Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.034421
Article

Tech Science Press

Enhanced Metaheuristics with Trust Aware Route Selection for Wireless Sensor Networks

A. Francis Saviour Devaraj[1], T. Satyanarayana Murthy[2], Fayadh Alenezi[3], E. Laxmi Lydia[4], Mohamad Adzhar Md Zawawi[5] and Mohamad Khairi Ishak[5,*]

[1]Department of IT, The University of Technology and Applied Sciences-Ibri, PO Box: 466, Ibri, Postal Code: 516, Sultanate of Oman
[2]Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India
[3]Department of Electrical Engineering, College of Engineering, Jouf University, Saudi Arabia
[4]Department of Computer Science and Engineering, Vignan's Institute of Information Technology, Visakhapatnam, 530049, India
[5]School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, Nibong Tebal, 14300, Penang, Malaysia
*Corresponding Author: Mohamad Khairi Ishak. Email: khairiishak@usm.my
Received: 16 July 2022; Accepted: 22 November 2022

Abstract: Recently, a trust system was introduced to enhance security and cooperation between nodes in wireless sensor networks (WSN). In routing, the trust system includes or avoids nodes related to the estimated trust values in the routing function. This article introduces Enhanced Metaheuristics with Trust Aware Secure Route Selection Protocol (EMTA-SRSP) for WSN. The presented EMTA-SRSP technique majorly involves the optimal selection of routes in WSN. To accomplish this, the EMTA-SRSP technique involves the design of an oppositional Aquila optimization algorithm to choose safe routes for data communication. For the clustering process, the nodes with maximum residual energy will be considered cluster heads (CHs). In addition, the OAOA technique gets executed to choose optimal routes based on objective functions with multiple parameters such as energy, distance, and trust degree. The experimental validation of the EMTA-SRSP technique is tested, and the results exhibited a better performance of the EMTA-SRSP technique over other approaches.

Keywords: Security; wireless sensor networks; trust factor; routing protocol; privacy

1 Introduction

Wireless Sensor Network (WSN) has evolved into one of the promising technologies utilized in the current ecosphere [1]. WSN observes the environments in which it may be placed for collecting data and can identify variations in observing regions of humidity, temperature, sound, vibration pressure, motion, and intensity [2]. WSN application programs are broadly utilized in smart home monitoring systems, environmental observing systems, bridges or building operational monitoring systems, bio-medical applications, military solicitations, inventory management systems, habitat monitoring systems, industrial

robotics systems, and health monitoring mechanisms natural disaster monitoring mechanisms, and traffic monitoring system [3].

A wireless network is considered an adaptable gadget meant for data communication. It uses radio frequency algorithms such as wireless channels for sending data via air, eradicating the wired requirements [4]. A common technique for some final transmission phases between the gadgets of wired networks and smartphones is enhancing the cellular network as an alternative one of wired connections [5]. In return, the availability of mass media for broadcasting causes the wireless network to be highly vulnerable to safety menaces. The safety assault is an action that interrupts the machine's safety in contrast to the unit via an intelligent threat. There may be various types of menaces [6]. The defence menaces are classified as passive and active assaults. Despite various services of safety authentication, counting access management, data completeness, and non-repudiation, encoding of data the assault lasts [7]. Moreover, WSNs are more sensitive as the nodes are recurrently positioned in an uncomfortable range. Even though, several applications routes at the atmospheres which are unreliable that further desire a sheltered routing and transmission [8]. Fig. 1 depicts the overview of WSN.

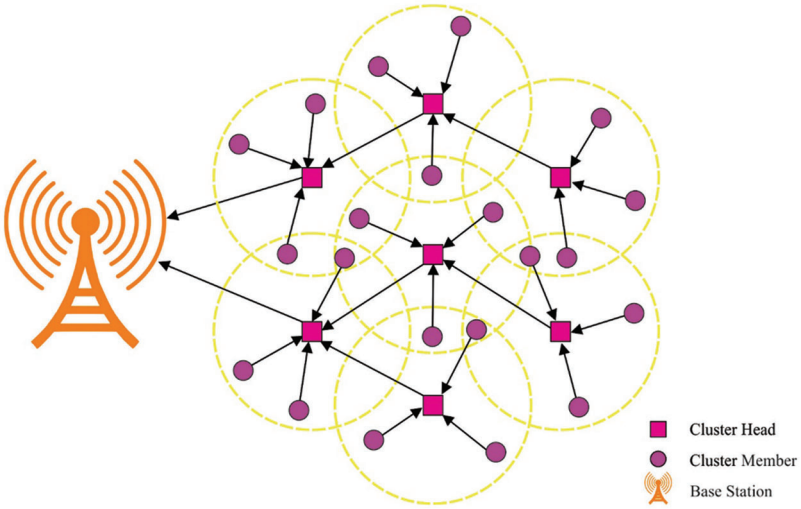

Figure 1: Overview of WSN

Otherwise, the sensor nodes (SN) route the accumulation of data to its transitional nodes that are linked with wireless gadgets for transmitting data against a receiver node. Yet, an appropriate or ideal protocol for routing in an optimum way is suitable for data communication via a few nodes which contain a routing path of multi-hop along with its extent inside them than the receiver [9]. Power utilization should be minimal by considering the delicate decision-making methodologies that rest on the regulations such as nodes clustering and routing to execute a perfect routing function [10]. However, the creation of cluster nodes and selecting the cluster head takes place for every cluster path and routing path, completely over CHs, therefore, diminishing the amount of the contributing node; so far, these grounds decrease in energy utilization. Though several models are available in the literature, it is still needed to design a secure routing protocol in WSN along with the clustering process. In addition, the usage of multiple input parameters for optimal clustering and routing becomes essential in WSN.

