Secure Routing using Multi-Objective Particle Swallow Swarm Optimization for Wireless Sensor Networks

Dr. A. Nithya

Assistant Professor
Department of Computer Science (SF)
Kongunadu Arts and Science College
Coimbatore, India.

Abstract: **In recent days, energy optimization and data security are the most important security issues when planning the network topology of Wireless Sensor Networks (WSNs).These types of malicious nodesareto be used to improve energy consumption and data delivery. Meanwhile the wireless sensor strategies are energy- constrained, the issues of high packet loss by the malicious nodes aresolved to enhance the network performance by reducing energy consumption and delay. In this work, a multi objective Particle Swallow Swarm optimization (MOPSSO) is proposed to secure data broadcast over the WSN. This optimization is the combination of the moth flame and hybrid swarm optimization (HSO), where it considers the four different parameters such as trust, distance, energy and number of hops for a cluster head (CH) selection and routing path generation. The proposed MOPSSO methods are used to provide security against the distributed denial of service (DDoS) attack. The performance ofthe MOPSO method calculated in terms of packet delivery ratio (PDR) and packet loss ratio(PLR).The existing methods such as multi-objective ant-colony-algorithm(MOACA),Genetic Algorithms(GA) for mobile nodes (MN) compares with the efficiency of MOPSSO method. The PDR of the MOPSSO method is 85.23% for DDoS attacks, when compared to the HSO and GA.**

***Keywords*: Particle Swallow swarm Optimization, Distributed denial of service attack, Multiobjective, Wireless sensor networks.**

I.INTRODUCTION

WSNone ofanad-hoc networkthat contains a large number of tiny sensors located in the sensor area. The sensors in that area are used for monitoring vibration, temperature, motions, sound, and soon[1,2].WSN sensors have some sensing tools and signal processing devices that provides various skills for generating WSN sensors to enable wireless communications[3].WSN applications applications such as healthcare, military, construction ,environment and location monitoring, and etc., [4].

Energy consumption is one of the main challenges as facedinthesensorsarecannotbeconsumableand rechargeable. So, clustering is used to preserve a large amount of energy while distributionof the data packets [5].

These sensors in- network are arranged in variouscollectionssuch as clusters during the grouping method. Every cluster has its node namely CH and the rest of the nodes are referred to as cluster members. Therefore, each sensor transmits the detected data to the respective CH and that CH transmits the collected data to the base station (BS) instead through single-hop or multi-hop communication [6, 7].

The clustering nodes in the network used to minimize the route discovery overhead [8]. An 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 etc., Every node in the network leads toloss of the energywhile eachnode broadcasting the data to the BS . Since, the sensors are utilizing the energy for various applications such as data transmission, data collection, and data analysis [13]-[15]. In this work, the proposed MOPSSO combined hybrid swallow swarm optimization with for improves WSN efficiency.

The main contributions of this research are given as follows:

- At first, the entire network isseparatedamong various clustersusingtheK-meansclusteringalgorithm. Network clustering are used to decreasetheenergyconsumption.
- The secure optimal CH is selected from the clusters using the MOPSSO method. Later, the MOPSSOisthecombination ofmoth flame and HSO while considering four different tasks such as trust, distance, energy and number of hops. So, the malicious nodes (i.e., DDoS attacks) are avoided during the CH selectionwhichhelpsreducethepacketloss.
- Moreover, the secure path from the source CH to BS is also exposed using MOPSSO method.Then, the MOPSSO used to improve the security of the WSN when minimizingtheenergyconsumption.

II. Relatedwork

Prithiand Sumathi [16] developed 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 intended SCBRP was flexible as well as it was used in both small and large scale networks.

Sun[18]introduced 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 black hole 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] proposed the realisable secure aware routing (RSAR) protocol for minimizing the control overhead of the network. The trust degree of each node was calculated by employs the conditional tug of war optimization in the RSAR protocol. Here, the energy consumption was optimized using cluster based data aggregation. Then, 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. Therefore, the trustworthy node was selected from the clusters using the trust score andtheselectednodewas referredtoasaCH.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.

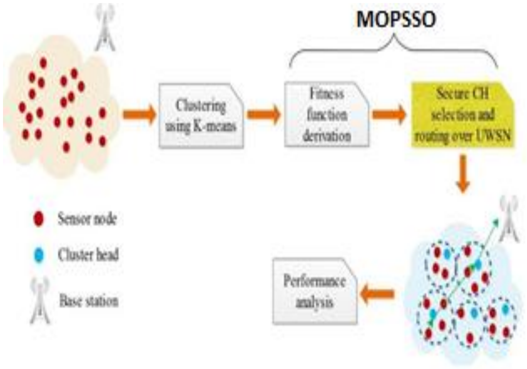


Figure.1Block diagram of the MOPSSO method

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 was network traffic, connectivity, hop-count, distance, energy, trust and QoS. This ETOR was performed two important steps.

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 was energy, distance, security and delay.

III. MOPSSO METHOD

The secure data transmission against DDoS attacks is attained using MOPSSO. The proposed MOPSSO method has three different stages such as clustering, selection of CH and route generation.TheCHandrouteselectionareachieved using the MOPSSO, then it is enhanced by using four distinct constraints such as trust, distance, residual energy and number of hops. Consequently, DDoS attacks are avoided during data transmission and also the energy of the nodes are minimized over the WSN. Fig. 1 shows the block diagram of the MOPSSO method.

