E2DA: Energy Efficient Data Aggregation and End-to-End Security in 3D Reconfigurable WSN

Karthick Ramasamy, Mohammad Hossein Anisi, *Senior Member, IEEE,* Anish Jindal, *Member, IEEE*

Abstract— **This paper deals with energy consumption and security limitations in the reconfigurable WSN's in order to improve the network lifetime with end-to-end data privacy. The network consists set of nodes placed in distributed environment such that each node performs a reconfiguration task to support users requirements. We proposed novel solutions that improved network lifetime through efficient reconfigurable routing and less network traffic. We proposed an in-network task to eliminate duplicate packets at the node level using hashing distance computation (HDC). Further, we introduced power-efficient reconfigurable cell-by-cell golden sector-based emperor penguin colony (CbC GSEPC) for trust-based routing. In terms of data confidentiality in the energy-constrained environment, a lightweight key expandable cryptography method was proposed for end-to-end confidentiality. Additionally, a reading-based dual validation (RbDV) audits the information at sink level for intrusion detection and isolates suspicion nodes. The proposed and existing works simulated with NS-3.26 and the results show that the proposed work's average energy consumption is 5.82% lower than the existing 2D-WSN while offering end-to-end confidentiality and node reconfiguration opportunity.**

Keywords: **3D Grid WSN, Encryption, Data Deduplication, Dual validation, Data Aggregation, End-to-End Security.**

I. INTRODUCTION

WSN has gained massive attention in recent times [1]-[2]. It comprises many sensor nodes dedicated to performing specific tasks such as environmental monitoring, transport and healthcare, etc [3-4]. Due to the wide range of applications, reconfigurable WSN becomes an emerging technology [5-6]. The set of sensor nodes monitors the environment's conditions and forward the data to the base station (BS) wirelessly [7]. Optimal network management and data transmission play an essential role in efficient data aggregation to the remote BS [8][9]. In a sensor node, energy dissipated in three significant ways -- sensing, transmitting and receiving. A cluster formation methodology was introduced to bridge the problem, which supports data aggregation [10]. The clustered network allows in-network data processing, reducing energy consumption and prolonging the network lifetime [11]. Among the several sensor nodes, a specific node is selected as grid head (GH) to act as a relay node to the BS. Importantly, finding an efficient path to the BS is more important and complex as the transmission energy is directly proportional to distance increases. Cluster-based routing protocols were proposed for efficient path management in the WSN environment [12]. Here, the K-means algorithm is imposed for cluster formation and routing. In [13] the author introduced an energy-efficient, compressive sensing-based routing (EECSR) protocol. It has been found that the protocols need more energy to select an optimal path. So, there is a need to efficiently calculate the path to BS. Further, there is a need to securely transfer the data through the path is vital [14]. As the sensor nodes are deployed in an open environment, security is a challenging issue [15]. End-to-end data security can be achieved through cryptography methods [16]. The existing security mechanism such as Okamoto-Uchiyama [17], and elliptic curve cryptography (ECC) [18], required high computational and memory requirements which is not suitable for WSN. Therefore, there is a need for an energy-aware highly secure end-to-end cryptographic method for reconfigurable WSN. The rest of this paper is organised as follows: Section II studies the existing research works. In section III, discussed the problem statement and contribution. In section IV, demonstrates the proposed work. Section V discusses outputs. In section VI, we conclude the contributions with future work.

II. RELATED WORK

Several studies were conducted to improve the GH reconfiguration to prolong the network lifetime. In [19], a distance similarity index with a dual GH was discussed to minimize the computation. Similarly, [20] proposed a fitness-based glowworm swarm with a fruit fly algorithm (FGF) to improve time delay in GH reconfiguration. Further, [21] proposed a load-balanced cluster-based scheme to reconfigure GH dynamically based on the remaining energy level and substitution GH. Also, the study [22] discussed the challenges involved in GH reconfiguration and proposed an improved version of the low energy adaptive clustering hierarchy (LEACH) algorithm based on energy dissipation threshold and nodes geographical position. Later, a game theory-based dual reconfigurable GH algorithm was presented with the Nash Equilibrium Point (NEP) [23]. It has been found that these high computation required algorithms lead to rapid energy dissipation. For example, In [23][24], the use of the dual GH reconfiguration method the computational delay but reduced network lifetime. The author in [25] proposed a redundant node elimination technique using the mesh partitioning technique. This work avoids sending packets from redundant nodes which reduces network traffic greatly. In [26], proposed a local outlier factor (LOF) algorithm which classifies the sensor readings into reliable and unreliable readings. However, this LOF method was not suitable for the large-scale network as it increases the

K. Ramasamy, M. H. Anisi and A. Jindal are with School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, United Kingdom.
e-mails: kr18215@essex.ac.uk, m.anisi@essex.ac.uk, a.jindal@essex.ac.uk

time consumption at every cluster. Further, An intelligent detection algorithm proposed suspicious node elimination as part of data aggregation in WSN [27]. The suspicious node was detected by fusing all aggregated data from various sources and determining the suspicious nodes during routing. The conventional key-based cryptographic system often required high computation which leads to in-efficient WSN [28]. Due to the energy and computation constrained nature of WSN, lightweight cryptographic schemes need to be implemented [29]. The paper [30] proposed a secure lightweight hash-based node verification protocol. Later, it has been found that the algorithm is vulnerable to DDOS attacks. [31] randomly assigned a unique identification to the sensor nodes to verify the identity. Then each sensor node is checked against the verification table to match its identity. Eventhough, there is a possibility that the node can be compromised as it maintains the same verification code over a period. Further to node verification, [32] [33] proposed symmetric key-based cryptographic function for privacy protection. In symmetric cryptography, the secret key must be shared with the participating sensor nodes. In addition, [33][34] proposed to encrypt selective bits from the data stream using public-key. A compressed sensing-based encryption technique is used to secure data packets with the public key. A number of energy-efficient reconfigurable routing approach has also studied for WSN. An auxiliary potential field-based technique was used with the node's queue length and energy potentials proposed in [35]. The research in [36] proposed a route assist enquiry method to find the efficient path by considering neighbouring node's parameters such as a number of successful transmissions and delay factors. A neuro-fuzzy algorithm was presented to enable cluster-routing in the WSN environment [37]. The neuro-fuzzy algorithm trained with a convolutional neural network (CNN) decides on cluster formation for optimal routing. However, clustering decision by CNN performed by each node drastically increases energy consumption.

III. Problem Definition And Contributions

In this section, we summarise the major research problems in reconfigurable WSN, define the problem statement for this work, and describe our contribution to overcome them.

A. Problem Statement

The reconfigurable WSN requires three-dimensional analyses rather than a two-dimensional approach to improve energy efficiency and security analysis significantly. Simultaneously, real-time applications such as the Ocean monitoring system requires a three-dimensional method for more efficiency. Performing data aggregation without privacy protections increases data vulnerability and leads to huge data loss are the drawbacks that need to be considered. Moreover, implementing a hop-by-hop encryption scheme (encryption and decryption performed in every hop) or end-to-end encryption (homomorphic operations performed) method increases vulnerability. In contrast, later increases energy consumption and computational overhead as the encrypted data needs to decrypt at every hop for similarity check and data fusion. Hence, there must be an end-to-end encrypted and redundant data elimination process over the encrypted (no needs to decrypt for redundant elimination) packets that need to be proposed to maintain end-to-end security. On the other hand, the WSN security-oriented literature such as fuzzy-based biometric schema [32], Okamoto-Uchiyama [25], and elliptic curve cryptography (ECC) [26] required high computational power were not suitable for energy-constrained WSN. Hence, a lightweight and secure encryption method must be identified to best suit the resource-constrained WSN. Besides, the previous studies were concentrated on the authenticity of a node using the constant identification key. Using the same key for each round can cause a potential security risk, which needs to be random at each round.

