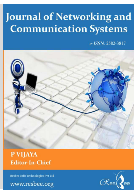
Vol.2 No.2 April 2019

Journal of Networking and Communication Systems

Received 12 December, Revised 28 February, Accepted 20 March



Chaotic based Hybrid Artificial Sheep Algorithm - Particle Swarm Optimization for Energy and Secure Aware in WSN

Fatema Murshid AlBalushi

Department of Logistics and Transport Management, International Maritime College Oman, Suhar OM, 332, Oman
fatemamurshidalbalushi@gmail.com

Abstract: The development of Wireless Sensor Network (WSN) in a huge number of applications has done it widespread. Nevertheless, energy is considered as the most important confront in the WSN environment which is represented as the battery-operated Sensor Network (SN) in the network utilizes a massive quantity of energy transmission. Moreover, this paper tackles energy problems and presents energy effectual multi-hop routing in WSN called Chaotic based Hybrid Artificial Sheep Algorithm (ASA) and Particle Swarm Optimization (PSO). This algorithm experiences 2 phases for obtaining multi-hop routing that comprises CHS, and data transmission. At first, the energy-efficient Cluster Heads (CHs) are chosen by exploiting the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol in order to effectual data transmission, the SNs transmits data through the CH that sends data to the Base Station (BS) via chosen optimal hop. The selection of optimal hop is performed by exploiting the developed Chaotic Hybrid ASA-PSO algorithm. In addition, the multi-hop security-aware routing is done through developing a trust model which included integrity factor, indirect trust, data forwarding rate and direct trust. The developed Chaotic based Hybrid ASA-PSO method shows optimal performance with respect to the energy, throughput, delay, and, number of alive nodes correspondingly.

Keywords: CHS; WSN; Energy; Optimization Methods; Trust; LEACH

Nomenclature

Abbreviations	Descriptions
CHS	Cluster Head Selection
SRPMA	Secure Routing Protocol based on Multi-objective ACO
ITS	Intelligent Transportation Systems
BS	Base Station
BOA	Bat Optimization Algorithm
CWSNs	Cognitive WSN
IIoT	Industrial Internet-of-the things
MOFPL	Multi-objective Fractional Particle Lion Algorithm
WSN	Wireless sensor networks
ACO	Ant Colony Optimization
SEMCL	SEMantic CLustering
SN	Sensor Nodes
REWLS	Robust and Efficient Weighted Least Square method
QoS	Quality of Service
TOD	True Outlier Detection
PSO	Particle Swarm Optimization
LEACH	Low Energy Adaptive Clustering Hierarchy
ASA	Artificial Sheep Algorithm

1. Introduction

In recent years, WSN [1] has an extensive application for instance healthcare, military, agriculture, and smart buildings. Generally, WSN is intermediate to large networks, which utilize contemptible wireless SNs that have abilities to intellect, process, and distribute data gathered from the environment by exploiting mutual methods between nodes. The most important benefits of WSN have distributed intelligence and minimum cost. The operating cost of their maintenance and installation is minimized as they employ not expensive devices that need no wiring. WSN distributed intelligence might facilitate the advance of diverse applications aiding real-time traffic safety. Nevertheless, the most important

https://doi.org/10.46253/jnacs.v2i2.a5

confronts are that the routing method in WSN can be damaged that may affect permanent loss because of a diversity of network attacks [2].

During the wireless communication medium, phrase routing describes the technique of transmitting packets among the base station and the SNs the WSN. At the time of routing of the nodes, the most important confront is the contemplation of every SNs energy in the WSN [5] [6]. Each sensor nodes the WSN network lifetime is directly based upon energy. Hence, routing protocol requires assuring an enhanced lifetime of the network for the WSN at the time of the competent routing of nodes. In the WSN nodes, energy is minimized because of the sender and the receiver of message packets. For routing nodes the routing protocols exploited which can be classified based on the network parameters, like the contribution of every node in the WSN, operational method of the nodes, a diversity of clustering models, and the network topology. For the WSN the routing protocol design directly based upon the factors, like scalability, energy utilization, node deployment, coverage, connectivity, security [18].

In Cluster-based WSN [4], security is a necessary and demanding problem as sensors are typically positioned in hostile environments. The conventional security technique might not be used for WSN because of its features, for example being the inadequate computational capability of nodes, an open communication medium, and the drawbacks of bandwidth constraints that construct these networks additionally vulnerable to malevolent attacks than conventional networks [19].

In different network layers, secure routing, data encryption, and malicious detection methods are conventional countermeasures for attacks. The novel necessary privacy and security level entails the employ of demanding algorithms and methods that should pretense satisfactory performance load on minimum resources nodes therefore unconstructively effect on the whole communication effectiveness [3].

The main contributions of the work are to propose a Chaotic Hybrid ASA-PSO method that is necessary for the effectual position of the hops to advancement multihop routing. The developed model is attained via the addition of the Chaotic Hybrid ASA-PSO method that is the incorporation of the ASA and PSO in order to determine the optimal hops to carry out multi-hop routing in WSN. The multihop security-aware routing is formulated via a comprising trust model in the fitness model. Hence, multihop routing is developed by exploiting developed Chaotic Hybrid ASA-PSO fitness model.

