Trust Aware Secure Routing Model in MANET: Self-improved Particle Swarm Optimization for Optimal Route Selection

S. Haridas, A. Rama Prasath

▶ **To cite this version:**

S. Haridas, A. Rama Prasath. Trust Aware Secure Routing Model in MANET: Self-improved Particle Swarm Optimization for Optimal Route Selection. 6th International Conference on Computer, Communication, and Signal Processing (ICCCSP), Feb 2022, Chennai, India. pp.193-212, 10.1007/978-3-031-11633-9_15 . hal-04388147

HAL Id: hal-04388147
https://inria.hal.science/hal-04388147v1

Submitted on 11 Jan 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Trust Aware Secure Routing Model in MANET: Self-Improved Particle Swarm Optimization for Optimal Route Selection

Haridas .S [1] Dr.A. Rama Prasath [2]

[1] Hindustan Institute of Technology and Science, Chennai, India
Email: harigoleson@gmail.com
[2] Hindustan Institute of Technology and Science, Chennai, India.
E-mail: mraprasath@gmail.com

Abstract. In the heterogeneous network, MANETs are the collective gathering of diverse mobile devices with the ability to join and leave the network at any moment as the most prominent feature. As a consequence, mobile nodes in the decentralized network may link, interact, and transfer information to one another without the need of an intermediary router. Several academics have recently explored a variety of routing approaches to tackle issues such as packet data transmission delays and poor PDR. This paper aims to introduce a new trust-aware routing in MANET that ensures the trust level among the nodes. For this, a new trust rate estimation process is introduced based on energy and mobility of nodes exist. Thereby, a Self-Improved Particle Swarm optimization algorithm (SI-PSO) is proposed for choosing the optimal trust aware route for data transmission. The optimal route selection is performed by considering certain parameters like trust rate (security), Packet Drop Ratio (PDR) distance, congestion, energy, and as well. The performance of the adopted work is examined to the existing schemes regarding Energy, Delay, and Network Lifetime.

Keywords: First Keyword, Second Keyword, Third Keyword.

Nomenclature

Abbreviation	Description
BFS	Breadth-First Search Trees
AODV	Ad Hoc On-Demand Distance Vector
QoS	Quality Of Services
MANET	Mobile Adhoc Network
GA	Genetic Algorithm
SI-PSO	Self-Improved Particle Swarm Optimization Algorithm
CHS	Cluster Head Selection
GR	Global State Routing
RBT	Reputation-Based Trust-Aware Routing Protocol
TEAR	Trust Based Energy Aware Routing
RSRA	Real-Time Secure Route Analysis
WSN	Wireless Sensor Networks
TECM	Trust Enhanced Cluster Based Multipath

CH	Cluster Head
NETAR	Novel Energy Efficient Trust Aware Routing
PDR	Packet Delivery Ratio
BPSO	Binary PSO
PSO	Particle Swarm Optimization
E2E	End-To-End
OLSR	Optimized Link State Routing
FPNT	Fuzzy Petri Based Trust

1 Introduction

MANET provides a self-configuring structure comprising diverse devices that are connected via wireless network [9]. The devices linked in the MANET are generally referred to as nodes. MANET nodes include the features of mobility, infrastructure less nature, and multi-hop packet transmissions [11]. Through the direct communication link, each node communicates with the others. If the nodes are separated by a long distance, communication happens through the intermediary nodes. MANET is used in various applications, including military applications, space applications, and mobile phones, among others [10]. MANET network ensured a constant communication flow among the transmitter and receiver nodes with improved security and service quality. However, finding of the secure routing path among the MANET nodes has been emerged as the primary problem in MANET routing [12]. MANET nodes rely on one another to form a link in wireless communication. As the MANET nodes are movable, communication links fail. The MANET architecture with multipath routing prevents communication connection failure among nodes [13].

Multipath routing [14] creates several communication path among the transmitter and receiver nodes. Load balancing and route dependability are two advantages of multipath routing. The downside of multipath routing methods is topology vulnerability. The routing table of the nodes is regularly changed by multipath routing. This exposes the network to hackers, allowing them to readily obtain information from the network. During multipath routing, MANET nodes [17] [18] are exposed to a variety of assaults. Wormhole attacks, Sybil attacks, black hole attacks, and rushing assaults are examples of MANET attacks [15]. The usage of topology concealing routing protocols can cover the open topology in multipath routing. Previous research developed topology-hidden multipath routing techniques in MANETs [16]. The topology concealing paradigm conceals routing information while securely transmitting the messages over the network.

Several deterministic and stochastic models have lately been developed. The strategies which rely on the gradient technique are the predictable methods. Stochastic approaches are the multimodal problem solving methods that rely on biological entities. Many metaheuristic strategies are more helpful to solve the issues in MANET [19] [20] [21] [22]. The clustering approach based on BFS is created to choose the lower load CHs and link the nodes with each other. Moreover, GA is implemented based on the Darwinian concept of survival of the fittest, in which it minimizes the highest load on gateway nodes. The dynamic clustering structure was determined in MANET using the PSO model [40] [41] [42]. They used a variety of CHS criteria to create stable clusters. However, the mobility of the nodes could not be handled efficiently. an energy-efficient routing approach has

been done with PSO [36] [37] [38] [39] algorithm [43], [23] [24] was presented for MANET. Still the model suffers from local optima issue, which needs an improvement to make efficiency in problem solving [25].
The main contribution of the adopted work is given in the succeeding section:
Implemented a novel optimization algorithm known as SI-PSO model which is an enhanced version of standard PSO for more trust aware secure path selection.
The optimal route selection is performed based on the constrains like the trust rate (security), distance, power, minimum congestion, and Packet Drop Ratio (PDR), respectively.
The rest of the paper is ordered as: Section II addresses the review on trust aware secure routing in MANET. Section III describes about the proposed methodology: trust aware secure routing in MANET. Section IV portrays trust aware secure routing model in manet: defined objectives. Section V describes the self-improved particle swarm optimization algorithm for optimal path selection. Section VI discusses the results acquired with the presented work.