B. Major Contributions

We have introduced various novel contributions to overcome the issues discussed in the above section. A novel MM-Fuse method was presented for optimal GH selection using the concentric spheres (Co-Spheres). A Random ID XOR-ed Authentication (RID-XOR) scheme was proposed with a two-factor authentication facility for node verification. A lightweight cryptography scheme called Cubic Chaotic-based Extended Tiny Encryption Algorithms (C2XTEA) has been proposed for end-to-end security. A secure deduplication method called hash distance computation (HDC), and a lightweight Photon algorithm is proposed for removing duplicate packet. Further, we proposed (C1-to-1M) algorithm and a novel cell-by-cell golden sector-based emperor penguin colony (CbC-GSEPC) optimisation algorithm for optimal and trust-based route selection. Emperor Penguin Colony (EPC) is a widely used optimal path selection protocol and it works based on huddling nature of emperor penguins [38]. A temperature profile and distance between emperor penguins is obtained from a randomly formed huddle to select an optimal path for the next move [39]. In our proposed CbC-GSEPC, a golden sector algorithm calculates two intermediate points from the multiple optimal routes to choose the suitable path. Finally, we also detect any intrusion using a reading-based dual validation (RbDV) technique and a sliding window-based neural neutrosophic (SW-NN) algorithm

IV. Proposed E2DA-based 3D-Grid WSN

This section describes the proposed energy-efficient data aggregation and end-to-end security (E2DA) for the 3D reconfigurable WSN in detail.

A. 3D-Grid Network Model and Assumptions

We consider a $m \times m \times m$ 3D-grid model from Hosen [40] in which the grid is divided into an equal number of grid cells where m is the size of the predefined cube (All sides are equal). For example, if $m = 3$, then the grid is split into 27 compartments. The formation of 3D-Grid cells improves network connectivity and provide node reconfiguration for specific grid area through dynamic program. Further, each grid area can dynamically modify its connection to the sink node to support network reconfiguration. In each cell, A Co-Sphere is formed to support efficient data aggregation to prolong the network lifetime. As shown in Fig 1, The Co-Sphere has three levels: level 1 (L_1), level (L_2) and level 3 (L_3). The L_1 the sphere is formed with the radius of r_1. where the radius r_1 derived from the size of the grid cell. Let us consider the grid cell with the side of $S(Grid\_$ (in cube height, width and height are the same).

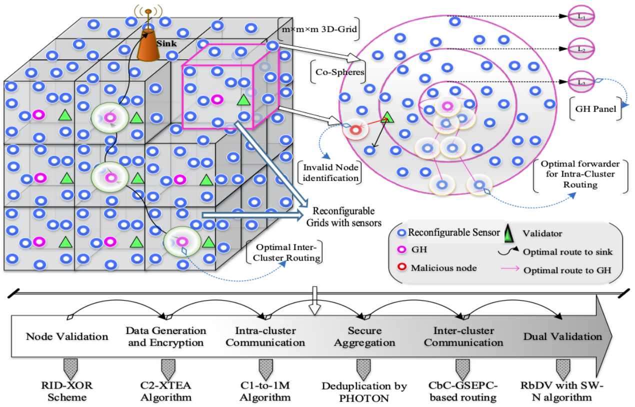

Fig. 1. 3D-Reconfigurable Grid Cell Model for WSN

Simiular the 3D network model from Hosen [44], the side of grid cells can be computed using Equation 1.

$$S(Cell) = \frac{S(Grid)}{m} \tag{1}$$

Then, the radius of L_1 sphere computed with Equation 2,

$$r_1 = \frac{S(Cell)}{2} \tag{2}$$

Similarly, the radius of L_2 and L_3 is represented by r_2 and r_3 respectively. Equation 3 and 4 gives the procedure for r_2, r_3 computation from r_1,

$$r_2 = \frac{r_1}{2} \tag{3}$$

$$r_3 = \frac{r_2}{2} = \frac{r_1}{4} \tag{4}$$

With the radius of r_1, r_2, r_3, the Co-Spheres are formed within each cell. After the construction of 3D-grid cells and Co-Spheres, the sensor nodes are deployed in the network uniformly. The overall network has n number of sensor nodes denoted as $N_1, N_2, N_3, .., N_n$ and a single sink node. The overall network model is shown in figure.1. In the network, the following assumptions made, Always $r_1 > r_2 > r_3$. The sensor nodes are static, and the sink node also fixed. All sensor nodes have an equal energy level initially. Each cell has a legitimacy validator node to perform the node validation process. The network has both valid and malicious nodes. The number of malicious nodes is always smaller than legitimate nodes. The validator and sink nodes are trustworthy, while the nodes can change their trust states.

i. *Energy Model*

In this work, we use a first-order radio model and the energy requirement computed by Equation 5. In Equation 5, E_{elec} represents energy dissipated by the transmitter (Tx) or receiver (Rx) per bit, and ρ represents the number of bits transmitted between Tx and Rx.,

$$E_{Tx/Rx} = E_{elec} \times \rho \tag{5}$$

Further, the transmission circuit consumes energy for the amplification model derived from Equation 6,

$$E_{Tx-Amp} = \begin{cases} \varepsilon_F \times \rho \times d^2, & if\ d < d_0 \\ \varepsilon_{mp} \times \rho \times d^4, & if\ d > d_0 \end{cases} \tag{6}$$

Here d_0 is the threshold used to determine a fading model, and it is given in Equation 7. Here ε_F and ε_{mp} denotes the free-space and multipath constants. Therefore, the total energy required by the transmitter is computed by Equation 8,

$$d_0 = \sqrt{\frac{\varepsilon_F}{\varepsilon_{mp}}} \tag{7}$$

$$E_{Tx} = \begin{cases} E_{elec} \times \rho \times \varepsilon_F \times \rho \times d^2, & if\ d < d_0 \\ E_{elec} \times \rho \times \varepsilon_{mp} \times \rho \times d^4, & if\ d > d_0 \end{cases} \tag{8}$$

Similarly, the energy required for the reception is computed as follows: $E_{Rx} = E_{elec} \times \rho$

B. *GH Selection and Node Validation*

i. *MM-Fuse Method*

We introduce a novel MM-Fuse method for optimal grid GH selection. GH helps for data aggregation from the corresponding cell. Thus, an optimal node must be selected as GH for improving overall performance. We introduced a novel MM-Fuse method that constructs an influential metric (φm) by fusing primary GH selection metrics. At first, the centroid value (C) is computed for each cell as per Equation 9, The x_i, y_i, z_i in Equation 9 denotes the (x,y,z) coordinates i^{th} the vertex of the cell, as shown in Fig 2. Then the following multiple metrics are considered for the optimal GH selection.

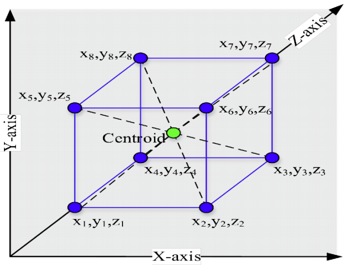

Fig. 2. Centroid Computation

Definition 1 (Centroid Distance)- For each node N_i, distance with the centroid $(d(N_i, C))$ is computed. Here distance computation considers three coordinates and uses 3D-Euclidean measure as Equation 10.

$$\mathbb{C}(x_{\mathbb{C}}, y_{\mathbb{C}}, z_{\mathbb{C}}) = \left(\frac{\sum_{i=1}^{8} x_i}{8}, \frac{\sum_{i=1}^{8} y_i}{8}, \frac{\sum_{i=1}^{8} z_i}{8}\right) \tag{9}$$

$$d(N_i, \mathbb{C}) = \sqrt{(x_{\mathbb{C}} - x_i)^2 + (y_{\mathbb{C}} - y_i)^2 + (z_{\mathbb{C}} - z_i)^2} \tag{10}$$

If N_i has a lower distance with centroid, then it has more possibility to become GH.

