifetime of WSN with 100 nodes

On interpreting the results tabulated from Table 3 and Figure 8, it is evident that the RHS outperforms the current methods for WSN for 1000 nodes in network lifetime. To be precise for 15% of sinkhole nodes, RHS outperforms EM-SD with 18.72%, MRH with 10.42%, LB-IDS with 10.71% and T-IDS with 4.86%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 19.03%, MRH with 11.33%, LB-IDS with 7.32% and T-IDS with 3.02%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 17.01%, MRH with 14.25%, LB-IDS with 5.55% and T-IDS with 2.37%.

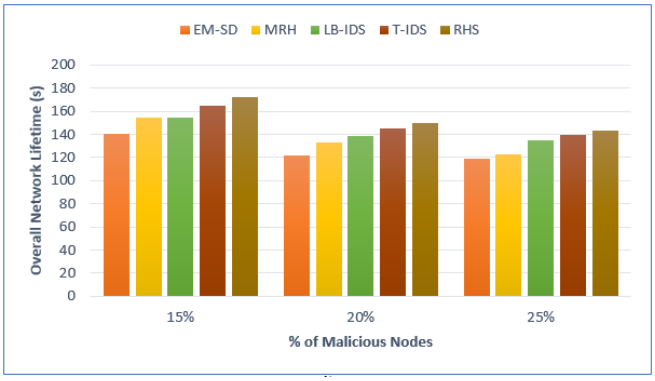

Figure 8: Lifetime of WSN with 1000 nodes

On interpreting the results tabulated from Table 3 and Figure 9, it is evident that the RHS outperforms the current methods for WSN for 100 nodes in network lifetime. To be precise for 15% of sinkhole nodes, RHS outperforms EM-SD with 20.51%, MRH with 16.41%, LB-IDS with 14.42% and T-IDS with 5.25%. For 20% of sinkhole nodes, RHS

outperforms EM-SD with 20.17%, MRH with 14.3%, LB-IDS with 11.27% and T-IDS with 2.71%. For 20% of sinkhole nodes, RHS outperforms EM-SD with 22.35%, MRH with 16.89%, LB-IDS with 16.49% and T-IDS with 2.27%.

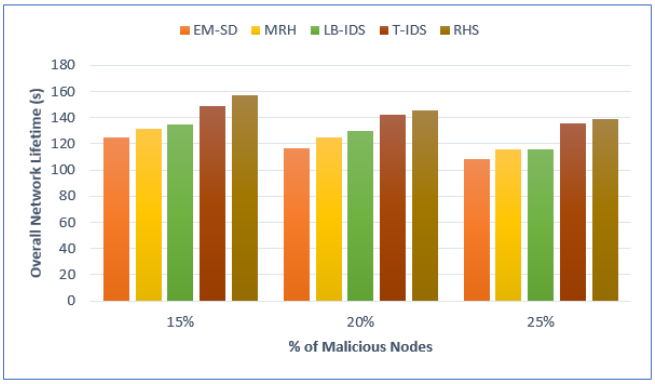

Figure 9: Lifetime of WSN with 10000 nodes

6. CONCLUSION

There will be many good outcomes from using the WSN in various applications. However, WSN isn't without its share of threats, namely those that target the WSN network itself. So, to improve the network's performance, security is essential. The proposed model was developed with an eye towards improving the security of data transmission between WSN nodes in open and remote networks. To strengthen the data transmission module's defence against sinkhole assaults, this model incorporates an RHS optimisation mechanism. The proposed approach offers security for the WSN network to prevent sinkhole attacks. The mathematical study has also shown the RHS model's effectiveness. The proposed RHS model uses either direct or indirect trust to identify a node's neighbour, but it does not use both types of trust to calculate trust. When the degree of the neighbour nodes drops below a certain threshold, the RHS model is also used.

