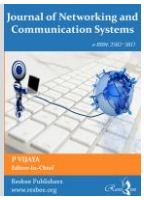
Resbee Publishers

Journal of Networking and Communication Systems

Received 9 May, Revised 23 June, Accepted 7 July



Secure Routing Protocol using Salp-Particle Swarm Optimization Algorithm

Heyan Zhang
Xidian University, China
heyanzhang1240@gmail.com

Abstract: In the Internet of Things (IoT), the routing makes the security over several network attacks as any attacker intrudes routing method for establishing the destructive methods over a network that persist essentiality of security protocols in IoT. Hence, this work develops a secure protocol based on an optimization method, Salp and Particle Swarm Optimization algorithm (S-PSO) that is the hybridization of the Salp-Particle Swarm Optimization approach to provide effectual network security. At first, the effectual nodes are chosen by exploiting the multilayer-Feed Forward Neural Network (FNN) classifier based on factors, like the trust and energy of nodes. The secure nodes engross in routing for that secure multipath is selected optimally exploiting developed S-PSO method that selects secure multipath based on the factors such as energy, and trust. The study of the proposed algorithm in attendance of attacks, like message replicate, black-hole, and DDOS, discloses that the developed algorithm outperforms the conventional algorithms. The developed Salp-PSO protocol obtained the high throughput, energy, and the rate of detection, correspondingly with the least delay.

Keywords: Iot; Attacks; Routing; Security; Energy; Trust; Optimization Algorithm

Nomenclature

Abbreviations	Descriptions
IoT	Internet of Things
p2p	peer-to-peer
CITS	Cooperative Intelligent Transportation Systems
KDE	Key Derivation Encryption
CoAP	Constrained Application Protocol
ECC-HM	Elliptic Curve Cryptography based Hybrid Multiplier Devices
ReLU	Rectified Linear Unit
CNNs	Convolutional Neural Networks
FNNs	Feed-Forward Neural Networks
DDoS	Distributed Denial of Service
FP	Food Place
KDE	Key Derivation Encryption
DTLS	Datagram Transport Layer Security
MBO	Monarch Butterfly optimization
SCOTRES	Self-Channel Observation Trust and Reputation System
LASeR	Lightweight Authentication and Secured Routing

1. Introduction

IoT is a network of a widespread of daily objects, which can produce exchange and exploit information using least human being contribution [23]. These devices differ in their energy, size, calculation power, and storage ability. For instance, IoT objects range from the smart home appliance (for example refrigerators and toasters) to monitor the health products (for example blood pressure monitors and pacemakers), to tiny actuators and sensors. In 2020, it is predictable that regarding a hundred billion IoT devices will attach to the Internet, most important to an 11 trillion-dollar economic force. In the subsequent decade, the power of IoT will not only make more available devices but also much data [1].

There are many protocols and methods to guarantee communication and connectivity among objects in the IoT environment, and ad-hoc mode indicates the most important algorithms [11]. An ad-hoc

https://doi.org/10.46253/jnacs.v3i3.a1

network is an impermanent infrastructure-less peer-to-peer network system, whereas every device gathers, stores processes, and forwards data [23]. In a multihop scenario, a transmitting object exploits other objects as a relay to expand it possesses coverage of transmission. Hence, a device lies on intermediate objects to set up routes and forward packets to their destinations. Ad-hoc networks present multiple benefits like speedy deployment and cost efficiency, flexibility, robustness, and mobility maintenance. Ad-hoc connectivity is enveloping in various IoT exploit scenarios like disaster rescue, environment sensing, e-health, logistics, CITS, battlefield, etc. Also, the ad hoc mode is the important support of 5G deployment modes which can aid in increasing the network's coverage area, assuring services' resiliency, and improving user experience.

An important augment in the exploit of IoT devices is transporting several business chances [7]. Nevertheless, still firms are not capable to assure their customers that these devices are safe [8]. Therefore, despite all of the benefits, security problems of these devices are act as an enormous rock in the method of leasing this instance creation an enormous effect on human lives. Unintended deployment of an extraordinary number of insecure and susceptible IoT nodes requests attackers for performing attacks, like DDoS attack. The extensive scale distribution and the open nature of these devices produces security confronts related using an enterprise of secure communication, authentication privacy, storage, and access control [10]. Thus far, there is perplexity among producers and customers of these devices as they stay on critical each other for vulnerabilities in these devices. In producer's opinion, customers are in charge of not update their devices and for not altering passwords frequently, while customers incessantly criticize manufacturers for not presenting adequate security features in devices themselves [9].

The main contribution of this work is to model and extend a secure routing protocol for IoT via presenting an optimization method. Two parameters are considered such as energy utilization and nodes trust in modeling secure routing protocol. Hence, Salp-Particle swarm-based (Salp-PSO) secure routing is developed. The complete process of the developed secure protocol comprises subsequent 4 steps: Initially, the route trust level is analyzed and subsequently, the multilayer-feed forward layer is used to choose the secure nodes. At first, the node's energy level is calculated, ensued by calculation of trust exploiting several trust factors, such as indirect and direct trust, mutually using a novel trust factor, called active trust that is devised recently on basis of the assured behavior of the nodes. Subsequently, a multilayer-feed forward layer is used for choosing the secure nodes. Once these secure nodes are selected, route selected and the discovery of route is carried out by exploiting the developed Salp-PSO approach.