This article introduces Enhanced Metaheuristics with Trust Aware Secure Route Selection Protocol (EMTA-SRSP) for WSN. The presented EMTA-SRSP technique involves the design of an oppositional Aquila optimization algorithm to choose secure routes for data communication. For the clustering

process, the nodes with maximum residual energy will be considered cluster heads (CHs). In addition, the OAOA technique gets executed to choose optimal routes based on objective functions with multiple parameters such as energy, distance, and trust degree. Since the EMTA-SRSP technique considers the trust level of the nodes, the routes with maximum security will be considered. The experimental validation of the EMTA-SRSP algorithm has been tested in several prospects.

2 Related Works

Awan et al. [11] devise an effective routing method by compiling IoT with Blockchain (BC) for distributed nodes that operate in a distributed way for using the transmission links professionally. The presented protocol employs smart contracts in heterogeneous IoT environments for finding a route to BS. Every node could ensure routes from IoT nodes to sink then BS, allowing IoT gadgets to collaborate at the transmission time. The presented routing protocol eliminates redundant data and IoT network assaults, results in lesser energy utilization, and enhances network life. Sanchez et al. [12] introduce a decentralized mechanism that ensures the security and autonomy of an IoT network. The devised technique helps protect data availability and integrity related to the security benefits BC offers and the use of cryptographic tools. The presented approach's accuracy has been measured on a temperature and humidity-sensed IoT-related WSN. The attained outcomes prove the proposal satisfies the major needs of an IoT network. It is autonomous, secure for sharing and sending information among users and gadgets, has privacy, is dependable, and the data can be accessible in the infrastructure.

A new trust-aware localized routing and class-related dynamic encryption method were offered in [13]. The technique initially finds the route to attaining the destiny and sends the data packets. By identification of the values of such variables, the value of trusted data forwarding support (TDFS) can be measured. Amjad et al. [14] modelled distance, degrees, and remaining energy-related low-energy adaptive clustering hierarchy (DDR-LEACH) protocols. DDR-LEACH can be employed for replacing CHs with the ordinary node depending on maximal RE, degree, and minimal distance from BS. In addition, saving a vast amount of data in BC can be expensive. An external data storage, called an interplanetary file system (IPFS), can be used to deal with this problem. Moreover, to ensure data security in IPFS, AES 128-bit was employed, which executes superior to the prevailing encryption methods.

An effectual real-time service-centric feature-sensitivity-analysis (RSFSA) method can be presented in [15]. The RSFSA algorithm examines the sensitivity of distinct features accessed through any service at many levels. At every stage, the technique verifies the feature set is accessed and the number of features the users have granted accessibility for computing the FLAG value for the user respective to the profile given. Depending on the value of FLAG, the users may be provided or denied access to the service. In contrast, the technique manages various encryption methods and keys for every feature level. Elhoseny et al. [16] aim to devise an IoT solution for AI-assisted privacy preservation with big data transmitting utilizing BC. Initially, the presented method employs a graph-modeling to advance a reliable and scalable system to collect and transmit data. Then, symmetric-related digital certificates were used to offer authentic and confidential communication with communication sources utilizing BC.

3 The Proposed Model

This article introduced a novel EMTA-SRSP algorithm for security in WSN. The presented EMTA-SRSP technique involves the optimal selection of safe routes in WSN. To accomplish this, the EMTA-SRSP technique involves the design of an oppositional Aquila optimization algorithm to choose secure routes for data communication. For the clustering process, the nodes with maximum residual energy will be considered CHs. In addition, the OAOA technique is executed to choose optimal routes based on objective functions with multiple parameters such as energy, distance, and trust degree.

3.1 Energy Model

All the sensors in the network have preliminary energy as J_0 and here, the deliberation made is that the node could not refresh the energy. The energy loss when transferring the information from *the* k^{th} node to the l^{th} *CH* pursue the multiple path fading models and free space models depending on the distance among receivers and transmitters. But the transmitter encompasses a power amplifier and radio electronics for energy dissipation [17]. Furthermore, the receiver end has radio electronics for energy dissipation. But the energy dissipated for all the data packets has the size of U depending on the distance and nature of nodes.

Consequently, energy dissipation through nodes when transmitting Ubytes of a dataset is characterized by,

$$J_{dis}\left(x^k\right) = J_{elc} * U + J_{amp} * U * \left\|\left\|x^k - G^l\right\|\right\|^4; \quad if \ \ \left\|\left\|x^k - G^l\right\|\right\| \geq s_0 \tag{1}$$

$$J_{dis}\left(x^k\right) = J_{elc} * U + J_w * U * \left\|\left\|x^k - G^l\right\|\right\|^2; \ if \ \left\|\left\|x^k - G^l\right\|\right\| < s_0 \tag{2}$$

$$V_{s0} = \sqrt{\frac{J_w}{J_{amp}}} \tag{3}$$

From the expression, J_{elc} shows the electronic energy determined by considering factors such as digital coding, spreading, filtering, amplifier, and modulation.

$$J_{elc} = J_{trans} + J_{agg} \tag{4}$$

In Eq. (4), J_{trans} denotes the energy transmitter and J_{agg} shows the energy of aggregating data. But J_{amp} characterizes the energy utilized for the power amplifier in the transmitter, and $\|x^k - G^l\|$ shows the distance between *CH* and standard sensors.