2. Literature Review

In 2019, Ziwen Sun et al [1], presented an SRPMA for WSN. The ACO method was enhanced to a multi-objective routing method with taking into consideration of the remaining energy of nodes and the rout path trust value as 2 optimization aims, in that a route path was created using the multi pheromone information and the multi heuristic information comprising two objective models. The node trust estimate technique was recognized exploiting an enhanced D-S substantiation theory with confliction preprocessing to assess nodes' trust degree. The outcome of multi-objective routing was attained through the Pareto optimal solution method utilizing the external archive technique with a crowding distance principle. In 2018, Tarek Gaber et al [2], developed a bio-inspired and trust-based CHS technique for WSN used in ITS techniques. A trust model was considered and exploited to calculate a trust level for every node and BOA was employed to choose CHS based on three parameters such as trust value, remaining energy, and the number of neighbors. In 2019, Elena Romero et al [3] developed a new artificial noise-making approach based on game theory to enhance security over the privacy attacks in CWSNs. To facade, the real information artificial noise generation comprises developing intrusions in the spectrum. The decision if or not to set up artificial noise was designed at the time of a light non-cooperative game modeled for minimum-resources networks that balance energy utilization and security improvement. In 2019, Shishupal Kumar et al [4], worked on the maximum scalability using the aid of a great number of Internet users using the procedure of IPv6 rather than IPv4. Moreover, it was necessary that operational components and protocols to be energy competent. The cause was, a deployed sensor lifetime was directly associated with its draining diminutive-term battery. After this point into the description, a variety of protocols were used and experimented with IIoT based on the WSN. Even though, these all do not present acceptable performance with respect to the suitable data rate. In 2019, Reeta Bhardwaj and Dinesh Kumar [5], developed the multi-objective fitness model based on the delay, energy, distance, traffic rate, and the density of the cluster. The energy-aware routing was performed based on the developed MOFPL. In the WSN, the developed MOFPL method discovers the optimal CH from diverse CH nodes. Subsequently, the best routing path was recognized based on the developed multi-objective model. In 2019, Srijit Chowdhury et al [6], worked an energy competent SEMCL design to alleviate maximum energy utilization problems in a clustered WSN. The proposed method creates energy competent clusters using strong intra-cluster data comparison to use the data spatial correlation. Moreover, they adopted the REWLS to present precise data prediction with insignificant errors. Since the REWLS technique was short in order to distinguish factual and fake outliers therefore to advance additional the QoS on data accurateness. Moreover, a detach method, called, TOD was proposed.

3. Proposed Chaotic based Hybrid ASA-PSO for Multihop Routing

In WSN the multi-hop security-aware routing protocol based on the multiple objectives is demonstrated by exploiting novel optimization methods in this section. Here, a trust model is used by taking into consideration of several trust factors, like indirect trust, integrating factor, direct trust, and forward rate factors beside with other parameters, that includes delay, intra , and inter-cluster distance, distance, energy, and link lifetime. The trust model is comprises to contribute the maximum network security. Subsequently, the multi-hop routing is done using developed Chaotic Hybrid ASA-PSO. The developed Hybrid ASA-PSO and the multi objectives are exploited to carry out the multi-hop security-aware routing in WSN. For multi-hop routing, the two phases are represented. Initially, CH is chosen by exploiting the LEACH [7] protocol to attain the best CH through the maximum energy. Subsequently, the next phase is developed using the chosen of best hops by exploiting the developed algorithm based on the formulated multi-objectives. Fig.1 demonstrates the architecture model of a multi-hop routing developed algorithm.

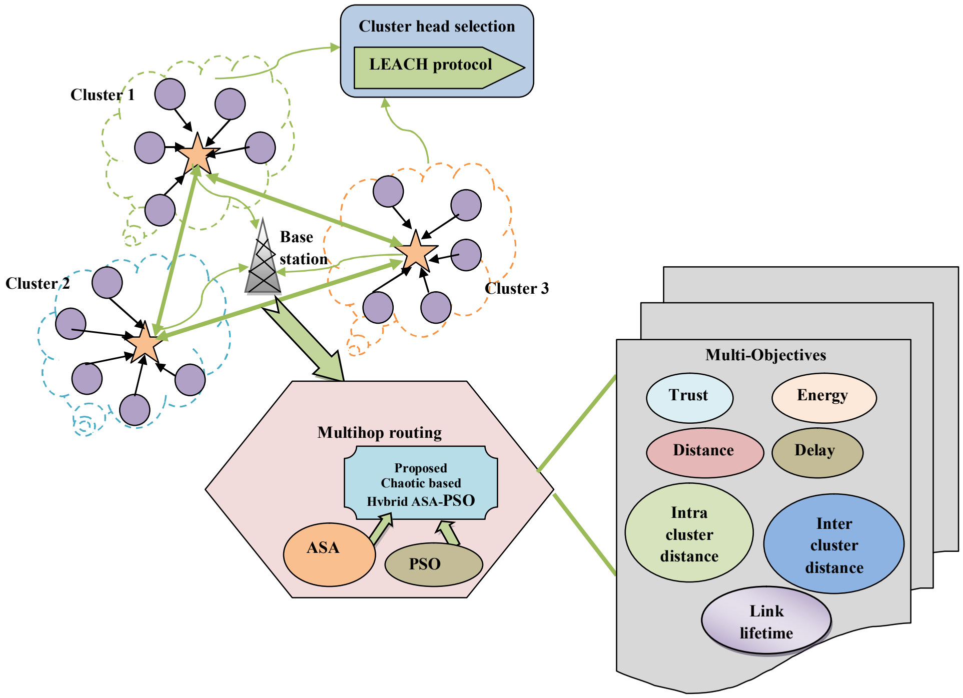


Fig. 1. *Architecture model of multihop routing using the proposed algorithm*

3.1 CHS using LEACH Protocol

The LEACH protocol [7] contemplates a dense sensor network comprising nodes with equal energy, whose task is to send the data to BS. Hence, an optimal cluster head is selected in order to collect and broadcast the data to the base station. In a few scenarios, the base station is positioned in distance, and therefore, the cluster head needs high energy for transmission. Hence, LEACH should choose a cluster head so that the chosen node pretenses superior energy. Hence, the LEACH protocol exploits an arbitrary number of rotations of cluster head for consistently dealing out with the energy between sensors. Moreover, LEACH protocol is set accurately, and once an optimal percentage of CH is decided, subsequently LEACHES protocol carried on in $\frac{1}{g}$ rounds. For every round, a cluster of Cluster Head is decided with size hg, where h indicates the total count of rounds. Here, each round comprises a set-up and steady-state stage. The setup stage comprises three sub-stage that comprises cluster setup, advertisement, and broadcast schedule substage. The advertisement stage is carried on as follows: every node h creates an arbitrary number in the range 0 and 1 and evaluates it with the predefined threshold. The eq. (1) states the threshold,

$$Q(h)=\begin{cases}\dfrac{g}{1-g\times(c \bmod \frac{1}{g})} & ;\text{if } e\in\alpha \\ 0 & ;\text{Otherwise}\end{cases} \tag{1}$$