2 Literature review

2.1 Related works

In 2021, Usha et al. [1] have implemented a NETAR protocol for the conventional AODV protocol for improving the 3 trust degrees between the MANET nodes by malicious behavior predictions, energy, bandwidth calculation, and neighbor-node trust rate estimation to select the reliable and efficient path. The channel capacity evaluation technique was used to estimate the intermediate nodes' residual energy, high trust rate, and bandwidth. Routing through these nodes enhances network efficiency. This was implemented using the NS2 simulator tool. When compared to GR, RBT Protocol, the proposed approach has a average delay time efficiency, throughput, less false positive, and higher PDR.
In 2018, Devi et al. [2] have introduced the TECM routing system in this work. To produce cluster formation and CHs, they employ the energy-efficient PSO method. Super CHs were chosen from trust values computed using the suggested TECM technique. Packet/frame loss ratio, received signal strength, packet/frame receiving energy, routing overhead, protocol deviation flag, average forward delay, Packet/frame forward rate, and Packet/frame forward energy was the many trust factors utilized in trust computation. The new TECM algorithm was combined with a typical multipath TECM-OLSR to evaluate its performance. The proposed TECM-OLSR protocol was extremely efficient with respect to routing overhead, loss and delivery rate, latency, and network lifespan.
In 2021, Sathyaraj et al. [3] have explored a RSRA technique in MANET for safe routing. This technique considered the strategy of intermediary nodes of discovered routes, as well as the presence of IoT devices and their trust. The approach begins via generating a list of possible paths among any transmitter and receiver. The trustworthiness of each mobile node was considered in determining the location, mobility speed, energy, and quantity of transmissions concerned, as well as their neighbor list. DS was tested for IoT devices, whereas MSRS was evaluated for mobile nodes. A single route was already chosen on the basis of DFS metric that enhances the MANET's QoS.

In 2019, Merlin et al. [4] has determined a novel TEAR technique for MANETs. The significant features of TEAR mechanism' was that it mitigates BHs via dynamic generation of different detection routes to identify BHs as feasible and attains best data route security via establishing nodal trust. Fundamentally, in the TEAR method, these multidetector routes were formed by fully using the energy in non-hotspots to increase the data route security and energy efficiency. The TEAR mechanism improves the network's lifespan by preventing black hole assaults and dramatically improves the probability of data routing.

In 2021, Anitha et al. [5] has suggested the TSVRCLPBC ensemble approach in MANET. The suggested method's major goal was to improve the secure communication with higher PDR and a lower E2E delay. The TSVRCLPBC was used to investigate node attributes including residual energy, cooperative communication, and node history. Moreover, the weak learners' results were merged to generate a powerful enhanced classifier output with weight function. To increase the Qos metric performance, the ensemble classification method in MANET computes the trustworthy nodes. Different metrics like E2E, PDR, latency, PLR, jitter, and energy consumption were used in the simulation. The simulation results have shown that the TSVR-CLPBC approaches improve PDR while reducing EC, PLR, E2E latency, and jitter than the existing methods.

In 2019, Ambekar et al. [6] has introduced the MANET's T-TOHIP method. The security element is described by four categories in the suggested routing scheme: the delay, energy, mobility, and trusted model. Based on the specified neighbor nodes, the adopted model finds the secure route among the transmitter and recipient. Ultimately, data exchange takes place via the chosen multipath. When there was an assault on the node, experimental outcomes has demonstrated that the adopted model has shown maximum throughput, latency, energy, and PDR after 50 seconds of simulation than the traditional system.

In 2019, Rajeswari et al. [7] has adopted a novel intelligent framework for secure routing that consists of 2 models like the TNFNS and the FBSSR algorithm. The trust based node selection method was used to provide efficient routing outcomes. The key feature of this suggested node selection mechanism was that it use trust values to separate hostile nodes from the routing process, thereby improving security. When compared to related secure routing protocol, it was shown that the suggested secured routing algorithm was more efficient in terms of enhanced PDR, reduction in delay, and FPR.

In 2019, Kukreja et al. [8] have proposed a T-SEA routing protocol for isolating the black/gray hole nodes in MANETs. The ability to conserve energy was a critical prerequisite for MANET lifetime. Black/gray hole nodes were monitored and caught using intrusion IDSs. IDS competent nodes have enough energy, a low trust value, and a large number of connections. T-SEA identified suspicious nodes throughout the data transmission phase without the need of any node into sniff mode. IDS identify a node as malicious while monitoring the present activity, current trust, and recorded behavior throughout previous transmissions. As the IDS operates on a few nodes at a time to the attack discovery, the detection approach was energy aware. The suggested approach was validated using NS-2 in this study.

3 Proposed methodology: trust aware secure routing in MANET

3.1 Architectural Description

The roles and responsibilities of routing mechanism's involve exchanging routing path, computing the shortest route employing factors like link lifetime, least power, and hop count, collecting information concerning broken links, repairing broken links, processing power and bandwidth. MANET's routing technology is entirely dispersed and adaptable to the topological structure's frequent changes. Nevertheless, in order to reduce the packet collisions, each node in the network has a shorter route discover latency and route information with the smallest possible packets. In order to avoid the message loss and stale routes, it is critical to have reliable data transfer. As a consequence, the fundamental objective in MANET is to construct and maintain an energy-efficient optimal path to extend the network's lifetime. The nodes in geographic routing are required to discover an appropriate path for implementing the successful routing performance during the data transmission. Thereby, novel optimization techniques are used in this research to implement an adaptive routing strategy. SI-PSO [44] model a conceptual enhancement of normal PSO is introduced for more trust aware secure route selection as a novelty. Data packets are routed optimally based on the parameters like trust rate (security), minimum distance, minimum Energy, minimum congestion, and minimum PDR. Fig.1 illustrates the framework of the adopted work.

