Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

DETECTION & PREVENTION OF BLACK HOLE ATTACK WITH OPTIMIZATION IN WSN

Bindu Rani[1], Gajender[2]

[1]Assistant Professor,Dept. of Computer Science and Technology Guru Jambheshwar University of Science and Technology Hisar, India

[2]Ph.D. Scholar, Dept. of Computer Science and Technology Guru Jambheshwar University of Science and Technology Hisar, India

ABSTRACT

Wireless sensor network is one of latest research field areas in modern era. This network consists of self-containing nodes that consists of battery for life, antenna for sensing. These nodes are used for data communication and routing to other devices. These sensing nodes have small range for data transmission and less speed. Also, they are vulnerable for attacks by various means. The objective of this study is to propose a methodology for the identification and mitigation of black hole attacks in wireless sensor network (WSN) infrastructures. The manifestation of a black hole attack can lead to a depletion of energy levels and a decline in the overall longevity of the network. After being deployed, specific sensor nodes have the potential to impede the flow of data towards a central sink due to their constrained energy harvesting capabilities. In this work, the main goal is to detect and prevent black hole attack by providing an improved rerouting scheme and also construct a fast tabu search algorithm for computing solutions so that max flow rate may achieve. The proposed technique showed better results as compared to existing techniques.

KEYWORDS- Black Hole, MATLAB, Max Flow, Optimization, Tabu Search, WSN.

I. INTRODUCTION

A wireless sensor network (WSN) is a low-cost network architecture made up of small sensing nodes, or sensors.Each sensor node is an independent entity with sensing, processing, and communication capabilities. Small-scale sensing devices, such as temperature sensors, all the way up to the complex and vital components found in jet engines could benefit from the use of wireless sensor networks (WSNs). The Wireless Sensor Network (WSN) is a system of interconnected

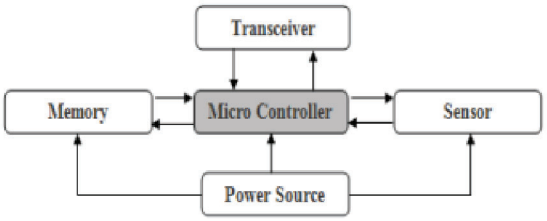
sensors that may function autonomously and cheaply. These devices employ actuators and sensors to reduce human interactions. Air conditioners (AC) and other temperature-regulating smart home gadgets use temperature sensing capabilities to keep rooms at comfortable temperatures. The user can be alerted to any questionable activity via a motion detection system. In a Wireless Sensor Network (WSN), the nodes are inexpensive and simple to set up, allowing for reliable wireless connectivity.

Nevertheless, the sensor nodes may confront restrictions in terms of battery capacity, computational capabilities, and processing capabilities. Traditional encryption methods cannot safeguard these devices. These systems are vulnerable to a variety of dangers due to the fact that they employ wireless communication and have finite resources [I].

A. Overview of WSN

WSN architecture includes (A) source nodes, which are the data producers and are typically sensors used to measure environmental characteristics like temperature and humidity. (B) Sink nodes: those that compile information from source nodes. There are also nodes in between the source and the washbasin, which we'll call "intermediate nodes" (C). Figure 1 shows structure of WSN [II].

Figure 1: Structure of WSN [II]



Source: Compiled by Author

The WSN consists if many sensor nodes for sensing operation. A remote sensor hub, likewise called "bit", comprise of five subsystems:

a. **Sensor Subsystem:** This interface is meant to pick up on physical characteristics like gravity and temperature that exist in the wild. Both exterior and internal sensors are incorporated into the system.
b. **Processing Subsystem:** it is to regulate several processes involved in information management.
c. **Memory Subsystem:** The ability to process and manipulate programming-related data.
d. **Communication Subsystem:** A device, such as a radio antenna, designed to transmit and receive information wirelessly through a remote communication channel.

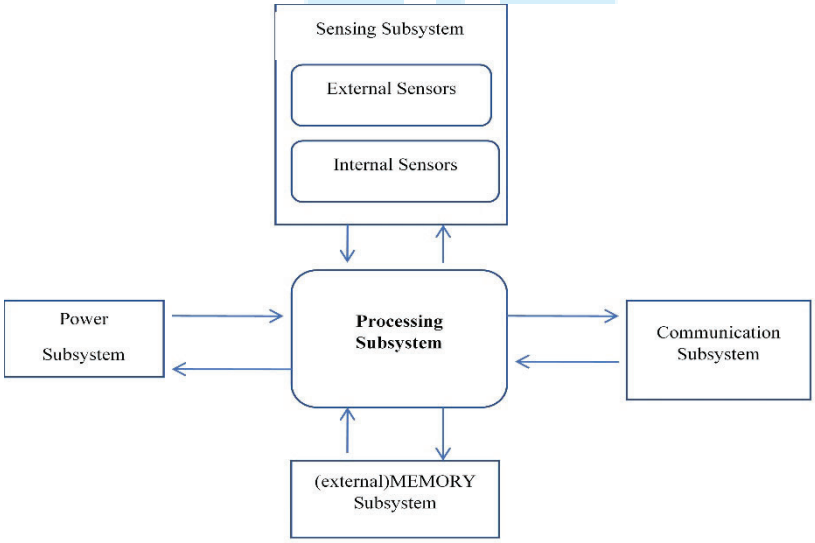
Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

e. **Power Subsystem:** The provision of energy required for the efficient functioning of a central system, analogous to a battery.

