International Journal of Business Data Communications and Networking
Volume 17 • Issue 1 • January-June 2021

Harris Hawks Jaya Algorithm-Based Routing Protocol in Delay Tolerant Network

Pradosh Kumar Gantayat, Department of Computer Science and Engineering, Veer Surendra Sai University of Technology, Burla, India

Satyabrata Das, Department of Information Technology, Veer Surendra Sai University of Technology, Burla, India

ABSTRACT

This paper introduces a trust-based multipath routing protocol for exploiting different paths between source as well as destination to mitigate energy constraints. The key idea is to determine optimal path from the entire paths available among source and target node. To improve the security in routing protocol, the factors, like trust factors, and distance are considered as major components. Based on these parameters, the multipath routing is carried out based on HH-Jaya Algorithm. The HH-Jaya is designed newly by integrating Harris Hawks Optimization (HHO) and Jaya Algorithm. After that, the reputation and trust-based context aware routing (RCAR) protocol is utilized to select the optimal path with more trust factor. Here, the trust is modelled by considering trust factors, like direct, indirect, history, forwarding rate, and availability factors, in addition to the utility function. The proposed HH-Jaya outperformed other methods with minimal delay of 0.007 sec, maximal throughput of 0.913 for 10 user and maximal packet deliver rate (PDR) of 0.991 for 20 users respectively.

KEYWORDS

Delay Tolerant Network, Harris Hawks Optimization, Jaya Algorithm, Reputation and Trust-Based Context Aware Routing, Trust Factor

1. INTRODUCTION

Due to the rapid growth of communications and computing resources that leads to exchange the data among wireless mobile devices, like laptops, cell phones, portable devices, and the tablets, regardless of guaranteed any end-to-end connection exists. Thus, the DTN faced the challenges on the communication between the devices that loss connectivity continuously because of mobility (Wan, *et al.,* 2015). However, the DTN is the network paradigm in which the connectivity between mobile nodes are not guaranteed continuously. In the network, each node participates in hop by hop, message routing among the destination and source of message. In addition, the DTN nodes containing less capacity of buffer and battery. Additionally, the mobility of the nodes are increased in network that communicates complex from the end to end among the nodes (Fall, 2003; Ababou, *et al.,* 2018). Thus, the DTN is introduced for solving the challenging situations in restricted networks with intermittent disruption, less energy, and the sparse density. Thus, the DTN having frequent disconnections due to low transmission range, nodes mobility, and the dynamic topology, along with several features,

DOI: 10.4018/IJBDCN.2021010103

self-organizations, without central administrations, and self-organizations (Fall & Farrell, 2008; Guo, *et al.,* 2017). The messages that are delivered through forward paradigm and store carry to reached their destinations (Ayub & Rashid, 2019).

The DTNs is introduced for the communication purpose in several fields, such as post-disaster scenario, interplanetary communication in the space, rural communication and so on. Unlike conventional wireless or wired networks, the communication is performed dynamically at the node pairs where the node movements are unpredictable in the network (Ababou, *et al.,* 2018; Roy, *et al.,* 2018). The DTN application are as follows: underwater communication, urban areas, military purposes, and deep space communication. In the recent years, the NASA works with DTN in the Deep space project (Pathak, *et al.,* 2017), but still the DTN faces several limitations. For instance, due to the absence of synchronous end-to-end connectivity, and the problem in forwarding the messages to destinations that results to limited message delivery rate and long transmission delay. The constraints parameters, like communication bandwidth, battery power, and the storage capacity are considered to increase the delivery rate of message. The DTN refer to the specific routing schemes for forwarding messages for delivering the messages based on probability-based (Musolesi & Mascolo, 2009; Dini & Duca, 2012) and epidemic-based (Lindgren, *et al.,* 2003; Dini & Duca, 2012). In probability-based approaches, the sender sends the message to the node with highest probability of the message delivery (Dini & Duca, 2012) whereas, in epidemic, the several messages are transmitted and one reaches the receiver. Hence, the routing is very challenging due to the DTN characteristics (Voyiatzis, 2012; Guo, *et al.,* 2017). DTN routing protocols (Guo, *et al.,* 2017) are partitioned into multi copy and single copy protocols. In single (Spyropoulos, *et al.,* 2004), the node forwards the unique message copy to their neighbors. Therefore, the message containing one carrier for reaching their destination. However, the single copy protocols needless resources with the long delivery delay. Thus, the multi copy protocols (Spyropoulos, *et al.,* 2007) forward and create various copies of every message. For example, the epidemic protocol produces several copies of the buffered messages and passes to the connected nodes, and thus results higher buffer space consumption, bandwidth and energy. Here, the mobile nodes are not equipped with large resources and the different solution is needed for managing resource requirement (Ayub, *et al.,* 2017). The performance of routing is significantly improved by exploiting the utilization of regular patterns. Another scheme, named 3R (Vu, *et al.,* 2011) is fine-grained history-enabled routing where the pair-wise encounters contact time is recorded accurately. When maintaining fine-grained encounter history, the predictability of encounter in the 3R is the time-dependent. Consequently, the 3R is also the forwarding-enabled approach (Wan, *et al.,* 2015).

The purpose of the research is to design the trust-based routing protocol for establishing the optimal paths for data transmission in DTN. The goal of multipath routing is to provide the source node a set of choices in order to select the suitable path for transmitting the data packets to the destination node. However, the trust-aware routing faces a trade-off by compromising distance and delay. Thus, in order to mitigate these issues and for providing trust-aware secure multipath routing, the newly designed optimization, namely HH-Jaya algorithm is proposed by reducing the trade-off and managing the network. The proposed HH-Jaya incorporates Harris Hawks in Jaya for initiating the multipath routing. Consequently, the secure routing is carried out by checking the presence of node based on RCAR. In addition, the fitness function is designed considering direct, indirect, history, and availability factors, forwarding rate along with utility function. The proposed method enhanced the energy efficiency of network by increasing the lifetime of network.

The major contribution of the research paper is illustrated below:

- *Proposed HH-Jaya algorithm for multipath routing in DTN:* The proposed HH-Jaya is employed for choosing the path optimally from source to destination. The proposed HH-Jaya is the combination of Harris Hawks in Jaya aims in formulating the optimal path in the secure manner;

- *Devise a fitness function:* The fitness function is newly devised considering several trust factors along with utility function to perform secure routing. Here, the fitness is considered as the maximal function.

