Received: October 29, 2021. Revised: December 7, 2021. 540

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Routing using Multi-Objective Trust Aware Hybrid Optimization for Wireless Sensor Networks

Kantharaju Veerabadrappa[1]* **Sanjeev Channaabasappa Lingareddy[2]**

[1]*Visvesvaraya Technological University-Belagavi, Karnataka, India*
[2]*Sri Venkateshwara College of Engineering, Vidyanagar, Bangalore, India*
* Corresponding author's Email: kantharajv@gmail.com

Abstract: Nowadays, energy optimization and data security are considered important security challenges while designing the network topology of Wireless Sensor Networks (WSNs). The problem of malicious nodes is required to be addressed to improve energy consumption and data delivery. Since the wireless sensor devices are energy-constrained, the issue of high packet loss by the malicious nodes must be addressed to enhance the network performance by making reduced energy consumption and delay. In this paper, a multi objective trust aware hybrid optimization (MOTAHO) is proposed to perform a secure data transmission over the WSN. The hybrid optimization is the combination of the moth flame and chicken swarm optimization (CSO), where it considered four distinct parameters such as trust, distance, energy, and number of hops for a secure cluster head (CH) selection and routing path generation. The developed MOTAHO method is used to provide security against the distributed denial of service (DDoS) attack. The performance of the MOTAHO method is analyzed in terms of routing load, packet delivery ratio (PDR), packet loss ratio (PLR), and average energy consumption. The existing methods namely secure routing protocol based on multi-objective ant-colony-algorithm (SRPMA), Energy-aware trust and opportunity-based routing (ETOR) for mobile nodes (MN) and grey wolf updated whale optimization algorithm (GU-WOA) are used to evaluate the effectiveness of the MOTAHO method. The PDR of the MOTAHO method is 97.44% for 4 DDoS attacks, which is high when compared to the SRPMA and ETOR-MN.

Keywords: Chicken swarm optimization, Distributed denial of service attack, Moth flame, Multi objective trust aware hybrid optimization, Wireless sensor networks.

1. Introduction

WSN is generally a special category of an ad-hoc network that contains a large number of tiny sensors located in the sensing field. The sensors in the geographical area are used for observing certain phenomena such as vibration, temperature, motions, sound, and so on [1, 2]. The sensors in the WSN have sensing equipment and signal processing devices that offer various abilities for processing the WSN sensors to enable wireless communications [3]. WSN is used in various applications such as healthcare, military, civil, environmental and scientific monitoring, and so on [4]. Energy consumption is considered as one of the main issues as the battery used in the sensors are cannot be replaceable and rechargeable. Therefore, clustering is used in the WSN to preserve a large amount of energy while broadcasting the data packets [5]. The sensors in-network is arranged as various groups namely clusters during the clustering process. Each cluster has a coordinator node namely CH and the remaining nodes in the cluster are referred to as cluster members. Accordingly, each sensor transmits the observed data to the respective CH and that CH transmits the collected data to the base station (BS) either through single-hop or multi-hop communication [6, 7].

The clustering over the network leads to minimizing the route discovery overhead [8]. Some of the existing methods used in the WSN are social spider algorithm-based routing [9], monarch-cat swarm optimization based routing [10], energy-aware trust-based secure routing method [11], energy

aware routing [12], and so on. All nodes in the network lead to losses of their energy when each node broadcasts the data to the BS and each node participates in the routing process for transmitting the data using intermediate nodes. Because, these sensors utilize the energy for various tasks such as data transmission, data collection, and data analysis [13]. Since the sensor nodes are located in abandoned environments, security is considered a key issue in cluster-based WSNs. The conventional secure mechanisms are infeasible because of restricted resources of the sensors such as less transmission range, memory, and processing power [14]. Additionally, an appropriate routing protocol is required to accomplish an effective data transmission, as well as the delayed/ manipulated data, are considered inadequate from the user perception [15]. In this research, the moth flame is combined with CSO for improving the WSN performances. In some cases, the CSO gets stuck inside the local optima during the searching process. Therefore, the moth flame is combined with the CSO to improve the searching probability of both the local and global search capabilities.