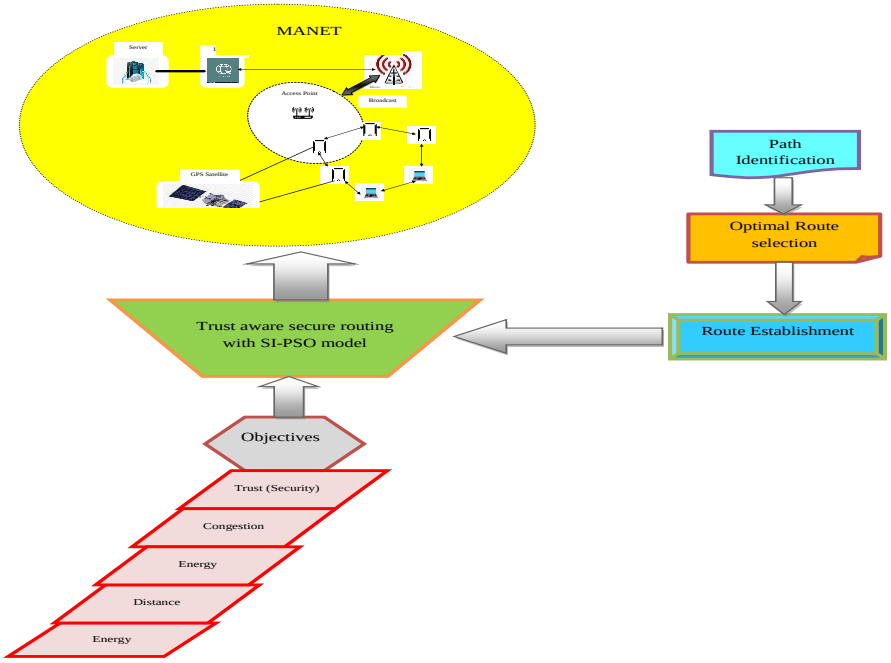

Fig. 1. Framework of the adopted work

3.2 System Model

The MANET's system model is represented in Fig. 2. Here, the count of sensor nodes is taken as$M = 100$. Moreover, the adopted network is constructed with the dimension of 500×500. Consider the graph$F(U, V)$, where $V = \{V_1, V_2, \ldots, V_l\}$denotes the link set, and $U = \{U_S, U_1, U_2, \ldots, U_R, U_M\}$ represents the nodes set. Moreover, the node sends the data packet is known as the sender $U_S$and the receiver $U_R$is one who receive the data packet. Further, the link state correlated the receiver U_R and senderU_S. It's difficult to send the message straight to the receiver because the sensor nodes are movable and have fluctuating neighbourhood conditions (nodes up to 400 metres could only act as a neighbour). As a result, the sender $U_S$sends the message to any of its nearby neighbours that are within the radio range. That usually results in the creation of a path between among the sender $U_S$and the receiver U_R. The network life span with less latency, less congestion, lower packet drop ratio, and lower energy usage is a major concern with path creation. As a consequence, the shortest and most optimum path to be determined among the sender $U_S$and receiver $U_R$is critical. Further, the gateways perform as the interface among the neighboring nodes which permit to maximize the connectivity and coverage.

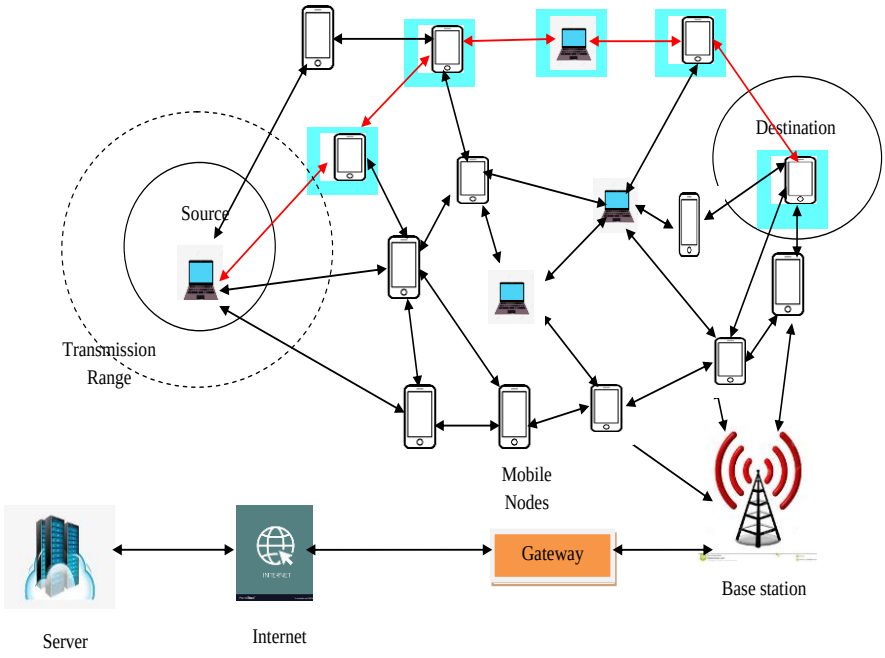

Fig. 2. System Model

Route discovery, route establishment, and link break prediction are some of the steps of routing stagey. The sender $U_S$determines the possible routes for transmitting the message to the destination during the route discovery phase. Using the suggested optimization technique, the optimal path is selected among the possible options in the route establishment phase based on the objectives (trust rate (security), minimum distance, minimum

power, minimum congestion, and minimum PDR). As the mobile nodes are dynamic, the path fixed is also dynamic and there is a risk of link breakage due to neighbour mobility. Further, the third step determines whether the route has any connection breaks. Separating all of these phases is a time-consuming but necessary task. Because all three phases function together, the network's lifetime could be extended or compressed. As a result, a novel routing algorithm is presented here to jointly select the best path that includes three phases. The routing algorithm is known as SI-PSO that is an improved version of PSO.

4 Trust Aware Secure Routing Model in MANET: Defined Objectives

4.1 Objective Function and Solution Encoding

The objective function to select the final optimal path in trust aware secure routing of MANET is given in Eq. (1).

$$Obj = w_1 \times (1 - T) + w_2(D) + w_3(E) + w_4(C) + w_5(PDR) \quad (1)$$

In Eq. (1),$w_1, w_2, w_3, w_4, and w_5$are the weights of parameters ranges from 0 to 1. Here, the trust (security) is to be high. The distance, energy, congestion, and PDR are to be low.
Distance: The distance between the sender $U_S$and the receiver$U_R$is calculated through the feasible paths. Moreover, the distance matrix is expressed in Eq. (2), and it is denoted as $D(m * n)$

$$D(m * n) = \begin{matrix} d_{M_{c1},u_1} d_{M_{c1},u_2} \ldots\ldots\ldots d_{M_{c1},u_n} \\ d_{M_{c2},u_1} d_{M_{c2},u_2} \ldots\ldots\ldots d_{M_{c2},u_n} \\ \vdots \\ \vdots \\ \lfloor d_{M_{cm},u_1} d_{M_{cm},u_2} \ldots\ldots\ldots d_{M_{cm},u_n} \rfloor \end{matrix} \quad (2)$$

Where, d_{M_c}indicates the Euclidean distance among a sender node $U_S$and the receiverU_R. In addition, the position of the sender and the receiver node is indicated as $y$and$z$, and the Euclidean distance $(d_{g,h})$is determined in Eq. (3).

$$d_{g,h} = \sqrt{(g_y - h_y)^2 + (g_z - h_z)^2} \quad (3)$$

All elements in the matrix of distance specify the distance exists within the g^{th}sender and the h^{th}receiver node. The packet transmission takes place and the shortest path between the sender and the receiver is selected. The distance function is indicated as $D$and it should be low.
Energy model (E): The nodes in MANET are utilized to transmit and receive the data with high power. Every node is assumed with maximum powers in the setup phase. The nodes with higher energy are chosen during the path selection and the nodes with lower energy are not actively takes part in the routing process. Overall power consumption should be less during the data packet transfer. Still, the energy consumed $E_{cons.}$ depends on the security level and it is determined in Eq. (4).

$$E_{cons.} = SecurityLevel * DataPackets \quad (4)$$

Also the node's energy level after transferring the data packet is specified in Eq. (5).

$$E_{remain.} = E_{node.} - E_{cons.} \quad (5)$$

In Eq. (5), $E_{node.}$denotes the energy of the node and $E_{remain.}$indicates the node's remaining energy.

Packet Drop ratio(PDR)**:** PDR is the ratio of the count of hops to the overall network nodes. Further, the congestion, link state stability, and QoS are considered during the packet transmission mechanism.