2. MOTIVATION

In this section, some of the previous multipath secure routing methods in DTN along with their demerits and merits are explained, which motivates the researchers to develop a new method to perform multipath secure routing in DTN.

2.1 Literature Survey

The eight conventional strategies employed for multipath secure routing in DTN is elaborated below: Dini & Duca, (2012) developed reputation-enabled protocol for the contrasting black holes in DTN. Here, each node handles the forwarding nodes reputation, and then the next forwarding nodes are selected with highest reputation. The developed model consists of node lists, aging, and acknowledgements, which makes the communication very effective for changing operation conditions. The method failed to deal with the selfish nodes. Ababou, *et al.,* (2018) presented Energy Efficient Routing Protocol on the basis of Fuzzy Ant colonies for selecting best relay between nodes. Then, the improved fuzzy logic system was introduced for making the decision. As the energy, nodes buffering, and mobility are very challenging while designing routing protocol. Thus, this framework uses encounters history among the nodes for determining the visibility between the nodes. The optimal delivery ratio and less overhead manages the battery of node efficiently. However, the method failed to consider limited copies of messages for more energy efficient. Ayub & Rashid, (2019) modelled resource refrain quota-enabled routing protocol for DTN where resource consumption per message was defined based on energy and buffer space. After that, the Congestion Impact (CI) was introduced for managing the buffer effectively. This framework produces the congestion and reduces network throughput. However, the buffer is not adequate for accommodating the message. Ayub, *et al.,* (2017) presented Probabilistic and Replication based Locking (RBL) routing protocol for DTN. Here, a node probability value was calculated based on dynamic parameters, like number of hops, elapsed time and speed. The number of transmissions is not increased when high probable nodes are considered.

Guo, *et al.,* (2017) developed Location Aided Controlled Spraying (LACS) routing to solve the long delay and intermittent disruption. Here, the routing information is only needed with contracted nodes for the hardware support and hardware support. In addition, semi-Markov process (SMP) was introduced to capture both spatial and temporal domains. Here, the current node was utilized for predicting the location of destination nodes by passing the message to target node with respect to time. The method achieves better performance based on network overhead, and the transmission delay under realistic trace model and random node movement, but the improvement is needed to find the optimal parameters in the SMP model. Kaviani, *et al.,* (2016) addressed energy-aware routing protocols for transmitting the data from the attacked sensors on animals back to collect the data. After that, the network protocol strategies were newly established for achieving the utilization of nodes energy in sensing and transmission. Different mobility patterns are not considered to observe the effect of the mobility patterns. Kawecki & Schoeneich, (2016) developed routing algorithm with the help of nodes in DTN. This DTN was characterized by permanent or temporary lack of continuous path among destination and source node. The developed model employs information about the node mobility and its contacts. The method attains better overhead ratio, but lot of sent messages damages the over-used network resources, like storage or band width. Dhara, *et al.,* (2018) presented fragmentation approach for contact utilization between the nodes, thus the good put in the deep space networks was maximized. In addition, the Contact Graph Routing (CGR) was introduced for the interplanetary networks because of their delay tolerant characteristics and nature. The method failed to find the capacity of routes to improve the utilization of the transmission opportunities.

2.2. Challenges

The challenges confronted by the existing techniques are deliberated below:

- The major challenges faced by DTNs is the less energy resources, which is utilized to constrain nodes into the local area communications, thus the data failed to streamed continuously in the remote base station (Kaviani, *et al.,* 2016);
- In the DTN protocol, providing the communication securely is very challenging. As the network operation is performed using the trust among the nodes. Thus, guaranteeing the delivered messages where the malicious nodes involved in exchange process or the network is protected against fake messages are very difficult (if not impossible) tasks (Wan, *et al.,* 2015);
- Dealing and detecting in DTN with congestion is very challenging task. The DTN forwarding algorithms direct traffic typically towards the particular nodes for increasing the delivery ratios and minimizing the delays, but the traffic become unusable at times when the nodes get improved (Dutt, 2015);
- In (Kaviani, *et al.,* 2016), Energy-Aware Forwarding Strategies is developed for DTN routing protocols. Here, the performance was found better, but failed to consider various mobility patterns for evaluating the protocols;
- In (Guo, *et al.,* 2017), LACS routing algorithm is devised for DTN. However, the information about the location are interchanged in DTNs, but failed to uploaded at the particular time.