2. Literature Review

In 2019, Jinbo Xiong et al [1], a new KDE approach that was subsequently exploited to model an SDDK method for IoT devices. At first, a nodal key tree based on flash memory's hierarchical model was designed, and a KDE approach was developed to create data key for make simpler key management and encrypting user's sensitive data. In the meantime, based on KDE, an SDDK strategy was proposed by integrating partial block erasure using a key deletion approach.

In 2019, Farhan Siddiqui et al [2], developed an open-source implementation for CoAP utilizing DTLS to apply secure data transfer among IoT devices. In real IoT testbed, the impact of DTLS on CoAP was examined. By exploiting the open-source software and resource-constrained IoT devices was developed.

In 2020, Badis Hammi et al [3], developed a lightweight and secure routing method that integrates trust management and multipath routing, which can adjust to diverse cases in the IoT environment. Moreover, a probabilistic model was proposed, which contemplates 2 kinds of events that influence the performance of routing for a given node such as mobility and uncooperative behavior to examine and assess the proposed method.

In 2020, Shivi Sharma and Hemraj Saini [4], implemented secure deduplication and task allocation over 4 layers of Fog aided Cluster-based Industrial IoT. To sense data and mitigate security threats, the IoT device layer was exploited. By exploiting the ECC-HM was modeled in this layer and was registered to the cloud server. In the fog layer, SHA-3 was developed for secure data deduplication. Moreover, for data encryption, the ECC HM private key was exploited before transmitted the data. By exploiting Merkle Hash Tree, a layer index was modeled in the cloud.

In 2020, Ankur Lohachab et al [5], worked on the new efforts comprise of re-inventing cryptographic solutions during the exploit of light-weight operations. Nevertheless, after observer the development of quantum computers, it can be incidental that cryptographic approaches based on the mathematical issues were not consistent sufficient. Hence, there was necessitating developing solutions, which can simply oppose the adversarial effects and were appropriate for the post-quantum world.

In 2019, Geetanjali Rathee et al [6], developed a secure Hybrid Industrial IoT mode exploiting the Blockchain method. In more than one country, a hybrid industrial architecture was exploited whereas diverse branches of a company were positioned. Even though IoT devices were exploited in numerous organizations and help in minimizing their production costs besides by means of enhancing quality, numerous threats can happen in IoT devices started by several intruders. Intruders might cooperate with IoT devices with the reason for doing malicious activities.

3 Advanced Secure Route Selection in IoT

In IoT, the selection of the secure route is efficient in order to enable the best communication against the secure routes that is the main objective of this work. Moreover, this work states the selection of a secure route on the basis of the optimization, Salp-PSO which selects the multipath to develop communication. At first, nodes are given to computation of energy and trust that creates input to secure node chosen system that is developed by exploiting the multilayer-FNN in IoT. The input to multilayer-FNN is direct, active trust, and indirect trust, and the energy that is evaluated for each network node and secure nodes, is completed. To tune optimal weights, a multilayer-FNN classifier is utilized and secure nodes require in a secure routing procedure. By exploiting secure nodes, paths are identified that are carried out via fixing a sender and receiver nodes and optimal paths are selected on the basis of the developed algorithm that is fitness-constrained. Fig. 1 exhibits the architecture model of secure routing in IoT. Let us represent an IoT network by means of m number of nodes and consider l^{th} node as, N_l; $(1 \le l \le m)$. The energy and the trust of m nodes are calculated and secure nodes are selected on the basis of multilayer-FNN, total secure nodes are stated as, s therefore $s < m$.