Congestion$C$**:** It is a significant problem in ad-hoc networks. When the count of packets maximizes beyond the limit, it is handled via network resources that provides degradation in network performance, which is stated as congestion. A network that is congested for one user is not necessarily congested for another user. It is an unwanted situation where the network faces the difficulty of more traffic than its rated capacity results in packet loss, bandwidth degradation, waste time and energy, etc.

Link State: It is taken into account than considering the path stability. The link stability is determined for selecting the optimal path at a particular time instance. The link state for any node $y$to node $z$is given in Eq. (6).

$$link(y,z) = tfinal - tInitial \quad (6)$$

In Eq. (6), $link$indicates the time duration among the initialization and breakage in link.

QoS: For MANETs, the QoS is a complex task due to the dynamic behaviour of the network topology. QoS is the service used to allow the users and network applications to access the novel capabilities. The QoS of the packet needs to be higher for ceaseless packet transmission. Moreover, QoS network is determined based on the guaranteed count of data that a network transfers from one place to another within a certain time.

Security: The security constraint [32] is designed based on the security rank (s_{Rank}) and security demand (s_{Dem}) of the nodes. If the node is said to be more secure, only it satisfies the conditions$s_{Dem} \leq s_{Rank}$. The security constraint model is defined based on the risk probability, and it is given in Eq. (7).

$$Risk_{prob} = \begin{cases} 0 & if \quad s_{Dem} - s_{Rank} \leq 0 \\ 1 - e^{\frac{(s_{Dem} - s_{Rank})}{2}} & if \quad 0 < s_{Dem} - s_{Rank} \leq 1 \\ 1 - e^{\frac{3(s_{Dem} - s_{Rank})}{2}} & if \quad 1 < s_{Dem} - s_{Rank} \leq 2 \\ 1 & if \quad 2 < s_{Dem} - s_{Rank} \leq 5 \end{cases} \quad (7)$$

Based on the difference among the $s_{Dem}$and s_{Rank}, the risk probability is assigned for a node that evaluates its security level.

Trust level: The trust relation among the sensor nodes is determined. The trust level includes three types they are

- Direct Trust
- Indirect Trust

- Social Trust

(i)Direct Trust: The direct trust is determined as in Eq. (8).

$$B_r(i,j) = \frac{W(i,j)}{W(i)} \tag{8}$$

In Eq. (8), $B_r(i,j) \in [0,1]$, $W(i,j)$indicates the degree of strength among neighboring sensors $i$and j,$W(i)$indicates the overall connection strength between$i$and $j$at neighborhood distance. The similarity among neighboring nodes is computed through establishing the entire count of neighboring sensor nodes among 2 sensor nodes.

$$B(i,j) = B_r(i,j) + B_x(i,j) \tag{9}$$

$$B_x(i,j) = \sum_{\hat{t} \in N(j) \in N(j)} \left(I(\hat{t})\right)^{-1} \tag{10}$$

Where, $I(\hat{t})$indicates the penetration degree of $\hat{t}$among $i$and j.

(ii)Indirect Trust: The indirect trust is determined as in Eq. (11).

$$I_x(i,j) = \begin{cases} k\hat{t}\,\dfrac{B_{\max} - B_{i,j} + 1}{B_{\max}} & if\ B_{i,j} \le B_{\max} \\ 0 & if\ B_{i,j} > B_{\max} \end{cases} \tag{11}$$

The intermediate route length is calculated using $k\hat{t} = kk\left(B(i,i_1), B(i_1,i_2), \ldots\ldots, B(i_{\hat{n}},j)\right)$and B_{max}

indicates the trust among sensor nodes with less distance.

(iii)Social Trust: The social trust is specified in Eq. (12).

$$ST(i,j) = f\left(I(i,j), G(i,j), L(i,j)\right) \tag{12}$$

Where, $I(i,j)$indicates the communication interval among the time duration or nodes, $G(i,j)$denotes the communication duration or the time duration of sensor node $i$and$j$, and $L(i,j)$refers to the context of communication that represents the communication scenario. Moreover, the overall trust is determined in Eq. (13).

$$Trust = B(i,j) + I_x(i,j) + ST(i,j) \tag{13}$$

5 Self-improved particle swarm optimization algorithm for Optimal Path Selection

5.1 Proposed SI-PSO model

Although, the existing PSO model offers better computational efficiency with robustness and satisfactory outcomes to control parameters; still, it easily falls into local optimum from the space that affects the optimization process. For overcoming the drawbacks of traditional PSO model, the proposed SI-PSO model intends to make some enhancement

on PSO that offers optimum results and better convergence. Moreover, self-enhancement is established to be capable in traditional optimization algorithms [26] [28] [29] [30] [31]. The objective function is fed as input to the proposed SI-PSO approach for optimal path selection and efficient data transmission. The PSO [27] algorithm was determined based on the social behavior of fish schooling and bird flocking. Every bird has a velocity and position at any time instant$a$. The position update is determined in Eq. (14).

$$P_o(a+1) = P_o(a) + v_o(a+1) \quad (14)$$

The proposed velocity update is given in Eq. (15).

$$v_o(a+1) = q_o v_o(a) + Z_1 e_1 (P_o^{best}(a) - P_o(a)) + Z_2 e_2 (K - Y_o(a)) \quad (15)$$

The position vector, memory vector and the velocity vector are determined asP_o,P_o^{best}andv_o, correspondingly. The random values are denoted as $e_1$and $e_2$in uniform manner in the interval of [0,1]. The random variables $e_1$and $e_2$are initialized as a single value in the PSO, they are initialized as follows.

$$e_1 = rand(A, Q) \quad (16)$$

$$e_2 = rand(A, Q) \quad (17)$$

In Eq. (16), Adenotes size of the solution, and$Q$denotes the count of Nodes

Moreover, $K$is used instead of $P_o^{best}$to maximize the accuracy of positional update. In the PSO, the P_o^{best} is repeated 10 times for each solution and this might increase the execution time while the count of solutions is higher. Since, the first best solution with K is kept and the rest of the solution is shuffled based on the fitness. The possibility of positional update is higher.

for $\tilde{\imath} = 2{:}A$

$$\tilde{a}(1,:) = P_o^{best};$$

$$idx = randperm(node)$$

$$X(1,:) = (1,:);$$

$$X(1, idx) = \tilde{a}(1,:);$$

End

The accelerating constant is indicated as Z_1 and Z_2. The best solution is explored by all particles is determined as$P_o^{best}$and q_o specifies the inertia weight of the particle. At last, if the fitness of the next solution $(a+1)$is greater than the fitness of the current solution, then the acceleration constants$Z_1$and $Z_2$are determined in Eq. (18) and Eq. (19).

$$Z_1 = Z_1 + 1 \quad (18)$$

$$Z_2 = Z_2 + 1 \quad (19)$$

If not, then the value of Z_1 andZ_2 are determined in Eq. (20) and Eq. (21).

$$Z_1 = Z_1 - 0.2 \quad (20)$$

$$Z_2 = Z_2 - 0.2 \quad (21)$$

The pseudo-code of the adopted SI-PSO technique is determined in Algorithm 1.

