Received: April 29, 2023. Revised: June 13, 2023.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

TCRP: Trust-aware Clustering and Routing Protocol based on Atom Search Optimization for WSNs

Venkatesh Prasad Bannikuppe Srinivasiah[1]* Roopashree Hejjaji Ranganathasharma[2] Venkatesh Ramanna[3]

[1]*Department of Computer Science and Engineering, Government Engineering College, Mandya, India*
[2]*Department of Computer Science and Engineering, GSSS Institute of Engineering & Technology for Women, Mysuru, India*
[3]*Department of Computer Science and Engineering, University of Visvesvaraya College of Engineering, Bangalore, India*
* Corresponding author's Email: venkyp25@gmail.com

Abstract: Wireless sensor network (WSN) is one of the fast-growing technology which can be implemented in large-scale applications due to their low-cost installation setup. But, the poor structural organization of the nodes present in WSN leads to various types of security threats and affects the overall performance. The ultimate goal of this paper is to provide a secured transmission of data with minimal consumption of energy. Here, a trust-aware clustering and routing protocol based on atom search optimization (TCRP) is proposed to select secured cluster heads (CHs) for large-scale WSNs and ensure the data's freshness. In addition, the secured path for routing is created with node authentication, where the fitness parameter for a node is defined in terms of distance, trust, and energy. The proposed secured clustering and routing protocol based on Atom Search Optimization (ASO) provides resistance against malicious nodes on the selected routing path, with minimum energy consumption, the proposed TCRP identify an optimal path and it ensures the data integrity and confidentiality of the network. The proposed TCRP protocol is analyzed in terms of energy consumption, throughput, and packet delivery ratio. The proposed TCRP achieved better network throughput of 99% for 80 nodes which are comparatively higher than the existing services aware energy-efficient routing protocol (SQEER) with 98% and probabilistic fuzzy chain set, An authentication-based routing protocol, And a hybrid clustering algorithm PFCD-ARP-CH with (98.5%), trust-aware and energy-efficient data gathering (TEDG) with (97%) and multiobjective-trust centric reptile search algorithm with (96.25%).

Keywords: Distance, Energy, Trust aware clustering, Trust based atom search optimization, Wireless sensor network.

1. Introduction

Wireless networks (WSNs) play an important role in communicating between objects and enabling the connection of multiple networks to the internet [1]. WSNs refer to the collection of wireless sensors to deliver the sensed information to the system and report them to a centralized base station [2]. Once sensor nodes are initiated from the system, they communicate with the base station in the multi-hop network through the forwarding node called cluster head [3]. Therefore, a suitable energy-aware routing protocol was required to balance the traffic load to conserve the hotspot nodes for enhancing the maximum lifetime coverage of WSNs [4, 5]. In the network, to reduce energy utilization, the river sensor network and WSNs are applied with limited bandwidth and physical security of the system. Additionally, it is subjected to various types of limits compared to wired networks, such as restricted communication distance, limited network communication bandwidth, and limited power resources [6, 7].

As mentioned, the secure-aware routing protocol design is a significant and critical problem in WSNs due to the attackers of the network. Therefore, developing a secure routing protocol is necessary to

effectively communicate the nodes to the network [8, 9]. Load balancing and reliable data transfer factors are used to improve the energy efficiency in the WSNs based on three classes: event reliability, packet reliability, and packet-event reliability [10, 11]. The two important techniques were used to improve the security data transmission first, using firewall and intrusion detection methods to determine the attackers in the path, and the second, trust-based routing protocol by performing the authentication using keys [12, 13]. This technique obtains key generation, encryption, decryption, and key distribution to improve security [14, 15]. Hence the novel trust model-based routing protocol achieves key-based authentication and calculates the node trust, network trust, and path trust to increase the security of the communication in the system.

The significant contribution of this research is as follows:

1. The secure routing path (TCRP) is developed using the ASO based on trust, distance, and energy, ensuring data integrity and confidentiality.
2. The life expectancy of the WSN is improved by designing the energy and trust-based routing protocol (TCRP) using ASO.
3. Secure and energy-aware routing is accomplished for consistent communication and reduces the node's energy consumption while broadcasting the data.

The remaining sections of this research paper are organized as follows: section 2 describes the related works and the creation of the ASO-based routing path was fully discussed in section 3. In section 4, the TCRP results are listed. The conclusion of this research is given in section 5.

