Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.021068
Article

Tech Science Press

DAMFO-Based Optimal Path Selection and Data Aggregation in WSN

S. Sudha Mercy[1,*], J. M. Mathana[2] and J. S. Leena Jasmine[3]

[1]Jeppiaar Institute of Technology, Kanchipuram, 631604, India
[2]St Peter's Institute of Higher Education and Research, Chennai, 600054, India
[3]Velammal Engineering College, Chennai, 600066, India
*Corresponding Author: S. Sudha Mercy. Email: sudhamercyresearch@gmail.com
Received: 22 June 2021; Accepted: 23 August 2021

Abstract: Wireless Sensor Network (WSN) encompasses several tiny devices termed as Sensor Nodes (SN) that have restriction in resources with lower energy, memory, together with computation. Data Aggregation (DA) is required to optimize WSN for secured data transmission at Cluster Head (CH) together with Base Station (BS). With regard to the Energy Efficiency (EE) along with the privacy conservation requirements of WSN in big-data processing and aggregation, this paper proposed Diversity centered Adaptive Moth-Flame Optimization (DAMFO) for Optimal Path Selection (OPS) and DA in WSN. In the proposed work, initially, the Trust Evaluation (TE) process is performed. The Pompeiu Distance-centered Fuzzy C-Means (PDFCM) is employed for Cluster Formation (CF) in addition to Cluster Head Selection (CHS) and then DAMFO algorithm chooses the optimal path to gather the data together with cluster centroids. The DHECC algorithm then generates keys and encrypts the aggregated data. The encrypted data is finally passed on to the BS. The experimentation outcomes exhibited that the proposed algorithm outweighs the traditional methods with respect to Energy Consumption (EC) 6.35 J, Packet Delivery Ratio (PDR) of 93%, Throughput of 0.956 bps, end-to-end delay 6.547 s, together with a lifetime of networks. Additionally, the proposed system exhibits the best Security Level (SL) of 94.2% amid the transmission.

Keywords: Wireless sensor network; base station; cluster head; pompeiu distance-based fuzzy c-means; diversity based adaptive moth-flame optimization; data hiding based elliptic curve cryptography

1 Introduction

Sensor networks are being utilized in several everyday applications recently. Furthermore, these WSN [1,2] are made of SN that encompasses lower battery power, minimal computing capacity, together with restricted memory aimed at data storage. SNs are arranged systematically or arbitrarily in a geographical terrain with restricted energy and with simple computation competence [3] for effectual sensing of the environment to accomplish data assortment and also to communicate the grouped data to the sink node (BS) via the application of effectual routing algorithms [4]. Once the SN's energy is spent, the node will

lose the function, and the WSN's performance will be much instigated. Thus, preserving SN's energy is the vital factor of ameliorating WSNs' performance. There are numerous methods concerning lessening nodes' EC, like developing higher-performance hardware, applying a load-balanced routing algorithm, and optimizing the WSN's topology [5]. DA [6] can spare the bandwidth as well as enhance EE in a resource-restrained WSN [7] amongst all methods.

The DA's principal objective is to lessen inessential data by means of extracting helpful information as of the collected data by utilizing DA functions, say MAX, MIN, MEAN, MEDIAN, etc. and advance the same to the BS [8]. The lessening of the nodes' EC and the Network Life-Time (NLT) enhancement are the distinctive traits of a good DA algorithm [9]. The DA utilizes the cluster-centered architecture for bigger networks. In a cluster-center scheme, the entire SN are gathered into clusters by means of '1' CH [10] to save energy and lessen routing overhead. The criteria under which the CH [11] ought to be selected is a challenging NP-Hard issue. In order to be chosen as CH, the Malicious Nodes (MN) often endeavors to upsurge their reputation. If these nodes get authenticated with authorized identities and valid keys, then they are regarded as genuine as of a cryptographic perspective but these nodes are malicious on considering their behaviors [12]. Trust has lately been recommended as an effectual security mechanism to enhance dependability and alleviate attacks in networked environments [13]. The restraint of energy, the limit of storage space, and the inherent susceptibilities of wireless communication bring about higher necessities to model an effectual trust framework in WSN [14].

The main issue of DA is to render security [15]. In a DA process, the adversaries are more attracted towards the nodes that do the aggregation function [16], and these nodes utilize a wireless link, which may help the attacker in monitoring the data (transmitted) and even participating in the communication [17]. Encryption and authentication are the customary approaches that are chiefly utilized for data transmission to guarantee security. Secure transmission of data and the association of secret keys to secure data amongst the communicating SN are the key issues [18]. Several encryption algorithms for instance, AES, DES, and RSA, etc. were employed in protecting the sensor data amid data transmission. Traditional encryption-centered methods are nevertheless restrained by means of memory size and face dilapidation of network performance and lessening its lifetime. Elliptic Curve Cryptography (ECC) is utilized for its ability to render high security with short key size [19] to trounce the conventional encryption schemes' complexity concerning storage space in WSN. Thus, an effectual trust-centered CH selection for safe DA and Modified ECC centered cryptography for safe data transmission in WSN is proposed. This trust mechanism discovers the MN as of the SN group in WSN, which aids to secure the DA, and MECC encrypts the amassed data and sent it to the BS that aids in preventing the data as of illegal access. The proposed framework can be used to monitor real-time data for intrusion detection and trust-based routing applications.

This paper is prearranged as: Section 2 renders the associated work of safe DA that attains extended network life and evades attacks to WSN. Section 3 evinces the proposed technique to safe data transmission in trust-centered clustered sensors in WSN. Section 4 delineates the experimentation outcomes as well as contribution. Section 5 concludes this paper.

2 Literature Review

This section surveyed some recent papers associated to secure DA and secure data communication utilizing trust-centric mechanisms and cryptographic algorithms.

Xiaowu et al. [20] rendered a Queries Privacy-Preserving approach for DA (QPPDA). This approach lessened the EC by permitting numerous queries to be aggregated onto a single packet and conserved the data privacy effectually by deploying a privacy homomorphic encryption framework. Nonetheless, it was a hard

approach to promote the QPPDA's security without the complex key distribution for diminishing the storage requirement and energy saving.

Vinitha et al. [21] resolved the energy issue and rendered an energy-effectual multi-hop routing in WSN termed integrated Taylor centric Cat Salp Swarm Algorithm (T-C-SSA). The energy-effectual CHs were picked utilizing the Low Energy Adaptive Clustering Hierarchy protocol for meliorated data transmission. The optimal hop selection was performed utilizing the T-C-SSA nonetheless, the performance rendered by the MH routing protocol has to be ameliorated.