But the dissipated energy through the receiver afterwards receiving Ubytes of a dataset through CH is characterized by,

$$J_{dis}\left(G^l\right) = J_{elc} * U \tag{5}$$

Afterwards, receiving or transmitting Ubytes of the dataset, the energy values of every node J_a get upgraded.

$$J_{a+1}\left(x^k\right) = J_a\left(x^k\right) - J_{dis}\left(x^k\right) \tag{6}$$

$$J_{a+1}\left(G^l\right) = J_a\left(G^l\right) - J_{dis}\left(G^l\right) \tag{7}$$

The data transmission technique continues; each node is assumed to be a dead node. The node is assumed to be a dead node as long as the node has an energy which is lesser than 0.

3.2 Design of OAOA Technique

In this work, the OAOA technique is designed using oppositional-based learning (OBL) with AOA. The AOA methodology is a novel swarm intelligence (SI) technique [18]. There exist 4 hunting approaches of Aquila; for a variety of prey, Aquila could adaptably shift the hunting approaches for dissimilar prey and then utilize faster speed integrated into claws and sturdy feet to attack the target. The overview of the arithmetic formula is illustrated below.

Step 1: Extended exploration (X_1): highest soar with the vertical stoop

The Aquila flies above the ground level and broadly examines the searching region, following a vertical dive taken while describing the prey region. These behaviours are arithmetically formulated by the following formula:

$$X_1(t+1) = X_{besi}(t) \times \left(1 - \frac{t}{T}\right) + (X_M(t) - X_{best}(t) \times r_1) \tag{8}$$

$$X_M(t) = \frac{1}{N}\sum_{i=1}^{N} X_i(t) \tag{9}$$

Now, $X_{best}(t)$ indicates the best-attained place, and $X(t)$ characterizes the average place of Aquila in the existing iteration. t and T specify the prevailing iteration and the maximum iteration count, N represents the population size, and r_1 denotes an arbitrary integer within [0, 1].

Step 2: Narrowed exploration (X_2): contour flight with shortest glide attack

It is a popular hunting methodology for Aquila. It employs shorter gliding for attacking the target afterwards, a descendant with the selected region, and flying nearby the prey, and it is represented as follows:

$$X_2(t+1) = X_{best}(t) \times LP(D) + X_R(t) + (y - x) \times r_2 \tag{10}$$

Here, $X_R(t)$ denotes an arbitrary place of Aquila, D represents the dimension size, and r_2 characterize an arbitrary value in $[0,\ 1]$. $LF(D)$ indicates Levy's flight as follows:

$$LP(D) = s \times \frac{u \times \sigma}{|v|^{\frac{1}{\beta}}} \tag{11}$$

$$\sigma = \left(\frac{\Gamma(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\left(\frac{\beta-1}{2}\right)}}\right) \tag{12}$$

Let s and β be constant values corresponding to 0.01 and 1.5; u and v refer to arbitrary values within zero and one. y and χ represent the spiral shape in the searching region and are evaluated as follows:

$$\begin{cases} x = r\ \times\ \sin(\theta) \\ y = r\ \times\ \cos(\theta) \\ r = r_3 + 0.00565 \times D_1 \\ \theta = -\omega \times D_1 + \dfrac{3 \times \pi}{2} \end{cases} \tag{13}$$

Now, r_3 denotes the number of searching cycles ranging from [1, 20], D_1 encompassed integer numbers from 1 to D dimension, ω corresponding to 0.005.

Step 3: Expanded exploitation (X_3): lowest flight with the slowest descent attack

Once the prey area is identified normally, the Aquila begins implementing an initial attack. AOA employs the designated location for approaching and attacking the target. These behaviours are arithmetically expressed as follows:

$$X_3(t+1) = (X_{best}(t) - X_M(t)) \times \alpha - r_4 + ((UB - LB) \times r_5 + LB) \times \delta \tag{14}$$

Now, $X_{besi}(t)$ characterizes the optimum obtaining position, and $X_M(t)$ shows the average number of existing locations. α and δ signify the exploitation finetuning variable fixed to 0.1, UB and LB signify the upper and lower bounds, and r_4 and r_5 represent arbitrary numbers in (0, 1).

Step 4: Narrowed exploitation (X_4): grabbing and walking prey

Now, the Aquila hunts the target regarding attacking the prey and escape trajectory and it is arithmetically formulated in the following:

$$\begin{cases} X_4(t+1) = QF \times X_{best}(t) - (G_1 \times X(t) \times r_6) - G_2 \times LF(D) + r_7 \times G_1 \\ QP(t) = t^{\frac{2 \times rand() - 1}{(1-T)^2}} \\ G_1 = 2 \times r_8 - 1 \\ G_2 = 2 \times \left(1 - \frac{t}{T}\right) \end{cases} \tag{15}$$

Now, $X(t)$ shows the existing position, and $QF(t)$ denotes the quality function value that balance the search technique. G_1 signifies the movement variable of Aquila in tracking prey, an arbitrary number within $[-1,\ 1]$. G_2 means the flight slope when hunting prey that linearly decreased from 2 to 0. r_6, r_7, and r_8 denotes arbitrary number within [0, 1]. Fig. 2 showcases the AO technique.

