Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.030540
Article

Cooperative Channel and Optimized Route Selection in Adhoc Network

D. Manohari[1,*], M. S. Kavitha[2], K. Periyakaruppan[3] and B. Chellapraba[4]

[1]Department of Computer Science and Engineering, St. Joseph's Institute of Technology, Chennai, 600119, Tamilnadu, India
[2]Department of Computer Science & Engineering, SNS College of Technology, Coimbatore, 641035, Tamilnadu, India
[3]Department of Computer Science & Engineering, SNS College of Engineering, Coimbatore, 641107, Tamilnadu, India
[4]Department of Information Technology, Karpagam Institute of Technology, Coimbatore, 641032, Tamilnadu, India
*Corresponding Author: D. Manohari. Email: sanmano1973@gmail.com
Received: 28 March 2022; Accepted: 09 May 2022

Abstract: Over the last decade, mobile Adhoc networks have expanded dramatically in popularity, and their impact on the communication sector on a variety of levels is enormous. Its uses have expanded in lockstep with its growth. Due to its instability in usage and the fact that numerous nodes communicate data concurrently, adequate channel and forwarder selection is essential. In this proposed design for a Cognitive Radio Cognitive Network (CRCN), we gain the confidence of each forwarding node by contacting one-hop and second level nodes, obtaining reports from them, and selecting the forwarder appropriately with the use of an optimization technique. At that point, we concentrate our efforts on their channel, selection, and lastly, the transmission of data packets via the designated forwarder. The simulation work is validated in this section using the MATLAB program. Additionally, steps show how the node acts as a confident forwarder and shares the channel in a compatible method to communicate, allowing for more packet bits to be transmitted by conveniently picking the channel between them. We calculate the confidence of the node at the start of the network by combining the reliability report for the first hop and the reliability report for the secondary hop. We then refer to the same node as the confident node in order to operate as a forwarder. As a result, we witness an increase in the leftover energy in the output. The percentage of data packets delivered has also increased.

Keywords: Adhoc Network; confident; forwarder; one-hop; optimized route selection; secondary report; channel selection

1 Introduction

For security reasons, the mobile Adhoc network uses extremely sensitive routing and employs a variety of communication channels to reach its objective. When nodes in a far away area communicate data wirelessly, there is a possibility that the reliability of the other nodes in the transmission will be compromised. Occasionally, information is forwarded to a node; however, if the receiver is unreliable or the forwarding node channel is unable to send all of the information, the network transmission is rendered useless; this condition has the potential to result in significant packet loss and network delay. In

this proposed CRCN paradigm, protocol approaches are used to address transmission issues and provide the necessary solution for safely reaching the target [1]. In this proposed CRCN architecture, we offer a network lifetime extension-aware cooperative channel access network that is utilized to adapt to performing a multi-unbiased object function, with the following inputs:

We have developed a multi-unbiased adaptive design that selects a confident forwarder from a source to send packets to a destination. The protocol used in this research improves the network life of nodes, energy management, node decoding performance, and finds responsive forwarders to transmit the packets [2]. The purpose of this research is to develop a dependable mobile Adhoc network. We offer an ideal method for nodes to choose the channel that uses the least energy to connect to a neighbor, and then select the channel based on the unusable condition directly, or jointly, thereby paving the way and transmitting information with a confident neighbor. We assume that nodes have asymmetric transmission due to node usage; the available transfer power at both the source and forwarder can be any value; it is determined by the node utilization from the start to the current state. Fig. 1 illustrates how the proposed architecture offers a powerful best confident forwarder selection technique for constructing a path from source to destination.