Latha et al. [22] propounded a 3-fold integrated framework. This framework governed seamless aggregation, secure neighbor selection, and energy-effectual routing that acted as a multi-objective purpose for WSN. The rendered Trust Assisted- Energy Efficient Aggregation (TA-EEA) framework ameliorated overall aggregation precision with restricted constraints in neighbor aggregation and reliability. The trade-off betwixt energy and security was exploited for progressing effectual EC under controlled OH with a higher most PDR. The scheme was corroborated to be inappropriate from the outcomes for the large scale WSNs.

Kumar et al. [23] proffered a methodology for secure and effectual data prediction in WSN. This methodology utilized a Time Series Trust Model (TSTM) grounded on the Trust-centric Auto-Regressive (TAR) process and Toeplitz matrix. The TAR for prediction was assessed against 3 disparate attack models. The TSTM model outweighed the prevailing trust frameworks for altering total compromised nodes. Nonetheless, the approach was not applicable to the heterogeneous large-scale networks.

Ping et al. [24] paid attention on a framework termed multi-functional secure DA (MODA). For rendering value order, and context-preservations, this framework encoded raw data onto well-defined vectors and thereby proffered the components for multi-functional aggregation. The outcomes corroborated that the schemes acquired the performance superior to the utmost closely associated work. The schemes failed to focus on the effectual acquisition of numerous statistics in a disseminated environment and did not utilize the lightweight security structure.

Sumalatha et al. [25] proffered the cross-layer security-centric fuzzy trust calculation (CLS-FTC) and least OH monitoring approaches for WSNs. These approaches were proffered with memory and energy demands for resolving some existent issue. The CLS-FLTC was effectual to facilitate optimal safety in WSN environments when contrasted to the former approaches. Nonetheless, the approach could not recognize disparate attacks in WSN.

Gupta et al. [26] developed an enhanced cuckoo search-based energy balanced node clustering technique that employs a unique goal function for cluster head uniform distribution. In order to data packet routing between cluster heads and sinks, an improved harmony search-based routing protocol is provided. The protocol did not solve the issues of communication void and latency sensitivity.

Rao et al. [27] offer PSO-ECHS, an energy-efficient cluster head selection approach based on particle swarm optimization (PSO). The technique is designed with an efficient particle encoding scheme and fitness function that takes into account many characteristics such as intra-cluster distance, sink distance, and sensor node residual energy. The energy balance, on the other hand, is not addressed in this approach.

The above surveys explicate the diverse mechanisms of DA and data transmission. Each one has its individual advantages. Nonetheless, such mechanisms are inefficient since WSNs encompass countless SNs with unfamiliar relationships and limited communications. It is therefore infeasible for a node to get familiar with all other nodes. The surveyed encryption algorithms faced the problem of degradation in network performance and NLT. So for secure data transmission, an efficient trust mechanism centric DA scheme utilizing Datagram hiding-centric Elliptical Curve Cryptography (DHECC) along with Diversity-centric Adaptive Moth-Flame Optimization (DAMFO) is proposed.

3 Diversity Based Adaptive Moth Flame Optimization for Optimal Path Selection and Data Aggregation in WSN

A WSN encompasses SNs that are fixed over unreachable areas for gathering information as of that environment. SN communicates with one another only utilizing wireless format. Nevertheless, the major concerns of utilizing WSN are the communication overhead together with the EE of SN. In WSN, DA is an energy-effectual technique. The same data can will be sensed by multiple nodes because of the higher node density on sensor networks, which in turn brings about redundancy. DA is utilized during routing packets from source nodes (SN) to BS can eradicate redundancy. Additionally, the network is susceptible to privacy disclosure if the SN is subjected to malicious behaviors, so a secure energy-efficient DA approach is proposed. Initially, the TE process is carried out for consistent communication. TE is a reliable way for both detecting MN and assuring security. Its purpose is to calculate the node's TV based on its communication patterns. Next, the SNs are organized into clusters and the CH is picked among them based on residual energy (RE), reachability, and reception power (RP) by utilizing the PDFCM strategy. Using DAMFO, the DA process is carried out from the most cost-effective ideal channel between SNs. Lastly, the system proposed the DHECC to enhance the SL. The proposed work's block diagram is exhibited in Fig. 1.

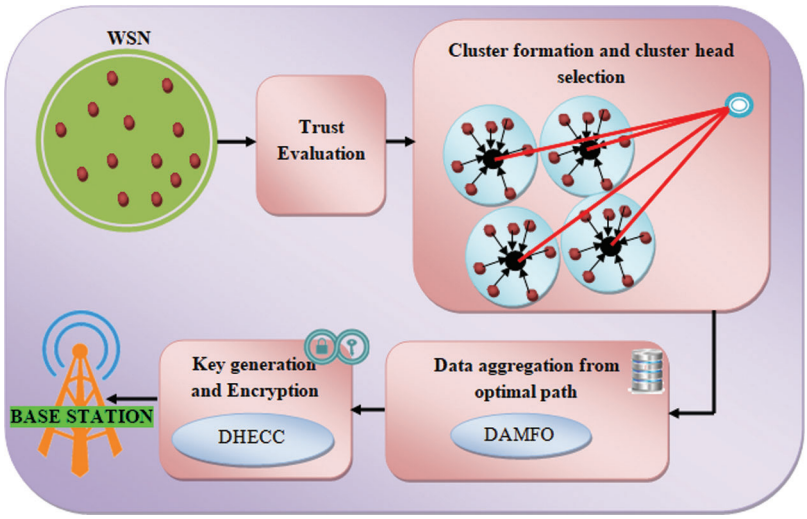


Figure 1: Architecture diagram for the proposed methodology

3.1 Network Setup

Here, a distributed network encompassing a large quantity of sensors is placed in a uniform as well as arbitrary manner. A multiple-hop network is presumed by means of a set of '*s*' SN, which is mathematically signified as:

$$WN = \{wn_1,\ wn_2,\ wn_3,\ \ldots\ldots\ldots wn_s\} \tag{1}$$

wherein, *WN* implies the multi-hop network along with WN_s signifies the *s*-number of SN. In addition, the network encompasses a single BS.

3.2 Trust Evaluation

In WSN, TE is an effectual method for detecting MN as well as ensuring security. It is accountable for computing the node's TV centered on its communication behavior. The trust can be well signified as a continuous variable over a particular range (−1 to + 1).

If the node receives the communication TV request as of the other node in the network, the node starts to calculate the TV of the requested node to have trusted communication, where the TV of each node is evaluated by considering two types of TVs i.e., direct trust and indirect trust. This TE is labeled as merged TE. The merged trust is illustrated as,

$$T_M = \sum (T_D + T_I) \tag{2}$$

Here, T_M signifies the TE, T_D implies the direct trust, and T_I implies the indirect trust.

