Received: February 24, 2022. Revised: April 22, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Cluster based Routing Using Improved Moth Flame Optimization for Wireless Sensor Networks

Bharathi Ramachandra[1]* **T. P. Surekha[2]**

[1]*GSSS Institute of Engineering & Technology for Women, Mysuru, India*
[2]*Vidyavardhaka College of Engineering, Mysuru, India*
* Corresponding author's Email: Bharathi.08r@gmail.com

Abstract: Wireless Sensor Network (WSN) is developed as a promising technology for a wide range of applications due to its low installation cost. However, the nodes in the WSN are susceptible to different security threats, because these nodes are located in hostile or harsh environments. The important goal of this paper is to obtain secure data transmission while minimizing energy consumption. In this paper, an Improved Moth Flame Optimization (IMFO) is used for selecting the optimal Cluster Head (CH) from the network. Moreover, the secure routing path is generated using the IMFO where the fitness function considers residual energy, distance, trust and node degree. Therefore, the Secure Clustering and Routing using IMFO (SCRIMFO) provides the resistance against the Distributed Denial-of-Service (DDoS) attack whereas the energy consumption is minimized by identifying the shortest path. The proposed SCRIMFO method is analysed in terms of Average Energy Consumption (AEC), Packet Loss Ratio (PLR), Packet Delivery Ratio (PDR) and routing load. Here, the SCRIMFO method is compared with the Secure Routing Protocol based on Multi-objective Ant-colony-optimization (SRPMA), Ant Colony Conveyance Algorithm (ACCA) and Energy-aware Trust and Opportunity-based Routing (ETOR) approaches. The PDR of the SCRIMFO is 94.64 % for 2 DDoS attacks that is high when compared to the SRPMA, ACCA and ETOR.

Keywords: Cluster head, Distributed denial-of-service attack, Energy consumption, Improved moth flame Optimization, Secure clustering and routing process, Trust, Wireless sensor networks.

1. Introduction

WSN comprises a huge amount of less power multi-functioning sensor nodes with restricted computational and detecting capacities for monitoring the various types of environmental or physical parameters [1]. WSNs are mainly utilized in different applications such as disaster management, security surveillance, medical and health, environments monitoring, industrial automation to collect the data about the respective applications [2]. Sensors in the network have the capacity for collecting and processing the information from the environment as well as the processed information is communicated between the nodes [3]. Specifically, each sensor in the network is used with a sensing unit, power supply, processing and data storage devices, and radio transmission module. But, these modules are designed with large resource restrictions whereas the energy depletion of the sensors is considered as challenging issue in the WSN [4, 5]. Because, the battery of the sensors located in harsh environments can't be replaced, once it is deployed in the WSN [6].

Routing is the method of choosing the most appropriate transmission path over the network [7]. The routing protocol is separated into two types based on the node's deployment. The types of routing protocols are flat routing and hierarchical routing or cluster-based routing protocols [8]. The nodes are gathered into various small groups namely clusters that lead to minimizing the energy by transmitting the information over the CHs. If the CHs or coordinators exist near to the BS, then the respective node directly transmits the data to the BS. Otherwise, the CH transmits the data through the multihop when it is not presented in the communication range of BS [9, 10].

The energy consumption is minimized using cluster-based routing protocols. However, the clusters in the network are susceptible to malicious nodes. These malicious nodes pass the fake message to the CH, which causes the packet drop, high overhead and energy consumption [11-13]. But, the trust based routing method faces challenging concerns i.e., the fundamental of the trust route mainly depends on trust identification. However, the trust identification between the group of nodes is difficult in the network [14, 15].

The contributions of this paper are mentioned as follows:

- The energy consumption of the network is reduced by using the K-means clustering followed by the IMFO is used for selecting secure CHs from the clusters. The conventional Moth Flame Optimization (MFO) considers only the distance during the searching process. However, the proposed IMFO considers four distinct fitness parameters such as residual energy, distance, trust and node degree for enhancing the searching process during the CH selection.
- A secure path between source CH to the Base Station (BS) is discovered by using the IMFO algorithm. Therefore, this secure clustering and routing offer high robustness against DDoS attacks.The security against DDoS attacks is achieved while minimizing the energy consumption of the nodes.

