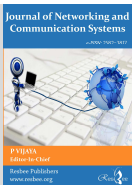
Resbee Publishers

Journal of Networking and Communication Systems

Received 16 December, Revised 20 February, Accepted 27 March



Routing Protocol using optimization algorithm in Delay Tolerant Network

P Pavan Kumar
Associate professor, Dept of CSE
CMR Institute of Technology, Bengaluru, Karnataka, India
pavan.panakanti@cmritonline.ac.in

Abstract: The Delay Tolerant Network (DTN) is exploited that is an effectual technology without definite incessant linkage in the network in order to provide effectual communication between the devices. In DTNs, numerous conventional routing techniques use the benefit of message replication in order to attain the maximum message delivery rate. However, they experience high communication overhead due to the shortage of effective models to control the message replication. Therefore, this work exploits a trust-based multipath routing protocol to exploit the diverse paths amid source and the destination to alleviate energy restraints. The main intention is to ascertain the optimal path from the whole paths that are present between the sender and destination node. In routing protocol, to enhance security, the metrics such as distance, trust factors are represented as the important modules. On the basis of the metrics, the multipath routing is performed using Particle Swarm Optimization (PSO) – Grey Wolf Optimization (GWO)approach. Subsequent to thereputation and trust-based Context Aware Routing (RCAR) protocol is used to choosethe optimal path with a high trust factor. Moreover, the trust is designed by taking into consideration of trust factors, such as direct, indirect, forwarding rate, history, and availability factors, as well asa utility function. The developed optimization algorithmoutperforms the conventional models with minimum delay, and maximum Packet Delivery Rate (PDR), maximum throughput correspondingly.

Keywords: Communication, Delivery Rate, Optimization Algorithm, Routing Protocol, Trust Factors.

Nomenclature

Abbreviations	Descriptions
POI	Point Of Interest
LDR	Large Data Routing
DoS	Denial of Service
PSO	Particle Swarm Optimization
GWO	Grey Wolf Optimization
RCAR	Reputation And Trust-based Context Aware Routing
MANET	Mobile Adhoc Network
PDR	Packet Deliver Rate
DTN	Delay-Tolerant Networking

1.Introduction

The main characteristics of the DTNs areextremely partitioned and intermittently linked ad-hoc networks whichaspire to aid theextensive delays and loss of data in confrontscases and environments. DTNs applications such as tactical as well as military systems, communication in rural as well as remote areas and developing countries, data offloading networks, interplanetary networking, disaster recovery networks, vehicular communication, wildlife tracking/monitoring sensor networks, as well as mobile crowdsensing networks. In DTNs, to aid the end-to-end communication, the store-carry-as well as-forward routing techniqueon the basis of the node mobility is exploited, here; messages are in the interimsaved and performed by a node till a communication chance with subsequent relay node occurs [1].

Opportunistic networks or DTNs are networks in that an end-to-end path between nodes set is not foreverassured. Some instances of such networks are deep space networks, underwater networks, ruralas well asremote area communication so onthat are operating in tremendous terrestrial environments. In

https://doi.org/10.46253/jnacs.v4i2.a3

DTN, the standard idea over the routing is store-carry as well as forward model, in thatevery node needs tosaveas well as cart the messages if it does not discover any relay/neighbor node to forward untilit discovers a contact to forward advance [2].

In order to enhance protocols as well as the approaches, extensive research studies have been performed for MANET which carries out in confronting disaster cases, and at last that an important option to handle the malfunctions and portioned networks are DTNs. For challenged networks, the DTNs were adopted to cope up with the in-attendance of end-to-end connectivity among devices for eg., rural communities, interplanetary transmissions, and disaster cases. Conventional opportunistic protocols are not capable to detain the specification of disaster cases that need a solution that possesses the energy costs awareness as well as other specifications namely participant nodes, and disaster areas [12].