The process of generation among the system's centers may involve flooding or directing. While undoubtedly reducing implementation expenses, remote sensor systems possess the capability to continuously adapt to changing circumstances. Adjustment systems have the capability to induce modifications in system topologies or transition the system between different modes of operation. Sensor hub characteristics consist of the following:

- Resource Limitation
- Topology Unknown Prior to Configuration
- Unattended and Unprotected Transmission
- Unreliable Remote Communication

Figure 2: Wireless Sensor System



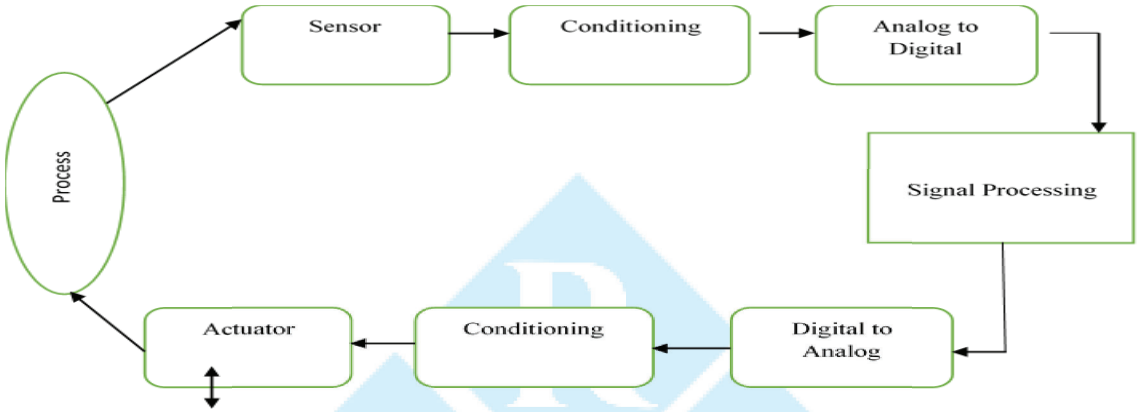
Source: Compiled by Author

B. Sensing and Sensors

The sensors contained within a Wireless Sensor Network (WSN) establish wireless communication among themselves, hence facilitating a significant level of adaptability in network setups. Additionally, the device's location is susceptible to alteration at any given point in time. Furthermore, the sensors include the capacity to establish connectivity with the Internet, utilizing

either wired or wireless methods. In the given scenario, the establishment of a multi-hop ad hoc network by wireless transmission is feasible [III].The device sensor is an entity that can perform sensing duties and also has the capacity for wireless connection and data storage. Also, it can perform some basic mathematics and signal processing functions. The aforementioned equipment is deployed around the area of interest to measure things like seismic activity, humidity, wind speed, and atmospheric pressure, among others [IV].

Figure 3: Data Acquisition and Actuation System



Source: Compiled by Author

C. Challenges and Constraints in WSN

The following are some of the most important factors influencing wireless sensor network design and performance:

- **Energy:** Sensors possess various power requirements. The process of collecting, processing, and transmitting data requires energy. Even when the components of a node, including as the CPU and radio, are not actively engaged in tasks, they still need to be attentive to the medium in order to maintain reliable functioning. Batteries that provide electrical energy must be replaced or recharged once they have been depleted. In certain instances, the ability to recharge or replace batteries may be hindered due to demographic reasons. The primary obstacle faced by the research community in the field of Wireless Sensor Networks (WSNs) is the task of designing, developing, and implementing hardware and software protocols that are capable of achieving energy efficiency [V-VII].
- **Infrastructure-less Communication:** Wireless sensor networks (WSNs) are often designed to function with limited or absent infrastructure. The communication channel between sensor

nodes is subject to a finite set of limitations, resulting in potential challenges such as unreliable communication. However, it has the benefit of widespread dissemination. The aforementioned feature enables the effective use of Wireless Sensor Networks (WSNs) in diverse applications with unique requirements [VIII].

- **Sensor Node Deployment:** There are two broad types of node deployment used in Wireless Sensor Networks (WSNs): manual and random. Sensors are placed by humans using a predetermined method in manual node deployment [IX]. When deployed manually, nodes use a predetermined path to communicate with one another. Ad-hoc substructures are used in random node deployment to put sensor nodes at random inside the sensing area [X]. For instance, take into account scenarios where nodes are deployed arbitrarily employing aero planes for deployment inside the operational region, including difficult and inhospitable places. Carefully planning the deployment process can help meet design goals while minimizing issues like communication and routing bottlenecks inside the network [XI-XII].
- **Coverage:** When referring to the sensing region being monitored by the set of active nodes, the term "coverage" is typically employed. When placed higher, sensors are able to more effectively and comprehensively monitor the designated area. However, connectivity displays how successfully a node communicates with the base station and surrounding nodes. Sensor nodes in the targeted area are well-covered thanks to the network's coverage and connectivity. They guarantee communication between all nodes after deployment. Different WSN protocols try to figure out how few sensors are needed to maintain a functional network. In order to collect all of the data in the sensing region, it is necessary to connect all of the nodes there either directly or via relay nodes [XIII].

II. LITERATURE REVIEW

- In [XIV] author suggested the utilization of anomaly-based hierarchical intrusion detection is elucidated as a method for the identification and mitigation of black hole attacks in wireless sensor networks (WSN). The issue of security in Wireless Sensor Networks (WSNs) is a significant one. The system implemented modifications to its active trust model and data routing strategy, which involved the integration of a data type checking method during the routing process. This enhancement aimed to detect and mitigate black hole attacks. A modified iteration of the low-energy adaptive clustering hierarchy (LEACH) protocol is employed to simulate the black hole attack on wireless sensor networks (WSNs).

- In [XV] author proposed method strongly depends on the accuracy of information gained from RREP packets, which are not studied in this work due to the lack of investigation of attacks based on packet alteration. The LEACH approach is capable of identifying passive black-hole attacks by classifying a cluster head (CH) that exhibits infrequent data transmission as a black-hole node with a relatively low likelihood of selection. RREQ and RREP refer to two distinct forms of collaborative sinkholes that act in tandem to produce counterfeit requests, posing potential challenges in their identification. Future work will widen this investigation to include numerous collaborating sinkhole nodes, and various assaults will be explored and tried out utilizing the proposed strategy.
- In [XVI] author suggests a different tactic of deploying IDSs to protect a WSN. We examined three routing protocols using the NS2.35 simulator to see how they fared against black hole assaults in the WSN model: AODV, AODV under Hacker Node (HNAODV), and the proposed solution (IDSHNAODV).
- In [XVII] author presented maximal destination sequence number is estimated by employing linear regression technique. The effectiveness of conventional, black-hole-based, and black-hole-detection routing systems are compared. The simulation findings show that the deployed technique increases QoS despite a black hole assault, which improves network performance.
- In[XVIII] Bayesian theory and a deep recurrent neural network (DRNN) were used in the proposed approach to detect malicious nodes in a network and the times it took to uncover their routes. Once harmful nodes have been removed from the network, the grasshopper optimisation algorithm (GOA) determines the optimal path to the objective. An analysis of the obtained data demonstrates that the proposed strategy increases throughput by lowering the delay and increasing the average residual energy.
- In [XIX] author presented the research which aims to evaluate the performance of the Ad hoc On-Demand Distance Vector (AODV) protocol in both static and mobile scenarios. A comparison analysis is conducted to assess the overall impact of the blackhole node inside the network.
- In [XX] The authors introduce a novel framework called POS-MKC to improve attack detection accuracy and reduce computing complexity in wireless sensor networks (WSNs). The architectural framework under consideration, known as the Physiological Data Collection (PDC), Proportional Overlapping Score (POS), and machine learning approach, consists of three distinct operations. The PDC module initially collects the relevant characteristics in

