Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 8
August 2023

EFGA-DoSLD: Energy Efficient Denial of Service attack Detection in WSN

Rahul Shingare [1] Dr. Md. Vaseem Naiyer[2]

[1] Research Scholar, Computer Science and Engineering Department, Madhyanchal Professional University Ratibad, Bhopal, M.P., INDIA
Email: rahulshingare20@gmail.com
[2] Computer Science and Engineering Department, Madhyanchal Professional University Ratibad, Bhopal, M.P., INDIA
Email: vaseemnaiyer@gmail.com

Abstract

Sensors, computation, and wireless communication on a single WSN device is a huge accomplishment. WSNs are distinguished by their energy restrictions and application-specific features. New communication protocols using WSN capabilities are created to suit a wide variety of applications. WSN. DoS attacks prevent battery-powered sensor nodes from sleeping, affecting network performance. Existing DoSL attack detection technologies are inefficient and waste energy. This paper proposes EFGA DoSLD, a genetic algorithm-based denial-of-sleep attack detection algorithm (EFGA DoSLD). It also reduces energy utilisation in wireless sensor networks by eliminating routing and trust concerns. The protocol relies on TAGA, an adaptive genetic algorithm. TAGA (Trust based adaptive genetic algorithm) derives comprehensive trust values from the nodes' direct and indirect trust values, which account for volatilization and adaptive penalty factors. The suggested solution uses the base station's modified-RSA (MRSA) algorithm for key creation and distribution (BS). First, sensor nodes employ AODV to identify a reliable relay node before sending messages. The crossover and mutation mechanisms allow for the discovery and study of new attack techniques. When an attacker node is detected, the Blocking Sensor (BS) notifies all other sensor nodes in the network. This approach outperforms X-MAC, ZKP, and TE2P.

Keywords: EFGA (Energy efficient Genetic algorithm), DoSLD (Denial of sleep attack), TAGA (Trust based adaptive genetic algorithm)

1. Introduction

Wireless sensor networks combine sensors, computers, and wireless communication in a tiny device (WSNs). WSNs differ from regular networks due to energy and application limits. Current DoSL attack detection systems are inefficient and waste energy. This may be illustrated by looking at how battery-constrained and interference-limited WSN deployments are more complicated when considering the influence of different network sizes on a certain network architecture. NL (network lifetime) is a significant metric for measuring WSN network performance and service quality. Since the sensor nodes in the WSN have a limited battery life, the NL frequently relies on those devices. Recharging or replacing the batteries of sensors in real-world applications, such as sensors buried in glaciers to monitor climate change, is often impracticable or expensive. As a result, the WSN's individual sensors' battery life limits the NL's ability to do its tasks. An adaptive method for balancing transmits rate and power usage has been proposed as a result of this research Physical layer factors, such as the amount of processing power dissipated by each sensor, were examined in fixed-rate systems. Few of the nodes in the network were capable of generating data, while the remainder served as relays, or "sink nodes," that carried data from one place in the network to another. String-topology transmission is the term for this method (DN).so long as connectivity is maintained data can only be sent to the sink node. Figure 1 shows the how the wireless sensor network communication take place.

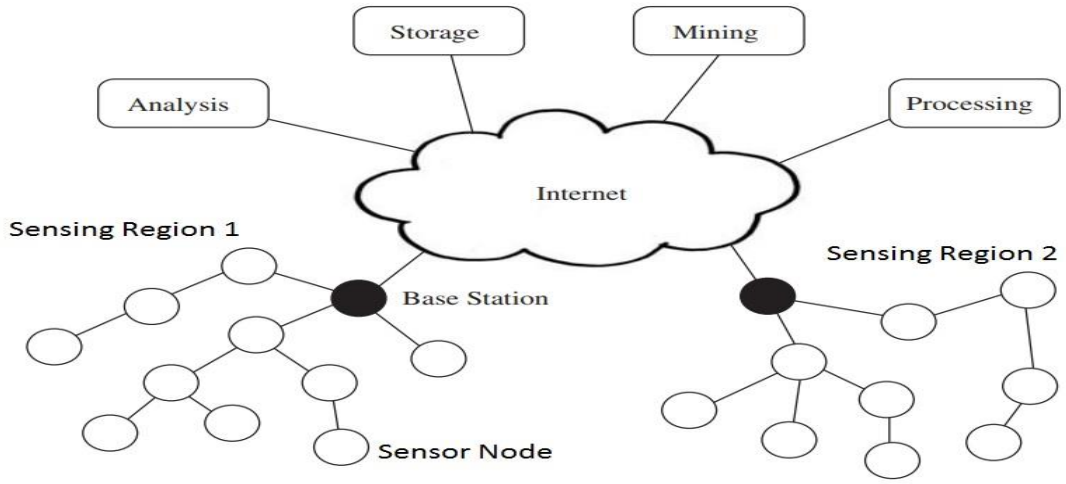

Figure 1: Wireless Sensor Network

2. Literature review

M. Dhami, V. Garg, and N. S. Randhawa proposed VGDRA, an energy-efficient evolutionary algorithm for wireless sensor networks. The dynamic approach is more energy-efficient than LEACH. It gives better results in fewer loops than previous methods, which is impossible. MATLAB simulates the method's results.

M. Dhami, V. Garg, and N. S. Randhawa introduced the VGDRA (Variable Generation Distance and Rate Adjustment) algorithm, designed for enhancing energy efficiency within wireless sensor networks. This dynamic approach demonstrates superior energy efficiency when compared to the LEACH (Low-Energy Adaptive Clustering Hierarchy) algorithm. Notably, the VGDRA algorithm yields improved outcomes within a reduced number of iterations compared to earlier methodologies, which was considered unattainable. The effectiveness of the proposed approach is validated through MATLAB simulations, which substantiate the positive impact of the VGDRA algorithm on wireless sensor network performance.

A WSN is a network of sensors that record data about the system's physical status in real time. A sensor sends data to a central place through network. A sensor's battery life is related to its charge. Reduced battery power shortens sensor life. To keep sensors functional, WSNs must share power. LEACH uses energy effectively up to a point, therefore it's called "low-energy adaptive clustering" (LEACH). R. Sujee and KE Kannammal compare LEACH, Genetic-LEACH, and Inter-Cluster Communication. Before using GA to lengthen LEACH's lifespan, examine its fundamental operations. Finally, LEACH is compared, which talks with other clusters to reach the sink. Compared to Genetic LEACH and LEACH, inter-cluster communication reduces node energy usage and increases WSN lifespan. MATLAB simulations confirm this..

