An Energy Efficient and Bandwidth Aware Optimal Routing for IoT in Agriculture

Jay Kumar Jain (jayjain.research@gmail.com)
Sagar Institute of Research and Technology https://orcid.org/0000-0002-9590-0006
Dipti Chauhan
Prestige Institute of Engineering Management and Research
Palash Jain
Sagar Institute of Research and Technology

Research Article

Keywords: Internet of Things (IoT), IoT in agriculture, Wireless Sensor Network (WSN), Quality of service (QoS), Clustering, Data aggregation, Energy aware routing, IoT security, Advanced Encryption Standard (AES)

Posted Date: April 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-429148/v1

An Energy Efficient and Bandwidth Aware Optimal Routing for IoT in Agriculture

Jay Kumar Jain
Associate Professor
Sagar Institute of Research & Technology, Bhopal, India

Dipti Chauhan
Associate Professor
Prestige Institute of Engineering Management & Research, Indore

Palash Jain
Assistasnt Professor
Sagar Institute of Research & Technology, Bhopal, India

Abstract: The agriculture that is enabled with the Internet of Things (IoT) in addition to Wireless Sensors Networks (WSN) can aid the farmers in monitoring their product along with conditions in real-time. The indispensable issues that one has to confront with WSN are Energy-saving along with effective bandwidth usage. Lately, for the amelioration of network stability together with lifetime, disparate cluster-centered solutions are modeled. Nevertheless, most techniques are merely modeled in an energy-aware manner and utilize merely a distance parameter aimed at the data communication. It is imperative for satisfying the bandwidth use of IoT. Here, a cluster-centered energy as well as bandwidth aware routing model is proposed for agriculture data on IoT-centered WSN. Optimal Clusters Head (CH) selection as well as clustering is performed on the WSN for carrying out cluster-centered Data Aggregation (DA). The novel chaos mapping and Opposition centered Learning Grasshopper Optimization Algorithm (CO2GA) chooses the collection of CH as of agricultural Sensor Nodes (SN). Next, centered upon the distance betwixt the chosen CH and SN, the clusters are generated. The clusters share the data to their CH, and the Chaos key generated Advanced Encryption Standard with Rivest–Shamir–Adleman (CKAES-RSA) algorithm encrypt the aggregated data of CH. Lastly, the encrypted data of IoT data are shared with the Base Stations (BS) or Sink Node (Sn) by means of the optimal routing. Aimed at Optimal Route Selection (ORS), the paper utilizes a Deep Learning (DL) approach, explicitly crossover and mutation-based optimal Multi-Layer Perceptrons (CM-OMLP), which computes the fitness of hidden layer by regarding energy, bandwidth, trust, delay, along with congestion level. The proposed encryption and routing mechanism's results are weighted against the first-rate techniques. The proposed work achieves the highest level of security aimed at the IoT data and fulfills the QoS requirements regarding packet delivery, throughput, delay, along with Network LifeTimes (NLT).

Key words: *Internet of Things (IoT), IoT in agriculture, Wireless Sensor Network (WSN), Quality of service (QoS), Clustering, Data aggregation, Energy aware routing***,** *IoT security***,** *Advanced Encryption Standard (AES).*

1. INTRODUCTION

This world is exceptionally fast-paced where everything is interlinked between each other. These things that are correlated with the internet make them smart [1]. Unparalleled opportunities are

created by the IoT in verticals, namely agriculture, healthcare, industry, along with home automation and also they are quickly spreading [2]. After becoming a part of the IoT, the WSN's potentiality will be completely unleashed [3]. A compilation of distributed along with dedicated sensors aimed at monitoring, organizing, and delivering information to remote locations are WSNs [4]. The upcoming fifty years will be beset by a multitude of severe water-related problems, threatening the welfare of numerous terrestrial ecosystems along with drastically weakening human health, mainly in the globe's poorer areas in the dearth of coordinated planning along with international cooperation at an unparalleled level [5]. The agricultural sector is encountering more issues and bigger challenges, namely falling land fertility and dwindling water reservoirs with the passage of time [6]. An internet-centered technology called the IoT appeared in these previous years for overriding this difficulty [7]. Particularly many advanced computer and information technologies are introduced by smart agriculture systems, namely the IoT, artificial intelligence, along with cloud computing into agricultural production [8]. Thus, the IoT applications permit farmers to examine these data, predict future conditions, and hence, improving productivity, minimizing expenses, and conserving resources [9].

The energy-hole problem in IoT is brought about by the enormous quantity of smart devices and the omnipresent connection demands [10]. Sensing along with transferring data is the task of the smart object [11]. A major criterion in WSN is bandwidth utilization along with energy-saving. Thus, developing the nodes in energy along with a bandwidth-aware manner is important [12]. A utmost energy-efficient architecture is the clustered network, particularly where SN leave in hundreds and thousands of numbers [13]. The environment's data is observed by means of the sensors. A routing technique or algorithm is required to create a network connection for collecting and transmitting data as of the source-destination node [14]. Routing Optimization (RO) strategies for flows are implemented for avoiding network congestion and ensure the QoS necessities of IoT applications [15]. Therefore, it is imperative to comprehend the configurable energy optimization of service composition quality in the IoT environment in the QoS-oriented service portfolio optimization process [16]. The notion of linking with the Internet aimed at performing the operations is given by IoT. There prevails a chance of hacking along with attacking while utilizing the Internet [17].

Machines learning (ML) is a tool in which their requirements are helpful for agriculture, and efficiently uses resources for prediction and management fields namely artificial intelligence in addition to agriculture [18]. Possible security protocols are provided by ML algorithms for IoT devices that are most dependable along with accessible than ever before [19]. An energy and bandwidth-aware routing mechanism, namely CM-OMLP is proposed for the agriculture domain in IoT-centered WSN. In addition, a novel CKAES-RSA for executing secure data transmission (DT) in WSN is proposed by this paper. The QoS and also energy efficiency is enhanced along the network's bandwidth utilization is maximized.

This paper is classified as: Section 2 examines the associated works concerning the proposed work. Section 3 gives the proposed work's full description. Section 4 surveys the experimental outcome. Section 5 completes the paper.

2. RELATED WORK

S. Sujanthi *et al.* [20] developed a Secure-DL (SecDL) aimed at dynamic cluster-centered WSN-IoT networks. The network was planned as Bi-Concentrics Hexagons and also Mobile Sink technology for improving energy efficiency. Dynamic clusters were created in the Bi-Hex network as well as Quality Predictions Phenomenon was employed to select optimum CH, which ensured QoS along with energy efficiency. DA was allowed in every cluster and managed with a '2' way Data Elimination together with a Reduction scheme. For achieving top-level security aimed at aggregated data, the One Time-PRESENT algorithm was designed. After that, for ensuring top-level QoS, the ciphertext was transferred to the mobile sink via an optimal route. Crossover-centered Fitted Deep Neural Networks (Co-FitDNN) was introduced for ORS. This work had attained security, QoS, as well as energy efficiency. But, in a small-level environment, SecDL was appropriate.

Jay Kumar Jain *et al*. [21] developed a Threshold-centered timeslot scheduling (T-TDMA) as well as energy-efficient and secure routing algorithm (ESRA) in the IoT-WSN setting. For allocating the timeslots aimed at every SN, the TDMA system was fixed in the scheduling process. ESRA was designed with '3' sets of methods: (1) Energy-aware route detection utilizing Type-2 Mamdanis Fuzzy Logic (2) Path reliability detection centered upon path reliability utilizing throughput, delay, along with packet loss ratios (3) Route modification. The old route is changed when the S_n is moved from one place to another and the new route is found utilizing the S_n's current location. However, for the routing method, much time is consumed by this technique.

Khalid Haseeb *et al*. [22] introduced an Energy-aware along with Secure Multiple hop Routing protocols through utilizing a secret sharing system for augmenting the energy efficiency's performance by multiple hop data security in opposition to malicious actions. This technique consists of '3' major aspects. Initially, centered upon the node's location, the network field was segmented to inner along with outer zones. Moreover, many clusters were produced according to node neighborhood vicinity in every zone. Secondly, utilizing this method's effective secret sharing system, the DT as of CH to the S_n was secured in every zone. Finally, the data link's quantitative analysis was assessed by this solution for diminution the routing trouble. A trivial answer was given by the provided work with safe data routing in IoT-centered restricted WSNs. But, the performance in heterogeneity networks was decreased by this technique.

K. Thangaramya *et al*. [23] developed Neuros-Fuzzy Rule-centered Cluster Formation along with Routing Protocol aimed at executing effective routing in IoT-centered WSN. The energy modeling was used by the cluster formation in WSN for effectively routing the packets via the application of ML utilizing a Convolutional Neural Networks (CNN) with fuzzy rules aimed at weight adjustment; therefore, the network's lifetime was extended. Besides, they deemed '4' components, like CH's residual energy, space between the CH along with the S_n, space between the SN together with the CH, and the degree of the CH which were major factors for the energy utilization and network life span. However, the supposition of every node was trustful nodes, which weren't always possible.

Khalid Haseeb *et al.* [24] presented a Secure along with Energy-aware Heuristic-centered Routing (SEHR) protocol for WSN for identifying and avert compromising data with effective performance. Initially, this protocol utilized an artificial intelligence-centered heuristic analysis for accomplishing a dependable and intellectual learning scheme. Secondly, the transmissions in opposition to enemy groups were protected for attaining security with minimal complexity. The

SEHR had enhanced the efficacy aimed at network's throughput by 18% average, 42% packet drop ratios, 26% end-to-end delay, 36% energy consumption, 38% faulty routes, 44% network overhead, in tandem with 43% computational overheads in dynamic scenarios when contrasted to prevailing work as shown by the simulation outcomes. However, this method of asynchronous duty cycles betwixt the SNs was not deemed.

Dnyaneshwar S. Mantri *et al*. [25] developed a Bandwidth Efficient Clusters-centered DA (BECDA) aimed at efficient data collecting with in-network aggregation. The network with heterogeneous nodes was deemed concerning energy and mobile sink aimed at aggregating the data packets. The intra along with inter-cluster aggregation had attained the optimum approach on the arbitrarily disseminated nodes with the varying data generation rates. The connection of data was utilized by this algorithm within the packet for implementing the aggregation function on the data produced by nodes. Considerable improvement in PDR (67.44% together with 26.79%) along with throughput (41.25% along with 26.16%) was shown by BECDA as contrasted to the existing solutions.