Figure 2: Processes involved in the AO technique

The OAOA is derived by using the oppositional-based learning (OBL) concept. OBL is a novel intelligent optimization technique [19]. The idea of reverse learning is to deliberate reverse and forward solutions, choose the optimum solution as the initialized population and initiate the population through reverse learning that could extend the searching interval of the population. Also, it improves the efficiency and speed of the model to search for the optimum solution. Presently, afterwards opposition based learning was developed, X_i in the individual population is formulated as follows:

$$X_i = \left[X_{i,1},\ X_{i,2} \cdots X_{i,j},\ X_{i,D}\right] \tag{16}$$

The inverse solution is formulated using Eq. (17):

$$X_{i'} = \left[X_{i,1'},\ X_{i,2'},\ \cdots X_{i,j'},\ X_{i,D}/\right] \tag{17}$$

where $i = 1,\ 2,\ 3 \ldots n,\ j = 1,\ 2,\ 3 \ldots D,\ n$ signifies the population count, D indicates the dimension of space, and the reverse and the forward solution must satisfy a specific relationship that is illustrated below:

$$X'_{i,j} = k\left(A_j + B_j\right) - X_{i,j} \tag{18}$$

In Eq. (18), k is a uniformly distributed arbitrary value among zero, and one viz., a common inverse factor, A_j and B_j show the lower limit and preceding term of the *jth* dynamic decision parameter. While choosing the AOA population, the summary of the reverse learning approach might improve the population count for improving the population diversity that makes the total optimization capability strong and fast convergence rate, reduces the possibility of getting trapped in optima, and improves the performance of AOA.

3.3 Trust-Aware Route Selection Process

In this study, the OAOA technique gets executed to choose optimal routes based on objective function with multiple parameters such as energy, distance, and trust degree. The OAOA aimed to extend the network lifespan and diminish the energy utilization of every sensor. Assume $h1$ denotes the objective function; thus, *CH* chooses the next hop *CH* with the highest RE for routing the data, thus maximizing the network lifetime, and then $h1$ is increased [20]. Consider $h2$ denotes another objective function: minimal distance between *CH* to the next hop *CH* and next hop CH to BS. To decrease the energy usage of the network should minimalize $h2$. Now, $h3$ refers to the third objective function. Thus, the CH chooses the next hop CHs with the maximal trust factor. To improve network lifetime should minimalize h_3.

Consider b_{ij} refers to a Boolean parameter determined by the following equation

$$b_{ij} = \begin{cases} 1 \ if \ next - hop(CH_i) \quad = CH_j \forall_{i,j} 1 \le i,\ \ j \le m \\ 0 \qquad\qquad\qquad\qquad\quad Otherwise \end{cases} \tag{19}$$

$$\text{Minimalize}\, F = 1/h_1 \times \beta_1 + h_2 \times \beta_2 + 1/h_3 \times \beta_3 \tag{20}$$

Subjected to,

$$dis\left(CH_i,\ \ CH_j\right) \times \le d_{\max}\, CH_j \varepsilon \{C + BS\} \tag{21}$$

$$\sum\nolimits_{j=1}^{m} b_{ij} = 1 \ \text{ and } 1 \ne j \tag{22}$$

$$0 < \beta_1,\ \ \beta_2,\ \ \beta_3 < 1 \tag{23}$$

The constraints (21) state that the next hop node of CHi lies in the interval of CHi, and the next hop node is *CHj*. The constraints (22) state that the next hop node of CHi is unique, viz., CHj, and the constraints (23) ensure that there must not be zero or hundred percent weight on any objective functions.

4 Performance Validation

The proposed model is simulated using the MATLAB tool. In this section, the performance of the EMTA-SRSP model is investigated under varying aspects. Table 1 and Fig. 3 provide packet delay (PDEL) examination of the EMTA-SRSP model with other models [4]. The results reported that the EMTA-SRSP model had enhanced results under all nodes. For example, with 500 nodes, the EMTA-SRSP model has presented a lower PDEL of 230 s, whereas the PSO and TDRS-WSN-DL models have obtained higher PDEL of 425 and 352 s correspondingly. Meanwhile, with 1000 nodes, the EMTA-SRSP method has offered a lower PDEL of 221 s, whereas the PSO and TDRS-WSN-DL algorithms have attained higher PDEL of 377 and 307 s correspondingly.

Table 1: Packet delay analysis of EMTA-SRSP approach with distinct nodes

Packet delay (sec)			
No. of nodes	PSO	TDRS-WSN-DL	EMTA-SRSP
500	425	352	230
1000	377	307	221
1500	332	253	156
2000	296	219	122
2500	251	183	113
3000	212	136	97

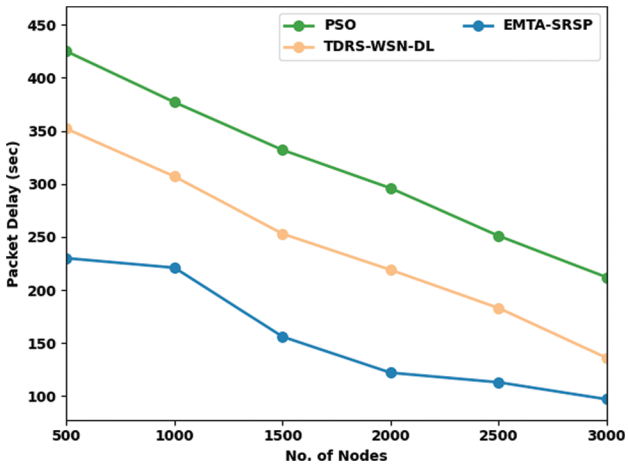

Figure 3: Packet delay analysis of EMTA-SRSP approach with distinct nodes

In addition, with 1500 nodes, the EMTA-SRSP approach has rendered a lower PDEL of 156 s, whereas the PSO and TDRS-WSN-DL models have acquired higher PDEL of 332 and 253 s correspondingly. Then, with 2000 nodes, the EMTA-SRSP model presented a lower PDEL of 122 s, whereas the PSO and TDRS-WSN-DL methodologies have attained higher PDEL of 296 and 219 s correspondingly.