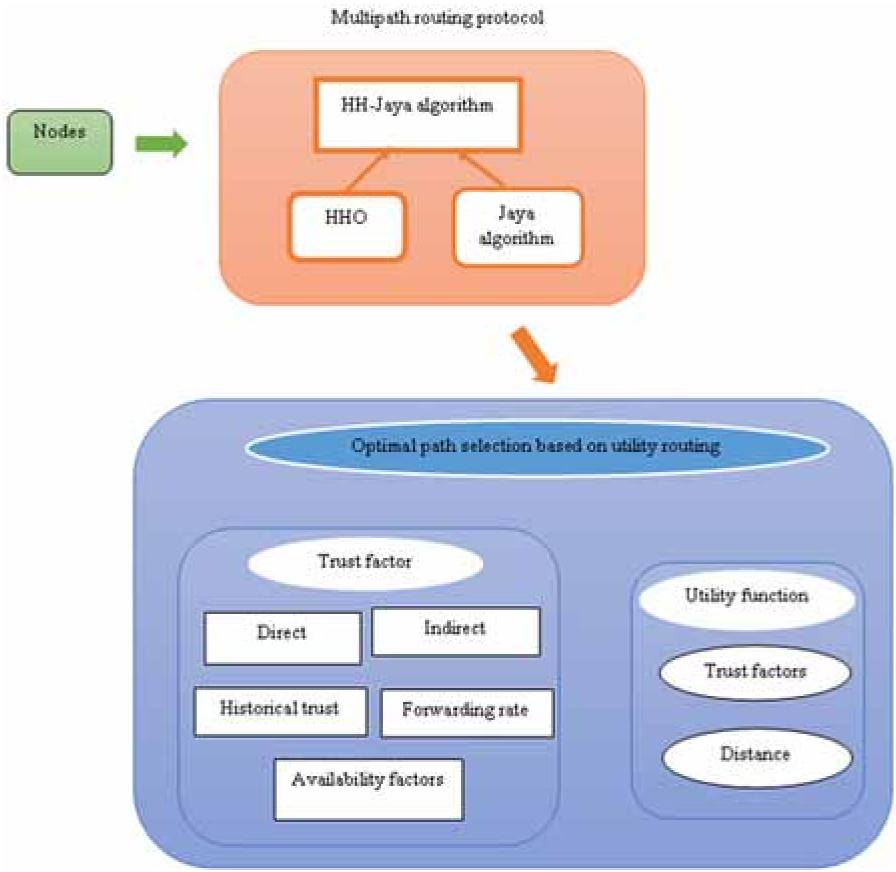
3. DELAY TOLERANT NETWORK

DTN consists of various wireless nodes, which moves within the fixed area. For example, the node is the device, which is held by the human or embedded in the bus. In network, the messages are subjected based on the below strategy. If the router is present between sender u and the receiver v, the message is passed based on the standard routing protocol, called synchronous routing. If the route failed to available, the sender followed the asynchronous routing strategy for delivering the message to forwarding node p with highest value. In addition, the node p stores the message in the local buffer till the route is established or encountering other forwarding node p' with higher message delivery value to destination. In other case, the node is utilized to deliver the message to receiver based on synchronous routing. Then, the node is given to the asynchronous routing and the messages are passed to the forwarding node. This routing steps are repeated until the messages reached the final destination. The important thing that keeps in mind is that if the buffer size is small, the message gets lost when the new message is arrived (Dini & Duca, 2012). The DTN is threatened by several attacks, because few nodes behave in selfish manner, and failed to help others to forward the messages for conserving limited resources, like power and buffer. In addition, some of the nodes are behaved maliciously, which is controlled by the adversary to produce grey hole, black hole, Denial of Service (DoS) attacks through networks by reducing maliciously tampering message packets, received message packets or producing fake message packets (Li, *et al.,* 2017).

3.1 Proposed Harris Hawks-Jaya Algorithm for Multipath Routing

This section depicts the proposed HH-Jaya algorithm is utilized for multipath routing. Figure 1 depicts the proposed multipath routing protocol in DTN using HH-Jaya algorithm. Trust factors and the distance are the two parameters considered as the utility function in the developed model. Based on the distance and the trust, a multipath routing model, termed as HH-Jaya-based multipath routing is introduced. The developed HH-Jaya algorithm is designed by integrating HHO (Heidari, *et al.,* 2019) and Jaya Algorithm (Rao, 2016). Once the multipath routing is done, the RCAR protocol

Figure 1. Schematic view of the proposed routing protocol using HH-Jaya algorithm



select the optimal path with several trust factors, like direct, indirect, history, forwarding rate, and the availability factors. In the RCAR algorithm, when the source wants to send the message to the receiver. Then, the presence of node will be checked in which the condition to perform secure routing based on several trust factors.

3.1.1. Solution Encoding

The solution encoding is the solution representation to be determined with the developed model. The solution vector contains path that taking part in routing process for sending the data packets from source to target node. Assume d number of paths in DTN from which g optimal path is chosen by the developed model such that g value ranging from $1 \leq g \leq d$, respectively. The solution requires d paths where the optimal route g is chosen on the basis of objective function using the developed model.

3.1.2. Fitness Function

The fitness function is calculated for all h paths such that the best route is chosen using the developed HH-Jaya algorithm. The path contributing towards direct, direct trust, historical trust, availability factors, and forwarding rate factor is chosen as the best path. The objective function is calculated by:

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

where, the term h denotes the number of paths, the total nodes in v^{th} path is denoted as k, and the term P_{vx}^{u} is expressed as:

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

where, the terms G_{vx}^{u}, H_{vx}^{u}, K_{vx}^{u}, L_{vx}^{u}, and B_{vx}^{u} are denoted as direct trust, historical trust, forwarding rate factor, indirect trust, and the availability factor. The term q_{vx}^{u} is given by:

$$q_{vx}^{u} = B_{q}\left(M_{v}^{loc}, M_{x}^{loc}\right) \tag{3}$$

where, $B_{q}\left(M_{v}^{loc}, M_{x}^{loc}\right)$ refer to the Euclidean distance between the location of nodes M_{v} and M_{x}.

3.1.3. Algorithmic Steps of the Developed HH-Jaya Algorithm

The HH-Jaya is the combination of the HHO (Heidari, *et al.,* 2019) and Jaya Algorithm (Rao, 2016) and thus, attains the advantages of Jaya algorithm in HHO. The HHO is the cooperative behaviour of Harris' hawks, termed surprise pounce. Here, various hawks pounce the prey cooperatively from various directions for surprising it. In addition, the Harris hawks reveals several chasing patterns are employed for escaping the patterns in prey. Jaya is performed using candidate solutions, and this framework works independently of any parameters. The Jaya algorithm is simpler in operation; because it works in a single phase. Here, the update equation of HHO is modified using Jaya algorithm. This modification makes the developed model more efficient, and thus enhances the convergence rate of optimization algorithm. The steps followed in the developed model are illustrated below:

Step 1: Initialization: The initial step of proposed HH-Jaya algorithm is the initialization of rabbit population that is represented as, Y with total b rabbits, and is given by:

$$Y = \left\{Y_{1}, Y_{2}, ..., Y_{e}, ..., Y_{g}\right\} \tag{4}$$

where, the term g signifies the total solution, and Y_{g} refer to the g^{th} solution.

Step 2: Evaluation of Objective Function: The objective function is estimated based on equation (1) for each solution Here, the fitness function is considered as the maximal solution, and the solution with maximum fitness value is taken as optimal solution.

Step 3: Update the Solution Based on HH-Jaya Algorithm: After computing the objective function, the solution undergoes the location update on the basis of HH-Jaya algorithm. In addition, the Harris Hawks enclose the anticipated prey by updating their position. Thus, the update equation of soft besiege behavior in HHO is expressed as:

$$Y\left(r+1\right)=\Delta Y\left(r\right)-D\left|IY_{rabbit}\left(r\right)-Y\left(r\right)\right| \tag{5}$$

$$Y\left(r+1\right)=Y_{rabbit}\left(r\right)-Y\left(r\right)-DIY_{rabbit}\left(r\right)+DY\left(r\right) \tag{6}$$