The realm of research and development within wireless mesh networks (WMNs) and wireless sensor networks (WSNs) has experienced significant growth, as highlighted by A. S. Hampiholi and B. P. Vijaya Kumar in their paper [3] pertaining to the Internet of Things (IoT). Addressing the optimization challenge within these networks holds the potential for substantial energy conservation, achieved through the efficient routing of data over the network, considering factors such as path, node energy, link quality, and traffic constraints. Genetic Algorithms (GAs) serve as a valuable tool in addressing these complex challenges by employing heuristic techniques across a network population. However, it is crucial to note that the premature convergence of the algorithm can impede its effectiveness, limiting its ability to explore the entire search space and identify energy-efficient alternatives. To mitigate such limitations, the integration of Local Search techniques can enhance the capabilities of GAs, addressing their inherent weaknesses and contributing to more robust optimization processes

MEGA (Maximum Enhanced Genetic Algorithm) combines Local Search with Sleep-Wake-Up, dynamically optimizing Wireless Sensor Networks (WSNs) considering communication constraints and energy usage. A comparative study contrasts MEGA with existing routing protocols, while software simulations mimic various WSN scenarios, highlighting energy savings and improved routing. Genetic optimization-based routing, particularly beneficial for dense WSNs [4], employs chromosomal templates and effective local searches. This approach prevents premature convergence, enhancing global optimization. Simulation results validate reduced energy consumption and extended network longevity.D. Mehetre and S. Wagh say designing good WSN topologies is key to boosting wireless sensor network longevity. The topology should balance and optimise energy consumption. The paper provides an energy-efficient disjoint path routing technique based on the Genetic Algorithm (GA). Simulations show the proposed solution uses less energy and extends network life. Other applications that require discontinuous paths to be fault tolerant can benefit from the proposed technique.

Energy-efficient protocols are vital for wireless sensor networks (WSNs), prolonging their lifespan. WSNs rely on node communication rather than physical media, often employing clustering to streamline data transmission. N. S. Randhawa and M. Dhami propose Virtual Grid-based Dynamic Routes Adjustment (VGDRA), an energy-efficient evolutionary algorithm that outperforms traditional methods like LEACH. VGDRA's dynamic approach yields better results in fewer iterations, validated through MATLAB simulations.

Research indicates that clustering has the potential to significantly extend the operational longevity of wireless sensor networks (WSNs). Nodes situated closer to the sink or base station (BS) often bear the responsibility of handling traffic not only from their own nodes but also from others, leading to complex traffic management. This scenario can result in fragmented network nodes, where remote sensors experience higher power consumption and premature failures compared to those in proximity to the BS. Notably, the work of S. R. Gupta, N. G. Bawane, and S. Akojwar [7] introduces a novel mechanism wherein cluster heads efficiently generate and transmit data to the BS. Each rotation of the cluster head (CH) involves unique tasks, finely tuned for energy distribution using a genetic algorithm (GA). Comprehensive studies underscore the stability and superiority of this technique over probabilistic and evolutionary computing (EC) algorithms.In [8] WSN research, one of the most critical concerns is how to save and reduce energy use. Using clustering as a design strategy can help you manage network energy consumption. This research uses GSAA to cluster a network and maximise its longevity. The new algorithm's goals are node placement and energy consumption. Simulations show that replacing various cluster-based routing protocols with GSAA improves the system's performance.

As per findings by H. B. Shah and H. Darji [9], traditional protocols like LEACH, PEGASIS, or TEEN are not suitable for Energy Harvesting-Wireless Sensing Element Networks (EH-WSN) due to their low-power requirements. To enhance energy efficiency, machine learning techniques have been explored, aiming to replace battery-dependent operations. This study endeavors to develop a machine learning-based routing strategy that harnesses renewable energy sources, diverging from conventional battery reliance. The investigation delves into the effectiveness of LEACH and customized LEACH algorithms in optimizing WSN energy efficiency. These solutions emphasize sensor node clustering and/or protocol adaptation. Our machine learning-driven approach presents a more energy-efficient and enduring network compared to the LEACH protocol.

A Wireless Sensor Network (WSN) consists of energy-limited sensors and dispersed Base Stations (BS) for efficient data transmission. This study focuses on BACREED-LEACH, an Antcuckoo-Optimized Relay-Based Energy-Efficient Data Aggregation approach. It comprises two stages, excluding BS from cluster

formation. CHs and RNs are identified in the initial phase, enabling data aggregation at CHs and subsequent transmission via RNs to the BS. Energy savings result from remote nodes communicating via ICH with CH nodes, sustained by RNs. Initial ACO and Cuckoo Search iterations determine CHs, followed by further refinement. Spyder-py3 tool evaluates network life, energy use, and throughput. Although the desired goal was not met, other energy-efficient algorithms (EEDAs) like BACEED-LEACH, AEED-LEACH, and GADA-LEACH are explored.

A. Sirbu and I. Alecsandrescu [11] propose employing genetic algorithms to enhance the energy efficiency of ad hoc wireless sensor networks (WSNs). Various algorithms were assessed within a tailored MATLAB environment for optimization purposes, particularly focusing on cluster count and arrangement. Swift execution is essential for real-time algorithms. To expedite GA convergence, custom genetic operators were formulated, alongside meticulous fine-tuning of GA settings. Extensive simulations have demonstrated the feasibility and efficiency of our approach. In contrast to other systems that have solely reduced minimum communication distance in an ad hoc network, our approach effectively doubled the speed of GA convergence within the WSN context.

Quality of Service (QoS) routing is a prominent concern in Wireless Sensor Networks (WSNs), particularly due to the demand for real-time services. Achieving QoS in sensor networks poses challenges, necessitating a delicate balance between battery life and QoS commitments. However, implementing multiple-objective QoS routing systems proves computationally impractical. In a two-tier WSN setup, high-power relay nodes can serve as cluster heads, facilitating data transmission to the sink. This approach heavily relies on these relay nodes to ensure the delivery of quality services (QoS). To address this, the present paper employs NSGA-II to propose an energy-efficient QoS routing scheme tailored for cluster-based WSNs. Simulation results demonstrate that the suggested protocol surpasses the current network in terms of both performance and energy consumption, highlighting its effectiveness.