Definition 2 (Average Distance)- This metric computes the average distance for all nodes. The average distance (d_{Avg}) computed for a node N_i by computing 3D-Euclidean measure with all other nodes in the specific grid cell. If a cell has a number of nodes. Then, the d_{Avg} for N_i is computed using Equation 11. A node that has a minimum d_{Avg} increases the aggregation cost. Thus, if N_i has a lower d_{Avg}, then it has a high possibility to become a GH.

$$d_{Avg} = \frac{\sum_{\substack{j=1 \\ j \neq i}}^{a} d(N_i, N_j)}{a-1} \tag{11}$$

Definition 3 (Energy Level)- This metric measures the residual energy level for N_i. Initially, this metric is equal for all nodes. However, the residual energy level of N_i varies for each node over time. The energy level (ω) for N_i is computed as per Equation 12. The ω of N_i is computed as the function of the initial energy level (IE) and energy consumed over time (t) (EC_t).

$$\omega(N_i) = IE - EC_t \tag{12}$$

Definition 4 (Node Degree)- This metric evaluates the connectivity degree of N_i with other nodes in the cell. The node degree ($D(N_i)$) is defined as the total number of nodes that connected with N_i.Finally, all four metrics are fused according to Equation (13). To make GH selection simple and to minimise the overhead, we MM-Fuse from $L_3$to $L_1$for GH selection. In Equation 13 α, β are the weighting parameters and selected as $\alpha + \beta = 1$. A node with high φm is selected as GH if the ω of current GH becomes lower than a predefined threshold (computed as $IE/2$), then it triggers the GH rotation process again.

$$\phi m(N_i) = \frac{\alpha(\omega + D(N_i))}{\beta(d(N_i,\mathbb{C}) + d_{Avg})} \tag{13}$$

ii. *Node Authentication*

It is essential to identify and verify the node authenticity in the network to prevent security vulnerabilities.

Algorithm 1: 3D-Grid Construction and Node validation

```
Begin
   Construct $m \times m \times m$ cells
   In each cell
   Form Co-Spheres→ $L_1, L_2, L_3$
   Assign$L_3 \rightarrow GH\ Panel$
   //Start MM-Fuse
   For each cell∈Grid
      Compute $\mathbb{C}(x_{\mathbb{C}}, y_{\mathbb{C}}, z_{\mathbb{C}})$
      For each $N_i \in Cell$
         Find $d(N_i, \mathbb{C}), d_{Avg}, \omega_i, D(N_i)$
         Fuse to find $\phi m(N_i)$
         If $\phi m(N_i) = High$, Then do
            Assign $N_i \leftarrow GH$
         Else
            Move to $N_{i+1}$
         End If
      End For
   End For Return (GH)
  //Start RID-XOR
   For all $N_i \in Cell_j$
      Register $\{ID_i, PW_i\}$
      Generate $\{\Re.ID_i, \varphi_i\}$
      If (Auth_Req) initiated, Then do
         Generate $\wp.ID_i$&&Auth_Cre
         Create Auth_Req←{$\wp.ID_i$ ⊕Auth_Cre}
         Submit $N_i$ → {Auth_Req} →Validator
         If (Auth_Req==Valid), Then do
            Send $\delta \rightarrow N_i$
         Else
            Drop Auth_Req
         End If
      Else
         Do
      End If
   End For
End
```

We proposed a random identification-XOR (*RID-XOR*) technique for node authentication. This algorithm runs on a dedicated network node called legitimacy validator using a simple XOR operation and *RID* number. The following sequential steps are involved in the proposed RID-XOR scheme:

Step 1 (Registration) - In this step, each node N_i register its ID, password PW to the legitimacy validator. The validator then generates a unique 8-bit integer and distributes a $R.ID$ for the node.

Step 2 (Authentication Request) - This sequence is triggered when a node wants to transmit a piece of information to GH. In this step, the node N_i sends authentication request (Auth_Req) to the validator. The Auth_Req contains Pseudonym ID ($\wp.ID$) and the authentication credentials (Auth_Cre). The random $\wp.ID$ is derived from the $R.ID$ and time stamp (TS) by the node itself at each round. Consider a $R.ID$ with the following bits $b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7$. At first, $\wp.ID$ is generated using Equation 14. The bits in $R.ID$ are shuffled to generate $\wp.ID$ based on the predefined pattern known only by the validator to ensure privacy. Similarly, the Auth_Cre is derived from the credentials like Grid ID ($G.ID$), Level ID ($L.ID$) and Version ID ($V.ID$).

*Definition 5 (**$V.ID$**)*- The $\boldsymbol{V.ID}$ defines the version of the corresponding cell based on the number of GH rotations. At the initial stage, $\boldsymbol{V.ID = 1}$. The Auth_Cre computed as $\{\boldsymbol{L.ID \oplus G.ID \oplus V.ID}\}$. Then, the Auth_Req is designed by using Equation 15. Algorithm 1 describes the sequence for network construction and node authentication.

Step 3 (Node Validation) - Upon receiving Auth_Req, the verification process is performed by performing XOR operations $\wp$. ID and Auth_Cre. The validator extracts the R.ID from the $\wp$. ID since it has a predefined pattern. If the ID and Auth_Cre are matched, then the node is valid, and the validator provides a shared secret (δ) which is valid for a short time. Also, the Legitimacy_Table is updated with the information of currently authenticated nodes.

$$\wp.ID(1) = (b_0 \oplus b_1 \oplus b_2 \oplus b_3 \| b_4 \oplus b_5 \oplus b_6 \oplus b_7) \oplus TS \tag{14}$$

$$\text{Auth\_Req} \rightarrow \{\wp.\text{ID} \oplus \text{Auth\_Cre}\} \tag{15}$$

C. *Energy-Efficient Secure Data Aggregation and Routing*

This section will securely aggregate the data without duplication and find a reliable and efficient forwarder in each grid to reach the sink node. We follow the following sequences: data encryption, intra-cluster transmission, secure deduplication, inter-cluster transmission, validation and verification.

i. *Data Generation and Encryption*

Here, node N_i senses the data μ, and securely transmits the data to GH. For all authenticated nodes, the validator node generates a 128-bits Master key (φ) using the Cubic Chaotic function. This Master key (φ) is used for encryption and decryption in the Cubic Chaotic-based Extended Tiny Encryption Algorithm (C2XTEA) algorithm. The XTEA is a lightweight and secure cryptosystem that uses a Feistel structure. To strengthen the XTEA algorithm, we integrate the Cubic Chaotic algorithm with the XTEA algorithm. The Cubic Chaotic is the strong cryptosystem that operated upon the Chaos theory. In the C2XTEA algorithm, the chaos theory is used as the key expansion function. Typically, the one-dimensional cubic map is defined in Equation 16. Where, u, v are the cubic parameters that are always greater than zero. From this function, the chaotic map sequence is generated using Equation 17. Here, the Y_k is derived from the sequence of X_k. And c

denotes the interval of Y_k (i.e.) if $X_k \in [-1,1]$, then Y_k will be in $[0,2c]$ and it computed as $c = 2^{S-1}$ (here S defines computer word size). From the cubic chaotic function, the composite sequence is generated. From the mixed cubic chaotic sequence, four random 32-bits were selected to create a 128-bis master key (i.e.) $\varphi = [\Phi_1, \Phi_2, \Phi_3, \Phi_4]$. Here Φ represents a 32-bit random number. This master key took for XTEA-based encryption.

Algorithm 2: Data encryption and decryption by C2XTEA

```
Begin
  // Key Generation
  $\varphi = [\varphi_1, \varphi_2, \varphi_3, .., \varphi_{16}]$
  For $j \leftarrow 1$ $to$ 16 do
      If $j\%2 == 0$
          $\varphi_j = Cubic(\varphi_j)$
      Else
          $\varphi_j = \varphi_j \oplus \varphi_{j+1}$
          $\varphi_j = Cubic(\varphi_j)$
          $\varphi_{j+1}\varphi_j = P(\varphi_{j+1}, \varphi_j)$
      End if
      $\varphi \lll 5bits$
      $\varphi_{r1} = \varphi_1 \oplus \varphi_9$
      $\varphi_{r2} = \varphi_5 \oplus \varphi_{13}$
      Return $\varphi_{r1}, \varphi_{r2}$
  End For
  //Encryption
  Initialize ($Z$,$\mu_1, \mu_2$, $\varphi$)
  Assign← [$\mu_1 = \mu[1], \mu_2 = \mu[2], sum = 0, delta = 0x9E3779B9$
  For ($i = 0; i < Z; i++$) do
      $\mu[1] += (((\mu[2] \ll 4)\hat{}(\mu[2] \gg 5)) + \mu[2])\hat{}\ (sum + \varphi[sum\&3])$
      Sum+=delta
      $\mu[2] += (((\mu[1] \ll 4)\hat{}(\mu[1] \gg 5)) + \mu[1])\hat{}(sum + \varphi[sum \gg$
        $11]\&3)$
      $\mu[1] = En(\mu_1);\ \mu[2] = En(\mu_2)$
      Return ($\mu[1], En(\mu_2)$ )
  End for
  Return ($En(\mu)$)
  //Decryption
  Initialize ($En(\mu), Z, \varphi$)
  Assign← [$\mu_1 = \mu[1], \mu_2 = \mu[2], sum = delta * Z, delta = 0x9E3779B9$
  For ($i = 0; i < Z; i++$) do
      $\mu[2] -= (((\mu[1] \ll 4)\hat{}(\mu[1] \gg 5)) + \mu[1])\hat{}(sum + \varphi[sum \gg$
        $11]\&3)$
      Sum−=delta
      $\mu[1] -= (((\mu[2] \ll 4)\hat{}(\mu[2] \gg 5)) + \mu[2])\hat{}\ (sum + \varphi[sum\&3])$
      $\mu[1] = \mu_1;\ \mu[2] = \mu_2$
      Return ($\mu$)
  End for
End
```