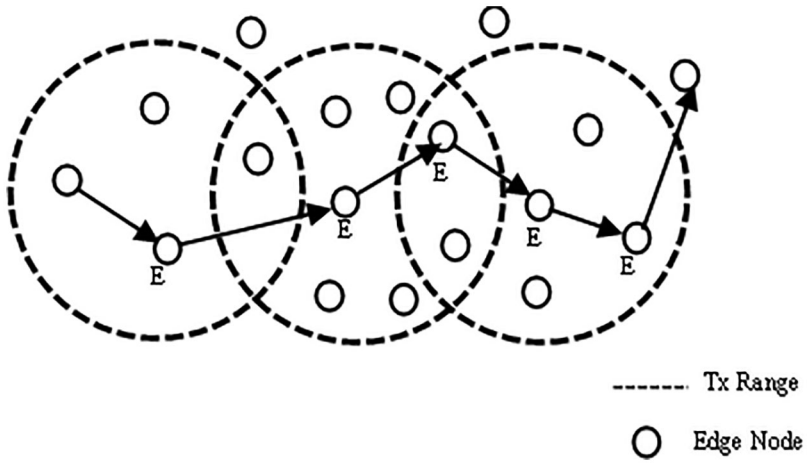

Figure 1: Transmission range nodes

Apart from the channel selection, this activity utilizes optimization calculations to provide multi-unbiased security and channel selection-based routing system. Here, we worked on the whale lioness calculations, which include lioness action into the whale to produce the ideal solution via perfect goal programming. The objectives identified in this suggested technique include numerous quality criteria derived from the media access control layer MAC, as well as distance and a confidence specification derived from the routing layer called the confidence of the node. We develop the fitness function to finalize the forwarder based on the afore said parameter adjustments [3]. The CRCN routing algorithm is composed of the following steps: (a) establishing quality measurements at two layers, (b) computing confidence levels, (c) identifying numerous disjoint paths, and (d) optimal pathfinding using the proposed multiple purpose channel selection methods. Thus, the proposed method provides an optimal transportation route with a favorable PDR, throughput, delay and energy consumption. The vital inputs of the suggested method for the confident based routing and lifetime extension aware channel access are as follows:

- Designing a multi unbiassed optimization system for reliable routing by recognizing the above quality of service metrics and a confidence parameter as multi unbiassed.

- Using many unbiassed models, i.e., energy, latency, link lifetime, distance, and confidence design, for the data transmission, so that the route is adopted and efficient, accelerating the convergence process [4], and reducing the number of discontinuous pathways.

It was necessary to extend the network's life span to identify the best possible relay node for a given transmission power given at each source and relay node. Relay node selection in the MAC layer was also influenced by the transmission gain and residual energy.

In this work, we have taken place channel selection when the routing packets sent to find the path reach the MAC layer. The rest of this manuscript is discussed as follows. The part II represents the literature surveys in brief. In part III, the document pointed out the CRCN-cooperative channel selection and optimized route formation based on confidence in the Adhoc network is discussed. In section, IV informed the performance evaluation of the CRCN protocol and the end part carries out the CRCN conclusion, aims, and future opinions.

2 Literature Survey

Due to the restricted amount of power available for computing and radio transmission in ad hoc networks, node performance is critical. Additionally, there may be considerable constraints on the available bandwidth and radio frequencies [5]. Ad hoc networks can also be beneficial for law enforcement, emergency response and rescue missions. Because the ad hoc networks can be created rapidly and inexpensively, they are well suited for the commercial applications such as wireless networks or virtual classrooms [6]. It has been an extended time since these devices reached their full capability. Thanks to wireless technologies, these massive pieces of equipment may now communicate with any new machinery and be used anywhere. Wireless medical technology such as CodeBlue and MobiHealth [7] is in use. This model's representation of the wireless channel includes broadcast omni-directional antennas, large-scale route loss, and fading. Utilize it in lieu of OSI layer design and specialized routing protocols to provide a comprehensive perspective of the routing challenge [8]. As the number of devices in an ad-hoc network grows, management becomes increasingly difficult. Connecting ad-hoc networks to wired networks is not possible. Ad-hoc networks provide a novel method of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations in mobile switching [9]. We undertake energy-efficient routing before scheduling nodes' transmissions to identify the least-powerful paths. The created schedule is based on end-to-end traffic data and preceding routing decisions [10]. A mobile node consumes battery power in addition to sending and receiving data by listening to the wireless medium for communication requests from other nodes [11]. The topology of the universe is constantly changing. The topology of a mobile ad hoc network is constantly changing as nodes move [12]. The radio range of the other nodes in the ad hoc network is continually changing, requiring constant updating of the routing information [13]. MANET's have a wide range of applications, from large-scale moveable and dynamic networks to small networks constrained by their power supply. Along with the legacy applications that migrate from the old infrastructure environment, a considerable number of new services can and will be developed for the ad hoc context [14]. Each node within a network's wireless range receives packets, regardless of whether they were meant for another node. Due to these characteristics, it is simple for each node to view the packets of other nodes or to the inject fault packets into the network. Vital nodes may experience battery drain and hence become unavailable for routing, resulting in broken links and a severe impact on the routing protocol's performance [15]. Another key objective is to conserve energy on nodes to ensure the network's longevity. Without an established communication infrastructure, a group of wireless mobile hosts forms its network dynamically. However, due to its open network architecture and shifting network topology, it is vulnerable to both internal and external attacks. Reactive routing protocols are more efficient in dynamic topologies such as MANET. A concerted effort is being made to improve

