Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network

P. Dinesh Kumar & K. Valarmathi

To cite this article: P. Dinesh Kumar & K. Valarmathi (2023) Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network, Automatika, 64:2, 199-210, DOI: 10.1080/00051144.2022.2119502

To link to this article: https://doi.org/10.1080/00051144.2022.2119502

Published online: 16 Sep 2022.

AUTOMATIKA
2023, VOL. 64, NO. 2, 199–210
https://doi.org/10.1080/00051144.2022.2119502

Taylor & Francis
Taylor & Francis Group

REGULAR PAPER

OPEN ACCESS Check for updates

Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network

P. Dinesh Kumar[a] and K. Valarmathi[b]

[a]Department of Information Technology, V.S.B. College of Engineering Technical Campus, Coimbatore, India; [b]Department of Electronics and Communication Engineering, P.S.R. Engineering College, Sivakasi, India

ABSTRACT

Nodes are deployed randomly in the network area of the WSN. data transmission from source to destination via intermediate nodes should be done in a secure fashion. Due to the large size of packet loss and energy consumption of sensor nodes, a secure and energy-efficient path must be required. The main objective of this research is to provide secure data transmission among node-to-node for efficient delivery of data packets to the destination. The system uses a novel hybrid firefly and BAT algorithm for path selection, an innovative trust value generation, and optimal neighborhood selection using fuzzy logic. The research employs Elliptic Curve Cryptography (ECC) combined with Diffie-Hellman exchange for key generation and key exchange. Path selection is done by fuzzy logic and optimization of selection has been carried out by hybrid BAT and Firefly algorithms. Key generation includes a time-based randomness factor that increases the complexity of cryptanalysis, thereby providing the most security. The performance of the simulation is analyzed and depicted in terms of delay, throughput, energy, and processing time. The research has been carried out using a network simulator with nodes deployed randomly in the network area with mobility as the primary concern that requires dynamic path selection.

ARTICLE HISTORY
Received 2 December 2021
Accepted 26 August 2022

KEYWORDS
WSN; firefly and BAT algorithm; fuzzy logic; security; path selection; ECC; and diffie-hellman

1. Introduction

Wireless Sensor Network (WSN) is a group of nodes/devices that are connected as a network that can transfer and share the data collected from an environment via intermediate links. In such a scenario, security is the significant factor to be considered for the transmission of data. Security, Computation, Privacy, Reliability, and Energy constraints are the several challenges to be taken into account mainly at the time of routing in WSN [1–5]. Various researchers suggested a clustering algorithm based on Particle Swarm Optimization (PSO) for WSNs with mobile sinks. Many simulations have been undertaken to determine the system's productivity. The results have shown that the system is found to be efficient in terms of network lifetime, energy consumption, and transmission delay. The research reduced the node's energy consumption, improved network lifetime, and reduced transmission delay using hybrid BAT and Firefly algorithms [6–8]. The research work, utilized LEACH along with an enhanced BAT algorithm (BA) to decrease the energy cost of the system in WSN. The performance analysis has shown that the system is more effective than the other state-of-the-art methods in improving the network lifetime and reducing energy consumption. Modified BA has to be employed yet for related problem optimization [9–11].

The research work used a dual assurance scheme and a two-stage security mechanism for the identification and prevention of attacks including selective forwarding and black hole attack with active trust in a clustered WSN. It has been observed that this research has established the trust path thereby providing data transmission in a secured manner. Several experiments have been performed and the results revealed that the system guarantees network lifetime in a prolonged manner and a high probability of secure routing in WSN [12–15]. To aggregate various types of data packets and increase energy efficiency, FAJIT primarily focuses on solving the parent node selection problem [16]. The distribution-adaptive protocol TTDFP is effective at running and scaling sensor network systems. An optimization framework to fine-tune the parameters utilized in the cluster analysis tier to optimize the performance of a particular WSN in addition to the two-tier protocol based on fuzzy logic [17]. The foundation of a Wireless Mesh Network (WMN), when a mesh router's mobility is limited, is made up of mesh clients and routers [18]. Spam frequently floods the network with extra versions of the same message that are continually delivered to different users without their permission or encouragement to open them. In this study, we compare the effectiveness of various machine learning methods even without feature selection methods to find the most

CONTACT P. Dinesh Kumar dineshkumarpphd12@gmail.com Assistant Professor, Department of Information Technology, V.S.B. College of Engineering Technical Campus, Coimbatore

accurate classifier for identifying spam mail [19]. The research employed the firefly algorithm in addition to adaptive PSO for secure routing based on the cluster in WSNs. The research has been evaluated using the NS3 simulation tool. Various metrics have been taken into account for evaluation. The metrics include decryption and encryption time, network lifetime, and Packet DropRate (PDR). Performance analysis of this research exhibits that the system performed and sustained better than the other conventional methods. This research has been planned to enhance further by executing it in a large-scale environment of WSN [20]. The research creates a Hybrid method of Firefly Algorithm with Particle Swarm Optimization (HFA-PSO) in WSN for cluster head selection in an optimal and energy-efficient manner. The research work has been assessed in terms of metrics including residual energy, number of alive nodes, and throughput. The attained results revealed that the proposed methodology enhanced the lifetime of the network and decreased the utilization of energy. Comparative analysis of various parameters has shown that the system accomplished better residual energy and throughput. The network lifetime has to be improved further by the use of nature-inspired algorithms and firefly algorithm [21]. The demand that WSNs have minimal deployment and manufacturing costs mandates the use of simple equipment in the sensor network.

As a result, academics have begun to look for solutions in this new field. An important feature of WSN security is described in this work. A variety of encryption techniques are investigated, including symmetric and public keys, as also Elliptic Curve Cryptography (ECC), Pairing Basis Cryptography (PBC), and Identity Based Cryptography (IBC). Because information is delivered across an unpredictable connection, information security is a key priority in every sector. Cryptographic techniques aid in the transformation of comprehensible data into incomprehensible data. Asymmetric keys and usually indicators are two major techniques of cryptography. The symmetric key employs only one secret for both encrypting and decrypting, which saves time and energy. The asymmetrical key is made up of 2 keys: a secret key for decryption and a public key for encryption. Since it uses two keys, the asymmetric encryption approach is substantially safer than the symmetrical approach. The production of two keys requires a lot of energy, time, and memory. Block and stream ciphers are two types of cryptographic techniques.

Three new innovative ideas have been presented in this to overcome the higher energy consumption, throughput, and lower network lifetime. The major contributions of the proposed work are the following:

Trust value generation and neighborhood selection using fuzzy logic, hybrid firefly and bat algorithm, and ECC with Diffie Hellman for secure transmission is the innovative ideas explored in this research. Trust value is generated to ensure trustworthy communication between various nodes in WSN.

Fuzzy logic is utilized to enhance decision-making and performance and decreases the consumption of resources. Here, Fuzzy logic is used for neighbor discovery based on historic information of the particular node. This historic information is analyzed to choose the efficient neighboring node. In addition, fuzzy logic also analyses the distance and energy of the node. Finally, an optimized path is selected via the Hybrid firefly and Bat algorithm.

The Hybrid firefly and Bat algorithm initializes the population and calculates intensity and fitness value to choose the best suitable path for data transmission. This optimized path provides secure data transfer from the source node to the sink node.

The strength of this research lies in providing effective ideal neighborhood discovery using Novel fuzzy-based optimal path selection with randomness (FPS-R) and finalization of the optimized path using a hybrid firefly and BAT algorithm (H-FBA).

The research work ensures integrity, availability, confidentiality, and authenticity of all packets in the existence of resourceful adversaries.

The upcoming section II describes several existing works about the secure transmission of data from the source node to the destination node in WSN. Section III describes the research methodology in which a novel hybrid firefly and bat algorithm, trust value generation and neighborhood selection using fuzzy logic has been implemented for secure data transmission. The results of the research work have been discussed in section IV. Finally, the entire proposed system is concluded in section V.

2. Related work

The following section describes the existing studies related to path selection approaches among the nodes and various optimization algorithms employed in wireless sensor networks.

The research compared and examined various data aggregation methods based on artificial intelligence (AI) in Wireless Sensor Networks (WSNs). Additionally, this study included the design and development of an enhanced protocol. An analysis has been made by comparing this protocol implementation with Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO). The results thus obtained from the comparative analysis showed that the proposed method guaranteed better results concerning throughput and network lifetime. Meta heuristic and AI-based methods can be used to surpass the current issues in WSN during data aggregation, which has to be done in near future [22]. In addition, [23] utilized a two-fish approach based on a novel hybrid routing algorithm in WSN to choose the right path for the safe transmission of messages from source to destination. Simulations have been carried out to assess the performance of the proposed work. Simulation results have shown that the proposed methodology showed better results in terms of monitoring and detection ratio for malicious attacks. The proposed method has to be extended further to be utilized in WSNs to assuring the authentication of security layers. Employed [24] interlock protocols and RSA cryptographic algorithm to prevent Denial-of-Service attacks for securing WSN. Simulations have been undertaken using the NS2 tool. Results obtained from simulation have shown that the proposed algorithm and protocol are found to be effective in terms of various metrics such as Packet Delivery Ratio (PDR), average throughput, average residual energy, detection ratio, and network lifetime. The research can be further improved by utilizing mobile sinks based on meta-heuristic algorithms for enhancing the network lifetime and energy consumption.