3.2.1 Direct Trust

Direct TV can well be attained when a node encompasses direct trades with a node. Actually, a node might not have dealt with a node formerly, thus, it has no other choice but to count on other nodes' suggestions. The node trust along with path trust is stated as,

✓ Node Trust

The mobile agent gauges the node trust centered on its communication gamut. Hither, the node trust is monitored as well as assessed for detecting whether the node is forwarding or dropping the packets.

The trust of a node T_N in another node T_A is a gauge to make sure that packets transferred by means of node T_N have actually been forwarded by node T_A . The node trust of node T_N in node T_A at time stamp t is denoted as $LT^t_{(N,\,A)}$, which is stated as follows,

$$LT^t_{(N,\,A)} = (\tilde{w}_1 * C^t_{pac}) + (\tilde{w}_2 * D^t_{pac}) \tag{3}$$

Here, D^t_{pac} and C^t_{pac} signifies the data packet forwarding ratio and control packet forwarding ratio, respectively at time step t, whereas, $\tilde{w}_1$ and $\tilde{w}_2$ specifies the assigned weight values of C^t_{pac} and D^t_{pac}, respectively.

✓ Path Trust

Path TV computation is done for ascertaining the reliability of the path via which the data packets are forwarded. It is evaluated as the weighted average of the TVs of the nodes in the path and is computed as,

$$HT^t_{(N,A)} = \prod LT^t_{(N,A)} | T_N,\ T_A \text{ and } T_N \rightarrow T_A \tag{4}$$

Here, $T_N \rightarrow T_A$ mean that T_A is the next hop ofT_N . At last, the direct trust is evaluated as,

$$T_{D_{(N,A)}} = \sum (LT_{(N,A)} + HT_{(N,A)}) \tag{5}$$

3.2.2 Indirect Trust

Indirect trust acts as the trust relations betwixt distributed nodes with no direct interactions. Indirect TV for any neighbor node is gathered as of its neighbor nodes excluding the evaluating node. For intensifying the TV's accuracy, it is vital to discover the indirect trust of node T_X as of the common adjacent nodes betwixt node T_N and T_A. The indirect TV of the neighbor node T_X to node T_A is evaluated as,

$$T_{I^{(T)}_{(N,A)}} = T_D(N,X) * T_D(X,A) \tag{6}$$

Here, $T_{I^{(T)}_{(N,A)}}$ - Indirect TV of node T_N and T_A in respect of T_X , $T_{D\ (N,X)}$ - Direct trust of node T_N in node T_X, $T_{D\ (X,A)}$ - Direct trust of node T_A in node T_X

The status of every node is identified grounded on this calculation. If the direct and indirect TV is less than 0.5, then the node is an MN; if it is equivalent to 0.5, then the node is concerned as a suspect node; if it is

greater than 0.5 and less than 0.75, then the node is a less trustworthy node; and also, if it is greater than 0.75, then the node is concerned as a trustworthy node.

3.3 Cluster Formation and Cluster Head Selection Using PDFCM

Clustering is the approach for routing in WSNs, which lessens the bandwidth and energy requirements for elevating NLT. The SNs are built onto clusters and the CH is chosen from those clusters grounded on the residual energy (RE), reachability, and reception power (RP) utilizing Pompeiu Distance-centric Fuzzy C-Means (PDFCM) algorithm. The FCM is an eminent algorithm for generating a cluster.

Step 1: First, initialize the "$WN = wn_1, wn_2, wn_3, \ldots wn_s$" number of SNs in WN, and partition it into clusters, say $R''_{cl} = c''_1,\ c''_2,\ c''_3,\ \ldots\ c''_n$.

Step 2: Next, G_c cluster centers are arbitrarily selected as of the initialized R''_{cl}

Step 3: The SN is allotted to the cluster center for which the distance as of the cluster center is the minimum of all the cluster centers. In a normal FCM, the distance is evaluated centered on Euclidean distance which is weak for a large number of values. So, the Pompeiu Distance that takes the distance betwixt the SN and cluster centroids is utilized and is expressed as:

$$D_{pd} = \max\left(|WN - G_c|\right) \tag{7}$$

Step 4: The membership values are finally updated by utilizing the below equation,

$$O_f = \sum_{k=1}^{s}\sum_{i=1}^{n} \lambda_{ik}^{\alpha}.\ \max\left(|WN_k - G_{c_i}|\right) \tag{8}$$

Here, s signifies the number of SNs, WN_k specifies the k^{th} node, G_{c_i} symbolizes the i^{th} cluster centre, α indicates a constant greater than 1, λ_{ik} signifies the degree of member-ship of the k^{th} node in the i^{th}cluster, whereas, n denotes the number of clusters.

Step 5: Repeat the steps as of 2 to 4 till the constant values are acquired for the membership values. In this manner, every node in WSN is clustered. The formed cluster is explicated as:

$$FC(d) = \{FC_1,\ FC_2,\ FC_3,\ \ldots\ FC_d\} \tag{9}$$

Here, $FC(d)$- Formed cluster set , FC_d - d-number of the clusters

After CF, the CH for each respective cluster is picked in respect of RE, reachability, and RP and is set as the fitness function as,

$$\psi_{(R''_{ey},R''_{ab},R''_{pow})} = \sum\left(R''_{ey},\ R''_{ab},\ R''_{pow}\right)_{initial} - \sum\left(R''_{ey},\ R''_{ab},\ R''_{pow}\right)_{current} \tag{10}$$

where, $(R''_{ey},\ R''_{ab},\ R''_{pow})_{initial}$ and $(R''_{ey},\ R''_{ab},\ R''_{pow})_{end}$ signify the initial and current RE, reachability, and RP of the SNs respectively, $\psi_{(R''_{ey},R''_{ab},R''_{pow})}$ symbolizes the RE, reachability, and RP of the SNs, which defines the difference betwixt the initial and current RE, reachability, and RP of the SNs. The best CH is chosen grounded on the $\psi_{(R''_{ey},R''_{ab},R''_{pow})}$, which means the proposed approach has fixed one threshold value. The SN's $\psi_{(R''_{ey},R''_{ab},R''_{pow})}$ value nearest to the threshold would be taken as a CH. In this manner, the CH is chosen for every cluster.