(Ad-hoc On-Demand Distance Vector) AODV, the most widely used reactive routing technique. The Internet technical task committee has designated AODV as the official routing protocol for MANET [16]. Radios can broadcast over a large region. To determine whether a packet should be sent or received locally, each node within that range must receive it. Even if the majority of these packets are discarded, they use energy under this basic energy model [13]. The capacity of the power management system to respond to variations in traffic load is reflected in the length of the soft-state timer. We give methods for determining a neighbor's power management [17], as broadcasting to a sleeping node is not the same as broadcasting to an active node. There are a variety of power control approaches that can be used to minimize network interference. Finally, the author Abdullah Waqas et al. [18] offered a routing algorithm for edge computing-enabled 5g networks, as well as a system of recommended metrics that is a function of the created and received interference in the network. The received interference term ensures that the Signal to Interference plus Noise Ratio (SINR) along the route remains greater than the threshold value, whilst the produced interference term ensures that only those nodes are chosen to forward packets that cause minimal interference to other nodes. The results indicate that the suggested method outperforms standard routing protocols in terms of network speed and outage probability.

3 CRCN Design and Implementation

3.1 Network Formation

Consider a Graph $G = (N, E)$ which is created as a adhoc network with set of N, and E, where $N = n_i \ldots . n_n$ stands for set of nodes, her i to n defines the number of nodes in the network. E is the set of neighbors of each node. We refer to this as $E = e_i \ldots . e_n$, here e_i is placed within the transmission variety of each node. The time taken to communicate between nodes can be calculated by the transmission delay between the two. Each node that transfer the data to it neighbor routing node and finally it reaches the destination, during which time it loses energy depending on the communication between the sender to neighbor. In this network, the distance between the nodes is calculated according to their location points and their displacement. The distance variations between the nodes vary continuously depending on the movements, at that point its location points will also change. These distance D_{ist} variations are monitored from the beginning of the network, so that the distance changes are calculated as follows, where x1 x2 and y1 y2 denote its location points. The contact time between the two nodes is considered as their channel life C_L.

$$D_{ist} = \sqrt{|x1 - x2|^2 + |y1 - y2|^2} \tag{1}$$

3.2 Confidence Evaluation

The initial confidence values for each wireless node is calculated using a differential evolutionary method. After calculating the initial confidence values, the multi-objective method is used based on the Lion whale optimization L_W, by which the functions of the nodes are accurately calculated. The degree of confidence for each node is designed using the degree of confidence calculated by one-hop contact of the nodes and the degree of confidence of the nodes in secondary contact. These two-degree vectors are connected using the weight factors for individual vectors. From the beginning of the network all normal nodes started to calculating the confidence level of the neighboring node.

3.3 One-Hop Trust Calculation

The degree of one-hop evolution is identified from a diverse evolution-based belief evaluation model as shown in Fig. 2. After calculating the one-hop confidence values, the table of confidence is broadcasting to one of its hop neighbors by the wireless sender.

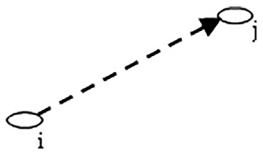

Figure 2: One hop communication

We calculate the one-hop confidence C_{OH} between the two nodes as shown below. Here S_P is the sum of packets sent by a node, while R_P is the sum of packets received by its neighbor e_i from the sender S_i. This information is obtained from the physical layer of the node, which i labelled in Eq. (2).

$$C_{OH} = \frac{R_P}{S_P} \tag{2}$$

Each node buys a one-hop report and checks the activities of its neighbors. When calculating the confidence value between two nodes, it falls between 0 and 1. Of these, 0 is taken as the confidence-less node and 1 is considered as a very reliable node. Each node start storing the information about the neighbor in an array format, they are:

- Neighbor's trust value,
- The amount of energy present in the node
- Changes in distances
- Channel life between two nodes
- Calculate how many routes can be set by a neighbor node

3.4 Secondary Node Trust Validation

Similarly, from the confidence tables obtained, the number of secondary hop confidence S_{HC} values for each neighboring node is checked and then the average confidence value is determined by their counts.

$$S_{HC} = \frac{1}{t}\sum C_{OH}$$

Here C_{OH} and S_{HC} of each node take place at regular intervals t. In this way, the confidence degree C_D is calculated with the help of weighted factors after checking the reports of one-hop and the confidence of the secondary nodes. In below Fig. 3 represent that the secondary hop communication, in this fugure there are three communication link as i, j *and* k.$C_D = C_{OH}\alpha + C_{OH}\beta$

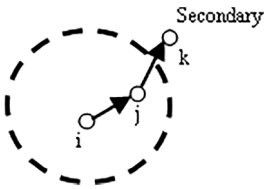

Figure 3: Secondary hop communication

With each iteration of the confidence I_{DC} assessment, the degree of confidence is renewed in several stages based on varying average values.

$$I_{DC} = \Delta C_{Di} + C_D(1 - \Delta)$$

This variable average model uses weighted distribution based on the weighting factor. Where α and β are considered as the tunable weight value. These two together will be within the number 1.