Algorithm 1: Proposed SI-PSO algorithm
Initialize P_o, $P_o^{best}$and v_o
The random values $e_1$and $e_2$are initialized as $e_1 = rand(A, Q)$; $e_2 = rand(A, Q)$;
The position updated in Eq. (14)
The velocity update is determined in Eq. (15).

Find the Kvalue	
	for $\tilde{\imath} = 2{:}A$
	$\tilde{a}(1,:) = P_o^{best};$
	$idx = randperm(node)$
	$X(1,:) = (1,:);$ $X(1, idx) = \tilde{a}(1,:);$
	End
	If $\big(Fit(a+1)\big) > \big(Fit(a)\big)$
	Z_1 andZ_2 is calculated in Eq. (18) and Eq. (19)
	Else
	Z_1 andZ_2 is calculated in Eq. (20) and Eq. (21)
	End
	end
Termination	

6 Results and discussion

6.1 Simulation Procedure

The proposed trust aware secure routing with SI-PSO model in MANET was executed in MATLAB and the resultants were determined. Accordingly, the proposed SI-PSO method was computed to the extant approaches including PSO [27], GA [33], GWO [35], and WOA [34], respectively. Further, the analysis was made with respect to convergence analysis, network congestion level, E2E delay, energy consumption, link state Network lifetime, packet drop ratio, trust and risk analysis respectively for the number of nodes 100, 150, 175 and 200.

6.2 Analysis on Energy Consumption

The analysis on energy consumption based on different count of nodes is represented in Fig. 3. Moreover, the energy consumption is a major concern in the routing network. Further, the proposed SI-PSO model attains lowest energy (~0.1×10^5) with better performance than other existing models for node count 200. Thus, for all number of nodes variation, the adopted scheme exhibits the minimal energy consumption and becomes efficient for routing.

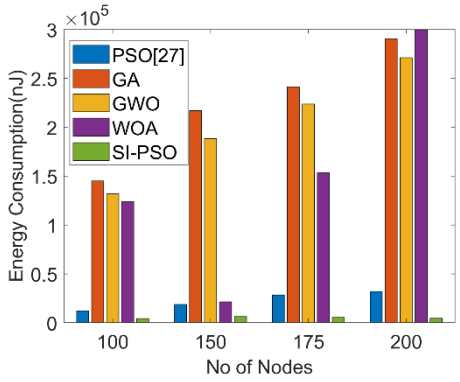

Fig. 3. Analysis on Energy consumption for adopted and traditional Models

6.3 Analysis on Network Congestion level

Fig. 4 illustrates the network congestion level of the presented scheme to the existing approaches. e GA approach has the highest level of congestion for node 100, 150, and 175; while the presented SI-PSO work has the lowest congestion level. In addition, the presented work has the lowest congestion level (~2) for node count 200 than traditional PSO, GA, GWO, and WOA approach, correspondingly.

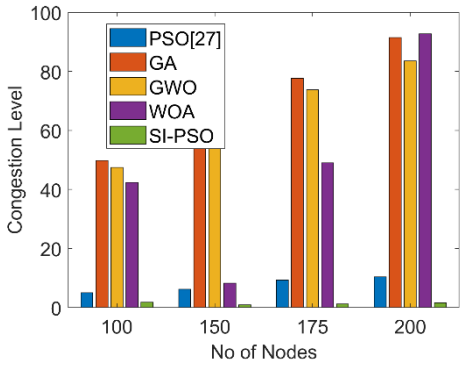

Fig. 4. Analysis on Network congestion for adopted and traditional Models

6.4 Analysis on Network Lifetime

The Lifetime ratio is utilized as the significant parameter in establishing the outcomes of adopted work. The network life span provides a decision regarding the network's transmission capability. The analysis on network lifetime by varying count of nodes is given in Fig. 5. Furthermore, the adopted SI-PSO model provides highest network lifetime than the existing works. In Fig. 5, the adopted SI-PSO model has attained (~200) alive nodes

with better performance for node count 200 than other existing approaches like PSO, GS, GWO, and WOA, respectively.

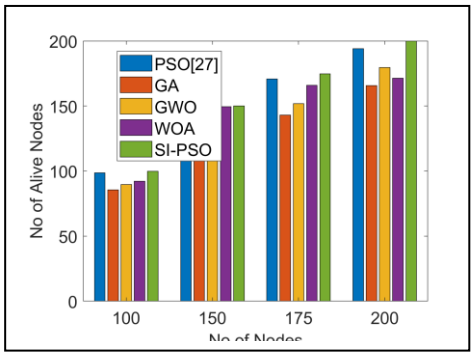

Fig. 5. Analysis on Network lifetime for adopted and traditional Models

6.5 Analysis on Link State

The graphical analysis on links state is illustrated in Fig. 6. In a routing table, the routes contain entries for the next hop neighbor and the destination node. The link-state should be lower to obtain an efficient routing. The presented SI-PSO model has shown the lowest link-state than the existing one for node 200. Further, the presented work has the lowest value (~0.1) than traditional PSO, GA, GWO, and WOA approach, correspondingly.

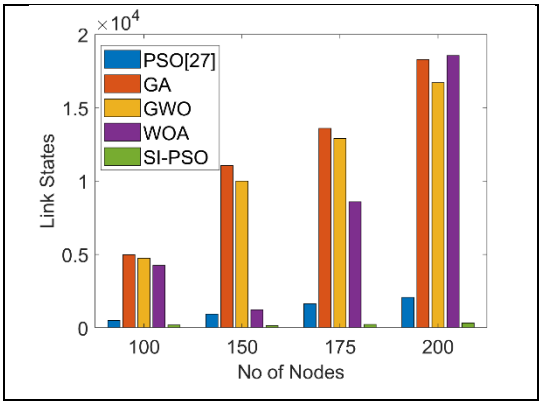

Fig. 6. Analysis on Network link state for adopted and traditional Models

6.6 Evaluation on E2E delay

The E2E delay of the adopted scheme to the traditional work is exhibited in Fig. 7. The presented work has the lowest E2E delay than the existing works for all node count. In

addition, the proposed SI-PSO model has attained minimum delay (~0.668) than the existing models like PSO, GA, GWO, and WOA, correspondingly for node count 140.