2. Literature survey

This section includes a review of the literature on the various protocols utilized in the authentication-based secure routing protocol. Thangaramya Kalidoss [16] provided an optimum routing strategy for boosting security and energy consumption by using the quality of services aware energy-efficient routing protocol (SQEER). With the key-based security mechanism, the authentication technique was used to produce an effective trust score. In particular, cluster-based secure routing strategies were presented to select the appropriate cluster head depending on the final path chosen to execute the secure routing procedure. However, the system achieved latency and energy consumption, and it requires restricted bandwidth to the network. Khalid Haseeb [17] introduced a constraint-based system that uses a lightweight secure, and energy-efficient fog-based routing protocol to minimize data latency and improve energy consumption. It successfully implemented QoS features and time-based applications with network edge. Furthermore, it is built on two-level cryptographic primitives for securing real-time data, namely the lightweight data confidentiality technique and the high-performance asymmetric encryption method used between the fog and cloud levels. As a result, the approach improves cluster exploitation and local solution. However, it results in excessive network latency and power use.

Lulwah M. Alkwai [18] introduced a probabilistic fuzzy chain set, authentication based routing protocol and hybrid clustering (PFCS-ARP-HC) algorithm. Using probability calculations, this system used a fuzzy-based chain rule set to successfully minimize vampire assaults. As a result, the protocol substantially improves network security while optimizing system energy consumption. As a result, the approaches performed effectively, with exceptional stability and minimal computational cost, despite having a high processing time and packet loss ratio.

Irin Loretta [19] suggested an optimum privacy multi-hop dynamic clustering routing algorithm based on cryptography to improve data security and energy efficiency in heterogeneous systems. Furthermore, elliptic curve integrated encryption key provisioning methods were used for the verification phase, successfully preventing assaults in sensor networks. The energy-aware routing protocol was created to guarantee dependable data transport while using as little energy as possible. Thus, the protocol provides the most data privacy with the lowest computational cost, however it has a longer processing time and a high packet loss percentage.

In the current diffusion difficulties, Xinying Yu [20] proposed an energy trust-based routing protocol to ensure data privacy and alleviate the unreliability of relay nodes. Furthermore, to offer the optimum communication way and send secret data packets, the trust-based secure directional diffusion routing protocol was designed. The routing protocol utilized in the proposed method helped in attaining end-to-end connections with high trust values. However, the connections with low trust values create an impact on nodes and made them death nodes which affect the overall performance.

Venkatesh [21] A two-hop geographic opportunistic routing (THGOR) protocol that selects a subset of 2-hop neighbors with the highest packet reception ratio and residual energy as the next forwarder node, as well as 1-hop neighbors with

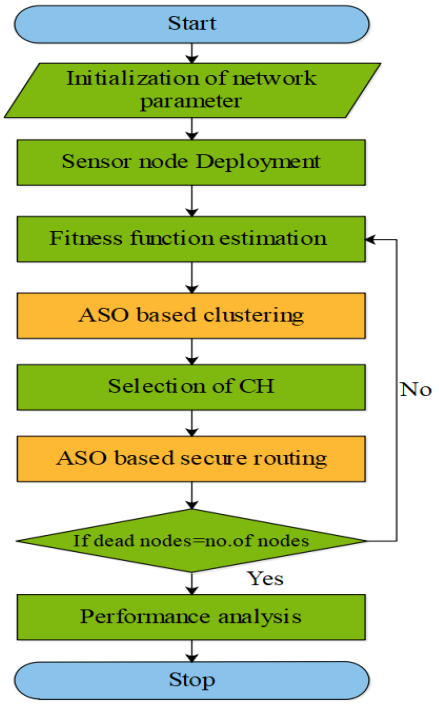

Figure. 1 Flow diagram of the proposed TCRP

outstanding 2-hop neighbor coverage as relay nodes [21]. Deepika [22] Grey wolf optimizer-based clustering scheme for WSN (GWO-C) necessitated some modifications to the original GWO. The proposed formulation's optimal solution takes into account mean intra-cluster distance, sink proximity, remaining energy and the CH balancing factor.

Keiwan Soltani [23] have introduced a trust-aware and energy-efficient data gathering (TEDG) algorithm to collect data in an effective manner. The TEDG is comprised with three stages such as clustering, construction of tree and selection of watch dog. The three stages were considered as the optimization problem and solution was obtained using particle swarm optimization (PSO). The TEDG enhance the convergence speed at the time constructing tree and minimize the time complexity. However, intended issues such as node buffer overflow and collision occurs during the time of transmitting high range of packets.

Seresane Venkata Krishna Reddy and Jayanthi Keshava Murthy [24] have introduced the multiobjective-trust centric reptile search algorithm (M-TCRSA) to perform secured cluster based routing in WSN. The M-TCRSA utilized in selecting the secured cluster heads and secure path to provide reliable transmission in WSN. The routing performed using M-TCRSA consumes minimal energy with extended network lifespan. However, the usage of RSA leads to low diversity in the population and diminish the search ability.