Let us assume $Y_{rabbit}\left(r\right)$ is greater, hence the solution becomes:

$$Y\left(r+1\right)=Y_{rabbit}\left(r\right)-DIY_{rabbit}\left(r\right)-Y\left(r\right)\left[1-D\right] \tag{7}$$

$$Y\left(r+1\right)=Y_{rabbit}\left(r\right)\left[1-DI\right]--Y\left(r\right)\left[1-D\right] \tag{8}$$

where, the term $Y\left(r+1\right)$ indicates the location of hawks in next iteration, $Y_{rabbit}\left(r\right)$ denotes the location of rabbit, the term $\Delta Y\left(r\right)$ refer to the difference among the location vector of the rabbit and the present location of prey at r^{th} iteration, and the term D indicates the energy of prey. The value of I randomly changes in every iteration for simulating the nature of rabbit motions. Then, the above equation (4) is modified using the Jaya for improving the effectiveness of approach and to solve several optimization problems. The standard equation of the Jaya optimization is given by:

$$Y\left(r+1\right)=Y\left(r\right)+s_1\left(Y_{best}\left(r\right)-\left|Y\left(r\right)\right|\right)-s_2\left(Y_{worst}\left(r\right)-\left|Y\left(r\right)\right|\right) \tag{9}$$

where, the term $Y\left(r+1\right)$ indicates the $r+1^{th}$ iteration, s_1 and s_2 refers to the random numbers ranging from 0 to1. The worst candidate solution at r^{th} iteration is represented as $Y_{worst}\left(r\right)$. As $Y_{rabbit}\left(r\right)$ is the target in HHO and Y_{best} is the best location in Jaya algorithm, which means $Y_{rabbit}\left(r\right)=Y_{best}\left(r\right)$. Then, the symbol $\left|\;\right|$ is removed in equation (5), assuming $Y\left(r\right)$ is positive. Hence, the equation (5) is modified as:

$$Y\left(r+1\right)=Y\left(r\right)+s_1Y_{best}\left(r\right)-s_1Y\left(r\right)-s_2Y_{worst}\left(r\right)+s_2Y\left(r\right) \tag{10}$$

$$Y_{best}\left(r\right)=\frac{Y\left(r+1\right)-Y\left(r\right)+s_1Y\left(r\right)+s_2Y_{worst}\left(r\right)-s_2Y\left(r\right)}{s_1} \tag{11}$$

Substituting equation (11) in equation (8):

$$Y\left(r+1\right)=\frac{Y\left(r+1\right)-Y\left(r\right)+s_1Y\left(r\right)+s_2Y_{worst}\left(r\right)-s_2Y\left(r\right)}{s_1}\left[1-DI\right]-Y\left(r\right)\left[1-D\right] \tag{12}$$

$$Y\left(r+1\right)=\frac{Y\left(r+1\right)}{s_1}\left[1-DI\right]-\frac{Y\left(r\right)-s_1Y\left(r\right)-s_2Y_{worst}\left(r\right)+s_2Y\left(r\right)}{s_1}\left[1-DI\right]-Y\left(r\right)\left[1-D\right] \tag{13}$$

$$Y\left(r+1\right)-\frac{Y\left(r+1\right)}{s_1}\left[1-DI\right]=\frac{-Y\left(r\right)-s_1Y\left(r\right)-s_2Y_{worst}\left(r\right)+s_2Y\left(r\right)}{s_1}\left[1-DI\right]-Y\left(r\right)\left[1-D\right] \tag{14}$$

$$Y\left(r+1\right)\left[1-\frac{1-DI}{s_1}\right]=\frac{-Y\left(r\right)-s_1Y\left(r\right)-s_2Y_{worst}\left(r\right)+s_2Y\left(r\right)}{s_1}\left[1-DI\right]-Y\left(r\right)\left[1-D\right] \tag{15}$$

$$Y\left(r+1\right)\left[\frac{s_1-1+DI}{s_1}\right]=\frac{-Y\left(r\right)-s_1Y\left(r\right)-s_2Y_{worst}\left(r\right)+s_2Y\left(r\right)}{s_1}\left[1-DI\right]-Y\left(r\right)\left[1-D\right] \tag{16}$$

$$Y\left(r+1\right)=\frac{s_1}{s_1-1+DI}\left\{\frac{s_1Y\left(r\right)+s_2Y_{worst}\left(r\right)-Y\left(r\right)-s_2Y\left(r\right)\left[1-DI\right]-s_1Y\left(r\right)\left[1-D\right]}{s_1}\right\} \tag{17}$$

$$Y\left(r+1\right)=\frac{\left[s_1Y\left(r\right)+s_2Y_{worst}\left(r\right)-Y\left(r\right)-s_2Y\left(r\right)\left[1-DI\right]\right]-s_1Y\left(r\right)\left[1-D\right]}{s_1-1+DI} \tag{18}$$

where, $I=2\left(1-s_r\right)$. Here, the s_r value ranging between 0 to 1, and the random numbers are denoted as s_1 and s_2 ranging from 0 and 1. The energy of prey is expressed as:

$$D=2D_0\left(1-\frac{r}{R}\right) \tag{19}$$

where, the term D_0 is indicated as initial state of energy, and the maximal iteration is denoted as R. Thus, the equation (14) is the final update equation of HH-Jaya algorithm.

Step 4: Replace the Best Solution: Based on fitness value, the feasibility is again computed, hence if the generated new solution is best than previous one, the old one is replaced by the new solution.
Step 5: Termination: The above steps are repeated until the best solutions are determined. Algorithm 1 portrays the pseudo code of the developed model.

3.2. Secure Routing Using RCAR

To transmit the data in the secure manner and to avoid the packet loss in DTN, it is very necessary to develop the secure routing mechanism to transmit the packet for finding the secure route without considering any path conjunction. Here, RCAR is utilized for selecting the forwarding node. Let us consider the node c passes the message n to p^{th} node. If the route present between node c to p, the c^{th} node performs synchronous routing or else the asynchronous routing is done. If the synchronous routing is present, the sender node chooses the next hop m for reaching the receiver node on the

Algorithm1. Pseudocode of HH-Jaya Algorithm

```
Input: Rabbit population Y = {Y_1, Y_2, ..., Y_e, ..., Y_g}
Output: Best solution
Procedure:
Begin
            Population Initiation: Y = {Y_1, Y_2, ..., Y_e, ..., Y_g}
While τ < max gen
        Calculate the fitness values for each solution using equation (1)
        Y_best(r) is the rabbit best solution
        Update the location of the solution using equation (18)
          End if
            End for
        End while
        Recompute the fitness of each solution
        Return the best solution
    r = r + 1
       End while
        End if
    End for
Optimal solution is obtained
End
```

basis of DSDV protocol. After selecting next hop, the node c checks the black hole is present or not using the condition $L_{cm} > 0$. Hence, if the black hole is not present, the sender sends the message. If $L_{cm} = 0$, the node tries to perform asynchronous routing. Here, the sender chooses the node q with highest L_{cm}. Once the message is received, the node q stores in the local buffer. In other words, the sender passes the message to the next hop if $L_{cm} > 0$ condition is satisfied otherwise the message is stored in its local buffer. In this case, the nodes c and q are trying to forward the messages present in local buffer using the above-mentioned mechanism.