Furthermore, the research proposed an Effective Path Selection and Security Control Logic Scheme (EPSSCLS) and Dynamic Authentication Key Agreement Scheme (DAKAS) for secure data transmission and key verification in WSN. The results showed that the proposed method performed better in improved security in WSN [25]. The system used the jumper firefly algorithm for energy-efficient clustering in WSN. The proposed methodology has also been compared with the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol which is one of the existing systems in which the proposed algorithm exhibited better results than the LEACH protocol. The hybrid Optimization method has to be implemented in WSN for clustering in near future [26].

The research exploited an MFA (multi-population firefly algorithm) in WSN for correlated data routing. Simulation has been undertaken and many existing methods have been compared with the proposed system by various metrics that includes energy consumption, packet delivery ratio, and network throughput. Thus, the proposed technique MFA has outperformed more efficiently than other traditional methods in terms of the mentioned metrics [27]. This study discussed a symmetric cryptography algorithm called Advanced Encryption Standard (AES) for the security of WSNs. Various findings revealed that the proposed methodology performs efficiently in WSNs. Further research has to be carried out regarding the execution of cryptographic circuit structures [28]. The research implemented a synchronous firefly algorithm in WSN for cluster head selection. Various simulations have been conducted to assess the effectiveness of the proposed method. The simulation results have shown that the proposed method outperformed other conventional methods by enhancing the network's energy efficiency and reducing the packet loss ratio [29]. Employed DHM (Dij-Huff Method) in WSNs for path optimization in an energy-efficient and secure manner. A network simulator has been used to validate the proposed approach. The simulation results have exhibited that the proposed method decreases the packet delay and loss thereby enhancing the network lifetime [30]. Utilized an algorithm called artificial bee colony in WSNs for path optimization based on the mobile sink. The proposed system has been simulated to examine its efficiency and effectiveness. The simulation results revealed that the proposed system has shown effective results in the performance of data collection in real-time and energy efficiency. Various study has yet to be conducted related to the strategy of mobile sink [31].

This research reviewed Ant Colony Optimization (ACO) algorithm for mobile and static sensor networks based on AI for path selection in an empowered manner. The research work has been summarized and various open challenges about the network design have been explored. The research contributes to the guidance of system design and enhancement in the performance of networks. Large transmission delay is a drawback in this study [32]. Proposed a Novel Fault Tolerance (NLFFT) model based on AI to enhance the performance of WSNs. The proposed model has been found to exhibit enhanced performance concerning end-to-end delay, throughput, and power consumption. Here, the proposed model has been employed only for the sensor nodes that have been statistically deployed. The work has to be expanded further by employing the proposed model in sensor nodes that have been dynamically deployed [33]. Employed ECC (Elliptic Curve Cryptography) based on mutual authentication for the secure transmission of medical data in WSNs. The results have revealed that the proposed methodology solved all the existing problems and was verified to be the efficient cryptographic technique for the safe transmission of data in an environment with resource constraints. Investigators can develop a new method to decrease the computation of the proposed method in the near future [34]. The study suggested a TDP (Trust Disrupt Protocol) for energy-aware and secure routing protocol in WSNs. The proposed method has been tested in Self-Organizing Networks (SON). A comparative analysis of the proposed system with the existing LEACH protocol has been performed. The proposed method showed better efficiency than the traditional methods for routing in WSN in terms of reduced energy consumption and high security. Further improvement has to be done by utilizing an agent-based system instead of cluster-based routing in the routing of WSN [35].

The research proposed an improved BAT algorithm through the use of a diversity function for the optimization of routing in WSN. Simulation has been conducted using the NS2 tool where the traditional BAT algorithm and the improved BAT algorithm have been compared to determine the efficiency of the system. Results have been summarized by taking into account the various metrics of end-to-end delay, PDR, etc. The results have revealed that the proposed Improved BAT algorithm performed well than the traditional BAT method in terms of the mentioned metrics. Implementation of QoS has to be done yet with the BAT algorithm [36]. Recommended MDF (Multisensor Data Fusion) approach for choosing the suitable path in WSN by the integration of the gathered network metrics such as centrality and bandwidth. Many simulations have been implemented and the results obtained from the simulation of the proposed method showed efficient performance when compared with other state-of-the-art methods. Application development has to be implemented in near future regarding the real-time issue through the use of the proposed method [37].

This research exploited Homomorphic encryption and ECC for safe data routing in WSN. It has been observed that the proposed system can function with various sensing environments that require capturing data in the image as well as textual format. The proposed system exhibited an effective outcome than the traditional methods regarding memory requirements, communication overhead, energy consumption, and network lifetime. It also prevents various attacks such as brute force attack, passive attack, and CH compromised attack [38]. Proposed re-encryption nodes for improvement of energy efficiency based on fuzzy logic for forwarding nodes selection in WSN. Simulation has been conducted to assess the performance of the proposed method. Thus, it has been found that the proposed method accomplishes improved conservation of energy at the en-route nodes. Further study has to be carried out to examine and execute the source authentication at intermediary nodes in a sensor network based on data aggregation [39].

The system suggested an outsourcing decryption method concerning novel partial to assure computational efficiency and data security for terminal equipment and resource-constrained WSNs. The proposed method has been compared with various existing methods. It has been found that the proposed methodology efficiently decrypts cipher text and improves data security. Simulation has also been performed to assess the proposed system's performance. The proposed system showed effective results in computation, and energy consumption when compared to traditional work. Multi-authorities and attribute key revocation for WSN have to be considered in the near future [40]. Recommended an Energy and Spectrum aware Unequal Cluster based Routing (ESUCR) to solve the challenges of routing and clustering in a Cognitive Radio Sensor Network (CRSN). Many simulations have been undertaken using the NS2 tool to determine the performance of the proposed method. The proposed method has also been compared with the existing system and it has been found that the proposed methodology works efficiently in terms of PDR, end-to-end delay, and reduction in energy consumption. The proposed algorithm has to be enhanced further to attain robust performance with adaption to several occupancy models of PU spectrum [41]. In WSN, [42] Proposed TSDDR (Trust-based Secure Directed Diffusion Routing) protocol. The proposed system has been analyzed and it has been found that the proposed TSDDR prohibits the impersonation of malicious attacks. It has also exhibited end-to-end communication securely.

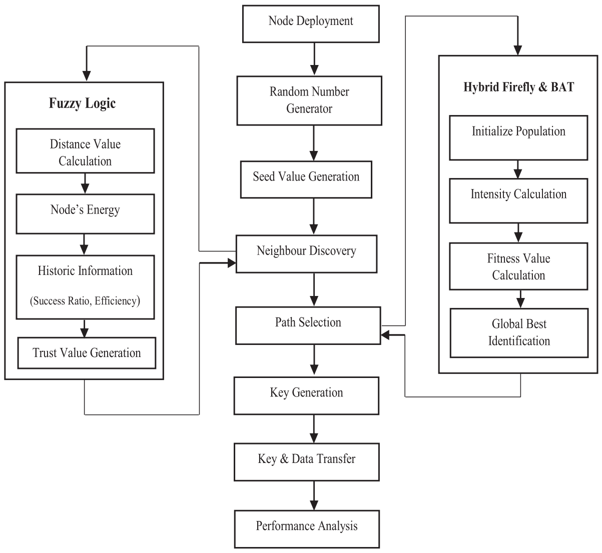


Figure 1. Novel fuzzy-based optimal path selection with randomness (FPS-R) and hybrid Firefly and Bat algorithm-H-FBA.

The foregoing are the shortcomings or drawbacks of WSN: Because it is wireless, it is vulnerable to hacking. Because it is developed for low-speed purposes, this can be utilized for high-speed communications. The cost of constructing such a system is prohibitive for most people.

3. Proposed work

In this research work, for secure path selection, the system proposes a novel fuzzy-based optimal path selection with randomness (FPS-R) to ensure the effective transmission of data. For an effective path selection, a newly formed hybrid firefly and bat algorithm (H-FBA) is developed. The system depends on asymmetric key generation and key exchange using Elliptic curve cryptography (ECC) combined with the Diffie-Hellman technique for providing maximum security. For data encryption, the system utilized ECC which provides integrity, authenticity, and confidentiality. The system uses a no-assumption-based methodology and relies on randomness and cryptographic algorithms to increase its complexity without compromising on security. A unique seed value is generated for each node that has no relevance to its neighbors. As no information is generated in common among sensor nodes, a compromised node produces no effect on its neighboring nodes. A detailed description of the proposed study is shown in below Figure 1.

3.1. Novel fuzzy-based optimal path selection with randomness (FPS-R)

Initially, the proposed system allocates a unique value for every sensor node before deployment. The values thus allocated possess no dependency among themselves. This unique node value is shared with the base station to prevent a masquerade attack. Each node after sensing its own defined value needs to perform a computation for the generation of a unique value called a seed value based on its allocated value. The computation is a modified form of Euler's identity and given below,

$$\begin{cases} 1 \\ S = \sum \lambda^{\alpha R} + 1 \\ i = 100 \end{cases} \tag{1}$$

Equation 1: Seed Value Generation
Where,
S - Seed Value
λ - Node ID
α - Sensed Value
Ŕ - Random value between "n" prime numbers.