accordance with the training dataset consists of recorded values of physiological parameters. The POS model is employed for the purpose of data preprocessing and to the aim of this task is to decrease the quantity of attributes present in the provided training dataset. As a result, this subsequently reduces the complexity involved in identifying and preventing assaults.

- In [XXI] author proposed approach that utilises a detection technique that leads to a rise in energy consumption, hence prolonging the lifespan of networks. The previous methodology demonstrates a notable enhancement of 19.51% in the rate of packet delivery, a substantial decrease of 53.3% in energy consumption, and a significant extension of 43.3% in the lifespan of the network.
- In [XXII] The author proposed a defensive technique that makes use of swarm intelligence to improve energy efficiency. Through simulation using NS2, we were able to verify that the proposed methodology works. The experimental findings validate the superior performance of the suggested technique in comparison to the state-of-the-art approaches in terms of packet delivery ratio, average end-to-end delay, and throughput.
- In[XXIII] author proposes evaluating packet delivery ratio, throughput, and packet drop as metrics by which to gauge RTSSM's success in mitigating Selective Forwarding Attacks (SFAs) and Black Hole Attacks (BHAs). The experimental findings provide evidence for the effectiveness of the suggested methodology and its ability to improve the durability of the network.
- In [XXIV] author presented a new clustering methodology called Dynamic Compromise Black hole attack Detection (DCBD). The primary aim of this strategy is to optimize network performance by increasing throughput, minimising latency, and enhancing packet delivery ratio, all while taking into account the selection process of cluster heads. The timely identification of black hole nodes holds significant significance in addressing network disturbances. The DCBD strategy, as presented, utilizes a direct and unique approach to detect black hole nodes in an AODV-based Cluster Wireless Sensor Network (WSN) at an early stage. The study determined the mean values for the evaluated metrics, specifically throughput (3918749.8 kbps), latency (186.6 ms), and packet delivery ratio (96.8%).
- In [XXV] author proposed methodology exhibits a notable enhancement in lifespan when compared to LEACH, LEACH-C, and TS-LEACH, exhibiting an approximately threefold improvement in efficacy. The proposed methodology demonstrates a fourfold enhancement in throughput when compared to both LEACH and LEACH-C, and a 77.8% improvement

when compared to TS-LEACH. The technique being discussed in this context also serves the purpose of identifying and mitigating the black hole attack, hence ensuring the security of data aggregation.

III. PROPOSED WORK

As remote specially appointed Without protection from the ground up, systems are extremely vulnerable. The Black Hole attack is one example. A malicious hub that is in operation for financial gain will absorb all data packets. A noxious hub in the system utilizes the vulnerabilities of the course disclosure parcels of the on-interest conventions, for example, AODV. In course disclosure procedure of AODV convention, middle of the road hubs is dependable to locate a crisp way to the goal, sending revelation bundles to the neighbor hubs. Pernicious hubs don't utilize this procedure and rather, they promptly react to the source hub with false data as if it has new enough way to the goal. In this manner source hub sends its information parcels by means of the malignant hub to the goal accepting it is a genuine way. Dark Hole assault may happen because of a pernicious hub which is purposely getting out of hand, just as a harmed hub interface. Regardless, hubs in the system will always endeavor to discover a course for the goal, which causes the hub to expend its battery notwithstanding losing parcels. In our examination, it mimics the Black Hole assault in remote impromptu systems and gives a way to deal with distinguish and forestall this assault in the system.

A. Fault Detection in Network

The identification of an unexpected failure inside the system framework is a critical aspect of fault location, which is the primary focus of the board. The identification of disappointment can be categorised under two approaches: unified and dispersed methodologies. In other words, it is not advisable to teach the control focus unless a system deficiency has occurred.

B. Node Self-Detection

This study proposes a self-recognition paradigm that utilises both hardware and software interfaces to detect and diagnose malfunctions in the physical components of a sensor hub. The hub's self-recognition of disappointment is evident through its observation of the parallel outputs from its sensors, which are compared to pre-defined models of problematic situations. In conventions for information dissemination, which include the transmission of large amounts of information to the entire or a portion of the network, the destination nodes are responsible for identifying the missing packet or the range of missing packets. In the context of data collection