S. Emalda Roslin[13] underscores WSNs' rising utility in scenarios beyond human reach, especially critical in nuclear power facilities where data interruption poses severe risks. Topology Control is essential for energy-efficient networks. This study deploys a genetic algorithm for topology management, yielding a three-tier architecture with Cluster Heads, Cluster Slaves, and Super Heads, surpassing two- and one-tier designs. Selection criteria encompass energy, bandwidth, and RAM. Quantitative analysis explores N-tier effects on algorithm performance, revealing energy savings in varied node densities of two-tier structures.

N. Dahda, M. Sindhwani, and C. Singh emphasize well-structured wireless sensor networks with multiple ad hoc sensor nodes. Our proposed hybrid approach integrates neural networks, evolutionary algorithms, and dynamic clustering to boost energy efficiency and lower latency. This technique enhances speed, efficiency, and data flow management in WSNs, considering various environmental conditions. The innovation is especially valuable in remote, Internet-deprived areas like forests and deserts. Minimizing sensor node battery usage is critical due to their limited recharge capacity, making the hybrid data aggregation technique a solution for improved energy efficiency, reduced latency, and enhanced data transmission.

In the study conducted by M. Niazi Torshiz, G. Tadayon, M. Jalali, and M. M. Tajari [15][16], a network of numerous low-energy nodes is deployed for local monitoring within a limited area, raising concerns about network durability. Addressing this, the Clustered WSN utilizing Fuzzy Logic and Genetic Algorithm (CFGA) employs a single-step approach for intra-cluster communication and a multi-step method for inter-cluster communication. A genetic algorithm is utilized to assess a node's suitability as a cluster head based on its fuzzy module and energy-efficient cluster head locations. This optimization ensures the base station benefits from the most optimal nodes. Interestingly, the researchers found that nodes with robust genetic algorithm capabilities expedited convergence rates.

Extending the longevity of wireless sensor networks holds significant importance, as emphasized by C. L. Urgaya and P. R. Savarapu [16]. The performance of these networks is notably influenced by the battery life of sensor nodes, where low energy levels often hinder or prevent battery replacement. This consideration ensures the centrality of cluster heads, maintaining equitable energy distribution among all clusters. The outcomes demonstrate that OMNeT++ nodes contribute to prolonged network stability and energy sustainability.

Z. T. Alisa and H. A. Nassrullah [18] emphasize clustering's role in minimizing data transmission power to the Base Station (BS). Intelligent clustering offers an innovative approach to enhance energy efficiency and network longevity. Adapting to dispersed nodes and changing field sizes, this protocol employs variable clusters using a refined genetic algorithm. The approach optimizes CH selection while preventing low-energy nodes from becoming cluster heads, resulting in extended network lifespan and reduced energy consumption, outperforming existing protocols.

Wireless sensor networks (WSNs) have garnered attention, as noted by R. A. Kovacs and colleagues [19]. While WSNs hold promise in computer science, challenges exist. The distributed nature of sensor nodes across diverse terrains and zones poses difficulties in access. This study employs a genetic approach to enhance energy efficiency and extend the lifespan of WSNs.

M. Thangaraj and P. P. Ponmalar [20] elucidate that a wireless sensor network (WSN) is composed of dispersed sensing elements, leading to duplicate sensory data and wasteful energy consumption. Employing data aggregation mitigates this issue by reducing redundant packet transmission to the sink, consequently prolonging the WSN's operational lifespan. The longevity of the WSN is contingent upon the energy level of individual nodes. Within energy-efficient data aggregation spanning trees, a genetic algorithm (GA) is employed to devise a balanced path considering data load and residual energy. Subsequently, mobile agents extract data from nodes following the path determined by the Artificial Bee Colony algorithm. Wireless Sensor Networks necessitate precise data, emphasizing the importance of Secure Hybrid (GA-ABC) Data Aggregation Trees (SHDT) to conserve energy. Simulations affirm that this approach holds the potential to significantly extend the network's operational lifespan.

RSM, AAO, and YEEAhmed [21] propose a wireless sensor network to monitor physical and environmental parameters. Nodes have sensors, wireless communication, limited computing power, and energy reserves, impacting network lifespan. Clustering minimizes redundancy and conserves energy. The Low-Energy Adaptive Clustering Hierarchy clusters the network, addressing the challenge of parameter cluster leader selection. This study introduces a framework using distance, node degree, and centrality for cluster head choice. Candidate selection employs fuzzy logic and a genetic algorithm, comparing methods for network longevity determination using fuzzy logic and probability values in the Genetic Algorithm construction.

All the acronyms mentioned in this paper are listed in Table 1.

Table 1: Definition of acronyms

Acronyms	**Definition**
WSN	Using a large number of wireless sensors, a Wireless Sensor Network (WSN) monitors the health of a system, its physical state, and the surrounding environment without the use of any additional infrastructure. Systems, physical conditions, and environmental circumstances all can be monitored via Wireless Sensor Networks (WSN).

CH	Senor nodes can be found in the network. In the cluster, this node is responsible for collecting data from other nodes. Other than that, it's in charge of gathering and transmitting data to the base station.
AODV	Routing in mobile networks can be done efficiently and without loops using AODV (Ad Hoc On-Demand Distance Vector). It can, for example, start on its own when nodes move, links break, and packets are lost.
RSA	Data transmission is protected using the RSA public-key cryptosystem, developed by Rivest, Shamir, and Adleman (RSA). Just because it's a classic doesn't disqualify it from this list. RSA is the name given to the algorithm by Ron Rivest, Adi Shamir, and Leonard Adleman when it was initially published in 1977. GCHQ created a similar technology in 1973, but it was kept secret.
Virtual Grid based Dynamic Routes Adjustment (VGDRA)	Route reconstruction costs for sensor nodes are minimized while preserving near-optimal routes for mobile sinks' most recent locations via the virtual grid-based dynamic route adjustment (VGDRA) approach. Only a small number of nodes must alter their data delivery routes in order to reach the mobile sink due to the communication rules that regulate the route reconstruction process. Route reconstruction costs can be reduced and network life expectancy increased by using the VGDRA plan, compared to earlier work.
TAGA	In order to secure both security and energy efficiency, TAGA was built by merging the trust-security mechanism and AGA together. An adaptive trust model developed by TAG helps to counter both ordinary and unusual attacks on the trust of network nodes. TAG improves security.