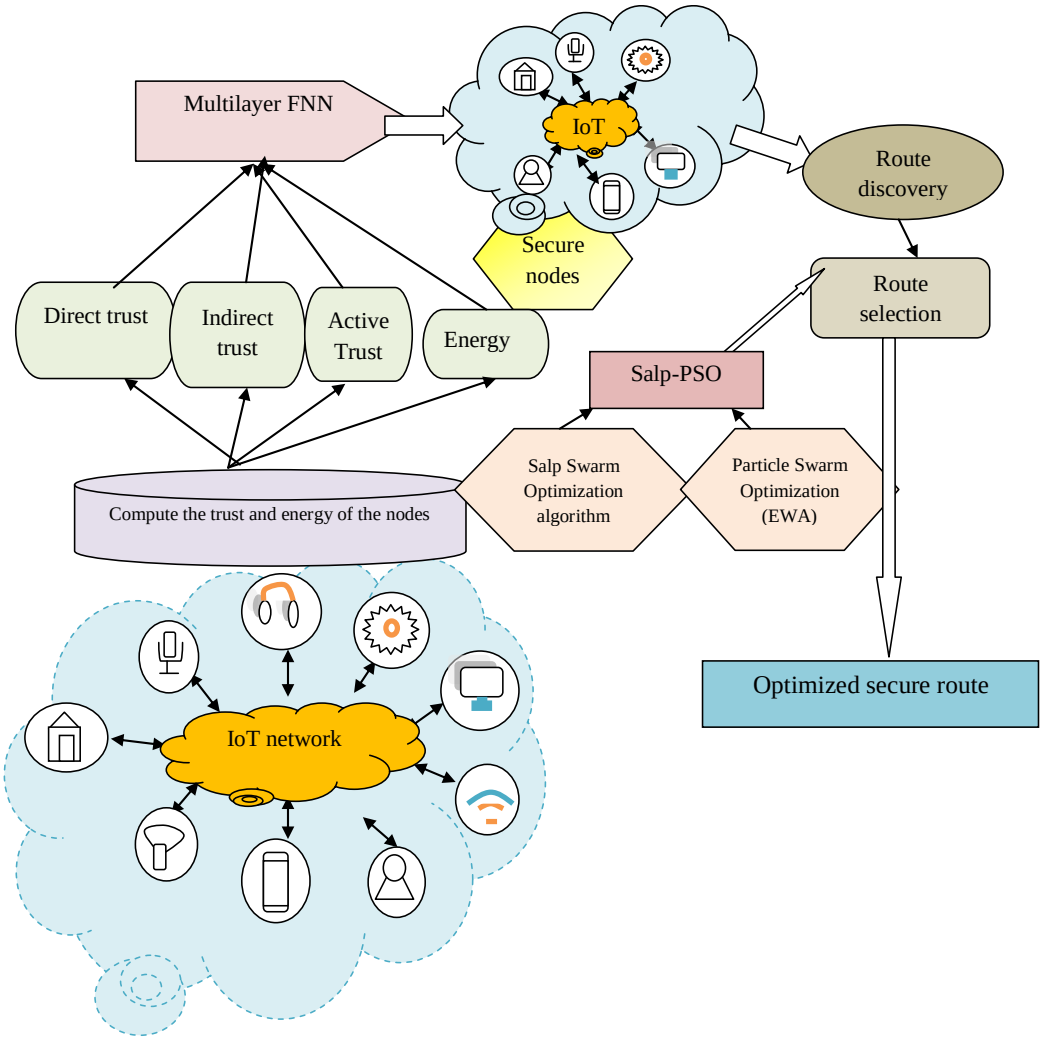


Fig. 1. *Architecture model of the secure routing in IoT*

3.1 Neural Networks for Selection of Secure Node

In IoT, secure nodes need to be determined in order to enable the secure routing that is selected on the basis of the multilayer-FNN for that the trust, and the energy of nodes, needs to determine. Moreover, the nodes with the maximum energy and trust residual in nodes are selected as secure nodes using a multilayer-FNN classifier.

3.1.1 Calculation of Energy and Trust

The energy and trust calculation of the nodes are stated as below:

There are 3 kinds of trust such as direct, indirect, and active trust [12] [13]. Besides the nodes energy is represented for devising the secure nodes.

i) Direct Trust: on account of the fulfillment of a node concerning the target, the node direct trust is calculated. Eq. (1) represents direct trust of l^{th} node based on its occurrence.

$$DT_l = \frac{1}{q}\sum_{\substack{p=1 \\ l\in p}}^{q} W_{lp} \tag{1}$$

In eq. (1), W_{lp} indicates the fulfillment degree of the node l on the basis of the p^{th} neighbors and q indicates the total neighbors of the node l. It is motivating to mention that node l obtains the superior degree of fulfillment when the service offered by a node l is fulfilled by node p and fulfillment degree is based on the fulfilled transaction of the neighboring node p. Hence, a fulfillment degree is offered by a node p to node l based on the winning transactions that are shown in eq. (2). In eq. (2), T_{lp} indicates the accomplishment transactions of total nodes and m indicates total nodes in the IoT network

$$W_{lp} = \frac{T_{lp}}{m} \tag{2}$$

ii) Indirect trust: In contrast with the direct trust, the indirect trust is on the basis of the suggestion of the neighboring nodes, and the indirect trust indicates the trust value of the nodes. The indirect trust of the node l based upon the suggestion of the neighboring node p beside with its neighbors h. Indirect trust is stated in eq. (3), r indicates the total neighbors of l and q indicates the neighbors of p

$$ID_l = \frac{1}{r*q}\sum_{\substack{p=1 \\ l\in p}}^{r}\sum_{\substack{h=1 \\ h\in p}}^{q} sat_{ph} \tag{3}$$

iii) Active Trust: The active trust is calculated on the basis of the data packets transferred and accepted, which is represented in eq. (4).

$$AT = \frac{1}{5}\left(P_1 + P_2 + P_3 + P_4\right) \tag{4}$$

In eq. (4), P_1, P_2, P_3, and P_4 indicates the active trust factors decided based on the data bytes. P_1 indicates the calculation by exploiting the total bytes transferred as stated in eq. (5), b_v indicates the total bytes send effectively and X indicates the total bytes transmitted.