3.4 Data Aggregation from Optimal Path Using DAMFO Algorithm

Subsequent to the CHS, the DA process is performed. The DA process gathers the data as of disparate sources and eradicates redundancy and thereby minimizes the transmission count. This process engenders energy conservation. It is essential to discover a secure routing path betwixt source and destination as of

the CH before gathering data. The best communication path selection framework lets the CH to attain the best copy of the source values sent by the source sensor. The Diversity-centric Adaptive Moth-Flame Optimization (DAMFO) is the best solution for the selection of cost lowest optimum path betwixt SNs. It proffers the optimum path for improving EE. MFO is a recent populace-centric algorithm inspired by moth's special navigation strategies. A moth flies by maintaining a steady angle with respect to the moon, which is a particularly efficient mechanism for covering great distances in a straight line. In the case of artificial light created by humans, the moths try to maintain the same angle with the light source. As a result, moths are circling lights in a spiral pattern. MFO begins by creating moths at random inside the solution space, then computing fitness values, i.e., each moth's position, and labelling the best position with flame. The existing MFO has slower convergence and lower precision. The proposed system utilizes an improved version of the MFO algorithm centered on a diversity approach, which is termed as the DAMFO algorithm for enhancing the updation process. The DAMFO algorithm has the below-explicated steps,

Step 1: The CH primarily broadcasts the data to the mobile sink or destination via disparate paths. A moth creates a path as of SN to the destination node and hence, initialization of the moths is first done. The moths are depicted in the sort of a matrix, which is described below,

$$I = \begin{bmatrix} i_{1,1} & i_{1,2} & \cdots & i_{1,x} \\ i_{2,1} & i_{2,2} & \cdots & i_{2,x} \\ \vdots & \vdots & \vdots & \vdots \\ i_{k,1} & i_{k,2} & \cdots & i_{k,x} \end{bmatrix} \tag{11}$$

Here, k- Number of solutions (moths) and x- Dimension of the problem which states the moth's position in search space

Step 2: Fitness calculation

Evaluate the fitness of every candidate solution which is concerned as selected paths. Therefore, the fitness of every solution is regarded as maximal path trust and minimal path distance, which is explicated in the below equation,

$$F''_{HS} = \left\{ \begin{array}{ll} \max \left(\sum_{m=1}^{s} HT\,(T_m,\ T_{m+1}) \right) & //Path\ trust \\ \min \left(\sum_{m=1}^{s} dist\,(T_m,\ T_{m+1}) \right) & //Path\ distance\ between\ source\ and\ destination \end{array} \right\} \tag{12}$$

Here, $HT(T_m, T_{m+1})$ and $dist\ (T_m, T_{m+1})$signify the path trust and path distance betwixt the nodes T_m and T_{m+1} , respectively, $m = 1$indicates source node, whereas, s specifies the destination node. The solutions are then arranged in ascending order grounded on the fitness values for updating the moth's position.

Step 3: Updating the Moth's positions

This algorithm updates the Moth's position subsequent to initialization and the MFO algorithm embraces '3' disparate functions to convergent the global-optimum of the optimization problems. It is mathematically written as:

$$D_s = \langle R''_l,\ M''_s,\ E''_c \rangle \tag{13}$$

$$R''_l : \varphi \rightarrow (I,\ N_o) \tag{14}$$

$$M_s^{''}: I \rightarrow I \tag{15}$$

$$E_c^{''}: I \rightarrow \{TRUE,\ \ FALSE\} \tag{16}$$

Here, $R_l^{''}$ signifies the function generating a random populace of moths and respective fitness values, $M_s^{''}$ symbolizes the main function which moves the moths around the search space, N_o specifies the number of moths, Isignifies the set of notes, whereas, $E_c^{''}$ specifies the function that returns true if the termination state is satisfied and false if unsatisfied. Subsequently, the position of moths is updated as:

$$P\left(I_u,\ H_v\right) = A_u . e^{cr} . \cos\left(2\,\pi\, r\right) + H_v \tag{17}$$

$$A_u = \left|H_v - I_u\right| \tag{18}$$

Here, A_u-Space betwixt the u^{th} moth and v^{th} flame, c-State the logarithmic spiral shape, r-Random number between [− 1, 1].

Step 4: Renewing the number of flames

Updation of the moths' positions in k-locations in the search space might lessen a chance of exploitation of the best propitious solutions, and on this account, decreasing the number of flames assists to trounce this issue centered on the subsequent equation:

$$N_{flames} = round\left(M_{nf} - N_{iter} \times \frac{M_{nf} - N_{iter}}{b}\right) \tag{19}$$

Here, M_{rf}-Maximum number of flames, N_{iter}-Present iteration number, b-Maximum iterations

Step 5: Updation of the current search agent's position

The current search agent's position is updated by utilizing the levy flight for elevating the diversity of the populace against pre-mature convergence and accelerating the convergence speed. This is written as,

$$P_u^{b+1} = P_u^b + j\ sign\ [rand - 0.5]\ \oplus\ L_y\ (\alpha) \tag{20}$$

$$L_y\ (\alpha) \sim \mu = b^{-1-\alpha}, \quad 0 \leq \alpha \leq 2 \tag{21}$$

Here, P_u^b-u^{th} moth or solution vector P_u in iteration b, μ-Standard normal distributions, $\oplus$-Dot product (entry-wise multiplications), j-Random parameter that conformed to a uniform distribution, *rand*-Random number in [0,1].

Now, compare the path traversed by every moth and pick the best optimal path utilizing the above procedure. This approach renders the optimum path with quick data gathering capacity, and thereby, augments the speed of reaching the destination. The aggregated data is written as proffered below.

$$A_{DS} = \{a_1,\ a_2,\ a_3,\ \ldots\ldots\ldots a_w\} \tag{22}$$

Here, A_{DS}-Aggregated data from the CH, a_w-w-number of data

This will thus lessen the amount of transmission energy spent at the time long-haul communication. The DAMFO algorithm could be comprehended with the below pseudocode Fig. 2.

3.5 Key Generation and Encryption Phase

The aggregated data is finally sent to the sink i.e., the BS. The aggregated data are encrypted before sending them as of source to destination for elevating their SL against data transmission attacks.