Numerous conventional DTN routing protocols concentrate to choose a relay node effectively to maintain neighboring nodes set [15] Hence, the message is assured to be delivered to the receiver node [13]. Therefore, numerous studies havebeen performed regarding the development of intelligent relay chosen schemes by exploiting the heuristics namely delivery probability, delivery mobility patterns, historical contacts, social relationships, so on. In addition, numerous DTN application cases, (predominantly, tremendous terrestrial environments) be short of frequent monitoring, which demands safe communication between nodes in the network [14].

The main objective of this work is to present a PSO-GWO to choose the path optimallyfrom sender to receiver node. The developedPSO-GWO is the integration of PSO in GWOthat aspires in formulates the optimal path safely. Finally, the fitness model is formulated and considers numerous trust metrics besides with usefulness function to carry out secure routing. Moreover, fitness is considered the maximum function.

2. Literature Review

In 2021, Tuan Le [1], developed anLDR protocol thatdivides a high amount of data into small portions and carries out and forwards at the chink level against the multiple consecutive contacts. A probabilistic technique was modeled and that integrates the contact frequency, inter contact time, as well as contact duration. The technique was exploited to calculate edge weights in a multi-hop contact frequency as well as a contact graph between network nodes.In 2020,Shudip Datta and Sanjay Madria [2], developed a model which was capable to dynamically update the record of POI on the basis of thepresent photo metadata, with minimized bandwidth utilization, energy, and storage at DTN nodes in order to send only significantphotos of POIs. In 2020, Erika Rosas et al [3], developed a context-aware self-adaptive routing protocol for DTN, which was capable to adapt to diverse cases, permitting the network participants of the network to routinely choose a DTN protocol based on previous performance of the routing protocols in the present case. In order to implement this, various measures were used with different techniques in disaster cases.In 2019, El ArbiAbdellaouiAlaoui et al [4], suggested a novel solution to convene the requirements and resolve DTN routing-related issues. Moreover, the solution was on the basis of DTN routing protocol with the QoS. Based on the integration of the benefit of the forwarding as well as following scheme to model a DTN routing protocol which was highly adapted to the heterogeneous kinds of novel technologies types of equipment to promise a superior swapping of information among such kinds of types of equipment.In 2019, Sobin C C et al [5], worked on the smart relay chosen schemes for DTNs. Nevertheless, the security affects namely integrity as well as confidentiality, and the message was transferred in the conventional DTN routing state-of-the-art. Therefore, the security problems were addressed in this paper related to the DTN message forwarding as well as adopted a secure technique for the forwarding message in DTN.

3. Description of DTN

DTN moves within the fixed area, which comprises several wireless nodes. For instance, the node is represented as the device that is embedded in the bus or held by humans.Based on the following scheme the messages are fed in the network. If the router is in attendance amid the source u and the destination v, on the basis of the standard routing protocol, the message is passed named synchronous routing. The sender pursued an asynchronous routing scheme if the route failed to access in order to deliver the message to the forward node p with maximum value. Moreover, in the local buffer, the node p saves message till the route is set up or it encounters the other forwarding node p' with a superior message delivery value to the receiver.

In some cases, on the basis of the synchronous routing to deliver the message to the destination the node is used. Subsequently, the messages are passed to the forwarding node; the node is subjected to

asynchronous routing. If the message is not attained at the last destination, the routing steps will be repeated. The most significant matter is if the buffer size is minimum, then the message will mislay while the new message is inwards [8]. By numerous attacks, the DTN is vulnerable due to some nodes act in a self-interested way, and it is unsuccessful to aid others in forwarding the message to conserve the restricted resources such as buffer as well as power. Moreover, few nodes act as malicious; the adversary controls the nodes to create the black hole, grey hole, DoS attacks via networks by minimizing maliciously received message packets,interfering message packets, or creating fake message packets [9]. Fig 1 demonstrates the block diagram of the proposed model for Delay Tolerant Networking.