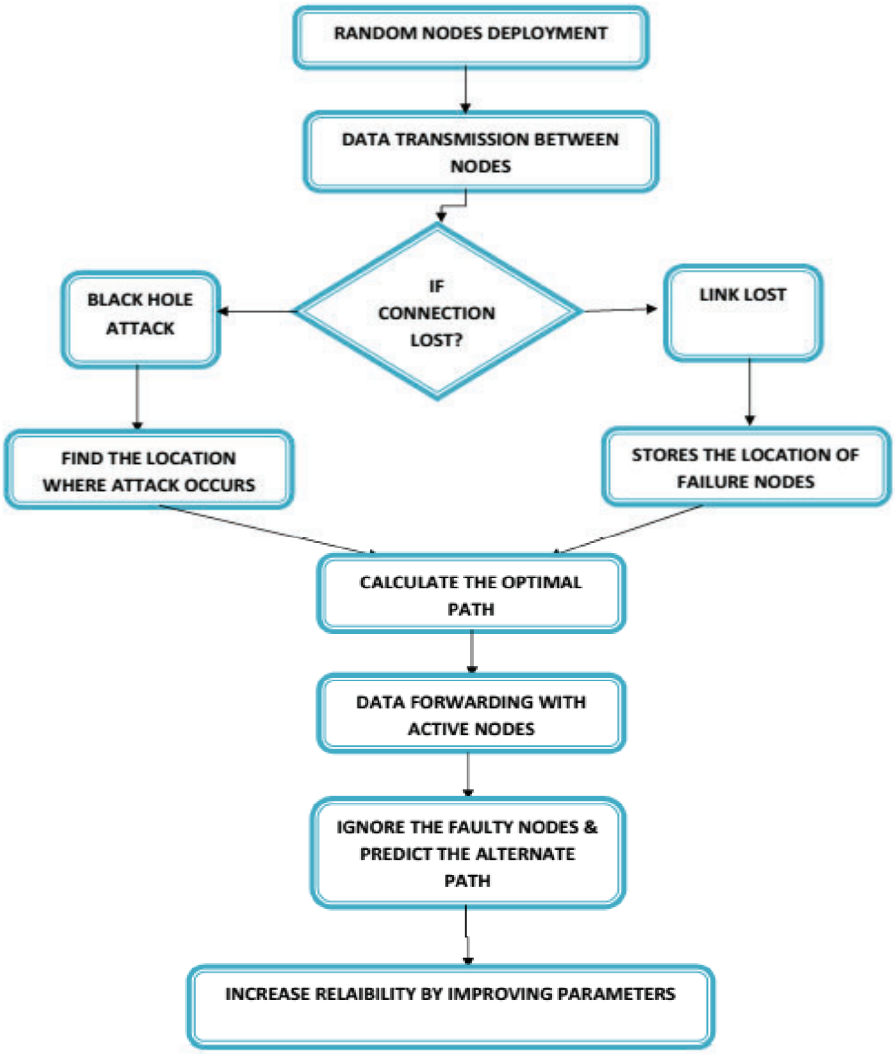
protocols, the detection of individual packet losses is infrequent due to the abundance of sensor hubs and the resulting large volume of reported sensing values. Instead, a comprehensive indicator such as bundle delivery rate or issue rate is taken into consideration. When a particular threshold is exceeded, communication is deemed flawed and appropriate remedial actions are taken. In addition to the occurrence of bundle misfortune, certain metrics such as incursion, delay, or the absence of regular network traffic are also regarded as indicators of defects.

C. Neighbour Coordination

The insufficiency in resource allocation management is demonstrated by the dissatisfaction arising from the utilisation of neighbour coordination for resource location. Hubs actively participate in cooperative endeavours with adjacent nodes in order to detect and distinguish system dysfunctions, such as the existence of a possibly dubious hub. This feature enables the decentralised indicative structure to effectively handle larger and denser sets of sensors as required. The optimal endeavour involves employing a versatile investigative methodology that prioritises the utilisation of the most efficient search methods currently accessible. The concept of the ideal defect in the context of Search refers to a meta-heuristic methodology that aids in the systematic examination of the solution space beyond local optimality through the utilisation of a neighbourhood heuristic search strategy. The utilisation of versatile memory in Optimal fault dealing with Search is a key component that enhances the adaptability of its search behaviour. One notable observation is that these norms can sometimes be sufficiently rigorous to generate effective critical thinking. In a broad range of problem-solving contexts, however, the strategic use of memory can provide significant variations in the ability to effectively address challenges. Unadulterated and hybrid Optimal deficiency handling Search methodologies have achieved remarkable achievements in the realm of finding improved solutions for issues in production planning and scheduling, resource allocation, network design, routing, financial analysis, telecommunications, portfolio planning, supply chain management, agent-based modelling, business process design, forecasting, artificial intelligence, data mining, bio-computation, molecular structure, forest management, and resource planning, among various other domains.

Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

Figure 4: Proposed Flow Chart of System

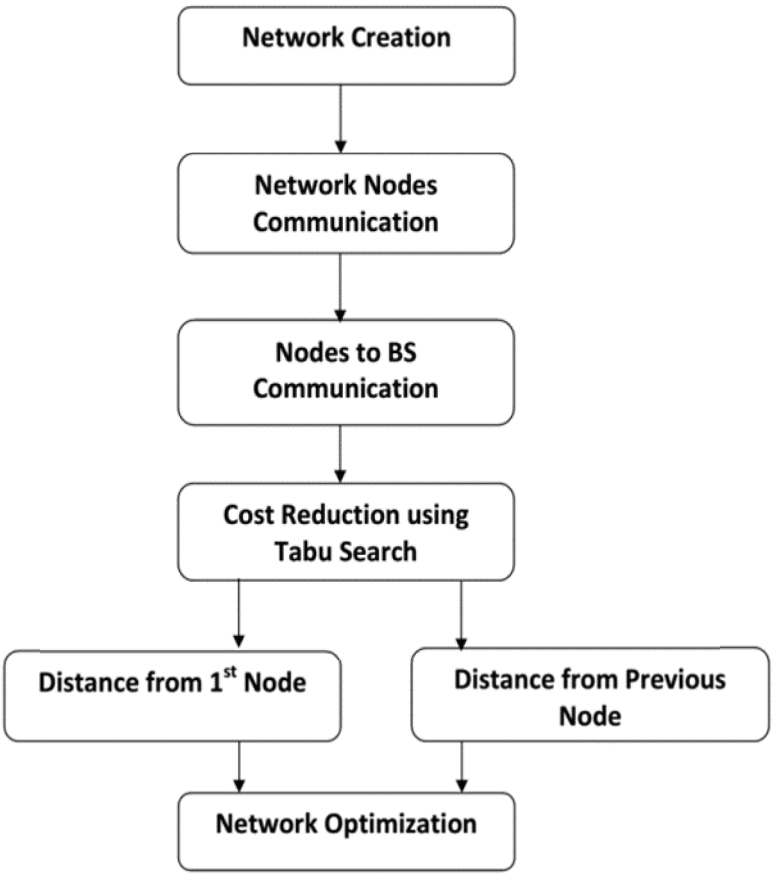


Source: Compiled by Author

The fundamental component of the conventional approach is the usage of the best improvement neighbourhood search, however there are many more steps involved in determining which paths to take in order to use Tabu search as a flexible search algorithm. Taboo pursuit prevents the search process from getting stuck at the local optimum by tolerating temporary degradation of the arrangement. Notably, researchers have found that these norms can sometimes have enough influence to independently generate successful problem-solving behaviour with only a moderate dependence on memory. In many problem-solving contexts, however, the strategic utilisation of memory can yield significant improvements in problem-solving abilities. The unadulterated and

