Salud, Ciencia y Tecnología - Serie de Conferencias. 2023; 2:593
doi: 10.56294/sctconf2023593

Categoría: Congreso Científico de la Fundación Salud, Ciencia y Tecnología 2023

ORIGINAL

Enhanced cryptography algorithm and improved butterfly algorithm for secured data transmission in wireless sensor network

Algoritmo criptográfico mejorado y algoritmo de mariposa mejorado para la transmisión segura de datos en redes de sensores inalámbricas

A. Prakash[1] ✉, M. Prakash[1] ✉

[1]Department of Computer Applications (PG). Hindusthan College of Arts & Science Coimbatore. Chennai, India.

Citar como: Prakash A, Prakash M. Enhanced cryptography algorithm and improved butterfly algorithm for secured data transmission in wireless sensor network. Salud, Ciencia y Tecnología - Serie de Conferencias 2023; 2:593. https://doi.org/10.56294/sctconf2023593

Recibido: 24-06-2023 **Revisado:** 22-08-2023 **Aceptado:** 23-10-2023 **Publicado:** 24-10-2023

ABSTRACT

Due of their many uses, WSNs (Wireless Sensor Networks) have drawn the greatest interest, but, existing methods do not support reliable data transfer. They face issues in energy consumptions and routing on shortest paths over WSNs. Also, they are incapable to stopping compromised nodes with legitimate identities from launching attacks. This study handled this issue with suggested schema based on CHs (Cluster Heads) and using IBO (Improved Butterfly Optimization) and DAES (Double key based Advanced Encryption Standard) algorithms. The main phases of this work contain system model, security model, CH node selection and shortest path routing with secured data transmission. Initially, system model is constructed via number of sensor nodes on the given setup. Then, CH nodes are selected using IBO algorithm based on best fitness values. These selections of CHs consider minimum delays and energy consumptions with maximum throughputs for establishing security assurances and energy conservations at sensor nodes along with secure protocol. The security levels for quick data transfers over multi-path routes in WSNs are improved using DAES. Attack nodes are eliminated for successful transfers. The intermediate layer CHs create routing backbones to gather, combine, and convey data from member nodes. The simulation results demonstrate that the proposed IBO-DAES framework outperforms existing approaches in terms of throughputs, network longevity, data transfer rates, and energy consumptions.

Keywords: Wireless Sensor Networks (WSNs); Cluster Head (CH); Based Improved Butterfly Optimization (IBO); Algorithm and Double Key Based Advanced Encryption Standard (DAES); Algorithm.

RESUMEN

Debido a sus múltiples usos, las redes de sensores inalámbricos (WSN, Wireless Sensor Networks) han despertado un gran interés, pero los métodos existentes no permiten una transferencia de datos fiable. Se enfrentan a problemas relacionados con el consumo de energía y el encaminamiento por los caminos más cortos en las WSN. Además, son incapaces de impedir que nodos comprometidos con identidades

legítimas lancen ataques. Este estudio trata este problema con un esquema sugerido basado en CHs (Cluster Heads) y utilizando los algoritmos IBO (Improved Butterfly Optimization) y DAES (Double key based Advanced Encryption Standard). Las fases principales de este trabajo contienen el modelo del sistema, el modelo de seguridad, la selección del nodo CH y el encaminamiento por el camino más corto con transmisión de datos segura. Inicialmente, el modelo del sistema se construye a través del número de nodos sensores en la configuración dada. A continuación, se seleccionan los nodos CH mediante el algoritmo IBO basándose en los mejores valores de aptitud. En la selección de los CH se tienen en cuenta los retardos y consumos de energía mínimos con los rendimientos máximos para establecer garantías de seguridad y conservación de la energía en los nodos sensores junto con un protocolo seguro. Los niveles de seguridad para transferencias rápidas de datos a través de rutas multitrayecto en WSN se mejoran utilizando DAES. Los nodos atacantes se eliminan para que las transferencias tengan éxito. Los CH de capa intermedia crean redes troncales de enrutamiento para recoger, combinar y transmitir datos de los nodos miembros. Los resultados de la simulación demuestran que el marco IBO-DAES propuesto supera a los enfoques existentes en términos de rendimiento, longevidad de la red, tasas de transferencia de datos y consumo de energía.

Palabras clave: Redes de Sensores Inalámbricos (WSNs); Cabeza de Cluster (CH); Optimización Basada en Mariposa Mejorada (IBO); Algoritmo y Estándar de Cifrado Avanzado Basado en Doble Clave (DAES); Algoritmo.

INTRODUCTION

WSNs are made up of several sensor nodes that co-operate to execute a single task. The system's key nodes collect information from outside conditions. The gathered data is then propagated to the BSs (ase stations) or sinks which are responsible for outside world collaborations. However, it is up to the sensor nodes to self-organize and work together to create and reserve the network.[1] These nodes often have modest sizes, restricted energy, limited memory, and regulated dispensing power.[2]

Cluster based approaches efficiently organise data aggregations and energy conservations in WSNs. CHs transfer data gathered by cluster nodes and aggregate/compress data before delivering them to sinks.[3] Nodes' higher workloads cause greater energy consumption or which result in uneven network degradations. Data aggregations are made simpler, by selections of CHs which combine sensors' sensed data. Integrations of the collected data near to data sources, minimize long-distance data transfers and reducing data gathering costs. CHs have different lifetimes based on their positions and balancing residual energies.

The design of routing paths for self-organized WSNs must address critical studies about energy balance and efficiency. A shortest-path algorithm identifies a route in the given network among two nodes that has reduced costs. Cost functions produce simple and efficient weighed shortest path trees without incurring any additional overheads.[4] Specific instances of energy-aware routes in WSNs were considered by the novel method for more acceptable energy-aware shortest paths. These nodes were constrained by their designs, which included limited memories and battery lives as well as processes and computational powers. Therefore, these limitations provide challenges for many application need designs, such as security.

A distributed, deterministic, and reactive routing protocol is AODV. Only when necessary are the routes configured. On demand routing is used in conjunction with AODV [5] with the goal of reducing the broadcast. It keeps broadcast, multicast, and unicast communication running. It makes use of the notion of packet sequence numbering and reduces the problem of routing loops. If connection breaks do occur,

they can be fixed locally. The several nodes in the described network configuration can benefit from AODV.

Moving nodes made routing far more complex in these systems, which calls for enhanced routing protocols. Finding the most recent topology of a network that is continually changing is the goal of routing in order to determine an exact route to a certain node in a WSN. A set of methods must be pursued to establish communication amongst sensor nodes. Protocols like the distance vector protocol and connection state routing method are employed. These protocols have limitations on routing and transmission due to several factors as QoS, energy use, throughput, and bandwidth.[6] To maintain the history of nodes and routing data, the system used the AODV protocol. The routing table stores the routing information, including address, node id, energy, and routing charge. Routing tables need to be changed as the system evolves over time.

Although various kinds of networks have successfully used public and private-key cryptography to safeguard data integrity and ensure authentication, they cannot be used in WSNs because they require more computational power and energy consumption, which reduces the network lifetime.[7] As a result, methods for protecting WSNs should not jeopardize the longevity of the network.