In eq (1), α indicates the node which is not at all been a cluster head, c denotes update time of current topology, and g indicate cluster head percentage. Hence, the nodes which create a result to be a cluster head notify its neighbor through an advertisement packet. In the cluster system stage, every other node in attendance in the network responds to the cluster head advertisement to notify their decisions. The responses of every node are collected for deciding the membership of the exacting cluster in the broadcast stage. Moreover, the cluster head creates a Time Division Multiple Access schedules based on the total nodes in the cluster. This schedule hits a chord between nodes relating to time with broadcast the message in an exact time. In conclusion, for transferring data, the data are gathered in the cluster head, and subsequently, the attained data is transmitted to the base station. Moreover, the node transfers the data to its cluster head and the cluster head then transmits to BS. Hence, the LEACH protocol is exploited for choosing the optimal cluster head based on the energy parameter. For this reason, the cluster head created using the LEACH protocol and is stated in eq. (2).

$$G=\{G_1,G_2,\cdots,G_t,\cdots,G_n\}\ ;1\le t\le n \tag{2}$$

In eq. (2), n indicates the total cluster head by exploiting the LEACH protocol.

3.2 Multihop Routing Using the Proposed Method

In WSN, the multihop routing has optimized the communication over the network. Generally, the multi-hop routing is used for the effectual transmission of the data. Nevertheless, energy is the most important limitation in multi-hop routing. Hecnce, in order to solve the problems of energy, the developed Chaotic Hybrid ASA-PSO uses multihop routing in that the source node sends its data to the cluster head via the transitional nodes within every cluster. Moreover, every source node in the cluster transmits its data to the neighbor node to minimize the transmission energy. Moreover, the developed Chaotic Hybrid ASA-PSO derives the best hops based on the recently formulated fitness model for succeeding in the routing in WSN.

By exploiting the developed method, the solution encoding is the depiction of the solution is decided. Moreover, the solution is the optimal route chosen in order to transmit the data. The optimization algorithms exploit the developed method based on the recently formulated multi-objective fitness model in order to find the optimal hop from the location of hops in attendance in the WSN. The hops are the selected cluster head which can present effectual routing in the network by minimizing the information loss which happened during the transmission. Moreover, the developed method is modified in order to determine the optimal path from the source node.

3.3 Objective Model

The fitness model is computed to discover the best solution from a solution by exploiting parameters set. The fitness calculated for the developed model exploits 7 parameters, such as energy, trust model, distance, inter-cluster – intra cluster distances, link lifetime, and delay. Moreover, fitness is represented as a maximization function. Hence, for the routing, the solution producing the utmost trust, link lifetime, intra-cluster distance energy, minimum delay, and inter-cluster distance is exploited. Moreover, the solution offering utmost fitness value is contemplated for multi-hop routing. Eq. (3) indicates the fitness model of the developed algorithm.

$$O=Wt_1\times P+Wt_2\times(1-T)+Wt_3\times\left(1-X^*\right)+Wt_4\times X+Wt_5\times(1-D)+Wt_6\times M+Wt_7\times K \tag{3}$$

In eq. (3), Wt_1, Wt_2, Wt_3, Wt_4, Wt_5, Wt_6 and Wt_7 indicates the weights calculated by exploiting the fuzzy membership function [8]. P states the energy of the node's, T sates delay transmission, D states the distance among two hops, X^* states the inter-cluster distance, X states the intra-cluster distance and M indicates the link-time, and K states the trust model. Eq. (4) denotes the computation of weight.

$$W=\begin{cases}0\ ; \text{if } r<f \\ \dfrac{r-f}{1-f}\ ;\text{if } f\le n\le m \\ \dfrac{m-n}{m-1};\ \text{if } 1\le n\le m \\ 0\ ; \text{if } n\ge m\end{cases} \tag{4}$$

In eq. (4), $l, m,$ and n indicate the triangular vertices membership function $T(f)$. Moreover, $l, m,$ and n represents the lower, medium, and upper boundary, the medium boundary with the value of membership value 1 and the upper boundary with the value of membership 0.

a) Energy: The energy of the network is described as the summing up of the energies for every hops that states the energy stayed in the nodes. The energy should states a maximum value as well it is stated in eq. (5). In eq. (5), b indicates the number of hops that are included in multihop routing, and $E(J_k)$ indicates the energy of the h^{th} hop.

$$L = \frac{1}{b}\sum_{h=1}^{b} E(J_h) \tag{5}$$

b) Delay: By exploiting the hops the delay is calculated that include in routing and the delay must be minimum for doing effective routing. It is calculated as the ratio of hops required for the routing entire nodes comprised in WSN and it is devised as eq. (6). In eq. (6), b denotes the total count of hops required for the routing, and p indicates the total nodes available in WSN.