The remaining of the paper is organized as follows: The literature survey about the secure data transfer over the WSN is provided in Section 2. Section 3 provides the detailed description about the SCRIMFO method. The outcomes of the SCRIMFO method is detailed in the Section 4. Finally, the conclusion is made in Section 5.

2. Literature survey

This section describes the existing researches related to secure data transmission over WSN.

Sun [16] SRPMA to improve WSN performances. Here, the node's residual energy and trust value are considered in the ant colony algorithm for generating a routing path. On the other hand, the enhanced D-S evidence method was used to evaluate the trust value. However, the SRPMA was used only the trust and energy in the fitness function which failed to consider the distance in the routing path. Because the path with higher distance caused higher energy consumption.

Kalidoss [17] developed the Secure and QoS aware Energy Efficient Routing (SQEER) to obtain an effective routing over the network. Here, the key based security technique was used in the authentication method of trust modelling to generate the trust value. Accordingly, the trustworthy node was selected from the clusters using the trust score and the selected node was referred to as a CH. Next, the hop count, trust and energy were considered for selecting the data transmission path. However, the routing path generation was failed to consider the distance value which may result in higher energy consumption.

Rathee [18] presented the QoS aware Energy Balancing Secure Routing (QEBSR) with Ant Colony Optimization (ACO) to identify the data transmission path in the network. The enhanced models to calculate the trust factor and End-to-End Delay (EED) were used in the QEBSR. Specifically, the node delay and path delay were considered while computing the EED. The packet loss and generation rate were used to calculate the trust factor of the node. The developed QEBSR was obtained less delay while transmitting the data packets. But, the PDR of the QEBSR was affected, when there was an increment in the compromised nodes.

Basha [19] developed the Realisable Secure Aware Routing (RSAR) protocol for reducing the overhead without affecting the performances of the network. The Conditional Tug of War Optimization (CTWO) was used in the RSAR to calculate the trust value of each node. Next, the energy depletion was reduced based on the cluster based data collection. This RSAR protocol was provided with the trust-based secure system without any control overhead. However, this RSAR protocol was considered only the energy in the fitness function.

Vijayalakshmi, and Senthilkumar [20] presented the Unequal Secure Cluster based Distributed Routing Protocol (USCDRP) to enhance security and energy efficiency. The developed USCDRP has two stages such as clustering and secure data transmission. The CHs in the unequal clustering was selected using the remaining energy of the nodes. In this USCDRP, the routing paths were identified earlier by using the proactive protocol. Therefore, the high energy efficiency was obtained using the cluster maintenance method of USCDRP. However, the selection of CH using the USCDRP doesn't consider appropriate fitness functions, it considered only energy level.

Sasi and Santhosh [21] developed the ACCA to accomplish the secure and energy efficient data transfer over the WSN. The objectives considered in the ACCA was included the residual energy, total time taken for data transfer, distance, and broadcasting and receiving packets. Here, the neighborhood search was extended for

accomplishing search with the appropriate nodes to estimate the distance, residual energy and trust. However, the routing without clustering approach affects the WSN performances in terms of data delivery.

Hajiee [22] presented the ETOR to select adequate route. The main processes included in the ETOR are selection of secure nodes and opportunistic node selection for performing the routing in WSN. Specifically, the usage of multipath routes was leads to improve the energy consumption. However, the PDR of the ETOR was affected because of the malicious nodes exist in the network.

Kantharaju Veerabadrappa [23] and Sowmyashree Malligehalli Shivakumaraswamy [24] developed the secure routing using hybrid optimization and cuckoo search algorithm respectively. Here, the hybrid optimization includes a moth flame and chicken swarm optimization. However, the huge amount of control packets transmitted while performing the route discovery caused higher routing load.

The existing researches has various limitations such as inappropriate fitness function estimation, high energy consumption, less PDR and high routing load. Therefore, the SCRIMFO with a distinct fitness measures such as residual energy, distance, trust and node degree is proposed to achieve secure and reliable data transfer under DDoS attacks.

3. Methodology

In this proposed SCRIMFO method, the IMFO is used to perform the secure cluster based routing for improving the performances of the WSN under the constraints of DDoS attacks. Here, the clustering and secure CH identification are done using the K-means and IMFO algorithms respectively. The fitness values considered in this IMFO are distance, residual energy, trust and node degree. Subsequently, the secure routing between the source to the BS is achieved by using the IMFO with the same fitness values. This secure CH and route identification avoid DDoS attacks for minimizing the packet loss over the WSN. The block diagram of the SCRIMFO method is shown in Fig. 1.