The purpose of this effort is to make sure that sensor nodes in WSNs transmit data securely. Numerous studies and approaches have been developed; however, reliability has not been considerably increased. The current methods have issues with energy usage and WSN dependability. The aforementioned issues are handled by the suggested IBO-DAES protocol, which increases the overall effectiveness of WSNs. The main contributions of this research include a system model, selections of CH nodes using IBO approach, routing, and secure data transfer using DAES+AODV protocol. Lives of WSNs are extended while energy consumptions are decreased with this approach.

The rest of the paper is organized as follows: The literature work on CH selection, attack detection, and security mechanisms in WSN is briefly summarized in Section 2. Additional details on the recommended technique for the IBO-DAES algorithm are provided in Section 3. The outcome of the assessment is presented in Section 4. Section 5 concludes with summarizing the findings.

Related work

In [8], Elshrkawey et al (2018) presented a method of improvement to lower energy use and increase network longevity. Enhancing energy balances in clusters of sensor nodes, successfully in reducing energy losses during network connections. The upgraded methods are built on selections of CHs which manage time divisions for multiple accesses. The development of the suggested technique exhibits improvement in terms of network lives, CHs counts, energy usages, and counts of packets transmitted to BSs when compared to ndother comparable protocols like LEACH.

In [9], Tabibi et al (2019) suggested Mobile sinks indirectly aid in balancing load and attaining uniform energy consumption. In this approach, the mobile sinks made predetermined stops within sensors' ranges called rendezvous spots, and selecting the best amongst them are NP-hard tasks. Hierarchical algorithms only utilise their local information to choose these locations, therefore the likelihood of selecting an optimal node as the rendezvous point will be quite low. The optimal rendezvous locations are selected in this research utilising a cutting-edge method called PSOBS (Particle Swarm Optimisation Based Selection). In order to find optimum or nearly perfect meeting locations for efficient network resource management, the approach makes use of PSO. Utilizing certain performance indicators, including throughput, energy consumption, and hop count, the approach is contrasted with the Weighted Rendezvous Planning Based Selection (WRPBS) algorithm. Simulation findings demonstrate PSOBS' superiority over WRPBS, yet it has a higher packet loss rate than WRPBS.

In [10], Mahajan et al (2014) presented CCWM (Cluster Chain Weight Metrics) approach, a technique for choosing cluster head weights that takes service factors into account to improve network performance, has been discussed. One of the primary issues with a clustering-based strategy is choosing the right cluster

https://doi.org/10.56294/sctconf2023593

heads for the network and creating balanced clusters. In a network, cluster creation begins with the selection of cluster heads based on a weight metric. This strategy balances load in addition to preserving sensor energy. Within the cluster, a local clustering method is used to cut down on computation and communication costs. Additionally, a novel data transfer method is developed.

In [11], Saidi et al (2020) presented a reliable election process of CHs and methods for misbehavior detections. The crucial indicators for elections and node trust, among others, were used. Additionally, a monitoring approach employing a range of trust types was developed to analyse the behaviours of sensor nodes with the aim of removing malicious nodes while preserving reliable nodes. The problem of picking CHs was also looked at. Local clustering methods and trust evaluation procedures at the level of the cluster members were employed in the compromised CH scenario to isolate the malicious CH without affecting network performance. The results demonstrate that the technique prevents malicious nodes from becoming CHs and protects the network from contaminated CH after the election. The approach successfully identified malicious nodes with a high incidence of false positive and false negative alarms when it came to misbehaviour identification.

In [12], Han et al (2015) introduced IDASA (Intrusion Detection Algorithm against Sinkhole Attack) based on neighboring information. In contrast to conventional intrusion detection methods, IDASA fully utilizes sensor node neighbor information to find sinkhole nodes. Additionally, assess IDASA in MATLAB as a result of the reliability of malicious node identification, energy usage, and network throughput. Findings demonstrate that IDASA works superior to alternative algorithms.

In [13], Abikoyeet al (2019) introduced the most effective symmetric encryption method, Advanced Encryption Standard (AES), has also made it more vulnerable to attacks. The actions of attackers continue to undercut efforts to secure information while utilizing AES. This has made it much more necessary for investigators to devise methods of improving the strength of AES. The SubBytes and ShiftRows transformations of the AES algorithm are modified in the work to create an improved AES algorithm. While the ShiftRows transformation is random, the SubBytes transformation has been adjusted to be round key dependant. Making the two transformations round key dependant is intended to make it so that even a small change in cypher text will be greatly influenced by the keys. The conventional and modified AES algorithms are implemented and evaluated in terms of their avalanche effect and execution time. In contrast to the 50,78 reported by the conventional AES algorithm, the avalanche effect generated by the modified AES technique was 57,81 %. However, the modified AES measured execution speeds of 0,18, 0,31, 0,46, and 0,59 ms, respectively, for 16, 32, 64, and 128 bytes of plain text. Compared to the results of the conventional AES, this is somewhat superior.

Proposed methodology

IBO-DAES technique is suggested in this study to enhance secured data transmission over the WSN. The system approach is the study's primary contribution,CH node selection via IBO algorithm, routing process and secured data transmission using DAES+AODV protocol. The recommended method's general block diagram is illustrated in figure 1.

System Model

This research takes into account the hierarchical network framework while it is more flexible and useful for WSNs. The network's sensor nodes are grouped together into clusters. Each one consists of a cluster head and some member nodes. The bottom layer's member nodes all engage in data sensing for relevant information. To gather, integrate, and forward the data from member nodes, cluster heads in the middle layer build the routing backbone. Data from cluster heads is relayed to the server by the base station in the top layer.