The main contributions of this research are given as follows:

- At first, the network is divided into various clusters using the K-means clustering algorithm. The clustering of the network is used for decreasing the energy consumption of the nodes.
- The secure optimal CH is selected from the clusters using the MOTAHO method. Since, the MOTAHO is the combination of moth flame and CSO which considered four distinct fitness functions such as trust, distance, energy and number of hops. Therefore, the malicious nodes (i.e., DDoS attacks) are avoided during the CH selection which helps to minimize the packet loss.
- Additionally, the secure route from the source CH to the BS is also discovered using the MOTAHO method. Therefore, the MOTAHO is used to enhance the security of the WSN while minimizing the energy consumption of the nodes.

The rest of this research paper is organized as follows: Section 2 provides the related work about the existing researches done in the secure data transmission over the WSN. The clear explanation about the MOTAHO method is provided in the section 3. Section 4 presents the results and discussion of the MOTAHO method. Finally, the conclusion of the paper is made in the section 5.

2. Related work

Prithi, and Sumathi [16] presented the combination of Particle Swarm Optimization (PSO) and Deterministic Finite Automata (DFA) to perform intrusion detection and secure data transmission over the WSN. Further, the Learning Dynamic Deterministic Finite Automata (LD2FA) was developed to observe the dynamic topology of the network as well as it used to optimize the route selection by using the PSO. The developed LD2FA-PSO was used to improve the energy efficiency of the nodes.

Pavani. and Rao [17] developed the secure cluster-based routing protocol (SCBRP) which used the adaptive PSO algorithm with the firefly algorithm. The developed SCBRP has used the hexagonal network architecture. In SCBRP, the fuzzy inference system was used to evaluate the security level of the node and the node with less security level was mitigated from the network. The designed SCBRP was flexible as well as it was used in both small and large scale networks.

Sun [18] implemented the secure routing protocol based on multi-objective ant-colony-algorithm (SRPMA) for WSN. Two distinct objective functions were mainly considered in the developed method. The first objective function of SRPMA was considered the typical residual energy of the routing path to minimize energy utilization. The second objective function was about considering the routing path's typical trust value which ensures the security of the route node. The SRPMA method achieved better performance against blackhole attacks in WSN. However, the routing path generation of the SRPMA method was considered only the energy and trust value of a node.

Basha [19] presented the realisable secure aware routing (RSAR) protocol for minimizing the control overhead of the network. The trust degree of each node was calculated by employing the conditional tug of war optimization in the RSAR protocol. Here, the energy consumption was optimized using cluster based data aggregation. But, the developed RSAR was considered only energy of the nodes, it failed to consider the distance and node degree of the nodes.

Kalidoss [20] 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 modeling 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,

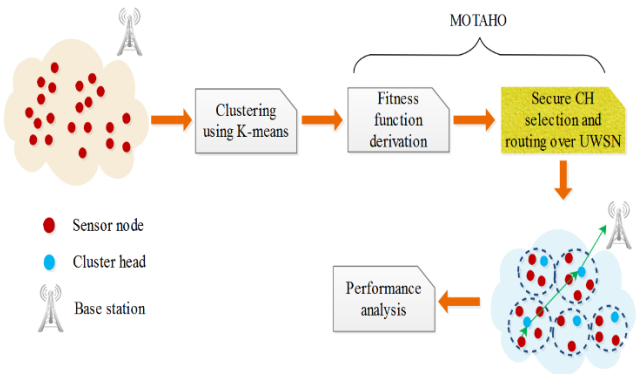

Figure. 1 Block diagram of the MOTAHO method

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.