Conversion of the aggregated data to ciphered data is done to block unauthorized access. The proposed system deploys DHECC. It encrypts the hidden aggregation data with disparate keys. Elliptic Curve Cryptography (ECC) proffers stronger security and faster computation over some asymmetric crypto-systems. For elevating the SL of ECC, the system effectuates a data hiding algorithm that could securely send packets over the network. The DHECC algorithm has the below-explained steps:

Input: Number of iteration and current iteration
Output: $A_{DS} = \{a_1, a_2, a_3, \ldots\ldots a_w\}$

Begin
Initialize the moths in a matrix form as I
Initialize fitness function vector as H
Define the MFO function, $D_s = \left\langle R_i^n, M_s^*, E_c^n \right\rangle$
While $(iter \le \max\_ iter)$
Update the moth's position by using the below equation,
$$P(I_u, H_v) = S_T . A_u . e^{cr} . \cos(2\pi r) + H_v$$
Renewing the number of flames by using
$$N_{flames} = round\left(M_{nf} - N_{iter} \times \frac{M_{nf} - N_{iter}}{b} \right)$$
If $(iter == 1)$
Sort the number of moths and flames
Else
Sort the number of moths and corresponding fitness values
End if
Update the current search agent position by using
$$P_u^{b+1} = P_u^b + j\ sign\ [rand - 0.5] \oplus L_y\ (\alpha)$$
Report the best solution among the moths
End while
End

Figure 2: Pseudocode for the DAMFO algorithm

3.5.1 Key Generation Phase

The existing ECC creates only 2 keys: a public key and a private key, signified as "U_{public}^k" and "$U_{private}^k$", respectively, for encryption. The proposed system creates another one key termed secret key (S_{key}) for ameliorating the system's security. This S_{key} is multiplied to the encryption equation and gets divided in the decryption equation. If the encryption and decryption become increasingly complex, then it is so hard for detecting the actual data. It automatically meliorates the SL of the data. The mathematical denotation of the DHECC is:

$$C^2 = q^3 + y\,q + z \tag{23}$$

Here, y and z-Integers, q-Rational number

By considering a point B_{pc} as a base point on the curve, the U_{public}^k is generated as,

$$U_{public}^k = U_{private}^k * B_{pc} \tag{24}$$

As $U_{private}^k$ is the arbitrarily generated key, there is a possibility that the attacker attacks the data. A good choice of the $U_{private}^k$ will give an excellent encryption process. The S_{key} would be assessed by summing up the U_{public}^k, $U_{private}^k$, and the B_{pc} on the curve. It is explicated using,

$$S_{key} = \sum (U^{k}_{public},\ U^{k}_{private},\ B_{pc}) \tag{25}$$

In this manner, the U^{k}_{public}, $U^{k}_{private}$, and S_{key} are created by the key generation center. These optimized keys are created with a high-SL.

3.5.2 Encryption Phase

This phase is performed for elevating the SL. With an aggregated data A_{DS}, S_{key} and sender's public key $U^{''}_{public}$, it generates a ciphertext.

$$E\ (A_{DS}) = A_{DS} + (rd * U^{''}_{public}) * S_{key} \tag{26}$$

Here, $E(A_{DS}$)-Cipher text of aggregated data, *rd*-Random number in the gamut of 1 to n−1.

After encrypting the A_{DS}, the data hiding strategy is deployed for shielding the data as of the attacker and embed the $E(A_{DS})$ in an alternate byte. Then, transmute every byte to 8 bits. Employ 1bit right shift operation on the complete file such that every byte would be concealed accordingly. These hidden messages embrace the encrypted message in the sort of bits, and this is mathematically signified as $E\ (H_{msg})$.

3.5.3 Decryption Phase

When the BS receives the transmitted data, the data are decrypted as in Eq. (26). Utilizing the below derivation, the final output is acquired,

$$A_{DS} = \left(\frac{E(H_{msg}) * U^{''}_{private}}{S_{key}} \right) \tag{27}$$

Here, A_{DS}-Original aggregated dataThe proposed method's effectiveness is evaluated in the subsequent section.

4 Results and Discussion

An efficient DAMFO algorithm is proposed to execute DA that chooses an optimal path for the data aggregator for gathering the sensor data as of the CH. By deploying the trust mechanism, the SNs are facilitated with security. The MNs can be recognized grounded on the trust mechanism. Afterward, the CF and CHS of the trusted SNs are done. Then, the DAMFO algorithm is utilized to execute the DA of the WSN. After DA, DHECC is implemented to provide security to the aggregated data. The work is implemented by utilizing the tool named "network simulation-2". The proposed work covers 1000 × 1000 m^2 network area and the number of SNs utilized for the analysis purpose is 100. This section contrasts the results shown by the proposed DA and encryption frameworks and the existing algorithms with respect of some measures mainly for analyzing the proposed work's performance efficiency, which is explicated below.

4.1 Performance Analysis of DAMFO

This section compares the proposed DAMFO with the existing algorithms, such as MFO, Cuckoo Search Optimization (CSO), Fish swarm optimization (FSO) and Genetic Algorithm (GA) centered on the performance regarding EC, NLT, Throughput, PDR, and delay. The basic explications of these metrics are proffered below,

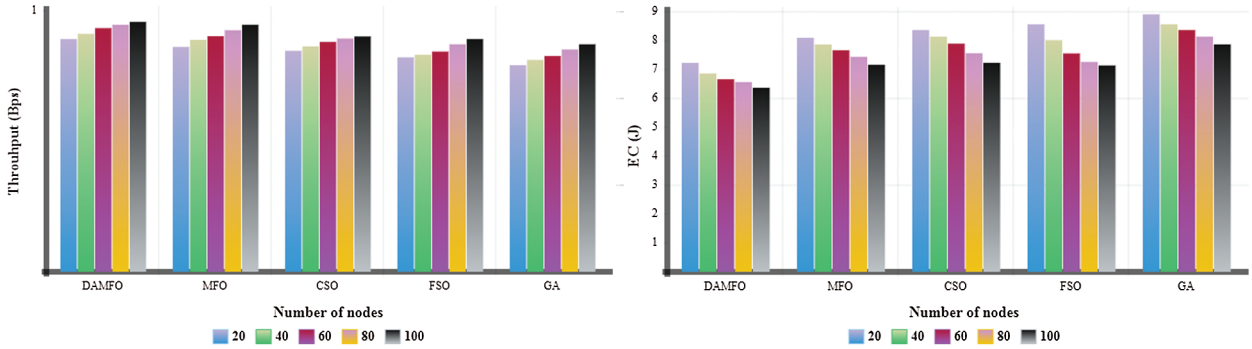
i) ***EC:*** It implies the energy consumed by a node for transmitting as well as receiving the packets. The EC for the network and the node has to be as less as feasible such that NLT can be elevated.
ii) ***PDR:*** It signifies the ratio betwixt the total packets received at the sink and the total packets transmitted by the nodes. If the PDR is high, then it indicates low packets loss.
iii) ***Throughput:*** It gauges the ratio betwixt the total bits reached the sink and the total bits generated.
iv) ***Delay:*** It is the time used by the packet to travel as of the source to the sink node. It has to be small for high-speed applications.
v) ***Network Lifetime:*** It signifies the time taken until 50% of the nodes existent in the network rest alive.