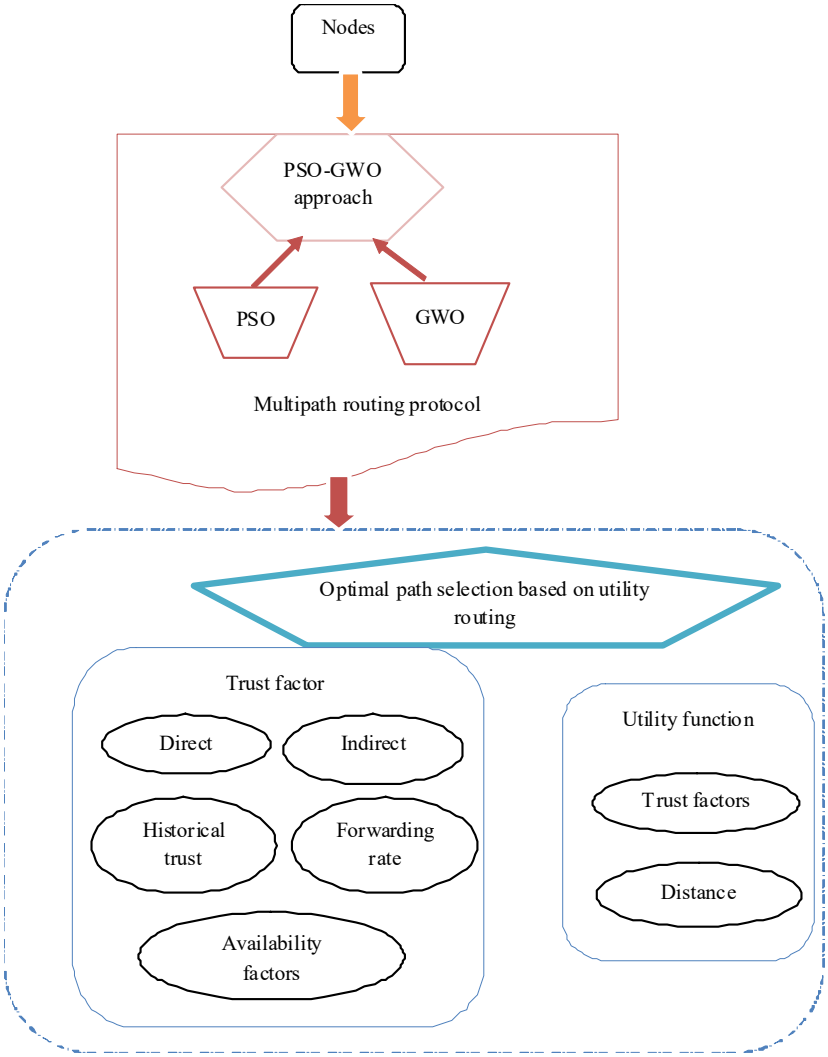


Fig.1*Block diagram of the proposed model for Delay Tolerant Networking*

3.1 Fitness Function

For all h paths, the fitness function is computed so that the optimal route is selected by exploiting the adopted optimization model. The path contributes to the indirect, direct, availability, historical trust as well as the forwarding factor is selected as the optimal path. The fitness function is computed as follows:

$$\text{Fitness, } F = \sum_{u=1}^{h} \sum_{\substack{v=1 \\ x \neq v}}^{k} \left[P_{vx}^{u} + \left(1 - q_{vx}^{u} \right) \right] \tag{1}$$

whereas the total nodes in v^{th} path are signified as k h signifies the number of paths, and the P_{vx}^{u} is stated as follows:

$$P_{vx}^{u} = \text{Trusts}\left(G_{vx}^{u} + H_{vx}^{u} + K_{vx}^{u} + L_{vx}^{u} + B_{vx}^{u} \right) \tag{2}$$

whereas, H_{vx}^{u}, G_{vx}^{u}, K_{vx}^{u}, L_{vx}^{u}, and B_{vx}^{u} represented as direct as well as indirect trust, availability factor as well as forwarding rate factor. The q_{vx}^{u} is stated as,

$$q_{vx}^{u} = B_q\left(M_v^{loc}, M_x^{loc}\right) \tag{3}$$

whereas, $B_q\left(M_v^{loc}, M_x^{loc}\right)$ indicates the Euclidean distance amid the location of the node M_v and M_x.