Here, a random value is taken from a pool of "n" prime numbers. This value is fed as input for the generation of private keys at sender and receiver. The complexity of the seed value lies in the chosen random prime number and node's sensed value which will be difficult for the intruder to predict and perform the cryptanalytic attack.

Further, Neighbour node discovery is accomplished using a fuzzy rule. For each nearby node, the following are calculated. Node's Distance Value (DV), Node's Energy Level (EL), and Node's Historic Information (HI) - (Success Ratio, Node's efficiency).

3.1.1. Fuzzy logic

Before communicating to the base station every node must be authenticated based on authentication scores from 0 to 1. If a node is not authenticated then it indicates to 0 value and if it is fully authenticated then it indicates to 1 value. If the node is authenticated partially, it indicates the intermediate value. In this research work, the data is encrypted and decrypted and key generation is performed using ECC, and Diffie-Hellman exchange performs the key exchange. The data is allowed to be forwarded to the base station after performing the authentication checks. Fuzzy logic identifies the trustworthy nodes among "n" nodes. Each node calculates its nearby trustworthy nodes using fuzzy logic. The selection of optimal nodes among the identified trustworthy nodes for path selection is done using the Hybrid Firefly and BAT algorithms. The neighbor trust value on success rate and packet sending efficiency are shown in table 1. The trust value of nodes is calculated based on their historic information such as success ratio and efficiency.

Table 1. Neighbour trust value based on success rate and packet sending efficiency.

Distance	
Distance $< \, = 0.5$	High
Distance > 0.5 and Distance $< \, = 0.9$	Medium
Distance $> \, = 1$	low
Energy	
Energy $> \, = \, 0.2$	High
Energy $> \, = \, 0.1$ and energy < 0.2	Medium
Energy < 0.1	Low
Trust value	
Trust value $> \, = \, 0.8$	High
Trust value < 0.8 and Trust value $> \, = 0.5$	Medium
Trust value < 0.5	Low

Instead of precise and fuzzy set concept derivation for reasoning, fuzzy logic is utilized which is a kind of logic with multiple approximate values. Uncertainty is considered a trust-based character within wireless sensor networks due to the prescribed rules and fuzzy verifications. In decision analysis, the logic trust model is established which is focused on uncertainties as probability values. The probability model is not utilized. By fuzzy rules set construction, certain fuzzy trust models handle the indecision in the trust management system. Based on fuzzy logic trust models, the patterns are identified and it follows if and then sequence rules. For moderating the rules of fuzzy logic, the result is evaluated and suitable feedback is obtained.

3.2. Effective and optimized path selection using new hybrid firefly & Bat algorithm-H-FBA

In this research, the firefly algorithm and bat algorithm are combined as a hybrid form to perform the effective path selection.

The flashing (mating) action of fireflies served as inspiration for the creation of the firefly algorithm. Tiny insects called fireflies are skilled at producing light to attract prey (mates). Each firefly includes information about the path that consists of and has a maximum of k elements. They decide to organise many policy subsets and release brief, rhythmic light flashes in order to select the best course of action. The echolocation activity of microbats with varying frequencies and loudness served as the inspiration for the bat algorithm. A bat flies unpredictably, loudly, and at an unpredictable frequency at a given location (solution). It adjusts the frequency, loudness, and pulse emission rate as it searches for and finds the optimum route (per). By taking the specific stop requirement into account, the best route is identified. The hybrid firefly bat technique is similar, but a node's location vector is taken into account as a trail instead.

3.2.1. Firefly algorithm

Generally, every firefly is unisex and hence the attractiveness of one firefly to another firefly is based on distance and the intensity of brightness among the fireflies.

The attractiveness of fireflies is indirectly proportional to the distance between them and directly proportional to their brightness. Based on the attraction, one firefly can advance to follow the next firefly. In a sorted list, there exists a particular objective function. The objective function value is expected to be high and thus better transmission takes place. At every node, the objective function is evaluated as,

$$\beta = \beta_0 e^{-\alpha} \tag{2}$$

From Eq. (2), brightness is β, delay is α and initial value is β_0. The modified objective function is given below,

$$\beta_t = \beta + |X_i - X_k|\alpha + \mu \tag{3}$$

$$\mu = \mu_f(1 - k/k_j) \tag{4}$$

Eq. (3) & (4), denotes the ith firefly movement to another kth firefly. Density is k, free speed flow is μ_f, jam density is k_j and the Cartesian distance among ith and kth firefly is $|X_i - X_k|$.

3.2.2. Bat algorithm

Bat algorithm is defined as the experimental intelligent algorithm in which the echolocation principle is simulated and it is used in this algorithm. For resolving continuous optimization issues, the bat algorithm is approved from basic test functions and better results are further obtained. Based on the bat echolocation characteristics, the three idealized rules followed in the bat algorithm are,

(i) To sense distance and the variations among the background barriers and food, all bats used echolocation.

(ii) Usually bats fly randomly with xi position, vi-velocity, loudness, and frequency for prey/food searching. Based on target proximity, the emitted pulse wavelength and pulse emission rate r ε [0, 1] are adjusted.

(iii) In various ways, the loudness is differentiated from the highly positive to the reduced constant value.

The algorithm for Hybrid Firefly and Bat approach (H-FBA) is described below.

From, the description of the above algorithm, the fitness function is evaluated by following Eq. (5). Based on every node's distance, energy, and trust value of each solution, the fitness function is measured. If the fitness solution is at its lowest then it is considered the best node as shown in Eq. (6). The average fitness solution with a minimum amount is presented in the best solution index in Eq. (7).

$$\mathit{Fitness\ Function} = \sum_{\mathit{each\ solution}} \mathit{Distance} + \mathit{Energy} + \mathit{trustvalue} \tag{5}$$

Algorithm 1 Hybrid Firefly and Bat algorithm

```
Get the selected number of nodes from network
Generate initial population based on selected nodes
Set number of iterations to process FBA
For each iteration
    For each solution
        Generate initial frequency and initial velocity
        Calculate intensity
        Calculate Fitness
        Update solutions based on best solution
    End for
    Choose the best node
    For each solution
        Update frequency, velocity, and solutions based on best solution
    End for
End for
Return best node
```

$$\mathit{Lowest\ fit\_sol} = \mathit{best\ node} \tag{6}$$

$$[\mathit{best\ sol\ index}] = \mathit{min}(\mathit{Average\ fit\_sol}) \tag{7}$$

3.3. Elliptic curve cryptography with diffie-hellman exchange

In ECC, even if the key size is smaller it provides compact implementations for provided security which are resulted in quicker cryptographic operations. In this research work, the data is encrypted and decrypted and key generation is performed using the ECC encryption and Diffie-Hellman exchange performing the key exchange. Currently, there were several kinds of (PKC) public-key cryptography like Diffie-Hellman, RSA, etc. Among them, ECC is a simple technique to encrypt and decrypt data only for specific authorized users. ECC utilizes 2 keys such as private and public keys for decryption and encryption purposes, so no one can easily hack or read encrypted information during the transmission process. The basic algorithm for this proposed study is shown below. For ECC 128 bits are generated and further, the bit values are converted into hexadecimal values.

Algorithm 2: ECC with key generation algorithm.

```
128 bit key phrase set generated for ECC.
Hexadecimal conversion of 128 bit key value – $hex_{(128bit)}$.
Generation of two random prime numbers - $PR_1$ and $PR_2$.
Set initial starting point – ($P_s$).
Identification of source $ID_s$ and destination $ID_d$ seed value $ID_{src(s)}$& $Id_{dest(s)}$.
Compute values: $A_s = (s*P)$ and $B_d = (d*P)$.
A and B points shared with sender and receiver.
Decrypt Key $Dc_{key(d)} = Pr_d * P_s$.
Shared data: ($Dc_{key(d)}$(Data))
```

4. Experimental results

The experimental results of the proposed methodology related to secure data transmission of data from source to destination in an optimized path with trust

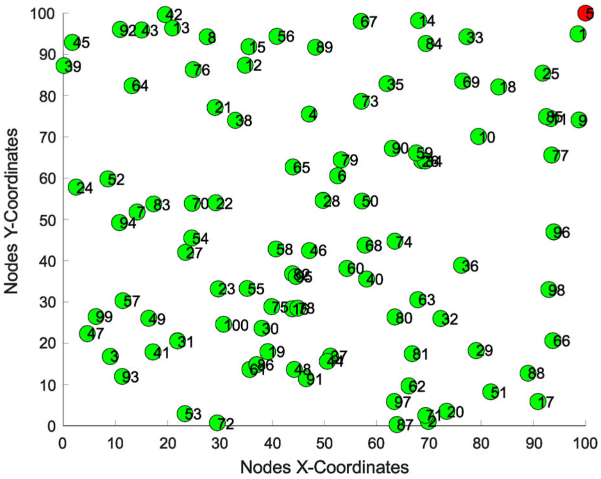


Figure 2. Sensor node deployment.