In Table 2 and Fig. 4, a comprehensive packet delivery ratio (PDR) investigation of the EMTA-SRSP model with recent models occurs. The results ensured that the EMTA-SRSP model had shown higher PDR values under each node. For example, with 500 nodes, the EMTA-SRSP method has gained a maximum PDR of 0.966 bps, while the PSO and TDRS-WSN-DL models have attained a minimal PDR of 0.693 and 0.892 bps, correspondingly. Similarly, with 1000 nodes, the EMTA-SRSP method has attained a maximum PDR of 0.942 bps, whereas the PSO and TDRS-WSN-DL approaches have attained a minimal PDR of 0.668 and 0.863 bps correspondingly. Also, with 1500 nodes, the EMTA-SRSP algorithm has obtained a maximum PDR of 0.884 bps while the PSO and TDRS-WSN-DL approaches have attained minimal PDR of 0.585 and 0.767 bps correspondingly. At last, with 2000 nodes, the EMTA-SRSP method has attained a maximum PDR of 0.788 bps whereas the PSO and TDRS-WSN-DL models have attained minimal PDR of 0.531 and 0.668 bps correspondingly.

Table 2: PDR analysis of EMTA-SRSP approach with distinct nodes

Packet delivery ratio (bps)			
No. of nodes	PSO	TDRS-WSN-DL	EMTA-SRSP
500	0.693	0.892	0.966
1000	0.668	0.863	0.942
1500	0.585	0.767	0.884
2000	0.531	0.668	0.788
2500	0.473	0.560	0.697
3000	0.374	0.486	0.635

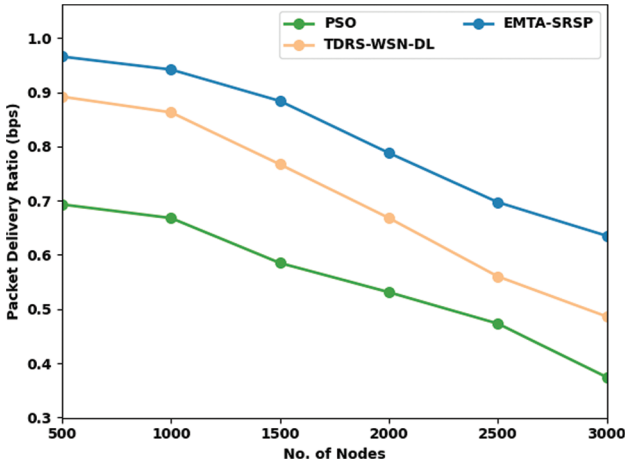

Figure 4: PDR analysis of EMTA-SRSP approach with distinct nodes

In Table 3 and Fig. 5, a comprehensive Packet drop (PDROP) study of the EMTA-SRSP algorithm with recent models occurs. The results ensured that the EMTA-SRSP approach displayed higher PDROP values under each node. For example, with 500 nodes, the EMTA-SRSP approach has attained a maximum PDROP of 40 p/s whereas the PSO and TDRS-WSN-DL approaches have attained minimal PDROP of 86 and 56 p/s correspondingly. Similarly, with 1000 nodes, the EMTA-SRSP method has obtained a maximum PDROP of 42 p/s whereas the PSO and TDRS-WSN-DL approaches have attained minimal PDROP of 92 and 63 p/s correspondingly. Also, with 1500 nodes, the EMTA-SRSP approach has achieved a maximal PDROP of 47 p/s whereas the PSO and TDRS-WSN-DL approaches have attained minimal PDROP of 103 and 71 p/s correspondingly. At last, with 2000 nodes, the EMTA-SRSP model has obtained a maximum PDROP of 54 p/s whereas the PSO and TDRS-WSN-DL models have gained minimal PDROP of 109 and 78 p/s correspondingly.

In Table 4 and Fig. 6, a comprehensive Energy Consumption (ECOM) examination of the EMTA-SRSP method with recent models takes place. The results ensured that the EMTA-SRSP model had shown higher ECOM values under each node. For example, with 500 nodes, the EMTA-SRSP model has achieved a maximal ECOM of 0.28j while the PSO and TDRS-WSN-DL techniques have attained minimal ECOM of 1.59 and 0.65j respectively. Similarly, with 1000 nodes, the EMTA-SRSP model has gained a maximal ECOM of 0.73j whereas the PSO and TDRS-WSN-DL models have attained minimal ECOM of 3.26 and 1.79j correspondingly. Also, with 1500 nodes, the EMTA-SRSP methodology has gained a maximum

ECOM of 1.30j whereas the PSO and TDRS-WSN-DL algorithms have attained minimal ECOM of 5.47 and 2.65j correspondingly. Finally, with 2000 nodes, the EMTA-SRSP model has gained a maximum ECOM of 2.04j whereas the PSO and TDRS-WSN-DL models have attained minimal ECOM of 7.84 and 3.75j correspondingly.