Reference

1. A. Bilal, S. M. N. Hasany, and A. H. Pitafi, "Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices", IET Commun., vol. 16, no. 8, pp. 845–855, May 2022, doi: 10.1049/cmu2.12385.
2. Z. Zhang, S. Liu, Y. Bai, and Y. Zheng, "M optimal routes hops strategy: Detecting sinkhole attacks in wireless sensor networks," Cluster Comput., vol. 22, no. S3, pp. 7677–7685, May 2019, doi: 10.1007/s10586-018-2394- 6.
3. U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, "LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system," J. Comput. Netw. Commun., vol. 2019, pp. 1–13, Jan. 2019, doi: 10.1155/2019/2054298.
4. J. Wang, S. Jiang, and A. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," Sensors, vol. 17, no. 6, p. 1227, May 2017, doi: 10.3390/s17061227
5. Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy, "Detecting sinkhole attack in WSN using hop count", I. J. Computer Network and Information Security, vol. 3, pp. 50-56, Feb 2015.
6. Mamta Patel and Mohammed Bakhtawar Ahmed, "Sinkhole Attack Detection Based On Redundancy Mechanism In Wireless Sensor Networks", Ijsdr, vol. 1, no. 6, 2016.
7. Liping Teng, "SeRA: A Secure Routing algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks", Second International Conference on Computer Modeling and Simulation, 2010.
8. Udaya Suriya Rajkumar and Rajamani Vayanaperumal, "A Leader Based Monitoring Approach For Sinkhole Attack In Wireless Sensor Network", Journal of Computer Science, vol. 9, no. 9, pp. 1106-1116, July 2013.
9. Sina Hamedheidari and Reza Rafeh, "A novel agent-based approach to detect sinkhole attacks in wireless sensor networks", Computer and Security, vol. 37, pp. 1-14, April 2014.
10. N. K. Sreelaja and G. A. Vijayalakshmi Pai, "Swarm intelligence based approach for sinkhole attack detection in wireless sensor

networks", Applied Soft Computing, vol. 19, pp. 68-79, January 2014
11. Mohamed Guerroumi and Abdelouahid Derhab, "Intrusion detection system against SinkHole attack in wireless sensor networks with mobile sink", 12th International Conference on Information Technology, 2015.
12. Vivek Tank and Amit Lathigara, "To Detect and Overcome Sinkhole Attack in Mobile Ad hoc Network", Communications on Applied Electronics, vol. 2, no. 6, pp. 2394-4714, August 2015.
13. Fabrice Le Fessanta, Anthonis Papadimitrioub, Aline Carneiro Vianac, Cigdem Senguld and Esther Palomare, "A Sinkhole Resilient Protocol for Wireless Sensor Networks: Performance and Security Analysis", Computer Applications and Security, May 2011.
14. Leovigildo Sanchez-Casado, Gabriel Macia-Fernandez, Pedro Garcia-Teodoro and Nils Aschenbruck, "Identification of contamination zones for sinkhole detection in MANETs", Journal of Network and Computer Application, vol. 4, pp. 62-77, May 2015.
15. A. Rajasekaran and V. Nagarajan, "Adaptive intelligent hybrid MAC protocol for wireless sensor network", 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 2284-2289, 2016.
16. Almuzaini, K. K., Joshi, S., Ojo, S., Aggarwal, M., Suman, P., Pareek, P. K., & Shukla, P. K. (2023). Optimization of the operational state's routing for mobile wireless sensor networks. Wireless Networks, 1–15
17. Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E., Harold Robinson, Y., & Shanmuganathan, V. (2021). Machine learning based detection and a novel EC-BRTT algorithm based prevention of DoS attacks in wireless sensor networks. Wireless Personal Communications, 1–25
18. Tabbaa, H., Ifzarne, S., & Hafidi, I. (2022). An online ensemble learning model for detecting attacks in wireless sensor networks. arXiv preprint arXiv:2204.13814.
19. Singh, A., Sah, A. K., Singh, A., Jaint, B., & Indu, S. Wormhole Attack Detection in Wireless Sensor Network Using SVM and Delay Per-hop Indication. Data Engineering and Communication Technology, 39
20. Kori, S., Krishnamurthy, G., & Sidnal, N. (2019). Distributed wormhole attack mitigation technique in WSNs. International Journal of Computer Network and Information Security, 11(5), 20–27
21. Gebremariam, G. G., Panda, J., & Indu, S. (2023). Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using Artificial Neural Network. Wireless Communications and Mobile Computing, 2023
22. N.A. Hikal, M.Y. Shams, H. Salem, M.M. Eid "Detection of black-hole attacks in MANET using adaboost support vector machine", Journal of Intelligent & Fuzzy Systems, 41 (1) (2021), pp. 669-682
23. Gopu, A., Thirugnanasambandam, K., R, R. et al. Energy-efficient virtual machine placement in distributed cloud using NSGA-III algorithm. J Cloud Comp 12, 124 (2023). https://doi.org/10.1186/s13677-023-00501-y
24. Thirugnanasambandam, K., Prabu, U., Saravanan, D. et al. Fortified Cuckoo Search Algorithm on training multi-layer perceptron for solving classification problems. Pers Ubiquit Comput 27, 1039–1049 (2023). https://doi.org/10.1007/s00779-023-01716-1
25. N. Pazhaniraja, Shakila Basheer, Kalaipriyan Thirugnanasambandam, Rajakumar Ramalingam, Mamoon Rashid, J. Kalaivani. Multi-objective Boolean grey wolf optimization based decomposition algorithm for high-frequency and high-utility itemset mining[J]. AIMS Mathematics, 2023, 8(8): 18111-18140. doi: 10.3934/math.2023920
26. Thirugnanasambandam, Kalaipriyan, Rajakumar Ramalingam, Divya Mohan, Mamoon Rashid, Kapil Juneja, and Sultan S. Alshamrani. 2022. "Patron–Prophet Artificial Bee Colony Approach for Solving Numerical Continuous Optimization Problems" Axioms