In C2XTEA, the input data block is divided into two halves as μ_1 and μ_2. Then, both inputs are applied to the Feistel network for Z rounds (typically $Z = 32$).

$$X_{k+1} = uX_k{}^3 - vX_k \tag{16}$$

$$Y_{k+1} = \begin{cases} \frac{4}{c^2}Y_k^3 - \frac{12}{c}Y_k^2 + 9Y_k + 1, & Y_k = 0\ or\ \frac{3}{2}c \\ \frac{4}{c^2}Y_k^3 - \frac{12}{c}Y_k^2 + 9Y_k - 1, & Y_k = c \\ \frac{4}{c^2}Y_k^3 - \frac{12}{c}Y_k^2 + 9Y_k, & Y_k \in (0,c) \cup (c, \frac{3}{2}c) \cup (\frac{3}{2}c, 2c-1) \end{cases} \tag{17}$$

For encryption, C2XTEA uses integer addition, and for decryption, it uses integer subtraction and XOR-operations. In each round, the round key is generated as per Equations 18 and 19. Here r represents the round and $\varphi_1, \varphi_9, \varphi_5, \varphi_{13}$ denotes the components from the master key. In this manner, the round key is generated in each round and the data is encrypted to generated ciphertext ($En(\mu)$). The proposed C2XTEA algorithm involves simple operations, and the use of chaotic theory assures high-level security. The pseudocode in Algorithm 2 depicts the process of data encryption and decryption in the C2XTEA cryptosystem. Here we use chaotic-based round key generation, which makes it secure and lightweight. Before encryption, the source node generates a hash value for corresponding μ ($H(\mu)$) by using the PHOTON algorithm (as explained later). Finally, the source node generates secure data as $\{En(\mu), H(\mu)\}$.

$$\varphi_{r1} = \varphi_1 \oplus \varphi_9 \tag{18}$$

$$\varphi_{r2} = \varphi_5 \oplus \varphi_{13} \tag{19}$$

ii. Intra-Cluster Communication

As we have constructed Co-Spheres to support effective data aggregation, the data from L_1 Co-Spheres can transmit to GH within two hops. In every hop, optimal forwarders nodes are selected to ensure reliable and secure data delivery. We introduce C1-to-1M algorithm, which selects optimal forwarders node cooperatively. In this proposed algorithm, the players are the source nodes that have data to transmit with GH If a source node belongs to $Level\ L_1$, then the target nodes are presented at $Level\ L_2$. In the cooperative game, multiple source nodes presented within the same level are combined and decide on target nodes. The game consists of,

Definition 6 (Cooperative Players)- The source nodes in the same level are represented as players (i.e.) if the source nodes as $N_1, N_2, .., N_l \in L_1$, then all nodes are considered as players.

Definition 7 (Actions)- The actions made by the players are known as actions. The steps include Transmit_, Drop_ or Move_. Here Transmit_ action is taken when a source node determines a stable match. Drop_ act taken when a stable partner is not determined by the source node (this case occurs occasionally). Similarly, Move_ action is made when the two source nodes select a node as a forwarder.

Definition 8 (Preferences)- Each source has strict preferences over forwarders and vice versa. When two or more source nodes are willing for data transmission, they form a coalitional group (G). In such a group, each player knows the other's decision. Similarly, the nodes in the next level are considered as targets (T). The preference level for a node $N_i \in G$ on a target $N_T \in T$ is measured based on the Preference Factor (Pre_{Fac}).using, Equation 20. Where γ is the trust value of the target node. The trust value is computed in terms of the number of data packets forwarded by the node successfully.

$$Pre_{Fac} = \frac{(\gamma/\max\gamma)\times(\omega/\max\omega)}{\Delta(\delta\times d)} \tag{20}$$

This metric's significance is that the malicious node will have a lower trust value as it involves a packet drop. Thus, the trust value will find the legitimacy of the node. Moreover, δ measures the expected delay for data transmission. Here Δ is the normalising factor and chosen from the [0,1] interval. If a target node has higher Pre_{Fac} values, then it has more possibility to become the optimal forwarder. Once the player node is selected, it informs the selections message to all other players. In this case, the other players eliminate that specific node from their target list. If any two players select the same target as an optimal forwarder, then a lower energy level wins and gets a transmission chance. The other player will continue the match to elect an optimal target. In this C1-to-M1 algorithm, each player finds an optimum target with cooperation, minimising energy consumption. In the pseudocode for algorithm 3, the process of the proposed C1-to-1M algorithm is illustrated. The process initiated with player, target and preference computations. At last, the data is transmitted to the GH through 2-hops optimal forwarders. Example 1- Consider a $G = \{N_1, N_2, N_3, N_4\} \in L_1$ and $T = \{N_5, N_6, N_7, N_8, N_9, N_{10}\} \in L_2$. At first, the game started with preference computation. Each player in G computes Pre_{Fac} for the targets in T. Here the possible node pairs are $\{\sum_{i=1}^{4} \sum_{j=5}^{10} (N_i, N_j)\}$. As the distance and delay metrics will vary for each node, the Pre_{Fac} is not the same for all nodes. For instance, N_1 will have higher Pre_{Fac} on N_5 if both are close together. But it is not sure that N_2 will also have higher Pre_{Fac} on N_5. That means, N_5 is more for N_1 to have the same preference level for N_2. Thus, the possibility to select the same node as a forwarder by two players is low. In case this situation occurs, then it will be resolved by selection message transmission. Similarly, the game played between the nodes in L_2 and L_3. In this case, L_2 nodes are players and the L_3 nodes are targets.

Algorithm 3: Intra-cluster communication by C1-to-1M

```
Begin
    For all $N_i \in L_3$
        Initialize Players, Actions, Preferences
        Form $\mathcal{G}$ and $\mathcal{T}$
        For each $N_i$ do
            For each $N_T \in \mathcal{T}$
            Compute $Pre_{Fac}$
            Sort Targets
            Find best $N_T$
        End For
        Send $SelectMessage \rightarrow all\ N_j \in L_3, \quad (i \neq j)$
        If (No Collision), do
            Take action (Transmit_)
        Else
            Take action (Move_)
            Elect other $N_T$
        End If
        Send $En(\mu), H(\mu) \rightarrow N_T$
    End For
End
```

iii. Secure Deduplication

Secure deduplication helps to reduce energy consumption by reducing the number of data transmissions and bandwidth consumption. As stated earlier, each node transmits the data in the form of $\{En(\mu), H(\mu)\}$. The hash generation is performed by the PHOTON hashing algorithm, which is lightweight and suitable for the resource-constrained environment. The photon hash function has the output hash size of o, which relies on $64 < o < 256$. Its input and output bitrates are denoted as br and br' respectively. Thus, the photon hash function can be denoted as PHOTON-$o/br/br'$. At first, the data μ is appended by appending '1' bit and as many zeros until it has the total length as the multiple of br'. Then the data is divided as Equation 21. Each block has br bits. Then, the k-bit internal state-initiated as Equation 22. Then, the sponge construction performed as per the traditional strategy. At iteration i, the data block μ_i on the leftmost part of the initial state IS_i^7 is absorbed and then the permutation PI_i is applied. It can represent as per Equation 23. Where C represents the capacity of the S-box for the permutation. When all data blocks are absorbed, the hash value is built by concatenating the successive br'-bit output blocks τ_i until the appropriate output size is reached. Algorithm 4 illustrates secure deduplication. The hash value is computed by Equation 24.