4 Network Resource Validations

The energy parameter for each neighboring node is intended based on the number of packets transferred and the energy cost E_C occurred because of receiving packets.

$E_C = E_{TP} + E_{RP}(P_i - 1)$, here, P_i indicates each bit of packet transmission E_{TP} and E_{RP}, explains the transmission packet counts and receiving packet counts of the network. The energy ratio E_R is the ratio between the energy network cost and the initial energy E_i level of the nodes is computed as $\frac{E_C}{E_i}$. The connection life of the current sender and the neighboring node is calculated using the moving speed M_S of the current node and the neighboring node is calculated as $\frac{D_{ist}}{t}$. As well as the moving directions varying depending on the moving angle of both the current node and the neighboring node, in this situation node speed variations, and angle deviations brings location coordinate variations, so the node position will continue to change till the end of network actions. From these values, the relative directional motion at both latitude and longitude is calculated as m and z.

$$m = cos_{\theta di} M_{Si} - cos_{\theta dj} M_{Sj} \tag{3}$$

$$z = sin_{\theta di} M_{Si} - sin_{\theta dj} M_{Sj} \tag{4}$$

The distance between both latitude and longitude is calculated in Eq. (5) and denoted as x and y.

$$x = x_{1i} - x_{2j}$$

$$y = y_{1i} - y_{2j} \tag{5}$$

The transmission range of the node is signified by the radius r. Using these values as input, the connection lifetime for each node is calculated as seen below Eq. (6).

$$C_L = \frac{-(mx + zy) + \sqrt{(m^2 + n^2)r^2 - (my - zx)^2}}{m^2 + y^2} \tag{6}$$

Parameter distance is calculated by means of Euclidean distance estimation using latitude and longitude as inputs. The next parameter is to calculate how many routes are available for each node to reach the destination by its neighbor with node counts R_C. The MR_C parameter indicates the source path with the minimum distance that can be verified and destined through all available neighboring nodes.

4.1 Optimized Path Selection Initiation

Once the objective parameters for each node have been calculated, the L_W optimization algorithm is invoked to calculate the optimal confidence values to finalize the path, in this optimization, approximate initial populations are generated for each entry in the confidence table. In the L_W process, vector coefficients such as a and b are determined using equations

$$a = R_1\, B_V\, v - R_1$$

$$b = vB_V \tag{7}$$

Here boundary value B_V is taken as 2, v is the approximate generated vector, and R_1 is a parameter that decreases in random number from 1 to 0.

4.2 The Following Steps are Implemented During Further Repetitions

The node status update during the optimization process is recognized by hunting behavior of L_W, such as prey rounding, bubble-net attack, and prey search. Through the process of prey rounding, the distance vector D_V is determined as $(bB_{AS} - P)$. P is the current population, and B_{AS} is the best search agent status vector for the first iteration of the L_W. At the stage of exploitation, the bubble-net attack process involves with the support of a spiral bubble-net attack, which uses the whale's helix-shaped motion as follows to find the location of each population.

$$P_{i+next} = D_V \cos(\pi IB_V) + S_{Pi}\, e^{Ic} \tag{8}$$

Here c is a continual that describes the shape of a logarithmic loop, and I is the number designated from the interval from −1 to 1. S_{Pi} is a selected population in the present iteration taken as $S_{Pi} = aD_V - B_{AS}$.

Using the L_W process, the vector v_r is generated, which is approximately selected from the range between 0 to 1. The search space is improved by utilizing the L_W update rule as follows Eqs. (9) and (10),

$$if\,(v_r < 0.5) \tag{9}$$

$$S_{Pi} = aD_V - B_{AS} \quad else$$

$$S_{Pi+next} = D_V \cos(\pi IB_V) + S_{Pi}\, e^{Ic} \tag{10}$$

Population-related solution vectors are calculated using the following Eq. (11),

$$S_{Pi+next} = \frac{1}{(0.05 + 1 - 0.1R_1)(P(R_1 0.05 + 1 - 0.1R_1R_2)) + aD_V\,(0.1R_1 - 0.05)} \tag{11}$$

where R_1 and R_2 are approximate random numbers selected between 0 and 1. Later fitness F value is calculated by combining estimated parameters such as confidence I_{DC}, energy E_C, C_L, distance D_{istC} and route counts R_C for each solution vector, which is labeled in Eq. (12).

$$F = \frac{1}{5}\frac{aD_{ist}}{R_C} + I_{DC} + E_C + C_L + \frac{R_C}{MR_C} \tag{12}$$

If the developed solution has more F compared to the previous iteration, the solution will be sent to the next iteration, Otherwise the old re-solution is used to create the next random solution in further iterations. Once the maximum number o repetitions of the recalculation are reached when the required criteria are met based on the best global solution, the iterative process is stopped. The estimated optimal confidence value is used to select the best forwarding node to transmit the data packet and we can finalize the node is confident.