11, no. 10: 523. https://doi.org/10.3390/axioms11100523

27. Thirugnanasambandam, K., Raghav, R.S., Anguraj, D.K. et al. Multi-objective Binary Reinforced Cuckoo Search Algorithm for Solving Connected Coverage target based WSN with Critical Targets. Wireless Pers Commun 121, 2301–2325 (2021). https://doi.org/10.1007/s11277-021-08824-2
28. Thirugnansambandam, Kalaipriyan, Debnath Bhattacharyya, Jaroslav Frnda, Dinesh Kumar Anguraj, and Jan Nedoma. "Augmented node placement model in t-WSN through multi objective approach." Comput. Mater. Contin. CMC Tech Sci. Press 69 (2021): 3629-3644.
29. Attuluri, Sasidhar, and Mona Ramesh. "Multi-objective discrete harmony search algorithm for privacy preservation in cloud data centers." International Journal of Information Technology 15, no. 8 (2023): 3983-3997
30. Attuluri, Sasidhar, Ch Bhupati, Lavu Ramya, Amit Tiwari, Raja Rao Budaraju, and Juan Carlos Cotrina-Aliaga. "Smart investigations into the development of an effective computer-assisted diagnosis system for CT scan brain depictions." SN Computer Science 4, no. 5 (2023): 504.
31. Samha, Amani K., Ghalib H. Alshammri, Sasidhar Attuluri, Preetam Suman, and Arvind Yadav. "AI-Assisted Enhanced Composite Metric-Based Intrusion Detection System for Secured Cyber Internet Security for Next-Generation Wireless Networks." International Journal of Cooperative Information Systems (2024): 2450003.
32. Attuluri, Sasidhar, Mona Ramesh, Raja Rao Budaraju, Sumit Kumar, Jhum Swain, and Jitendra Kurmi. "Original Research Article Defending against phishing attacks in cloud computing using digital watermarking." Journal of Autonomous Intelligence 7, no. 5 (2024).
33. Hazzazi, Mohammad Mazyad, Raja Rao Budaraju, Zaid Bassfar, Ashwag Albakri, and Sanjay Mishra. "A Finite State Machine-Based Improved Cryptographic Technique." Mathematics 11, no. 10 (2023): 2225.
34. Jammalamadaka, Sastry Kodanda Rama, Bhupati Chokara, Sasi Bhanu Jammalamadaka, Balakrishna Kamesh Duvvuri, and Rajarao Budaraju. "Enhancing the Fault Tolerance of a Multi-Layered IoT Network through Rectangular and Interstitial Mesh in the Gateway Layer." Journal of Sensor and Actuator Networks 12, no. 5 (2023): 76.
35. Budaraju, Raja Rao, and O. Sri Nagesh. "Multi-Level Image Thresholding Using Improvised Cuckoo Search Optimization Algorithm." In 2023 3rd International Conference on Intelligent Technologies (CONIT), pp. 1-7. IEEE, 2023.