3.2 RCAR for Secure Routing

Securely, to transfer the data as well as to evade the loss of packet in DTN, it is important to adopt a secure routing model to transfer the packet to find a secure route by not considering any path conjunction.

Moreover, to select the forwarding node, the RCAR is used. Let node c transmitsa message n to p^{th} node. If route availableamid node c to p, c^{th} node carries outasynchronous or synchronous routing is performed. The sender node selects subsequent hop m to reach the destination node if the synchronous routing is available based on the DSDV protocol. Subsequent to the choice of the next hop, by exploiting or not exploiting the condition $L_{cm} > 0$ the node c checks the blackhole is available. Therefore, the sender transmits the message if the blackhole is not available. If $L_{cm} = 0$, the node attempts to carry out asynchronous routing. Moreover, the transmitterselectsa node q with maximum L_{cm}. In the local buffer, the node q saves while receiving the message. Conversely, if $L_{cm} > 0$ the circumstance is satisfied the sender transmits the message to the subsequent hop,or elsethe message is saved in its local buffer. In this scenario, nodes q and c try to forward messages available in the local buffer.

3.3 Local utility function

The local utility function is calculatedby exploiting the trust metrics, like direct, indirect, availability factor, historical trust, forwarding rate factor, besides with utility function. Presume the Q_{yz} indicates the reputation of y^{th} node at z^{th} node as well as V_u indicates utility function of u. Subsequently, the global utility function formulations arestated as follows,

$$J_{yz} = \sum_{v=1}^{k} V_u \tag{4}$$

Subsequently, the local utility function is calculatedas follows,

$$V = \left(G_{vx} + H_{vx} + K_{vx} + L_{vx} + B_{vx}\right) * U_{vx} \tag{5}$$

whereas, v indicates evaluation node and the node to be estimatedareindicated as x.

i) Trust model

In DTN, trust is considered an important metric for the precise communication procedure. Hence, identifying the trusted nodes available in b^{th} path is calculated based on the trust factor.

a. Direct trust

The local trust is also stated as the direct trust [1] that is carried out on the basis of the satisfaction prevailing amid the interaction of the nodes.The satisfaction degree is estimated based on the direct trust amid the nodes x as well as v. While the v^{th} node satisfies with the x^{th} node, the satisfaction degree is high, presents the direct trust. If the v^{th} node trusts by the x^{th} node the direct trust G_{vx} is attained. Subsequently, the direct trust formulation is stated as below, $G_{vx} = (1-\beta) * C_{vx}(r) * E_{vx}(r) * N_{vx}(r) + \beta * G_{vx}(r-1)$ (6)whereas E_{vx} indicates the packet loss rate factor, consistency factor is stated as $N_{vx}(r)$, $C_{vx}(r)$ indicates sending rate factor at the time r, and β indicates constant and the value ranges from 0 to 1.

b. Indirect trust

Each node is subjected to analyze if a subsequent hop is trusted after selecting the next hop if a next-hop node is trusted by calculating the next-hop node trust. Hence, to reduce the deviation, the indirect trust [10] value is considered and the formulation is stated as below:

$$H_{vx} = w_r\left(G_{vx}, G_{xj}\right) \tag{7}$$

whereas, G_{xj} indicates direct trust of an estimated x^{th} node by j^{th} node as well as G_{vx} indicates the direct trust of an estimated x^{th} node by v^{th} node. The $w_r(.)$ is calculatedbased on the actual network requirements.

c. Historical trust

Historical trust [10] is performedbased on theobject's behavior or interaction. Moreover, to calculate the trust value, the record is used. The K_{vx} indicates the historical trust, and it is stated as,

$$K_{VX} = \frac{\alpha \times K_{VX}(h-1) + XT_{VX}(h-1)}{2} \tag{8}$$

whereas α indicatesarbitrarycount ranging from $0\ and\ 1$, the transactions areindicated as h and XT_{VX} signify recent trust.