$$P_1 = \frac{b_v}{X} \tag{5}$$

The second factor P_2 is on the basis of the received bytes, and it is shown in eq. (6), b_u indicates the total bytes obtained effectively and Y indicates total bytes obtained by a node.

$$P_2 = \frac{b_u}{Y} \tag{6}$$

P_3 is the third active factor, which is on the basis of the packet received by means of error and it is stated in eq. (7), ε_{rxd} indicates package obtained by error and Y indicates total bytes received.

$$P_3 = \left[1 - \frac{\varepsilon_{rxd}}{Y}\right] \tag{7}$$

The fourth factor P_4 indicates the active trust based on the error packets transmitted as stated in eq. (8), ε_{send} states the total number of error bytes transmitted using nodes.

$$P_4 = \left[1 - \frac{\varepsilon_{send}}{X}\right] \tag{8}$$

iv) IoT nodes energy: The energy is considered as a third parameter [14] of IoT nodes and energy is a necessary module as the sensor nodes in IoT are operating using energy-constrained batteries that maintain on the detail of energy conservation of nodes to increase network lifespan.

Consider, E_0 as IoT node initial energy. During communication, when the transferred data is obtained by recipient data-loss arises and this loss is considered as on the basis of the nodal features and broadcast distance among nodes in IoT. In network, the routing protocol permits broadcast and dissipation of energy is because of the occurrence of radio electronics and power amplifier in the transmitter. In a node, the energy dissipation at the time of the data packet transmission is formulated as stated in eq. (9).

$$E_{dis}(N_l) = E_{elc} \times B_l + E_{pa} \times B_l \times \left\| N_l - C_g \right\|^4 \text{ if } \left\| N_l - C_g \right\| \geq \eta_0 \quad (9)$$

In eq. (9), $E_{dis}(N_l)$ indicates the energy dissipation and E_{elc} indicates the electronic energy of l^{th} node. B_l indicates the total bytes transmitted from l^{th} node, and E_{pa} indicates the energy, which is similar to the power amplifier in attendance with transmitter. The parameter η_0 is based upon the energy dissipation and it is calculated on the basis of the evaluation amid the distance among the g^{th} head and parameter η_0 and l^{th} sensor node. In particular, while the distance among the l^{th} node N_l regarding the CH C_g remnants under η_0. In a normal sensor node, the energy dissipation is updated by exploiting the eq. (9) otherwise, the energy dissipation in N_l is computed by exploiting the eq. (10). $\left\| N_l - C_g \right\|$ indicates the distance among the g^{th} cluster head and l^{th} node.

$$E_{dis}(N_l) = E_{elc} \times B_l + E_{fs} \times B_l \times \left\| N_l - C_g \right\|^2 ; \text{if } \left\| N_l - C_g \right\| < \eta_0 \quad (10)$$

$$L = \sqrt{\frac{E_{fs}}{E_{pa}}} \quad (11)$$

In the free space, E_{fs} indicates the energy in eq. (11). The electrical energy is based upon the coding, modulation, filtering, etc, similar to the data aggregation and transmitter, and it is indicated in eq. (12).

$$E_{elec} = E_{tx} + E_{agg} \quad (12)$$

In eq. (12), E_{agg} indicates the energy equivalent to the data aggregation and E_{tx} indicates the transmitter energy. It is significant to state that when a normal node N_l in the environment tries to communicate by means of C_g, energy-loss happens in cluster head and this energy loss based upon the electrical energy accessible at receiver side and in addition, on the data bytes obtained at the cluster head. Eq. (13) represents the dissipation of energy at g^{th} CH.

$$E_{dis}(C_g) = E_{elec} \times B_l \quad (13)$$

Ahead of the conclusion of the communication, sensor nodes, and cluster heads occupied in broadcast and receiver, updates its energy and the eq. (14) and (15) states the energy dissipated at nodes.

$$E_{t+1}(N_l) = E_t(N_l) - E_{dis}(N_l) \quad (14)$$

$$E_{t+1}(C_g) = E_t(C_g) - E_{dis}(C_g) \quad (15)$$

In eq. (14), $E_t(C_g)$ indicates the accessible energy in the node at a time t, $E_{t+1}(C_g)$ indicates the updated energy of the CH, and $E_{dis}(C_g)$ indicates the dissipation of energy in the cluster head or the receiver at the time of obtaining data packets from the normal node.

Similarly, $E_t(N_l)$ indicates the earlier accessible energy in normal node, $E_{t+1}(N_l)$ indicates the updated energy of normal node, and $E_{dis}(N_l)$ indicates the dissipated energy in normal nodes at the time of transmission. In nodes, the energy, and cluster heads, persist till the node is deceased with "0" energy.

3.2 Multilayer FNN for Finding The Secure Nodes

The multilayer-FNN model is used to determine the secure nodes by exploiting the energy, direct trust, active trust, and indirect nodes' trust in the environment. The need for facilitating the secure routing in IoT persevered to assess energy and the trust of all nodes and lead to chosen of the nodes by means of the maximum value of trust and energy.