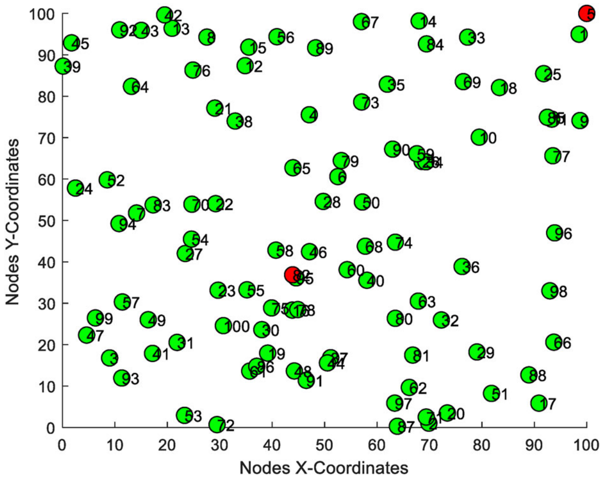


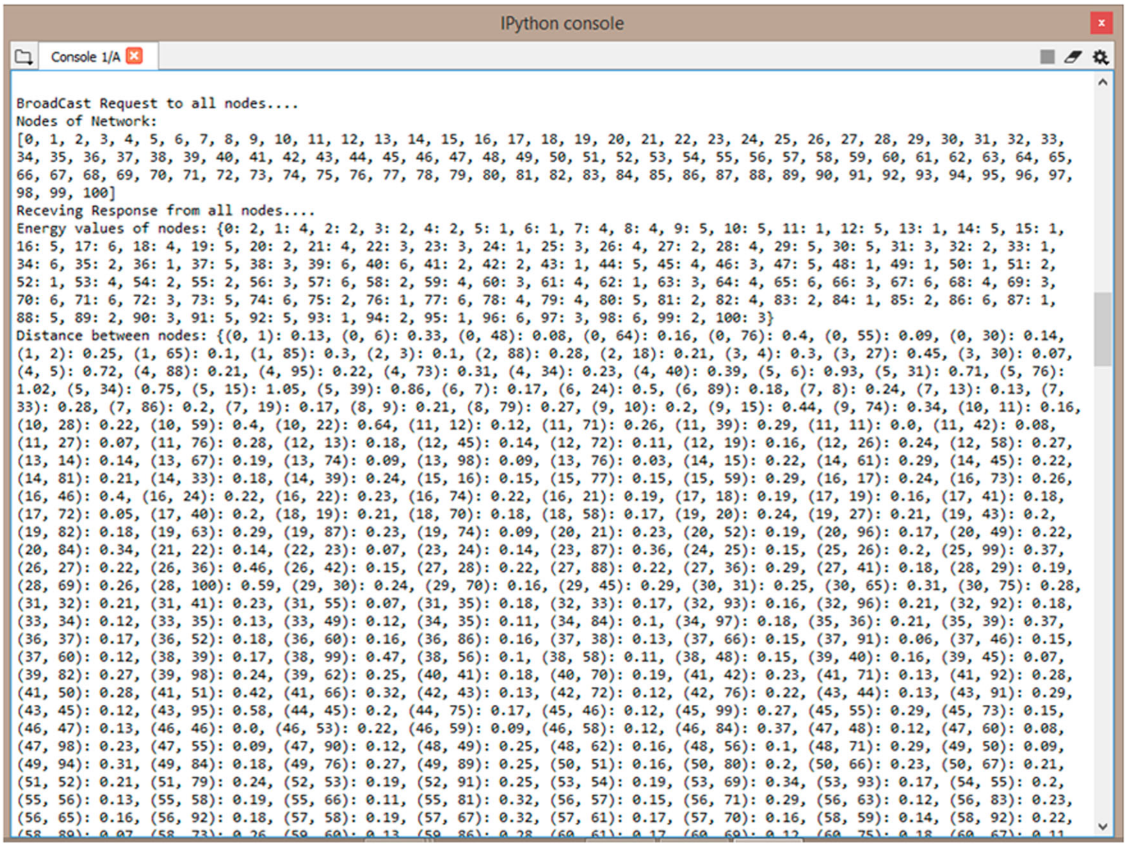
Figure 3. Source and destination identification.

value generation, efficient neighbor discovery, and key generation are discussed in this section. Additionally, performance analysis is accomplished to determine the efficiency of the proposed system[45].

Simulation is carried out using a simulation tool called NS-3. The nodes are deployed randomly in the network area of WSN. Here, a hundred (100) sensor nodes are taken for deployment. The deployment of the sensor nodes is shown in Figure 2.

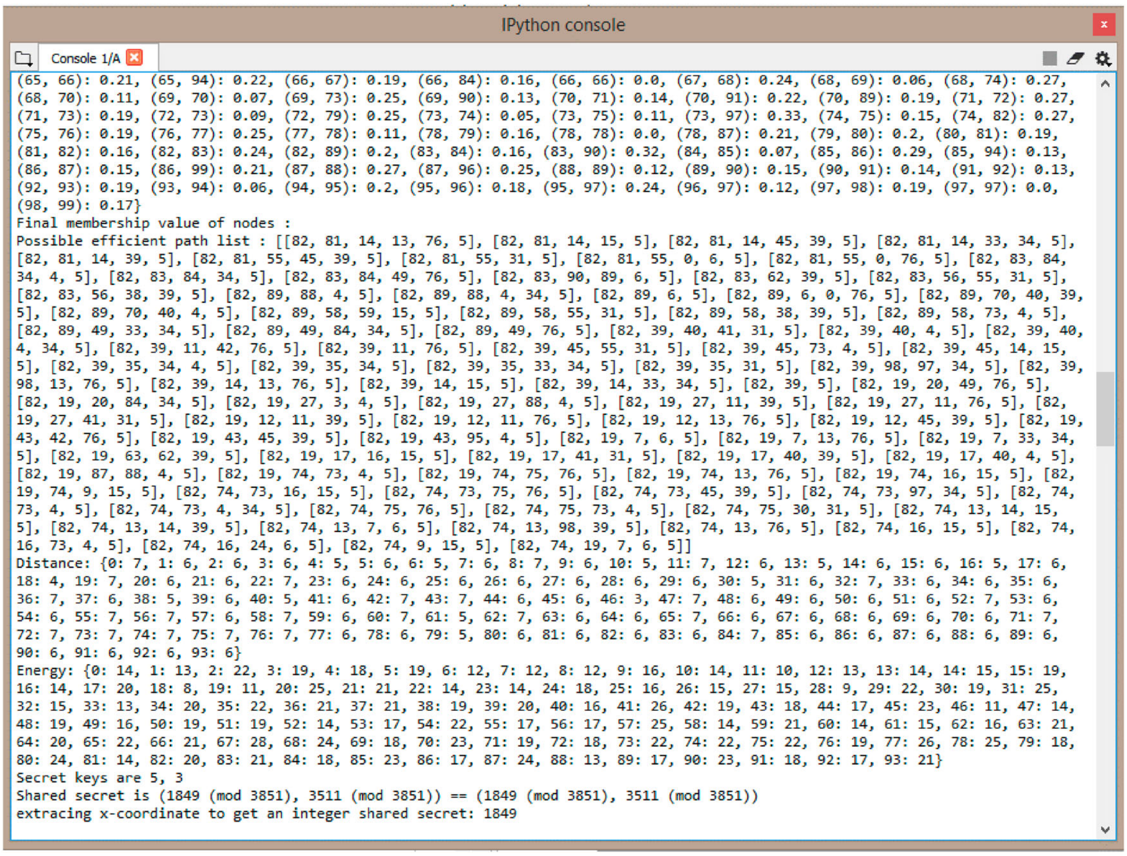
After deploying the sensor nodes, a source node is selected for initiating the data transmission. In this simulation, 82 is selected as a source node. Hence, from node 82, data transmission occurs as shown in Figure 3. After source node selection, the destination is also fixed. Here node 5 is chosen as the destination node which is also shown in figure 3. The source and destination nodes are selected for transmitting the data.