3.1 Clustering using K-means algorithm

In this SCRIMFO method, the K-means algorithm is utilized to cluster the network as k clusters. Here, the network is separated as clusters by using the Euclidian distance in the K-means algorithm (i.e., unsupervised clustering method). Furthermore, this K-means algorithm has resulted in

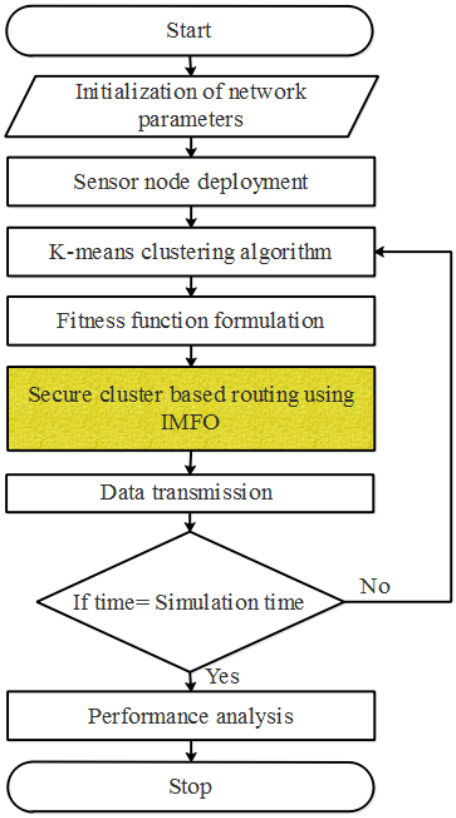

Figure. 1 Block diagram of the SCRIMFO method

less inter-cluster similarity and high intra-cluster similarity. Eq. (1) shows the Euclidian distance used in the clustering process.

$$Dist = \sqrt{\left(x_i - x_j\right)^2 - \left(y_i - y_j\right)^2} \qquad (1)$$

Where, $x_i \& y_i$, and $x_j \& y_j$ are the coordinates of the node i and j.

3.2 Overview of the MFO

MFO is generally a population-based metaheuristic algorithm which is developed by the Mirjalili. At first, MFO randomly creates the moths inside the solution space and fitness values are generated for each moth. Next, an optimal location is tagged by the flame. The function of spiral movement is used to define the location update of the moths. This location update is used to obtain the optimal location labelled by the flame and a new best individual location is updated in the MFO. The same processes such as location update of the moth and new location generation are performed in the MFO.

The processes carried out by the MFO algorithm is mentioned as follows:

3.2.1. Initial location generation of the moth

Eq. (2) is the set of moths generated by the MFO algorithm.

$$M = \begin{bmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,d} \\ m_{2,1} & m_{2,2} & \dots & m_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ m_{n,1} & m_{n,2} & \dots & m_{n,d} \end{bmatrix} \quad (2)$$

Where the amount of moths is represented as n and the dimension of the solution space is represented as d. The moth's fitness values are stored in an array manner as shown in Eq. (3).

$$OM = \begin{bmatrix} OM_1 \\ OM_2 \\ \vdots \\ OM_n \end{bmatrix} \quad (3)$$

The other fundamental of the MFO is flame which is expressed in Eq. (4) and the fitness function for the flame is expressed in the Eq. (5).

$$F = \begin{bmatrix} F_{1,1} & F_{1,2} & \dots & F_{1,d} \\ F_{2,1} & F_{2,2} & \dots & F_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ F_{n,1} & F_{n,2} & \dots & F_{n,d} \end{bmatrix} \quad (4)$$

$$OF = \begin{bmatrix} OF_1 \\ OF_2 \\ \vdots \\ OF_n \end{bmatrix} \quad (5)$$

It is well-known that both the moths and flames are the solutions. The dissimilarity among the moths and flames are the way of treating and updating them in each iteration. A definite search agent in the search space is the moths and the optimal location of the moth is given in the flame.