Jay Kumar Jain *et al*. [26] proposed a bi-layered WSN architecture for dynamic clustering based routing and coverage hole detection and recovery. The proposed work has four steps cluster formation, cluster head (CH) selection, coverage hole detection, and recovery and routing. Clusters are formed by the K-means algorithm. CH is elected by Determined Weight (DW). This DW is calculated by residual energy, distance from cluster and center to the base station. Based on the weight CH is selected. Author implement the proposed approach for Agriculture Applications in WSN assisted with IoT. Finally, we analyse the performance of our proposed approach with respect to following metrics: Energy consumption, Network lifetime, Number of alive nodes and Packet delivery ratio. According to, author comparison of proposed approach and heterogeneous network coverage hole detection and recovery and repair algorithm, our proposed method gives better accuracy results. In proposed approach, energy consumption is reduced, network lifetime is increased, number of alive nodes is high and packet delivery ratio is increased.

3. PROPOSED METHODOLOGY

Presently, WSN is attracting huge attention in numerous applications, like environmental surveillance, smart cities and also battlefield, agriculture management, traffic monitoring, military target monitoring, healthcare tracking, et cetera, owing to IoT's application on large scales. Intelligent routing, in WSN aimed at IoT, has been a vital measure, which is essential aimed at boosting the QoS in the network. It provides an energy-effective and also optimized bandwidth design aimed at communicating in the IoT centred sensor networks. It is the main challenge to evade the huge packet drop, speedy energy depletion, and also the unfairness prevalent over the network causing a decrement in the node's performance and also an increment in the delay regarding packet delivery. This work proffers the energy as well as bandwidth aware routing (CM-OMLP) in IoT centred WSN aimed at the agricultural data by executing the cluster-centred DA. Primarily, the WSN is pondered with a set of IoT SNs that is utilized in the agricultural domain. The agricultural domain SN includes various sensor types, like mechanical sensors, location, airflow, optical, dielectric soil moisture, et cetera. Aimed at performing the cluster-centred DA and also wireless SN's routing in an energy-effective and optimized bandwidth consumption approach, the WSN's CHs are picked optimally utilizing the CO^2GA by

pondering a few parameters, like energy, node centrality, distance, et cetera. Next, centred on the distance betwixt the chosen CH and cluster members (SN), the clusters are created in the network. The WSN's DA is performed that aggregates the SN data as of every optimal CH. A novel (CKAES-RSA) cryptography technique is modelled aimed at attaining higher-level security aimed at the aggregated data. At last, aimed at ensuring high-level QoS, the data encrypted is sent onto the S_n via an optimal route. Aimed at optimal route selection, the work employs the CM-OMLP. Likewise, the protocol proposed attains security, QoS, energy efficacy, and also maximal bandwidth use. Figure 1 exhibits the proposed design's architecture,

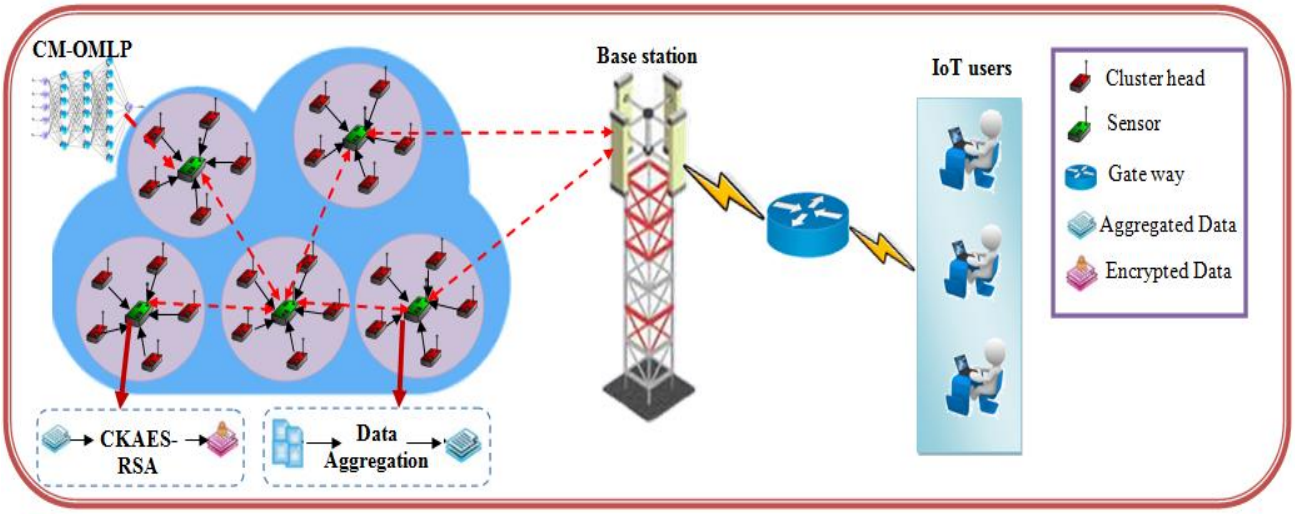


Figure 1: Structural design of the proposed methodology

3.1 Cluster Head Selection

In this work, the WSN's CH selection is optimally performed utilizing the CO^2GA, which enumerates the fitness centred on energy, distance, node degree, and also centrality. The CO^2GA's inputs are the set of the WSN's SN ($S_1, S_2, ...S_N$) and the output attained by the OLGOA are the WSN's CH. The grasshoppers' swarm behaviour in nature is implemented by the Grasshopper Optimization Algorithm (GOA). Like all other swarm algorithms, every grasshopper or individual specifies a candidate solution, arbitrarily produced in initialization. The finest grasshopper is elected as the leader in relation to the evaluation function. The leader attracts the other grasshoppers towards it. Finally, all grasshoppers travel to the leader grasshopper. GOA comprises the lesser accuracy and also slower convergence problems. It is simple to incorporate within the local optima. Also, GOA and its alterations can't perform efficiently in resolving the higher-dimensional optimization issues. This work involves '2' diverse methodologies, like chaos mapping and Opposition centred Learning (OL), into the traditional GOA aimed at overcoming the drawbacks like this. Implementation of these techniques into GOA handles the initial population's diversity aimed at global search, boosts GOA's quality, and increments the probability of attaining global optimal solution in the CH's selection procedure. This Chaos mapping and OL centred GOA (CO) is termed COGOA that is furthermore shortened as CO^2GA.

Step 1: Initially, the CO^2GA's population is initialized centred on the logistic chaos mapping as

$$S_{i+1} = a \times S_i\left(1 - S_i\right) \tag{1}$$

Here, the parameter a signifies the random positive integer. Usually, it is fixed as 4.

Step 2: Signify N as the population's size and then D as the search dimension; then, create the population's logistic map sequence (in relation to S_{i+1}) as,

$$s_{ij}\left(i = 1,2\Lambda\ N\ and\ j = 1,2,\Lambda\ D\right) \tag{2}$$

Step 3: Create the grasshoppers' ($S_1, S_2, ...S_N$) initial population $\left(P_I = S_{ij}\right)$or else its position by mapping it into the search space, in relation eqn. (3),

$$S_{ij} = s_{ij}\left(U_j - L_j\right) + L_j + T_i + Q_i + W_i \tag{3}$$

Herein, S_{ij} implies the i^{th} grasshopper's j^{th} dimension; L_j and U_j implies the jth dimension's lower as well as upper bounds. $T_i, Q_i, and\ W_i$ signify the social interaction, gravity force, and then wind advection. The grasshoppers' movements are fully simulated by these components; however, the core component, which emerges out of the grasshoppers themselves is the social interaction talked about as:

Step 4: Examine each individual's objective function or else fitness (O_F) in S_{ij} by pondering the node's energy consumption (E_c), distance (D_t), centrality (C_f), and also node degree (N_d) prevalent in the network. The CO^2GA's O_F is equated as,

$$O_F = \frac{\alpha.E_c + \beta.N_d + \gamma.C_f}{\lambda D_t} \tag{4}$$

Here, $\alpha, \beta, \gamma, and\ \lambda$ signify the weight values of $E_c, N_d, C_f\ and\ D_t$ that are chosen in a manner that $\alpha + \beta + \gamma + \lambda = 1$. The $E_c, N_d, C_f\ and\ D_t$ parameters' expressions along with their explanation are described as,

- ✓ ***Energy consumption**:* E_c specifies the node's current energy level, which is enumerated as the divergence betwixt a node's initial energy and a node's total consumed energy over a period. As the CH is accountable aimed at data gathering and also DA, a node comprising greater E_c is selected as the CH.

- ✓ ***Node degree**:* N_d determines the measurement of the number of neighbouring nodes linked with the candidate node. As the candidate nodes comprising greater cluster members lose their energy in less duration, the candidate node comprising less number of sensors is chosen as the CH. The node's N_d prevalent in the WSN is enumerated utilizing the eqn.(5),

$$N_d = \sum_{i=1}^{N} N_i \tag{5}$$

Here, N_i implies the number of SNs originating as of CH_i.

- ✓ ***Centrality factor:*** C_f specifies the candidate node's closeness with its neighbours. It enumerates the average distance betwixt the candidate node and its neighbouring nodes; that is analyzed utilizing eqn.(6),

$$C_f = \frac{N_d - 1}{\sum_{i \neq j} d(i, j)} \tag{6}$$

- ✓ **Distance:** D_t determines the distance as of the candidate node up to mobile S_n towards the BS. In data transmission, the node comprising a less distance as of the S_n is pondered as CH. The CO^2GA's D_t is equated as,

$$D_t = \sum_{i=1}^{N} dis(CH_i, M_{sn}) \tag{7}$$

Step 5: Past initialization and then fitness examination, the T_i's computation aimed at the i^{th} grasshopper is equated as,

$$T_i = \sum_{\substack{p=1 \\ p \neq i}}^{N} t(d_{ip}) \hat{d}_{ip} \tag{8}$$

Here, d_{ip} signifies the distance betwixt i^{th} and p^{th} grasshopper; $\hat{d}_{ip}$ implies a unit vector; t is a function, which determines the social forces. Every parameter is articulated via the subsequent expressions as,

$$d_{ip} = \left| s_p - s_i \right| \tag{9}$$

$$\hat{d}_{ip} = \frac{s_p - s_i}{s_{ip}} \tag{10}$$

$$t(r) = a e^{\frac{-r}{l}} - e^{-r} \tag{11}$$

Here, a implies the attraction's intensity; l signifies the attractive length scale.

Step 6: Normalize the distance betwixt individuals for solving the function t's problems, since the function t does not possess the capability to implement strong force betwixt grasshoppers that comprising maximal distances betwixt them.

Step 7: Calculate the CO^2GA's Q_i and W_i utilizing eqns. (12) and (13)

$$Q_i = -q\left(\overline{\omega}_{e_w}\right) \tag{12}$$

$$W_i = w\left(\overline{\omega}_{e_{dw}}\right) \tag{13}$$

Here, q signifies the gravitational constant; $\left(\overline{\omega}_{e_w}\right)$implies the unity vector towards the earth's centre; w signifies a drift constant; $\left(\overline{\omega}_{e_{dw}}\right)$ symbolizes the unity vector in the wind's direction.