In multilayer- FNNs, former layer neurons are fully linked to the ensuing layer, whereas no intra-layer associations are set up [16]. FNNs were widely used in image classification, scene labeling trend prediction, and other tasks. Currently, one more the majority well-liked application of FNNs is represented as concluding CNN's output layer, whereas high-level feature extraction is attained via pooling, convolutional, and normalization layers. In existing FNNs, otherwise called rate-based FNNs, neurons represent linear static units that openly summation of weighted input signals from the preceding layer and get ahead of attained value to the subsequent layer.

For many application issues, activation functions for softmax and ReLU were extensively exploited in the output layer for intermediary feature processing in hidden layers, correspondingly. In [15] developed that the stage function ReLUs very much faster the stochastic gradient descent convergence evaluated to sigmoid/tanh functions because of its linear, non-saturating model. In addition to taking into consideration, the improvement of ReLUs in order to calculate performance in order to determine the secure nodes by exploiting the energy, direct trust, active trust, and indirect trust of nodes, ReLUs in networks at the time of the training process. A characteristic mathematical formulation is stated in (16).

$$y_i = \max\left(0, \sum_j w_{ij} y_j\right) \tag{16}$$

In eq. (16), y_i indicates the unit activation i, w_{ij} indicates weight linking unit j in the preceding layer to unit i in the present layer, and y_j indicates unit activation j in the previous layer.

The Multilayer-FNN has various neurons modeled in layers namely input, hidden and output layers shown in Fig. 2. The output layer considers additional numerous neurons present output for additional numerous inputs. In one neuron instance, the training process undergoes to discover appropriate weights for neuron connections that in amalgamation by means of inputs, attains preferred output. This procedure is achieved using the backpropagation model [17].

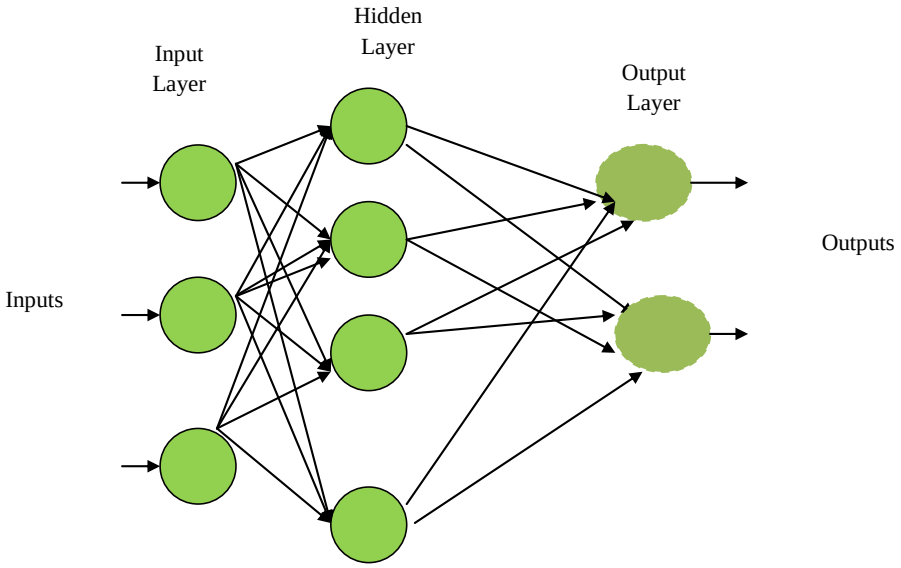


Fig. 2. *Diagrammatic representation of the Multi-layer FNN model*

4. By the Developed Salp-PSO Algorithm for Optimal Multipath Selection

In this section, steps to choose multipath by exploiting secure nodes, and it is determined by employing multilayer FNN and an optimal selection of multipath is performed via the developed Salp-PSO are presented. At first, all probable paths are identified by exploiting the Dijkstra shortest path method and the optimal multipath is determined on the basis of the developed Salp-PSO utilizing the fitness constraints like energy, trust, and the distance of the secure nodes.

4.1 Route Discovery

The probable paths are produced via arbitrarily fixing the sender and receiver nodes for the chosen of the optimal multipath. A total of n paths are produced via fixed sender and receiver nodes for the creation of paths, the least distance among the sender and receiver is considered. Hence, on the basis of minimum distance, the paths are created that are chosen on the basis of the fitness constraints using the Salp-PSO algorithm.

4.2 PSO Algorithm

PSO is easy and a competent population-based optimization algorithm [18]. The algorithm's main objective is to discover the global optimal solutions by exploiting community communication of group and self occurrence elements. In PSO, each iteration comprises updated particles via a velocity that is updated by inertia, group and self-experience movements.

This algorithm is learned from the animal's behavior to compute the global optimization functions/issues, each partner of swarm/crowd is known as a particle. In the PSO method, the location of every partner of the crowd in the global search space is updated using two mathematical formulations.

$$u_i^{k+1} = u_i^k + c_1 r_1 \left(p_i^k - y_i^k\right) + c_2 r_2 \left(g_{best} - y_i^k\right) \tag{17}$$

$$y_i^{k+1} = y_i^k + u_i^{k+1} \tag{18}$$

4.3 Salp Swarm Optimization (SSO) Algorithm

Salp swarming approach is the most important motivation to construct SSA [19]. For the number of control variables N, the salp position is decided in N dimensional space of searching. As a result, salp positions are stored in a matrix by means of 2 dimensions called Yl. The FP represents the objective of salp swarms. The most important steps of SSO are described as below:

(a) Initialize the SSO population in allowable restrictions.