Table 3: Packet drop analysis of EMTA-SRSP approach with distinct nodes

Packet drop (p/s)			
No. of nodes	PSO	TDRS-WSN-DL	EMTA-SRSP
500	86	56	40
1000	92	63	42
1500	103	71	47
2000	109	78	54
2500	117	84	59
3000	124	91	59

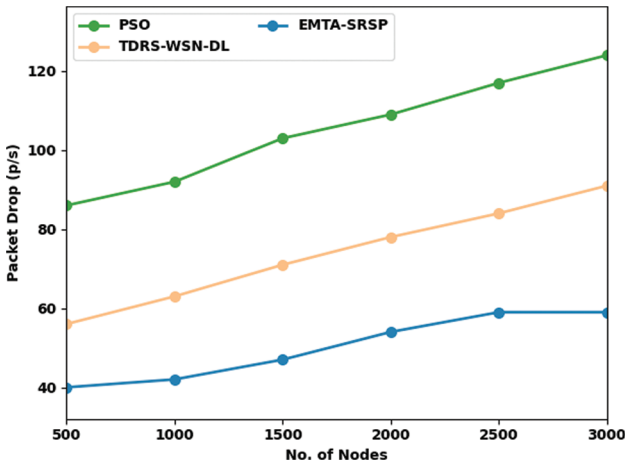

Figure 5: Packet drop analysis of EMTA-SRSP approach with distinct nodes

Table 4: Energy consumption analysis of EMTA-SRSP approach with distinct nodes

Energy consumption (j)			
No. of nodes	PSO	TDRS-WSN-DL	EMTA-SRSP
500	1.59	0.65	0.28
1000	3.26	1.79	0.73
1500	5.47	2.65	1.30
2000	7.84	3.75	2.04
2500	9.06	4.65	2.24
3000	11.47	5.59	3.18

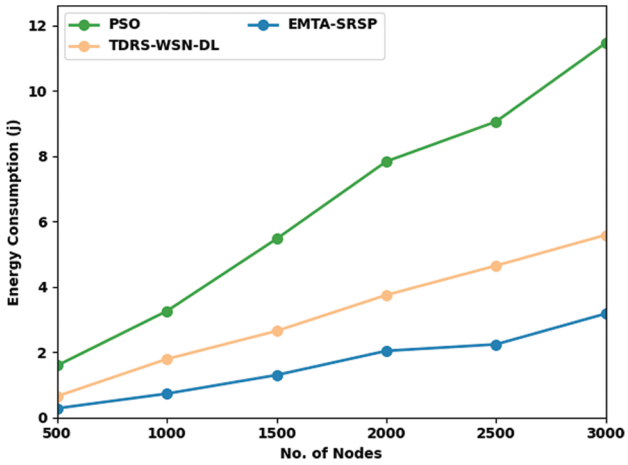

Figure 6: ECOM analysis of EMTA-SRSP approach with distinct nodes

In Table 5 and Fig. 7, a wide-ranging Latency (LAT) analysis of the EMTA-SRSP algorithm with recent models occurs. The results assured the EMTA-SRSP model had shown higher LAT values under all nodes. For example, with 500 nodes, the EMTA-SRSP model has gained maximum LAT of 0.216 bps whereas the PSO and TDRS-WSN-DL models have attained minimal LAT of 0.599 and 0.288 bps correspondingly. Likewise, with 1000 nodes, the EMTA-SRSP model has gained maximum LAT of 0.243 bps, whereas the PSO and TDRS-WSN-DL models have attained minimal LAT of 0.609 and 0.366 bps, respectively. Besides, with 1500 nodes, the EMTA-SRSP approach has acquired maximal LAT of 0.274 bps whereas the PSO and TDRS-WSN-DL models have gained minimal LAT of 0.644 and 0.418 bps correspondingly. Finally, with 2000 nodes, the EMTA-SRSP model has achieved a maximum LAT of 0.315 bps whereas the PSO and TDRS-WSN-DL models have obtained minimal LAT of 0.661 and 0.496 bps, correspondingly.

Table 5: Latency analysis of EMTA-SRSP approach with distinct nodes

Latency (bps)			
No. of nodes	PSO	TDRS-WSN-DL	EMTA-SRSP
500	0.599	0.288	0.216
1000	0.609	0.366	0.243
1500	0.644	0.418	0.274
2000	0.661	0.496	0.315
2500	0.712	0.503	0.349
3000	0.787	0.599	0.421

In Table 6 and Fig. 8, a widespread Throughput (THROU) investigation of the EMTA-SRSP model with recent models occurs. The results implicit in the EMTA-SRSP algorithm have shown higher THROU values under each node. For example, with 500 nodes, the EMTA-SRSP model has achieved a maximal THROU of 1514 bps whereas the PSO and TDRS-WSN-DL models have gained minimal THROU of 954 and 1265 bps correspondingly. Likewise, with 1000 nodes, the EMTA-SRSP approach has acquired a maximum THROU of 1711 bps whereas the PSO and TDRS-WSN-DL algorithms have reached a minimal PDR of 1141 and 1141 bps correspondingly. Moreover, with 1500 nodes, the EMTA-SRSP technique has achieved maximal

THROU of 1898 bps while the PSO and TDRS-WSN-DL models have attained minimal THROU of 1317 and 1638 bps correspondingly. At last, with 2000 nodes, the EMTA-SRSP approach has reached a maximum THROU of 2053 bps whereas the PSO and TDRS-WSN-DL techniques have attained minimal THROU of 1493 and 1804 bps correspondingly.