Step 8: The population attained past every iteration is signified as,

$$P = \left\{S_{ij}\right\} \tag{14}$$

$$S_{ij} = s_{ij}\left(U_j - L_j\right) + L_j + \sum_{\substack{p=1 \\ p \neq i}}^{N} t \cdot \left|s_p - s_i\right| \cdot \left(\frac{s_p - s_i}{s_{ip}}\right) - q\left(\overline{\omega}_{e_w}\right) + w\left(\overline{\omega}_{e_{dw}}\right) \tag{15}$$

Step 9: Create the S_{ij}'s opposite population (S_{ij}^{OL}) to execute OL. OL is utilized to enumerate the grasshoppers' opposite solutions at every iteration's end; executing this not just boosts the population's quality and its diversity; however, it also increments the probability of looking for global optimal solutions.

$$S_{ij}^{OL} = \left(S_{ij}\right)^{\perp} \tag{16}$$

$$\left(S_{ij}\right)^{\perp} = U_j + L_j - S_{ij} \tag{17}$$

Step 10: Combine the population of (S_{ij}^{OL}) and S_{ij} P and also P′; then organize the merged one's result in the ascending order regarding the fitness value. Choose the 1st N-individuals comprising good fitness value like the best CH or else grasshoppers to execute the succeeding iteration. At last, by executing n number of iteration, the optimal CHs are chosen. Figure 2 exhibits CO^2GA's pseudo-code aimed at CH selection.

CO²GA for CH selection

Input: Set of SNs in WSN

Output: Optimally selected CHs for data aggregation

Begin

Initialize the CO²GA parameters U_j, L_j *and* M_{iter}

Initialize the population of SNs in the WSN with chaos variable

Compute the O_F of each individual by considering E_c, D_t, C_f, *and* N_d

Choose the best search agent

While $(i < M_{iter})$

Update S_{ij}

for each S_i in the search space do

Normalize the distance between individuals

Compute Q_i and W_i of the CO2GA

Update S_{ij} after each iteration

Generate S_{ij}^{OL} by sorting the individuals with O_F

Merge the population of S_{ij} with S_{ij}^{OL}

Select the first N individuals with better O_F

end for

$t = t + 1$

Return best search agents

End

Figure 2: Pseudocode of CO²GA

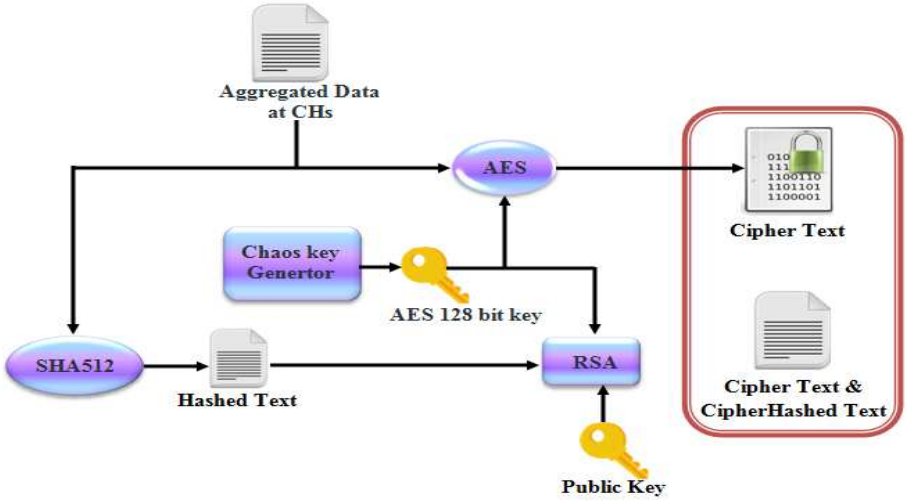
3.2 Cluster Formation

Past the WSN's CH selection, every CH conveys a join request (J_R) onto its neighbouring SN. Every non-CH node enumerates its distance from the CH by acquiring the requested message. After that, the node conveys a J_R onto the chosen CH that comprises a minimal distance. Whilst the CH is nearer to the node, the energy efficacy and QoS can be enhanced. Hence, clustering is executed here centred on the distance metric. Past the SN's cluster formation utilizing the chosen CH, in all clusters, the SN's sensed data are aggregated by its CH.

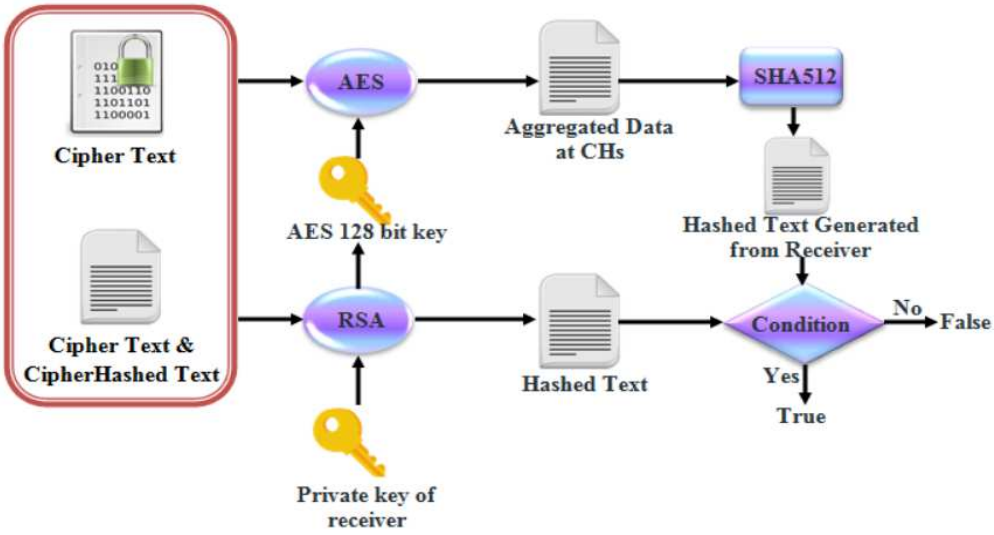
3.3 Encryption

The CH executes encryption aimed at securing the aggregated data A_D, past the data packets' collection as of the cluster members. This work proposes a new technique aimed at encryption termed CKAES-RSA, which is a compilation of chaos mapping, symmetric block cipher (AES), and also asymmetric encryption technique (RSA). The AES is utilized aimed at attaining

confidentiality; the RSA is utilized aimed at acquiring authenticity, integrity, and also non-repudiated centred digital signature; the chaotic keys generator is employed aimed at creating random keys to execute encryption and also decryption. The reason to select the chaos sequences aimed at key generation is the chaotic sequences prevalent in the non-linear systems; they have been extremely sensitive to alterations in an initial value, and also the strings provided by the chaotic systems aren't just random however regenerative. The proposed CKAES-RSA's encryption (E_c) and also decryption (D_c) are detailed below; figure 3 exhibits the CKAES-RSA's diagrammatic workflow.



(a) Encryption



(b) Decryption

Figure 3: Workflow of proposed CKAES-RSA

Encryption: Primarily, A_D has been encrypted at every CH by executing a triple encryption technique. This signifies that the data has been encrypted first utilizing AES with a 128-bit Chaos Key's (CH_K) help created utilizing the chaos random sequence. Next, A_D is modified into hashed data (H_{D1}) utilizing the SHA-512's hash function; then, this hashed data is again encrypted utilizing the RSA; also, the CH_K produced aimed at AES has been encrypted utilizing the RSA. The CH_K is created utilizing the logistic chaos map that is articulated as,

$$X_{n+1} = 1 - 2(X_n)^2 \tag{18}$$

Here, (X_n) ranges as of $-1\ to\ 1$ and also $n = 0,1$. Therefore, '2' ciphertext kinds are obtained totally on the receiver side: One is the ciphertext 1 (C_1) that is acquired by implementing the AES block cipher with CH_K and the next one is the ciphertext 2 (C_2) and the cipher key (C_K) that is attained by implementing RSA on the $SHA-512$ hashed data and also on the CH_K.

Decryption: In the D_c procedure**,** the acquired $C_1, C_2, and\ C_K$ have been encrypted by the subsequent process. Primarily, by implementing RSA, $C_2\ and\ C_K$ are decrypted. The decrypted C_K is utilized as a key aimed at decrypting C_1 that provides the CH's A_D. This A_D is next hashed utilizing the $SHA-512$; then, this hashed data (H_{D2}) is examined with the H_{D1} that is decrypted utilizing the RSA. If the H_{D1} and H_{D2} are identical, it implies that the data is received securely at the BS, or else, it is signified as an attacked data. Herein, the proposed methodology's integrity is examined. The A_D's security level is immensely decremented by executing triple encryption.

3.4 Path Selection

Past data encryption, the CH sends the aggregated ciphertext onto the S_n along the optimal path. The trusted optimal path's selection aimed at data transmission yields QoS. This selection boosts the security level. This work proffers a DL technique termed CM-OMLP, which chooses a trusted optimal route aimed at data transmission. Processing route selection in a deep structure obtains efficient performance. MLP is stated as a monitored learning technique, which studies a non-linear function and also maps inputs onto the outputs via training. Provided a set of inputs $R_i = R_1, R_2, ...R_n$, and also outputs $OR_i = OR_1, OR_2, ...OR_v$, in which n signifies the number of inputs and then v implies the number of outputs; the MLP study a non-linear function approximator ($f(.): R \to OR$) aimed at classification or else regression. The MLP comprises 3 or else many layers (an Inputted Layer (IL), an Outputted Layer (OL), and also one or else many Hidden Layers (HLs)).

CM-OMLP implements the crossover and also mutation procedures on MLP's 1st layer aimed at creating every accessible path betwixt CH and S_n. After that, every route is analyzed

centred on the HL's fitness function. The optimal route is chosen in the OL aimed at data transmission. Figure 4 exhibits the proposed CM-OMLP's overall structure.