3.2.2. Location update of the moth

Three different functions are considered in the MFO for converging the global optimization of the optimization issues. Eq. (6) is used to define the function used in the converging purpose.

$$MFO = (I, P.T) \quad (6)$$

Where, the moth's initial random position is represented as I; the moth's movement in the search space is P and search process completion is denoted by the T. The random distribution of the moths are denoted in Eq. (7).

$$M(i,j) = (ub(i) - lb(j)) \times rand() + lb(i) \quad (7)$$

Where, the ub and lb denote the upper bound and lower bound of the variables respectively. Here, the moths are flown in the search space based on the transverse direction. Eq. (8) shows the logarithmic spiral of the MFO.

$$S(M_i, F_j) = D_i . e^{bt} . \cos(2\pi t) + F_j \quad (8)$$

Where the distance among the moth i and flame j is denoted as D_i; the fix to refer to the form of the logarithmic spiral is represented as b and the random number created in the range of $[-1,1]$ is represented as t. The spiral movement of moth close to the flame is used to balance the exploration and exploitation features.

3.2.3. Updating the amount of flame

This phase is used to improve the exploitation of the MFO in which location of the moth is updated at the n locations of the search space. This leads to reducing the probability of exploitation of optimal solutions. Hence, it is solved by reducing the number of flames as shown in Eq. (9).

$$flame\ no = round\left(N - l \times \frac{N-l}{T}\right) \quad (9)$$

Where, the amount of flames is represented as N; current iteration number is l and a maximum iteration number of T.

3.3 Selection of CH using IMFO

The IMFO chooses the secure optimal CHs from the clusters for obtaining secure data transmission over the network. Specifically, this IMFO avoids DDoS attacks during the CH selection.

3.3.1. Representation of moth

The potential solution of the IMFO is called as moth and this moth represents the group of nodes that are required to be selected as CH from the clusters. Each moth's dimension is equal to the amount of CHs in the WSN.

3.3.2. Initialization of moth

In IMFO, each moth is set with the random ID of the node between the 1 to num, here num specifies the number of sensors in the WSN. Consider, the ith moth of the IMFO is $M_i = (M_{i,1}, M_{i,2}, \dots, M_{i,q})$, where each moth location $M_{i,d}, 1 \le d \le q$ denotes

the ID of the node among the 1 to num while the q denotes the amount of CHs in the network.

3.3.3. Formulation of fitness value

The fitness value formulated for the CH selection is described in terms of Residual energy, Distance, Trust value, Node degree

3.3.3.1. Residual energy

The CH gathers the information from its cluster members and the collected data is transmitted to the destination node. The CH requires a high amount of residual energy to perform the mentioned tasks. Hence, the sensor with large energy is an optimal solution for identifying the CH where residual energy (f_1) is expressed in Eq. (10).

$$f_1 = \sum_{i=1}^{q} \frac{1}{E_{CH_i}} \quad (10)$$

Where, E_{CH_i} defines the residual energy of the candidate CH.

3.3.3.2. Distance

This fitness value defines the average distance among the CH and its cluster member nodes. The distribution of the node energy is mainly related to the distance of the route. The energy depletion of the sensor is less when the routing path is short. Eq. (11) expresses the distance (f_2) considered in the fitness value.

$$f_2 = \sum_{j=1}^{q} \left(\sum_{i=1}^{cm_j} dis(s_i, CH_j) / cm_j \right) \quad (11)$$

Where the cm_j represents the number of nodes that exist in the cluster and $dis(s_i, CH_j)$ represents the distance between the sensor i and jth CH.

3.3.3.3. Trust value

The trust value used in this IMFO is one of the important values used to improve the security against DDoS attacks. The nodes in the network are used to communicate with each other by using the mutual trust value. Here, the packet forwarding ratio is used to compute the trust value as shown in Eq. (12). The trust value (f_3) is the relation among the amount of forwarded and received packets of the node.

$$f_3 = \frac{PT_{s_{i,j}}}{PR_{s_{i,j}}} \quad (12)$$

Where the number of packets transmitted and received between the sensor i and j is represented as $PT_{s_{i,j}}$ and $PR_{s_{i,j}}$ respectively.