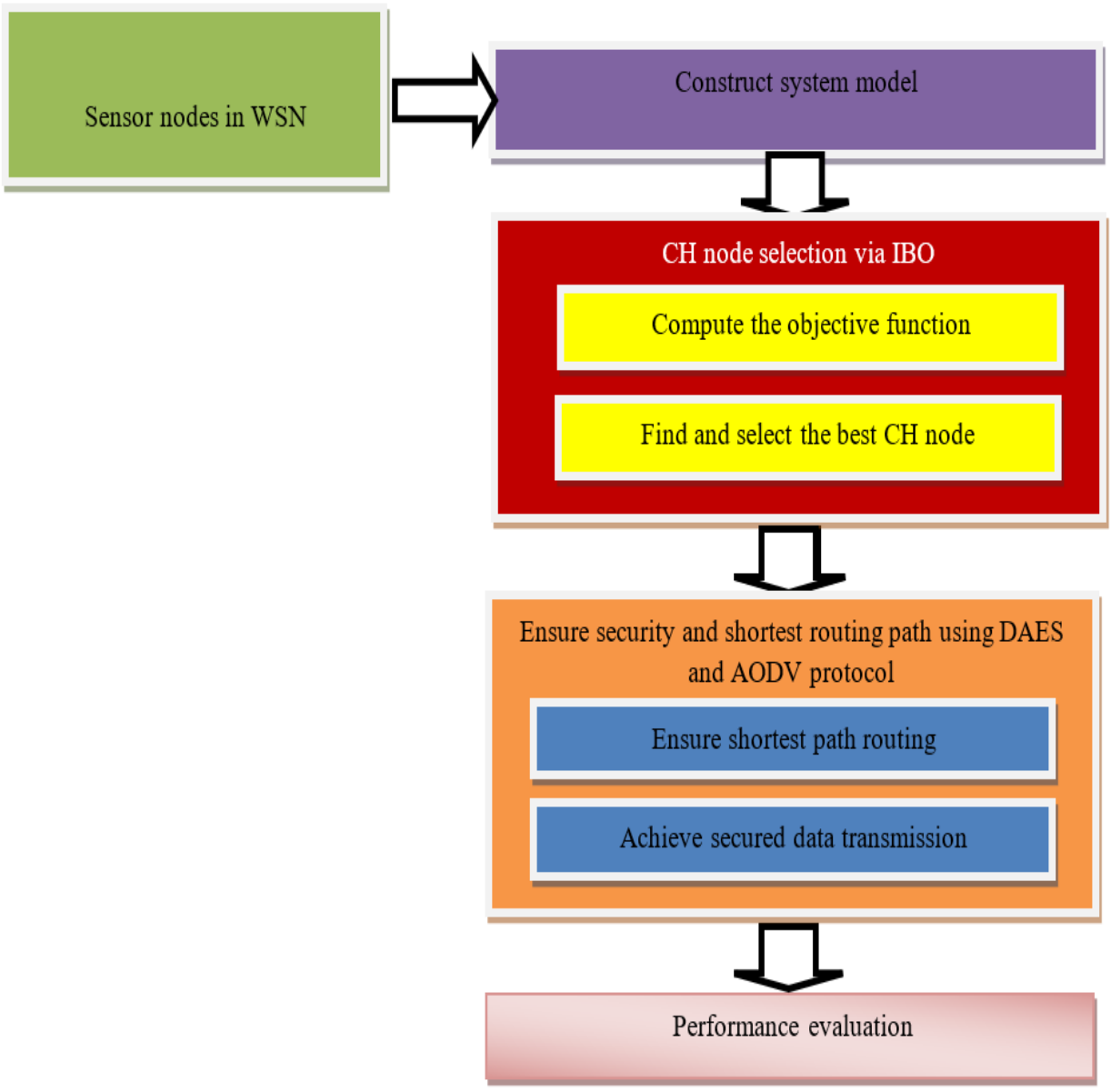


Figure 1. Overall block diagram of the proposed system

Radio model

An open wireless medium's channel quality is erratic and can occasionally be either excellent or tragic due to interferences. The time-varying wireless medium is then modelled in this work using a Markov chain with two states$S$ = {s0, s1}.[14]

Here s0 and s1 denote the bad and good states of the channel quality correspondingly. The time interval t over which the channel quality changes into each condition is a random variable that exhibits an exponential distribution as

$$p(t) = \begin{cases} \alpha_i e^{-\alpha_i t} & t \geq 0 \\ 0 & t < 0 \end{cases} \quad (1)$$

here $\alpha_i, i \in \{0,1\}$ are the rates of bad and good states. The probability that the channel state will change from bad to excellent is then determined by$p_0 = \alpha_0/(\alpha_0 + \alpha_1)$ and $p_1 = \alpha_1/(\alpha_0 + \alpha_1)$correspondingly

https://doi.org/10.56294/sctconf2023593

The free-space propagation model or the two-ray ground reflection model, according to the *d*amongst the transmitter and receiver, can both represent the wireless transmission loss. The first model is better suited to represent the transmission loss if *d* is less than a threshold, d_0. The second model is suitable in all other cases. The threshold $d_0$in this case can be calculated by

$$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{amp}} \quad (2)$$

here $\varepsilon_{fs}$and $\varepsilon_{amp}$are the amplified characteristic constants regarding the transmission loss models

The amount of energy used by a node to send a k-bit data packet over distance *d* can be expressed as

$$E_{Tx}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, & d < d_0 \\ kE_{elec} + k\varepsilon_{amp}d^4, & d \geq d_0 \end{cases} \quad (3)$$

where $E_{elec}$is the energy spent by the transmitter or receiver circuitry

For a k-bit data packet, the energy used by the receiver can be estimated by

$$E_{Rx}(k) = kE_{elec} + kE_{DA} \quad (4)$$

here $E_{DA}$is the energy consumed by the receiver for aggregating a one-bit packet

Security model

Resource-constrained WSNs are safe guarded in this work by security architecture that uses fuzzy evaluation for gathering trust based evidences, recommendations, grouping along with detection of outliers. Sensor nodes periodically collect trust evidences of other nodes by listening to their broadcasts. An IT2 FLS (fuzzy logic system) computes trust values using fuzzy inference to successfully reduce uncertainties in trust evidences which are updated. Each node can accumulate a large number of trust values when combined with the trust recommendation process. These values are then further examined via trust grouping. The outliers are then found using group means, and a node's maliciousness can be determined.

Cluster Head (CH) node selection via IBO Algorithm

Here, CH nodes are chosen from the specified network using the IBO algorithm, which is centred on choosing the best nodes as CHs. Routing issues of WSNs addressed by IBO which imitates the food searches (least latency, minimum energy consumption, and maximum throughput metrics with chosen nodes) and mating behaviour of wild butterflies. The suggested IBO algorithm is mostly based on the foraging method used by butterflies to locate a nectar partner by using their sense of smell to find the best CH nodes.[15] According to scientific research, butterflies have a very good sense of smell and can locate the source of it (minimum delay, minimum energy consumption and maximum throughput metrics with selected nodes).

An intensity of fragrance produced by a butterfly is connected with its fitness (minimum delay, minimum energy consumption and maximum throughput metrics with selected nodes), i.e., a butterfly's fitness will change as it travels from one place to another. In IBO Algorithm, whole concept of sensing and processing of important parameters namely sensory modalities (c), stimulus intensities (I) and power exponents (a) for selecting optimal nodes.[16] Fitness (minimum delay, minimum energy consumption and maximum throughput metrics with selected nodes) assessments for for selections of nodes in WSNs is based on I. Stimulated fragrances of butterflies are IBO functions wand computed based on equation (5),

$$f = cI^a \quad (5)$$

Where f implies perceived fragrance magnitudes or the capacity of other butterflies to detect fragrances, c refers to sensory modalities produced in shorter paths, In represents stimulus intensities while a are modality based power exponents where $a \,\&\, c$ lie in the interval $[0,1]$. $a = 0$ depicts non-detections of fragrances. The algorithm's behaviour is thus controlled by the parameter a. c is a vital parameter for determining the IBO algorithm's speed of convergence. It is another significant parameter. The following properties of butterflies are idealized in order to illustrate the topics with regard of a search algorithm:

1. Butterflies release odours that attract other butterflies, or nodes.

https://doi.org/10.56294/sctconf2023593

2. Every butterfly will migrate at random or in the direction of the one that is best and emits the most smell.
3. Objective functions evaluate butterflies' stimulus intensities.