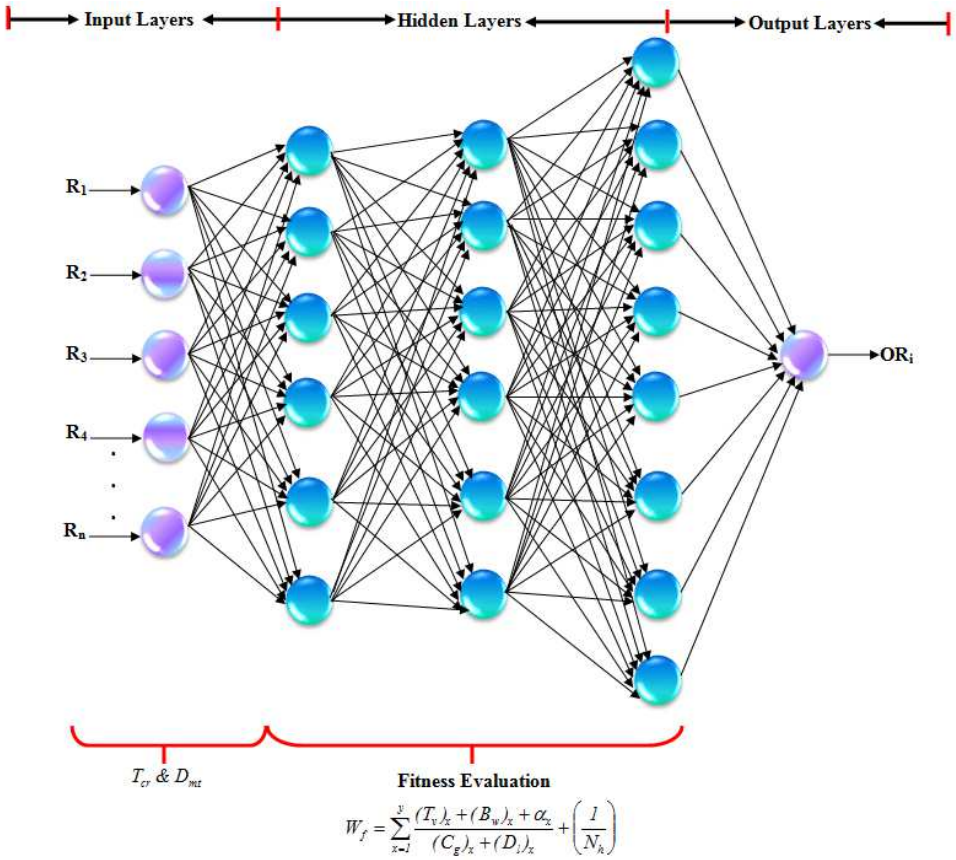


Figure 4: Structure of CM-OMLP

Input layer: IL comprises inputted neurons. Here, the candidate routes $\left(R_i = R_1, R_2, ...R_n\right)$have been initialized aimed at data transmission. The direct routes betwixt the source CH and the S_n are termed candidate routes.

Hidden layers: The CM-OMLP comprises numerous HL (till G) as $\left(H_i = H_1, H_2, ...H_G\right)$. In the HL, every neuron gathers the values as of the former layer as a weighted linear summation comprising a bias, pursued by a non-linear activation function. In the 1st HL, the CM-OMLP implements a cross-over operator on the inputted routes, and then the mutation operator is implemented on the crossover operator's results. This work utilizes the '2'-point cross-over (T_{cr}) and also the displacement mutation (D_{mt}) operators on the inputted neurons aimed at attaining a novel solution. Figure 5 exhibits the crossover and also mutation operations' working.

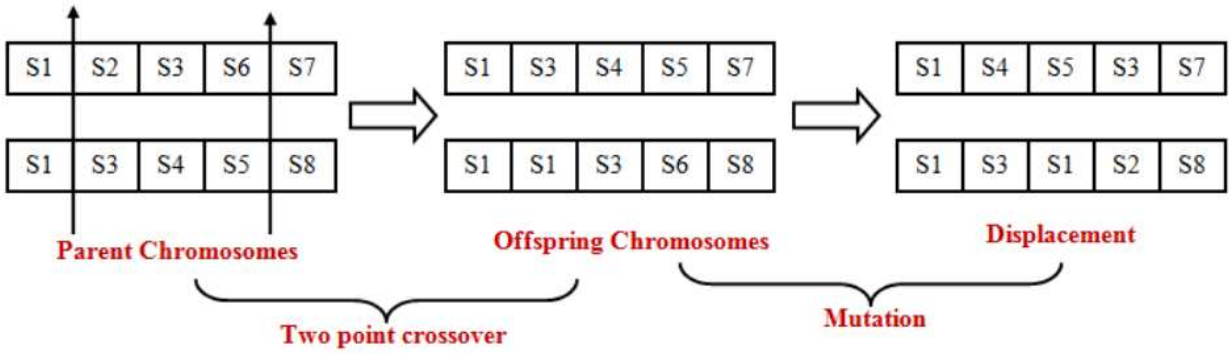


Figure 5: Working of crossover and mutation

Every accessible route as of CH towards S_n has been determined by executing crossover and also mutation. It is signified as $C_M(R_i) = R_1, R_2, ...R$. Next, every route is offered with a weight value in the HLs. Here, rather than creating the MLP's weight value arbitrarily, the weight value is optimally enumerated regarding fitness value or else adaptive weight factor W_f. The CM-OMLP's W_f is enumerated utilizing eqn. (20) that ponders the metrics, like bandwidth (B_w), delay (D_l), congestion (C_g), trust (T_v), energy (E_c), and number of hops (N_h). B_w signifies the existent bandwidth betwixt the nodes; D_l is calculated centred on the propagation, processing, and also queuing delay presented in that node; C_g determines the number of packets existent in the buffer; N_h counts up the number of hops betwixt CHs and BS. But, the T_v is enumerated as the nodes' forwarding capability in a route. The trust value aimed at the p node is enumerated as,

$$T_v = \sum_{q=1}^{n} \frac{Nb_{pq} + 1}{Nb_{pq} + Mb_{pq} + 2} \tag{19}$$

Here, Nb_{pq} and Mb_{pq} signifies the node p 's normal and malevolent behaviour, which is observed by the q node. The normal behaviour counts up the number of packets transmitted successfully by the node; the malicious behaviour counts up the number of packets the node drops.

$$W_f = \sum_{x=1}^{y} \frac{(T_v)_x + (B_w)_x + \alpha_x}{(C_g)_x + (D_l)_x} + \left(\frac{1}{N_h}\right) \tag{20}$$

Herein, x signifies the x^{th} node prevalent in R; y implies the number of nodes prevalent in the route R. The HL's output is equated as,

$$H_i = \rho\left(\sum_{i=1}^{n} W_{fi} R_i + b_i\right) \tag{21}$$

Herein, $\rho(.)$ implies the Leaky ReLU's (LReLU's) non-linear activation function; W_{fi} signifies the adaptive weight factor; b_i symbolizes the HL's bias value.

Output Layer: The final OL chooses the optimal route as of every existent route created in HLs. The output is equated as,

$$OR_i = \rho.\left(W_f\right)_G.\rho\left(W_f\right)_{G-1}.\rho\left(....\left(W_f\right)_1\right) \tag{22}$$

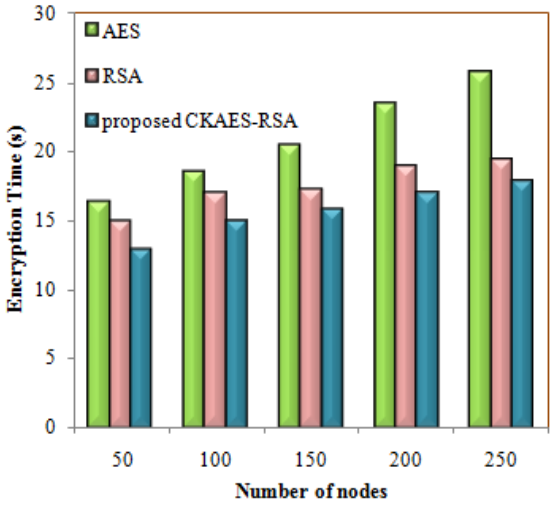
The CH sends the encrypted aggregate data onto the BS via this OR_i. The BS transmits the data received by the cloud server. After acquiring the data as of the cloud server, on the receiver side, the data encrypted is decrypted utilizing the proposed CKAES- RSA technique and then utilized by the users.

4. RESULTS AND DISCUSSION

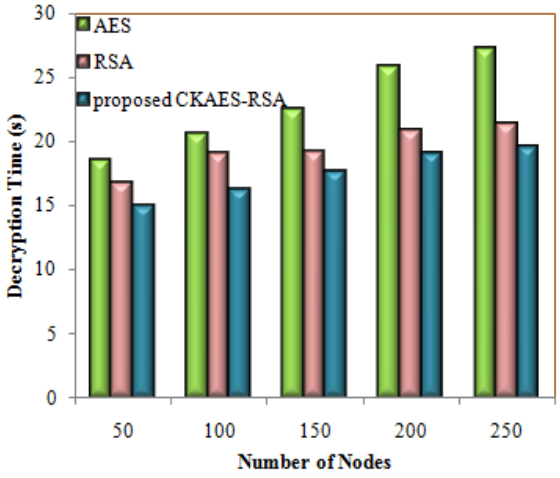
CM-OMLP and CKAES-RSA are the '2' mechanisms proposed in this paper for executing energy along with bandwidth-aware routing mechanism of agriculture data safely in IoT-centered WSNs. The proposed one is applied in the Network Simulator-2 (NS2) with the following parameters: network range [1000m x 1000m], total nodes considered - 250, Initial energy level –750J, number of packets -1000, and packet size – 1024bits. The proposed method's results are contrasted with the prevailing work regarding few performance metrics, which are provided in the below section.

4.1 Performance Analysis of CKAES-RSA

The proposed CKAES-RSA's performance is analyzed by this phase with existing techniques namely, Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) concerning encryption time (ET) along with decryption time (DT), which are shown in figure 4. The efficient performance of the proposed CKAES-RSA is understood by the results.



(a)



(b)

Figure 6: ET and DT of proposed CKAES-RSA with existing methods

Figure 6 demonstrates the performance of the proposed CKAES-RSA with conventional methodologies, like AES along with RSA. The proposed CKAES-RSA's fastest ET is shown in Figure 6 (a). The CKAES-RSA encrypts the data in 12.78s for '50' nodes, while the ET of 16.25s and 18.42s is taken by the existing AES and RSA. AES and RSA acquire the ET of 20.37s and 17.16s for '150' nodes of data, while the CKAES-RSA encrypts the data in a lesser time (15.67s). Likewise, a large amount of ET is taken by a huge quantity of nodes. The CKAES-RSA encrypts the data in 17.76s for '250' numbers of node data. The DT's performance for the encryption algorithms is shown in Figure 6 (b). The DT of existing AES and RAS is 18.45s and 16.62s for '50' nodes of data, while the proposed CKAES-RSA takes 14.78s for decrypting the data. Similarly, for 100 nodes of data, a vast quantity of time is taken by the existing AES (20.49s) and RSA (18.92s) for decrypting the data, whereas lesser time is taken by the proposed CKAES-RSA (16.98s) for decryption. The proposed CKAES-RSA possesses a lowest value of DT for all nodes (50-250). These results understand the proposed CKAES-RSA's better performance for secure encryption along with decryption.