3.3.3.4. Node degree

An amount of cluster members for the respective CH is represented as node degree (f_4) which is expressed in Eq. (13).

$$f_4 = \sum_{i=1}^{q} cm_j \quad (13)$$

The aforementioned fitness values are conflicting with each other, so these multi-objective fitness values are converted into single objective fitness values as shown in Eq. (14).

$$OM = (\delta_1 \times f_1) + (\delta_2 \times f_2) + (\delta_3 \times f_3) + (\delta_4 \times f_4) \quad (14)$$

Where OM is the fitness function of the MFO which is used to improve the searching process of the CH selection. In a conventional MFO, the moth considers only distance during the searching process. But, four unique fitness values such as residual energy, distance, trust and node degree are considered for detecting the secure CH. Hence, this MFO is referred to as IMFO which is used for choosing an appropriate CH from the clusters as well as it is used to avoid DDoS attacks. This leads to a decrease the energy depletion and packet loss during the communication.

3.4 Secure routing using IMFO

In this SCRIMFO method, the secure routing path is generated between the source CH to the destination.

3.4.1. Initialization for secure route selection

Each moth in the routing process is initialized with the possible transmission path among the source node to the destination BS. The dimension of each moth is identical to the amount of CHs exist in the respective transmission path. Consider, the ith moth of the IMFO for routing is $M_i = (M_{i,1}, M_{i,2}, \ldots, M_{i,q})$, where each moth $M_{i,k} = (x_{i,k}, y_{i,k})$ and $1 \leq k \leq q$ represents the next hop CH.

3.4.2. Route selection

The IMFO uses the same fitness function which is already formulated in section 3.3.3 to identify the secure data transmission path. The control messages used in the ad hoc on-demand distance vector routing protocol is also used by this IMFO based routing path

Table 1. Simulation parameters

Parameter	Value
Area	$1200 \times 1200\ m^2$
Simulation time	100 s
Number of nodes	100
MAC layer	Mac/802.11
Initial energy	50 J
Wireless propagation protocol	TwoRayGround
Antenna pattern	Omni antenna
Network interface type	WirlessPhy
Queue type	PriQueue
Attack model	DDoS attack

generation. The IMFO uses different control messages such as Route Request (RREQ), Route Reply (RREP), Route Error (RERR), and hello (HELLO). The source node broadcasts the RREQ message to the neighbour nodes for initializing the route discovery process. Then, the next-hop node which has a better fitness value sends the RREP message to the source CH using the reverse route. The routing path is generated, once the source CH receives the RREP message from the adjacent nodes. After generating the routing path, the data transmission is initiated in the network. The IMFO based routing avoids DDoS attacks during the data communication phase. On the other hand, the RERR and HELLO messages are used for maintaining the routes.

4. Results and discussion

The results and discussion of this SCRIMFO method are clearly described in this section. The Network Simulator-2.34 (NS-2.34) is used for the implementation of the SCRIMFO method where the system uses the 4-GB RAM and Intel Core processor. The implemented SCRIMFO method is used to accomplish the secure data transmission between the source to the BS. The design and simulation of the SCRIMFO method in NS-2.34 with different parameters such as area, propagation model, queue type and so on are provided in Table 1.

4.1 Performance analysis

The performance of the SCRIMFO method is analyzed in terms of AEC, PDR, PLR and routing load. The SRPMA [16], ACCA [21] and ETOR [22] are used to analyse the SCRIMFO method.

4.1.1. Average energy consumption

AEC represents the average amount of energy consumed by all nodes in the network.

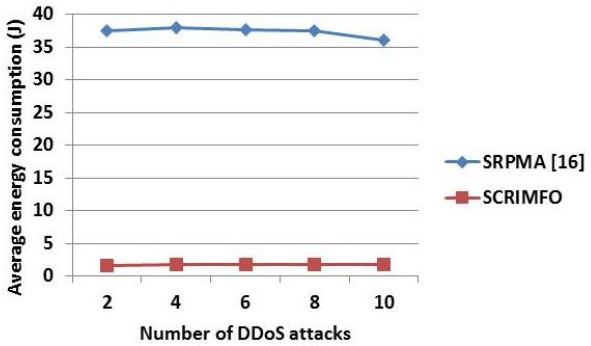

Figure. 2 Comparison graph of AEC

Table 2. Analysis of AEC

Number of DDoS attacks	SRPMA [16]	SCRIMFO
2	37.5 J	1.64 J
4	37.9 J	1.70 J
6	37.6 J	1.78 J
8	37.5 J	1.71 J
10	36 J	1.80 J