3. Proposed methodology for TCRP

TCRP is an improved trust-based routing that is being developed to increase the data delivery and the life span of WSN. The three key steps in this TCRP approach are ASO-based clustering, cluster head selection, and secure data routing. The node is first arranged randomly in the network area with the same energy and the flowchart for TCRP is represented in Fig. 1.

3.1 Deployment of sensors

The sensor nodes are first distributed among the network in a random manner. The cluster heads (CHs) are then picked from the regular nodes using ASO, and clusters are constructed in the system. Following that, routing was performed to improve data transfer and network security. Effective routing helps to maintain the network data by restoring the hostile nodes.

3.2 Use ASO to find secured CH(SCH)

Secure cluster heads are chosen in this phase to increase the security and energy consumption of the network-based trust value. An authentication-based routing protocol is used to determine if the sink is ready to accept or deliver the data packet from the source and to allow secure route finding. The SCH selection is used to prevent communicating with malicious nodes.

3.2.1. Representation and initialization

In this stage, the candidate solutions are known as atoms, which signify group of CHs that must be selected as CH from the standard sensors. Each atom denotes a possible solution, which indicates which candidate sensors may be chosen as CHs. The number of CHs equals the dimension of atoms. Each atom location is initialized with the ID of a random node between 1 and N, where N is the total number of sensors in the network. The ith atom of the ASO is shown in Eq. (1).

$$x_i = (x_{i,1}, x_{i,2}, .., x_{i,NCH}) \quad (1)$$

where, the location of the widow is $x_{i,d}$, $1 \leq d \leq NCH$ specifies candidate sensors among the total sensors.

3.2.2. Iterative process of CH selection

To avoid the selection of a malicious node as a CH, it is critical to choose a trustworthy and effective CH. It is necessary to authenticate the nodes to

discover the malicious nodes in the path and assure the secure route path in the communication. The remaining processes in the ASO atoms are atom acceleration, depth function, and min-max function. ASO is a population-based global optimization technique inspired by the network's molecular dynamics. The following examples, based on Newton's second law, mathematically show the link between the atomic systems. F_i represents the iteration's force, while G_i reflects the restrictions action of atom i.

$$a_i = \frac{F_i + G_i}{m_i} \tag{2}$$

Where a_i denotes the acceleration of atom i and m_i represents the mass of the atom. The following equation shows the interaction force in d dimensional and t time. Eq. (3) helps atoms to converge to a specific point.

$$F'_{ij}(t) = -\eta(t)\left[2(h_{ij}(t))^{13} - (h_{ij}(t))^{7}\right] \tag{3}$$

Based on the above expression, $\eta(t)$ is defined for the depth function which is represented in Eq. (4).

$$\eta(t) = \alpha\left(1 - \frac{t-1}{T}\right)^3 e^{\frac{-20t}{T}} \tag{4}$$

Where α and T denote the depth weight and the maximum number of iterations. Attracting regions and adjusting repulsion using the latter function $h_{ij}(t)$ which represents an Eq. (5)

$$h_{ij}(t) = \begin{cases} h_{min} & \frac{r_{ij}(t)}{\sigma(t)} < h_{min} \\ \frac{r_{ij}(t)}{\sigma(t)} & h_{min} \le \frac{r_{ij}(t)}{\sigma(t)} \le h_{max} \\ h_{max} & \frac{r_{ij}(t)}{\sigma(t)} > h_{max} \end{cases} \tag{5}$$

Where the distance between two atoms is signified by r while, h_{min} and h_{max} represents the lower and upper bounds of the system. The terms of g_0 and u express the drift factors of the min-max function are represented in Eq. (6).

$$h_{min} = g_0 + g(t) \text{and } h_{max} = u \tag{6}$$

Based the Eq. (6) the length scale is signified by $\sigma(t)$ and given as Eq. (7).

$$\sigma(t) = ||x_{ij}(t), \frac{\Sigma_{j \in Kbest,} x_{ij}(t)}{K(t)}||_2 \tag{7}$$

Where the best among the population of K atom is denoted as $Kbest$. The total force acting on an atom i with dimensional d^{th} are represented in Eq. (8).

$$F_i^d(t) = \Sigma_{j \in Kbest,} rand_j F_{ij}^d(t) \tag{8}$$

Where the $rand_j$ is the demonstration for a random number ranging among [0,1]. Atomic motion, which is simplified in ASO by assuming a covalent link between the best and the other, is significantly affected by the geometric constraint atoms. This can be written as Eq. (9) for atom i.