(b) For the initial locations, the computation of the fitness function is performed.

(c) Update location of salps: In this algorithm, the salps population initiates at arbitrary locations in the search domain. The length of the salp is equivalent to several control variables. Subsequently, the locations of salps are performed as below:

$$Yl_i^1 = \begin{bmatrix} FP_i + r_1\left(r_2\left(V_i - L_i\right) + L_i\right) & r_3 \geq 0 \\ FP_i + r_1\left(r_2\left(V_i - L_i\right) + L_i\right) & r_3 \geq 0 \end{bmatrix} \tag{19}$$

The above formulation is extremely used to salps target FP and it indicates optimal food source. The controlling parameter c_3 balances among exploitation and exploration around salps target.

$$r_3 = 2e^{-\left(\frac{4t}{T}\right)} \tag{20}$$

Finlay, location of j^{th} salp is updated as below:

$$Yl_i^t = \frac{1}{2}\left(Yl_i^t + Yl_i^{t-1}\right), \; t > 2 \tag{21}$$

(d) Ensure the constraints.

(e) Do again the preceding steps until the halting criterion is attained. Here, the halting condition is considered as the utmost iteration number.

4.4 Proposed Salp- PSO Algorithm

The flow chart of the hybrid Salp-PSO algorithm is exhibited in Fig. 3. The most important characteristic of this hybridization is the capability to evade drawbacks associated with the PSO method and to employ the benefit of SSO technique. The hybridization method is initiated by the arbitrary population initialization. Subsequently, by the PSO method, the population is updated and the best solution is chosen. The chosen solutions are sophisticated and updated using the SSO algorithm. The better solution is chosen and subjected to the subsequent iteration. This procedure is sophisticated until any halting condition is fulfilled.

5. Result and Discussion

5.1 Experimental Procedure

In this section, outcomes of the developed Salp-PSO model and performance evaluation of conventional techniques to disclose the efficiency of the protocol was presented.

The experimentation of IoT was performed in MATLAB by means of various parameters such as simulation area, energy, number of nodes, mobility and propagation model. The algorithms exploited for comparison such as MBO [20], LASeR [21], and SCOTRES [22] that was evaluated with the developed algorithm to reveal the competence of developed technique of secure routing.

5.2 Performance Analysis

In this section, the analysis of algorithms in attendance of attacks and values for energy, rate of detection, delay, and throughput, is envisaged at the end of the iteration.

Fig 4 states the analysis of developed and conventional techniques concerning energy and delay. It is comprehensible that the delay of the developed algorithm is less and energy is high when compared with the conventional models from Fig 4. Fig 5 states the analysis of developed and conventional models

concerning the rate of detection and throughput. It is comprehensible from Fig 4 that both the rate of detection and of the developed algorithm is high when compared with the conventional models.