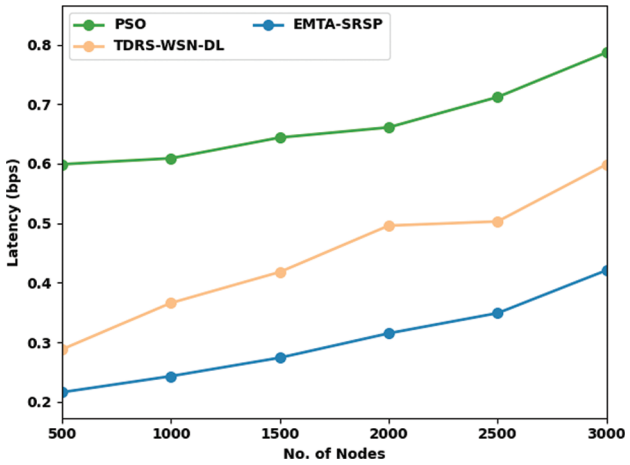

Figure 7: Latency analysis of EMTA-SRSP approach with distinct nodes

Table 6: Throughput analysis of EMTA-SRSP approach with distinct nodes

Throughput (bps)			
No. of nodes	PSO	TDRS-WSN-DL	EMTA-SRSP
500	954	1265	1514
1000	1141	1441	1711
1500	1317	1638	1898
2000	1493	1804	2053
2500	1742	1939	2146
3000	1908	2105	2374

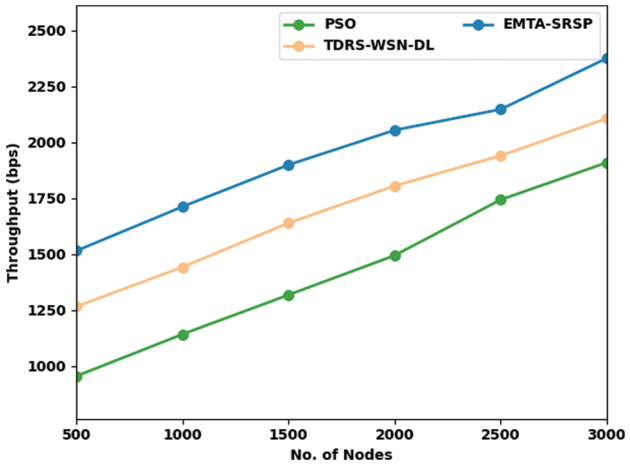

Figure 8: Throughput analysis of EMTA-SRSP approach with distinct nodes

In Table 7 and Fig. 9, a comprehensive Cluster Overhead (COH) inquiry of the EMTA-SRSP model with recent models take place. The results denoted the EMTA-SRSP methodology has shown higher COH values under each node. For example, with 500 nodes, the EMTA-SRSP method has reached a maximum COH of 790 p/s whereas the PSO and TDRS-WSN-DL models have attained minimal COH of 1170 and 980 p/s correspondingly.

Table 7: COH analysis of EMTA-SRSP approach with distinct nodes

Cluster overhead (p/s)			
No. of nodes	PSO	TDRS-WSN-DL	EMTA-SRSP
500	1170	980	790
1000	1402	1244	928
1500	1729	1444	1065
2000	1919	1634	1286
2500	2172	1909	1371
3000	2383	2130	1645

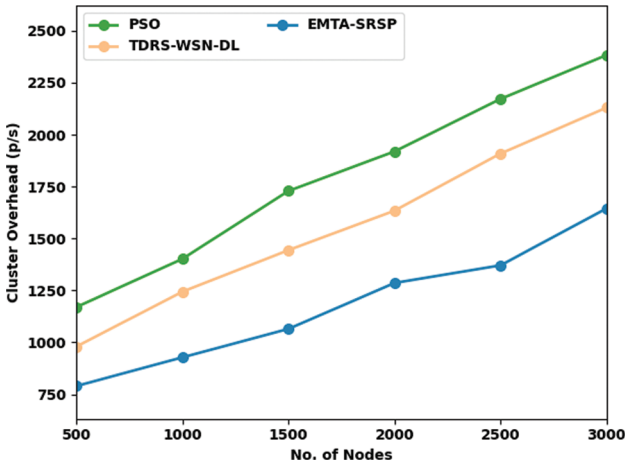

Figure 9: COH analysis of EMTA-SRSP approach with distinct nodes

Similarly, with 1000 nodes, the EMTA-SRSP approach has obtained a maximum COH of 928 p/s whereas the PSO and TDRS-WSN-DL models have attained minimal COH of 1402 and 1244 p/s correspondingly. Also, with 1500 nodes, the EMTA-SRSP algorithm has obtained maximal COH of 1065 p/s whereas the PSO and TDRS-WSN-DL approaches have attained minimal COH of 1729 and 1444 p/s correspondingly. At last, with 2000 nodes, the EMTA-SRSP model has gained a maximum COH of 1286 p/s whereas the PSO and TDRS-WSN-DL models have attained minimal COH of 1919 and 1634 p/s correspondingly.