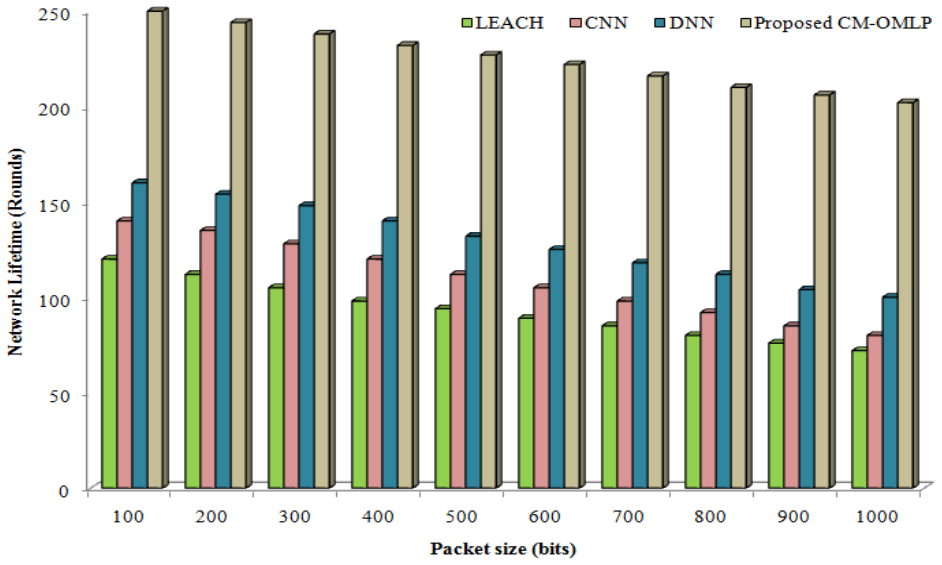
4.2 Performance Analysis of CM-OMLP

The proposed CM-OMLP's performance is analyzed by this section with existing techniques, namely Low-energy adaptive clustering hierarchy (LEACH), CNN, along with Deep Neural Network (DNN) centered on two scenarios: network size and also the packet size. The proposed ones are contrasted with existing methodologies concerning few performance metrics namely Packet Delivery Ratio(P_{DR}), Throughput(T_{hr}), along with Network life time(N_{LT}). The technique's results for the first scenario (network size) are displayed in table 1.

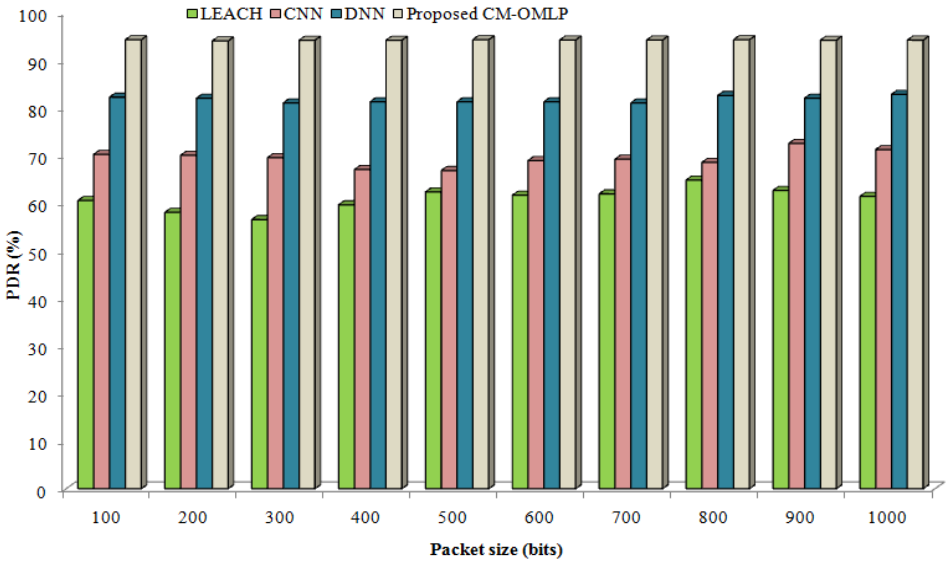
Table 1: Performance of proposed CM-OMLP with existing techniques

Metrics	*Number of nodes*	*Techniques*			
		LEACH	CNN	DNN	proposed CM-OMLP
Packet Delivery Ratio (%)	20	65.56	70.01	85.25	95.29
	40	66.32	70.56	84.56	94.85
	60	65.23	72.68	84.69	94.63
	80	66.89	71.82	83.99	93.56
	100	66.01	72.32	84.88	95.23
Throughput (%)	20	71.98	76.01	80.09	95.89
	40	68.52	78.77	82.56	95.23
	60	64.89	74.03	80.23	94.86
	80	66.58	72.89	78.23	94.02
	100	62.56	70.88	76.89	93.56
Network Lifetime (rounds)	20	85	110	150	200
	40	95	115	160	210
	60	90	120	170	220
	80	100	118	180	230
	100	105	120	190	240

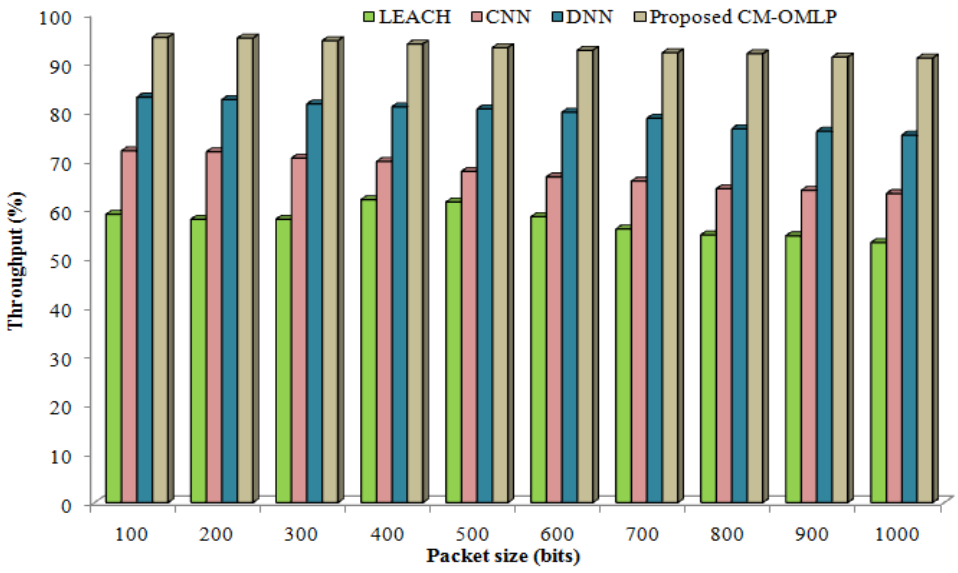
Table 1 shows the proposed CM-OMLP's performance with existent techniques, like LEACH, CNN, and DNN. Initially, P_{DR} is contrasted between proposed and previous research works. A measure of the total packets delivered by the optimal routing as of source-destination is the metric P_{DR}. P_{DR} is also augmented with the increase in the number of nodes. For '100' numbers of nodes, above 95% P_{DR} is provided by CM-OMLP. Concurrently, LEACH, CNN, and DNN only sent 66.01%, 72.23%, and 84.88% packets without loss. After that, the T_{hr} attained by proposed CM-OMLP is contrasted with prior existing works. The T_{hr} is reduced with an increase in network size as shown by the analysis. 95% of T_{hr} is attained by the proposed CM-OMLP for '20' nodes, while the existing LEACH (71.98%), CNN (76.01%), and DNN (80.09%) attain lower throughput than CM-OMLP. Besides, the proposed CM-OMLP improves the network's lifetime even with a huge quantity of nodes over other techniques as shown by the results of techniques for 'N_{LT}'. N_{LT} is also increased when the total nodes increases. The proposed CM-OMLP attains 240rounds (the first node dies at 105th round) for '100' numbers of nodes, but the existing LEACH, CNN, and DNN dies in 105, 120, and 190th rounds. For all the other nodes also, the highest N_{LT} is achieved by the CM-OMLP. The results of techniques centered on packet size are shown in figure 7.


LEACH
CNN
DNN
Proposed CM-OMLP
Network Lifetime (Rounds)
250
200
150
100
50
0
100
200
300
400
500
600
700
800
900
1000
Packet size (bits)

(a)


LEACH
CNN
DNN
Proposed CM-OMLP
PDR (%)
100
90
80
70
60
50
40
30
20
10
0
100
200
300
400
500
600
700
800
900
1000
Packet size (bits)

(b)



(c)

Figure 7: Lifetime, PDR, and throughput of the techniques

Figure 7 demonstrates the results of $N_{LT}, P_{DR}, and\ T_{hr}$ for the proposed and existing techniques centered on packet size. The attained results of the techniques for the number of packet sizes (100 to 1000) are shown centered on the packet size. Initially, when contrasting the technique's results concerning N_{LT} (figure 7 (a)), the highest N_{LT} is attained by the proposed CM-OMLP for every packet plotted. The proposed CM-OMLP acquires a N_{LT} of 250 rounds when the number of packet size is 100bits, which is higher than the N_{LT} of existing LEACH (120), CNN (140), and DNN (160). The N_{LT} will reduce when the number of packet sizes increases, and the highest value of N_{LT} is attained by the CM-OMLP for every packet size when compared with LEACH, CNN, and KNN.

The P_{DR} results are planned for techniques in figure 7 (b). When implementing the techniques, the P_{DR} value shows the packet's percentage sent to the destination. If it is high, the technique fulfills the QoS requirements along with energy efficiency in the network. The existing LEACH provides the very lowest score of P_{DR} (60.5%) among all for the packet size of 100 (bits). The average performance in the network is attained by the CNN and DNN. They provide 70.2 and 82.2 of P_{DR} for 100bits, but 94.25% of P_{DR} is provided by the proposed CM-OMLP, which is higher than every other existing work. Besides, the CM-OMLP provides good results for the remaining packet sizes (200 to 1000bits) also. After the packet size or network's node increases, the network' P_{DR} not gradually increase or reduce. It will differ for every time of transmission. The P_{DR} is achieved by the CM-OMLP in the range of (94%) for every bit, which is very higher than others.

Next, the comparison results of methods are planned centered on $T_{hr}(\%)$ in figure 7 (c). When the number of node count or packet size augments, the value of T_{hr} will reduce. 95.23% of T_{hr} is attained by the CM-OMLP for 100 bits, while the existing LEACH, CNN, and DNN attain 59, 72, and 83% of T_{hr} that are less when weighted against the T_{hr} of CM-OMLP. Likewise, the CM-OMLP acquires the highest T_{hr} for every packet size. Therefore, better results are achieved by the proposed work for all the metrics. The CM-OMLP focuses on every '3' main aspects, namely QoS, energy efficiency, along with security, which is the major reason behind the results. The network lifetime will be enhanced in the existence of better QoS and strong security. The performance analysis of the techniques centered on delay is demonstrated in figure 8.