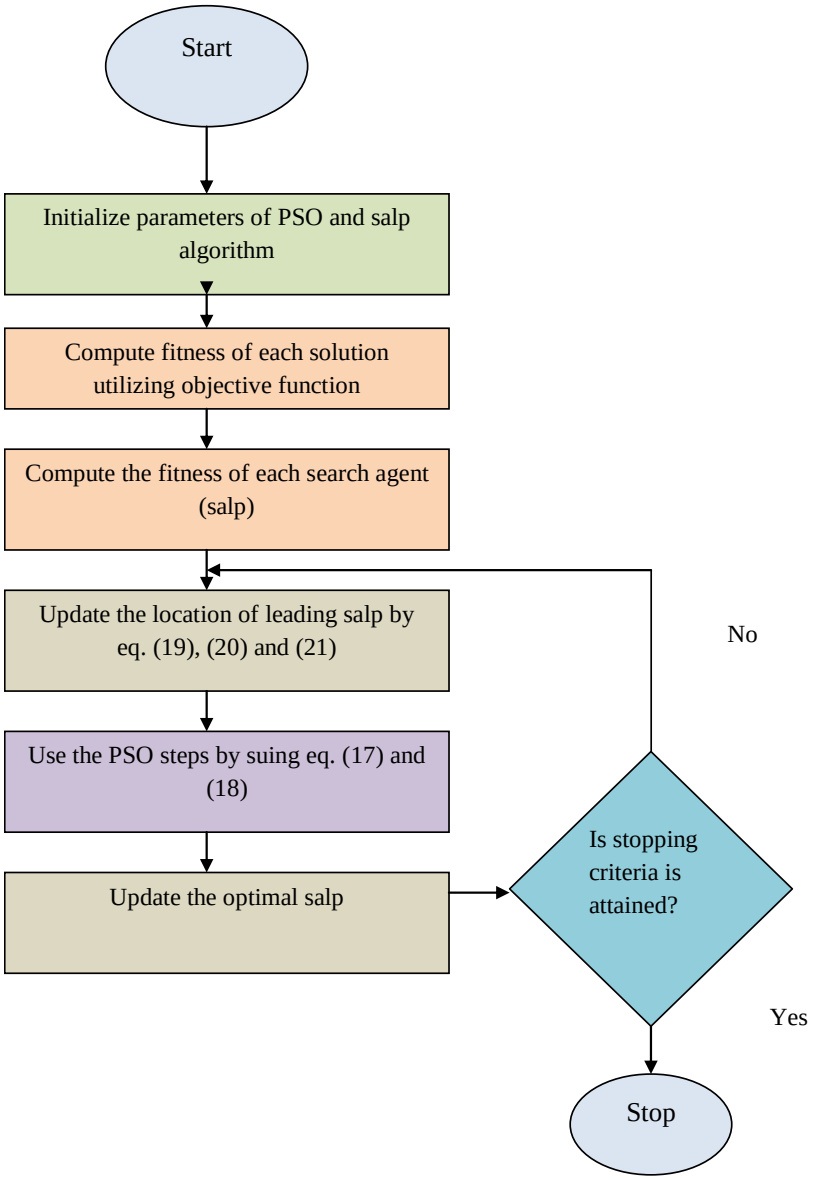


Fig. 3. *Flowchart of the proposed Salp-PSO model*

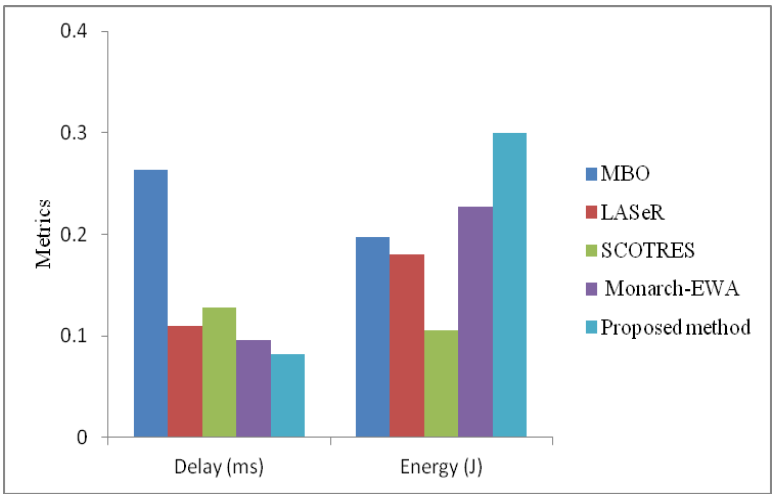


Fig. 4. *Analysis of developed and conventional techniques concerning delay and energy*

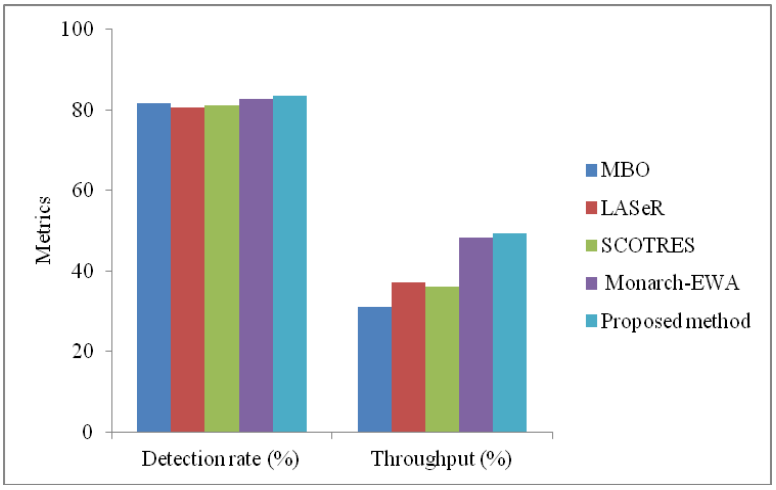


Fig. 5. *Analysis of developed and conventional techniques concerning detection rate and throughput*

6. Conclusion

In IoT the secure routing is done by exploiting the secure routing protocol, Salp-PSO that was the incorporation of the Salp with PSO therefore that energy, and throughput of nodes, was not affected even in attendance of attacks. The rate of attacker exposure was found to be enhanced for the developed algorithm by means of improved performance. In the network, to facilitate security, energy, and the trust of nodes, was calculated and secure nodes were selected by exploiting the multilayer-FNN method. In the multipath routing, the secure nodes were concerned for that the optimal multipath was selected based on the developed Salp-PSO by exploiting the constraints, like distance, energy, and nodes trust in path, it is considered significant to employ any path generation method for that Dijkstra shortest path method was exploited. Hence, the paths created by exploiting the Dijkstra shortest path method were optimally selected employing the developed method to enables secure routing in the network. The experimentation of IoT network shows that developed algorithm outperforms conventional algorithms by means of maximum throughput, energy, and the rate of detection and the least delay.