3.3. Local Utility Function

The local utility function is computed using the trust factors, like direct, indirect, historical trust, forwarding rate factor, availability factor along with utility function. Assume V_u refer to the utility function of u and the term Q_{yz} signifies the reputation of y^{th} node at z^{th} node. Then, the expression of global utility function is given by:

$$J_{yz} = \sum_{v=1}^{k} V_u \tag{20}$$

Then, the local utility function is computed using the below expression:

$$V = \left(G_{vx} + H_{vx} + K_{vx} + L_{vx} + B_{vx}\right) * U_{vx} \tag{21}$$

where, the direct trust, historical trust, forwarding rate factor, indirect trust, availability factor and the utility is denoted as G_{vx}, K_{vx}, H_{vx}, L_{vx}, B_{vx}, and U_{vx}, the term v refer to the evaluation node and the node to be evaluated is represented as x.

3.4 Trust Model

Trust is one of the major factors considered for the accurate communication process in DTN. The trust model provides the security in the developed model for routing. The trust factor for each node is estimated to evaluate the set of trusted nodes. Therefore, the trust factor utilized for identifying the trusted nodes present in b^{th} path is computed based on direct trust, availability factor, indirect trust, forwarding rate factor, historical trust, and utility.

3.4.1. Direct Trust

The direct trust (Chen, *et al.,* 2015) is also known to be local trust, which is performed based on the contentment prevailing between the interaction of nodes. The direct trust is estimatedusing the degree of satisfaction between the nodes v and x. When the v^{th} node feels satisfied with the x^{th} node, the datisfaction degree is said to be high, providing the direct trust. The trust is defined as the measure that one node holds the other using past experiences, nodes behaviour information, and the suggestion from trusted nodes. The direct trust G_{vx} is obtained if the v^{th} node trust by the x^{th} node. Then, the direct trust expression is given below:

$$G_{vx} = \left(1-\beta\right) * C_{vx}\left(r\right) * E_{vx}\left(r\right) * N_{vx}\left(r\right) + \beta * G_{vx}\left(r-1\right) \tag{22}$$

where, the term $C_{vx}\left(r\right)$ refer to the sending rate factor at time r, E_{vx} signifies the packet loss rate factor, the consistency factor is represented as $N_{vx}\left(r\right)$, and the term β refer to constant and the value ranges from 0 to 1.

3.4.2. Indirect Trust

Once the next hop node is selected, every node is fed to check whether a next-hop node is trusted by estimating the next-hop node trust. Therefore, the indirect trust (Chen, *et al.,* 2015) value is considered for reducing the deviation, and the expression is given as:

$$H_{vx} = w_r\left(G_{vx}, G_{xj}\right) \tag{23}$$

where, the term G_{vx} signifies the direct trust of evaluated x^{th} node by v^{th} node to, and G_{xj} refer to direct trust of evaluated x^{th} node by j^{th} node. The term $w_r\left(.\right)$ is computed based on the requirements of actual network.

3.4.3. Historical Trust

The historical trust (Chen, *et al.,* 2015) is carried out based on the interaction or object behavior. Here, the record is utilized for calculating the trust value. The term K_{vx} represents the historical trust, and is expressed as:

$$K_{vx} = \frac{\alpha \times K_{vx}\left(h-1\right) + XT_{vx}\left(h-1\right)}{2} \tag{24}$$

where, the term α refer to random number ranging from $0 \ and \ 1$, the transactions is represented as h, and the recent trust is indicated as XT_{vx}.

3.4.4. Forwarding Rate Factor

The nodes of DTN containing limited energy that needs to be relayed when transmitting and sensing the data. Therefore, it is very necessary for evaluating the node is attacked or not by computing the data forwarding the nodes. The function of forwarding rate factor (Zhu, 2018) is given by:

$$L_{vx} = \frac{ACK_{vx}(r)}{\mathrm{TP}_{vx}\left(r\right)} \tag{25}$$

where, the total feedback packets is represented as $ACK_{vx}(r)$, and number of forwarding packets is indicated as $\mathrm{TP}_{vx}\left(r\right)$.

3.4.5. Availability Factor

In the availability factor, the node is not utilized due to the interference of network channel, hence it is very appropriate for evaluating the node by inspecting or passing the data packet. The availability faction is expressed as:

$$B_{vx} = \frac{ACK_{vx}(r)}{ACK_{vx}(r) + \mathrm{N}ACK_{vx}(r)} \tag{26}$$

where, the term $ACK_{vx}(r)$ represents the responded packets, and the amount of un-responded packets are indicated as $\mathrm{N}ACK_{vx}(r)$. Then, the utility is expressed as:

$$U_{vx} = Q\left(\frac{K}{B}\right) \tag{27}$$

where:

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

Here, the variance of event delay to event attack, and the term K indicates the trust factors, like availability factor, forwarding rate factor, historical trust, direct and indirect trust.

4. RESULTS AND DISCUSSION

The results of the developed model are discussed in this section based on the evaluation metrics.

4.1 Experimental Arrangement

The experimentation of the HH-Jaya algorithm is performed on Windows 10 OS with 2GB RAM and Intel i3 core processor. The implementation of the proposed method was done using MATLAB.

4.2 Evaluation Metrics

The performance of the developed HH-Jaya algorithm is employed to analyze the methods using delay, PDR and throughput rate, and they are illustrated below:

1. **Delay:** It is defined as the time used by the data packets for reaching the source to the target node in the network.

Throughput: It is used to measure the number of received data packets by destination at the particular time, and is represented as:

$$Throughput = {}^{Z}\!/_{r} \tag{28}$$

where, the term $-$ refer to number of nodes received at simulation time r .