Tab. 1 renders the performance values acquired by the existing and proposed approaches.

Table 1: Results of the proposed DAMFO and existing techniques

Metrics	Number of nodes	Proposed DAMFO	MFO	CSO	FSO	GA
Energy Consumption (J)	20	7.2145	8.0823	8.3547	8.5478	8.8974
	40	6.8478	7.8541	8.1254	8.0024	8.5478
	60	6.6478	7.6547	7.8795	7.5412	8.3547
	80	6.5478	7.4258	7.5478	7.2463	8.1247
	100	6.3547	7.1473	7.2145	7.1254	7.8547
Throughput (Bps)	20	0.89	0.86	0.845	0.82	0.79
	40	0.91	0.887	0.901	0.924	0.945
	60	0.932	0.862	0.879	0.892	0.9
	80	0.945	0.83	0.842	0.87	0.89
	100	0.956	0.81	0.825	0.85	0.87
Network lifetime (s)	20	70	68	65.87	64	61.45
	40	74	70	68.74	66.54	63.54
	60	78	72	70.87	68.78	65.87
	80	83	75	73	71.21	69.47
	100	88	79	76	73.54	72.54

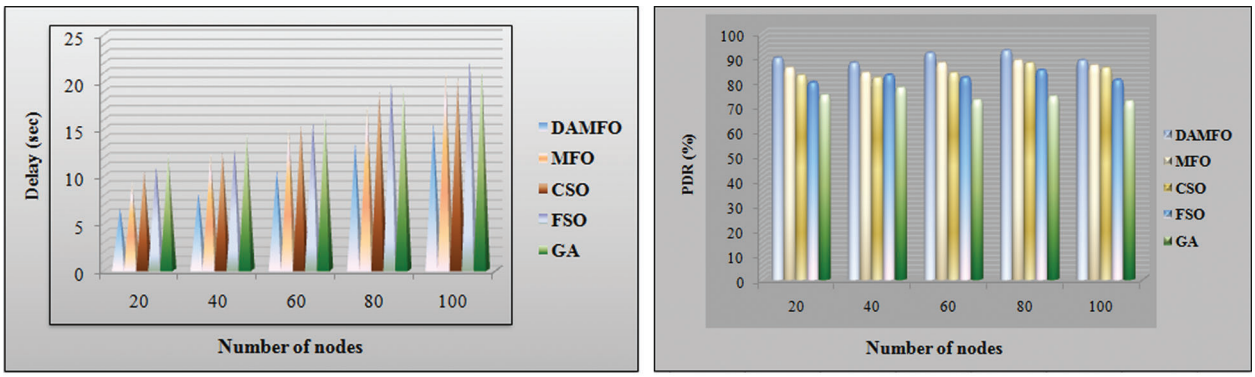
Tab. 1 proffers the results acquired by the proposed DAMFO and existing approaches. Here, the comparison is performed in respect of EC, throughput, and NLT by varying the number of SNs as of 20 to 100. On comparing the results, the DAMFO acquires the highest throughput and NLT values, and the lowest EC value for all 20 to 100 nodes. From these outcomes, the proposed DAMFO is corroborated to be excellent for the DA when contrasted against the existing algorithms. Fig. 3(a&b) proffers the comparison regarding EC and throughput graph. For the 20 nodes, the throughput acquired by the proposed DAMFO is 0.89, whereas the existing techniques, MFO, CSO, FSO, and GA give the throughput of 0.86, 0.84, 0.82, and 0.79, respectively, which are lower when contrasted to DAMFO. Likewise, for the remaining 40, 60, 80, and 100 nodes, the DAMFO shows the highest throughput of 0.910, 0.932, 0.945, and 0.956, respectively, when contrasted to others. The throughput has to be high for a WSN when utilizing an optimal algorithm and this is achieved only by the proposed DAMFO.



(a) (b)

Figure 3 (a&b): Throughput and EC of the techniques

For 20 nodes, the proposed DAMFO shows 7.2145-EC, which is lower when contrasted to the existing algorithms. Likewise, for 40 to 100 nodes, the proposed DAMFO gives the lowest EC values. The network must have less EC for an efficient algorithm and this is achieved by the proposed DAMFO. From this comparison, the proposed DAMFO is found to show better throughput and EC values when contrasted against the existing ones. Fig. 4(a&b) proffers the delay and PDR values of both techniques.



(a) (b)

Figure 4 (a&b): Delay and PDR of the techniques

Fig. 4. contrasts the existing and proposed approaches regarding the delay and PDR values. For 20 nodes, the proposed DAMFO has 6.5478 s delay, whereas the existing MFO, CSO, FSO, and GA approaches show 9.3577, 10.5478, 10.9874, and 12.3654 s delay, respectively, which are higher when analogized with the proposed DAMFO. And also for the other 40 to 100 nodes, the delay acquired by the DAMFO is lower when contrasted to the existing approaches. From these outcomes, the proposed DAMFO is the only approach that shows superior performance for DA in respect of delay. And, on considering PDR, the higher most PDR value signifies that the algorithm has several capabilities of delivering packets as of source to destination. For the first 20 nodes, the PDR acquired by the proposed DAMFO is 90% that is higher than the existing MFO (86%), CSO (83%), FSO (80%), and GA (755). Likewise, for 40, 60, 80, and 100 nodes, the proposed DAMFO acquires the highest PDR of 88%, 92%, 93%, and 89% when contrasted to the existing approaches. The approaches show different PDR values centered on the considered number of nodes the network used. But the proposed DAMFO achieves

superior outcomes. So, the proposed DAMFO was found to deliver the packets as of source to destination with minimal loss when contrasted to others. Fig. 5. explicates the comparison regarding NLT values.