$$\theta_i(t) = \left[|x_i(t) - x_{best}(t)|^2 - (b_{i,best})^2\right] \tag{9}$$

Where the best atom position is represented by $x_{best}(t)$ and the fixed length among the i^{th} and the best atoms are defined by $b_{i,best}$. The Eq. (10) the constraints force of the atoms i represents as;

$$G_i^d(t) = \lambda(t)(x_{best}^d(t) - x_i^d(t)) \tag{10}$$

Where $\lambda(t)$ denotes the lagrangian multiplier and defined as follows Eq. (11)

$$\lambda(t) = \beta e^{\frac{-20t}{T}} \tag{11}$$

Where in the above Eq. (11), β represents the multiplier weight and the acceleration time t of the atom i of $a_i^d(t)$ is given as Eq. (12)

$$a_i^d(t) = \frac{F_i^d(t)}{m_i^d(t)} + \frac{G_i^d(t)}{m_i^d(t)} \tag{12}$$

The latter expression briefly explains how an atom with achieves more mass can obtain a higher fitness value by reducing its acceleration. The following Eq. (13) and Eq. (14) are used to compile the i^{th} atom mass.

$$a_i^d(t) = \frac{M_i(t)}{\Sigma_{j=1}^N M_j(t)} \tag{13}$$

$$M_i(t) = e^{-\frac{Fit_i(t) - Fit_{best}(t)}{Fit_{worst}(t) - Fit_{best}(t)}} \tag{14}$$

Where the atoms with the best and worst fitness function at a time t is denoted as $Fit_{best}(t)$ and $Fit_{worst}(t)$. The $Fit_i(t)$ is the representation of the fitness value of the function for an atom i at iteration t which is defined in Eq. (15) and Eq. (16) as

$$Fit_{best}(t) = min_{i\in(1,2,\dots N)} Fit_i(t) \quad (15)$$

$$Fit_{worst}(t) = max_{i\in(1,2,\dots N)} Fit_i(t) \quad (16)$$

The probability of interactions with the K neighbors of each atom has higher fitness values which are needed for exploration improvement, however, this should be less for exploitation. Here k is a time-dependent function which is calculated as following Eq. (17)

$$k(t) = N - (N-2) \times \sqrt{\frac{t}{T}} \quad (17)$$

3.3 Derivation of fitness to choose the CH

It is essential to elect a trustworthy and effective CH to prevent the choice of a malicious node as CHs. Therefore, authentication is used to select the secure path for data distribution and address the malicious nodes in the path. The selection of the best CHs was depending on the weight of the nodes. This weight is calculated using various metrics, including time, trust, and energy.

3.3.1. Distance

It is the best one to choose the node that is located in the middle of the cluster. The distance between nodes x and the center o along with the location (x_a, x_b) and (o_a, o_b) is compiled using Eq. (18)

$$d(x,o) = \sqrt{(x_a - o_a)^2 + (x_b - o_b)^2} \quad (18)$$

The sensor with the best chance of becoming CH is the one closest positioned to the cluster center of the system.

3.3.2. Trust

The trust value of a node i is determined as the total weighted value of direct and indirect trust of the node i as specified in the Eq. (19).

$$T_i = W_1 DT_i + W_2 IT_i \quad (19)$$

The weights for these values are W_1 and W_2, and DT_i and IT_i in the equation represent the direct and indirect trust values, respectively. In addition, the impact of these trusts can also provide effective figures on decision-making by applying different values to W_1 and W_2. A node that relies on advice provided by a neighbor node to other nodes is known as indirect trust and is calculated as Eq. (20).

$$IT_i = \frac{\sum_{j=1}^{n} T_j^i * T_j}{n} \quad (20)$$

Here, T_j^i describe the advice trust of the node j on the node i and T_j is the trust rate of the trust of node j. Direct trust is defined as Eq. (21)

$$DT_i = m_1 * \frac{n_{correct_i}}{n_{total_i}} + m_2 * re_i \quad (21)$$

Where, $n_{correct_i}$ is the amount of data packet sent and n_{total_i} is the amount of data packets sent by the node i. The endure energy of the node i is re_i along with trust weight m_2. This trust value is used to effectively identify malicious attackers in the WSNs. The node authentication is need to be performed for a secured routing and verify whether the node is attacked by the malicious node. The attacker's node claimed that it has a lot of energy for absorbing the data packets and reporting to the neighbor node so the node was chosen as the best node for sending their packet to the destination.