The comparison of AEC for the SRPMA [16] and SCRIMFO is shown in Table 2 and Fig. 2. From the analysis, conclude that the AEC of the SCRIMFO method is less when compared to the SRPMA [16]. For example, the AEC of the SCRIMFO with 10 DDoS attacks is 1.80 J, whereas the SRPMA [16] consumes 36 J of energy. The energy consumption of the SCRIMFO method is minimized by avoiding DDoS attacks as well as by identifying the shortest path over the network. However, the SRPMA [16] doesn't consider the energy while generating the path that causes huge energy depletion.

4.1.2. Packet delivery ratio

PDR is the ratio among the amount of received packets and the number of forwarded packets from the source which is expressed in Eq. (15).

Fig. 3 shows the PDR comparison between the SRPMA [16] and SCRIMFO method. Moreover, the

$$PDR = \frac{Amount\ of\ received\ packets}{Amount\ of\ forwarded\ packets} \times 100 \quad (15)$$

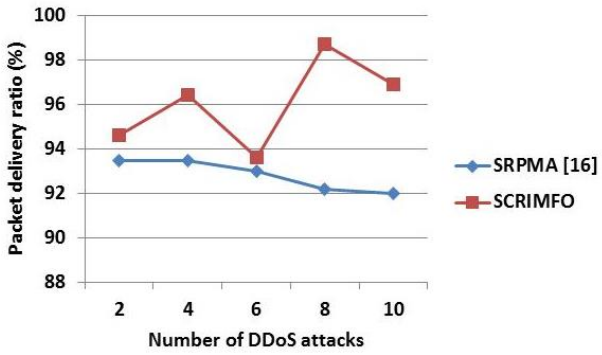

Figure. 3 Comparison graph of PDR

Table 3. Performance analysis of PDR

Number of DDoS attacks	SRPMA [16]	ACCA [21]	ETOR [22]	SCRIMFO
2	93.5 %	90 %	65 %	94.64 %
4	93.5 %	NA	NA	96.42 %
6	93 %	NA	NA	93.62 %
8	92.2 %	NA	NA	98.72 %
10	92 %	NA	NA	96.93 %

Table 3 shows the PDR comparison between the SRPMA [16], ACCA [21], ETOR [22] and SCRIMFO method. From the PDR analysis, it is determined that the SCRIMFO method obtains huge PDR than the SRPMA [16], ACCA [21] and ETOR [22]. For example, the SCRIMFO achieves a PDR of 94.64 % for 2 DDoS attacks, which is high when compared to the SRPMA [16], ACCA [21] and ETOR [22]. The secure routing path identification using the SCRIMFO is led to improve the packet delivery. Here, the DDoS attacks are avoided by using the trust value used in the SCRIMFO.

4.1.3. Packet loss ratio (PLR)

PLR is the proportion between the amount of dropped packets and the number of packets forwarded from the source. This PLR is expressed in the following Eq. (16).

$$PLR = \frac{Amount\ of\ dropped\ packets}{Amount\ of\ generated\ packets} \times 100 \quad (16)$$

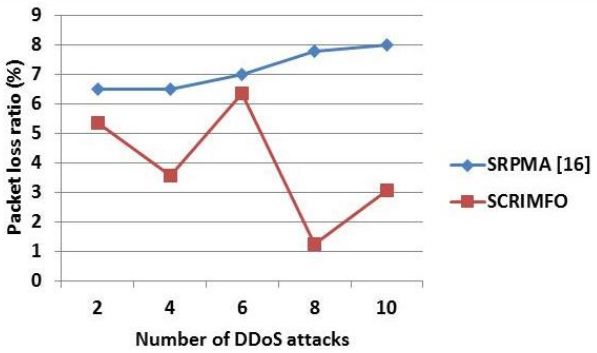

Figure. 4 Comparison graph of PLR

Table 4. Performance analysis of PLR

Number of DDoS attacks	**SRPMA [16]**	**ACCA [21]**	**ETOR [22]**	**SCRIMFO**
2	6.5 %	10 %	35 %	5.35 %
4	6.5 %	NA	NA	3.57 %
6	7 %	NA	NA	6.37 %
8	7.8 %	NA	NA	1.27 %
10	8 %	NA	NA	3.06 %