Hajiee [21] presented the energy-aware trust and opportunity-based routing (ETOR) with hybrid fitness function. The ETOR operated under mobile nodes (MN) was referred as ETOR-MN. The fitness function considered in this ETOR were network traffic, connectivity, hop-count, distance, energy, trust and QoS. This ETOR was performed two important steps. In that, the tolerance constant was used to select the secure nodes followed by the opportunistic nodes were selected for performing the routing. The transfer failure's probability was minimized by using this ETOR. However, the PDR of the ETOR was high, only when the network has high amount of nodes.

Reddy [22] developed the grey wolf updated whale optimization algorithm (GU-WOA) to choose an optimal CH. The multi objective function considered for the GU-WOA were energy, distance, security and delay. This GU-WOA was used to minimize the distance among the node and chosen CH. However, this work failed to perform the multi hop routing. If the network performed a single hop transmission, then the CHs rapidly depleted their own energy in the network.

3. MOTAHO method

The secure data transmission against DDoS attacks is achieved using the MOTAHO. The developed MOTAHO method has three different phases such as clustering, selection of CH and route generation. The CH and route selection is performed using the MOTAHO, where it is optimized by using four distinct parameters such as trust, distance, residual energy and number of hops. Therefore, the DDoS attacks are avoided during the data transmission and also the energy of the nodes is minimized over the WSN. Fig. 1 shows the block diagram of the MOTAHO method.

3.1 Clustering using K-means

In this proposed method, the network is divided into various clusters using the Euclidian distance. At first, c amount of samples are randomly chosen from the sets of data (i.e., node coordinates), and the Euclidian distance among the c centers and each node co-ordinate is calculated for clustering the network. Further, the mean of subsets to form a cluster is computed to generate a cluster.

3.2 Cluster head selection

In this phase, the MOTAHO is used to select the secure optimal CHs from each cluster. Since the MOTAHO is the integration of the moth flame and chicken swarm optimization (CSO). Moth flame is generally a population-based optimization algorithm and it mimics the actions of the moths. CSO is one of the intelligent bionic algorithms and it mimics the food searching behavior of the cocks, hens, and chicks. Chicken swarm in the searching space is referred to as a specific particle individual. The developed MOTAHO is used to select the CHs from the network using four distinct parameters trust, distance, residual energy, and number of hops. The process of CH selection using MOTAHO is described as follows:

3.2.1. Representation and initialization

The probable solution for the MOTAHO is referred as a moth. The moth represents the group of sensors are required to be chosen as CH during the CH selection. A dimension of each moth is equal to the CHs in the network. The location of each moth is set by the random candidate node ID among the 1 and NS, where NS defines the number of sensor nodes. Eq. (1) shows the initialization of the ith moth for the MOTAHO.

$$M_i = \left(M_{i,1}, M_{i,2}, \ldots, M_{i,a}\right) \tag{1}$$

Where the location of each moth is $M_{i,d}, 1 \leq d \leq a$ indicates the node_ID among the 1 and NS over the network.

3.2.2. Iterative process

The location of the moth i updated at iteration k is represented as M_i^k and it is expressed in the following Eq. (2).

$$M_i^k = D_i^{k-1} e^{bt} \cos(2\pi t) + F_i^{k-1} \quad (2)$$

Where the distance among the moth i and flame i in iteration $k-1$ is $D_i^{k-1} = \left|F_i^{k-1} - M_i^{k-1}\right|$; the position of the flame i in iteration $k-1$ is F_i^{k-1} and the spiral shape is represented by b. The value t defines the closeness between the moth and flame and it is a random number between $[r, 1]$. In that, r is linearly decreased from -1 to -2 according to the iteration k which is expressed in Eq. (3).

$$r(k) = -1 - \frac{k}{K} \quad (3)$$

Where, the current and maximum number of iteration are denoted as k and K respectively. To update moth location according to the optimal flame from the overall solutions, the number of flames in the MOTAHO is decreased as shown in Eq. (4).

$$n_f(k) = \left[n - \frac{k}{K}(n-1)\right] \quad (4)$$

Where, the maximum amount of flames is represented as n and the number of flames decreased in each iteration is represented as n_f. The solution from the moth flame is further enhanced by optimizing with CSO.