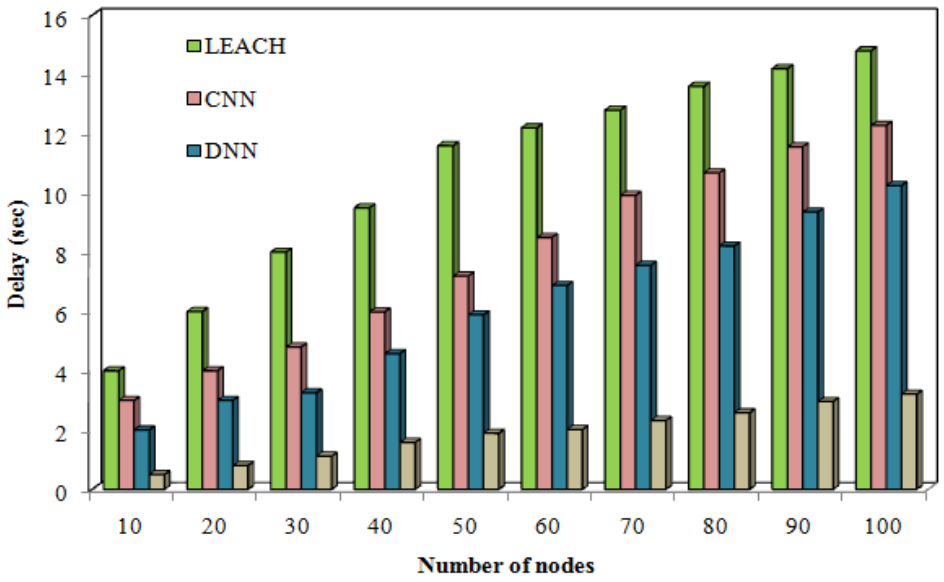


Figure 8: Delay of the techniques

Figure 8 demonstrates the comparison graph of the proposed and existing works concerning the delay (seconds). The time taken by a data packet for reaching its destination as of the source is measured by delay along with the highest performance of the system for the network is indicated by the delay's lowest value. The number of nodes is differed from 10 to 100, the delay is estimated for the techniques. The delay of the CM-OMLP is 0.5s for '10' nodes, but the delay of 4, 3, and 2s is acquired by the existing LEACH, CNN, and DNN that are higher than CM-OMLP. Similarly, the lowest time (delay) is taken by the CM-OMLP for delivering the packets as of source to destination for the remaining nodes. Due to improper algorithm and initial path set-up phase, the existing works cannot minimize the delay. However, optimal CH is elected by the proposed CM-OMLP and the data is aggregated. Furthermore, the energy-efficient route is chosen for DT. Therefore, the delay of the network is reduced by the CM-OMLP.

5. CONCLUSION

In this work, an energy and bandwidth aware routing method named CM-OMLP has been proffered aimed at the agricultural data prevalent in the IoT centred WSNs. Furthermore, to execute secured data transmission in WSN, a new CKAES-RSA is presented in this work. The work proposed is analogized with the existent works like LEACH, CNN, and also DNN

concerning a few performance metrics, like N_{LT}, P_{DR}, $and\ T_{hr}$. The analogy outcomes exhibit an efficient performance of the CM-OMLP proposed in both the network's and packet's size circumstances. The CKAES-RSA's ET and DT consume lesser time aimed at the data's encryption and also decryption analogized with the existent AES and also RSA. So as of the outcomes, it is noticed that the clustering centred routing methodology's implementation boosts the bandwidth's utilization and also network's lifetime. CKAES-RSA's execution boosts the IoT data's security level whilst it is sent as of the source onto the destination. In IoT, utilization of these methods yields efficient outcomes. This work can be prolonged in the upcoming future aimed at offering an optimal load balancing methodology aimed at the IoT agricultural data, for evading heavy traffic or else bottlenecks on specific nodes or else on the IoT network's paths.

DECLARATION

*Funding: **Not applicable.**
*Conflicts of interest/Competing interests: **Not applicable.**
*Availability of data and material: **Not applicable.**
*Code availability: **Not applicable.**

REFERENCES

1. Sanika Ratnaparkhi, Suvaid Khan, Chandrakala Arya, Shailesh Khapre, Prabhishek Singh, Manoj Diwakar, and Achyut Shankar, "Smart agriculture sensors in IOT: A review", Materials Today: Proceedings, 2020, 10.1016/j.matpr.2020.11.138.

2. Kutila Gunasekera, Armando Navas Borrero, Fabian Vasuian, and Kim P. Bryceson, "Experiences in building an IoT infrastructure for agriculture education", Procedia Computer Science, vol. 135, pp. 155-162, 2018, 10.1016/j.procs.2018.08.161.

3. Mohammad Samunul Islam and Golap Kanti Dey, "Precision agriculture: renewable energy based smart crop field monitoring and management system using WSN via IoT", In IEEE International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1-6, 2019, 10.1109/STI47673.2019.9068017.

4. Madhvi Saxena, and Subrata Dutta, "Improved the efficiency of IoT in agriculture by introduction optimum energy harvesting in WSN", In IEEE International Conference on Innovative Trends in Information Technology (ICITIIT), pp. 1-5, 2020, 10.1109/ICITIIT49094.2020.9071549.

5. Sushanth G and Sujatha S, "IOT based smart agriculture system", In IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1-4, 2018, 10.1109/WiSPNET.2018.8538702.

6. Uddin M. Ammad, Ali Mansour, Denis Le Jeune, and El Hadi M. Aggoune, "Agriculture internet of things: AG-IoT", In IEEE 27th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-6, 2017, 10.1109/ATNAC.2017.8215399.

7. Murugaiyan Pachayappan, Ganeshkumar C, and Narayanasamy Sugundan, "Technological implication and its impact in agricultural sector: An IoT Based

Collaboration framework", Procedia Computer Science, vol. 171, pp. 1166-1173, 2020, 10.1016/j.procs.2020.04.125.

8. Fanyu Bu, and Xin Wang, "A smart agriculture IoT system based on deep reinforcement learning", Future Generation Computer Systems, vol. 99, pp. 500-507, 2019, 10.1016/j.future.2019.04.041

9. Badreddine Miles, El-Bay Bourennane, Samia Boucherkha, and Salim Chikhi, "A study of LoRaWAN protocol performance for IoT applications in smart agriculture", Computer Communications, vol. 164, pp.148-157, 10.1016/j.comcom.2020.10.009.

10. Zijing Wang, Xiaoqi Qin, and Baoling Liu, "An energy-efficient clustering routing algorithm for WSN-assisted IoT", In IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, 2018, 10.1109/WCNC.2018.8377171.

11. Santiago S and Arockiam L, "A novel fuzzy based energy efficient routing for Internet of Things", In IEEE International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), pp. 1-4, 2017, 10.1109/ICAMMAET.2017.8186645.

12. Mohammed Falih Hassan, Shiva Raj Pokhrel, and Bahaa Al-Musawi, "Energy-Balanced and Distributed Clustering Protocol for IoT Wireless Sensors", In IEEE Wireless Communications nd Networking Conference Workshops (WCNCW), pp. 1-6, 2020, 10.1109/WCNCW48565.2020.9124835.

13. Syed Bilal Shah, Zhe Chen, Fuliang Yin, Inam Ullah Khan, and Niqash Ahmad, "Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks", Future Generation Computer Systems, vol. 81, pp. 372-381, 2018, 10.1016/j.future.2017.09.043.

14. Omkar Singh, Vinay Rishiwal, Lalit Kumar, and Preeti Yadav, "Secure Energy Aware Routingin Wireless Sensor Networks", In 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1-6, 2019, 10.1109/IoT-SIU.2019.8777705.

15. Shizhong Xu, Xiong Wang, Guangxu Yang, Jing Ren, and Sheng Wang, "Routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint", Journal of Communications and Networks, vol. 22, no. 2, pp. 145-158, 2020.

16. Xiaojing Zhu, "Energy optimization of the configurable service portfolio for IoT systems", Computer Communications, vol. 154, pp. 491-500, 2020.

17. Sakshi Anand, and Avinash Sharma, "Assessment of security threats on IoT based applications", Materials Today: Proceedings, 2020, 10.1016/j.matpr.2020.09.350.

18. Huang Xing, and Li Xiaofeng, "Agricultural labor market equilibrium based on FPGA platform and IoT communication", Microprocessors and Microsystems, pp. 103332, 2020.

19. Syeda Manjia Tahsien, Hadis Karimipour, and Petros Spachos, “Machine learning based solutions for security of Internet of Things (IoT): A survey”, Journal of Network and Computer Applications, vol. 161, pp. 102630, 2020, 10.1016/j.jnca.2020.102630.

20. Sujanthi S and Nithya Kalyani S, “SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT”, Wireless Personal Communications, vol. 114, no. 3, pp. 2135-2169, 2020.

21. Jay Kumar Jain, “Secure and energy-efficient route adjustment model for internet of things”, Wireless Personal Communications, vol. 108, no. 1, pp. 633-657, 2019.

22. Khalid Haseeb, Naveed Islam, Ahmad Almogren, Ikram Ud Din, Hisham N. Almajed, and Nadra Guizani, “Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs”, IEEE Access, vol. 7, pp. 79980-79988, 2019.

23. Thangaramya K, Kanagasabai Kulothungan, R. Logambigai, M. Selvi, Sannasi Ganapathy, and Arputharaj Kannan, “Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT”, Computer Networks, vol. 151, pp. 211-223, 2019.

24. Khalid Haseeb, Khaled Mohamad Almustafa, Zahoor Jan, Tanzila Saba, and Usman Tariq, “Secure and energy-aware heuristic routing protocol for wireless sensor network”, IEEE Access, vol. 8, pp. 163962-163974, 2020.

25. Dnyaneshwar S.Mantri, Neeli Rashmi Prasad, and Ramjee Prasad, “Bandwidth efficient cluster-based data aggregation for Wireless Sensor Network”, Computers & Electrical Engineering, vol. 41, pp. 256-264, 2015.

26. Jain, Jay Kumar. "A Coherent Approach for Dynamic Cluster-Based Routing and Coverage Hole Detection and Recovery in Bi-layered WSN-IoT." Wireless Personal Communications 114, no. 1 (2020): 519-543.