3. Proposed Method

Here, we present the EFGA-DoSLD algorithm, specifically designed to analyze misbehavior among sensor nodes in Wireless Sensor Networks (WSNs). The overarching approach is outlined in Figure 2. The procedure initiates with the establishment of the network's foundational infrastructure, followed by configuring the Base Station (BS), monitoring node behavior, and determining chromosomal fitness. This is succeeded by the exploration of routes and continued behavior observation. It's worth noting that conventional cryptographic protection proves inadequate in safeguarding innocent nodes, leading to potential misidentification as malicious counterparts. WSNs leverage human-to-human trust relationships for the identification and removal of malevolent nodes, contributing to heightened node security through established trust. This comprehensive process entails reconnaissance to locate trust information sources, complemented by watchdog mechanisms overseeing packet transmission and reception. [19] The Trusted Aggregator Genetic Algorithm (TAGA) introduces a hierarchical system of trusted values that facilitates dynamic trust behaviour. The procedural workflow of the proposed approach is visually depicted in Figure 2.

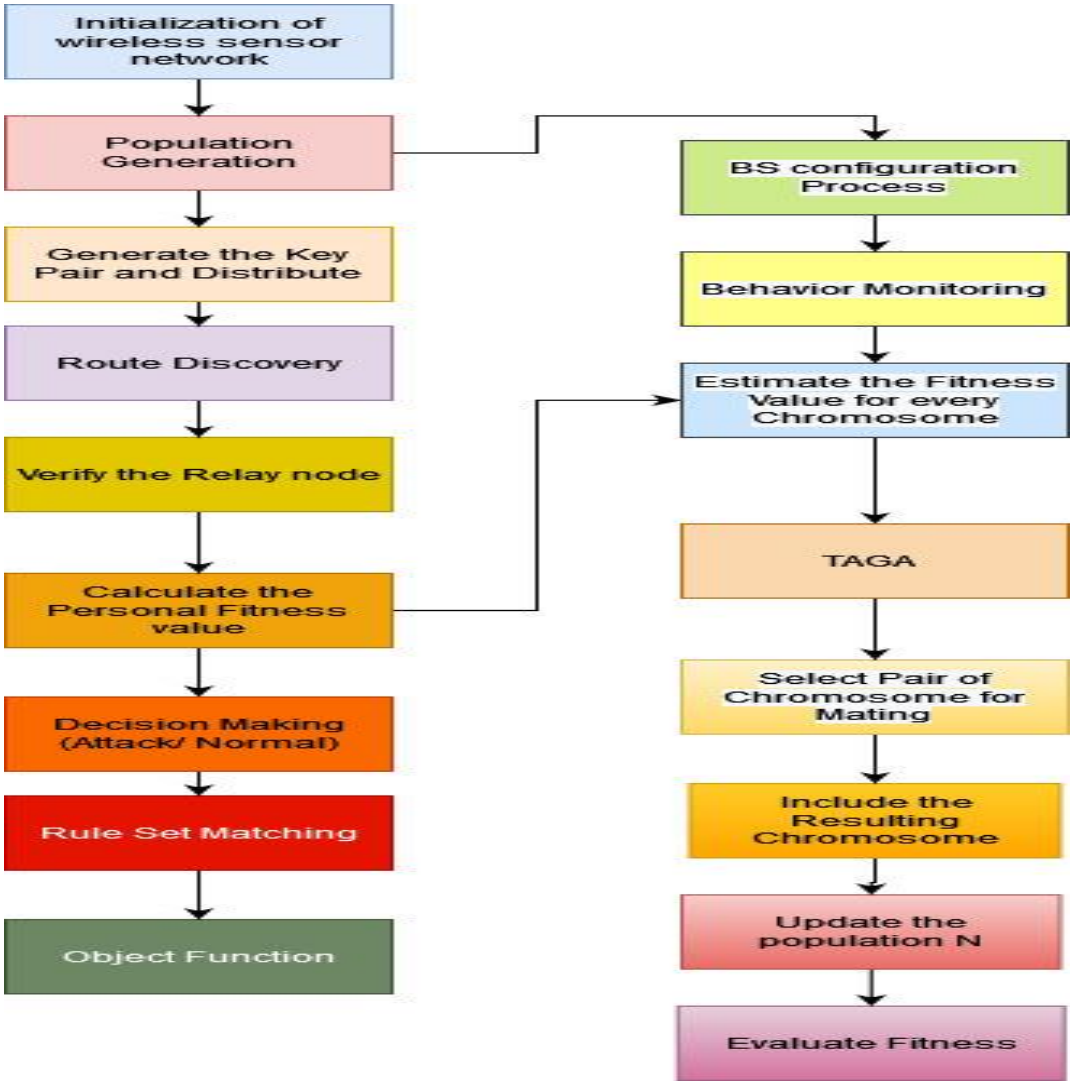

Figure 2: Flow Diagram of Proposed work

The graphic clearly shows the major phases:
(i) WSN initialization
(ii) Population generation
(iii) Generation and distribution of key pair
(iv) Route discovery with TAGA Trust model
(v) Behaviour monitoring
A detailed description of every step is provided in the following sections.

3.1. WSN Initialization

Initialization of the WSN is the first step in the proposed method. With the help of the NS2 tool, 100 sensor nodes are added to the WSN with a random waypoint mobility model. 250 metres is the maximum distance that the WSN can transmit. To begin with, the initialised WSN has the attributes indicated in Table 1.

3.2. Population and BS setup

Once WSN is setup, EFGA-DoSLD After the population is formed, the BS utilises the MRSA algorithm to generate a public-private key pair. Sensor nodes employ private keys, while BS uses public keys. This stage aims to prevent the DoSL attack. This phase prevents the attacker node from sending or receiving packets, saving sensor nodes' energy. The algorithm's steps [20].

3.4. Route Discovery With TAGA Trust Model

Sensor nodes use AdHoc On-Demand Distance Vector (AODV) before sending packets. The suggested protocol emphasises route discovery and maintenance. They provide an optimal path to the final destination after receiving RREQ messages. When the intermediary node is the

destination node, RREP packets are delivered to the source node.