The swarms in the CSO are one rooster, many hens, and many chicks which are divided based on the particle's fitness. Moreover, the swarms in the CSO have distinct location update expressions. In that, the rooster's location update is expressed in Eq. (5).

$$M_i^R(k\ +1) = M_i^R(k) \times (1 + N(0, \sigma^2)) \quad (5)$$

where, the rooster is denoted as R, the iteration is denoted as k, and the Gaussian distribution with 0 mean and σ^2 variance is represented as $N(0, \sigma^2)$. Eq. (6) denotes the expression used to the variance.

$$\sigma^2 = \begin{cases} 1 & if\ f_i < f_j \\ \exp\left(\frac{(f_j - f_i)}{|f_i| + \varepsilon}\right), & otherwise \end{cases}$$
$$i, j\ \epsilon [1,2, \dots, RN], j \neq i \quad (6)$$

where, amount of roosters is represented as RN and ε is the constant utilized for avoiding the zero-division error. The fitness of the rooster i and j are represented as f_i and f_j respectively.

The location update formulae of hen are expressed in Eq. (7).

$$M_i^H(k+1) = M_i^H(k) + S_1 \times rand \times \left(M_{r1}^R(k) - M_i^H(k)\right) + S_2 \times rand \times (M_{r2}^R(k) - M_i^H(k)) \quad (7)$$

Where, S_1 and S_2 of Eq. (7) is expressed in Eqs. (8) and (9) respectively.

$$S_1 = \exp((f_i - f_{r1})/(abs(f_i) + \varepsilon)) \quad (8)$$

$$S_2 = \exp(f_{r2} - f_i) \quad (9)$$

Where, the individual swarm of hen is denoted as H; the index of the rooster taken from the hen i's group-mate is represented as $r1$ and the index of the chicken randomly taken from the swarm is represented as $r2$ whereas $r1 \neq r2$.

The location update formulae of hen are expressed in the Eq. (10).

$$M_i^C(k+1) = M_i^C(k) + FL \times (M_m^H(k) - M_i^C(k)) \quad (10)$$

Where, the individual swarm of chick is denoted as C; the index of chick's mother from the group i is represented as m and follow coefficient is denoted as FL which is generated as a uniform random number between [0,2].

3.2.3. Fitness function derivation

The fitness function used in this MOTAHO for selecting the topical CHs are derived in this section. Here, the fitness function is formulated using four distinct parameters such as trust, distance, residual energy and number of hops.

a. Trust

In this CH selection, trust is considered as a major parameter in the fitness function for improving the security against DDoS attacks. The mutual trust generated in a certain time period is used to accomplish the communication. Here, the trust is calculated based on the packet forwarding behavior that is the relation among the transmitted data (TDP_{ij}) and the received data (RDP_{ij}). Eq. (11) shows the calculated trust value (g_1) which is used for mitigating the DDoS attacks while broadcasting the data packets.

$$g_1 = \frac{TDP_{ij}}{RDP_{ij}} \quad (11)$$

b. Distance

It defines the distance (g_2) among the cluster head to the next-hop node and the BS. Since the energy utilization of the node is proportional to the distance of the transmission path. Therefore, it is required to discover the transmission path with less distance for minimizing the energy consumption.

c. Residual energy

The candidate CH with high residual energy (g_3) expressed in Eq. (12) is highly preferable during the CH selection. Because the CH has to do various operations such as data collection, aggregation and transmission.

$$g_3 = \sum_{i=1}^{a} E_{CH_i} \quad (12)$$

Where, E_{CH_i} indicates the remaining energy of the CH.

d. Number of hops

An amount of normal nodes belonging to the particular CH is defined as a number of hops. The energy consumption of the CH is less when it has less number of hops. Hence, the CH with less hops are considered in CH selection and the number of hops (g_4) is expressed in Eq. (13).

$$g_4 = \sum_{i=1}^{a} I_i \quad (13)$$

Where, the amount of normal nodes for the particular CH is denoted as I_i.