Once the source and destination nodes are identified, the neighbor node is discovered using fuzzy logic. The broadcast request is sent to all nodes and a response is received from all nodes accordingly. Neighbour node is discovered based on the energy of the node, distance value calculation, trust value generation, and historic information. Here, the historic information of the node



```
BroadCast Request to all nodes....
Nodes of Network:
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33,
34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65,
66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97,
98, 99, 100]
Receving Response from all nodes....
Energy values of nodes: {0: 2, 1: 4, 2: 2, 3: 2, 4: 2, 5: 1, 6: 1, 7: 4, 8: 4, 9: 5, 10: 5, 11: 1, 12: 5, 13: 1, 14: 5, 15: 1,
16: 5, 17: 6, 18: 4, 19: 5, 20: 2, 21: 4, 22: 3, 23: 3, 24: 1, 25: 3, 26: 4, 27: 2, 28: 4, 29: 5, 30: 5, 31: 3, 32: 2, 33: 1,
34: 6, 35: 2, 36: 1, 37: 5, 38: 3, 39: 6, 40: 6, 41: 2, 42: 2, 43: 1, 44: 5, 45: 4, 46: 3, 47: 5, 48: 1, 49: 1, 50: 1, 51: 2,
52: 1, 53: 4, 54: 2, 55: 2, 56: 3, 57: 6, 58: 2, 59: 4, 60: 3, 61: 4, 62: 1, 63: 3, 64: 4, 65: 6, 66: 3, 67: 6, 68: 4, 69: 3,
70: 6, 71: 6, 72: 3, 73: 5, 74: 6, 75: 2, 76: 1, 77: 6, 78: 4, 79: 4, 80: 5, 81: 2, 82: 4, 83: 2, 84: 1, 85: 2, 86: 6, 87: 1,
88: 5, 89: 2, 90: 3, 91: 5, 92: 5, 93: 1, 94: 2, 95: 1, 96: 6, 97: 3, 98: 6, 99: 2, 100: 3}
Distance between nodes: {(0, 1): 0.13, (0, 6): 0.33, (0, 48): 0.08, (0, 64): 0.16, (0, 76): 0.4, (0, 55): 0.09, (0, 30): 0.14,
(1, 2): 0.25, (1, 65): 0.1, (1, 85): 0.3, (2, 3): 0.1, (2, 88): 0.28, (2, 18): 0.21, (3, 4): 0.3, (3, 27): 0.45, (3, 30): 0.07,
(4, 5): 0.72, (4, 88): 0.21, (4, 95): 0.22, (4, 73): 0.31, (4, 34): 0.23, (4, 40): 0.39, (5, 6): 0.93, (5, 31): 0.71, (5, 76):
1.02, (5, 34): 0.75, (5, 15): 1.05, (5, 39): 0.86, (6, 7): 0.17, (6, 24): 0.5, (6, 89): 0.18, (7, 8): 0.24, (7, 13): 0.13, (7,
33): 0.28, (7, 86): 0.2, (7, 19): 0.17, (8, 9): 0.21, (8, 79): 0.27, (9, 10): 0.2, (9, 15): 0.44, (9, 74): 0.34, (10, 11): 0.16,
(10, 28): 0.22, (10, 59): 0.4, (10, 22): 0.64, (11, 12): 0.12, (11, 71): 0.26, (11, 39): 0.29, (11, 11): 0.0, (11, 42): 0.08,
(11, 27): 0.07, (11, 76): 0.28, (12, 13): 0.18, (12, 45): 0.14, (12, 72): 0.11, (12, 19): 0.16, (12, 26): 0.24, (12, 58): 0.27,
(13, 14): 0.14, (13, 67): 0.19, (13, 74): 0.09, (13, 98): 0.09, (13, 76): 0.03, (14, 15): 0.22, (14, 61): 0.29, (14, 45): 0.22,
(14, 81): 0.21, (14, 33): 0.18, (14, 39): 0.24, (15, 16): 0.15, (15, 77): 0.15, (15, 59): 0.29, (16, 17): 0.24, (16, 73): 0.26,
(16, 46): 0.4, (16, 24): 0.22, (16, 22): 0.23, (16, 74): 0.22, (16, 21): 0.19, (17, 18): 0.19, (17, 19): 0.16, (17, 41): 0.18,
(17, 72): 0.05, (17, 40): 0.2, (18, 19): 0.21, (18, 70): 0.18, (18, 58): 0.17, (19, 20): 0.24, (19, 27): 0.21, (19, 43): 0.2,
(19, 82): 0.18, (19, 63): 0.29, (19, 87): 0.23, (19, 74): 0.09, (20, 21): 0.23, (20, 52): 0.19, (20, 96): 0.17, (20, 49): 0.22,
(20, 84): 0.34, (21, 22): 0.14, (22, 23): 0.07, (23, 24): 0.14, (23, 87): 0.36, (24, 25): 0.15, (25, 26): 0.2, (25, 99): 0.37,
(26, 27): 0.22, (26, 36): 0.46, (26, 42): 0.15, (27, 28): 0.22, (27, 88): 0.22, (27, 36): 0.29, (27, 41): 0.18, (28, 29): 0.19,
(28, 69): 0.26, (28, 100): 0.59, (29, 30): 0.24, (29, 70): 0.16, (29, 45): 0.29, (30, 31): 0.25, (30, 65): 0.31, (30, 75): 0.28,
(31, 32): 0.21, (31, 41): 0.23, (31, 55): 0.07, (31, 35): 0.18, (32, 33): 0.17, (32, 93): 0.16, (32, 96): 0.21, (32, 92): 0.18,
(33, 34): 0.12, (33, 35): 0.13, (33, 49): 0.12, (34, 35): 0.11, (34, 84): 0.1, (34, 97): 0.18, (35, 36): 0.21, (35, 39): 0.37,
(36, 37): 0.17, (36, 52): 0.18, (36, 60): 0.16, (36, 86): 0.16, (37, 38): 0.13, (37, 66): 0.15, (37, 91): 0.06, (37, 46): 0.15,
(37, 60): 0.12, (38, 39): 0.17, (38, 99): 0.47, (38, 56): 0.1, (38, 58): 0.11, (38, 48): 0.15, (39, 40): 0.16, (39, 45): 0.07,
(39, 82): 0.27, (39, 98): 0.24, (39, 62): 0.25, (40, 41): 0.18, (40, 70): 0.19, (41, 42): 0.23, (41, 71): 0.13, (41, 92): 0.28,
(41, 50): 0.28, (41, 51): 0.42, (41, 66): 0.32, (42, 43): 0.13, (42, 72): 0.12, (42, 76): 0.22, (43, 44): 0.13, (43, 91): 0.29,
(43, 45): 0.12, (43, 95): 0.58, (44, 45): 0.2, (44, 75): 0.17, (45, 46): 0.12, (45, 99): 0.27, (45, 55): 0.29, (45, 73): 0.15,
(46, 47): 0.13, (46, 46): 0.0, (46, 53): 0.22, (46, 59): 0.09, (46, 58): 0.12, (46, 84): 0.37, (47, 48): 0.12, (47, 60): 0.08,
(47, 98): 0.23, (47, 55): 0.09, (47, 90): 0.12, (48, 49): 0.25, (48, 62): 0.16, (48, 56): 0.1, (48, 71): 0.29, (49, 50): 0.09,
(49, 94): 0.31, (49, 84): 0.18, (49, 76): 0.27, (49, 89): 0.25, (50, 51): 0.16, (50, 80): 0.2, (50, 66): 0.23, (50, 67): 0.21,
(51, 52): 0.21, (51, 79): 0.24, (52, 53): 0.19, (52, 91): 0.25, (53, 54): 0.19, (53, 69): 0.34, (53, 93): 0.17, (54, 55): 0.2,
(55, 56): 0.13, (55, 58): 0.19, (55, 66): 0.11, (55, 81): 0.32, (56, 57): 0.15, (56, 71): 0.29, (56, 63): 0.12, (56, 83): 0.23,
(56, 65): 0.16, (56, 92): 0.18, (57, 58): 0.19, (57, 67): 0.32, (57, 61): 0.17, (57, 70): 0.16, (58, 59): 0.14, (58, 92): 0.22,
(58, 89): 0.07, (58, 73): 0.26, (59, 60): 0.13, (59, 86): 0.28, (60, 61): 0.17, (60, 69): 0.12, (60, 75): 0.18, (60, 67): 0.11
```