5 Conclusion

In this article, a novel EMTA-SRSP technique has been introduced for security in WSN. The presented EMTA-SRSP technique majorly involves the optimal selection of secure routes in WSN. To accomplish this,

the EMTA-SRSP technique involves the design of an oppositional Aquila optimization algorithm to choose secure routes for data communication. For the clustering process, the nodes with maximum residual energy will be considered as CHs. In addition, the OAOA technique gets executed to choose optimal routes, based on objective functions with multiple parameters such as energy, distance, and trust degree. Since the EMTA-SRSP technique considered the trust level of the nodes, the routes with maximum security will be chosen into account. The proposed model can be employed in real-time applications such as environmental monitoring, smart cities, fault diagnosis, etc. The experimental validation of the EMTA-SRSP technique is tested and the results exhibited a better performance of the EMTA-SRSP technique over other approaches. In future, the performances of the EMTA-SRSP method can be enhanced using data aggregation techniques.

Acknowledgement: The authors would like to thank Universiti Sains Malaysia (USM) and the Ministry of Higher Education Malaysia for providing the research grant, Fundamental Research GrantScheme (FRGS-Grant No: FRGS/1/2020/TK0/USM/02/1) that helped to carry out this research.

Funding Statement: This research was supported by the Universiti Sains Malaysia (USM) and the Ministry of Higher Education Malaysia through Fundamental Research GrantScheme (FRGS-Grant No: FRGS/1/2020/TK0/USM/02/1).

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

References

[1] H. Lazrag, A. Chehri, R. Saadane and M. D. Rahmani, "Efficient and secure routing protocol based on blockchain approach for wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 22, pp. e6144, 2021.

[2] J. Yang, S. He, Y. Xu, L. Chen and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, pp. 970, 2019.

[3] S. Awan, N. Javaid, S. Ullah, A. Khan, A. Qamar *et al.,* "Blockchain based secure routing and trust management in wireless sensor networks," *Sensors*, vol. 22, no. 2, pp. 411, 2022.

[4] M. Revanesh and V. Sridhar, "A trusted distributed routing scheme for wireless sensor networks using blockchain and meta-heuristics-based deep learning technique," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, pp. 1–19, 2021.

[5] O. I. Khalaf and G. M. Abdulsahib, "Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2858–2873, 2021.

[6] H. Trabelsi, A. Guermazi and W. Jerbi, "A novel secure routing protocol of generation and management cryptographic keys for wireless sensor networks deployed in internet of things," *International Journal of High Performance*, vol. 16, no. 2/3, pp. 87, 2020.

[7] A. M. Srivastava, P. A. Rotte, A. Jain, and S. Prakash, "Handling data scarcity through data augmentation in training of deep neural networks for 3D data processing," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–16, 2022.

[8] J. Chu, X. Zhao, D. Song, W. Li, S. Zhang *et al.,* "Improved semantic representation learning by multiple clustering for image-based 3D model retrieval," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–20, 2022.

[9] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker *et al.,* "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, pp. 1788, 2019.

[10] R. Bharanidharan, "A novel blockchain approach for improve the performance of network security using polynomial ephemeral blockchain-based secure routing in wireless sensor network," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 12, pp. 5598–5604, 2020.

[11] S. H. Awan, S. Ahmed, A. Nawaz, S. Sulaiman, K. Zaman *et al.,* "BlockChain with IoT, an emergent routing scheme for smart agriculture," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, pp. 420–429, 2020.

[12] A. E. G. Sanchez, E. A. R. Araiza, J. L. G. Cordoba, M. T. Ayala and A. Takacs, "Blockchain mechanism and symmetric encryption in a wireless sensor network," *Sensors*, vol. 20, no. 10, pp. 2798, 2020.

[13] M. H. Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar and G. Nagalalli, "Trust aware localized routing and class-based dynamic blockchain encryption scheme for improved security in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 5287–5295, 2021.

[14] S. Amjad, S. Abbas, Z. Abubaker, M. Alsharif, A. Jahid *et al.,* "Blockchain-based authentication and cluster head selection using ddr-leach in internet of sensor things," *Sensors*, vol. 22, no. 5, pp. 1972, 2022.

[15] A. S. Kumar, S. G. Winster and R. Ramesh, "Efficient sensitivity orient blockchain encryption for improved data security in cloud," *Concurrent Engineering*, vol. 29, no. 3, pp. 249–257, 2021.

[16] M. Elhoseny, K. Haseeb, A. A. Shah, I. Ahmad, Z. Jan *et al.,* "IoT solution for ai-enabled privacy-preserving with big data transferring: An application for healthcare using blockchain," *Energies*, vol. 14, no. 17, pp. 5364, 2021.

[17] N. Mittal and U. Singh, "Distance-based residual energy-efficient stable election protocol for WSNs," *Arabian Journal for Science and Engineering*, vol. 40, no. 6, pp. 1637–1646, 2015.

[18] S. Wang, H. Jia, L. Abualigah, Q. Liu and R. Zheng, "An improved hybrid aquila optimizer and harris hawks algorithm for solving industrial engineering optimization problems," *Processes*, vol. 9, no. 9, pp. 1551, 2021.

[19] M. F. Ahmad, N. A. M. Isa, W. H. Lim and K. M. Ang, "Differential evolution with modified initialization scheme using chaotic oppositional based learning strategy," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 11835–11858, 2022.

[20] J. Duan, D. Yang, H. Zhu, S. Zhang and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, pp. 209436, 2014.