3.3.3. Energy

Each sensor node along with the maximum residual energy level is selected as CHs on the network. According to Eq. (22), each sensor evaluates its energy weights. After the process of integrating the ID with their weights, the sensors transmit messages regarding voting to the neighboring nodes. Then a message signal is transmitted by the sensor nodes with the highest weight. Before the expression of CHs, each sensor node waits for a time t which denotes the competition periods. To prevent more energy utilization, the competition period should not be too short or long.

$$EN_{rd} = EN_{int} - EN_{con} \quad (22)$$

At the initial stage, the Hello packets are transmitted to the nearby neighboring nodes when the value for the data is generated. Whenever the weight value of the node gets lower, it waits to receive the invite packets which consider CH. If the node does not receive any invite message within the period, then it states itself as CHs.

3.4 Cluster formation

The normal sensors are assigned to the selected CHs in the cluster creation phase. Here, the cluster is created according to the residual energy and distance

Table 1. Simulation parameter

Parameters	Value
Area	$200m \times 200m$
Nodes	100
$E_{elec\ value}$	50J per bit
ε_{fs}_value	10 J per bit per m2
E_{mp_value}	0.0013 J per bit per m4
Size of the packets	4000 bits
Initial energy	0.5 J

whereas the potential function is used in creating the cluster which is expressed in the Eq. (23).

$$Potential\ of\ sensor\ (N_i) = \frac{E_{CH}}{dis(N_i,CH)} \quad (23)$$

The formulated potential function is utilized in assigning the normal sensor node to CH with the minimal transmission of data with high residual energy.

3.5 TCRP algorithm:

The cluster head selection is performed using TCRP which is represented as follows:

Initialize the set of atoms X, velocity V and $Fit_{Fit_i best} = \text{Inf}$

While the stop criterion is not satisfied do

For each atom X_i do

Calculate the fitness value Fit_i;

If $Fit_i < Fit_{best}$ then

$Fit_i = Fit_{best}$;

$X_{Best} = X_i$;

End If.

Calculate mass using Eq. (13) and Eq. (14)

Determine its K neighbors using Eq. (17)

Calculate the interaction force F_i and constraint force G_i using Eq. (8) and Eq. (10) respectively.

Calculate the acceleration using Eq. (12)

Update the velocity and position

End for

End while.

Output: CH from the network (an optimal solution)

3.5 Secured optimal routing path using ASO

TCRP has the additional responsibility of generating the routing path. Furthermore, to efficiently detect the malicious node in the routing path and transmit the data, a secure way is necessary to verify the route, which improves network routing security. For optimizing the creation of the transmission route, three optimum fitness functions were used: trust, distance, and energy.

The following steps are performed at this routing stage:

1. First, the atoms are initialized with the feasible route from the source CHs to BS, and the dimensionality of each atom equals the number of intermediate nodes in the path.
2. The acceleration of atoms, depth function, and min-max function are then simulated based on the fitness of each route. The depth and min-max functions were previously discussed in the preceding section.
3. The fitness factors examined during transmission route generation include residual energy, distance and trust between CH and BS, and node degree. The fitness employed in the ASO-based route creation is shown in Eqs. (18-22).

This aids in identifying the route with the most residual energy, shortest transmission distance, and highest security. Furthermore, it would improve data integrity and confidentiality in this work by ensuring that the destination node does not change the data during network connection between nodes. As a result, node energy consumption is minimized, and trust-based thresholding values are used to eliminate hostile nodes in selected route paths by employing this TCRP based routing, which was utilized in enhancing the lifespan of the network.

4. Results and discussion

This section explains the TCRP's findings and debate. MATLAB R2020a is used to design and execute reliable transmission. The analytical system is powered by an i5 CPU with 8GB of RAM. The primary goal of the proposed approach is to enhance security and minimize the consumption of energy in WSNs. The simulation parameters of the TCRP are listed in Table 1.

4.1 Performance analysis

The TCRP's performance is measured using energy consumption, throughput, and packet delivery ratio. The performance of the proposed TCRP is evaluated with existing approaches such as SQEER [16], PFCS-ARP-HC [18], TEDG [23] and M-TCRSA [24]. The existing methodologies such as TEDG and M-TCRSA are implemented with the same simulation parameter in table 1 to evaluate the efficiency of TCRP.