The aforementioned objective values are transformed into a single objective based on the weighted sum approach as shown in Eq. (14).

$$f = \delta_1 \times g_1 + \delta_2 \times g_2 + \delta_3 \times g_3 + \delta_4 \times g_4 \quad (14)$$

Where, the $\delta_1, \delta_2, \delta_3$ and δ_4 are the weights allocated to each fitness function value. The formulated fitness function is used in the MOTAHO for selecting the optimal CH from the clusters. This MOTAHO based CH selection avoids the DDoS attacks by considering the trust value which leads to avoiding the packet dropping between the node's data transmission. The distance considered in the finesses used to discover the path with less transmission distance, hence the energy consumption of the nodes is less over the network. Next, the energy is considered in MOTAHO for avoiding node failure while generating the path. Further, the number of hops is considered in the fitness function for minimizing the energy consumption of the nodes.

3.3 MOTAHO based secure data transmission

In this phase, the secure routing path is generated by using the same fitness function mentioned in section 3.2.3. Here, each particle in the MOTAHO is initialized with the possible routing path between the source CH to the BS. The MOTAHO uses the control messages of the ad hoc on-demand distance vector routing protocol while generating the routing path. The control messages used by the MOTAHO are route request (RREQ), route reply (RREP), route error (RERR), and hello (HELLO). At first, the RREQ message is broadcasted by the source node while starting the route discovery phase. Subsequently, the next hop node with better fitness transmits the RREP over the reverse route. If the source node receives the RREP message from the neighbor node, then the routing path is generated from the source CH to the BS. The secure data transmission is enabled over the WSN by mitigating DDoS attacks. Besides, the HELLO and RERR messages are utilized to perform route maintenance.

The proposed MOTAHO method is used to improve the security of the WSN by identifying the attacker nodes in each level of communication. At first, the DDoS attacks are avoided by considering the trust value in the fitness function of the MOTAHO. Additionally, the secure routing is developed to obtain a reliable data transmission. Therefore, the MOTAHO method is achieves the higher PDR while achieving lesser energy consumption.

4. Results and discussion

The results and discussion for the MOTAHO method are described in this section. The design and simulation of this MOTAHO method are performed in the network simulation (NS2) tool where the system has the 6-GB RAM and Intel Core processor. The network is considered with the normal nodes and DDoS attacks for analyzing the performances of MOTAHO, where the nodes are positioned in the area of $1200\text{m} \times 1200\text{m}$. Additionally, the sensors in the WSN are fixed with the preliminary energy level of 50 J. The specification parameters of the MOTAHO are specified in Table 1.

The MOTAHO method is analyzed in terms of the routing overhead, PDR, PLR and average energy consumption. The existing methods namely SRPMA [18], ETOR-MN [21] and GU-WOA [22] are used to evaluate the MOTAHO method.

Table 1. Specification parameters

Parameter	Value
Number of nodes	100
Area	1200m × 1200m
DDoS attacks	2, 4, 6, 8 & 10
Initial energy	50 J
MAC protocol	Mac/802.11
Network interface type	WirlessPhy
Antenna pattern	OmniAntenna
Wireless propagation protocol	TwoRayGround
Queue type	PriQueue
Simulation time	100 s