4.3 Multi-Purpose Optimization Evaluated in MAC Layer

Second multi-purpose optimization is used in the mac layer for optimal medium access-based transmission during data transmission. During the data transfer period, node sends request to send-R_{TS} packet to a targeted node to book the channel. The required time node takes for the data transmission is

enclosed along with the R_{TS} packet is calculated as follows: Here TR_{TSD}defines the total time required to forward the data from a node to the next confident neighbor.

$$TR_{TSD} = A_{CKt} + 2S_{IFSt} + \frac{8 + C_{TS}(B_D + P_S)}{B_W} \tag{13}$$

Here B_D meant the data bytes holding to transfer, P_S describes the data packet size, B_W explains the current bandwidth to transfer the packets, C_{TS} defines the channel free status as clear to send packet send to the R_{TS} sender, this packet transferred after the period of short inter frame space period S_{IFS} multiplied with 2 to avoid the channel competition issues as shown in Figs. 4 and 5, A_{CK} tells the acknowledgement of the data packet reception by the neighbor node. Later R_{TS} sender waiting time S_W is calculated as follows to get the C_{TS} message: Here M_{BO} defines the maximum back off period at mac layer.

$$S_W = \Delta + S_{IFS} + M_{BO} + I_N \tag{14}$$

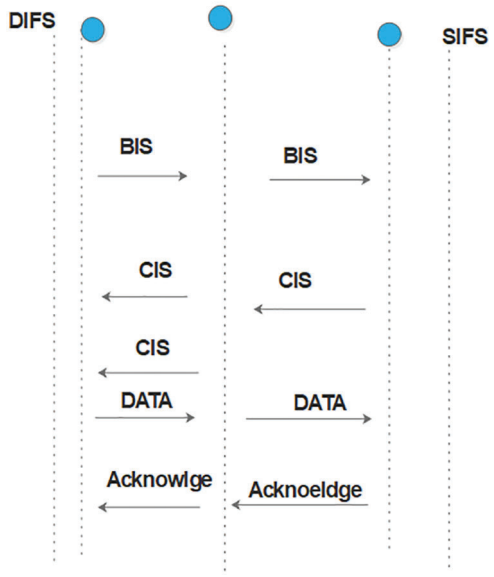

Figure 4: Channel selection

Even after the waiting period if the node is unable to get the channel confirmation, it cancels the previous request and initiates the new one as a timeout of C_{TS} reception computed as $C_{TSN} = 2\Delta + C_{TS} + S_{IFS} + TR_{TS}$, where Δ is channel propagation delay. Once the channel is confirmed by the C_{TS} reception then the sender transmits the packets, after the data transmission from the sender to the confident neighbor acknowledgment confirmation is computed by the node as

$$A_{CK} = A_{CKt} + 2S_{IFSt} + 2\Delta + \frac{(B_D + P_S)8}{B_W} \tag{15}$$

In cooperative transmission period, the optimal T_P at the source and forwarding node changes the approval time as follows Eqs. (16)–(18):