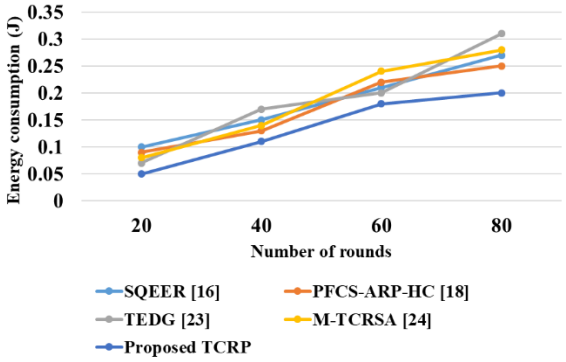

Figure. 2 Comparison of energy consumption of TCRP

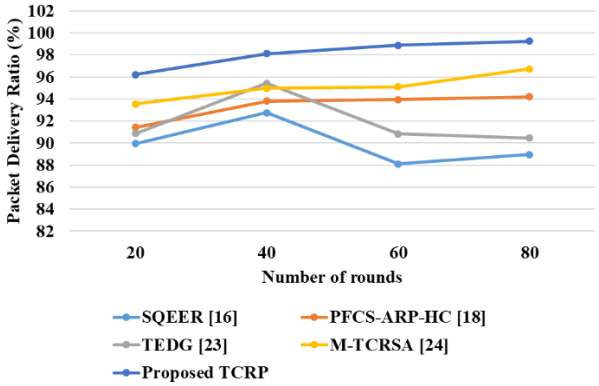

Figure. 3 Comparison of packet delivery ratio of TCRP

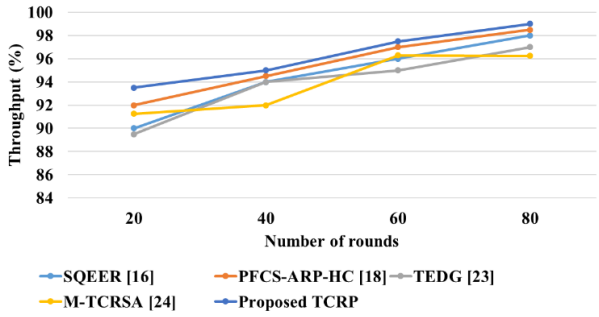

Figure. 4 Comparison of throughput of TCRP

4.1.1. Consumption of energy

A network's energy consumption is represented as the quantity of energy required to receive and send the data. Fig. 2 shows a comparison of energy consumption between the TCRP and existing approaches such as SQEER, PFCS-ARO-HC, TEDG and M-TCRSA. According to Fig. 2, the TCRP consumes less energy than the existing approaches. For example, when the number of rounds is 80, the proposed approach consumes energy of 0.2J whereas the existing SQEER, PFCS-ARO-HC, TEDG and M-TCRSA had consumed 0.27J, 0.25J, 0.31J and 0.28J respectively. The better result of TCRP is due to its improved energy efficiency via the use of a trust to minimize rogue nodes and the establishment of the shortest route.

4.1.2. Throughput

The number of packets received successfully at the sink is referred to as throughput, which is measured in bits per second. Fig. 3 shows a comparison between TCRP and the existing approaches. The throughput of the proposed approach is 93.5% for 80 rounds whereas the existing SQEER, PFCS-ARO-HC, TEDG and M-TCRSA had obtained throughput of 98%, 98.5%, 97% and 96.25% respectively. The better throughput is due to the secure data transfer of the proposed TCRP with minimal node/link failure when broadcasting data packets.

4.1.3. Packet delivery ratio

Packet delivery ratio is defined as the ratio of the number of data packets lost to the total number of data packets sent. The packet delivery ratio reflects the efficiency of proposed system. It utilized to improve the performance of algorithm. Fig. 4 compares the performance of the TCRP with existing approaches in terms of packet delivery. This scenario's simulation experiment employs 80 nodes. The PDR of the proposed TCRP is 94.21% whereas the PDR of existing SQEER, PFCS-ARO-HC, TEDG and M-TCRSA is 88.95%, 94.21 %,90.45% and 93% respectively. The better result is due to the selection of optimal CHs which perform an effective search to find the path to deliver the packets.

4.2 Comparative analysis

This section provides a comparative examination of the TCRP with prior studies. The previous study SQEER [16], PFCS-ARP-HC [18], TEDG [23] and M-TCRSA [24] are utilized to assess the TCRP's efficiency. Table 2 shows a comparison of the SQEER [16], PFCS-ARP-HC [18], TEDG [23] and M-TCRSA [24]. According to Table 2, the TCRP outperforms the existing approaches due to its effective balance between the exploration and exploitation phases. The derived phase is utilized to ensure safe and energy-conscious data transmission across large-scale WSNs and has promise for optimization challenges.