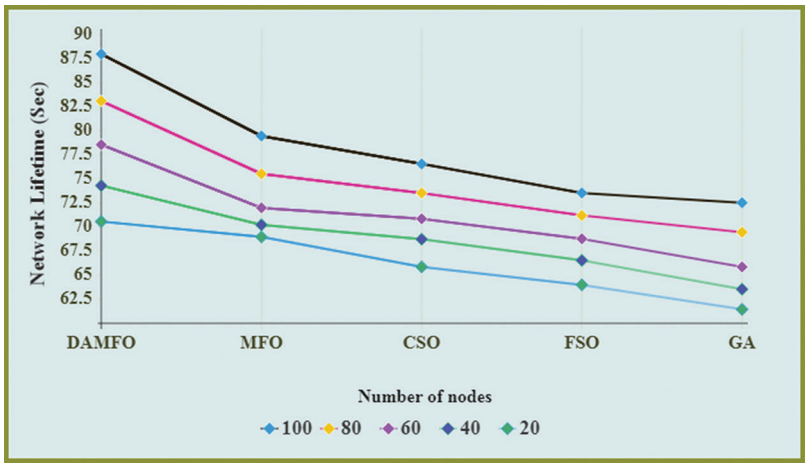
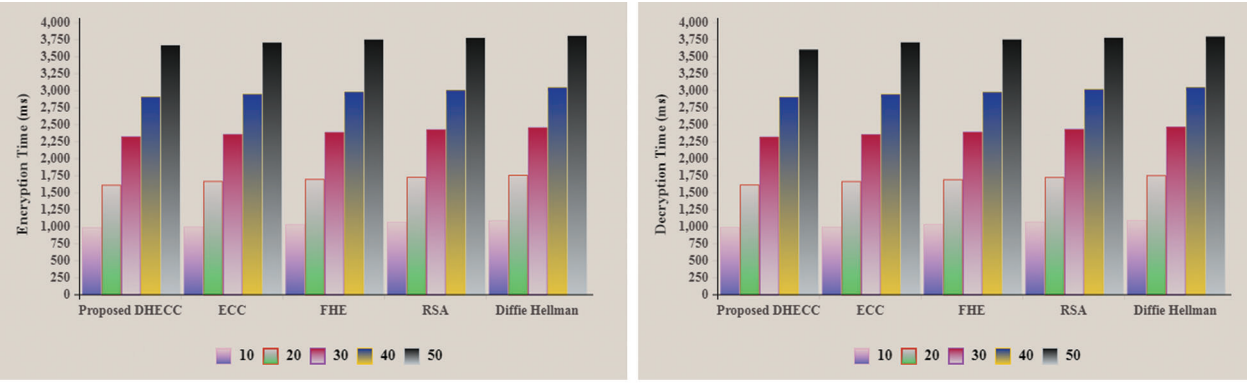


Figure 5: Network lifetime of the techniques

Fig. 5. contrasts the proposed and existing approaches centered on performance in respect of the NLT graph. The NLT is gauged in seconds by varying the SN-count as of 20 to 100. For 20 nodes, the proposed DAMFO has 70.58 s-NLT, whereas, the existing MFO, CSO, FSO, and GA approaches achieve 68.98 s, 65.87 s, 64 s, and 61.45 s-NLTs for the same 20 nodes that are lower when analogized with the proposed DAMFO. Likewise, for 40 to 100 nodes, the proposed DAMFO achieves the higher most NLT when analogized against the existing algorithms. When the number of nodes elevates, the NLT also increases, but the proposed DAMFO has high NLT for all nodes.

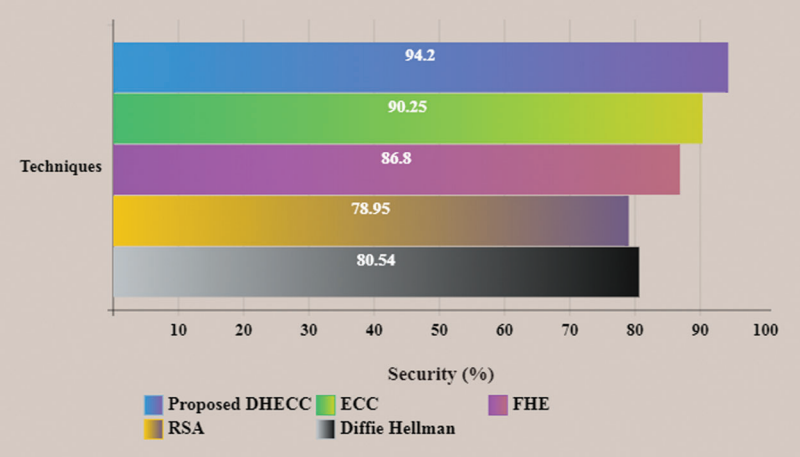
4.2 Performance Analysis of DHECC

Here, the proposed DHECC algorithm is analyzed by comparing it with the existing FHE, Diffie Hellman (DH), ECC, and RSA, algorithms centered on performances in respect of decryption time (DT), encryption time (ET), and SL, which can be explicated further using Fig. 6. The ET Fig. 6a and DT Fig. 6b of the approaches are plotted by varying the packet size of the data as of 10 to 50Kb. The overall security analysis Fig. 6c of the approaches is as well plotted. For a 10Kb packet size, the proposed DHECC algorithm takes 980 ms- ET, whereas, the existing ECC, FHE, RSA, and DH algorithms take 992, 1025, 1060, and 1080 ms- ET.



(a) (b)

Figure 6: (continued)



(c)

Figure 6: (a, b) Encryption and Decryption Time of the technique, (c) Performance graph of the encryption techniques

Here, the proposed DHECC takes less ET than the existing algorithms. Likewise, for the other 20, 40, 30, and 50 packet sizes, the proposed DHECC obtains the lowest ET when contrasted to ECC, FHE, RSA, and DH. Whenever the packet size elevates, the ET of the approaches as well increases but the proposed DHECC acquires the lowest ET for all packet sizes when contrasted to existing algorithms. This evinces the proposed DHECC's encryption efficiency. Fig. 4b evinces the comparison graph of the approaches for DT. As same as ET, the DT of the approaches is plotted by varying the packet size as of 10 to 50Kb. For the10Kb packet size, the DHECC takes 983 ms- DT, which is lower when contrasted to the DT of other existing approaches, say ECC (990 ms), RSA (1062 ms), FHE (1027 ms), and DH (1085 ms). Likewise, for the other packet sizes also, the proposed DHECC algorithm shows the lowest DT. ET and DT must be low for an efficient encryption algorithm, and this is acquired by the proposed DHECC.

Fig. 6c. contrasts the SL of the techniques for data transmission in WSNs. The SL obtained by the proposed DHECC is high (94.2%) whereas the existing ECC, FHE, RSA, and DH approaches obtain the SL of 90.25%, 86.8%, 78.95%, and 80.54%. Amongst the existing techniques, the ECC and FE acquire the highest SL, and the RSA and DH obtain the average SL. But when analogized to the DHECC, the existing approaches show lower SL. From this, the proposed DHECC is confirmed to work-well for data transmission and provide the highest SL in the WSNs.