half and half Tabu Search methodologies have achieved notable advancements in the field of problem-solving, specifically in the domains of production scheduling and booking, resource allocation, network design, routing, financial analysis, telecommunications, portfolio planning, supply chain management, agent-based modelling, business process design, forecasting, artificial intelligence, data mining, bio-computation, molecular structure, forest management, and resource plan.

Figure 5: Proposed Steps of System using Tabu Search



Source: Compiled by Author

The TS system is quickly turning into the strategy for decision for structuring arrangement strategies for hard combinatorial enhancement issues. Across the board triumphs in reasonable utilizations of advancement have prodded a quick development of the technique as a method for distinguishing amazingly brilliant arrangements effectively. TS strategies have additionally been utilized to make half and half methodology with other heuristic and algorithmic techniques, to give improved answers for issues.

Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

D. Proposed Steps of System

a. *Connect to MATLAB.*
b. *Generate M randomly.*
c. *Find Node a , Node b.*
d. *Calculate*
e. *dist=* $\sqrt{((Node\ a\ (1) - Node\ a\ (2))^2 + ((Node\ b\ (1) - Node\ b\ (2))^2}$
f. *If (Black hole attack) then*
g. *If (link fail) then*
h. *Find that Node a & Node b where connection lost End*
i. *If (node Fail) then*
j. *Store the FNode a &FNode b*
k. *End*
l. *Find the most direct route between any two points.*
m. *If (fail node in path occurs) then*
n. *coordi1=s_coordi;*
o. *while coordi1(1)~=r_coordi(1) && coordi1(2)~=r_coordi(2)*
p. *nn=infotransfer(coordi1,r_coor,Node a ,Node b);*
q. *[coordi2]=check_avg(coordi 2,coordi 1,Node a ,Node b);*
r. *for i=fni*
s. *if coordi2(1)==node a (i)&& coordi2(2)==node b(i)*
t. *Estimates the Next Best Shortest Route*
u. *End*
v. Improve Availability by lowering the likelihood of blocks

E. Key Parameters of System

Although sensor systems exhibit many similarities to other appropriated systems, they are susceptible to a variety of distinct challenges and requirements. The aforementioned constraints influence the design of a WSN, necessitating distinct protocols and calculations compared to those found in other distributed frameworks. This section illustrates the most crucial elements of a WSN's plan requirements.

a. Energy: Hubs in a system consume a lot of power because of the energy transferred to and from them.

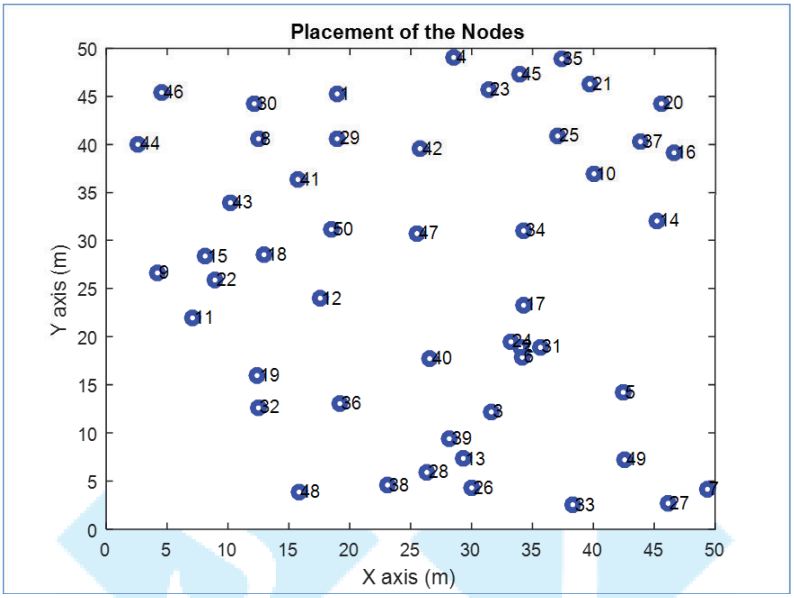
b. Self-Management: organize, cooperate, and form alliances with various centers; adapt to setbacks, planetary shifts, and ecological developments; and all this without human intervention.

Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

IV. RESULTS & DISCUSSION

The entire WSN proposal outcomes are documented here. In this study, a more efficient system is proposed that generates maximum flow while using less power. We need to control the most essential factors, which are the dispersal energy levels in the correspondence method. The situation's usage results are shown below. In this work, we consider the configuration of 50 hubs shown in fig. 6, and the results that follow will provide information about the distribution of sensor hubs across a given region.