$$T = \frac{b}{p} \tag{6}$$

c) Intra-cluster distance: It is calculated based on summing up of distances among the individual nodes and hop the available in the least hop. Suppose the intra-cluster distance is least, subsequently the nodes are nearer to the hop therefore information loss, and energy, is least. The eq. (7) is used for the calculation of intra-cluster distance. In eq. (7), $X(J_h, L_t)$ indicate the distance among the h^{th} hop, β states the regularization factor, and t^{th} node, the total nodes, and are indicated as s.

$$X = \frac{1}{b}\left(\frac{\sum_{k=1}^{b}\sum_{t=1}^{s} X(J_k, L_t)}{\beta}\right) \tag{7}$$

d) Inter-cluster distance: The distance ratio is calculated among 2 clusters is called as inter-cluster distance and it should be high for presenting the effectual routing. Eq. (8) represents the procedure of inter-cluster distance. In eq. (8), $X(G_x, G_t)$ indicate distance among 2 clusters, and n indicates the total CH.

$$X^* = \left(\frac{\sum_{x=1}^{n}\sum_{t=1}^{n} X(G_x, G_t)}{\beta}\right) \tag{8}$$

e) Distance: Eq. (9) represents the summing up of the distance calculated among the two hops. The distance must be least for multi-hop routing.

$$D = \frac{1}{b}\times\left(\frac{\sum_{h=1}^{b-1} X(J_h, J_{h+1})}{\beta}\right) \tag{9}$$

f) Link Lifetime: The network lifetime is resultant from the lifetime of the link and it must be maximum to obtain effectual routing. Eq. (10) indicates the link, $M(J_k, J_{k+1})$ indicates the lifetime of the link of the $(k+1)^{th}$ hop and k^{th} hop.

$$M = \frac{1}{b}\times\sum_{k=1}^{b-1}\frac{M(J_k, J_{k+1})}{\beta} \tag{10}$$

g) Trust model: It [9] [10] presents security in the developed model at the time of the routing process. The computation model of the trust is exploited for calculating the agents' trust in attendance of apprehensive behaviour. Numerous parameters are used for calculating the trust that includes indirect trust, direct trust, factor rate for forwarding, and integrity factor. Moreover, every hop in the wireless sensor network presents superior trust degrees to estimate the trust level between the hops and the neighboring hop. It presents superior scalability as the value is calculated by exploiting the network topology information. The trust model is devised by exploiting the 4 parameters namely indirect and direct trust, rate factor of forwarding, and integrity factor, and it is stated in eq. (11), H^i is the indirect trust, H^d represents the direct trust, H^I states the integrity factor and H^F indicate the rate factor of forwarding.

$$H = \left\{H^d + H^i + H^F + H^I\right\} \tag{11}$$

i) Direct trust: The direct trust [10] is called as local trust and it states the trust value then an agent computes from the informality when interrelating through the target agent. In Eq. (12), fun indicates the satisfaction measure, $\left(H^d\right)_y^z$ indicates the direct trust for y^{th} transaction and z^{th} time interval, y states transactions, k represents the estimate hop z states the time interval, and the $h+1$ states the hop to be estimated.

$$\left(H^d\right)_y^z(h,h+1) = \mathrm{fun}_y^z(h,h+1) \tag{12}$$

The satisfaction measure is exploited to calculate the satisfaction degree of an agent that contains a particular service. Hence, the satisfaction measure remains the record of the satisfaction level by exploiting the exponential model for average updating which is stated in eq. (13), $U^z(h,h+1)$ indicates the amount of completely forwarded packets and $E^z(h,h+1)$ indicates the number of packets to forward.

$$\mathrm{fun}_y^z(h,h+1) = \eta \times \mathrm{fun}_v + (1-\eta) \times \mathrm{fun}_{y-1}^z(h,h+1) \tag{13}$$

In eq. (13), fun_v indicate the satisfaction value of recent transaction η denotes the weight and indicate the satisfaction value of $y-1$ the transaction at z^{th} time interval.

$$\mathrm{fun}_v = \begin{cases} 0\ ;\ \text{if transaction is fully unsatisfactory} \\ 1\ ;\ \text{if transaction is fully satisfactory} \\ \in (0,1)\ ;\text{otherwise} \end{cases} \tag{14}$$

The weight η deviates based on the collected variation $Z_y^z(h,h+1)$ and it is stated in eq. (15), (16) and (17), $\mathrm{fun}_{y-1}^z(h,h+1)$, Y state the threshold and pretenses fixed value and it is set to 0.25, j states the user-defined constant factor, $\gamma_y^z(h,h+1)$ state the current error, and $Z_y^z(h,h+1)$ is the accumulated deviation. Initially, the weight η is set as 1 and modified based on eq. (15).

$$\eta = Y + j \times \frac{\gamma_y^z(h,h+1)}{1 + Z_y^z(h,h+1)} \tag{15}$$

$$\gamma_y^z(h,h+1) = \mid \mathrm{fun}_{y-1}^z(h,h+1) - \mathrm{fun}_v \mid \tag{16}$$

$$Z_y^z(h,h+1) = j \times \gamma_y^z(h,h+1) + (1-j) \times Z_{y-1}^z(h,h+1) \tag{17}$$

ii) Indirect trust: It [10] is computed from the information increased via other hops. Every hop exploits the information of other hops to present effective decisions for every transaction. To achieve indirect trust, every hop demands other hops to present suggestions concerning the other hop. The ensuing hop gathers the ideas from other hops besides feedback trustworthiness of suggested hops. As a result, indirect trust of h^{th} hop regarding $(h+1)^{th}$ hop, and it is stated in eq. (18).

$$(K^i)_y^z(h,h+1) = \begin{cases} \dfrac{\sum_{a \in V-\{h\}} K_y^z(k,a) \times (H^d)_y^z(a,k+1)h}{\sum\limits_{a \in V-\{h\}} K_y^z(h,a)}\ ;\ \text{if} \mid V-\{h\} \mid = 0 \\ 0\ ;\ \text{If} \mid v-\{h\} \mid > 0 \end{cases} \tag{18}$$