$$\mu \rightarrow \mu_0, \mu_1, \mu_2, .., \mu_{l-1} \tag{21}$$

$$IS = \{0\}^{k-24} \| o/4 \, \| br \| br' \tag{22}$$

$$IS_{i+1} = IP_k(IS_i \oplus (\mu_i \| \{0\}^C)) \tag{23}$$

$$Hash = \tau_0 \| \tau_0 \| \dots \dots \| \tau_{l'-1} \tag{24}$$

Algorithm 4: PHOTON for secure deduplication

```
Begin
   //Hash generation (Photon)
   Initialize $o, br, br'$
      Divide $\mu \rightarrow \mu_0, \mu_1, .., \mu_{l-1}$
      For each block
         Estimate $k$-bit $IS$
         Construct Sponge
         Find $l'$
      End For
   End
   //Deduplication (HDC)
   Initialize hash values $\{H(\mu_1), H(\mu_2), .., H(\mu_a)\}$
   For each $H(\mu_i)$
      Compute $HDC(\mu_i . \mu_j)$
      If $HDC = 0$, Then do
         Drop $\mu_i$
      Else
         Move to $\mu_j$
      End If
   End For
End
```

Where l' denotes the number of squeezing iterations (i.e.) $l' = [0/br'] - 1$. In this manner, the hash value is computed by the source node. This hash value is appended with the data and transmitted to GH. Upon receiving data with the hash value, the GH performs a secure deduplication process.

Deduplication is a concept of eliminating duplicate or redundant data in the storage system. Here we apply the same concept to eliminating the redundant data. The basic idea is to find Hashing Distance Computation (HDC) between two hash values rather than computing the similarity between two data. Decrypting the data for the similarity check increases the vulnerability. Here we use the lightweight hash function, which has a lower overhead and preserves the security level. Let GH_i receives data from a number of GMs as $\{\mu_1, \mu_2, \dots, \mu_a\}$. Then, it finds HDC between each data against other data as per Equation 25. If $HDC = 0$, then both data is similar (i.e.) redundancy occurs. In this case, the GH drops one information and adds the source ID into other data. Otherwise, both data is different. In the following example case, the data value is considered as 5 and 6. It shows that the HDC between 5 and 6 varies, which means there is no redundancy. By executing, HDC, the redundant data is detected and eliminated securely.

iv. Inter-Cluster Routing

The aggregated data is transmitted to the sink from GH through an optimal and secure route. For this purpose, Cell-by-Cell Golden Sector-based Emperor Penguin Colony CBC-

GSEPC algorithm was proposed. In the CBC-GSEPC algorithm, the optimal route is identified based on three criteria as energy requirement (E), delay requirement (D) and security requirement (S). For a GH, all nearby cells will have the route to the sink node. Considering all available routes will increase the time consumption for route selection. Thus, we first find candidate cells based on the direction to the sink. Then, the routes generated by candidate cells are initiated in the CBC-GSEPC algorithm. Emperor Penguins Colony (EPC) is a new meta-heuristic algorithm that performs well in many cases. Due to its efficacy, we use the EPC algorithm for route selection with the golden sector concept. In the CBC-GSEPC algorithm, all candidate routes are initialised as a population array of penguins (each route considered penguin). Let $R_1, R_2, .., R_q$ be the candidate routes. In the CBC-EPC algorithm, all these routes are initialised as emperor penguins (EPs). At first, each EP is initialised in its position, and the cost function ($f(x)$) is computed. The $f(x)$ is often called a fitness function. In this work, the $f(x)$ for R_i is computed by Equation 26. Each function can be represented as Equation 27, 28 and 29, respectively.

$$F(i) = \frac{\mathbb{E}+\mathbb{S}}{\mathbb{D}} \tag{26}$$

Each function can be represented as follows,

$$\mathbb{E} = \frac{\sum_{j=1}^{h}[\omega_j - xEC_j]}{h} \tag{27}$$

$$\mathbb{S} = \frac{\sum_{j=1}^{h}[\frac{\gamma_j + I(\gamma_j)}{2}]}{h} \tag{28}$$

$$\mathbb{E} = h + \frac{\sum_{j=1}^{h}[xD_j]}{h} \tag{29}$$

Here h denotes the number of nodes in the route and xEC_j represents the expected energy consumption of j^{th} node to transmit the data. Similarly, $I(\gamma_j)$ is the indirect trust value provided by other neighbouring GHs and xD_j denotes the expected delay experienced by node j to transmit the data.

$$Q_{Penguin} = A\epsilon\sigma\Psi^4 \tag{30}$$

In the CBC-GSEPC algorithm, all penguins move towards the penguin, which has a higher $f(x)$. Then heat radiation is computed for each penguin as per Equation 30. Where, $Q_{Penguin}$ is heat transfer per unit time, A is total surface area, σ is the Stefan-Boltzmann constant, and Ψ is the absolute temperature. By using the following expression, the attractiveness of each penguin is computed in Equation 31, where x is the distance between two linear sources and η is the attenuation coefficient. Then, the coordinated movement is determined as Equations 32 and 33. Where, x_p, y_p are the x and y coordinates of the position (p). Upon the position of the best EP, the current penguin updates its position value. To optimise this, we introduce the golden sector concept. In this, the interval set as $[J_1, J_2]$. In this interval, two intermediate points are generated as Equation 34 and 35.

$$At_{Penguin} = Q_{Penguin}e^{-\eta d} \tag{31}$$

$$x_p = w_1 \cos\theta_p e^{w_2\theta p} \tag{32}$$

$$y_p = w_1 \sin\theta_p e^{w_2\theta p} \tag{33}$$

Here, $\zeta = \frac{1+\sqrt{5}}{2}$ the golden ratio. The evaluation is performed in this interval to identify the optimal solution within the most specific search space. This concept also minimises the time consumption to find the optimal solution. Algorithm 5 illustrates the procedure of proposed inter-cluster routing.

$$JP_1 = J_2 - \frac{J_2 - J_1}{\zeta} \tag{34}$$

$$JP_2 = J_1 + \frac{J_2 - J_1}{\zeta} \tag{35}$$

Algorithm 5: CBC-GSEPC for inter-cluster routing

```
Begin
  Initialize candidate cells
  Find $R_1, R_2, .., R_q$ ∈ Candidate Routes
  Assign $R_i \rightarrow EP_i$
  For Iteration<maximum
      For $i = 1$ to $q$
          For $j = 1$ to q ($i \neq j$)
              Set [$J_1$,$J_2$]
              Find [$JP_1$,$JP_2$]
              Evaluate EPs
              Compute $f(i)$
              If $f(i) > f(j)$, Then do
                  Compute $Q_{Penguin}$
                  Compute $At_{Penguin}$
                  Compute $(x, y)$
                  Determine new position (p)
                  Evaluate new solutions
              Else
                  Move to next sector
              End If
          End For
      End For
  End For
End
```

v. Data Validation at Sink Level

For this purpose, an RbDV technique was proposed. The sink node is designed with three blocks as verification block, monitoring block, and decision-making block in the proposed work. The responsibilities of each block are provided as follows,

Verification Block- This block validates the received data packets and inspects the received data integrity using the hash verification process. If the hash value is not matched with the source node appended value, then the received information is concluded as modified and rejected by the sink node and informs the next block. The modification ratio (Mod_Rat) can be computed by Equation 36. It is computed in terms of a total number of modified packets ($M(\mu)$) and a total number of received packets ($Re(\mu)$).