Figure 4. Neighbour node discovery.



```
(65, 66): 0.21, (65, 94): 0.22, (66, 67): 0.19, (66, 84): 0.16, (66, 66): 0.0, (67, 68): 0.24, (68, 69): 0.06, (68, 74): 0.27,
(68, 70): 0.11, (69, 70): 0.07, (69, 73): 0.25, (69, 90): 0.13, (70, 71): 0.14, (70, 91): 0.22, (70, 89): 0.19, (71, 72): 0.27,
(71, 73): 0.19, (72, 73): 0.09, (72, 79): 0.25, (73, 74): 0.05, (73, 75): 0.11, (73, 97): 0.33, (74, 75): 0.15, (74, 82): 0.27,
(75, 76): 0.19, (76, 77): 0.25, (77, 78): 0.11, (78, 79): 0.16, (78, 78): 0.0, (78, 87): 0.21, (79, 80): 0.2, (80, 81): 0.19,
(81, 82): 0.16, (82, 83): 0.24, (82, 89): 0.2, (83, 84): 0.16, (83, 90): 0.32, (84, 85): 0.07, (85, 86): 0.29, (85, 94): 0.13,
(86, 87): 0.15, (86, 99): 0.21, (87, 88): 0.27, (87, 96): 0.25, (88, 89): 0.12, (89, 90): 0.15, (90, 91): 0.14, (91, 92): 0.13,
(92, 93): 0.19, (93, 94): 0.06, (94, 95): 0.2, (95, 96): 0.18, (95, 97): 0.24, (96, 97): 0.12, (97, 98): 0.19, (97, 97): 0.0,
(98, 99): 0.17}
Final membership value of nodes :
Possible efficient path list : [[82, 81, 14, 13, 76, 5], [82, 81, 14, 15, 5], [82, 81, 14, 45, 39, 5], [82, 81, 14, 33, 34, 5],
[82, 81, 14, 39, 5], [82, 81, 55, 45, 39, 5], [82, 81, 55, 31, 5], [82, 81, 55, 0, 6, 5], [82, 81, 55, 0, 76, 5], [82, 83, 84,
34, 4, 5], [82, 83, 84, 34, 5], [82, 83, 84, 49, 76, 5], [82, 83, 90, 89, 6, 5], [82, 83, 62, 39, 5], [82, 83, 56, 55, 31, 5],
[82, 83, 56, 38, 39, 5], [82, 89, 88, 4, 5], [82, 89, 88, 4, 34, 5], [82, 89, 6, 5], [82, 89, 6, 0, 76, 5], [82, 89, 70, 40, 39,
5], [82, 89, 70, 40, 4, 5], [82, 89, 58, 59, 15, 5], [82, 89, 58, 55, 31, 5], [82, 89, 58, 38, 39, 5], [82, 89, 58, 73, 4, 5],
[82, 89, 49, 33, 34, 5], [82, 89, 49, 84, 34, 5], [82, 89, 49, 76, 5], [82, 39, 40, 41, 31, 5], [82, 39, 40, 4, 5], [82, 39, 40,
4, 34, 5], [82, 39, 11, 42, 76, 5], [82, 39, 11, 76, 5], [82, 39, 45, 55, 31, 5], [82, 39, 45, 73, 4, 5], [82, 39, 45, 14, 15,
5], [82, 39, 35, 34, 4, 5], [82, 39, 35, 34, 5], [82, 39, 35, 33, 34, 5], [82, 39, 35, 31, 5], [82, 39, 98, 97, 34, 5], [82, 39,
98, 13, 76, 5], [82, 39, 14, 13, 76, 5], [82, 39, 14, 15, 5], [82, 39, 14, 33, 34, 5], [82, 39, 5], [82, 19, 20, 49, 76, 5],
[82, 19, 20, 84, 34, 5], [82, 19, 27, 3, 4, 5], [82, 19, 27, 88, 4, 5], [82, 19, 27, 11, 39, 5], [82, 19, 27, 11, 76, 5], [82,
19, 27, 41, 31, 5], [82, 19, 12, 11, 39, 5], [82, 19, 12, 11, 76, 5], [82, 19, 12, 13, 76, 5], [82, 19, 12, 45, 39, 5], [82, 19,
43, 42, 76, 5], [82, 19, 43, 45, 39, 5], [82, 19, 43, 95, 4, 5], [82, 19, 7, 6, 5], [82, 19, 7, 13, 76, 5], [82, 19, 7, 33, 34,
5], [82, 19, 63, 62, 39, 5], [82, 19, 17, 16, 15, 5], [82, 19, 17, 41, 31, 5], [82, 19, 17, 40, 39, 5], [82, 19, 17, 40, 4, 5],
[82, 19, 87, 88, 4, 5], [82, 19, 74, 73, 4, 5], [82, 19, 74, 75, 76, 5], [82, 19, 74, 13, 76, 5], [82, 19, 74, 16, 15, 5], [82,
19, 74, 9, 15, 5], [82, 74, 73, 16, 15, 5], [82, 74, 73, 75, 76, 5], [82, 74, 73, 45, 39, 5], [82, 74, 73, 97, 34, 5], [82, 74,
73, 4, 5], [82, 74, 73, 4, 34, 5], [82, 74, 75, 76, 5], [82, 74, 75, 73, 4, 5], [82, 74, 75, 30, 31, 5], [82, 74, 13, 14, 15,
5], [82, 74, 13, 14, 39, 5], [82, 74, 13, 7, 6, 5], [82, 74, 13, 98, 39, 5], [82, 74, 13, 76, 5], [82, 74, 16, 15, 5], [82, 74,
16, 73, 4, 5], [82, 74, 16, 24, 6, 5], [82, 74, 9, 15, 5], [82, 74, 19, 7, 6, 5]]
Distance: {0: 7, 1: 6, 2: 6, 3: 6, 4: 5, 5: 6, 6: 5, 7: 6, 8: 7, 9: 6, 10: 5, 11: 7, 12: 6, 13: 5, 14: 6, 15: 6, 16: 5, 17: 6,
18: 4, 19: 7, 20: 6, 21: 6, 22: 7, 23: 6, 24: 6, 25: 6, 26: 6, 27: 6, 28: 6, 29: 6, 30: 5, 31: 6, 32: 7, 33: 6, 34: 6, 35: 6,
36: 7, 37: 6, 38: 5, 39: 6, 40: 5, 41: 6, 42: 7, 43: 7, 44: 6, 45: 6, 46: 3, 47: 7, 48: 6, 49: 6, 50: 6, 51: 6, 52: 7, 53: 6,
54: 6, 55: 7, 56: 7, 57: 6, 58: 7, 59: 6, 60: 7, 61: 5, 62: 7, 63: 6, 64: 6, 65: 7, 66: 6, 67: 6, 68: 6, 69: 6, 70: 6, 71: 7,
72: 7, 73: 7, 74: 7, 75: 7, 76: 7, 77: 6, 78: 6, 79: 5, 80: 6, 81: 6, 82: 6, 83: 6, 84: 7, 85: 6, 86: 6, 87: 6, 88: 6, 89: 6,
90: 6, 91: 6, 92: 6, 93: 6}
Energy: {0: 14, 1: 13, 2: 22, 3: 19, 4: 18, 5: 19, 6: 12, 7: 12, 8: 12, 9: 16, 10: 14, 11: 10, 12: 13, 13: 14, 14: 15, 15: 19,
16: 14, 17: 20, 18: 8, 19: 11, 20: 25, 21: 21, 22: 14, 23: 14, 24: 18, 25: 16, 26: 15, 27: 15, 28: 9, 29: 22, 30: 19, 31: 25,
32: 15, 33: 13, 34: 20, 35: 22, 36: 21, 37: 21, 38: 19, 39: 20, 40: 16, 41: 26, 42: 19, 43: 18, 44: 17, 45: 23, 46: 11, 47: 14,
48: 19, 49: 16, 50: 19, 51: 19, 52: 14, 53: 17, 54: 22, 55: 17, 56: 17, 57: 25, 58: 14, 59: 21, 60: 14, 61: 15, 62: 16, 63: 21,
64: 20, 65: 22, 66: 21, 67: 28, 68: 24, 69: 18, 70: 23, 71: 19, 72: 18, 73: 22, 74: 22, 75: 22, 76: 19, 77: 26, 78: 25, 79: 18,
80: 24, 81: 14, 82: 20, 83: 21, 84: 18, 85: 23, 86: 17, 87: 24, 88: 13, 89: 17, 90: 23, 91: 18, 92: 17, 93: 21}
Secret keys are 5, 3
Shared secret is (1849 (mod 3851), 3511 (mod 3851)) == (1849 (mod 3851), 3511 (mod 3851))
extracing x-coordinate to get an integer shared secret: 1849
```

Figure 5. Node and path selection.

is analyzed based on the efficiency and success ratio of each node to select the best neighboring node for each node, and the discovery of the neighbor node is shown in Figure 4.

Initially, all the possible paths for data transmission from source to destination are computed using the hybrid firefly and BAT algorithm as shown in Figure 5 and then intensity and fitness values are calculated. After this calculation, the best-optimized path is obtained. Safe and trustworthy transmission of data from the source node to the destination node occurs through this path. In this simulation, the safe transmission of data occurs from the source node (82) to the destination node (5) through an identified optimized path. Here 82-81-14-15-5 is obtained as an optimized path that transmits data efficiently as shown in Figure 6.

5. Performance analysis

The performance analysis of secure data transmission through an optimized trustworthy path is evaluated in terms of delay calculation, throughput computation, energy consumption, and overall processing time.

5.1. Analysis of delay calculation

The delay calculation is shown in Figure 7. The analysis has shown that the proposed system provides data transmission without delay.

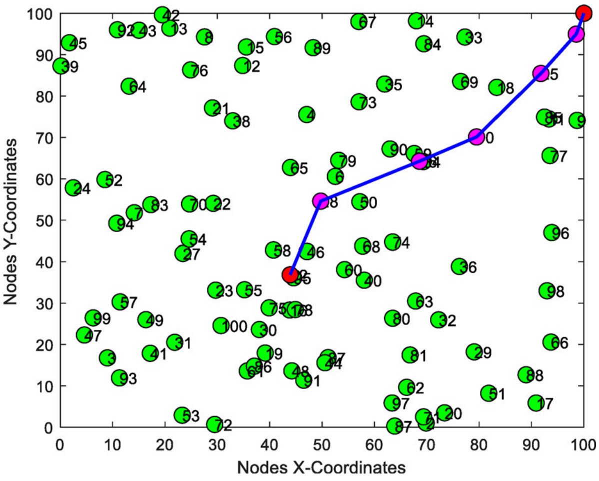


Figure 6. Data transmission.

5.2. Analysis of throughput computation

Subsequently, the proposed system is analyzed in terms of throughput. The analysis of performance by throughput computation is shown in Figure 8. From the analysis, it has been found that the proposed system provides high throughput.