Figure 6: Placement of Nodes in Network



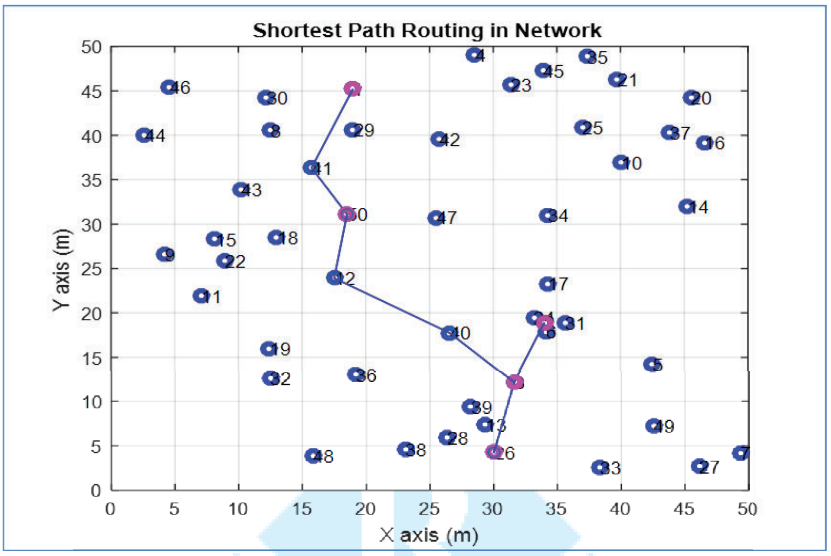
Source: Compiled by Author

A unique sensor ID is displayed alongside each sensor. No two hubs cover one another. In this case, we choose a 50 by 50 metre area for the distribution of sensor nodes. However, we can effectively change it for a large number of hubs (as shown in fig. 6). The existence of a head CH proves that all hubs used for detection are directly related to the head. Every hub is in open communication with the central hub. The location and types of nodes can be used together with class-based care to reach every node. Through restricted flooding, the convention establishes a connection that is then used to discover every possible path between any given source and any given destination, together with an estimate of the associated cost, and finally to construct the directing tables. By selecting adjacent hubs in a cost-effective manner, a sending table is constructed, and the surprisingly expensive paths are abandoned. Information is then sent to its final destination via sending tables, with the likelihood of delivery inversely proportional to the

Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

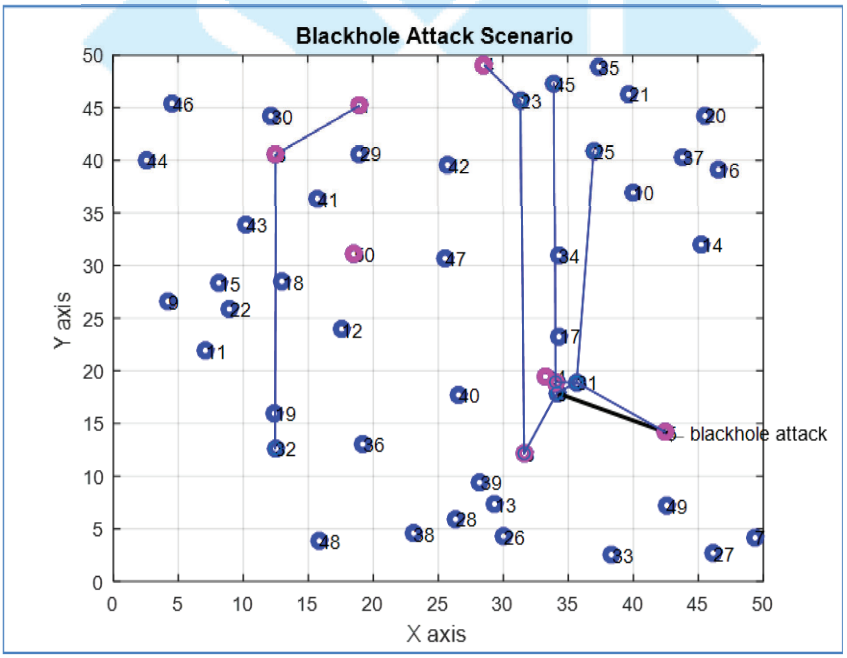
cost of the hub. Distances from both the initial hub and previous hubs are calculated. All gaps are mentally filed away. Figures 8 and 9 display the results.

Figure 7: Shortest Routing using Path Algorithm with Multiple Senders



Source: Compiled by Author

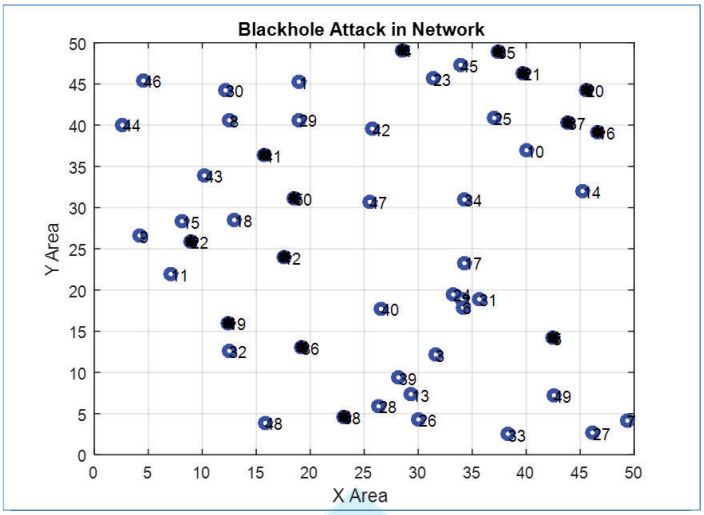
Figure 8: Black hole Scenario in Network



Source: Compiled by Author

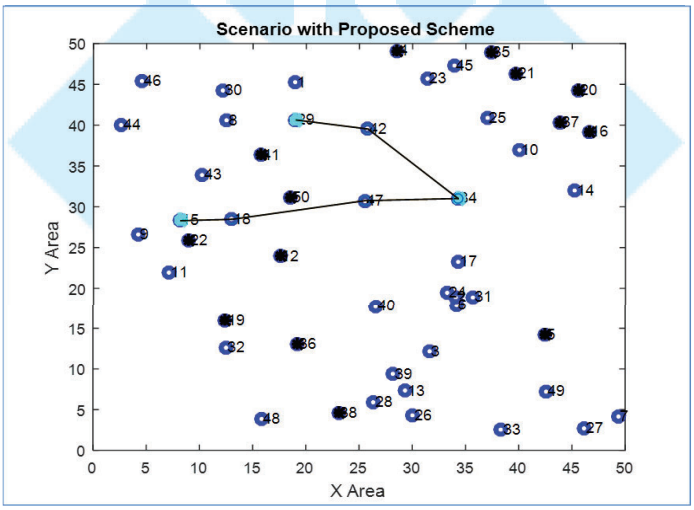
Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