Monitoring Block- This block maintains a sliding window (SW) to monitor the network traffic. This block has prior knowledge of received data for each cell. In the sliding window, the average sensor reading value was maintained for some time. For a grid cell i, the sliding window contains an average reading for some time ($\daleth$). A time period is the combination of time intervals as $\{\daleth = \daleth_1, \daleth_2, .., \daleth_\varkappa\}$. If $\varkappa = 5$, then the last five-set of average readings are maintained in the sliding window. The average reading value for data received from GH_i is computed as Equation 37. Further, the average value is determined for the current data packets. Then the distance between the current average and previous average values is determined by Equation 38.

$$Mod\_Rat = \frac{(M(\mu))}{(Re(\mu))} \tag{36}$$

$$Avg(\mu_i) = \frac{\sum_{j=1}^{a} \mu_1, \mu_2, .., \mu_a}{a} \tag{37}$$

$$Avg\ Dis = |Current\ Avg - Previous\ Avg| \quad (38)$$

Decision-Making Block- This block makes the final decision on a particular GH's security level based on previous blocks' reports and the SW-NN algorithm to make an accurate decision on the GH validity. In SW-NN, the Neutrosophic set is used with the artificial neural network (ANN). The Neutrosophic set is the potential technique that resolves the problems which are complex in the fuzzy process. The corresponding parameters are learned from the previous blocks, along with the past behaviour of GH. Typically, the Neutrosophic algorithm has three components as Truth, Indeterminacy and Falsity. For a Neutrosophic set, three membership functions as truth-membership (U), indeterminacy membership (V) and non-membership (W) are designed. Unlike the traditional system, the membership functions are in the interval of "$]^{-}0,1^{+}[$". Upon the membership function, the Neutrosophic rule applied as follows, ***If Mod_Rat [Low, IntdetermincyLow, FalseLow] $$ If AvgDis [Low, IntdetermincyLow, FalseLow] && If P.Be [High, IntdetermincyHigh, FalseHigh] && Then Output [High, IntdetermincyHigh, FalseHigh].*** Here all three sets have {Low, Medium, High} membership functions. If Mod_Rat, AvgDis is low, then the data modification is downward. If the PastBe is high, then the GH has well past behaviours regarding previous data transmission. In this case, the GH will have a high result which denotes that the GH is valid. Based on the membership functions, the GH is validated As a remedy, the sink changes the GH for that cell. This way of GH validation improves security in the next round and improves overall network performance. Therefore, the proposed E2DA scheme provides energy efficiency and end-to-end security by using a novel deduplication concept. As lightweight algorithms are used for protection, the complexity is also optimised.

V. Experimental Analysis

We analyse the proposed E2DA-3D reconfigurable WSN scheme through an extensive simulation experiment.

A. Simulation Setup

The overall simulation is carried in the network simulator-3.26. Ns-3 is the discrete event simulator that supports various networks and protocols. All algorithms are written and built-in ns-3 using C++ and Python languages. In the simulation, setting up the configurations is the prime responsibility. Thus, we set the simulation parameters as per Table 1.

i. Prototype Testing

Here, we demonstrated the use case of the proposed reconfigurable WSN in ocean monitoring applications.

In ocean monitoring applications, the sensor nodes are deployed in the 3D environment. As per our proposed work, the 3D environment is further divided into grid cells. In each cell, sensor nodes are deployed to perform monitoring tasks. The ocean monitoring application was constructed, as shown in Fig 3, using the above sensors. The sensor node senses the environment and transmits the sensed data to the sink node, placed on the ocean's top. This real-time Ocean monitoring system with the 3D-reconfigurable-WSN E2DA approach provides end-to-end security and prolongs the networks lifetime.

TABLE 1
SIMULATION SETTINGS

Parameter			Value
Hardware Configuration	Simulator		NS-3.26
	Operating System		Ubuntu 14.04
	RAM		2 GB
	Processor		Pentium III
Network Configuration	Simulation Area		900×900×900
	Simulation Time		100s
	Physical Model		IEEE 802.11a
	Number of Grid Cells		27 (3× 3 × 3)
	Number of Sensor Nodes		100
	Number of the Sink node		1
	Number of Validators		27
	Sink Node Position		(450,900,900)
Node Configuration	Initial Energy Level		100J
	Transmission Range		150m
	Tx Power		1.4 Watt
	Rx Power		1.0 Watt
Packet Configuration	Packet Size		1024 Bytes
	Header Size		24 bits
	Number of Packets		200
	Packet Interval		0.1 ms
	Number of retransmissions		7
	Traffic Type		TCP and UDP
	Mean Packet Arrival		0.01 s
Channel Configuration	Channel Bandwidth		20 MHz
	Carrier Frequency		5170-5250 MHz
	Data Rate		54 Mbps
	Propagation Model		Nakami
Protocol Configuration	MM-Fuse	α, β	0.3, 0.7
	C2XTEA	Key size	128-bits
		Block size	64-bits
		Number of rounds	32
		Key generation	Cubic Chaotic Function
	PHOTON	o	128
		br	16
		br'	16
		Number of rounds	64
	CBC-GSEPC	Initial Population	200
		A	0.56
		ϵ	0.98
		Number of iterations	100

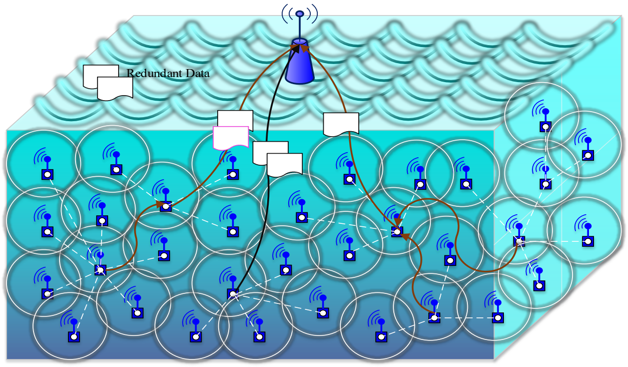

Fig. 3. E2da In Ocean Monitoring

ii. Comparative Analysis

The performance of the proposed work evaluated three different aspects: energy efficiency, transmission efficiency and security. Also, we compared with NEP [23], homomorphic algorithm [17], SMEER [26], EEICS [37] and 3D-PEGASIS [38]. The observations were made in terms of performance metrics: average energy consumption, average residual energy, packet delivery ratio (PDR) and delay.

iii. Analysis of energy efficiency

As we have used the first-order radio model, energy consumption is measured based on Eqn. (8). In this analysis, each node n has initial energy of $100J$. And the sink node $sn$is assumed to have infinite energy. In contrast, to prolong the network lifetime, it is primary to utilise less energy as possible for each sensor node. Our proposed techniques at the various stages in this work helped to reach better results while offering end-to-end security than the existing work. Fig 4 shows the average energy consumption and Fig 5 shows residual energy levels over the simulation period of $100s$, and the number of node $n = 100$. In Fig 5, we observed that our proposed E2DA 3D WSN has considerably less average energy consumption than previous works on every $20s$ period. Similarly, the existing nep and homomorphic algorithm have a higher energy consumption of 85.8% and 89.6% vice versa. After 100s of simulation time. Fig 4 observed that due to heavy computational in the homomorphic algorithm has a sharp drop in the residual energy down to 4J while energy consumption of 94%. Simultaneously, our proposed lightweight encryption model and efficient routing techniques show much better results than the other works. Table 2 shows the numerical comparison of energy levels for the proposed and existing works. The proposed network construction supports energy efficiency in the network. We also eliminate the invalid nodes (i.e.) minimise energy consumption.

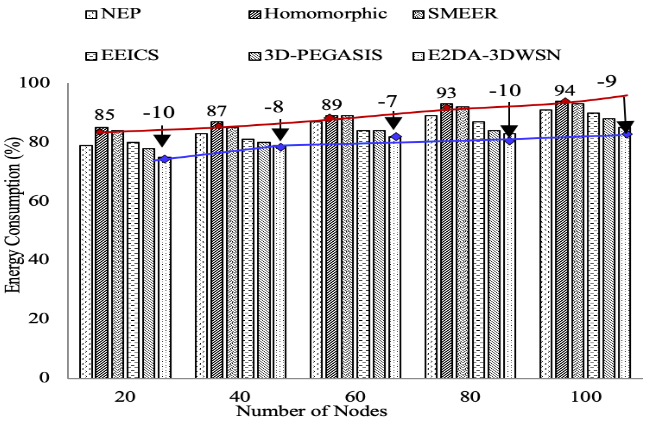

Fig. 4. Analysis of average energy consumption

iv. Analysis of data transmission efficiency

The data transmission efficiency was measured in terms of PDR and delay in transmission time. PDR defines the ratio between the number of packets transmitted from the source node to the sink node. Simply, the delay metric measures the time taken by the data packet to reach the source's sink nodes. Fig 6 and Fig 7 shows the observed PDR and delay results from the simulator. In terms of PDR, the proposed trust-based C1-to-1M, CBC-GSEPC routing algorithms helped transmit 92% of packets successfully that the other works. For a reliable PDR, it is necessary to route the packages in an optimal route through the best forwarder node identified through our equality (20). In the NEP method and homomorphic method, the optimal route selection process is ignored. In SMEER, EECIS and 3D-PEGASIS, either intra-cluster or inter-cluster routing is performed. Optimal routing is not only improved PDR but also minimises the transmission delay.