5.3. Analysis of energy consumption

The consumption of energy by various nodes during data transmission from source to destination is computed which is shown in Figure 9. The analytical

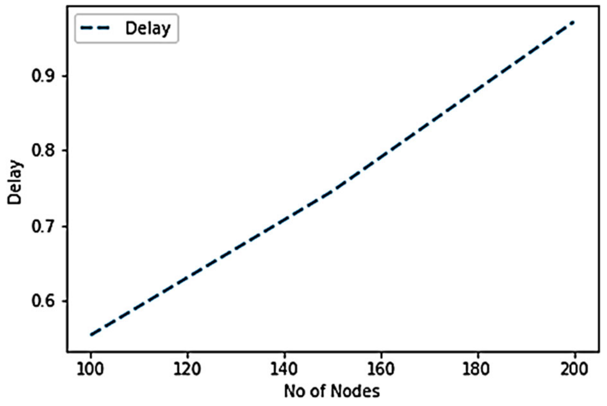


Figure 7. Performance analysis of delay calculation.

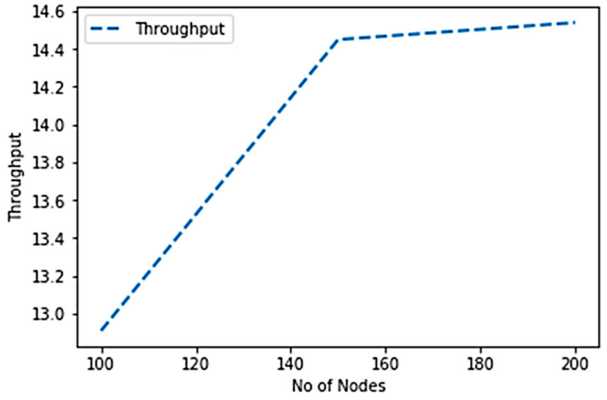


Figure 8. Performance analysis of throughput computation.

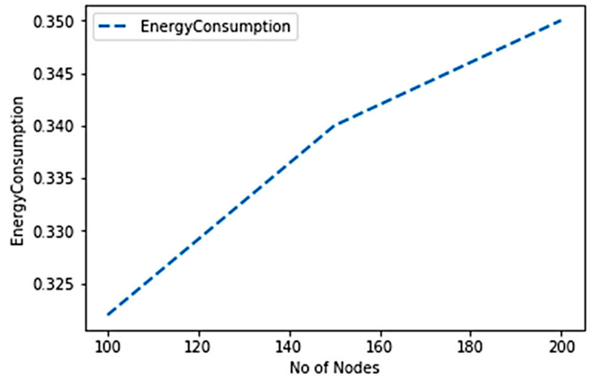


Figure 9. Performance analysis of energy consumption.

results reveal that the proposed system consumes less energy thereby increasing system efficiency.

5.4. Analysis of overall process time

Analysis of throughput computation.

Subsequently, the proposed system is analyzed in terms of throughput. The analysis of performance by throughput computation is shown in figure 8. From the analysis, it has been found that the proposed system provides high throughput Figure. 10 shows Performance analysis of overall process time (Figure 10).

Through simulation carried out using NS-3, the attained execution time is 1.306473970413208 s, the obtained noise power is 0.0006 dBm/Hz, the attained minimum packet drop rate is 8.33 and the signal power is 0.2039dBm. Thus, the final optimized path is [82, 81, 14, 15, and 5]. Hence, successful data transmission occurs from the source to the destination node via the proposed method.

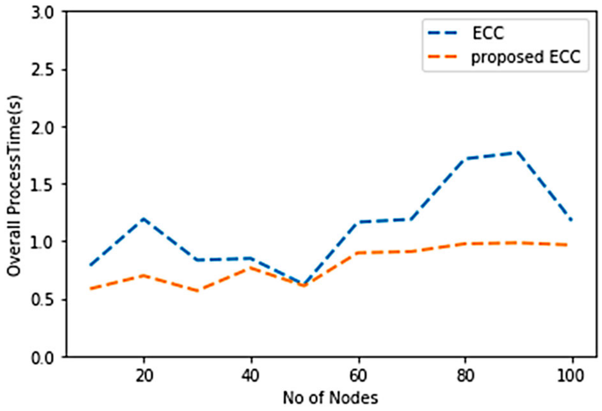
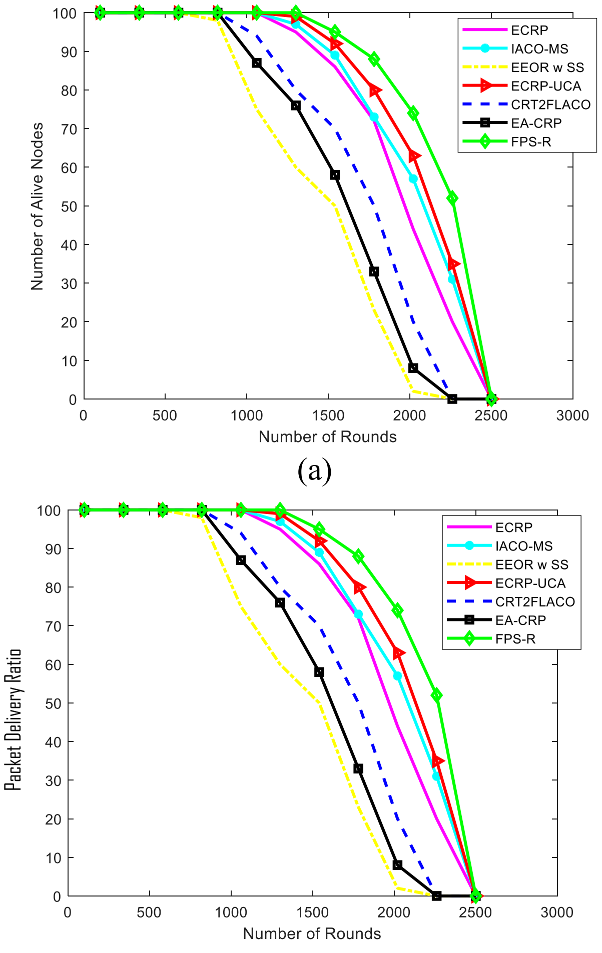


Figure 10. Performance analysis of overall process time (Existing [43] and proposed system).



(a)

(b)

Figure 11. Comparative analysis of the proposed and existing system 28 (a) in terms of number of alive nodes, and (b). in terms of packet delivery ratio.

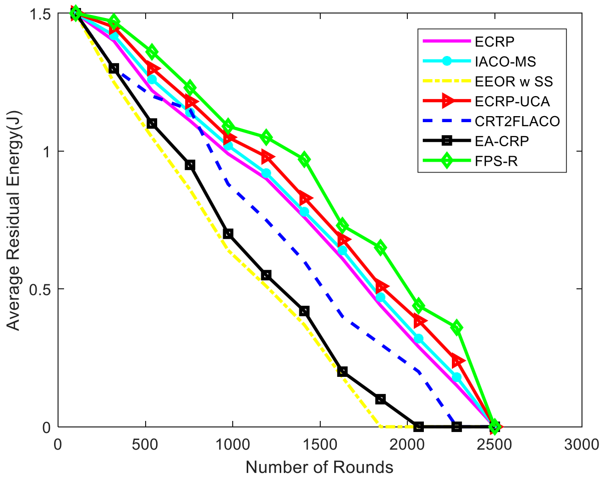


Figure 12. Comparative analysis of the proposed and existing system in terms [44] of average residual energy.

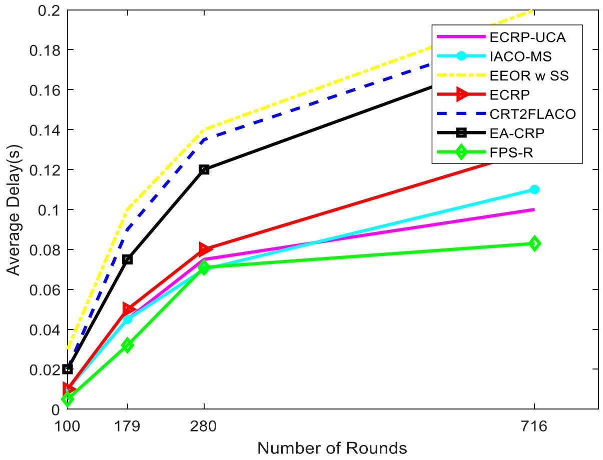


Figure 13. Comparative analysis of the proposed and existing system [44] in terms of average delay.

6. Comparative analysis

This section discusses the comparative analysis of the proposed and existing methods in terms of various metrics. The proposed novel fuzzy-based optimal path selection with randomness (FPS-R) is compared with various existing methods to validate the efficiency of the introduced methodology.

From the above Figure 11, it is clear that the number of alive nodes decreases as the number of rounds increases. It is found that the nodes are alive for the maximum number of rounds when using the proposed FPS-R than the existing systems. This proves the efficiency of the proposed methodology in terms of the number of alive nodes. In addition, the performance of the proposed and existing systems is compared in terms of average residual energy. The obtained results are shown below in Figure 12.

Average Residual Energy is the important parameter necessary for a node to efficiently transmit and receive packets during data transmission. From the above figure 12, it is clear that the Average Residual Energy of a node decreases only when the number of rounds increases. It is found that the Average Residual Energy decreases only at the 2500th round when using the proposed FPS-R. Thus, the Average Residual Energy decreases later when using the proposed system than the existing systems. This proves the efficiency of the proposed methodology in terms of Average Residual Energy. Additionally, the performance of the proposed and existing systems is compared in terms of average delay. The obtained results are shown below in Figure 13.