5 Conclusion

WSN networks are susceptible to security attacks because once deployed they become unprotected and unattended. This work proposed diversity centric adaptive moth flame optimization for OPS and DA in WSN. The proposed work undergoes phases, such as network setup, TE, CF and CH selection, DA from optimal path, and key generation and encryption. The DAMFO algorithm is utilized for efficiently doing the DA process, and also a DHECC is adopted for meliorating the SL of data packets against data transmission attacks. The proposed DA and cryptography approaches are contrasted to several conventional approaches for validating the system's performance. The PDR, end to end delay, EC, throughput, and NLT of the proposed DAMFO are gauged by varying the number of nodes as of 20 to 100. The ET, DT, and SL of the proposed DHECC algorithm are also evaluated for disparate sizes of data packets. The DAMFO acquires 0.79bps- throughput, and it meliorates the 88 s- NLT. Contrarily, the

proposed DHECC approach renders 94.2%- SL, and also it takes only 980 ms to encrypt data for packet size 10. Thus, the proposed scheme was found to be secure and energy-efficient to resist disparate attacks. For augmenting the model's performance in respect of NLT and EC in the future, advanced algorithms could be utilized for effective data communication. The proposed model will be extended to various types of WSNs in the future, such as heterogeneous and dynamic WSNs, and will be used to assess sensor node and data transmission performance.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Xindi, Z. Qingfeng and C. Chi-Tsun, "A uav-assisted topology-aware data aggregation protocol in wsn," *Physical Communication*, vol. 34, no. 1, pp. 48–57, 2019.

[2] I. Ummer and M. Ajaz Hussain, "Secure and practical access control mechanism for wsn with node privacy," *Journal of King Saud University-Computer and Information Sciences*, vol. 23, no. 2, pp. 87–101, 2020.

[3] X. Kun, N. Xueping, W. Xin, H. Shiming, N. Zuoting *et al.*, "An efficient privacy-preserving compressive data gathering scheme in wsns," *Information Sciences*, vol. 390, no. 1, pp. 82–94, 2017.

[4] C. Ramalingam and P. Mohan, "An efficient applications cloud interoperability framework using i-anfis," *Symmetry*, vol. 13, no. 2, pp. 1–16, 2021.

[5] T. Ravichandran, "An efficient resource selection and binding model for job scheduling in grid," *European Journal of Scientific Research*, vol. 81, no. 4, pp. 450–458, 2012.

[6] P. Govind Gupta, M. Manoj and G. Kumkum, "Towards scalable and load-balanced mobile agents-based data aggregation for wireless sensor networks," *Computers & Electrical Engineering*, vol. 64, no. 2, pp. 262–276, 2017.

[7] D. Paulraj, "An automated exploring and learning model for data prediction using balanced ca-svm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 4979–4990, 2021.

[8] V. Ramalakshmi, "Honest auction based spectrum assignment and exploiting spectrum sensing data falsification attack using stochastic game theory in wireless cognitive radio network," *Wireless Personal Communications - an International Journal*, vol. 102, no. 2, pp. 799–816, 2018.

[9] K. Mandeep and M. Amit, "Data aggregation algorithms for wireless sensor network: A review," *Ad Hoc Networks*, vol. 100, no. 1, pp. 102083, 2020.

[10] G. Tarek, A. Sarah, E. Mohamed and H. Aboul Ella, "Trust-based secure clustering in wsn-based intelligent transportation systems," *Computer Networks*, vol. 146, no. 1, pp. 151–158, 2018.

[11] A. Amuthan and A. Arulmurugan, "Semi-markov inspired hybrid trust prediction scheme for prolonging lifetime through reliable cluster head selection in wsns," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 10, pp. 1201–1216, 2018.

[12] T. Priyadharshini and T. Chindrella, "An efficient cache consistency scheme in mobile networks," *Wireless Communication*, vol. 3, no. 9, pp. 604–609, 2011.

[13] B. Zhang, H. Zhenhua and X. Yang, "A novel multiple-level trust management framework for wireless sensor networks," *Computer Networks*, vol. 72, no. 2, pp. 45–61, 2014.

[14] Y. Yanli, L. Keqiu, Z. Wanlei and L. Ping, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[15] A. Ramanathan and R. J. Sonia, "Social media networks owing to disruptions for effective learning," *Procedia Computer Science*, vol. 172, pp. 145–151, 2020.

[16] P. Subbulakshmi, "Mitigating eavesdropping by using fuzzy based mdpop-q learning approach and multilevel stackelberg game theoretic approach in wireless crn," *Cognitive Systems Research*, vol. 52, pp. 853–861, 2018.

[17] B. Omar Rafik Merad, S. Sidi Mohammed and F. Mohammed, "A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography," *Ad Hoc Networks*, vol. 32, pp. 98–113, 2015.

[18] S. Divyabharathi, S. Rahini and G. Vijayalakshmi, "Large scale optimization to minimize network traffic using mapreduce in big data applications," in *2016 Int. Conf. on Computation of Power, Energy Information and Commuincation IEEE*, Chennai, India, pp. 193–199, 2016.

[19] B. P. Sankaralingam, U. Sarangapani and R. Thangavelu, "An efficient agro-meteorological model for evaluating and forecasting weather conditions using support vector machine," *Smart Innovation*, *Systems and Technologies Springer*, vol. 2, pp. 65–75, 2016.

[20] L. Xiaowu, Z. Xiaowei, Y. Jiguo and F. Can, "Query privacy preserving for data aggregation in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 32, no. 4, pp. 123–136, 2020.

[21] A. Vinitha and M. S. S. Rukmini, "Secure and energy aware multi-hop routing protocol in wsn using taylor-based hybrid optimization algorithm," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 5, pp 329–345, 2019.

[22] A. Latha, S. Prasanna, S. Hemalatha and B. Sivakumar, "A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks," *Cognitive Systems Research*, vol. 56, no. 2, pp. 14–22, 2019.

[23] G. Edwin Prem Kumar, K. Baskaran, R. Elijah Blessing and M. Lydia, "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," *Computers & Electrical Engineering*, vol. 72, no. 2, pp. 894–909, 2018.

[24] Z. Ping, W. Jianxin, G. Kehua, W. Fan and G. Min, "Multi-functional secure data aggregation schemes for wsns," *Ad Hoc Networks*, vol. 69, no. 23, pp. 86–99, 2018.

[25] M. S. Sumalatha and V. Nandalal, "An intelligent cross layer security based fuzzy trust calculation mechanism (cls-ftcm) for securing wireless sensor network (wsn)," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 1–15, 2020.

[26] G. P. Gupta and S. Jha, "Integrated clustering and routing protocol for wireless sensor networks using cuckoo and harmony search based metaheuristic techniques," *Engineering Application of Artificial Intelligence*, vol. 68, pp. 101–109, 2018.

[27] P. C. S. Rao, P. K. Jana, and H. Banka, "A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks," *Wireless Networks*, vol. 23, no. 7, pp. 2005–2020, 2017.