There are 3 phases of IBO namely Initializations, Iterations and conclusions where IBO's initializations during each run of the algorithm, followed by an iterative search for optimal nodes, and lastly, the method is completed when the most optimal selection solution is discovered. Shortest distance is calculated using the IBO algorithm and its solution space during the initialization phase. Additionally, the parameters utilized by IBO are given assigned values. In the CH selection search space, the placements of butterflies (nodes), together with their fitness and scent values, are produced at random. The algorithm begins the iteration phase after completing the initialization step. Butterflies' keep moving to new locations throughout iterations for selecting CHs, after which their shortest distance values are calculated. In the algorithm, all butterfly fitness values are first calculated at various locations in the solution space. Equation (6) will then be used to create aroma where these butterflies are located. The butterfly moves toward the fittest solution (g∗) (optimal nodes) during the global search phase, which is portrayed by equation (6).

$$x_i^{t+1} = x_i^t + (r^2 \times g^* - x_i^t) \times f_i * ECE_W \quad (6)$$

where x_i^t represents solution vectors x_i for ith butterflies in iterations t, g^*implies current best selected nodes in current iterations' solutions. Fragrances of ith butterflies are f_i and $r \in [0,1]$ are random numbers in local searches depicted as equation (7),

$$x_i^{t+1} = x_i^t + \left(r^2 \times x_j^t - x_k^t\right) \times f_i * ECE_W \quad (7)$$

where x_j^t and x_k^t are jth and kth butterflies from selected CHs and when they are from same swarms with $r \in [0,1]$, it implies local random walks. For the best choice of node from the given network, Butterflies can conduct both local and worldwide searches for food and mates. In IBO, the move from common global search to intense local search is made using the switch probability p. Up until the halting requirements are not met, the iteration process is continued. At the conclusion of the iteration phase, the approach produces the best solution with the highest fitness. Node weight is also applied to the IBO method in equation (7) to choose the ideal number of nodes for the arrangement. The IBO algorithm focused to improve the routing process using optimal selections of CHs. By minimizing the distance among two sample distributions, an optimization issue is solved, and the best probability distribution parameters are then obtained. This technique is known as cross entropy (CE). The CE approach provides high robustness, excellent adaptability, and good global search capabilities.

$$CE = \frac{1}{N}\sum_{i=1}^{N} I_{S<r} \frac{f(x^i, v)}{g(x^i)} \quad (8)$$

here x^i signifies random samples from $f(x; v)$ with consequent sampling densities $g(x)$. The cross-entropy is used to calculate the distance between two sampling distributions and to define the optimal significance sampling density, which is known as the Kullback-Leibler divergence.

Algorithm 1 shows the general stages of the proposed IBO algorithm. The number of nodes in the selected network is used to build the initial populations in Step 1 of the Algorithm 1, and the stimulus intensity I_i at $x_i$is determined in Step 2 based on sensor modalities c and power exponents a in in Step 3 of the algorithm. These variables are generated using the shortest distance. Next, halting conditions are determined (Step 4), following which each butterfly in the network's network has its scent value determined (Step 6). Next, choose the population's top node (Step 8), and finally, generate r at random (Step 10). Use equation (7) If $r < p$ to travel toward the best butterfly; else, move randomly. Step 17 involves updating a value, and Step 18 involves evaluating people in light of their new positions. Lastly, use the end while command (Step 19) to finish the procedure. The flowchart of the suggested IBOsystem is illustrated in Fig 2.

https://doi.org/10.56294/sctconf2023593

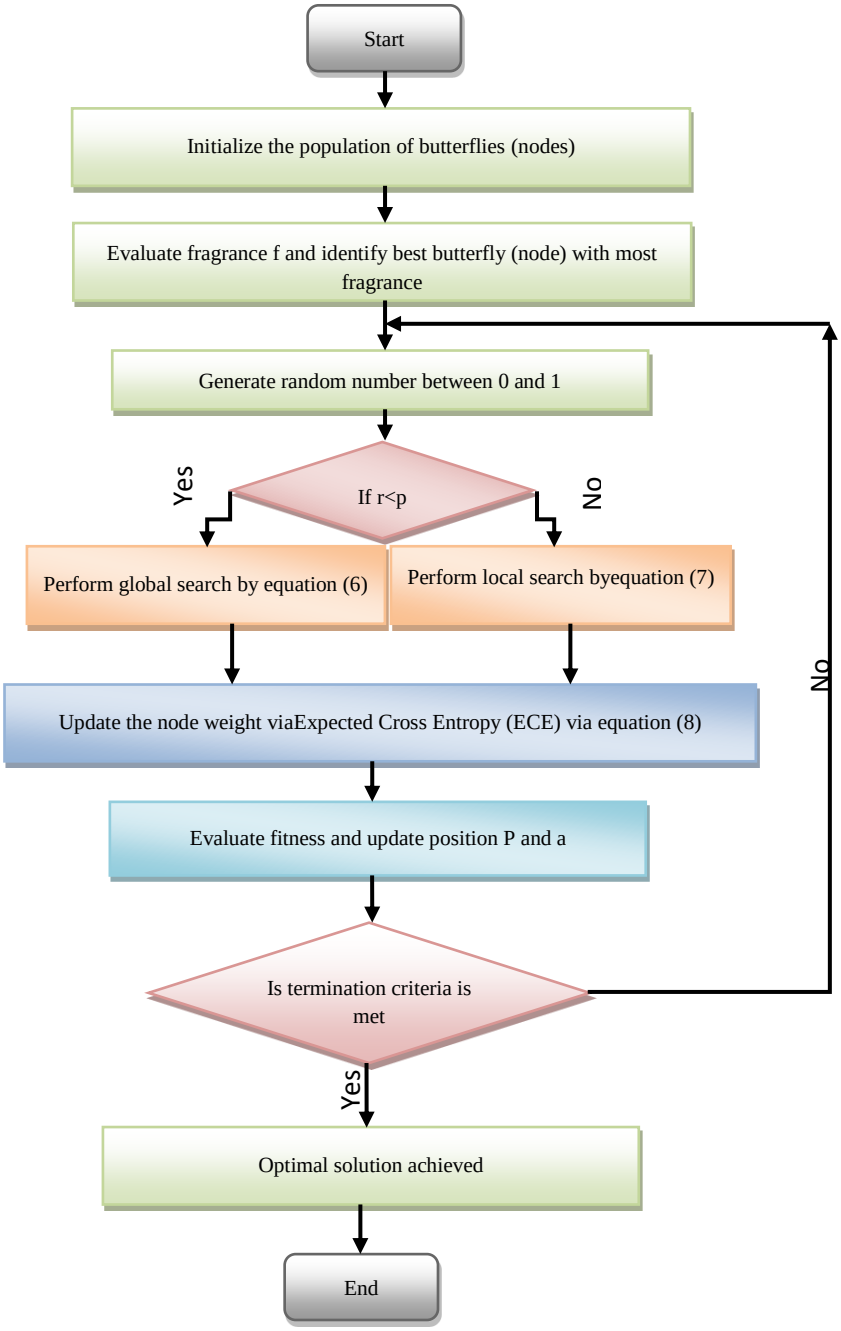


Figure 2. Flowchart IBO algorithm

Algorithm 1: IBO Algorithm
Input: WSN with number of sensor nodes
Objective function:minimum delay, minimum energy consumption and maximum throughput metrics with selected nodes
Output: Selection of optimal CH nodes
1. 1.1 Use the number of network nodes to generate the initial population of n butterflies, x_i=(i=1,2,...,n).
2. Stimulus Intensities I_i at x_i
3. Specify sensor modalities c, switch probabilities p and power exponents a