In eq. (18), V indicates the set of agents interrelated with $h+1$, a indicate a hop that interrelated with other hops for creating prediction concerning maintenance trust, feedback creditability is indicated as H_y^z . The feedback suggested trustworthiness is exploited to calculate the accurateness of feedback information that the hop presented to the estimator. Hence, feedback trustworthiness is devised as eq. (19).

$$K_y^z(h,h+1) = \begin{cases} 1 - \dfrac{\ln(N_y^z(h,h+1))}{\ln \phi}\ ;\ \text{if}\ N_y^z(h,h+1) > \phi \\ 0\ ;\ \text{Otherwise} \end{cases} \tag{19}$$

In eq. (19), N^{z}_{y} indicates the similarity. The similarity measure is denoted as to decide to what degree the 2 hops are alike. Moreover, the similarity is calculated by discovering the personalized dissimilarity based on the satisfaction rating regarding the interacted agents and subsequently used the different ratings in order to describe the similarity. Hence, the similarity of 2 hops h and $(h+1)$ is devised in eq. (20).

$$N^{z}_{y}(h,h+1)=\begin{cases} N^{z}_{y-1}(h,h+1)+\dfrac{1-N^{z}_{y-1}(h,h+1)}{\omega} & ;\text{ if } R^{z}_{y}(h,h+1)<p \\ N^{z}_{y-1}(h,h+1)-\dfrac{N^{z}_{y-1}(h,h+1)}{\delta} & ;\text{otherwise} \end{cases} \tag{20}$$

In eq. (20), E denotes the set of agents,+ ω and δ denotes reward and the factor of punishment, and $R^{z}_{y}(h,h+1)$ states personalized difference and it is stated in eq. (21).

$$R^{z}_{y}(h,h+1)=\sqrt{\frac{\sum_{a\in E(h,h+1)}(\text{fun}^{z}_{y}(h,a)-\text{fun}^{z}_{y}(h+1,a))}{|E(h,h+1)|}}^{2} \tag{21}$$

iii) Forwarding rate factor: In WSN, the nodes encompass minimum energy which is detached when sensing and transmitting the data. Hence, it becomes probable to analyze and judge if the node is assaulted or not with estimating the forwarding nodes data. Hence, the forwarding rate factor, and it is stated in eq. (22), $A^{z}(h,h+1)$ states the number of feedback packets, h states evaluation hop, $B^{z}(h,h+1)$ indicates the number of packets to forward, and $h+1$ indicates the hop to be estimated.

$$(K^{F})^{z}(h,h+1)=\frac{A^{z}(h,h+1)}{B^{z}(h,h+1)} \tag{22}$$

iv)Integrity factor: When the data packet is transferred to the neighboring node, the source node inspects if the data packet is obstructed or not and inspects if the data packet is transferred with explicit time, and guarantees the integrity and the accuracy of the data. The integrity factor [9] is devised in eq. (23).

$$H^{I}(h,h+1)=\frac{U^{z}(h,h+1)}{E^{z}(h,h+1)} \tag{23}$$

4. Optimal Hop Selection Using Proposed Chaotic based Hybrid ASA-PSO

Based on [11], the conventional ASA comprises four kinds, such as the principle of the bellwether, strolling of individual, update locations, and competition scheme. Moreover, $y_{i}(h)$ indicates a location vector for the group in the h^{th} iteration of the i^{th} sheep, h indicates the current iteration number; $y_{i,d}(h)$ indicates the d^{th} dimension of $y_{i}(h)$; $y^{bw}_{i}(h)$ indicates the bellwether influence based upon the i^{th} sheep in the h^{th} iteration, $y^{B}(h)$ indicates bellwether location vector of in the h^{th} iteration, $y^{bw}_{i,d}(h)$ indicates the d^{th} dimension of $y^{bw}_{i}(h)$; $y^{self}_{i}(h)$ indicates self-awareness in foraging of the i^{th} sheep in the h^{th} iteration, $y^{B}_{d}(h)$ indicates the d^{th} dimension of $y^{B}(h)$; and $y^{self}_{i,d}(h)$ indicates the d^{th} dimension of $y^{self}_{i}(h)$.

4.1. Principle of Bellwether

The bellwether movement posses' considerable predominant on the sheep group. Conversely, the bellwether prevails over the group. Moreover, the bellwether location is y^{B}_{d} and the effect of the bellwether performs on other sheep $y^{bw}_{i,d}(h)$ indicates dominant to the group. Therefore, the bellwether vector y^{bw}_{i} will influence every sheep flock movement. The y^{bw}_{i} represents the bellwether vector for the i^{th}, $i=1,....,N$, $\Delta_{i,d}$ represents the effect extent of the bellwether take part in the i^{th} sheep for the d^{th} dimension,

$c_{1}=2w\cdot r_{1}$, $c_{2}=1+(1-\alpha)r_{1},\alpha$ is chosen in [0,1], r_{1} indicates an arbitrary number produced in [-1, 1], $w=\dfrac{h_{max}-h}{h_{max}}$, h_{max} is total iteration number, and h indicates the current iterative number.

$$\begin{cases} y^{bw}_{i,d}(h) = y^{B}_{d}(h) + c_1 \cdot \Delta_{i,d} \\ \Delta_{i,d} = c_2 \cdot y^{B}_{d}(h) - y_{i,d}(h) \end{cases} \tag{24}$$

4.2. Individual Update Positions and Strolling

The vector of self-awareness y^{self}_{i} indicates the individual sheep's self-awareness in the procedure of foraging, which defines the individual strolling course. y^{self}_{i} highlights the effect of the bellwether on the other individual's movement which is distinctive from y^{bw}_{i}. Hence, the d^{th} dimension of y^{self}_{i} , $y^{self}_{i,d}$ is explained in eq. (25), r_1 and r_2 indicates both arbitrary numbers in [0, 1], i indicates the i^{th} sheep agent, $i = 1,.....,N$, N indicates the total amount of sheep group.