3.4.1 TRUST MODEL

Because a normal node is mistaken for a malicious node, cryptographic security measures fail to protect it. Because of this, WSNs use trust relationships between humans to determine whether or not a node is malevolent. The more trusted a node is, the more secure it is. Reconstitution of the data source for trust evaluation [19] is accomplished with the help of the watchdog mechanism, which primarily monitors the nodes along the route during packet transmission and reception. The dynamic behaviour of trust is maintained via TAGA's use of hierarchical trust values.

3.5. Behavior Monitoring

No packets are sent until the sensor nodes have verified the trustworthiness of their neighbors. If the sensor node notices any of the following during transmission, it uses the BS's information to estimate the fitness value:

(i) Large data packets that surpass the sensor node's capability

(ii) Flooding of data packets

The attacker ID is used to measure the fitness value of a chromosome. After assessing fitness, sensor nodes send BS alarms on neighbor node behaviors. After receiving an alarm, the BS performs chromosome crossover and mutation operations to discover and analyses the attacker's attack strategy. Crossover and mutation create new chromosomes for the population. If an attacker node is found, a neighbor's status is updated in real time. EFGA-DoSLD destroys attacker nodes to prevent DoSL attacks.

The provided pseudocode outlines the initialization and functioning of a Wireless Sensor Network (WSN). It begins by initializing the network, configuring communication protocols, deploying sensor nodes, and establishing a base station for centralized management.\ Next, the code covers population generation, where individuals are created with initialized attributes, forming a diverse population with unique characteristics. Key pair generation and distribution are addressed, ensuring secure communication across the network by generating pairs of encryption keys and sharing public keys among nodes. The pseudocode also describes the route discovery process using the TAGA Trust Model, involving the initialization of a routing algorithm, selection of source and destination nodes, determination of routes based on trust, and transmission of data along the chosen route. Lastly, behaviour monitoring is outlined, focusing on each node's actions. Suspicious behaviour triggers notifications to administrators and appropriate actions, safeguarding the network's integrity.The sudo code of algorithm is given below:

```
(i) WSN Initialization:
 Initialize_WSN()
 Configure_Communication_Protocols()
 Deploy_Sensor_Nodes()
 Establish_Base_Station()
 // Other relevant initialization steps

(ii) Population Generation:
 Generate_Population(size)
 For each individual in Population:
  Initialize_Attributes()
  // Other attribute initialization

(iii) Generation and Distribution of Key Pair:
 For each node in WSN:
  Generate_Key_Pair(node)
  Distribute_Public_Key(node)
  // Other key pair generation and distribution steps

(iv) Route Discovery with TAGA Trust Model:
 Initialize_Routing_Algorithm()
 For each data transmission:
  Select_Source_Node()
  Select_Destination_Node()
  Determine_Route_TAGA(source, destination)
  Transmit_Data_Along_Route(route)
  // Other route discovery and data transmission steps

(v) Behavior Monitoring:
 For each node in WSN:
  Monitor_Behavior(node)
  If Suspicious_Behavior Detected:
   Notify_Admin()
   Take_Appropriate_Action()
```

// Other behavior monitoring and response steps

4. Result and simulation

The proposed research paper presents a comprehensive solution to address the critical issue of Denial-of-Sleep (DoSL) attacks in Wireless Sensor Networks (WSNs). By combining genetic algorithms, trust-based mechanisms, and adaptive strategies, the paper's EFGA DoSLD algorithm offers a promising approach to enhance the security and energy efficiency of WSNs. The result analysis of the paper's key contributions can be summarized as follows:

4.1 Efficient DoSL Attack Detection: The EFGA DoSLD algorithm introduces a novel method for detecting DoSL attacks efficiently. By leveraging genetic algorithms, the algorithm can intelligently evolve and adapt to emerging attack techniques. This advancement is crucial in ensuring the timely identification and mitigation of malicious activities that disrupt sensor node sleep patterns.

4.2 Trust-Based Adaptive Genetic Algorithm (TAGA): The integration of TAGA provides a robust foundation for evaluating trustworthiness within the network. By considering both direct and indirect trust values, along with factors like volatility and adaptive penalties, the algorithm can make informed decisions about node behaviours. This enhances the accuracy of DoSL attack detection and reduces false positives/negatives.

4.3 Energy Efficiency and Key Distribution: The adoption of the modified-RSA (MRSA) algorithm for key creation and distribution at the base station contributes to the overall energy efficiency of the network. This cryptographic approach ensures secure communication while minimizing energy overhead, aligning with the energy constraints inherent to WSNs.

4.4 Reliable Relay Node Selection and Routing: The paper introduces the use of the AODV routing protocol to identify reliable relay nodes before transmitting messages. This selection mechanism enhances the reliability of data transmission while conserving energy by avoiding unnecessary communication attempts.

4.6 Comparison with Existing Solutions: The result analysis demonstrates that the EFGA DoSLD algorithm outperforms other existing solutions such as X-MAC, ZKP, and TE2P. This suggests that the proposed algorithm effectively mitigates DoSL attacks and exhibits superior performance in terms of accuracy, energy conservation, and overall network stability.

4**.7 Practical Implications:** The implications of this research are significant, as WSNs are increasingly being deployed in various applications ranging from environmental monitoring to industrial automation. The EFGA DoSLD algorithm's ability to detect and counteract DoSL attacks contributes to the reliability and longevity of WSNs, enabling them to operate optimally even in the presence of malicious actors.

5. Performance Analysis

In this part, the suggested EFGA-DoSLD algorithm's performance is examined using the following metrics:
(i) Energy consumption
(ii) Packet count
(iii) Time from beginning to end
(iv) Consumption of energy on a daily basis
(v) Ratio of delivered packets
(vi) The ratio of throughput to packet rate
The zero-knowledge protocol (ZKP), the X-MAC, and the two-tier energy efficient secure (TE2S) scheme are some of the current algorithms that are evaluated and contrasted with the EFGA-DoSLD approach that is recommended in this study [23].

Table 1: Network Properties

Properties	Values
No of Nodes	100
Initial Energy	0.5J

Idle State Energy	50 n/J
Data Aggregation Energy	10 Pj/bit/m^2
Amplification Energy (CH to BS)	10 pl/bit/m^2
Amplification Energy (Node to BS)	0.0003 pl/bit/m^2
Packet Size	400

5.1 Normalized energy consumption

The amount of energy required to transfer three packets per second is referred to as the "normalised energy consumption" (NEC). Figure 3 shows that the proposed EFGA-DoSLD method consumes very little energy at all attack intervals.