https://doi.org/10.56294/sctconf2023593

4. Do while stopping requirements are not fulfilled,
5. For butterflies f in population do
6. Assess fragrances for f using (3) and generate weights using equation (8) for entropies
7. End for
8. Find best butterflies (CHs)
9. For butterflies f in populations do
10. Spawn random numbers r
11. If $r < p$ then
12. Use Equ. (6) to direct movements towards best butterflies (optimal nodes), and using equation (5) spawn entropy weights
13. Else
14. Move in a randomized manner using equation (7)
15. End if
16. End for
17. Update values for a
18. Investigate nodes in terms of new locations
19. End while

Shortest path routing based secured data transmission using Double key based Advanced Encryption Standard (DAES) algorithm

In this study, the secured data transmission is carried out using DAES algorithm. AES rest on the principle of design called replacement network.[17] The blocks and keys can be selected from sets of 128, 160, 192, 224, or 256 bits. AES can only handle keys with a block size of 128 bits and one of three different key lengths: 128, 192, or 256 bits, according to the AES standard. Depending on whatever version is in use, the standard's name is modified to AES-128, AES-192, or AES-256. The data block's two halves are first utilized to alter the other half, and then they are switched. Permutations and replacements are utilized in this illustration to process the entire data block concurrently during each cycle. To improve the key size and shift operations, DAES algorithm is proposed

Keyword Generation

For this task, generating an AES encryption key is a significant process for encryption purposes. The key size for encryption is the same as the size of the entry. Here, the 16-byte encryption key is used in the proposed system for the purpose of encryption. The 16-byte keys are arranged in the format of the 4x4 matrix displayed below.

$$\text{Key}=\begin{matrix} k0 & k4 & k8 & k12 \\ k1 & k5 & k9 & k13 \\ k2 & k6 & k10 & k14 \\ k3 & k7 & k11 & k15 \end{matrix} \qquad (9)$$

Generally speaking, there are several stages to the AES algorithm's process of encrypting the input data file. Additionally, this is an iterative block cypher with changeable key lengths and 128 block sizes. States are intermediate products that are impacted by various transformations. The state resembles a rectangle collection of bytes in essence. The following table shows that if the block is 16 bytes in size, the rectangular array is 4 by 4.

Block size of the AES algorithm

b0	b1	b2	b3	b4	b5	b6	……	b15

The arrangement of the input files is in 4 x 4 as showed below. The first four-byte of the input is

https://doi.org/10.56294/sctconf2023593

$$\begin{matrix} b0 & b4 & b8 & b12 \\ b1 & b5 & b9 & b13 \\ b2 & b6 & b10 & b14 \\ b3 & b7 & b11 & b15 \end{matrix} \quad (10)$$

The state only performs small sets of operations in rounds where tasks include:

- Sub-bytes
- Shift row
- Mix column
- Add round key

Sub-bytes operation

Subbyte operations are non-linear byte substitutions that work independently for every byte of report. The S-Box is reversible and is built using two transformations.

Round-based Shift operation

The following actions are carried out during this typical shift row operation,

- 1st row to 0 positions to the left
- 2nd row to 1 position to the left
- 3rd row to 2 positions to the left
- 4th row to 3 positions to the left

Normally, for 128 bits, the AES algorithm performs the operation in 10 turns. Here, the new system has been ameliorated by altering the shift operation. Each turn, the sub-byte operation is performed first. The next step is a round-based shift operation. The suggested approach determines if the number of turns is odd or even for each turn. The row shift transforms operate on the rows in the state table if the number of rounds is seven. The row shift transform travels to two different locations in the matrix if the number of rounds is even. Operation of the gear shift is depicted in figures 3 and 4.

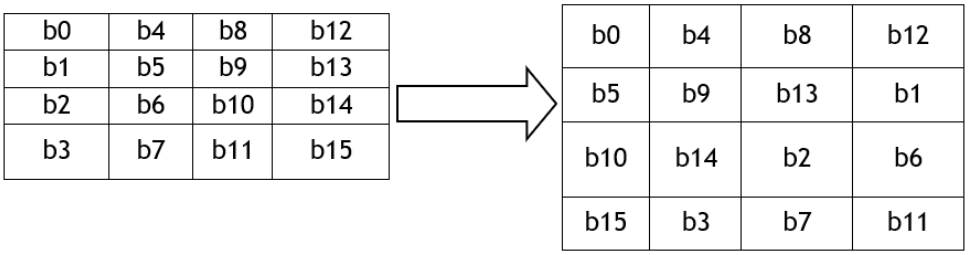


Figure 3. Shift Operation for odd

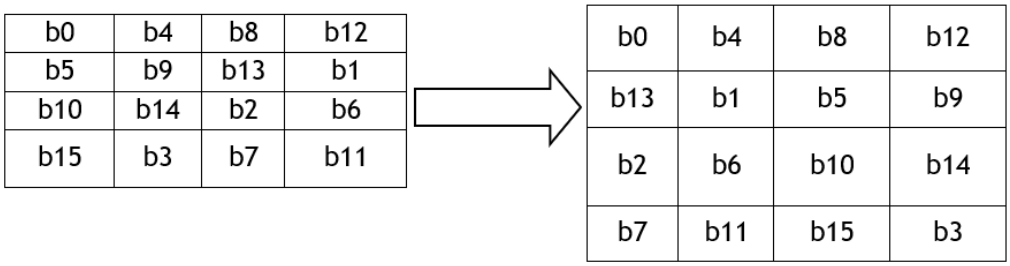


Figure 4. Shift Operation for even

Mix-column operation

The latest mathematical calculations are used by mix column operations.

https://doi.org/10.56294/sctconf2023593

Add round key

With the addition of the round key, the group key is used for reporting by XOR at the bit level. The circular solution can be attained from the encryption key with a key program.

Here, to enhance multipath data transmission and attack detection over WSN, the AODV algorithm was developed. The suggested method prevents message rebroadcast from source node and does not result in connection failure issues. In AODV algorithm, during the evaluation process,The multipath route is chosen together with nodes with lower energy usage. The node with the lowest energy use, lowest delay, higher network lifetime, and highest throughput is chosen using this method. Efficiently distributes the data packet between generated paths. The AODV protocol uses enhanced metrics to choose best multi-paths where best CHs are used. This situation prominently results in a considerable increase in node energy and multipath routing.