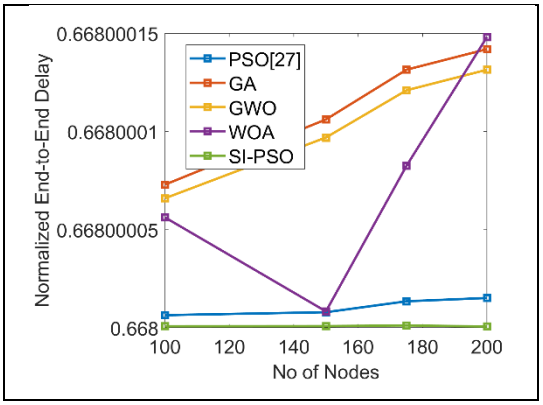

Fig. 7. Analysis on E2E delay for adopted and traditional Models

6.7 Analysis on Packet Drop Ratio

The analysis of packet drop ratio is exhibited in Fig. 8. It is the ratio of the count of neighbours to the count of the overall nodes. The packet drop ratio should be minimal for a successful data transmission of packets from the source to the target. Likewise, the presented SI-PSO model attains the lowest value (~2) than other traditional models like PSO (~8), GA (~90), GWO (~80), and WOA (~52), respectively for the count of node175. As the node count =200, the adopted SI-PSO model attained the least value and hence the traditional approaches shows the maximum value.

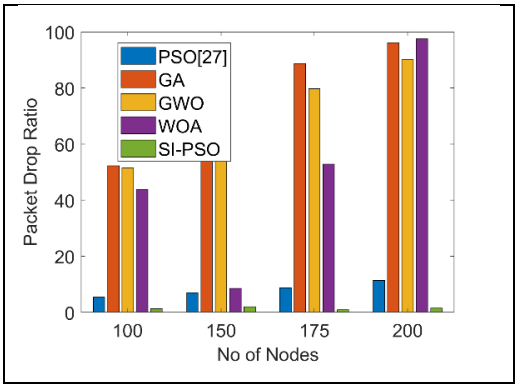

Fig. 8. Analysis on Packet drop ratio for adopted and traditional Models

6.8 Risk Analysis

The risk analysis for varying count of nodes is illustrated in Fig. 9. This say about the probability of the risk linked in identifying the optimal path and transmission of the data packets. Moreover, the proposed SI-PSO model holds superior outcomes than other traditional models for node 100. In all the cases, the adopted model exhibits the least value as the best model in MANET for trust aware secure routing.

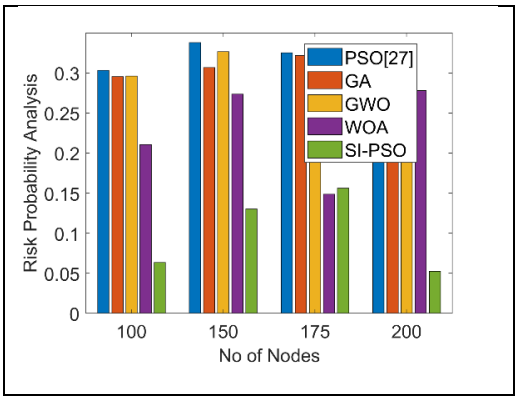

Fig. 9. Risk Analysis for adopted and traditional Models

6.9 Trust Analysis

Fig. 10 illustrates the trust analysis of the presented scheme to the existing approaches. Here, the trust values of the proposed work are higher for all node count. In addition, the proposed SI-PSO approach achieved highest trust value for node 175; while the traditional models like PSO, GA, GWO, and WOA has lowest trust value. Further, the presented work has maximum trust value (~5.8) for node count 150 than traditional PSO, GA, GWO, and WOA approach, respectively.

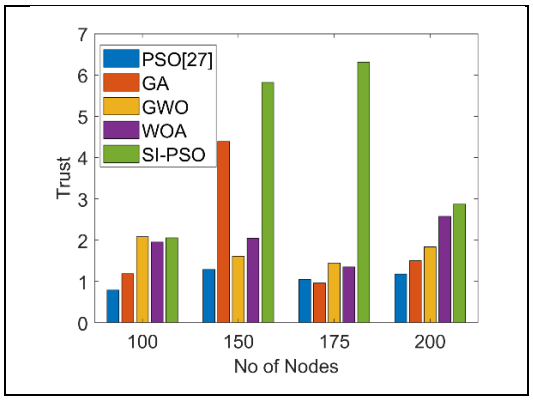

Fig. 10. Trust Analysis for adopted and traditional Models

6.10 Convergence Analysis

The convergence analysis of adopted SI-PSO scheme to the extant approaches for different iterations ranges from 0, 20, 40, 60, 80, and 100 is demonstrated in Fig. 11. Fig shows a decrement of cost function with increased iterations. In the graph, it is clearly shown that the adopted SI-PSO method obtained minimal cost values than other compared methods. The performance of proposed SI-PSO method at 80th iteration is (~1.2) lower values with better outcomes for node 150 to the extant approaches including PSO, GA, GWO and WOA, correspondingly. From the convergence analysis graph, the proposed SI-PSO method has shown better resultant outcomes.