Figure 9: Detection of Nodes with Black hole Attack in Network



Source: Compiled by Author

Figure 10: Proposed Routing Scheme with Black hole Attack Prevention in Network

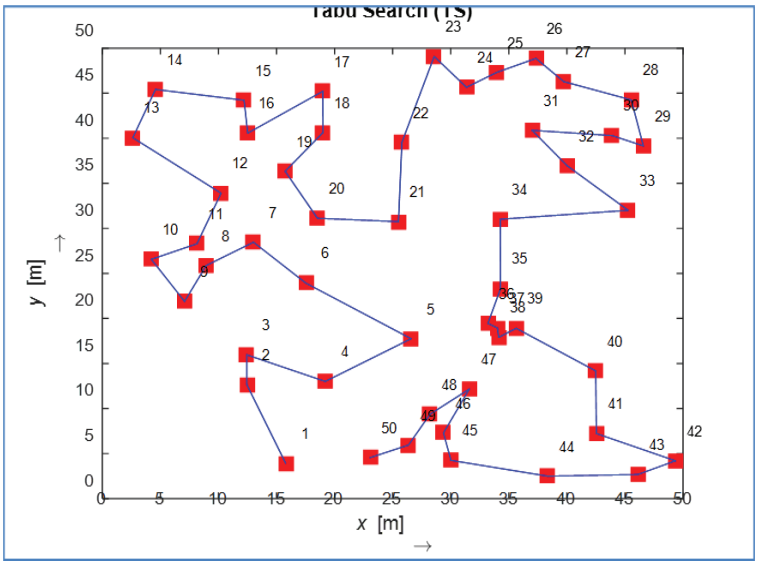


Source: Compiled by Author

Load value is used as the metric by which network costs are calculated. Lower the cost means network is optimised and performance is better. As seen in fig. 11, Tabu search optimises the network by recalculating the distance between nodes and by changing the positions of existing nodes

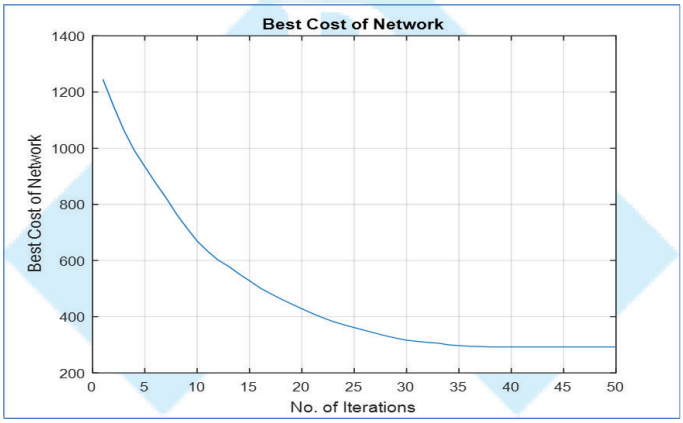
Sudarshan Research Journal
Volume – 1, Issue - 6, October-2023
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

Figure 11: Optimized Output using Tabu Search



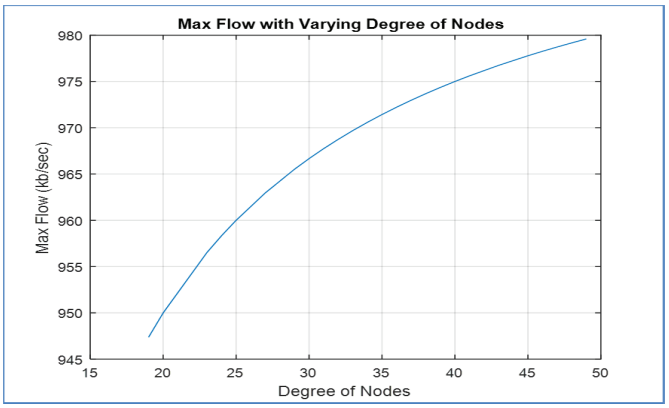
Source: Compiled by Author

Figure 12: Optimized Network Cost in System



Source: Compiled by Author

Figure 13: Max Flow Output in Network



Source: Compiled by Author

The greatest stream issue is personally identified with the base cut issue. A cut is insect set of coordinated circular segments containing in any event one curve in each way from the starting point hub to the goal hub. Lower the cost methods system is enhanced and execution is better as appeared Table 1. To start with, if there is just one course from a source to the sink, the stream is constrained by the hub with the base vitality. Conversely, as we increment δ, a source has more neighbours with the end goal that the quantity of courses from sources to the sink increments and in this manner more information can be sent. Additionally, according to requirement, the accessible vitality of a hub decides the measure of information it can advance. A moderate hub may not deplete its vitality when δ is low.

Table.1: Network Cost of System (For 35 Nodes)

Iterations	Network Cost
1	810
10	600
10	404
15	320
20	276
25	270
30	267
35	267

Source: Compiled by Author

V. CONCLUSION

When the energy in the central ring of hubs surrounding the sink hub runs out, the system fails because the sink hub is cut off from the rest of the functional hubs. This work proposes a location and counteractive action of dark opening fault in WSN framework. This dark gap fault causes connect disappointment and hub disappointment in the framework. In this work, the primary objective is to develop a quick tabu quest calculation for processing arrangements with the goal that maximum stream rate may accomplish. In this work, it gives ideal expense in system utilizing tabu calculation. The fundamental goal is to amplify the stream rate at least one sinks and advance the system cost. The consequences of max stream versus level of hubs and max stream versus no. of hubs are displayed and demonstrate better when contrasted with existing one. It researches the issue of redesigning sensor hubs to augment the stream rate. It utilizes the idea of way and Tabu to examine the exhibition of framework. To begin with, if there is just one course from a source to the sink, the stream is constrained by the hub with the base vitality. Interestingly, as it increments δ, a source has more neighbors to such an extent that the quantity of courses from sources to the sink increments and along these lines more information can be sent.

VI. REFERENCES

I. Abdalkafor, A. S., & Aliesawi, S. A. (2022, October). Data aggregation techniques in wireless sensors networks (WSNs): Taxonomy and an accurate literature survey. In *AIP Conference Proceedings* (Vol. 2400, No. 1). AIP Publishing.