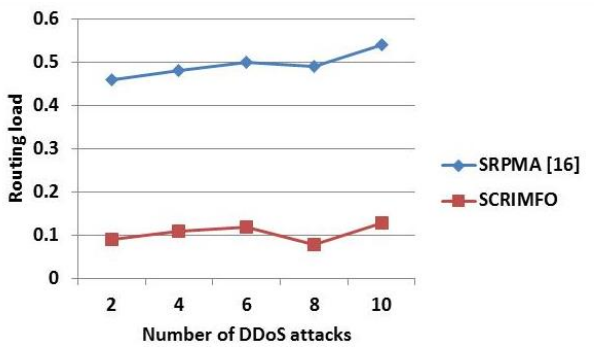

Figure. 5 Comparison graph of routing load

Table 5. Performance analysis of routing load

Number of DDoS attacks	**SRPMA [16]**	**ETOR [22]**	**SCRIMFO**
2	0.46	12	0.09
4	0.48	NA	0.11
6	0.5	NA	0.12
8	0.49	NA	0.08
10	0.54	NA	0.13

The comparison of PLR for the SRPMA [16] and SCRIMFO is shown in Fig. 4. Additionally, the PLR analysis for SRPMA [16], ACCA [21], ETOR [22] and SCRIMFO is shown in Table 4. From the analysis, conclude that the PLR of the SCRIMFO method is less than the SRPMA [16], ACCA [21] and ETOR [22]. For example, the PLR of the SCRIMFO with 10 DDoS attacks is 3.06 %, whereas the SRPMA [16] achieves 8 % of PLR. The PLR of the SCRIMFO is minimized by avoiding DDoS attacks during the CH selection and path generation. Moreover, the energy used in the IMFO helps to minimize packet loss by avoiding node failure.

4.1.4. Routing load

The routing load is the proportion between the amount of generated control packets and the amount of packets forwarded from the source.

$$RL = \frac{Amount\ of\ generated\ control\ packets}{Amount\ of\ \ packets\ forwarded\ from\ the\ source} \quad (17)$$

Fig. 5 shows the routing load comparison between the SRPMA [16] and SCRIMFO method. Additionally, the routing load analysis for SRPMA [16], ETOR [22] and SCRIMFO is shown in the Table 5. From Fig. 5 and Table 5, it is concluded that the SCRIMFO method achieves less routing load when compared to the SRPMA [16] and ETOR [22]. For example, the SCRIMFO achieves a routing load of 0.13, which is less when compared to the SRPMA [16]. The routing load of the SCRIMFO is decreased based on control packets reduction which is

transferred during the route discovery process. An optimal fitness value determines the secure optimal node while accomplishing the data transmission which further minimizes the requirements of control packets.

5. Conclusion

The secure clustering and routing are developed using the IMFO algorithm to obtain secure data transmission between the nodes. The node's energy depletion is minimized using the K-means clustering algorithm and IMFO based optimal CH selection. Next, the secure route between the desired nodes is generated using the IMFO. The CH selection and routing path generation using IMFO are improved using distinct fitness parameters such as residual energy, distance, trust and node degree. The trust considered in the IMFO helps mitigate the DDoS attacks during the data transmission. The performance of the SCRIMFO method was analyzed in terms of AEC, PDR, PLR and Routing Load. By the results obtained it is concluded that the SCRIMFO method outperforms well when compared to the SRPMA, ACCA and ETOR under varying DDoS attacks. The PDR of the SCRIMFO is 94.64 % for 2 DDoS attacks that is high when compared to the SRPMA, ACCA and ETOR. In future, a novel optimization algorithm can be used for improving the performances of the WSN.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first author. The supervision, review of work and project administration, have been done by second author.

References

[1] O. R. Ahutu and H. E. Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks", *IEEE Access*, Vol. 8, pp. 63270-63282, 2020.

[2] L. Yang, Y. Z. Lu, and Y. C. Zhong, "An unequal cluster-based routing scheme for multi-level heterogeneous wireless sensor networks", *Telecommun. Syst.*, Vol. 68, pp. 11-26, 2018.