$$EA_{CK} = 2 - A_{CK}\Delta + 2\Delta + S_{IFS} \tag{16}$$

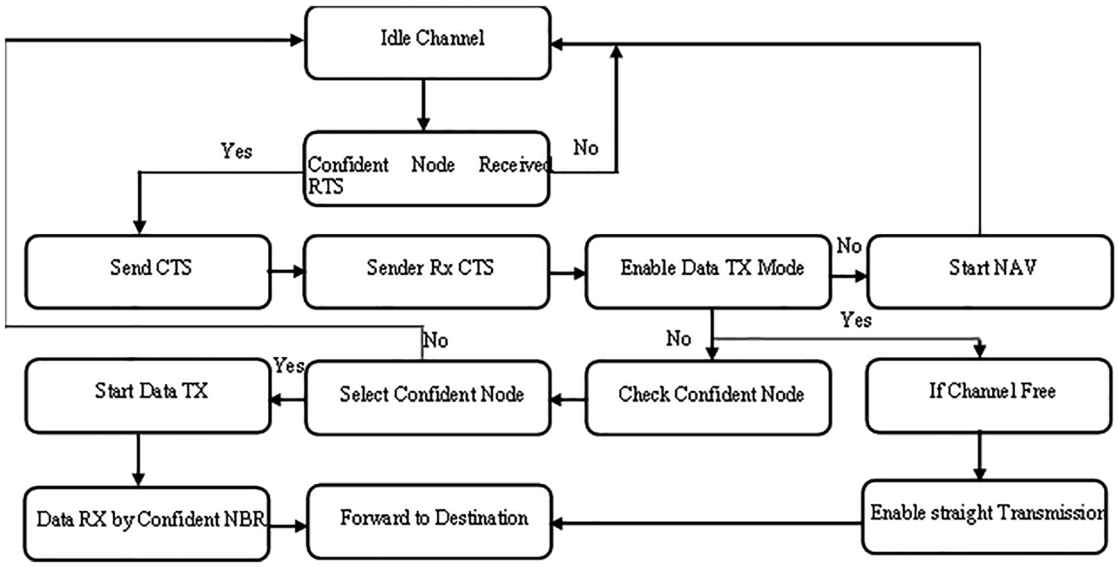

Figure 5: Communication at MAC layer

Then the confident node C_{St} not replied timeout is computed as

$$C_{St} = 2\Delta + C_{TS} + R_{TS} + S_{IFSP} + I_{DCS} \tag{17}$$

and the confident node connection C_{SC} duration is computed as

$$C_{SC} = A_{CKt} + 2S_{IFSt} + \frac{2(B_D + P_S)8}{B_W} \tag{18}$$

Then, the waiting period for the C_{Sw} frame is determined

$$C_{Sw} = C_{SC} + \frac{(B_D + P_S)8}{B_W} + A_{CKt} + 2S_{IFS} + 2\Delta \tag{19}$$

Then, the time takes for the data packets to reach the B_S is calculated as $D_D = +S_{IFS} + A_{CK}$

After receiving the R_{TS} frame, the node that received the packet sends the C_{TS} packet to the source node after the S_{IFS} period. Here, direct transmission is used if the channel is free with no competition, and the A_{CK} packet is sent to the source node when the data transfer is complete.

If another transaction occurs within that transmission region at the same time, the joint exchange is initiated by updating CC_{TS} as follows Eq. (20)–(23),

$$CC_{TS} = CI_{DC} + CC_{TSW} + S_{IFS} \tag{20}$$

$$CI_{DC} = 2\Delta + M_{BO} + C_{TS} + S_{IFS} + C_T \tag{21}$$

$$C_T = \frac{8C_{PH}}{B_W} //\text{Confident Node Time} \tag{22}$$

$$CC_{TSW} = \frac{8 + C_T B_D + P_S}{B_W} + S_{IFS} + 2\Delta \tag{23}$$

If the frame transmission delay is less than the C_{TS} duration, the transmission period will be renewed as $D_T = D + S_{IFS} + \Delta$. Forwarder back off helpfulness calculated as per the node energy metric E_M , direct and cooperative transfer rate as inputs. The energy parameter is computed as follows Eq. (24),

$$E_M = \frac{R_E}{I_E - S_{TP}} \tag{24}$$

Transmission power parameter is computed as ratio between the straight connection power $S_{TP} = T_P$ and cooperative forwarder channel power F_{Pc} computed as below Eqs. (25)–(28).

$$F_{Pc} = F_P + S_{TP} \tag{25}$$

$$\varphi = \frac{\boldsymbol{\mu}}{2l_{og}(\lambda 2 + T_S + \rho)} \tag{26}$$

$$T_S = D + S_{IFS+}\Delta \tag{27}$$

$$F_P = \boldsymbol{\varphi} - \frac{(T_R 2^{R_T 2})}{(R_G)^2 D_{ist} - \alpha} \tag{28}$$

Here $\boldsymbol{\mu}$, ρ and $\boldsymbol{\lambda}$ are the Lagrangian multipliers. Also, transmission rate parameter is computed as ratio between the S_{TP} rate and F_{Pc} rate. Where R_T is the rate of transmission, T_S is the packet delivery period, R_G explains the receiving channel gain, This is where the cooperative transmission power is estimated as a sum of the optimal transmit power at source and the individual relaying nodes. The forwarder node power is computed as F_P. A defines the constant propagations as 2. From these values, the forwarder back off helpfulness F_{PH} is computed as Eq. (29):

$$F_{PH} = \frac{\boldsymbol{\beta} F_{Pc}}{S_{TP}} \frac{E_I}{R_E - T_P} \frac{T_R}{B_W} \tag{29}$$

beta is set to ensure timely selection of the forwarder. Based on the estimated optimal transmission power, the forwarder power strong helping node for the current transmission is calculated as F_{PH}. If the estimated $F_{PH}$is less than the current F_{PH}period, the newly rated F_{PH} is assigned as the optimal departure period to achieve effective data transmission, which is designed in Eq. (30).

$$\text{Max} F_{PH} = min(maxF_{PH}, M_{BO}) \tag{30}$$

5 Results and Discussions

Network size is tested as 1000 × 1000 within an area in this experiment. As well as making changes to protocol routing and the mac layers and testing the performance of those changes in graphs format as given below Tab. 1. This protocol tells the best way to select a reliable forwarder and select the appropriate channel for the packets as they go through the network at regular intervals, here we see their test results.