Figures

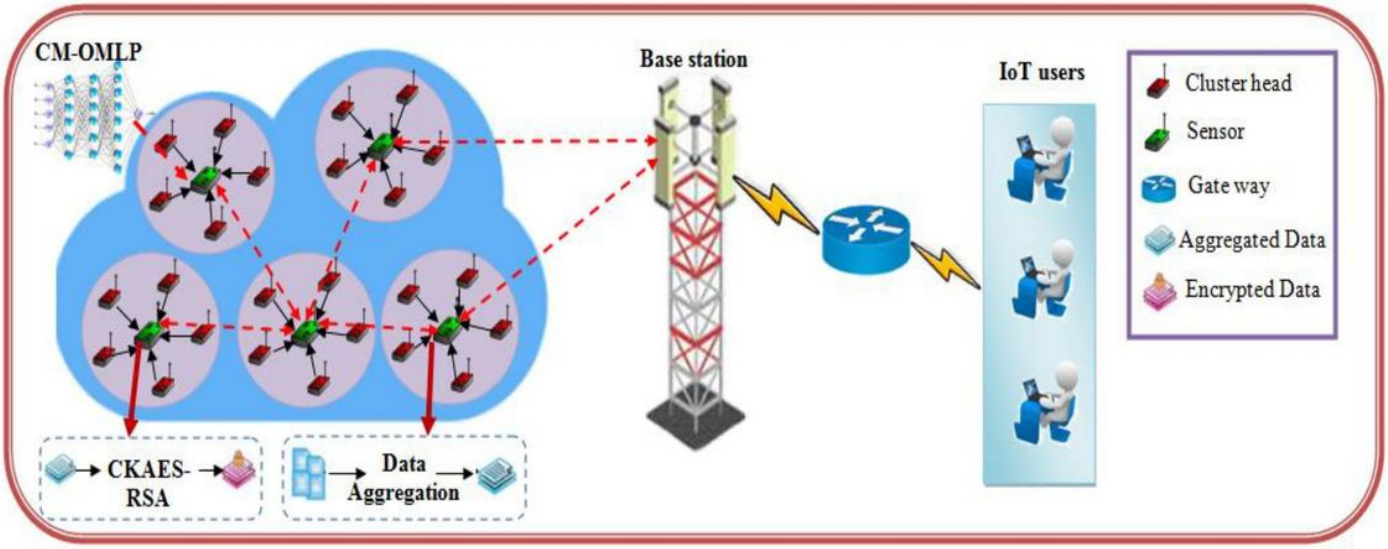


Figure 1

Structural design of the proposed methodology

CO²GA for CH selection

Input: Set of SNs in WSN

Output: Optimally selected CHs for data aggregation

Begin

Initialize the CO²GA parameters U_j, L_j *and* M_{iter}

Initialize the population of SNs in the WSN with chaos variable

Compute the O_F of each individual by considering E_c, D_t, C_f, *and* N_d

Choose the best search agent

While $(i < M_{iter})$

Update S_{ij}

for each S_i in the search space do

Normalize the distance between individuals

Compute Q_i and W_i of the CO2GA

Update S_{ij} after each iteration

Generate S_{ij}^{OL} by sorting the individuals with O_F