For these reasons, data transmission efficiency decreased in previous research works. The homomorphic method has been drastically delayed to 115s since the data has to process at each intermediate node. Involvement of lightweight cryptography schemes and optimal route selection schemes in proposed E2DA supports better PDR and delay.

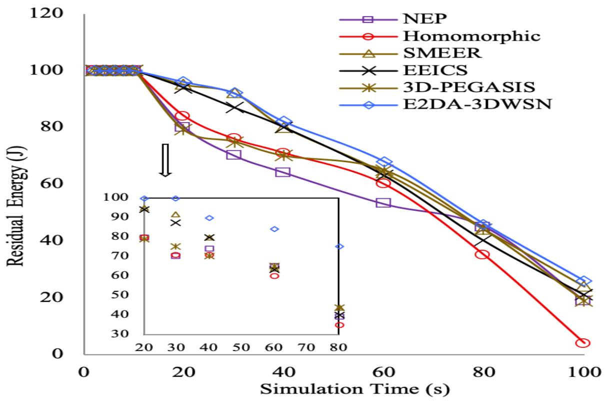

Fig. 5. Analysis of average residual energy

TABLE 2
NUMERICAL COMPARISON OF ENERGY EFFICIENCY

Method	Average energy consumption (J)		Average Residual Energy (J)	
	$n = 100$	Simulation time	$n = 100$	Simulation time
NEP	85.8	45	15	55
Homomorphic	89.6	45	11	55
SMEER	88.6	34	12	66
EEICS	84.4	36	16	64
3D-PEGASIS	82.2	42	18	58
E2DA-3DWSN	**80.8**	**32**	**19**	**68**

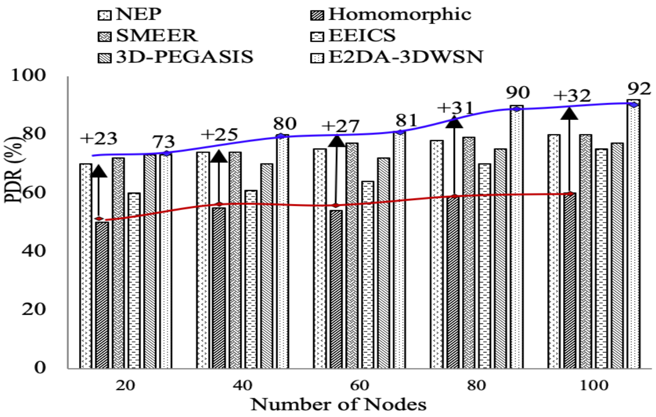

Fig. 6. Analysis of PDR

In table 3, the data transmission efficiency of the proposed work analyzed. The analysis shows that the proposed E2DA method achieves better performance in terms of PDR and delay.

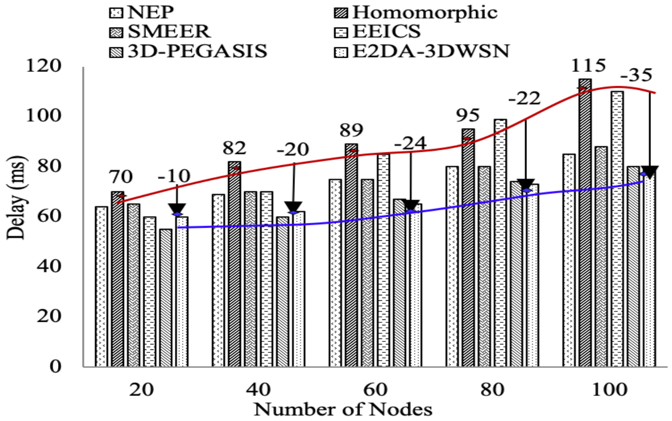

Fig. 7. Analysis of delay

TABLE 3
NUMERICAL COMPARISON OF DATA TRANSMISSION EFFICIENCY

Method	PDR (%)	Number of packets transmitted	Number of packets lost	Delay (ms)
NEP	75.4	150	50	74.6
Homomorphic	55.6	111	89	90.2
SMEER	76.4	152	48	75.6
EEICS	66	132	68	84.8
3D-PEGASIS	73.4	146	64	67.2
E2DA-3DWSN	**83.2**	**166**	**64**	**68**

B. Security Analysis

As stated earlier, we have considered three types of threats associates with the WSN. This section discusses how the proposed work mitigates those threats. ***I) Modification Attack:*** The HDC algorithm and RbDV based validation techniques help verify the integrity of the information and isolate affected nodes using our proposed methods. ***II) Eavesdropping:*** The information overhearing problem in the existing work has now been overcome with our novel C2CXTEA encryption algorithm. ***III) Unauthorised Access:*** This threat has been resolved using the proposed RID-XOR based node authorisation.

C. Energy Efficiency Analysis

Along with the security, we considered prolonging network lifetime by minimising nodes energy consumption with our proposed network model and routing techniques. Table 4 summarizes the contributions of the proposed scheme in terms of energy efficiency.

D. Complexity Analysis

The overall complexity of the proposed E2DA method includes computations for GH selection ($O(F/3)$), hash generation ($O(F\text{-}3)$), encryption (2^F), and routing ($O(F)$). Since the dual validation process performed in the sink node (which has no energy restrictions), we have not included this process. From this analysis, we can conclude the overall complexity of our proposed work as follows,

$$Complexity = O\left(\frac{7F-3}{3}\right)(2^F) \tag{39}$$

The complexity of the proposed work is much lower than exiting homomorphic process ($O(F \log F * 2^F)$ as it has multiple computations at each intermediate nodes. Thus the proposed work is suitable for resource-constrained WSN environments.

TABLE 4
ENERGY EFFICIENCY SUMMARIZATION

Proposed Scheme	Impact on observations
3D-Grid Construction and MM-Fuse	3D-Grid cell construction with Co-Spheres supports data aggregation Increases residual energy and minimizes energy consumption Optimal GH selection supports energy efficiency and also improves delay, PDR and throughput
C1-to-1M and Secure Deduplication	Optimal routing increases data transmission efficiency, and duplication removes securely
CBC-GSEPC	Improves overall performance Increases PDR, delay, throughput and reliability helps minimum energy consumption

VI. Conclusion

This paper proposed a cost-aware, energy-aware, and privacy protected 3D reconfigurable WSN. We proposed a novel lightweight C2XTEA encryption method, HDC based secure deduplication technique over encrypted data, the RbDV technique, and SW-NN algorithm for privacy protection and data validation. Moreover, the C1-to-1M and the CbC-GSEPC algorithms were proposed for energy-aware intra-cluster and inter-cluster routing purposes. This work has been demonstrated on Linux based NS-3.26 network simulator. The simulator's result shows that the proposed work has improved the network lifetime and ensured end-to-end data security for WSN. This proposed work can develop further to consider cloud-assisted intrusion detection and network routing, which are not represented in our proposal.

REFERENCES

[1] Anjum, S. S., Noor, R. M., Anisi, M. H., Ahmedy, I. B., Othman, F., Alam, M., & Khan, M. K. (2017). Energy management in RFID-sensor networks: Taxonomy and challenges. IEEE Internet of Things Journal, 6(1), 250-

[2] Tsoumanis, G., Oikonomou, K., Aïssa, S., & Stavrakakis, I. (2020). Energy and Distance Optimization in Rechargeable Wireless Sensor Networks. IEEE Transactions on Green Communications and Networking.