The AODV protocol is designed to increase the efficiency of WSNs by enhancing multipath data transfer using route discovery and maintenance functions. By generating routes on demand, it lowers the volume of transmissions. When a source needs to broadcast data, this protocol checks the route table.[18] A distance vector protocol with a single path and no loops called AODV is according to hop-by-hop routing. In AODV, there are two primary procedures:

- Route discovery
- Route maintenance

Route Discovery: In order to find the path to the destination, the source broadcasts an RREQ packet in the direction of the destination, which responds by broadcasting an RREP packet. The RREP then takes the same path that the RREQ did before and adds this to its database of routes. The two routing tables that are present on each node are the Primary Routing Table (PRT) and Alternate Path Routing Table (ART). For each destination node, a different PRT entry is used. PRT denotes any item in node X's routing table for any destination D.

Route Maintenance: The process of route maintenance begins whenever a route failure is discovered on the route. When a route failure is discovered on the active path, the process is started.

Algorithm 2: AODV protocol for attack detection

Start
Generate WSNs with 100 nodes
Construct clusters
Choose the CH node from among the cluster members.
Data packets are sent from the cluster member to the CH node.
Start the route discovery and maintenance procedure for the multipath route.
Start the data transfer if the route in the routing database is legitimate.
Else
Launch route explorations
Recognise the assaults
Create backup route
Transmit the number of packets through backup route
Return all possible paths
Select best multiple routing paths
Apply DAES algorithm
Ensure secured data transmission
Continue to data transfer
Stop

The above Algorithm 2 describes that the best multiple routing path selection is achieved using optimal parameters. The protocol can handle topology and routing information because of on-demand route

https://doi.org/10.56294/sctconf2023593

discoveries, hop-by-hop routes, maintenance of routes and using sequential node numbers. The attack detection is done optimally which improves secured data transmission in WSN. By sharing numerous information based on minimum distance, the bandwidth, and energy consumption together with multiple routes, AODV is highly effective for getting the routes solely on demand, and WSN nodes are working collaboratively as well as effectively. The best multiple routes are chosen by the AODV using the best CHs for multi-path routes using improved metrics.

RESULT

Here, the efficiency of the recommendedIBO-DAEStechnique is assessed and compared with otherapproaches such as EGSCFO (Evolutionary Game based Secure Clustering protocol with Fuzzy trust evaluation and Outlier) detections,[19] TKFCC (Taylor Kernel Fuzzy C-means Clustering) [20] and WRDA (Weight Red Deer Algorithm) algorithms. In Table 1, the simulation parameters are listed and this work is simulated on NS-2 tool. The present and suggestedapproaches are compared according to throughput, energy consumption, data transfer rate and network lifetime

Table 1. Simulation parameters

Parameter	values
No. of Nodes	100
Area Size	1100 * 1100(Meter)
Mac	802,11
Total energy	150 Joule
Initial value of energy	1,5 Joule
Radio Range	250m
Simulation Time	60 sec
Packet Size	80 bytes

Throughput

Throughputs are rates at which data packets are transmitted in network's communications.

$$Throughput = total\ number\ of\ packets\ sent\ /time \quad (11)$$

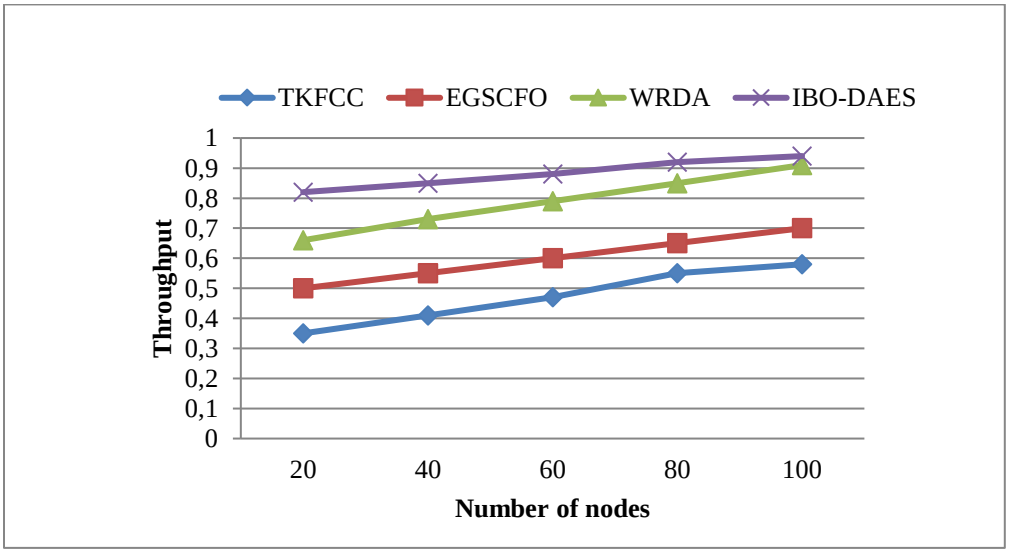


Figure 5. Throughput comparison

Figure 5 demonstrates the comparison between the existing TKFCC, EGSCFO, WRDA and IBO-DAES methods for the throughput metric. In the x-axis number of nodes is taken and in the y-axis throughput metric is taken. The suggestedIBO-DAES method is utilized to determine and select the CH nodes

https://doi.org/10.56294/sctconf2023593

effectively in WSN. This helps to accurately gather and transmit the secured data in different node without any information loss. It demonstrates that the previous TKFCC, EGSCFO, WRDA approaches whereas the suggested IBO-DAES offers a better throughput.

Energy consumptions

"Energy consumptions" refer to energies used over a period of time for packet transmissions, receptions, or forwards by networks' nodes.

$$Energy\ (e) = [(2 * pi - 1)(e_t + e_r)d \quad (12)$$

Where pi is the data packet, e_t is the energy for transmission of packet i, e_r is the energy for receiving the packet i and d is the distance among transmission and destination node