From the above figure 13, it is clear that the average delay is minimum when using the proposed novel FPS-R than the existing methodologies. Thus, the proposed FPS-R transmits the data from source to destination quickly when compared to existing systems. This proves the efficiency of the proposed methodology in terms of Average Delay. Table 2 shows Comparison of alive nodes.

Table 2. Comparison of alive nodes.

Round	Number of alive nodes in 1st simulation	Number of alive nodes in 2nd simulation	Number of alive nodes in 3rd simulation
100	100	100	100
150	67	70	64
200	40	40	42
250	28	26	28
300	15	15	15
350	0	1	1

7. Conclusion and future work

In this proposed work, a novel fuzzy-based optimal path selection with randomness (FPS-R) to ensure effective transmission of data has been employed. For an effective path selection, a newly hybrid firefly and bat algorithm (H-FBA) is developed. For asymmetric key generation and key exchange, Elliptic curve cryptography-ECC combined with the Diffie-Hellman technique which provides maximum security has been used. Optimal neighborhood discovery is performed to choose the trustworthy nodes for data transfer. Subsequently, the various possible paths are attained and optimized using a hybrid firefly and BAT algorithm to choose the secure and efficient path for data transfer. The proposed analytical results revealed that the proposed system ensures minimum delay, high throughput, low energy consumption, and decreased overall processing time which is compared with the existing ECC approach. It has also provided an optimized path for securely transmitting the data. This system can be further enhanced by implementing it in real time.

Declaration:

Ethics approval and consent to participate:

No participation of humans takes place in this implementation process.

Human and animal rights:

No violation of Human and Animal Rights is involved.

Authorship contributions:

There is no authorship contribution.

Acknowledgement

There is no acknowledgement involved in this work.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

No funding is involved in this work.

References

[1] Wang J, Cao Y, Li B, et al. Particle swarm optimization based clustering algorithm with mobile sink for WSNs. Future Gener Comput Syst. 2017;76:452–457. doi:10.1016/j.future.2016.08.004.

[2] Shahbaz AN, Barati H, Barati A. Multipath routing through the firefly algorithm and fuzzy logic in wireless sensor networks. Peer-to-Peer Netw Appl. 2021;14:541–558. doi:10.1007/s12083-020-01004-2

[3] Mosavifard A, Barati H. An energy-aware clustering and two-level routing method in wireless sensor networks. Computing. 2020;102:1653–1671. doi:10.1007/s00607-020-00817-6

[4] Yousefpoor E, Barati H, Barati A. A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks. Peer-to-Peer Netw Appl. 2021;14:1917–1942. doi:10.1007/s12083-021-01116-3

[5] Raval G, Bhavsar MD, Patel N, et al. Performance Comparison of Various Clustering Techniques in Wireless Sensor Networks. 2015.

[6] Naghibi M, Barati H. SHSDA: secure hybrid structure data aggregation method in wireless sensor networks. J Ambient Intell Humaniz Comput. 2021: 1–20.

[7] Hajipour Z, Barati H. EELRP: energy efficient layered routing protocol in wireless sensor networks. Computing. 2021;103:2789–2809. doi:10.1007/s00607-021-00996-w

[8] Sharifi SS, Barati H. A method for routing and data aggregating in cluster-based wireless sensor networks. Int J Commun Syst. 2021;34. doi:10.1002/dac.4754

[9] Cai X, Sun Y, Cui Z, et al. KSII Trans Internet Inf Syst. 2019;13(5).

[10] Dezfuli NN, Barati H. Distributed energy efficient algorithm for ensuring coverage of wireless sensor networks. IET Commun. 2019;13:578–584. doi:10.1049/iet-com.2018.5329

[11] Dezfouli NN, Barati H. A distributed energy-efficient approach for hole repair in wireless sensor networks. Wirel Netw. 2020;26:1839–1855. doi:10.1007/s11276-018-1867-0

[12] Yousefpoor MS, Yousefpoor E, Barati H, et al. Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. J Netw Comput Appl. 2021;190:103118. doi:10.1016/j.jnca.2021.103118

[13] Ghorbani Dehkordi E, Barati H. Cluster based routing method using mobile sinks in wireless sensor network. Int J Electron. 2022.

[14] Hatamian M, Barati H, Hatamian M, et al. Congestion-Aware routing and fuzzy-based rate controller for wireless sensor networks. Radioengineering. 2016;25:114–123. doi:10.13164/re.2016.0114

[15] Hatamian M, Ahmadpoor SS, Berenjian S, et al. A centralized evolutionary clustering protocol for wireless sensor networks. 2015 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2015: 1–6.

[16] Bhushan, S, Kumar, M, Kumar, *P*, et al. FAJIT: a fuzzy-based data aggregation technique for energy efficiency in wireless sensor network. Complex Intell Syst. 2021;7:997–1007. doi:10.1007/s40747-020-00258-w.

[17] Sert SA, Alchihabi A, Yazici A. A Two-tier distributed fuzzy logic based protocol for efficient data aggregation in multihop wireless sensor networks. IEEE Trans Fuzzy Syst. 2018;26(6):3615–3629. doi:10.1109/TFUZZ.2018.2841369.

[18] Bhushan S, Singh AK, Vij S. Comparative study and analysis of wireless mesh networks on AODV and DSR. 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). 2019: 1–6. doi:10.1109/IoT-SIU.2019.8777466.

[19] Singh AK, Bhushan S, Vij S. Filtering spam messages and mails using fuzzy C means algorithm. 2019 *4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India. 2019: 1–5. doi:10.1109/IoT-SIU.2019.8777483.

[20] Pavani M, Rao PT. IET Wirel Sens Syst. 2019;9(5): 274–283. doi:10.1049/iet-wss.2018.5227

[21] Pitchaimanickam B, Murugaboopathi G. Neural Comput Appl. 2020;32(12):7709–7723. doi:10.1007/s00521-019-04441-0

[22] Kumar H, Singh PK. Procedia Comput Sci. 2018;132: 498–506. doi:10.1016/j.procs.2018.05.002

[23] Bhalaji N. J Trends Comput Sci Smart Technol. 2020;2(03):134–140. doi:10.36548/jtcsst.2020.3.002

[24] Fotohi R, Firoozi Bari S, Yusefi M. Int J Commun Syst. 2020;33(4):e4234. doi:10.1002/dac.4234

[25] Wozniak M, Krishnaswamy D, Callegari C, et al. 2015.

[26] Sarma PN, Gopi M. arXiv preprint arXiv:1405.1818 (2014).

[27] Xu M, Liu G. Int J Distrib Sens Netw. 2013;9(3):865154. doi:10.1155/2013/865154

[28] Li J. Int J Online Eng. 2017;13(11):102–110. doi:10.3991/ijoe.v13i11.7752

[29] Baskaran M, Sadagopan C. Sci World J. 2015;2015. doi:10.1155/2015/780879

[30] Alghamdi TA. IEEE Access. 2018;6:53576–53582. doi:10.1109/ACCESS.2018.2865909

[31] Lu Y, Sun N, Pan X. IEEE Access. 2019;7:11668–11678. doi:10.1109/ACCESS.2018.2885534

[32] Chen X, Yu L, Wang T, et al. IEEE Access. 2020;8:71497–71511. doi:10.1109/ACCESS.2020.2984329

[33] Menaria VK, Jain S, Raju N, et al. IEEE Access. 2020;8: 149231–149254. doi:10.1109/ACCESS.2020.3015985

[34] Shankar SK, Tomar AS, Tak GK. Procedia Comput Sci. 2015;70:455–461. doi:10.1016/j.procs.2015.10.078

[35] Karthick S. Int J Intell Syst. 2018;11(2):76–84. doi:10.22266/ijies2018.0430.09

[36] Ahirwar GK, Goyal S, Mishra N, et al. Int J Control Theory Appl. 2017;10(13):255–264.

[37] Kumar S, Chaurasiya VK. Concurr Comput. 2018; 30(18):e4477. doi:10.1002/cpe.4477

[38] Elhoseny M, Elminir H, Riad A, et al. J King Saud Univ - Comput Inf Sci. 2016;28(3):262–275. doi:10.1016/j.jksuci.2015.11.001

[39] Ashraf M, Cho TH. KSII Trans Internet. 2018;12(9): 4271–4294.

[40] Wang Q, Yu CW, Li F, et al. Secur Commun Netw. 2016;9(17):4138–4150. doi:10.1002/sec.1594

[41] Stephan T, Al-Turjman F, Joseph KS, et al. J Parallel Distrib Comput. 2020.

[42] Yu X, Li F, Li T, et al. J Ambient Intell Humaniz Comput. 2020: 1–13.

[43] SriVenkateswaran C, Sivakumar D. Int J Bus Inf Syst. 2019;31(2):153–169. doi:10.1504/IJBIS.2019.100277

[44] Moussa N, El Alaoui AEB. Peer-to-Peer Netw Appl. 2021: 1–14.

[45] Mehetre DC, Roslin SE, Wagh SJ. Cluster Comput. 2019;22(1):1313–1328. doi:10.1007/s10586-017-1622-9