References

[1] Jinbo Xiong, Lei Chen, Md Zakirul Alam Bhuiyan, Chunjie Cao, Ximeng Liu,"A secure data deletion scheme for IoT devices through key derivation encryption and data analysis",Future Generation Computer Systems, 2 November 2019.

[2] Farhan Siddiqui, Jake Beley, Sherali Zeadally, Grant Braught,"Secure and lightweight communication in heterogeneous IoT environments", Internet of Things, September 2019.

[3] Badis Hammi, Sherali Zeadally, Houda Labiod, Rida Khatoun, Lyes Khoukhi,"A Secure Multipath Reactive Protocol for Routing in IoT and HANETs", Ad Hoc NetworksIn press, journal pre-proof,Available online 28 February 2020.

[4] Shivi Sharma, Hemraj Saini,"Fog assisted task allocation and secure deduplication using 2FBO2 and MoWo in cluster-based industrial IoT (IIoT)",Computer Communications, Volume 15215, Pages 187-199, February 2020.

[5] Ankur Lohachab, Anu Lohachab, Ajay Jangra,"A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks", Internet of Things, Volume 9, March 2020.

[6] Geetanjali Rathee, Ashutosh Sharma, Rajiv Kumar, Razi Iqbal,"A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology", Ad Hoc Networks,Volume 94, Nov. 2019.

[7] R. K. Lenka, A. K. Rath and S. Sharma, "Building Reliable Routing Infrastructure for Green IoT Network," IEEE Access, volume. 7, page no. 129892-129909, 2019.

[8] T. D. Nguyen, J. Y. Khan and D. T. Ngo, "A Distributed Energy-Harvesting-Aware Routing Algorithm for Heterogeneous IoT Networks," IEEE Transactions on Green Communications and Networking, volume. 2, number. 4, page no. 1115-1127, December. 2018.

[9] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, K. Saleem and S. A. Kozlov, "Improving the Performance of LOADng Routing Protocol in Mobile IoT Scenarios," IEEE Access, volume. 7, page no. 107032-107046, 2019.

[10] J. Lin, P. R. Chelliah, M. Hsu and J. Hou, "Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling," IEEE Access, volume. 7, page no. 14022-14034, 2019.

[11] T. A. Al-Janabi and H. S. Al-Raweshidy, "A Centralized Routing Protocol With a Scheduled Mobile Sink-Based AI for Large Scale I-IoT," IEEE Sensors Journal, volume. 18, no. 24, page no. 10248-10261, 15 Dec.15, 2018.

[12] Dhumane, A., Prasad, R and Prasad, J.: 'Routing issues in internet of things: a survey', In Proceedings of the international multiconference of engineers and computer scientists,1, page no: 16-18, 2016.

[13] Wang, B., Chen, X and Chang, W.: 'A Light-weight Trust-based QoS Routing Algorithm for Ad Hoc Networks', Pervasive and Mobile Computing,13,page no: 164-180, 2014.
[14] Yang, J and Yang, G.: 'Modified Convolutional Neural Network Based on Dropout and the Stochastic Gradient Descent Optimizer', 2018,11,(3).
[15] V. Nair , G.E. Hinton , Rectified linear units improve restricted Boltzmann ma- chines, in: Proceedings of International Conference on Machine Learning, page no. 26–30, 2010 .
[16] S. J. Russell and P. Norvig, "Artificial intelligence: A modern approach (international edition)", Pearson US Imports & PHIPEs, Nov.2002.
[17] S. Haykin., "Neural networks: A comprehensive fundation", McMMillan, New York, 1994.
[18] Mingquan Zhang, Xiaorong Cheng, Huawei Mei and Jujie Zhang, "Research of routing optimization based on improved PSO algorithm in power communication network," International Conference on Electric Information and Control Engineering, Wuhan, page no. 2494-2497, 2011.
[19] B. Xiao, R. Wang, Y. Xu, W. Song, J. Wang and Y. Wu, "Salp swarm algorithm based on particle-best," IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, pp. 1383-1387, China, 2019.
[20] Hashemi, S.M and He, J.: 'LA-Based Approach for IoT Security,' Journal of Robotics, Networking and Artificial Life, 2017, 3, (4), pp: 240-248.
[21] Shah, S.B., Chen, Z., Yin, F., Khan, I.U and Ahmad, N.: 'Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks, Future Generation Computer Systems, 2018,81, pp: 372-381.
[22] Huia, T.K.L., Sherratt, R.S and Sánchez, D.D.: 'Major requirements for building Smart Homes in mart Cities based on Internet of Things technologies', Future Generation Computer Systems, 2017, 76, page no: 358-369.
[23] Moresh Madhukar Mukhedkar,Uttam Kolekar,"Hybrid PSGWO Algorithm for Trust-Based Secure Routing in MANET",Journal of Networking and Communication Systems (JNACS), Volume 2, Issue 3, July 2019.
[24] Praveen Kumar Reddy. M,Rajasekhara Babu M,"Cluster Head Selection in IoT Using Enhanced Self Adaptive Bat Algorithm", Journal of Networking and Communication Systems (JNACS), Volume 2, Issue 4, October 2019.