3.2.Clusterhead (CH) selection

In this stage, the MOPSSO are used to select the secure optimal CHs from every cluster. Meanwhile the MOPSSO is the integration of the Hybrid swarm Optimization (HSO). The developed MOPSSO is used to select the CHs from the network using four separateareas such as trust, distance, residual energy, and number of hops.

The process of CH selection using MOPSSO is described as follows:

3.2.1. Representation and initialization

The possible solution for the represents the group of sensors is essential to be chosen as CH during the CH selection. Where NS defines the number of sensor nodes. Eq. (1) shows the initialization of the ith moth for the MOPSSO.

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

Here the location is $Mi,$, $1 \leq d \leq a$ indicates the node_ID among the 1 and NS over the network.

3.2.2. Iterative process

The location is efficient at iteration k is represented as Mik and it is expressed in the following Eq. (2).

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

$Dik-1 = |Fik-1 - Mk-1\ |$; the position of the flame i in iteration $k-1$ is $Fik-1$ and the spiral shape is represented by b . The value t defines closeness and it is a random number between $[r, 1]$. In that, r is linearly reduced 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 extremenumber of iteration isrepresented as k and Kcorrespondingly. MOPSSO is decreased as shown in Eq. (4).

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

Where, the maximum amount represented as n and the number of flames decreased in each iteration is represented as nf. In that, the 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.

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

where, amount is represented as RN and ε. The location now can be 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, $S1$ and $S2$ of Eq. (7) is expressed in Eqs. (8) and (9) respectively.

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

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

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

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

3.2.3. Fitness function derivation

Now, the 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 measured as a major parameter in the function for refining the security against DDoS attacks. The mutual trust generated in a certain time period is used to accomplish the communication. Now, the trust is intended based on the packet forwarding performance that is the relation among the transmitted data ($TDPij$) and the received data ($RDPij$) . Eq. (11)

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

b. Distance

It defines the distance ($g2$) between the cluster head to the next-hop node and the BS. Since the energy utilization of the node is comparative to the distance of the transmission path.

c. Residual energy

The candidate CH with high residual energy ($g3$) 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.

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

Where, $ECHi$ 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 ($g4$) is expressed in Eq. (13).

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

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

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

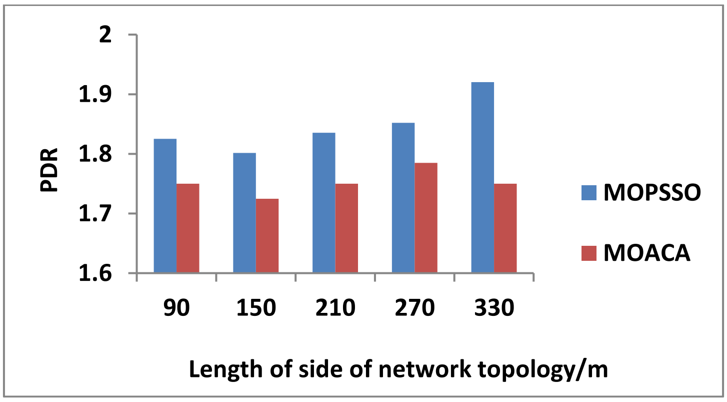
$$f = \delta_1 \times g_1 + \delta_2 \times g_2 + \delta_3 \times g_3 + \delta_4 \times g_4 \quad (14)$$

IV. RESULTS AND DISCUSSION

The results and discussion for the MOPSSO method are described in this section. The design and simulation of this MOPSSO 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 MOPSSO, where the nodes are positioned in the area of 1200m × 1200m. The MOPSSO method is analyzed in terms of the routing overhead, PDR and PLR.

4.1 Packet delivery ratio

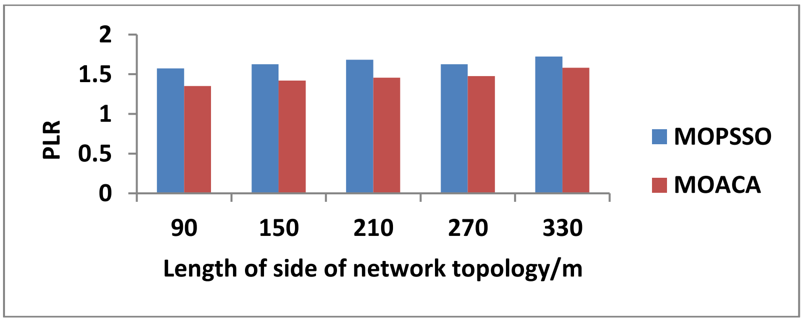
PDR is the ratio among the number of received packets at the BS and the amount of packets generated at the source. Eq. (15) is used to estimate the PDR. The MOPSSO reaches 1.8 in the PDR,where the MOACA reaches 1.7 in the ratio.



$$PDR = \frac{RDP}{TDP} \qquad (15)$$

4.2 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. The MOPSSO reaches 1.6 in the PLR,where the MOACA reaches 1.5 in the ratio.



V. CONCLUSION

In this paper, a multi objective Particle swallow swarm optimization (MOPSSO) is proposed to perform a secure data transmission over the WSN. The hybrid optimization has considered four distinct parameters such as trust, distance, energy, and a number of hops for achieving a secure CH selection and routing path generation.

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 UsingCluster Head Selection", *Wireless PersonalCommunications,*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,andN.M.Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks",*AdHoc 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 QoSBasedSecure 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,andD.Gupta,"AnImproved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network",*MobileNetworksandApplications,*
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, "Trustandopportunitybasedroutingframework 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,andX.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.PrithiandS.Sumathi,"LD2FA-PSO:Anovel 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- basedroutinginwirelesssensor 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 realizable 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,