$$\begin{cases} y^{self}_{i,d}(h) = y_{i,d}(h) + r_1 \cdot \in_{i,d} \\ \in_{i,d} = e^{-\beta . r_2} \cos(2\pi . r_2) . \Delta_{i,d} \end{cases} \tag{25}$$

In the ASA movement approach, every individual improves its location via its self-awareness and foremost of the bellwether. In the artificial sheep group, every individual will update its location using eq. (26), $w = \frac{h_{max} - h}{h_{max}}$ indicates a total iteration number, r_3 indicates a random number in [0,1] and h indicates the current iterative number.

$$\begin{cases} y_{i,d}(h+1) = \psi_i \cdot y^{self}_{i,d}(h) + (1 - \psi_i) \cdot y^{bw}_{i,d}(h) \\ \psi_i = w . r_3 \end{cases} \tag{26}$$

4.3 Competition Scheme

In the competition scheme of this approach, the value of the average fitness model group is exploited as the decision criterion. In the h^{th} iteration, the fitness model value of every individual is computed. All fitness model values of sheep flock are augmented and the average value of the objective model for the flock called Fl^{h}_{ave} is attained. For the i^{th} sheep, Fl^{h}_{i} indicates objective function value the i^{th} sheep, if $Fl^{h}_{i} > Fl^{h}_{ave}$, location vector of i^{th} sheep, called $y_i(h)$, is unnecessary and reproduced among a range of $y_i(h)$.

4.4 Proposed Chaotic based Hybrid ASA-PSO

To improve the search capability of ASA, 3 enhancements are developed into conventional ASA. The three enhancements are correspondingly used on the initialization algorithm and the movement scheme of ASA. The initialization algorithm is used in sheep flock initialization, and the movement scheme comprises 2 kinds, i.e. a movement scheme enthused by PSO and a movement scheme based on the chaotic mutation operator, h indicates present iterative number, N indicates the total count of members for sheep group.

4.4.1. Opposition-based learning

In [12], if $y \in [a,b]x$ indicates the opposition count of y and $x = a + b - y$. Here, Y indicates the location vector set of sheep flock and Y_{opp} indicates the opposition count set of Y . A novel set called Y_{nov} comprises Y and Y_{opp} , specifically $Y_{nov} = [Y, Y_{opp}]$. The value of the objective function for every member of Y_{nov} is calculated and every member in Y_{nov} can be reorganized based on the size of their values of the fitness model. Those members of Y_{nov} its values of the fitness model are in the peak preeminent 50% is chosen to create the initialization location set of sheep group. This step can make the optimal value of the objective function for the sheep group enhanced in the initialization stage.

4.4.2. Movement scheme enthused using PSO

The PSO has an enhanced search capability as the leadership scheme for the elite's memory was used on the movement scheme for each iteration of PSO. The movement scheme based on an enhanced PSO is shown in eq. (27) (28) [13], by that every particle agent updates its location vector. In the proposed model, after every location, the sheep group vector is updated via movement schemes of ASA, movement scheme enthused using PSO is used to update every location sheep flock vector. This procedure can improve the search capability of ASA efficiently, ω indicates a constant in [0,1], r_4, r_5 are random in [0,1],

c_3 and c_4 indicates coefficients generated from [0,2], y_{gb} indicates the personal best location in present iteration, y_{pb} indicates the global best location in present iteration, $i = 1, \ldots N$.

$$u_i^d(h+1) = \omega \cdot u_i^d(k) + c_3 \cdot r_4 \cdot \left(y_{pb}{}^d(h) - y_i{}^d(h)\right) + c_4 \cdot r_5 \cdot \left(y_{gb}{}^d(h) - y_i{}^d(h)\right) \quad (27)$$

$$y_i^d(h+1) = y_i^d(h) + u_i^d(h+1) \quad (28)$$

4.4.3. Movement scheme using chaotic mutation operator

In this paper, the chaotic mutation operator is used which can overcome disadvantages of the issue occurred by arbitrariness and enhance the capability of evading prematurity or local convergence. In [14], 10 types of chaotic maps are developed. In conclusion, the sinusoidal chaotic map that is considered as chaotic maps it is stated in eq.(29), which is chosen and carried out for the sheep group as the movement scheme, $a = 2.3,\ i = 1, \ldots, N$.

$$y_i(h+1) = a \cdot y_i^2(h) \cdot \sin(\pi \cdot y_i(h)) \quad (29)$$

While every location sheep group vector is updated using eq.(29), a novel location vector can be obtained. In contrast with the value of the objective function, every location vector through that of the novel location, the one whose value of the fitness model is lesser is reserved in the location vectors of the sheep group. Fig 2 demonstrates the flowchart of the proposed approach.

5. Results and Discussions

5.1. Experimental Procedure

In this section, the analysis of the developed approach based on the energy, throughput, alive nodes, and delay, was performed regarding conventional techniques which were exploited for secured multihop routing. The analysis of the developed technique can be calculated by analyzing the performance attained using conventional techniques. Hence, for the analysis, the conventional techniques such as C-SSA, Grid clustering [15], FABC-EACO clustering [16], Taylor Geo clustering [17], C-SSA and proposed method chaotic based Hybrid ASA-PSO algorithm was used.