II. AKOURMIS, S., Fakhri, Y., & Rahmani, M. D. (2023). Protecting AODV Protocol from Black Hole Attack in WSN.

III. Alkanhel, R., El-kenawy, E. S. M., Abdelhamid, A. A., Ibrahim, A., Abotaleb, M., & Khafaga, D. S. (2023). Dipper Throated Optimization for Detecting Black-Hole Attacks inMANETs. *Computers, Materials & Continua*, *75*(1).

IV. Anisi, M. H., Abdullah, A. H., & Abd Razak, S. (2011). Energy-efficient data collection in wireless sensor networks. *Wireless Sensor Network*, *3*(10), 329-333.

V. Anitha, A., & Mythili, S. Robust Tristate Security Mechanism to Protect Against Selective Forwarding Attack and Black Hole Attack in Intra-Cluster Multi-Hop Communication.

VI. Arunmozhi, S. A., Rajeswari, S., & Venkataramani, Y. (2023). Swarm Intelligence Based Routing with Black Hole Attack Detection inMANET. *Computer Systems Science & Engineering*, *44*(3).

VII. Ashraf, H., Khan, F., Ihsan, U., Al-Quayed, F., Jhanjhi, N. Z., & Humayun, M. (2023, March). MABPD: Mobile Agent-Based Prevention and Black Hole Attack Detection in Wireless Sensor Networks. In *2023 International Conference on Business Analytics for Technology and Security (ICBATS)* (pp. 1-11). IEEE.

VIII. Cheena, K., Amgoth, T., & Shankar, G. (2023). Deep Learning-Based Black Hole Detection Model for WSN in Smart Grid. In *Computational Intelligence: Select Proceedings of InCITe 2022* (pp. 19-30). Singapore: Springer Nature Singapore.

IX. Dargie, W., & Poellabauer, C. (2010). *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons.

X. El Khediri, S. (2022). Wireless sensor networks: a survey, categorization, main issues, and future orientations for clustering protocols. *Computing*, *104*(8), 1775-1837.

XI. El Khediri, S., Thaljaoui, A., Dallali, A., Harakti, S., & Kachouri, A. (2018, April). A novel connectivity algorithm based on shortest path for wireless sensor networks. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

XII. Guiloufi, A. B. F., El Khediri, S., Nasri, N., & Kachouri, A. (2014, December). EDD clustering algorithm for wireless sensor networks. In *CS IT conference proceedings* (Vol. 4, No. 13).

XIII. Hassan, E. S. (2023). Energy-Efficient Resource Allocation Algorithm for CR-WSN-Based Smart Irrigation System under Realistic Scenarios. *Agriculture*, *13*(6), 1149.

XIV. Kumar, V. N., Srisuma, V., Mubeen, S., Mahwish, A., Afrin, N., Jagannadham, D. B. V., & Narasimharao, J. (2023, March). Anomaly-Based Hierarchical Intrusion Detection for Black Hole Attack Detection and Prevention in WSN. In *Proceedings of Fourth International Conference on Computer and Communication Technologies: IC3T 2022* (pp. 319-327). Singapore: Springer Nature Singapore.

XV. Kumar, V. N., Srisuma, V., Mubeen, S., Mahwish, A., Afrin, N., Jagannadham, D. B. V., & Narasimharao, J. (2023, March). Anomaly-Based Hierarchical Intrusion Detection for Black Hole Attack Detection and Prevention in WSN. In *Proceedings of Fourth International Conference on Computer and Communication Technologies: IC3T 2022* (pp. 319-327). Singapore: Springer Nature Singapore.

XVI. Pradhan, K. M., & Shinde, M. A. (2012). Wireless Sensor Network: An Overview. *International Journal of Advanced Research in Computer Science and Electronics Engineering*, *1*(6), 146-155.

XVII. Pullagura, J. R., & Dhulipalla, V. R. (2023). Black-hole attack and counter measure in ad hoc networks using traditional routing optimization. *Concurrency and Computation: Practice and Experience*, *35*(9), e7643.

XVIII. Rani, B., Sehrawat, H., &Siwach, V. (2020). Blackhole attack in wireless sensor network (WSN) using AODV protocol. *International Journal Of Advanced Science and Technology (2005-4238) Volume*.

XIX. Shanmugapriya, S., & Shanmugapriya, N. (2023, September). DCBD: An Efficient Design of Dynamic Compromise Black Hole Attack Detection (DCBD) in WSN. In *2023 International Conference on Network, Multimedia and Information Technology (NMITCON)* (pp. 1-7). IEEE.

XX. Sharma, S., Bansal, R. K., & Bansal, S. (2013, December). Issues and challenges in wireless sensor networks. In *2013 international conference on machine intelligence and research advancement* (pp. 58-62). IEEE.

XXI. Sharma, S., Bansal, R. K., & Bansal, S. (2013, December). Issues and challenges in wireless sensor networks. In *2013 international conference on machine intelligence and research advancement* (pp. 58-62). IEEE.

XXII. Shinde, A., & Bichkar, R. S. (2023, August). Energy Efficient Cluster Based Secured Data Aggregation Using Genetic Algorithm for WSN. In *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)* (pp. 1-6). IEEE.

XXIII. Wadhaj, I., Thomson, C., & Ghaleb, B. (2022). Wireless sensor networks (WSN) in oil and gas industry: Applications, requirements and existing solutions. In *Proceedings of International Conference on Emerging Technologies and Intelligent Systems: ICETIS 2021 Volume 2* (pp. 547-563). Springer International Publishing.

XXIV. Wang, T., Zhang, G., Yang, X., & Vajdi, A. (2018). Genetic algorithm for energy-efficient clustering and routing in wireless sensor networks. *Journal of Systems and Software*, *146*, 196-214.

XXV. Webber, J. L., Arafa, A., Mehbodniya, A., Karupusamy, S., Shah, B., Dahiya, A. K., & Kanani, P. (2023). An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks. *Computers and Electrical Engineering*, *111*, 108964.