d. Forwarding rate factor

The DTN nodes compriserestricted-energy whichrequires to be relayed whiletransferring and sensing the data. Hence, it is importantto evaluate the node is attacked or not by calculating the data forwarding nodes. The forwarding rate factor [11] function is stated as,

$$L_{VX} = \frac{ACK_{VX}(r)}{TP_{VX}(r)} \tag{9}$$

whereas, $ACK_{VX}(r)$ indicates total feedback packets, and $TP_{VX}(r)$ indicates the count of forwarding packets.

e. Availability factor

In the availability factor, the node is not usedbecause of the network channel interference;therefore it is suitableto evaluate the node by examining or passing the data packet. The availability factor is stated as,

$$B_{VX} = \frac{ACK_{VX}(r)}{ACK_{VX}(r) + NACK_{VX}(r)} \tag{10}$$

whereas, $ACK_{VX}(r)$ indicates the responded packets, and $NACK_{vx}(r)$ indicates several un-responded packets. Subsequently, the utility is stated as,

$$U_{VX} = Q\left(\frac{K}{B}\right) \tag{11}$$

whereas, $Q\left(\frac{K}{B}\right) = \frac{1}{\sqrt{2\Pi\mu^2}} \exp\left(\frac{-(\omega/\gamma)^2}{2\mu^2}\right)$.

whereas, the event delayvariance to event attack and K states the trust factors.

4. Proposed PSO-GWO optimization algorithm

The PSO approach possesses some disadvantages such as that are trapped to the local minima while it is fed to a maximum constraint, although it possesses a few benefits namely robustness, simplicity, and also it can experiment simply. Conversely, GWO evades and is trapped locally and it preserves a balance amid the exploitation as well as exploration [7]. Therefore, both the amazing spotlights of both approaches are integrated into the proposed optimization algorithm.

In the PSO algorithm [6] the fitness function of each particle is estimated. Individual P_{best} and G_{best} are calculated. Each swarm velocity is updated based on eq. (12), and the position of the swarm is updated based on eq. (13). Then the fitness value for each particle is calculated. By exploiting eq. (14), for the next iteration, the optimal solution is chosen, c_1 and c_2 indicates the coefficients, ω indicates the initial weights,

$$v_i^{k+1} = \omega v_i^k + c_1 rn\left(P_{i,pbest}^k - x_i^k\right) + c_2 rn\left(P_{i,gbest}^k - x_i^k\right) \tag{12}$$

$$x_i^{new} = x_i + v_i \tag{13}$$

$$x_i^{k+1} = \left\{ \frac{x_{i,new} \text{ iff} \left(x_{i,new} \right) \leq f(x_i)}{x_i \text{ Otherwise}} \right\} \tag{14}$$

The final population of PSO represents the initial population of GWO.By exploiting the parameters based on eq. (15) and (16), are updated. For each search agent, the random location is generated. On the basis of the fitness model, the objective values are computed for the grey wolves. The parameters $a, A \text{ and } C$ are updated and the grey wolves are updated. For the next iteration, the optimal solution is selected by comparing the fitness models. $X_\alpha, X_\beta \text{ and } X_\delta$ are updated.

$$\vec{A} = 2.\vec{a}.\vec{r}_1 - \vec{a} \tag{15}$$

$$\vec{C} = 2..\vec{r}_2 \tag{16}$$

5. Experimental Procedure

In this section, the proposed method and the conventional model outcomes were demonstrated based on the evaluation measures. Here, the performance was performed regarding the packet delivery ratio rate, delay, and throughput rate. Moreover, the proposed was compared with the conventional models such as PSO, Genetic Algorithm (GA) and Artificial Bee Colony (ABC).

Fig 2,3, and 4 demonstrate the performance analysis of the proposed and conventional models such as PSO, GA, and ABC based on the various measures such as packet delivery ratio rate, delay, and throughput rate for no of users 10 and 20. Here, the overall analysis states that the minimum delay, maximum PDR, and throughput. In Fig 2, the performance analysis of the proposed model over the conventional models regarding the delay. Here, the proposed method is 20% better than the PSO, 25% better than the GA, and 40% better than the ABC for number of users=10. In Fig 3, the performance analysis of the proposed model over the conventional models regarding the throughput rate. Here, the proposed method is 12% better than the PSO, 13% better than the GA, and 33% better than the ABC for number of users=10. In Fig 3, the performance analysis of the proposed model over the conventional models regarding the packet detivery rate. Here, the proposed method is 11% better than the PSO, 10% better than the GA, and 29% better than the ABC for number of users=20.