[3] W. Fang, X. Wen, J. Xu, and J. Zhu, "CSDA: a novel cluster-based secure data aggregation scheme for WSNs", *Cluster Computing*, Vol. 22, No. 3, pp. 5233-5244, 2019.

[4] A. A. A. Ari, B. O. Yenke, N. Labraoui, I. Damakoa, and A. Gueroui, "A power efficient cluster-based routing algorithm for wireless sensor networks: Honeybees swarm intelligence based approach", *Journal of Network and Computer Applications*, Vol. 69, pp. 77-97, 2016.

[5] S. Dehghani, B. Barekatain, and M. Pourzaferani, "An enhanced energy-aware cluster-based routing algorithm in wireless sensor networks", *Wireless Personal Communications*, Vol. 98, pp. 1605-1635, 2018.

[6] C. Deepa and B. Latha, "HHSRP: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks", *Cluster Computing*, Vol. 22, pp. 10449-10465, 2019.

[7] D. C. Mehetre, S. E. Roslin, and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust", *Cluster Computing*, Vol. 22, pp. 1313-1328, 2019.

[8] S. H. Kang, "Energy optimization in cluster-based routing protocols for large-area wireless sensor networks", *Symmetry*, Vol. 11, p. 37, 2019.

[9] R. Logambigai, S. Ganapathy, and A. Kannan, "Energy-efficient grid-based routing algorithm using intelligent fuzzy rules for wireless sensor networks", *Computers & Electrical Engineering*, Vol. 68, pp. 62-75, 2018.

[10] K. Haseeb, K. A. Bakar, A. H. Abdullah, and T. Darwish, "Adaptive energy aware cluster-based routing protocol for wireless sensor networks", *Wireless Networks*, Vol. 23, pp. 1953-1966, 2017.

[11] M. Pavani and P. T. Rao, "Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks", *IET Wireless Sensor Systems*, Vol. 90, pp. 274-283, 2019.

[12] A. Mehmood, A. Khanan, M. M. Umar, S. Abdullah, K. A. Z. Ariffin, and H. Song, "Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks", *IEEE Access*, Vol. 6, pp. 5688-5694.

[13] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah, and A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks", *Wireless Personal Communications*, Vol. 105, pp. 1475-1490, 2019.

[14] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks", *IEEE Transactions on Information Forensics and Security*, Vol. 11, pp. 2013-2027, 2016.

[15] Q. Shi, L. Qin, Y. Ding, B. Xie, J. Zheng, and L. Song, "Information-aware secure routing in wireless sensor networks", *Sensors*, Vol. 20, pp. 165, 2020.

[16] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks", *Applied Soft Computing*, Vol. 77, pp. 366-375, 2019.

[17] 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, pp. 1637-1658, 2020.

[18] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks", *IEEE Transactions on Engineering Management*, Vol. 68, No. 1, pp. 170-182, 2019.

[19] A. R. Basha, "Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network", *IET Wireless Sensor Systems*, Vol. 4, pp. 166-174, 2020.

[20] V. Vijayalakshmi and A. Senthilkumar, "USCDRP: unequal secure cluster-based distributed routing protocol for wireless sensor networks", *The Journal of Supercomputing*, Vol. 76, pp. 989-1004, 2020.

[21] S. B. Sasi and R. Santhosh, "Multiobjective routing protocol for wireless sensor network optimization using ant colony conveyance algorithm", *International Journal of Communication Systems*, Vol. 34, No. 6, p. e4270, 2021.

[22] M. Hajiee, M. Fartash, and N. O. Eraghi, "An Energy-Aware Trust and Opportunity Based Routing Algorithm in Wireless Sensor Networks Using Multipath Routes Technique", *Neural Processing Letters*, Vol. 53, No. 4, pp. 2829-2852, 2021.

[23] K. Veerabadrappa and S. C. Lingareddy, "Secure Routing using Multi-Objective Trust Aware Hybrid Optimization for Wireless Sensor Networks", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 1, pp. 540-548, 2022, doi: 10.22266/ijies2022.0228.49.

[24] S. M. Shivakumaraswamy and C. S. Mala, "Security and Energy Aware Adaptive Routing using Cost Centric Cuckoo Search Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 6, pp. 596-604, 2021, doi: 10.22266/ijies2021.1231.53.