3. **PDR:** It is defined as the ratio of the received data packets by sent data packets, which is utilized to compute the routing efficiency:

$$PDR = \frac{Received\ \ data\ \ packets}{Sent\ \ data\ \ packets} \tag{29}$$

4.3 Experimental Results

This section illustrates the simulation set-up of developed model. Figure 2 depicts the sample results of the developed model. Figure 2a), 2b) and 2c) depicts the sample outputs of the developed approach with the consideration of 10 nodes. When transmitting the data where the nodes may transmit within the transmission range. If the node is placed far from range, then it failed to entail communication and is marked with red colour in below figure, while the black nodes depicts the sent messages. The green colour circle signifies the source node and the red green circle indicates the destination node, whereas the blue triangle refer to intermediate nodes.

4.4 Competing Methods

The methods, like RCAR (Dini & Duca, 2012), fuzzy logical ant colony (Ababou, *et al.,* 2018), and energy aware forwarding (Kaviani, *et al.,* 2016) are employed for comparison with developed model for the analysis.

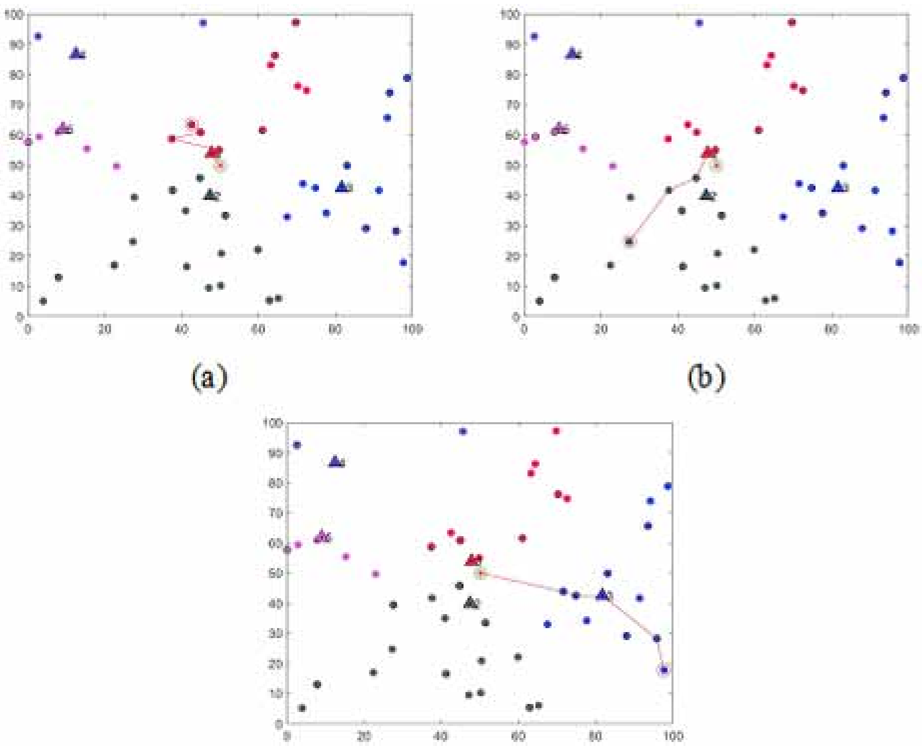
4.5. Comparative Analysis

The comparative analysis of the developed model with conventional methods with respect to delay, packet delivery rate, and the throughput rate parameters is evaluated. The analysis is performed by varying the rounds.

4.5.1. Analysis Using 10 Users

The comparative analysis is performed based on delay, PDR, and throughput rate by varying the rounds using 10 users is deliberated in figure 3. Figure 3a) illustrates the analysis using delay. When the round=800, the delay computed by existing RCAR, fuzzy logical ant colony, energy aware forwarding, and proposed HH-Jaya algorithm are 0.085sec, 0.087sec, 0.085sec, and 0.084sec. The

Figure 2. Sample results using 10 nodes



analysis in terms of PDR is illustrated in figure 3b). When round=200, the PDR computed by existing RCAR, fuzzy logical ant colony, energy aware forwarding, and proposed HH-Jaya algorithm are 0.989, 0.988, 0.988, and 0.991. The analysis with respect to throughput rate is illustrated in figure 3c). When round=800, the throughput rate computed by existing RCAR, fuzzy logical ant colony, energy aware forwarding, and proposed HH-Jaya algorithm are 0.826, 0.826, 0.786, and 0.826, respectively.