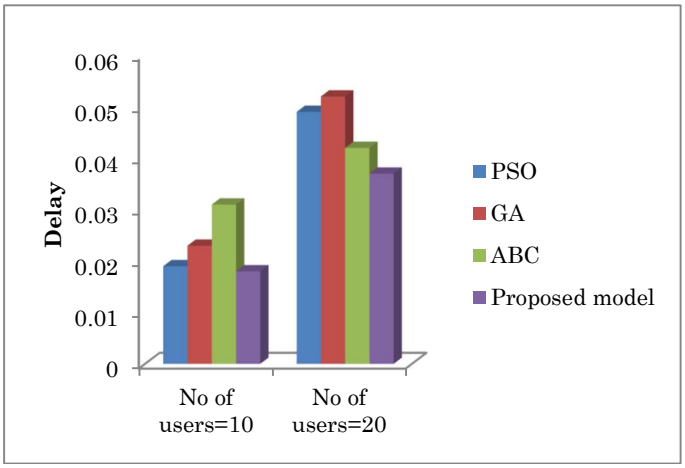


Fig. 2*Performance analysis of the proposed model regarding delay*

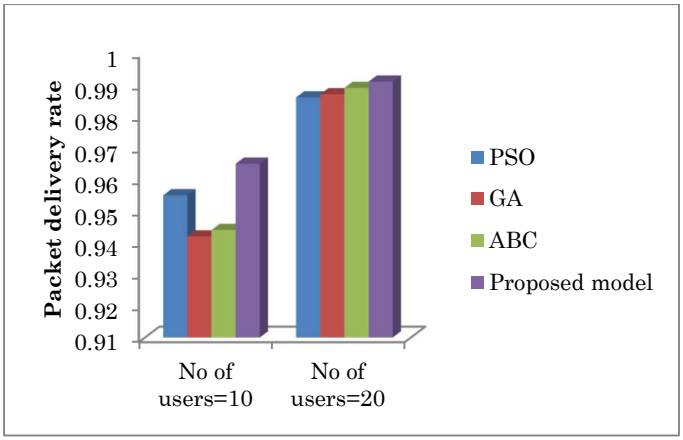


Fig. 3*Performance analysis of developed model regarding packet delivery rate*

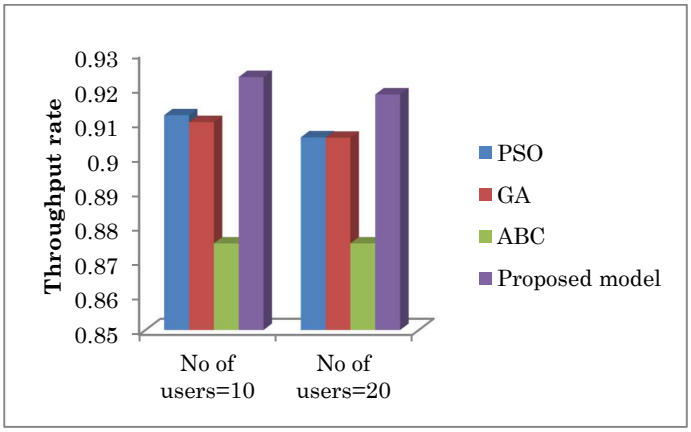


Fig. 4*Performance analysis of developed model regarding throughput rate*

6.Conclusion

Mobile devices are able of communicating, storing, and disseminating large data files over the network as technologies develop. Particularly communicating great data is demanding in DTNowing tobe short of connectivity and small contacts between network nodes. To make simpler the routing, conventional works frequentlytake no notice of the data size and duration of a contact. Specifically, the data always effectively arrives at the receiver once transmitted. Hence, these protocols are not appropriate in the data-intensive mobile era. The trust-enabled routing approach was worked in this paper called PSO-GWO to start multipath routing in DTN. The developedPSO-GWO wasmodeledas the integration ofPSO in the GWOtechnique. The techniqueimproved the energy effectivenessas well as maximizes the node's lifetime thus the algorithm performance was maximized. By exploiting the trust as well as distance factors, the developed technique and the fitness model were considered. The developed technique as well as the fitness model enhanced the complete performance of the network and aid to choose the optimal path to transfer data packets from sender to receiver node. Subsequent to that, by verifying the attendance of node in RCAR, the secure routing was experimentedwith by exploiting the direct, availability factors, indirect, forwarding rate as well as a utility function. Here, besidesadopted optimization, the fitness metric was also performed in order to estimate the secure routes. The developed model efficiency was calculated regarding the conventional techniques and revealed efficient outcomes with minimum delayand maximum throughput.

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] Tuan Le,"Multi-hop routing under short contact in delay tolerant networks", Computer Communications, vol.165, pp. 1-8, 2 November 2020.

[2] Shudip DattaSanjay Madria,"Efficient photo crowdsourcing with evolving POIs under delay-tolerant network environment", Pervasive and Mobile Computing, vol.67, 18 June 2020.