Packet delivery ratio is the percentage of packets conventional at the destination depending on the number of packets shipped. Here, the CRCN protocol has received more packets at the destination. This Fig. 6 shows that this is achieved by the neighbor's reliable selection module and by changing the channel selection method on the mac layer. By adding the largest number of packets to the destination, the designed CRCN protocol can see to it that the data packets are delivered to the destination in the correct manner. Here, we give the packet size as input and see the output of the resulting changes. By comparing between two techniques, the proposed method reaches the better Packet Size *vs*. Packet Delivery Ratio results.

Table 1: CRCN network parameters simulation parameters

CRCN Network Parameters	
Simulation parameters	**Value**
Channel type	Wireless Channel
Tool	MATLAB 2018(a)
Radio-propagation model	Two Ray Ground
Routing protocol	CRCN
Number of Nodes	50
X dimension of Network Size	1000 sqm
Y dimension of Network Size	1000 sqm
Simulation Time	200 s
Initial energy in Joules	100
Receiving Power	0.01 mw
Transmission Power	0.02 mw

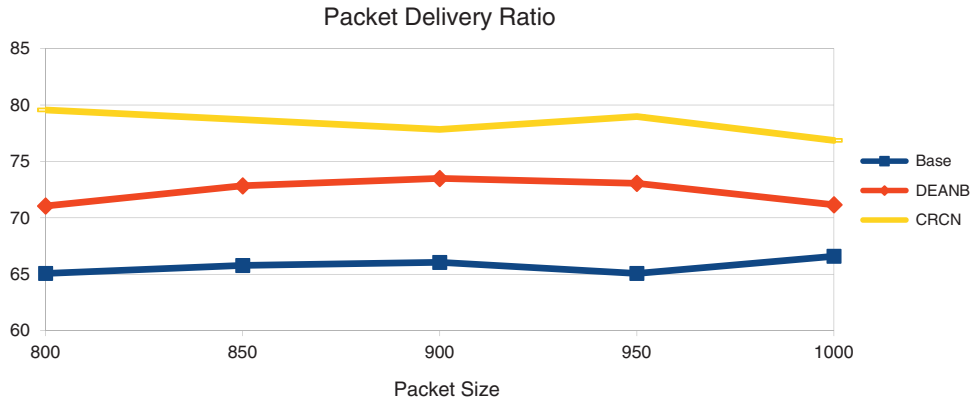

Figure 6: Packet size *vs*. packet delivery ratio

Throughput is the bits count of packets going to the destination. If the destination has received too many bits, we can know that the network is performing better. Here we can see that the CRCN protocol has received more packets than the compared others as shown in Fig. 7. This is an expression of the secured network and the network transmission is increased by selecting the proper node as the forwarder by the reports of the neighboring nodes and the reports of the nodes around it. And, by easily selecting the channel between them, more packet bits are delivered.

This is an expression of the secured network, and the network transmission is increased by selecting the proper node as the forwarder by the reports of the neighbors and the reports of the second level nodes. And, by easily selecting the channel between them, more packet bits are delivered. Also, the reliability of the node is a factor, so in this proposed CRCN protocol, the reliability of the node and their channel selection act as an important parameter. By comparing between two techniques, the proposed method reaches the better packet transmission range *vs*. delay results. The Fig. 8 shows that its functions are very good.