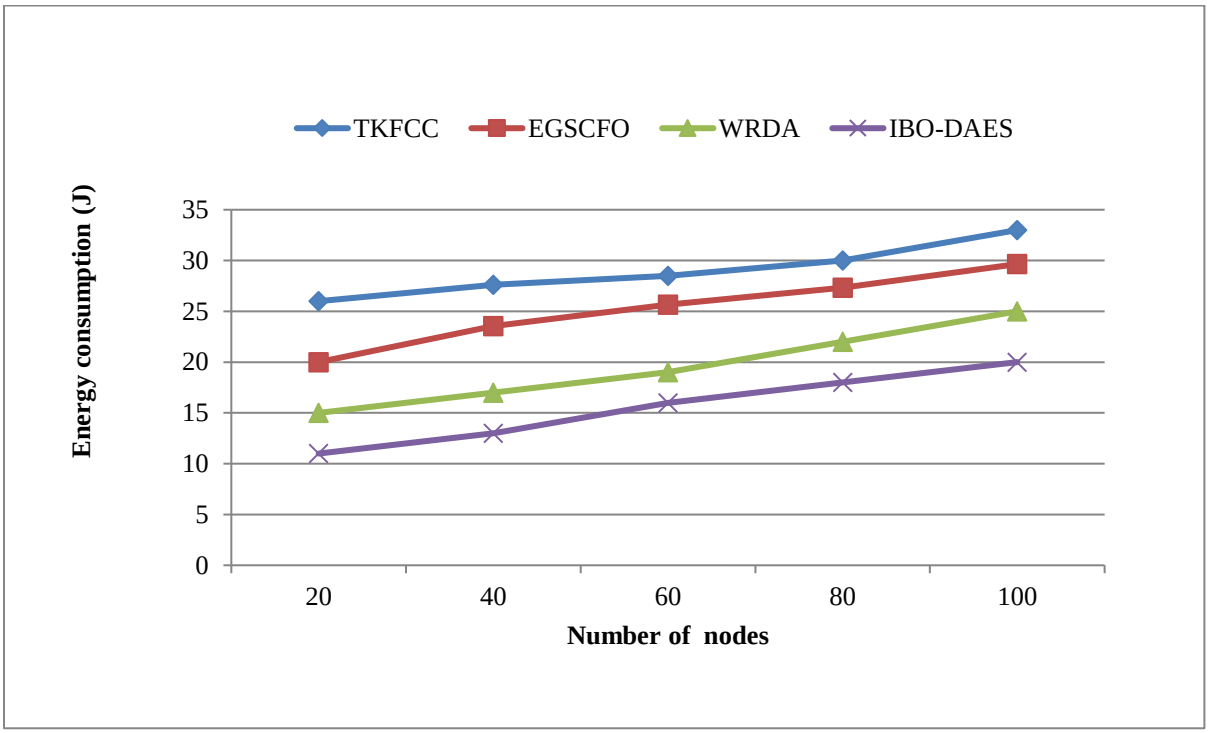


Figure 6. Energy consumption comparison

The energy consumption of the existing TKFCC, EGSCFO, WRDA, and created IBO-DAES techniques was compared using figure 6. The x-axis measures the number of nodes, while the y-aximetes measures the energy consumption metre.When transmitting data packets over the WSN, the IBO-DAES algorithm significantly decreases energy consumption. This is since non-CH nodes in IBO can join benign clusters with the maximum probability, reducing the likelihood that they will waste energy because their data packets will most likely be sent to the base station on time. It indicates that the IBO-DAES technique uses less energy than the more energy-intensive conventional techniques.

Network lifetime

When the optional solution increases network longevity, the system is considered optimal.

$$Lifetime\ \mathbb{E}[L] = \frac{\varepsilon_0 - \mathbb{E}[E_w]}{P + \lambda \mathbb{E}[E_r]} \quad (13)$$

where P are networks' consistent continuous power consumptions, λ implies averages of sensor report rates,ε_0 refers to total non-rechargeable initial energies, $\mathbb{E}[E_w]$ is the expected wasted energy or unused energy when the network dies and $\mathbb{E}[E_r]$ is the expected reporting energy used by all sensors

https://doi.org/10.56294/sctconf2023593

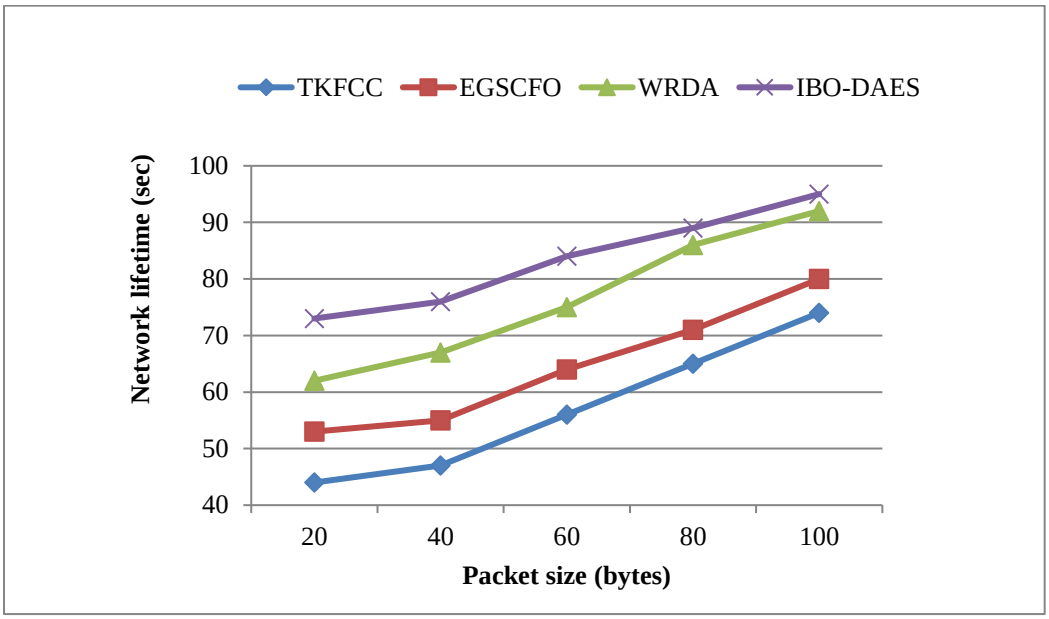
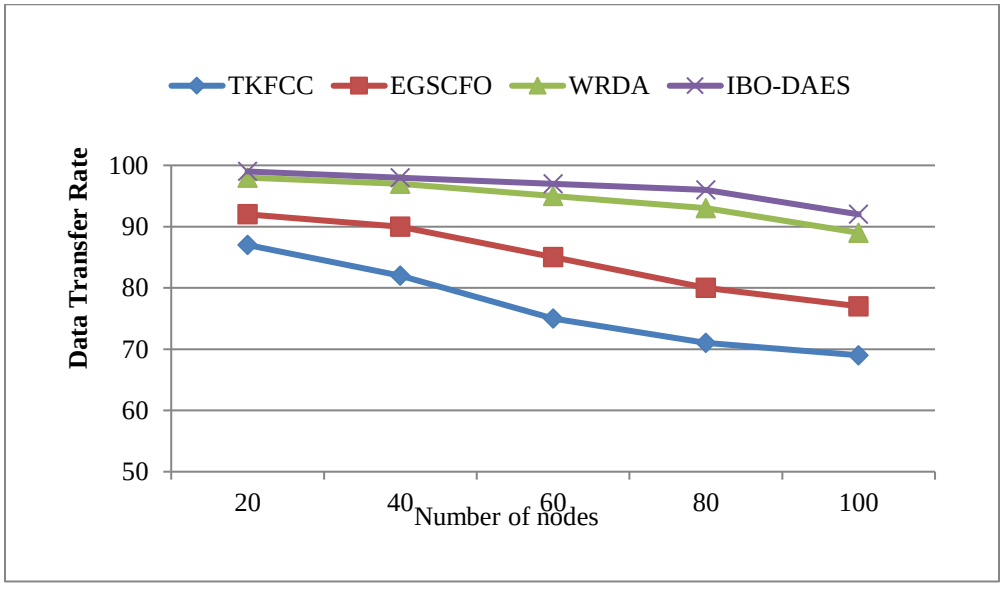


Figure 7. Network lifetime

Network lifespan of specific packet sizes are shown in Fig. 7. Nodes counts are depicted on x-axis, and corresponding network lifetime are y-axis values. The suggested IBO-DAES technique considerably extends the lifetime of the sensor node during data packet transmission. The IBO algorithm was used to transmit CH-based data. Additionally, it has been found that the optional technique lengthens the network lifetime as packet sizes grow. It demonstrates the suggested IBO-DAES gives a longer network lifetime.