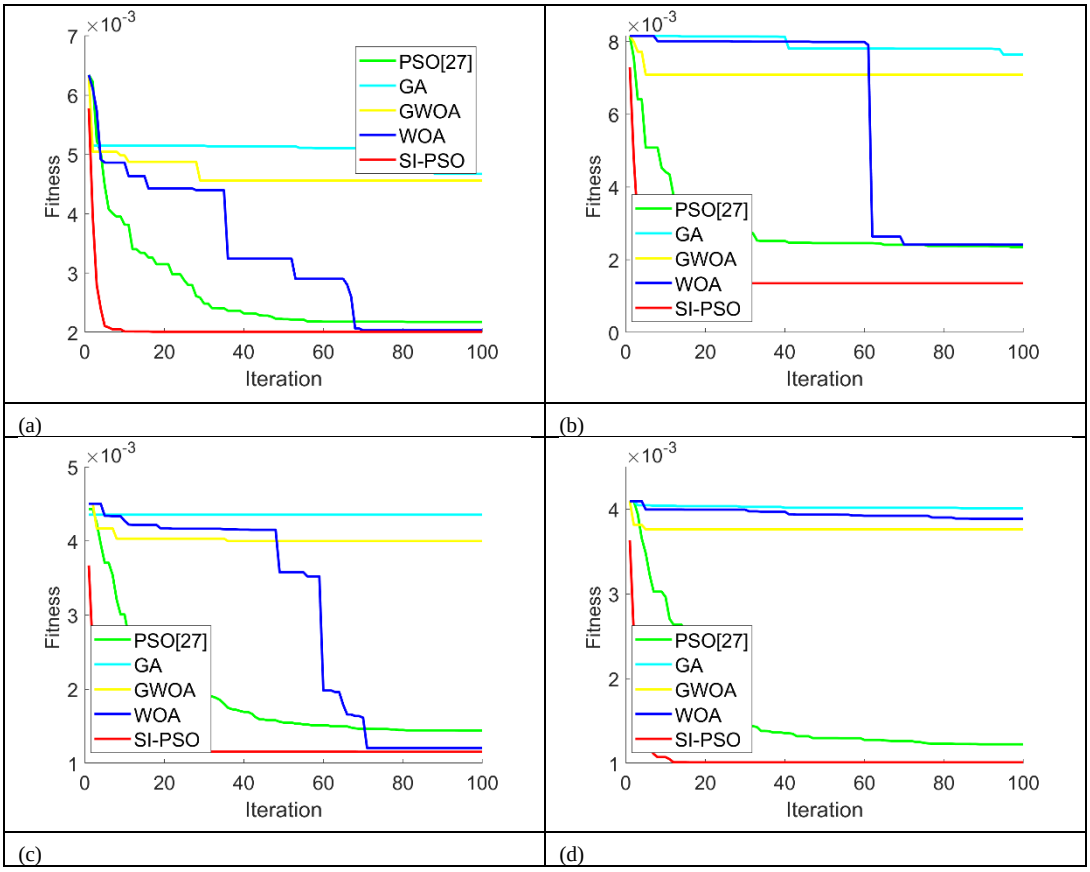

Fig. 11. Convergence Analysis of the adopted scheme to the traditional approaches for (a) node 100, (b) node 150, (c) node 175, and (d) node 200

6.11 Analysis on Computational time

The computational time consumed by the adopted SI-PSO model and the extant approaches for varying node count is shown in Table VI. The presented SI-PSO model

shows the lowest computational time than the existing one. The unit of the computational time is in Seconds. In addition, the proposed SI-PSO method is (~36.85) lower values with better outcomes for node 150 than the traditional models PSO, GWO and WOA, correspondingly.

Table 1. Evaluation on Computational Time

Approach	Node-100	Node-150	Node-175	Node-200
PSO[27]	17.36362	37.4027	46.68733	52.28492
GA [33]	14.61194	32.91267	41.94701	52.00466
GWO [35]	140.2613	299.1416	377.7777	509.5856
WOA [34]	169.9888	292.6161	400.7701	527.9015
SI-PSO	16.94271	36.83512	47.20496	54.39663

7 Conclusion

This paper has introduced a new trust-aware routing in MANET that ensures the trust level among the nodes. For this, a new trust rate estimation process was introduced based on energy and mobility of nodes exist. Thereby, a SI-PSO algorithm was proposed for choosing the optimal trust aware route for data transmission. The optimal route selection was performed by considering certain parameters like trust rate (security), PDR, distance, congestion, energy, and as well. The performance of the adopted work was examined to the existing schemes regarding Energy, Delay, and Network Lifetime. Further, the proposed SI-PSO model attained lowest energy (~0.1) with better performance than other existing models for node count 200. Moreover, the GA approach has the highest level of congestion for node 100, 150, and 175; while the presented SI-PSO work has the lowest congestion level. Likewise, the presented SI-PSO model attained the lowest value (~2) than other traditional models like PSO (~8), GA (~90), GWO (~80), and WOA (~52), respectively for the count of node 175. Further, the mean energy of the presented SI-PSO model was the lowest value with better outcomes for node 200 than extant models like PSO, GA, GWO, and WOA, correspondingly.

References

1. Usha, M.S., Ravishankar, K.C. Implementation of Trust-Based Novel Approach for Security Enhancements in MANETs. SN COMPUT. SCI. 2, 257 (2021). https://doi.org/10.1007/s42979-021-00628-2
2. Devi, V.S., Hegde, N.P. Multipath Security Aware Routing Protocol for MANET Based on Trust Enhanced Cluster Mechanism for Lossless Multimedia Data Transfer. Wireless Pers Commun 100, 923–940 (2018). https://doi.org/10.1007/s11277-018-5358-5.
3. Sathyaraj, P., Rukmani Devi, D. Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method. J Ambient Intell Human Comput 12, 6987–6995 (2021). https://doi.org/10.1007/s12652-020-02358-4
4. Merlin, R.T., Ravi, R. Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET. Wireless Pers Commun 104, 1599–1636 (2019). https://doi.org/10.1007/s11277-019-06120-8.

5. Anitha Josephine, J., Senthilkumar, S. Tanimoto Support Vector Regressive Linear Program Boost Based Node Trust Evaluation for Secure Communication in MANET. Wireless Pers Commun 117, 2973–2993 (2021). https://doi.org/10.1007/s11277-020-07209-1
6. Ambekar, R.K., Kolekar, U.D. T-TOHIP: Trust-based topology-hiding multipath routing in mobile ad hoc network. Evol. Intel. (2019). https://doi.org/10.1007/s12065-019-00280-z
7. Rajeswari, A.R., Kulothungan, K., Ganapathy, S. et al. A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. Peer-to-Peer Netw. Appl. 12, 1076–1096 (2019). https://doi.org/10.1007/s12083-019-00766-8
8. Kukreja, D., Sharma, D.K. T-SEA: trust based secure and energy aware routing protocol for mobile ad hoc networks. Int. j. inf. tecnol. (2019). https://doi.org/10.1007/s41870-019-00392-w
9. Veeraiah, N., Krishna, B.T. An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evol. Intel. (2020). https://doi.org/10.1007/s12065-020-00388-7
10. Tripathy, B.K., Jena, S.K., Bera, P. et al. An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks. Wireless Pers Commun 114, 1339–1370 (2020). https://doi.org/10.1007/s11277-020-07423-x
11. Nivedita, V., Nandhagopal, N. Improving QoS and efficient multi-hop and relay based communication frame work against attacker in MANET. J Ambient Intell Human Comput 12, 4081–4091 (2021). https://doi.org/10.1007/s12652-020-01787-5
12. Jamaesha, S.S., Bhavani, S. A secure and efficient cluster based location aware routing protocol in MANET. Cluster Comput 22, 4179–4186 (2019). https://doi.org/10.1007/s10586-018-1703-4.
13. Hemalatha, R., Umamaheswari, R. & Jothi, S. LF Distribution and Equilibrium Optimizer Based Fuzzy Logic for Multipath Routing in MANET. Wireless Pers Commun 120, 1837–1861 (2021). https://doi.org/10.1007/s11277-021-08537-6
14. Tamil Selvi, P., Suresh GhanaDhas, C. A Novel Algorithm for Enhancement of Energy Efficient Zone Based Routing Protocol for MANET. Mobile Netw Appl 24, 307–317 (2019). https://doi.org/10.1007/s11036-018-1043-x
15. Desai, A.M., Jhaveri, R.H. Secure routing in mobile Ad hoc networks: a predictive approach. Int. j. inf. tecnol. 11, 345–356 (2019). https://doi.org/10.1007/s41870-018-0188-y
16. V S, J., M S K, M. Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks. J Wireless Com Network 2018, 25 (2018). https://doi.org/10.1186/s13638-017-1001-5
17. Rajashanthi, M., Valarmathi, K. A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs. Wireless Pers Commun 112, 75–90 (2020). https://doi.org/10.1007/s11277-019-07016-3
18. Pushpalatha, K., Karthikeyan, M. A generalized framework for disruption tolerant secure opportunistic routing during emergency situations using MANETs. Cluster Comput 22, 9905–9913 (2019). https://doi.org/10.1007/s10586-018-1849-0
19. Kukreja, D., Dhurandher, S.K. & Reddy, B.V.R. Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack. J Ambient Intell Human Comput 9, 941–956 (2018). https://doi.org/10.1007/s12652-017-0496-2
20. M V S S, N., Babu, A.R. An efficient mobility aware stable and secure clustering protocol for mobile ADHOC networks. Peer-to-Peer Netw. Appl. 13, 1185–1192 (2020). https://doi.org/10.1007/s12083-019-00868-3
21. Kushwah, R., Tapaswi, S. & Kumar, A. A Detailed Study on Internet Connectivity Schemes for Mobile ad Hoc Network. Wireless Pers Commun 104, 1433–1471 (2019). https://doi.org/10.1007/s11277-018-6093-7