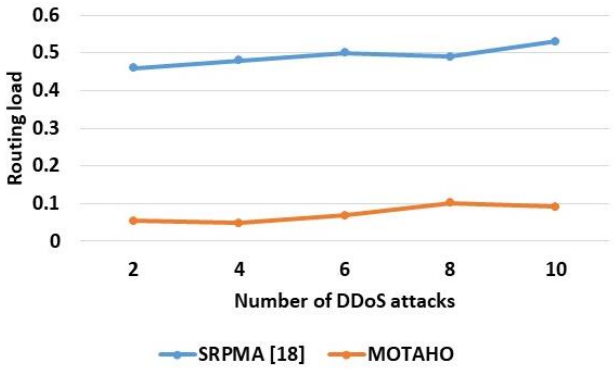

Figure. 2 Routing load

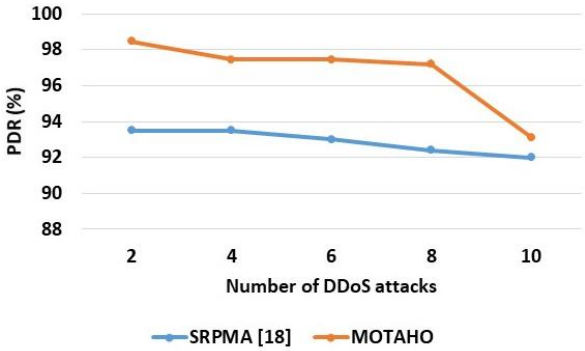

Figure. 3 Packet delivery ratio

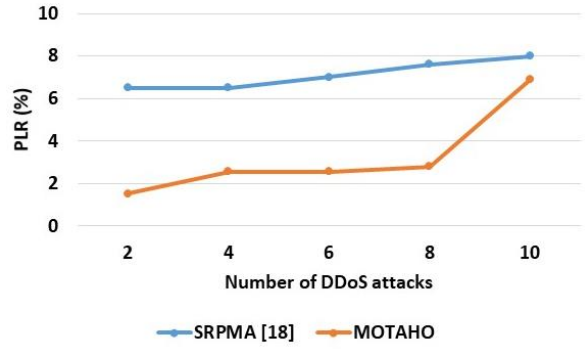

Figure. 4 Packet loss ratio

4.1 Routing load

Routing load is defined as the ratio of the amount of generated routing packets to the number of packets received at the BS.

Fig. 2 shows the routing load comparison of the MOTAHO and SRPMA [18], where it is analyzed for varying DDoS attacks. From Fig. 2, it is concluded that the MOTAHO method achieves less routing load when compared to the SRPMA [18]. For example, the MOTAHO achieves a routing load of 0.13, which is less when compared to the SRPMA [18]. The routing load of the MOTAHO is minimized by reducing the control packets transferred during the route discovery process. Optimal fitness values are employed to identify the secure optimal node during the data transmission which further minimizes the requirements of control packets.

4.2 Packet delivery ratio

PDR is the ratio among the number of received packets at the BS and the amount of packets generated at the source. Eq. (15) is used to estimate the PDR.

$$PDR = \frac{RDP}{TDP} \tag{15}$$

Fig. 3 shows the PDR comparison between the SRPMA [18] and MOTAHO method. From Fig. 3, it is decided that the MOTAHO method obtains an improved PDR than the SRPMA [18]. For example, the MOTAHO achieves a PDR of 93.11 % for 10 DDoS attacks, which is high when compared to the SRPMA [18]. The secure routing path identification using the MOTAHO is led to improve the packet delivery. Here, the DDoS attacks are avoided by using the trust value used in the MOTAHO.

4.3 Packet loss ratio

The PLR is calculated to identify the percentage of the lost packet during the data transmission. The following Eq. (16) is used to estimate the PLR.

$$PLR = \frac{TDP-RDP}{RDP} \tag{16}$$

The comparison of PLR for the SRPMA [18] and MOTAHO is shown in Table 2 and Fig. 4. From the analysis, conclude that the PLR of the MOTAHO method is less when compared to the SRPMA [18]. For example, the PLR of the MOTAHO with 10 DDoS attacks is 6.88 %, whereas the SRPMA [18] achieves 8 % of PLR. The PLR of the MOTAHO is minimized by avoiding the DDoS attacks during the CH selection and path generation. Moreover, the