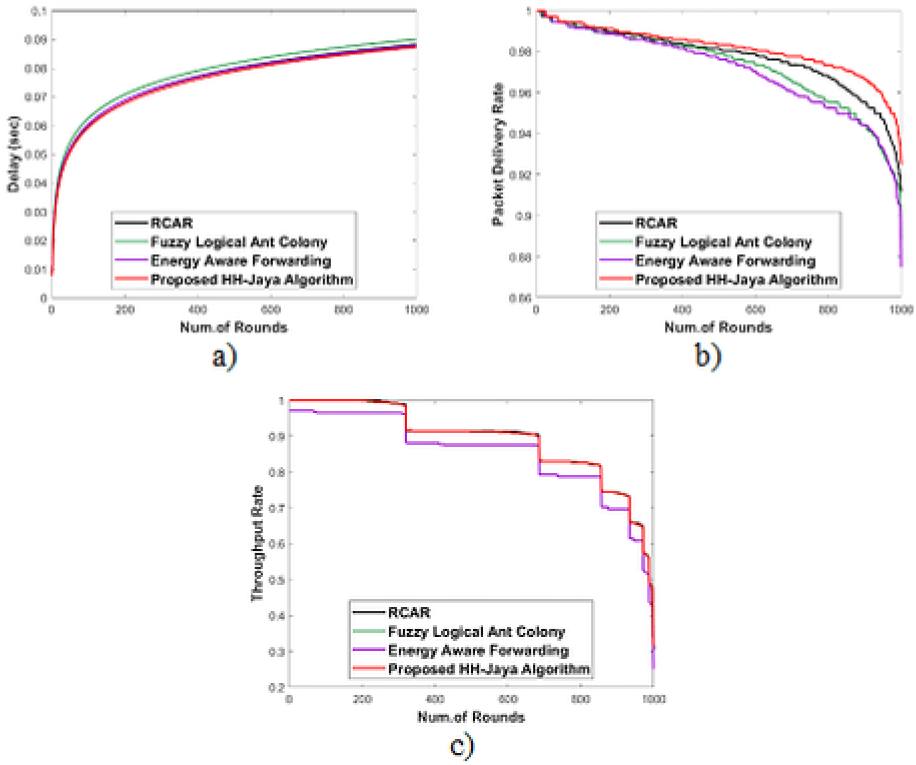
4.5.2. Analysis Using 20 Users

The analysis with respect to delay, PDR, and throughput rate by varying the rounds using 20 users is deliberated in figure 4. The analysis on the basis of delay parameter is illustrated in figure 4a). When round=400, the delay computed by existing RCAR, fuzzy logical ant colony, energy aware forwarding, and proposed HH-Jaya algorithm are 0.096sec, 0.094sec, 0.077sec, and 0.070sec. The analysis of methods using PDR is illustrated in figure 4b). When round=400, the PDR computed by existing RCAR, fuzzy logical ant colony, energy aware forwarding, and proposed HH-Jaya algorithm are 0.976, 0.977, 0.982, and 0.985. The analysis in terms of throughput rate is illustrated in figure 4c). When round=500, the throughput rate computed by existing RCAR, fuzzy logical ant colony, energy aware forwarding, and proposed HH-Jaya algorithm are 0.913, 0.912, 0.875, and 0.914, respectively.

4.6 Comparative Discussion

Table 1illustrates the analysis of previous RCAR, fuzzy logical ant colony, energy aware forwarding, and proposed HH-Jaya algorithm in terms of metrics with users 10, and 20by varying the rounds. The minimal delay computed by developed HH-Jaya algorithm is 0.007sec, whereas the existing RCAR, fuzzy logical ant colony, and energy aware forwardingare0.009sec, 0.013sec, and 0.010sec, respectively. The maximal PDR computed by the HH-Jaya algorithm with value of 0.991, whereas

Figure 3. Comparative analysis by varying the number of rounds with 10 user (a) Delay, (b) packet delivery rate, and (c) throughput rate



the RCAR, fuzzy logical ant colony, energy aware forwarding acquired the PDR of 0.986, 0.987, and 0.989, respectively. The minimal throughput rate value computed by HH-Jaya algorithm is 0.913, whereas the RCAR, fuzzy logical ant colony, energy aware forwarding methods acquired the throughput rate of 0.912, 0.910, and 0.875, respectively.

5. CONCLUSION

This paper presents the trust-enabled routing algorithm, named HH-Jaya to initiate multipath routing in DTN. The proposed HH-Jaya is designed by incorporating HHO in the Jaya model. The method enhanced the energy efficiency and increased the lifetime of nodes thereby, increase the performance of algorithm. Along with the proposed HH-Jaya model, a fitness function is considered using distance, and trust factors. The proposed HH-Jaya model and the fitness function improved the overall network performance and help to select the optimal path to transmit the data packets from source node to destination node. After that, the secure routing is performed by checking the presence of node in RCAR using direct, history, indirect, availability factors, forwarding rate, and utility function. The major significance of HH-Jaya model is that the optimal convergence of the model parameters is boosted due to the extraordinary performance of the developed model and in addition, the importance of the research is on the fitness measure for estimating secure routes. The effectiveness of the proposed HH-Jaya model is computed with respect to other methods and showed effective results with minimal delay of 0.007 sec, maximal

Figure 4. Comparative analysis by varying the number of rounds with 20 user (a) Delay, (b) packet delivery rate, and (c) throughput rate

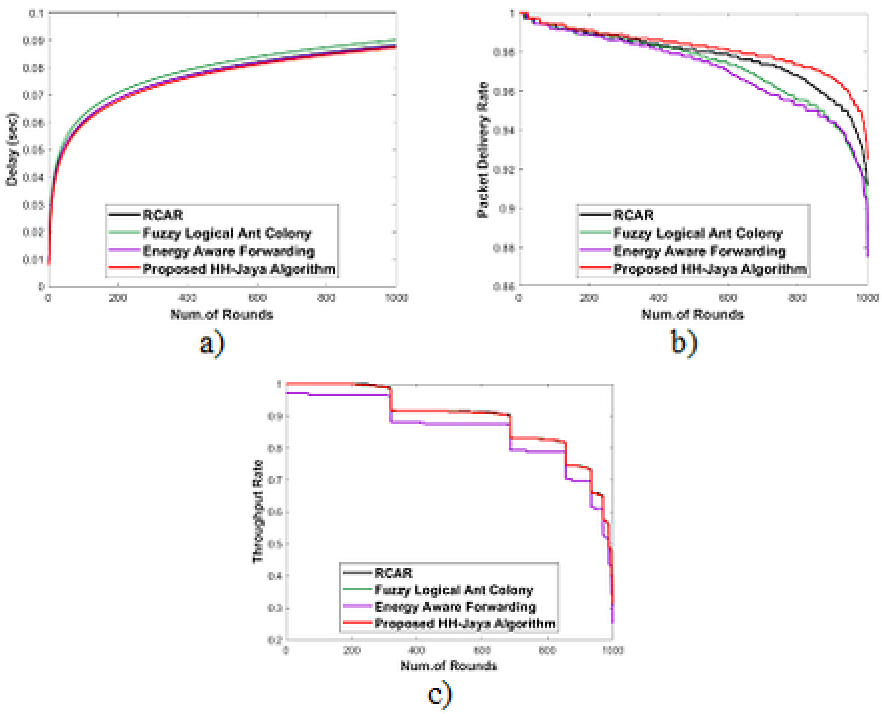


Table 1. Comparative analysis

Number of Users	Metrics	RCAR	Fuzzy Logical Ant Colony	Energy Aware Forwarding	Proposed HH-Jaya Algorithm
10	Delay (sec)	0.009	0.013	0.010	0.007
	Packet delivery rate	0.955	0.942	0.944	0.965
	Throughput rate	0.912	0.910	0.875	0.913
20	Delay (sec)	0.049	0.052	0.042	0.037
	Packet delivery rate	0.986	0.987	0.989	0.991
	Throughput rate	0.9056	0.9055	0.875	0.907

throughput of 0.913 and maximal PDR of 0.991, respectively. The research can be extended by determining the solutions for the limitations encountered in the survey of conventional multipath routing techniques.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

Funding Statement

No funding was received for this work.