Merge the population of S_{ij} with S_{ij}^{OL}

Select the first N individuals with better O_F

end for

$t = t + 1$

Return best search agents

End

Figure 2

Pseudocode of CO2GA

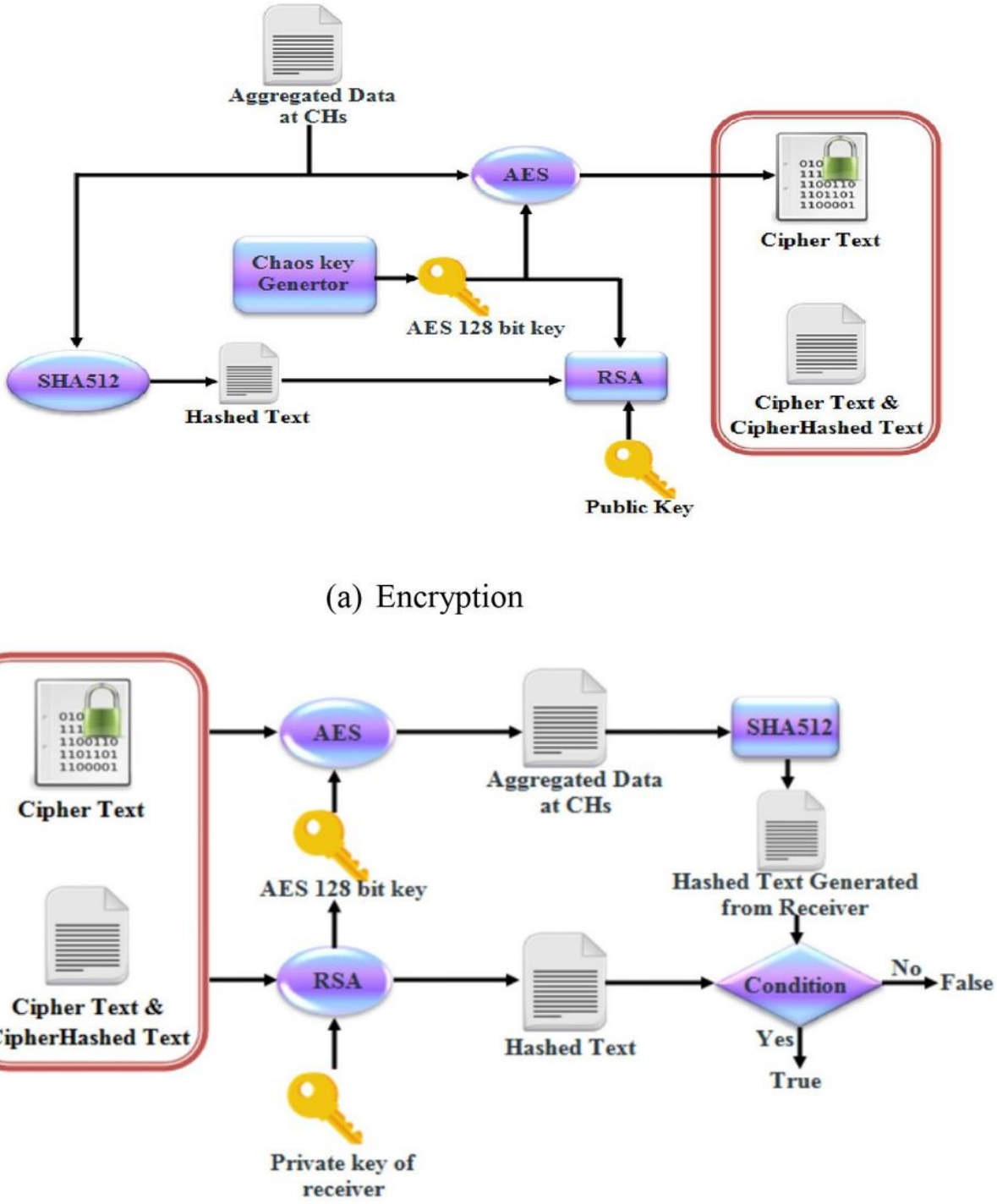


Figure 3

Workflow of proposed CKAES-RSA

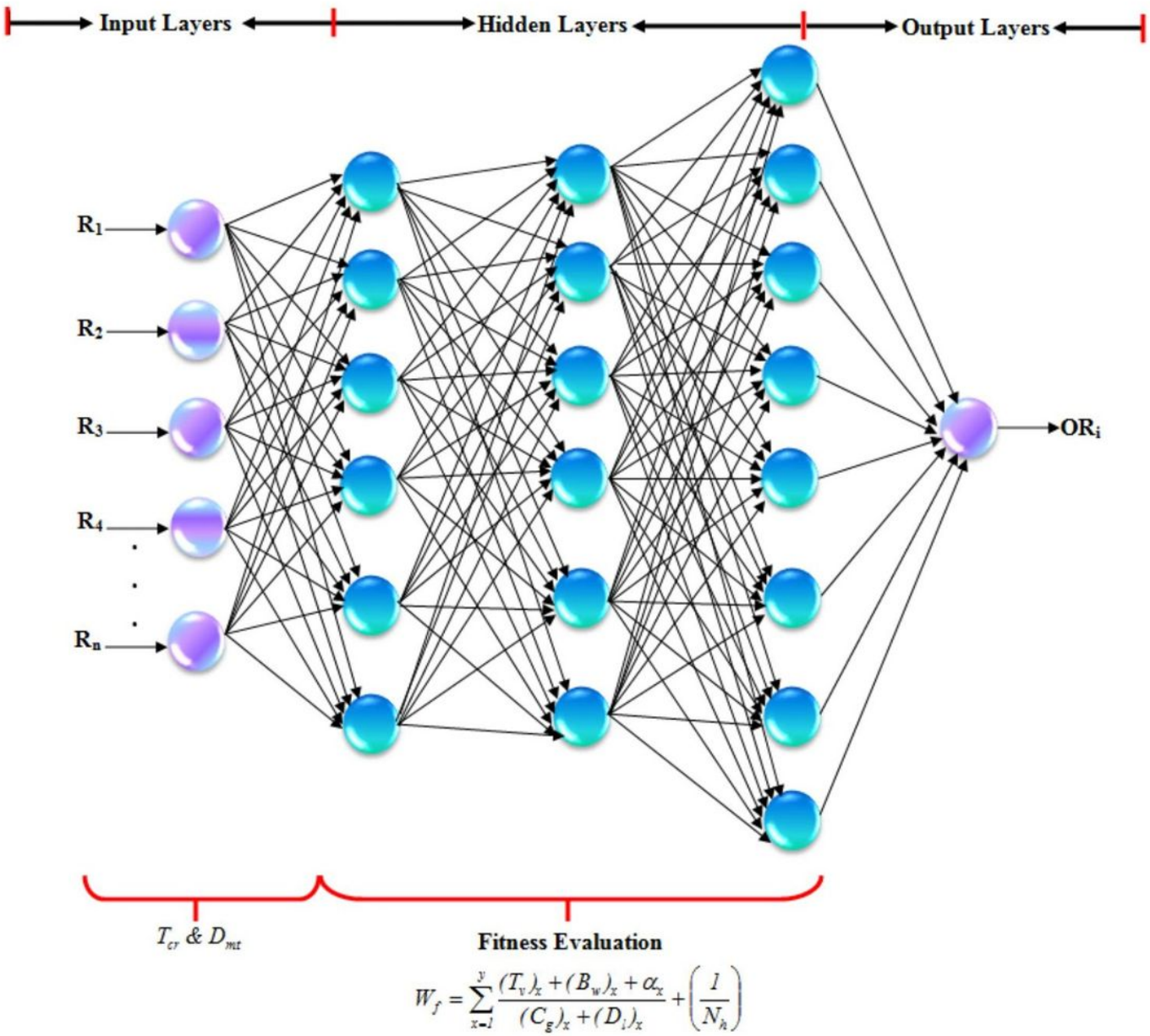


Figure 4

Structure of CM-OMLP

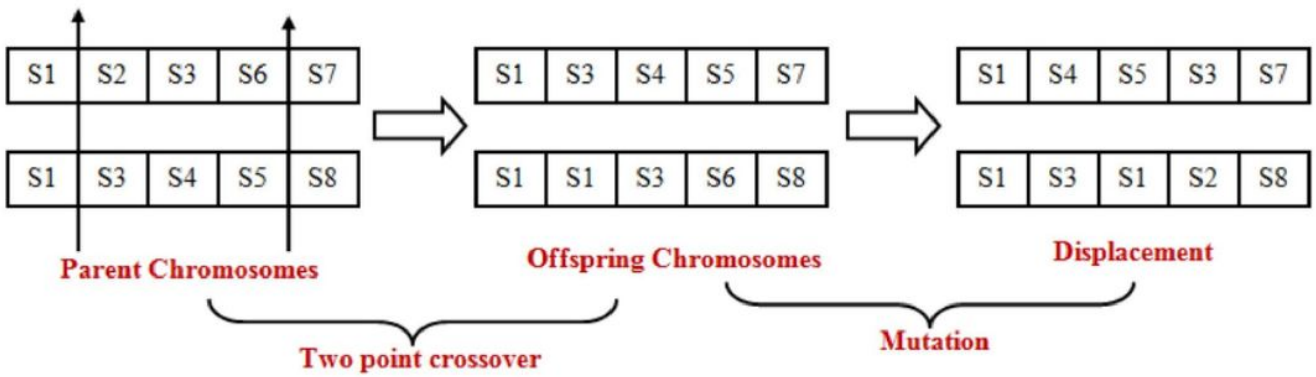


Figure 5

Working of crossover and mutation

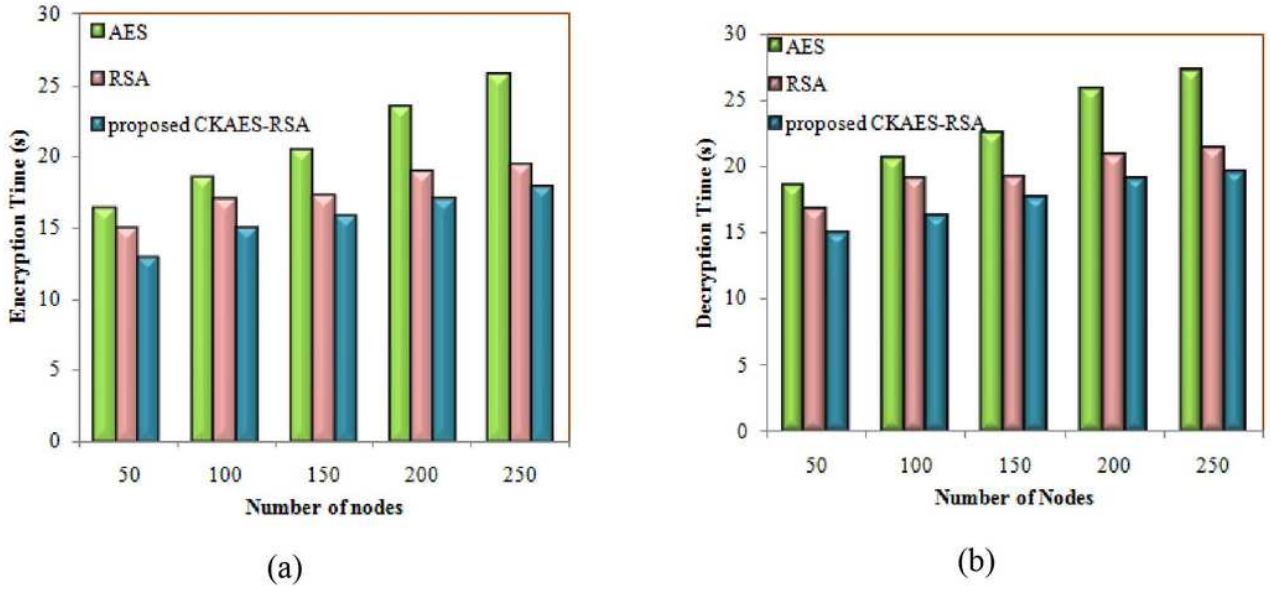


Figure 6

ET and DT of proposed CKAES-RSA with existing methods

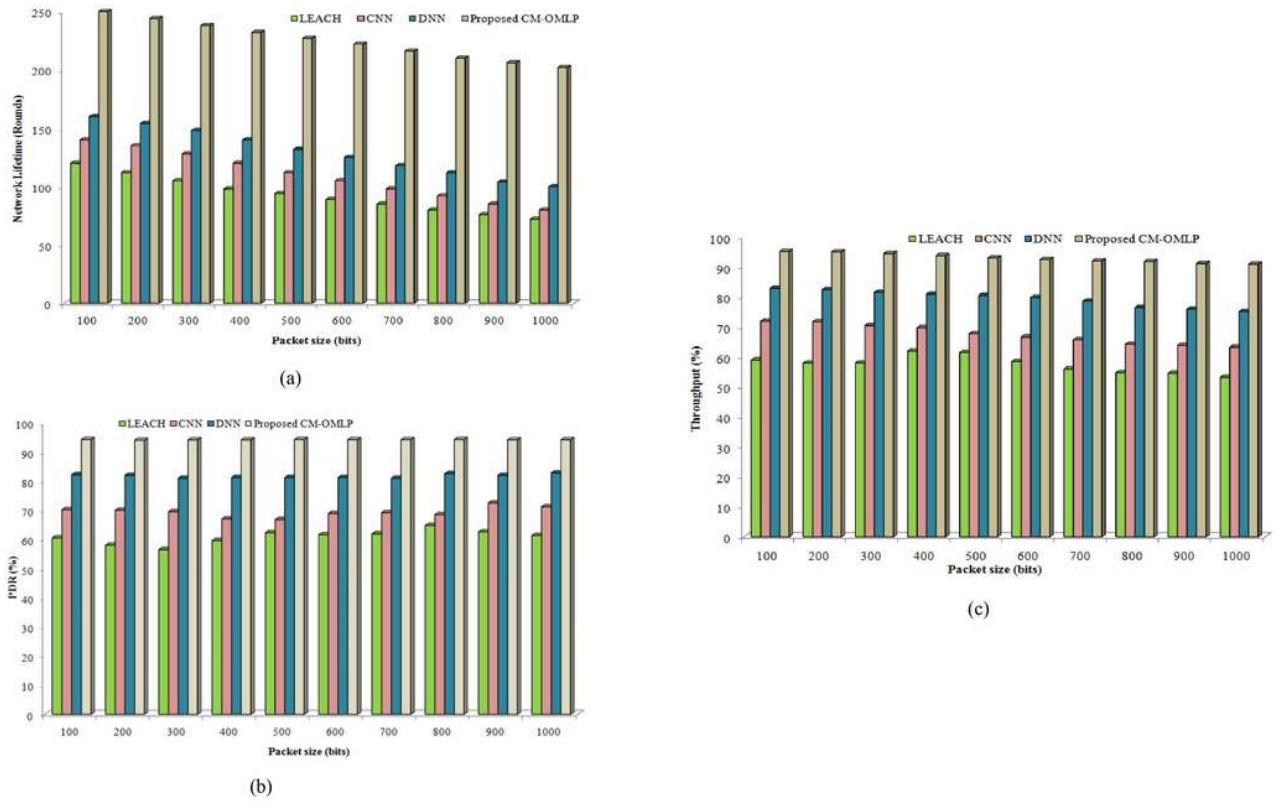


Figure 7

Lifetime, PDR, and throughput of the techniques

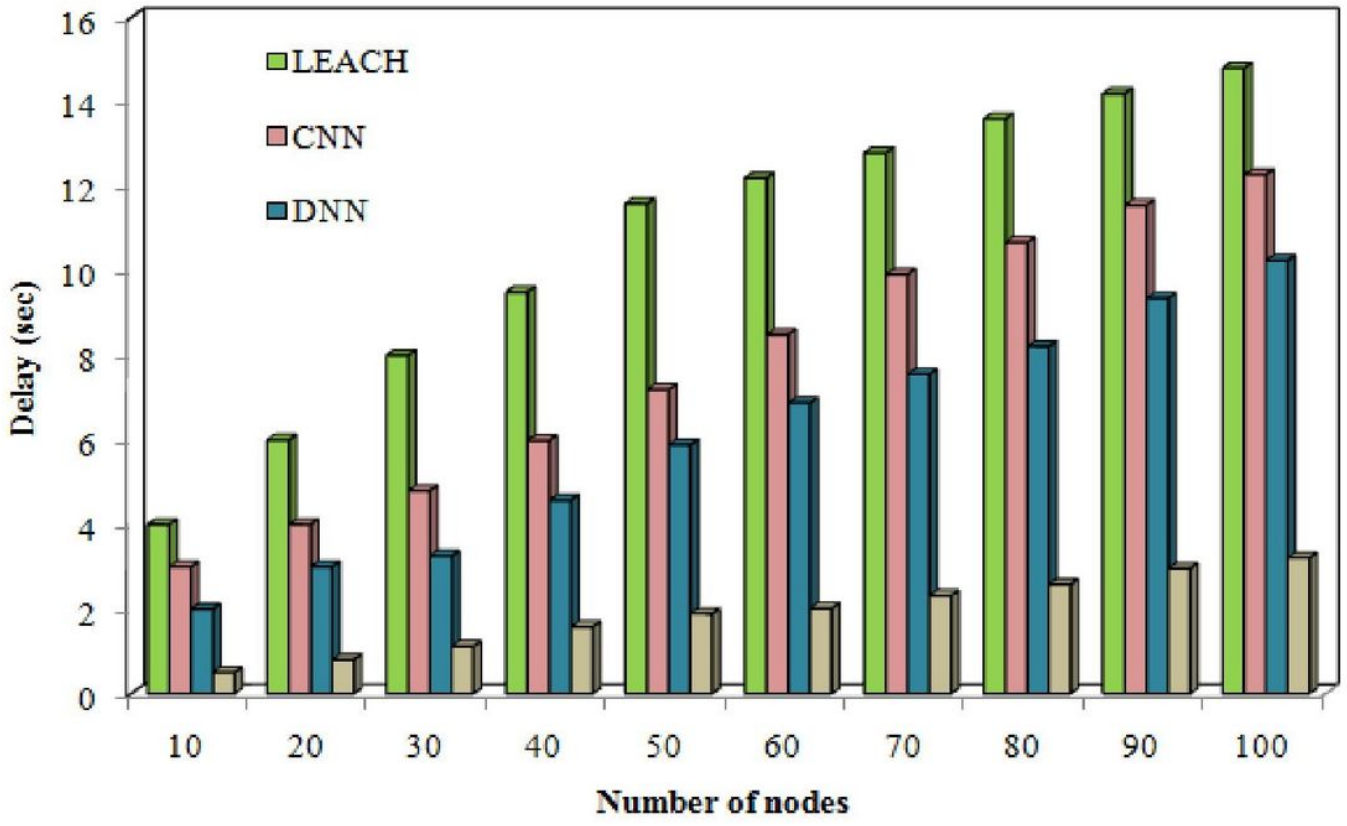


Figure 8

Delay of the techniques