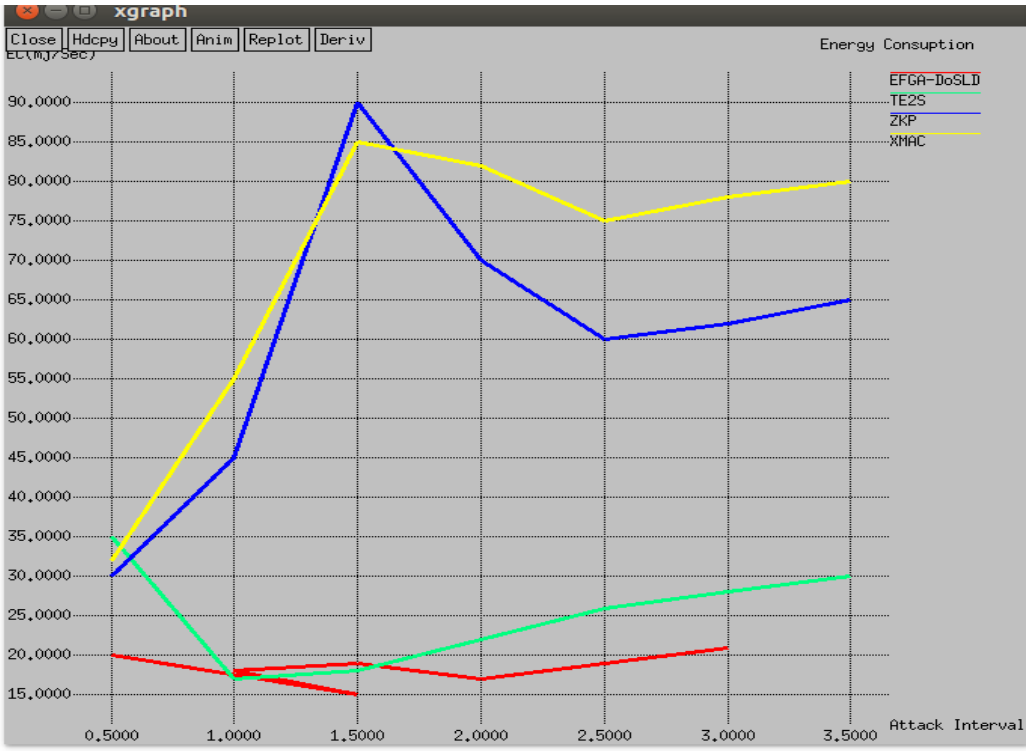

Figure 3. Comparison of Network Lifetime

5.1.1 Effective packet number

Validated for various attack intervals is the effective packet number of the existing algorithms. The comparison is based on a pace of one packet per three seconds. Figure 5 illustrates that the proposed EFGA-DoSLD algorithm outperforms the previous schemes in terms of effective packet number.

5.1.2 End-to-end delay

It is defined as the average amount of time it takes to send a packet from one end of the network to the other. Figure 4 depicts the end-to-end delay as a function of packet size. As shown in the image, the proposed EFGA-DoSLD algorithm delivers the lowest end-to-end delay for varying packet sizes . Consumption of energy on a daily basis The ratio of throughput to packet rat Figure 4 depicts a wireless sensor network with a distributed network of independent sensors (WSN). Networks and processing must be energy-efficient when it comes to WSN because energy costs are a big constraint. A gateway node, WSN's most energy-intensive node, may be used to broadcast sensor data only when an incident of relevance occurs. This saves money on communication because sensors only communicate when an issue occurs. Security, home automation, disaster relief, traffic management, and health care are all examples of network-enabled services. This reduces the

amount of energy that is used by nodes because they only return when something happens. This can be challenging in dynamic settings when the vast majority of the data collected is of negligible or even no consequence. In order to tackle the problem, it is necessary to loosen the definition of what defines an event, threshold, or probability.