Process Dates:

Received: May 4, 2020, Accepted: September 16, 2020

Corresponding Author:

Correspondence should be addressed to Pradosh Kumar Gantayat, gpradoshkumar@gmail.com

REFERENCES

Ababou, M., Bellafkih, M., & El kouch, R. (2018). Energy Efficient Routing Protocol for Delay Tolerant Network Based on Fuzzy Logic and Ant Colony. *International Journal of Intelligent Systems and Applications*, *1*(1), 69–77. doi:10.5815/ijisa.2018.01.08

Ayub, Q., & Rashid, S. (2019). Resource refrain quota based routing protocol for delay tolerant network. *Wireless Networks*, *25*(8), 4695–4704. doi:10.1007/s11276-018-1763-7

Ayub, Q., Ngadi, A., Rashid, S., Ahmedy, I., Sharif, J. M., & Zahid, M. S. M. (2017). Probabilistic and Replication Based Locking Routing Protocol for Delay Tolerant Network. *Wireless Personal Communications*, *97*(2), 3239–3259. doi:10.1007/s11277-017-4673-6

Chen, Z., He, M., Liang, W., & Chen, K. (2015). Trust-Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network. *Journal of Sensors*, *2015*, 1–10. doi:10.1155/2015/716468

Dhara, S., Burleigh, S., Datta, R., & Ghose, S. (2018). CGR-BF: An Efficient Contact Utilization Scheme for Predictable Deep Space Delay Tolerant Network. *Acta Astronautica*, *151*, 401–411. doi:10.1016/j.actaastro.2018.06.023

Dini, G., & Duca, A. L. (2012). Towards a reputation-based routing protocol to contrast black holes in a delay tolerant network. *Ad Hoc Networks*, *10*(7), 1167–1178. doi:10.1016/j.adhoc.2012.03.003

Dutt, I. (2015). Issues in Delay Tolerant Networks: A Comparative Study. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(6).

Fall, K., & Farrell, S. (2008). DTN: An Architectural Retrospective. *IEEE Journal on Selected Areas in Communications*, *26*(5), 828–836. doi:10.1109/JSAC.2008.080609

Fall, K. (2003). A Delay-Tolerant Network Architecture for Challenged Internets. *Proceedings of SIGCOMM conference on Applications, technologies, architectures, and protocols for computer communications*, 27-34. doi:10.1145/863955.863960

Guo, H., Wang, X., Cheng, H., & Huang, M. (2017). A location aided controlled spraying routing algorithm for Delay Tolerant Networks. *Ad Hoc Networks*, *66*, 16–25. doi:10.1016/j.adhoc.2017.08.005

Heidari, A. A., Mirjalili, S., Faris, H., Aljarah, I., Mafarja, M., & Chen, H. (2019). Harris hawks optimization: Algorithm and applications. *Future Generation Computer Systems*, *97*, 849–872. doi:10.1016/j.future.2019.02.028

Kaviani, M., Kusy, B., Jurdak, R., Bergmann, N., & Liu, V. (2016). Energy-Aware Forwarding Strategies for Delay Tolerant Network Routing Protocols. *Journal of Sensor and Actuator Networks*, *5*(18).

Kawecki, M., & Schoeneich, R. O. (2016). Mobility-based routing algorithm in delay tolerant networks. EURASIP Journal on Wireless Communications and Networking. doi:10.1186/s13638-016-0578-4

Li, F., Si, Y., Lu, N., Chen, Z., & Shen, L. (2017). A Security and Efficient Routing Scheme with Misbehavior Detection in Delay-Tolerant Networks. *Security and Communication Networks*, *2017*, 1–16. doi:10.1155/2017/2761486

Lindgren, A., Doria, A., & Schelen, O. (2003). MobiHoc Poster: Probabilistic Routing in Intermittently Connected Networks. *Mobile Computing and Communications Review*, *7*(3), 19–20. doi:10.1145/961268.961272

Musolesi, M., & Mascolo, C. (2009). CAR: Context-Aware Adaptive Routing for Delay-Tolerant Mobile Networks. *IEEE Transactions on Mobile Computing*, *8*(2), 246–260. doi:10.1109/TMC.2008.107

Pathak, S., Gondaliya, N., & Raja, N. (2017). A Survey on PROPHET Based Routing Protocol in Delay Tolerant Network. In *Proceedings of International Conference on Emerging Trends & Innovation in ICT (ICEI)*. Pune Institute of Computer Technology. doi:10.1109/ETIICT.2017.7977020

Rao, R. V. (2016). Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems. *International Journal of Industrial Engineering Computations*, *7*, 19–34.

Roy, A., Acharya, T., & DasBit, S. (2018). Quality of service in delay tolerant networks: A survey. *Computer Networks*, *130*, 121–133. doi:10.1016/j.comnet.2017.11.010

Spyropoulos, T., Psounis, K., & Raghavendra, C. S. (2004). Single-Copy Routing in Intermittently Connected Mobile Networks. *Proceedings of First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON*, 235-244.

Spyropoulos, T., Psounis, K., & Raghavendra, C. S. (2007). Spray and Focus: Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility. *Proceedings of Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*, 79-85.

Voyiatzis, A.G. (2012). A Survey of Delay- and Disruption-Tolerant Networking Applications. *Journal of Internet Engineering*, *5*(1).

Vu, L., Do, Q., & Nahrstedt, K. (2011). 3R: Fine-grained Encounter-based Routing in Delay Tolerant Networks. *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 1-6.

Wan, L., Liu, F., Chen, Y., & Zhang, H. (2015). Routing protocols for delay tolerant networks: Survey and performance evaluation. *International Journal of Wireless and Mobile Networks*, *7*(3), 55–69. doi:10.5121/ijwmn.2015.7305

Zhu, J. (2018). Wireless Sensor Network Technology Based on Security Trust Evaluation Model. *International Journal of Online and Biomedical Engineering*, *14*(4), 211–226. doi:10.3991/ijoe.v14i04.8590

Pradosh Kumar Gantayat is a research scholar in the Department of Computer Science and Engineering at VSSUT, Burla, Odisha. He received his M.Tech degree from KIIT University, Odisha in the year 2007.He has published 8 numbers journal in various International/National Journals. His current research interests include Delay Tolerant Network, Cloud Computing.

Satyabrata Das is presently working as Associate professor in the Department of Information Technology at VSSUT, Burla, Odisha, India. His main research area is Mobile Computing, Cloud Computing, Fault Tolerant Computing. He has published more than 30 Numbers papers in various reputed international and National journals. He was awarded Best Teacher award by ISTE in the year 2014, Bhubaneswar chapter and Sandeep Mohapatra Memorial award in 2016 from the Institute of Engineers (India) Odisha state Chapter Bhubaneswar.