5.2. Performance Analysis

In this section, a comparative analysis of the developed approach regarding the throughput, delay, energy, and alive nodes is presented. Moreover, the results attained by exploiting a network comprising 50 and 100 nodes with 2 and 3 hops based on the estimated measures on the utmost rounds. Fig 3 exhibits the evaluation of the developed and conventional methods regarding the energy. Fig 4 shows the analysis of the developed and traditional approaches regarding the delay. Fig 5 exhibits the analysis of the developed and traditional approaches regarding the throughput. Fig 6 shows the analysis of the developed and traditional approaches regarding the alive nodes. The overall analysis illustrates the analysis of the developed and traditional approaches such as Grid clustering, C-SSA, FABC-EACO clustering Geo clustering, and Taylor C-SSA algorithms.

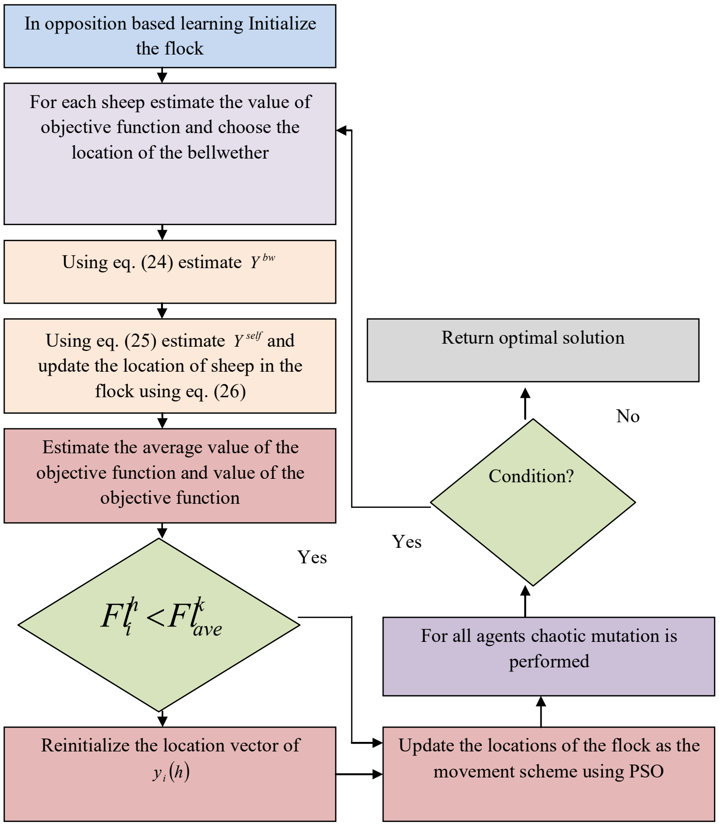

In opposition based learning Initialize the flock
For each sheep estimate the value of objective function and choose the location of the bellwether
Using eq. (24) estimate Y^{bw}
Using eq. (25) estimate Y^{self} and update the location of sheep in the flock using eq. (26)
Estimate the average value of the objective function and value of the objective function
$F_i^h < F_{ave}^k$
Yes
Reinitialize the location vector of $y_i(h)$
Update the locations of the flock as the movement scheme using PSO
For all agents chaotic mutation is performed
Condition?
Yes
No
Return optimal solution

Fig. 2. *Flowchart of the proposed algorithm*

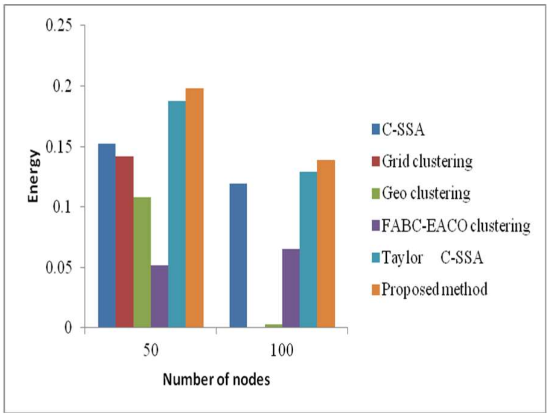


Fig. 3. *Analysis of the developed and traditional approaches regarding energy*

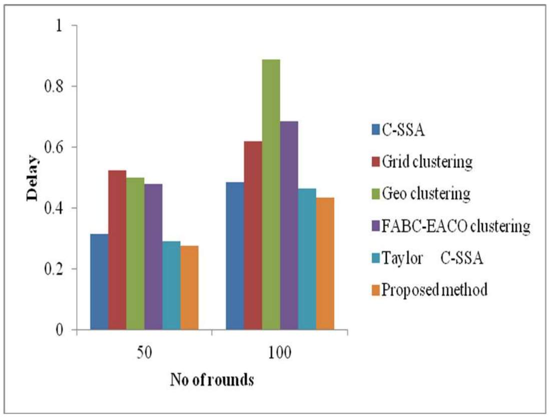


Fig. 4. *Analysis of the developed and traditional approaches regarding the delay*

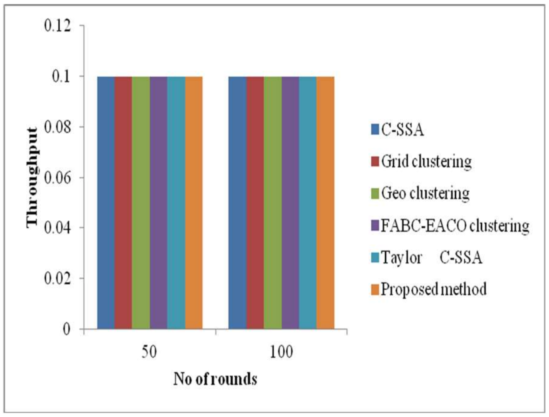


Fig. 5. *Analysis of the developed and traditional approaches regarding throughput*