Table 2. Comparative analysis of the MOTAHO with SRPMA, ETOR-MN and GU-WOA

Performances	Methods	Number of DDoS attacks				
		2	4	6	8	10
Routing overhead	SRPMA [18]	0.46	0.48	0.5	0.49	0.53
	ETOR-MN [21]	NA	13	NA	NA	NA
	MOTAHO	0.0539	0.0477	0.0685	0.101	0.0920
PDR (%)	SRPMA [18]	93.5	93.5	93	92.4	92
	ETOR-MN [21]	NA	66	NA	NA	NA
	GU-WOA [22]	95.5	NA	NA	NA	NA
	MOTAHO	98.46	97.44	97.44	97.19	93.11
PLR (%)	SRPMA [18]	6.5	6.5	7	7.6	8
	ETOR-MN [21]	NA	34	NA	NA	NA
	GU-WOA [22]	4.5	NA	NA	NA	NA
	MOTAHO	1.53	2.55	2.55	2.80	6.88
Average energy consumption	SRPMA [18]	37.5	37.9	37.6	37.5	36
	MOTAHO	0.97	0.90	0.87	1.10	1.05

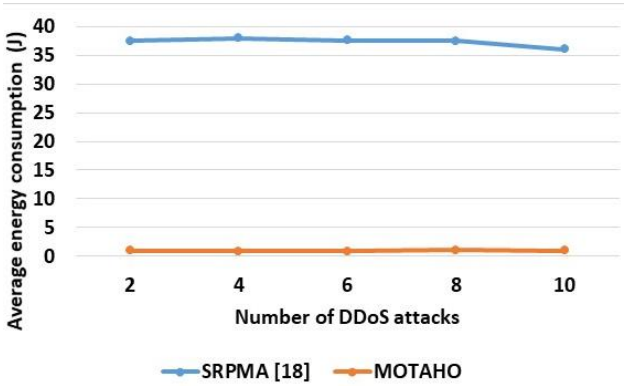

Figure. 5 Average energy consumption

residual energy used in the fitness helps to minimize the packet loss by avoiding node failure.

4.4 Average energy consumption

The node's energy consumption is the amount of energy consumed during the data collection and transmission. Specifically, the average energy consumption is the energy consumed by all the nodes.

The comparison of average energy consumption for the SRPMA [18] and MOTAHO is shown in Fig. 5. This analysis concludes that the MOTAHO method has lesser energy consumption than the SRPMA [18]. For example, the average energy consumption of the MOTAHO with 10 DDoS attacks is 1.05 J, whereas the SRPMA [18] consumes 36 J of energy. The energy consumption of the MOTAHO method is minimized by avoiding DDoS attacks as well as by identifying the shortest path over the network. However, the SRPMA [18] doesn't consider the energy while generating the path which leads to higher energy consumption.

The comparative analysis of the MOTAHO method with SRPMA [18], ETOR-MN [21] and GU-WOA [22] is shown in the Table 2, where NA specifies the parameter which is not available. This analysis concludes that the MOTAHO method outperforms well than the SRPMA [18], ETOR-MN [21] and GU-WOA [22]. The trust value considered in this MOTAHO is used to avoid the DDoS attacks during the communication process. Accordingly, the packet delivery and routing overhead of the MOTAHO are improved by selecting an optimal CHs and routing path over the network. Specifically, the routing overhead of the MOTAHO is less, because it doesn't require high amount of control packets while performing the route discovery.