22. Srivastava, A., Gupta, S.K., Najim, M. et al. DSSAM: digitally signed secure acknowledgement method for mobile ad hoc network. J Wireless Com Network 2021, 12 (2021). https://doi.org/10.1186/s13638-021-01894-7
23. Kumar, S. Prediction of Node and Link Failures in Mobile Ad Hoc Network Using Hello Based Path Recovery Routing Protocol. Wireless Pers Commun 115, 725–744 (2020). https://doi.org/10.1007/s11277-020-07596-5
24. Vatambeti, R. A Novel Wolf Based Trust Accumulation Approach for Preventing the Malicious Activities in Mobile Ad Hoc Network. Wireless Pers Commun 113, 2141–2166 (2020). https://doi.org/10.1007/s11277-020-07316-z
25. Selvakumar, K., Seethalakshmi, N. Secure group key management protocol for mobile ad hoc networks. Cluster Comput 22, 11989–11995 (2019). https://doi.org/10.1007/s10586-017-1535-7
26. B. R. Rajakumar, "Impact of Static and Adaptive Mutation Techniques on Genetic Algorithm", International Journal of Hybrid Intelligent Systems, Vol. 10, No. 1, pages: 11-22, 2013, DOI: 10.3233/HIS-120161
27. Devi Manickavelu, Rhymend Uthariaraj Vaidyanathan ,"Particle swarm optimization (PSO)-based node and link lifetime prediction algorithm for route recovery in MANET",EURASIP Journal on Wireless Communications and Networking,2014.
28. B. R. Rajakumar, "Static and Adaptive Mutation Techniques for Genetic algorithm: A Systematic Comparative Analysis", International Journal of Computational Science and Engineering, Vol. 8, No. 2, pages: 180-193, 2013, DOI: 10.1504/IJCSE.2013.053087
29. S. M. Swamy, B. R. Rajakumar and I. R. Valarmathi, “Design of Hybrid Wind and Photovoltaic Power System using Opposition-based Genetic Algorithm with Cauchy Mutation”, IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), Chennai, India, Dec. 2013, DOI: 10.1049/ic.2013.0361
30. Aloysius George and B. R. Rajakumar, "APOGA: An Adaptive Population Pool Size based Genetic Algorithm", AASRI Procedia - 2013 AASRI Conference on Intelligent Systems and Control (ISC 2013), Vol. 4, pages: 288-296, 2013, DOI: https://doi.org/10.1016/j.aasri.2013.10.043
31. B. R. Rajakumar and Aloysius George, "A New Adaptive Mutation Technique for Genetic Algorithm", In proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pages: 1-7, December 18-20, Coimbatore, India, 2012, DOI: 10.1109/ICCIC.2012.6510293
32. Hongbo Liu, Ajith Abraham, Václav Snášel, Seán McLoone, "Swarm scheduling approaches for work-flow applications with security constraints in distributed data-intensive computing environments", Information Sciences, vol.192, pp. 228-243, 1 June 2012.
33. Theodoros D. Vrionis, Xanthi I. Koutiva, and Nicholas. A. Vovos,"A Genetic Algorithm-Based Low Voltage Ride-Through Control Strategy for Grid Connected Doubly Fed Induction Wind Generators",IEEE Transactions on Power Systems, vol. 29, no.3, May2014.
34. Seyedali Mirjalili, Andrew Lewis, "The Whale Optimization Algorithm" Advances in Engineering Software, vol. 95, pp. 51-67, May 2016.
35. Seyedali Mirjalili, Seyed Mohammad Mirjalili, Andrew Lewis, "Grey Wolf Optimizer" Advances in Engineering Software, Volume 69, March 2014, Pages 46-61.
36. kulkarni,Senthil Murugan T, "Hybrid Weed-Particle Swarm Optimization Algorithm and C-Mixture for Data Publishing", Multimedia Research, Vol.2,No.3, pp.33-42,2019.
37. Vasamsetti Srinivas,Santhirani Ch, "Hybrid Particle Swarm Optimization-Deep Neural Network Model for Speaker Recognition", Multimedia Research, Vol.3,No.1, pp.1-10,2020.

38. Cristin R,Gladiss Merlin N.R,Ramanathan L,Vimala S, "Image Forgery Detection Using Back Propagation Neural Network Model and Particle Swarm Optimization Algorithm", Multimedia Research, Vol.3,No.1, pp.21-32,2020.
39. Rajeshkumar G, "Hybrid Particle Swarm Optimization and Firefly Algorithm for Distributed Generators Placements in Radial Distribution System", Journal of Computational Mechanics, Power System and Control, Vol.2,No.1, pp.41-48,2019.
40. Gayathri Devi K.S, "Hybrid Genetic Algorithm and Particle Swarm Optimization Algorithm for Optimal Power Flow in Power System", Journal of Computational Mechanics, Power System and Control, Vol.2,No.2, pp.31-37,2019.
41. Rupam Gupta Roy, "Economic dispatch problem in power system using hybrid Particle Swarm optimization and enhanced Bat optimization algorithm", Journal of Computational Mechanics, Power System and Control, Vol 3, No 3, 2020.
42. Fatema Murshid AlBalushi, "Chaotic based Hybrid Artificial Sheep Algorithm - Particle Swarm Optimization for Energy and Secure Aware in WSN", Journal of Networking and Communication Systems, Vol.2,No.2, pp.37-48,2019.
43. Nitin Deotale,Uttam Kolekar,Anuradha Kondelwar, "Self-adaptive Particle Swarm Optimization for Optimal Transmit Antenna Selection", Journal of Networking and Communication Systems, Vol.3,No.1, pp.1-10,2020.
44. Haridas,S & Rama Prasath,A (2020). Enhancement of Network Lifetime in MANET: Improved Particle Swarm Optimization for Delayless and Secured Geographic Routing. Jour of Adv Research in Dynamical & Control Systems, Vol. 12, 07-Special Issue, 2020