5 Conclusion

In this research, trust-aware clustering and routing protocol (TCRP) based on Atom Search Optimization was proposed to select secured cluster

Table 2. Comparative analysis of TCRP method

Performance measure	Method	Number of rounds			
		20	40	60	80
Energy Consumption (Joules)	SQEER [16]	0.1	0.15	0.21	0.27
	PFCS-ARP-HC [18]	0.09	0.13	0.22	0.25
	TEDG [23]	0.07	0.17	0.20	0.31
	M-TCRSA [24]	0.08	0.14	0.24	0.28
	Proposed TCRP	0.05	0.11	0.18	0.2
Packet delivery ratio %	SQEER [16]	89.95	92.76	88.10	88.95
	PFCS-ARP-HC [18]	91.43	93.82	93.95	94.21
	TEDG [23]	90.87	95.43	90.82	90.45
	M-TCRSA [24]	93.54	94.96	95.12	96.74
	Proposed TCRP	96.21	98.11	98.89	99.25
Throughput %	SQEER [16]	90	94	96	98
	PFCS-ARP-HC [18]	92	94.5	97	98.5
	TEDG [23]	89.5	94	95	97
	M-TCRSA [24]	91.25	92	96.30	96.25
	Proposed TCRP	93.5	95	97.5	99

heads (CHs) for large-scale WSNs. It ensured secured transmission among the nodes. The secure routing path was developed using the ASO based on trust, distance, and energy, ensuring data integrity and confidentiality.

The energy depletion of the node and network was reduced by selecting optimum number of CHs, and the proposed ensures the system's data freshness. In addition, the secured path for routing was created with node authentication, where the fitness parameter for a node was defined in terms of distance, trust, and energy. The fitness factors examined during transmission route generation include residual energy, distance and trust between CH and BS, and node degree.

The proposed TCRP protocol was analysed in terms of energy consumption, throughput, and packet delivery ratio. It was determined that the TCRP outperformed the SQEER, PFCS-ARP-HC and TEDG and M-TCRSA methods. The future work will be based on utilizing hybrid optimization techniques to obtain better performance.

Nomenclature

Parameters	Description
N	Total number of sensors in the network
x_i	The atom present in ASO
NCH	Candidate sensors among the total sensors.
F_i	Force of iteration of atom i
G_i	Restriction of atom i
a_i	Acceleration of atom i
m_i	Mass of the atom i
$\eta(t)$	Depth function
α	Depth weight
T	Maximum number of iterations
$h_{ij}(t)$	Repulsion adjusting function
r	Distance between two atoms
h_{min}	Lower bound
h_{max}	Upper bound
u	Drift factor of the min-max function
$\sigma(t)$	Length of the scale
$Kbest$	Best among the population of K atom
$rand_j$	Random number ranges between [0,1]
$x_{best}\ (t)$	Best position of the atom
$b_{i,best}$	Fixed length among the i^{th} and the best atoms
$\lambda(t)$	Langrangian multiplier
β	Weight of the multiplier
$a_i^d(t)$	Acceleration time of the atom
$Fit_{best}(t)$	Best fitness function at time t
$Fit_{worst}(t)$	Worst fitness function at time t
k	Time-dependent function
DT_i	Direct trust
IT_i	Indirect trust
T_j	Trust rate of node j
T_j^i	Advice trust of the node j on the node i
re_i	Endure energy of the node i

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

For this research work all authors' have equally contributed in Conceptualization, methodology, validation, resources, writing—original draft preparation, writing—review and editing.

References

[1] R. K. Lenka, M. Kolhar, H. Mohapatra, F. A. Turjman, and C. Altrjman, "Cluster-based routing protocol with static hub (CRPSH) for WSN-assisted IoT networks", *Sustainability*, Vol. 14, No. 12, p. 7304, 2022.

[2] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, and K. Shankar, "A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing", *Wireless Personal Communications*, Vol. 127, No. 1, pp. 39-62, 2022.

[3] K. Hamouid, S. Othmen, and A. Barkat, "LSTR: lightweight and secure tree-based routing for wireless sensor networks", *Wireless Personal Communications*, Vol. 112, No. 3, pp. 1479-1501, 2020.

[4] K. Haseeb, A. Almogren, K. U. Din, N. Islam, and A. Altameem, "SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things", *Sensors*, Vol. 20, No. 9, p. 2468, 2020.

[5] B. Han, F. Ran, J. Li, L. Yan, H. Shen, and A. Li, "A Novel Adaptive Cluster Based Routing Protocol for Energy-Harvesting Wireless Sensor Networks", *Sensors*, Vol. 22, No. 4, p. 1564, 2022.