[3] Samanta, A., & Misra, S. (2017). Energy-efficient and distributed network management cost minimization in opportunistic wireless body area networks. IEEE Transactions on Mobile Computing, 17(2), 376-389.

[4] Goudarzi, S., Kama, N., Anisi, M. H., Zeadally, S., & Mumtaz, S. (2019). Data collection using unmanned aerial vehicles for the internet of things platforms. Computers & Electrical Engineering, 75, 1-15.

[5] ElMossallamy, M. A., Zhang, H., Song, L., Seddik, K. G., Han, Z., & Li, G. Y. (2020). Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities. IEEE Transactions on Cognitive Communications and Networking, 6(3), 990-1002.

[6] Kavousi-Fard, A., Su, W., & Jin, T. (2020). A Machine-Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids. IEEE Transactions on Industrial Informatics, 17(1), 650-658.

[7] Misra, S., Moulik, S., & Chao, H. C. (2015). A cooperative bargaining solution for priority-based data-rate tuning in a wireless body area network. IEEE transactions on wireless communications, 14(5), 2769-2777.

[8] Anisi, M. H., Rezazadeh, J., & Dehghan, M. (2008, September). FEDA: fault-tolerant energy-efficient data aggregation in wireless sensor networks. In 2008 16th international conference on software, telecommunications and computer networks (pp. 188-192). IEEE.

[9] Misra, S., & Chatterjee, S. (2014). Social choice considerations in cloud-assisted WBAN architecture for post-disaster healthcare: Data aggregation and channelization. Information Sciences, 284, 95-117.

[10] Saleem, A., Khan, A., Malik, S. U. R., Pervaiz, H., Malik, H., Alam, M., & Jindal, A. (2019). FESDA: Fog-enabled secure data aggregation in smart grid IoT network. IEEE Internet of Things Journal, 7(7), 6132-6142.

[11] Boudia ORM, Senouci SM, Feham M (2015) A novel secure aggregation scheme for WSN using stateful public key. Ad Hoc Networks 32:98–113

[12] Razzaq, M., Devi, N.D., & Shin, S. (2018). Energy-efficient K-means clustering-based routing protocol for WSN using optimal packet size. 2018 International Conference on Information Networking (ICOIN), 632-635.

[13] Wang, Q., Lin, D.,& Zhang, Z. (2019). An Energy-Efficient CS-Based Clustering Routing Protocol for WSNs. IEEE Sensors Journal, 19, 3950-3960.

[14] Tomić, I., & McCann, J.A. (2017). A Survey of Potential Security Issues in Existing WSN Protocols. IEEE IoT Journal, 4, 1910-1923.

[15] Sharma, N., & Bhatt, R. (2018). Privacy Preservation in WSN for Healthcare Application. Procedia Computer Science 132, 1243–1252.

[16] Latha, A., Prasanna, S., Hemalatha, S., & Sivakumar, B. (2019). A harmonised trust assisted energy-efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[17] Cui, J., Shao, L., Zhong, H., Xu, Y., & Liu, L. (2018). Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks. Peer-to-Peer Networking and Applications, 11, 1022-1037.

[18] Kumar, K.A., Krishna, A.V. and Chatrapati, K.S., 2017. New secure routing protocol with elliptic curve cryptography for military heterogeneous WSN. Journal of Information and Optimizatio Sciences, 38(2), pp.341-365.

[19] Zhao, Z., Shi, D., Hui, G., & Zhang, X. (2019). An Energy-Optimization Clustering Routing Protocol Based on Dynamic Hierarchical Clustering in 3D WSNs. IEEE Access, 7, 80159-80173.

[20] Dattatraya, K.N., & Rao, K.R. (2019). Hybrid based cluster head selection for maximising network lifetime and energy efficiency in WSN. Journal of King Saud University - Computer and Information Sciences.

[21] Neamatollahi, P., Abrishami, S., Naghibzadeh, M., Moghaddam, M.H.Y. and Younis, O., 2017. Hierarchical clustering-task scheduling policy in cluster-based WSN. IEEE Transactions on Industrial Informatics, 14(5), pp.1876-1886.

[22] Ngangbam, R., Hossain, A., & Shukla, A. (2019). Improved low energy adaptive clustering hierarchy. International Journal of Electronics.

[23] Lin, D., & Wang, Q. (2019). An Energy-Efficient Clustering with Game Theory and Dual-Cluster-Head for WSNs. IEEE Access, 7, 49894-49905.

[24] Kakkar, D., 2018, December. TOPSIS optimized Dual-Hop Routing Protocol for Homogeneous WSN with Grid-Based Clustering. In 2018, Secure Cyber Computing and Communication (ICSCCC) (pp. 154-159). IEEE.

[25] Wang, F., & Hu, H. (2019). Multipath data fusion method based on a routing algorithm for WSN. International Journal of Computers &Applications.

[26] Yessembayev, A., Sarkar, D., & Sikder, F. (2018). Detection of Good and Bad Sensor Nodes in the Presence of Malicious Attacks. IEEE Transactions on Signal and Information Processing over Networks, 4, 549-563.

[27] Yuvaraj, D., Sivaram, M., & Navaneetha Krishnan, S. (2019): Intelligent detection of untrusted data transmission to optimise energy in sensor networks, Journal of Information and Optimization Sciences.

[28] Deb, S. and Haque, M., 2019. Elliptic curve and pseudo-inverse matrix based cryptosystem for WSN. International Journal of Electrical & Computer Engineering (2088-8708), 9(5).

[29] Tiberti, W., Caruso, F., Pomante, L., Pugliese, M., Santic, M. and Santucci, F., 2020. Development of an extended topology-based lightweight cryptographic scheme for IEEE 802.15. 4 WSN. International Journal of Distributed Sensor Networks, 16(10), p.1550147720951673.

[30] Attkan, A. and Ahlawat, P., 2020. Lightweight two-factor authentication protocol and session key generation Scheme for WSN in IoT deployment. Advances in Machine Learning for Communication Technologies, pp.189-198.

[31] Wang, A., Shen, J., P., & Tian, L. (2019). Secure big data communication for energy-efficient intra-cluster in WSNs. Inf. Sci., 505, 586-599.

[32] Nivedetha, B., & Vennila, I. (2019). FFBKS: Fuzzy Fingerprint Biometric Key Basedsecurity schema for WSN. Computer Communications.

[33] Wang, J., Zhang, L.Y., Chen, J., Hua, G., Zhang, Y., & Xiang, Y. (2019). Compressed Sensing Based Selective Encryption With Data Hiding Capability. IEEE Transactions on Industrial Informatics, 15, 6560-6571.

[34] Qiu, H., Qiu, M. and Lu, Z., 2020. Selective encryption on ECG data in body sensor network on machine learning. Information Fusion, 55, pp.59-67.

[35] Anuradha, D. and Srivatsa, S.K., 2019. Energy effectual reconfigurable routing protocol (E2R2P) for cluster based underwater wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-8.

[36] Gao, S. and Piao, Y., 2014, May. DRRP: A dynamically reconfigurable routing protocol for WSN. In 2014 IEEE International Conference on Progress in Informatics and Computing (pp. 460-465). IEEE.

[37] Thangaramya, K., Kulothungan, K., Logambigai, R., Selvi, MK, Ganapathy, S., & Kannan, A. (2019). Energy-aware cluster and neuro-fuzzy based routing algorithm for WSN in IoT. Computer Networks,151, 211-223.

[38] Thebiga, M. and Pramila, S.R., 2021. Energy efficacious modified routing emperor penguin colony optimization multi-faceted metaheuristics algorithm for MANETS. Wireless Personal Communications, 118(2), pp.1245-1270.

[39] Harifi, S., Khalilian, M., Mohammadzadeh, J. and Ebrahimnejad, S., 2019. Emperor Penguins Colony: a new metaheuristic algorithm for optimization. Evolutionary Intelligence, 12(2), pp.211-226.

[40] Hosen, A.S.M., G.H. and Ra, I.H., 2017. An eccentricity based data routing protocol with uniform node distribution in 3D WSN. Sensors, 17(9), p.2137.