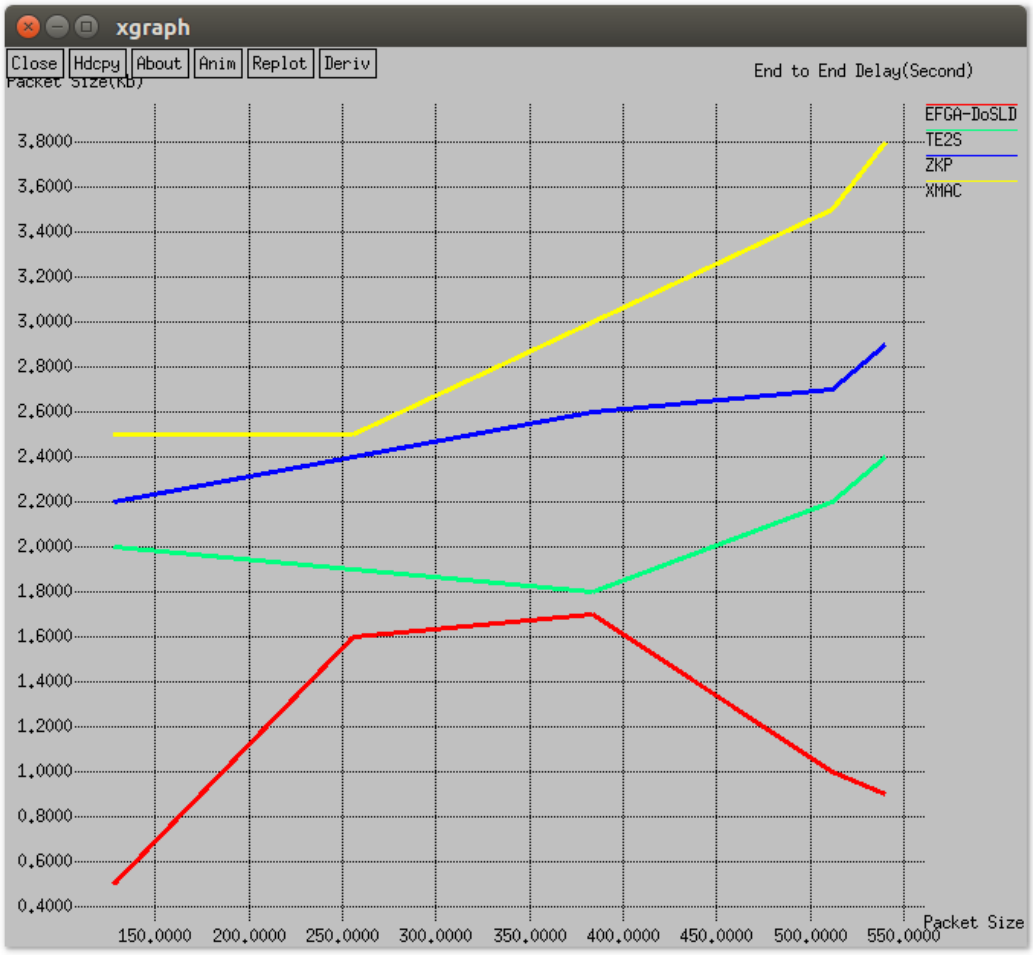

Figure 4: Compression of End to END Delay

5.1.3 Packet Delivery Ratio.

The PDR analysis within the study "EFGA-DoSLD: Energy Efficient Denial of Service Attack Detection in WSN" reinforces the practicality and effectiveness of the proposed approach. The favorable PDR results underline the successful integration of security enhancements while ensuring reliable packet delivery in a resource-constrained WSN environment. This research contributes to the broader field of WSNs by offering a comprehensive solution that addresses both security and communication requirements, ultimately enhancing the network's overall performance and longevity.

Number of data packets transmitted from source divided by a number of data packets delivered to the destination node (PDR). The formula for PDR:

PDR= Total Number of Packets Sent/ Number of Packets Successfully Delivered ×100%

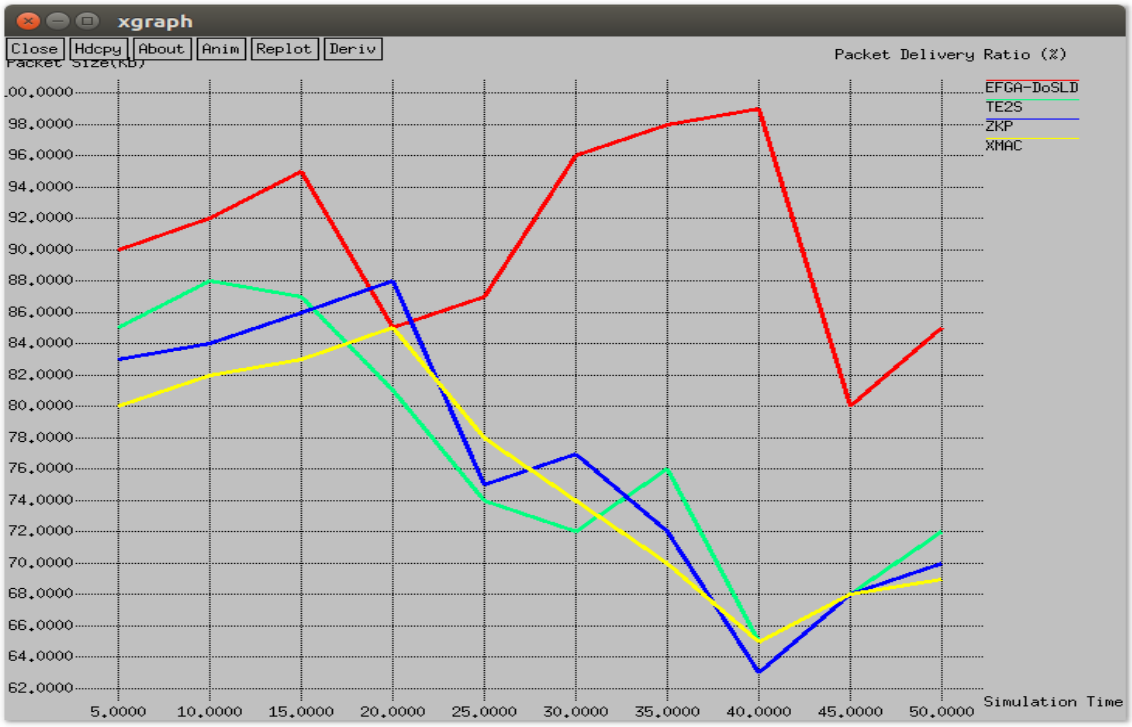

Figure 5: Compression of Packet Delivery Ratio

In Figure 5 End-to-end delay or one-way delay (OWD) is the time required to transport a packet from source to destination over a network.

6. Conclusion and Future Direction

In conclusion, the EFGA DoSLD algorithm demonstrates a commendable effort in addressing the critical challenge of DoSL attacks in WSNs. By combining genetic algorithms, trust-based mechanisms, and adaptive strategies, the paper offers a promising solution that enhances both security and energy efficiency. The extensive result analysis showcases the algorithm's superiority over existing solutions and sets the stage for continued advancements in securing and optimizing wireless sensor networks.

An adaptive evolutionary algorithm called as TAGA is proposed in this research to resist typical routing assaults and special trust attacks in order to withstand numerous attacks, enhance the speed of recognising the attackers, and pick secure and energy-efficient routes while maintaining network integrity.

Future Research Directions: While the paper presents a comprehensive approach, there are potential avenues for further exploration. Future research could delve deeper into optimizing the genetic algorithm's parameters, refining the trust calculation model, and evaluating the algorithm's performance under diverse network scenarios and attack variations.