[3] Erika RosasFelipe GarayNicolas Hidalgo,"Context-aware self-adaptive routing for delay tolerant network in disaster scenarios", Ad Hoc Networks, vol. 102, 20 February 2020.

[4] El Arbi Abdellaoui AlaouiHanane ZekkoriSaid Agoujil,"Hybrid delay tolerant network routing protocol for heterogeneous networks", Journal of Network and Computer Applications, vol. 148, 5 October 2019.

[5] C C SobinCt LabeebaK Deepika Chandran," An Efficient method for Secure Routing in Delay Tolerant Networks", vol. 143, pp. 820-826, Procedia Computer Science19 November 2018.

[6] R. AbinayaR. Sowmiya,"Soft biometric based keystroke classification using PSO optimized neural network", Materials Today: Proceedings, Available online 28 February 2021.

[7] Mahdis Banaie-DezfouliMohammad H. Nadimi-ShahrakiZahra Beheshti,"R-GWO: Representative-based grey wolf optimizer for solving engineering problems", Applied Soft Computing17 March 2021.

[8] Gianluca Dini, Angelica Lo Duca,"Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network", Ad Hoc Networks, vol. 10, pp.1167–1178, 2012.

[9] Feng Li, Yali Si, Ning Lu, Zhen Chen, and Limin Shen, "A Security and Efficient Routing Scheme with Misbehavior Detection in Delay-Tolerant Networks", Security and Communication Networks, 2017.

[10] Zuo Chen, Min He, Wei Liang, and Kai Chen, "Trust-Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network", Journal of Sensors, 2015.

[11] Jinghua Zhu,"Wireless Sensor Network Technology Based onSecurity Trust Evaluation Model", International Journal of Online and Biomedical Engineering (iJOE), vol.14, no.4, pp.211-226, 2018.

[12] Amol V Dhumane,"Examining User Experience of eLearning Systems using EKhool Learners", Journal of Networking and Communication Systems, vol 3, no 4, October 2020.

[13] Jiarui Wang,"Hybrid Wolf Pack and Particle Swarm Optimization Algorithm for Multihop Routing Protocol in WSN", Journal of Networking and Communication Systems, vol 3, no 3, July 2020.

[14] Shruti Tambulunde,"Spiral Optimization Algorithm for Lifetime Enhancement of Wireless Multimedia Sensor Networks", Journal of Networking and Communication Systems, vol 4, no 1, January 2021.

[15] Deepak Rewadkar and Dharmpal Doye,"Traffic-aware Routing Protocol in VANET using Adaptive Autoregressive Crow Search Algorithm", Journal of Networking and Communication Systems, vol.1, no.1, October 2018

.