5. Conclusion

In this paper, a multi objective trust aware hybrid optimization (MOTAHO) is proposed to perform a secure data transmission over the WSN. The hybrid optimization has the moth flame and CSO, where it considered four distinct parameters such as trust, distance, energy, and a number of hops for achieving a secure CH selection and routing path generation. The developed MOTAHO method is used to provide security against DDoS attacks. From the performance analysis, it is concluded that the MOTAHO provides better performance than the SRPMA, ETOR-MN and GU-WOA. The PDR of the MOTAHO method is 97.44% for 4 DDoS attacks, which is high when compared to the SRPMA and ETOR-MN. Additionally, the PDR of the MOTAHO method is 98.46% for 2 DDoS attacks, which is high when compared to the SRPMA and GU-WOA. In future, a novel optimization technique can be used for improving the WSN performances.

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] A. Saidi, K. Benahmed, and N. Seddiki, "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks", *Ad Hoc Networks*, Vol. 106, p. 102215, 2020.

[2] P. S. Khot and U. Naik, "Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection", *Wireless Personal Communications*, Vol. 119, pp. 2405–2429, 2021.

[3] A. Vinitha and M. S. S. Rukmini, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm", *Journal of King Saud University-Computer and Information Sciences*, 2019.

[4] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks", *Ad Hoc Networks*, Vol. 115, p. 102448, 2021.

[5] M. Revanesh, V. Sridhar, and J. M. Acken, "Secure Coronas Based Zone Clustering and Routing Model for Distributed Wireless Sensor Networks", *Wireless Personal Communications*, Vol. 112, No. 3, pp. 1829-1857, 2020.

[6] P. S. Khot and U. L. Naik, "Cellular automata-based optimised routing for secure data transmission in wireless sensor networks", *Journal of Experimental & Theoretical Artificial Intelligence*, pp. 1-19, 2021.

[7] M. Maheswari and R. A. Karthika, "A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks", *Wireless Personal Communications*, Vol. 118, No. 2, pp. 1535-1557, 2021.

[8] M. V. Babu, J. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, "An Improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network", *Mobile Networks and Applications*, pp. 1-9, 2020.

[9] U. Meena and A. Sharma, "Secure key agreement with rekeying using FLSO routing protocol in wireless sensor network", *Wireless Personal Communications*, Vol. 101, No. 2, pp. 1177-1199, 2018.

[10] P. A. Patil, R. S. Deshpande, and P. B. Mane, "Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm", *Wireless Personal Communications*, Vol. 115, No. 1, pp. 415-437, 2020.

[11] 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, No. 4, pp. 1475-1490, 2019.

[12] K. Selvakumar, L. Sairamesh, and A. Kannan, "An intelligent energy aware secured algorithm for routing in wireless sensor networks", *Wireless Personal Communications*, Vol. 96, No. 3, pp. 4781-4798, 2017.

[13] K. Thangaramya, K. Kulothungan, S. I. Gandhi, M. Selvi, S. S. Kumar, and K. Arputharaj, "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN", *Soft Computing*, Vol. 24, No. 21, pp. 16483-16497, 2020.

[14] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption", *Journal of King Saud University-Computer and Information Sciences*, Vol. 28, No. 3, pp. 262-275, 2016.

[15] V. Vijayalakshmi and A. Senthilkumar, "USCDRP: unequal secure cluster-based distributed routing protocol for wireless sensor networks", *The Journal of Supercomputing*, Vol. 76, No. 2, pp. 989-1004, 2020.

[16] S. Prithi and S. Sumathi, "LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network", *Ad Hoc Networks*, Vol. 97, p. 102024, 2020.

[17] 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. 9, No. 5, pp. 274-283, 2019.

[18] 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.

[19] A. R. Basha, "Energy efficient aggregation technique-based realisable secure aware routing

protocol for wireless sensor network", *IET Wireless Sensor Systems*, Vol. 10, No. 4, pp. 166-174, 2020.

[20] 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.

[21] 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, pp. 2829-2852, 2021.

[22] D. L. Reddy, C. G. Puttamadappa, and H. N. G. Suresh, "Hybrid optimization algorithm for security aware cluster head selection process to aid hierarchical routing in wireless sensor network", *IET Communications*, Vol. 15, No. 12, pp. 1561-1575, 2021.