[6] J. D. Abdulai, K. S. A. Manu, F. A. Katsriku, and F. Engmann, "A modified distance-based energy-aware (mDBEA) routing protocol in wireless sensor networks (WSNs)", *Journal of Ambient Intelligence and Humanized Computing*, 2022.

[7] K. Haseeb, A. Almogren, I. U. Din, N. Islam, and A. Altameem, "SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things", *Sensors*, Vol. 20, No. 9, p. 2468, 2020.

[8] X. Wang, "Low-Energy Secure Routing Protocol for WSNs Based on Multiobjective Ant Colony Optimization Algorithm", *Journal of Sensors*, Vol. 2021, p. 7633054, 2021.

[9] H. Koyuncu, G. S. Tomar, and D. Sharma, "A new energy efficient multitier deterministic energy-efficient clustering routing protocol for wireless sensor networks", *Symmetry*, Vol. 12, No. 5, p. 837, 2020.

[10] B. D. Deebak, and F. A. Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks", *Ad Hoc Networks*, Vol. 97, p. 102022, 2020.

[11] M. Almazaideh and J. Levendovszky, "Novel reliable and energy-efficient routing protocols for wireless sensor networks", *Journal of Sensor and Actuator Networks*, Vol. 9, No. 1, p. 5, 2020.

[12] G. Natesan, S. Konda, R. P. D. Prado, and M. Wozniak, "A Hybrid Mayfly-Aquila Optimization Algorithm Based Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks", *Sensors*, Vol. 22, No. 17, p. 6405, 2022.

[13] C. C. Vignesh, C. B. Sivaparthipan, J. A. Daniel, G. Jeon, and M. B. Anand, "Adjacent node based energetic association factor routing protocol in wireless sensor networks", *Wireless Personal Communications*, Vol. 119, No. 4, pp. 3255-3270, 2021.

[14] V. Sivasankarareddy, G. Sundari, C. R. Reddy, F. Aymen, and E. C. Bortoni, "Grid-Based Routing Model for Energy Efficient and Secure Data Transmission in WSN for Smart Building Applications", *Applied Sciences*, Vol. 11, No. 22, p. 10517, 2021.

[15] M. E. A. Ibrahim and A. E. S. Ahmed, "Energy-aware intelligent hybrid routing protocol for wireless sensor networks", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 3, p. e6601, 2022.

[16] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks", *Wireless Personal Communications*, Vol. 110, No. 4, pp. 1637-1658, 2020.

[17] K. Haseeb, N. Islam, Y. Javed, and U. Tariq, "A lightweight secure and energy-efficient fog-based routing protocol for constraint sensors network", *Energies*, Vol. 14, No. 1, p. 89, 2020.

[18] L. M. Alkwai, A. N. M. Aledaily, S. Almansour, S. D. Alotaibi, K. Yadav, and V. Lingamuthu, "Vampire attack mitigation and network performance improvement using probabilistic fuzzy chain set with authentication routing protocol and hybrid clustering-based optimization in wireless sensor network", *Mathematical Problems in Engineering*, Vol. 2022, p. 4948190, 2022.

[19] I. G. Loretta and V. Kavitha, "Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment", *Peer-to-Peer Networking and Applications*, Vol. 14, No. 2, pp. 821-836, 2021.

[20] X. Yu, F. Li, T. Li, N. Wu, H. Wang, and H. Zhou, "Trust-based secure directed diffusion routing protocol in WSN", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 13, No. 3, pp. 1405-1417, 2020.

[21] Venkatesh, L. A. Achar, P. Kushal, and K. R. Venugopal, "Geographic opportunistic routing protocol based on two-hop information for wireless sensor networks", *International Journal of Communication Networks and Distributed Systems*, Vol. 23, No. 1, pp. 93-116, 2019.

[22] D. Agarwal, M. H. W. Qureshi, P. Pincha, P. Srivastava, S. Agarwal, V. Tiwari, and S. Pandey, "GWO-C: Grey wolf optimizer-based clustering scheme for WSNs", *International Journal of Communication Systems*, Vol. 33, No. 8, p. e4344, 2020.

[23] K. Soltani, L. Farzinvash, and M. A. Balafar, "Trust-aware and energy-efficient data gathering in wireless sensor networks using PSO", *Soft Computing*, pp. 1-24, 2023.

[24] S. V. K. Reddy and J. K. Murthy, "Secure Cluster based Routing Using Multiobjective Trust Centric Reptile Search Algorithm for WSN", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 2, pp. 526-535, 2023, doi: 10.22266/ijies2023.0430.43.