Data Transfer Rate

The quantity of data that is sent from one location to another in a certain period of time is known as the data transfer rate. The speed at which a certain amount of data is sent from one location to another is known as the data transfer rate. In general, the bandwidth of a specific route grows with the data transmission rate.[21,22]



https://doi.org/10.56294/sctconf2023593

Figure 8. Data transfer rate

From the above figure 8, it can observe that the comparison of existing TKFCC, EGSFO, WRDA and proposed IBO-DAES in terms of data transfer rate. In x axis the number of nodes and in y axis the data transfer rate values are plotted. In the current situation, the data transfer rate values are lower by using TKFCC, EGSFO and WRDA methods. In suggested technique, the data transfer rate value is increased significantly by using the proposed IBO-DAES. Thus it shows that efficient and secured data transmission in WSN is performed by using proposed IBO-DAES method.

CONCLUSION

The recommended IBO-DAES technique is employed in this study to secure data transmission via WSN while optimising the choice of CH nodes. The best method for selecting CH nodes is considered to be the IBO algorithm. The most effective CH node is chosen based on fitness measures. The optimum outcome is achieved when selecting a CH node by considering the fitness function and the remaining energy, throughput, and end-to-end delay. The AODV protocol is designed to enhance the efficiency of WSNs by utilizing route discovery and route management functions to better secured multipath routing data delivery. DAES+AODV protocol avoids the attack nodes and therefore the packet loss is reduced prominently. DAES algorithm provides secured data transmission via modified shift operation and AODV protocol improves WSN performance. As an outcome, the suggested IBO-DAES methodology outperforms current techniques in terms of throughput, data transfer rate, network lifetime, and energy usage. Future research may examine how well the suggested model performs in an IoT network. Additionally, hybrid swarm optimization and a unique encryption technique can be created to deal with the problems associated with computational complexity.[23,24]

REFERENCES

1. Yang, Liu, et al. "An unequal cluster-based routing scheme for multi-level heterogeneous wireless sensor networks." Telecommunication Systems 68 (2018): 11-26.

2. Yang, Guisong, et al. "Global and local reliability-based routing protocol for wireless sensor networks." IEEE Internet of Things Journal 6.2 (2018): 3620-3632.

3. Thakkar, Ankit, and Ketan Kotecha. "Cluster head election for energy and delay constraint applications of wireless sensor network." IEEE sensors Journal 14.8 (2014): 2658-2664.

4. Saleh, Nayif, Abdallah Kassem, and Ali M. Haidar. "Energy-efficient architecture for wireless sensor networks in healthcare applications." IEEE Access 6 (2018): 6478-6486

5. Fu, Xiuwen, et al. "Environment-fusion multipath routing protocol for wireless sensor networks." Information Fusion 53 (2020): 4-19.

6. Raghavendra, Y. M., and U. B. Mahadevaswamy. "Energy efficient routing in wireless sensor network based on composite fuzzy methods." Wireless Personal Communications 114.3 (2020): 2569-2590

7. Ayadi, Hayfa, et al. "Network lifetime management in wireless sensor networks." IEEE Sensors Journal 18.15 (2018): 6438-6445

8. Elshrkawey, Mohamed, Samiha M. Elsherif, and M. ElsayedWahed. "An enhancement approach for reducing the energy consumption in wireless sensor networks." Journal of King Saud University-Computer and Information Sciences 30.2 (2018): 259-267

9. Tabibi, Shamineh, and Ali Ghaffari. "Energy-efficient routing mechanism for mobile sink in wireless sensor networks using particle swarm optimization algorithm." Wireless Personal Communications 104.1 (2019): 199-216.

10. Ñope EMG, Claudio BAM, Ruiz JAZ. The Service Quality of a Feed Industry Company. Southern Perspective / Perspectiva Austral 2023;1:9–9. https://doi.org/10.56294/pa20239.

11. Jeronimo CJC, Basilio AYP, Claudio BAM, Ruiz JAZ. Human talent management and the work performance of employees in a textile company in Comas. Southern Perspective / Perspectiva Austral 2023;1:5–5. https://doi.org/10.56294/pa20235.

12. Mahajan, Shilpa, Jyoteesh Malhotra, and Sandeep Sharma. "An energy balanced QoS based cluster head selection strategy for WSN." Egyptian Informatics Journal 15.3 (2014): 189-199

13. Saidi, Ahmed, Khelifa Benahmed, and Nouredine Seddiki. "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks." Ad Hoc Networks 106 (2020): 102215

14. Han, Guangjie, et al. "Intrusion detection algorithm based on neighbor information against sinkhole attack in wireless sensor networks." The Computer Journal 58.6 (2015): 1280-1292

15. Dionicio RJA, Serna YPO, Claudio BAM, Ruiz JAZ. Sales processes of the consultants of a company in the bakery industry. Southern Perspective / Perspectiva Austral 2023;1:2–2. https://doi.org/10.56294/pa20232.

16. Velásquez AA, Gómez JAY, Claudio BAM, Ruiz JAZ. Soft skills and the labor market insertion of students in the last cycles of administration at a university in northern Lima. Southern Perspective / Perspectiva Austral 2024;2:21–21. https://doi.org/10.56294/pa202421.

17. Abikoye, Oluwakemi Christiana, et al. "Modified advanced encryption standard algorithm for information security." Symmetry 11.12 (2019): 1484

18. Chan, Wai Hong Ronald, et al. "Adaptive duty cycling in sensor networks with energy harvesting using continuous-time Markov chain and fluid models." IEEE Journal on Selected Areas in Communications 33.12 (2015): 2687-2700

19. Arora, S. and Singh, S., 2019. Butterfly optimization algorithm: a novel approach for global optimization. Soft Computing, 23(3), pp.715-734.

20. Tubishat, M., Alswaitti, M., Mirjalili, S., Al-Garadi, M.A. and Rana, T.A., 2020. Dynamic butterfly optimization algorithm for feature selection. IEEE Access, 8, pp.194303-194314

21. Panda, Madhumita. "Data security in wireless sensor networks via AES algorithm." 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO). IEEE, 2015

22. Zhang, De-gan, et al. "Extended AODV routing method based on distributed minimum transmission (DMT) for WSN." AEU-International Journal of Electronics and Communications 69.1 (2015): 371-381

23. Yang, Liu, et al. "An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks." IEEE Sensors Journal 21.12 (2021): 13935-13947.

24. Augustine, Susan, and John Patrick Ananth. "Taylor kernel fuzzy C-means clustering algorithm for trust and energy-aware cluster head selection in wireless sensor networks." Wireless Networks 26 (2020): 5113-5132.

FINANCING

The authors did not receive funding for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: A. Prakash, M. Prakash.
Research: A. Prakash, M. Prakash.
Writing-original draft: A. Prakash, M. Prakash.
Writing-review and proof editing: A. Prakash, M. Prakash.