References

1. M. Dhami, V. Garg and N. S. Randhawa, "Enhanced Lifetime with Less Energy Consumption in WSN using Genetic Algorithm Based Approach," *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, 2018, pp. 865-870.doi: 10.1109/IEMCON.2018.8614754

2. R. Sujee and K. E. Kannammal, "Energy efficient adaptive clustering protocol based on genetic algorithm and genetic algorithm inter cluster communication for wireless sensor networks," *2017 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2017,pp.1-6.doi:10.1109/ICCCI.2017.8117753

3.A. S. Hampiholi and B. P. Vijaya Kumar, "Efficient routing protocol in IoT using modified Genetic algorithm and its comparison with

existing protocols," *2018 3rd International Conference on Circuits, Control, Communication and Computing (I4C)*, Bangalore, India, 2018, pp. 1-5 doi: 10.1109/CIMCA.2018.8739759

4.Wei Qu and Mengmeng Yang, "An energy-efficient routing control strategy based on genetic optimization," *Proceeding of the 11th World Congress on Intelligent Control and Automation*, Shenyang, China,2014,pp.2038-2041.doi:10.1109/WCICA.2014.7053035

5.D. Mehetre and S. Wagh, "Energy Efficient Disjoint Path Routing Using Genetic Algorithm for Wireless Sensor Network," *2015 International Conference on Computing Communication Control and Automation*,P0une,India,2015,pp.182-185.doi:10.1109/ICCUBEA.2015.40

6.N. S. Randhawa and M. Dhami, "Reduction of Energy Consumption in WSN using Hybrid VGDRA Approach," *2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, Riga, Latvia, 2018, pp. 1-6. doi: 10.1109/ITMS.2018.8552974

7.S. R. Gupta, N. G. Bawane and S. Akojwar, "A Clustering Solution for Wireless Sensor Networks Based on Energy Distribution & Genetic Algorithm," *2013 6th International Conference on Emerging Trends in Engineering and Technology*, Nagpur, India, 2013, pp. 94-95.doi: 10.1109/ICETET.2013.24

8.M. Xie, T. -l. Huang and X. -s. Zhu, "A Novel Routing Algorithm for Energy-Efficient in Wireless Sensor Networks," *2009 Third International Conference on Genetic and Evolutionary Computing*, Guilin, China2009,pp.65-68.doi:10.1109/WGEC.2009.116

9.H. Darji and H. B. Shah, "Genetic algorithm for energy harvesting-wireless sensor networks," *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, 2016, pp. 1398-1402.doi:10.1109/RTEICT.2016.7808061

10.G. Devika, D. Ramesh and A. G. Karegowda, "An Energy Efficient Routing and Compression Based Data Collection Applying Bio-Inspired Ant-Cuckoo Technique for Wireless Sensor Network," *2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*, Bengaluru, India, 2019, pp. 1-8. doi: 10.1109/CSITSS47250.2019.9031048

11.A. Sirbu and I. Alecsandrescu, "Enhanced genetic algorithm for energy efficient dynamic ad hoc wireless sensor networks," *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*, Iasi, Romania,2017,pp.1-4.doi:10.1109/ISSCS.2017.8034920

12. G. H. EkbataniFard, R. Monsefi, M. Akbarzadeh-T and M. H. Yaghmaee, "A multi-objective genetic algorithm based approach for energy efficient QoS-routing in two-tiered Wireless Sensor Networks," *IEEE 5th International Symposium on Wireless Pervasive Computing 2010*, Modena, Italy, 2010, pp. 80-85.doi:10.1109/ISWPC.2010.5483775

13. S. Emalda Roslin, "Genetic algorithm based cluster head optimization using topology control for hazardous environment using WSN," *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 2015, pp. 1-7. doi: 10.1109/ICIIECS.2015.7193039

14. N. Dahda, M. Sindhwani and C. Singh, "Energy Efficient Hybrid Technique Based on Dynamic Clustering in Wireless Sensor Network," *2018 International Conference on Intelligent Circuits and Systems (ICICS)*, Phagwara, India, 2018, pp. 229-234.doi:10.1109/ICICS.2018.00055

15. E. Saeedian, M. Niazi Torshiz, M. Jalali, G. Tadayon and M. M. Tajari, "CFGA: Clustering Wireless Sensor Network Using Fuzzy Logic and Genetic Algorithm," *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, China, 2011, pp. 1-4.doi: 10.1109/wicom.2011.6040358

16.C. L. Urgaya and P. R. Savarapu, "Genetic algorithm inspired energy efficient balanced clustering for sensor networks," *2016*

International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016, pp. 627-633.doi: 10.1109/WiSPNET.2016.7566209

17. Ming Zou and Shijue Zheng, "Energy balancing routing algorithm based on HGACA in WSNs," *2010 2nd International Conference on Computer Engineering and Technology*, Chengdu, China, 2010, pp.V2-637-V2-640.doi:10.1109/ICCET.2010.5485663

18. Z. T. Alisa and H. A. Nassrullah, "Minimizing energy consumption in wireless sensor networks using modified genetic algorithm and an energy balance filter," *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, Baghdad, Iraq, 2016,pp.1-6.doi:10.1109/AIC-MITCSA.2016.7759947

19. R. A. Kovacs, B. Iancu, V. T. Dadarlat, E. Cebuc and S. Buzura, "Extending K-cover genetic algorithm for efficient energy consumption in WSNs," *2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Galati, Romania, 2019, pp. 1-6. doi: 10.1109/ROEDUNET.2019.8909581

20. M. Thangaraj and P. P. Ponmalar, "Swarm intelligence based secured data aggregation in wireless sensor networks," *2014 IEEE International Conference on Computational Intelligence and Computing Research*, Coimbatore, India, 2014, pp. 1-5.doi:10.1109/ICCIC.2014.7238519

21. R. S. M. Saadaldeen, A. A. Osman and Y. E. E. Ahmed, "Clustering for Energy Efficient and Redundancy Optimization in WSN using Fuzzy Logic and Genetic Methodologies a Review," *2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, Khartoum,Sudan,2018,pp.1-5.doi:10.1109/ICCCEEE.2018.8515880

22. V. K. Singh, V. Sharma and A. K. Sagar, "Hybrid genetic algorithm based technique to maximize the network lifetime in WSN," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, India, 2016, pp.383-387.doi:10.1109/CCAA.2016.7813751

23.A. Taha, S. S. Soliman and A. Badawi, "Genetic algorithms for lifetime elongation of clustered WSN," *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, 2017, pp. 1-7.
doi:10.1109/PIMRC.2017.8292597

24.Nimisha T.S and R. Ramalakshmi, "Energy efficient Connected Dominating Set construction using Ant Colony Optimization technique in Wireless Sensor Network," *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 2015, pp.1-5.doi:10.1109/ICIIECS.2015.7192912

25. A. Abro, D. Zhongliang, K. A. Memon and N. ul Ain, "Novel Genetic Algorithm with Efficient Routing Paradigm for Multi-hop WSNs," *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Beijing, China, 2019, pp. 28-31. doi: 10.1109/ICEIEC.2019.8784677