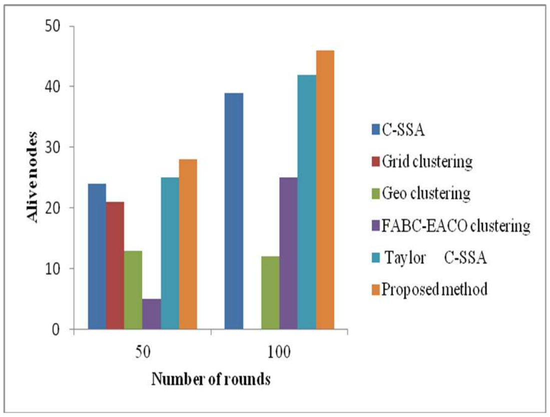


Fig. 6. *Analysis of the developed and traditional approaches regarding alive nodes*

6. Conclusion

This work concentrates on a multi-hop security-aware routing protocol and contemplates security as a significant model to perform the multi-hop routing. The protocol was modeled by taking into consideration of a trust model that integrates various trust factors like direct trust, rate of data forwarding, indirect trust, and integrity factor. The procedure experiences 2 phases for obtaining efficient multi-hop routing. The initial phase was the selection of CH, and the next phase was the transmission of data. In the selection of CH, the best node is chosen as CH by exploiting the LEACH protocol and subsequently the data transmission was done from one node to another node based on the diverse hops that were chosen optimally by exploiting the developed Chaotic Hybrid-ASA-PSO based multi-objective fitness function. The developed technique exhibits better convergence and the hybrid optimization operates based on ensuing constraints, namely delay, energy, Link-Lifetime, intra-cluster distance, inter-cluster distance, trust, and delay. The developed technique exhibits optimal performance regarding the alive nodes, energy, throughput, and delay.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Ziwen Sun, Min Wei, Zhiwei Zhang, Gang Qu,"Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks", Applied Soft Computing, Volume 77, Pages 366-375, April 2019.

[2] Tarek Gaber, Sarah Abdelwahab, Mohamed Elhoseny, Aboul Ella Hassanien,"Trust-based secure clustering in WSN-based intelligent transportation systems"Computer Networks, Volume 1469, pp. 151-158, December 2018.

[3] Elena Romero, Javier Blesa, Alvaro Araujo," An adaptive energy aware strategy based on game theory to add privacy in the physical layer for cognitive WSNs",Ad Hoc Networks, Volume 92, September 2019.

[4] Shishupal Kumar, Nidhi Lal, Vijay Kumar Chaurasiya,"An energy efficient IPv6 packet delivery scheme for industrial IoT over G.9959 protocol based Wireless Sensor Network (WSN),"Computer Networks", Volume 1548, Pages 79-87, May 2019.

[5] Reeta Bhardwaj, Dinesh Kumar,"MOFPL: Multi-objective fractional particle lion algorithm for the energy aware routing in the WSN", Pervasive and Mobile Computing, Volume 58, August 2019.

[6] Srijit Chowdhury, Ambarish Roy, Abderrahim Benslimane, Chandan Giri,"On semantic clustering and adaptive robust regression based energy-aware communication with true outliers detection in WSN", Ad Hoc Networks, Volume 94, 2019.

[7] M. Masdari, S. M. Bazarchi, and M. Bidaki, “Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks,” J. Netw.Comput.Appl., vol. 36, no. 4, pp. 1243–1260, 2013.

[8] B. Dennis and S. Muthukrishnan, “AGFS: Adaptive Genetic Fuzzy System for medical data classification,” Appl. Soft Comput. J., Volume. 25, page no. 242–252, 2014.

[9] Zhu, J., "Wireless Sensor Network Technology Based on Security Trust Evaluation Model," International Journal of Online Engineering (iJOE), vol.14, no.4, pp.211-226, 2018.

[10] Das, A. and Islam, M.M., "SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems," IEEE Transactions on Dependable and Secure Computing, vol.9, no.2, pp.261-274, 2012.

[11] Wenxiao Wang, Chaoshun Li, Xiang Liao, Hui Qin,” Study on unit commitment problem considering pumped storage and renewable energy via a novel binary artificial sheep algorithm”, Applied Energy, volume.187, page no.612–626, 2017.

[12] H.R. Tizhoosh. Opposition-based learning: a new scheme for machine intelligence, CIMCA-IAWTIC'06, page no. 695-701. IEEE, 2005.

[13] Y. Shi , R. Eberhart , A modified particle swarm optimizer”, Evolutionary Com- putation Proceedings, IEEE World Congress on Computational Intelli- gence, The 1998 IEEE International Conference on, IEEE, pp. 69–73, 1998 .

[14] Seyedali. Mirjalili,Amir, H. Gandomi,” Chaotic gravitational constants for the gravitational search algorithm”, Applied Soft Computing, volume53, page no.407-419, 2017.

[15] J. Huang, Y. Hong, Z. Zhao, and Y. Yuan, “An energy-efficient multi-hop routing protocol based on grid clustering for wireless sensor networks,” Cluster Computing, 2017.

[16] [37] R. Kumar, D. Kumar, and D. Kumar, “Exponential Ant Colony Optimization and Fractional Artificial Bee Colony to Multi-Path Data Transmission in Wireless Sensor Networks,” IET Commun., Volume. 11, num. 4, page no. 522–530, 2017.

[17] I. S. Akila and R. Venkatesan, “An energy balanced geo-cluster head set based multi-hop routing for wireless sensor networks,” Cluster Computing., 2018.

[18] S Vinusha and J.S. Abinaya,"Performance analysis of the Adaptive Cuckoo Search Rate Optimization Scheme for the Congestion Control in the WSN", Journal of Networking and Communication Systems (JNACS), Volume 1, Issue 1, October 2018.

[19] W.Brajula and Praveena S,"Energy Efficient Genetic Algorithm Based Clustering Technique for Prolonging the Life Time of Wireless Sensor Network", Journal of Networking and Communication Systems (JNACS), Volume 1, Issue 1, October 2018.