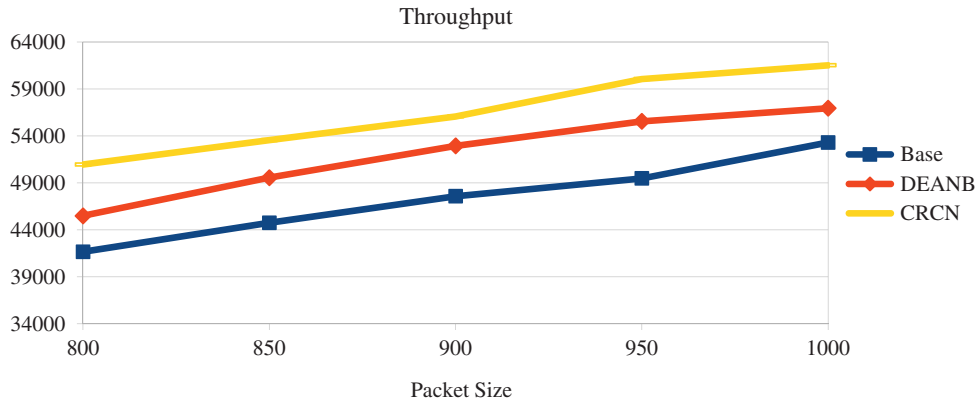

Figure 7: Packet size *vs*. throughput

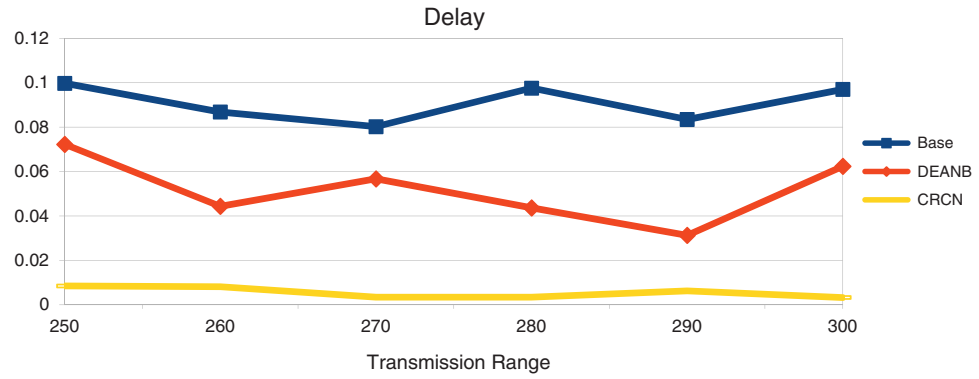

Figure 8: Transmission range *vs*. delay

Energy plays an important role in this. Network energy management is done with initial energy, remaining energy, packet transmission power, receiving power, so energy is also calculated as an important parameter when selecting the confident node. The Fig. 9 shows that the amount of energy stored in the network has increased due to this. Energy will be depleted very fast by unreliable nodes and that issue is solved here. Also, packets may expire if the correct channel is not set. The same issue is solved here. Due to this, the remaining energy in CRCN has increased.

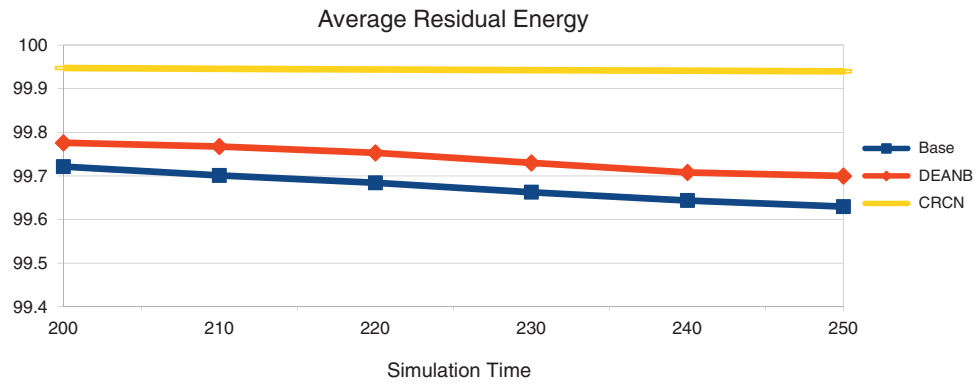

Figure 9: Simulation time *vs*. remaining energy

6 Conclusion

In this study, the steps show how the node acts as a confident forwarder and shares the channel in a way that is compatible with communication. We calculate the confidence of the node at the start of the network with the reliability report of the one hop and the reliability report of the secondary hop report. We figure out the combined confidence and use the same node as the most confident node as a forwarder, so we can move things along faster. When the routing packets sent to find the path reach the MAC layer, the next node in the path can be contacted directly if the channel is not used by any other nodes, and the channel is chosen. There will be no way to connect the channel unless there is a node that is sure. Then the path will be set. In this experiment, the amount of energy that is stored in the network is more than before. The nodes that aren't reliable will use up a lot of energy very quickly, but that problem has been solved here. Even if the right channel is set, packets may not last long if they don't reach the right person. The same thing has been solved here. Because of this, the amount of energy left in CRCN has gone up. When a node is confident, it chooses the best channel and the path is set up so that the network performance can be better than with the other protocols. To make the network work better, we can use this network security to let us use cognitive based channel selection and scheduling.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. H. Jhaveri Patel, N. M. Zhong and Y. Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT," *IEEE Access*, vol. 5, no. 6, pp. 20085–20103, 2018.

[2] J. A. Anser, G. Han and H. Wang, "A novel reliable adaptive beacon time synchronization algorithm for large-scale vehicular ad hoc networks,IEEE," *Transactions on Vehicular Technology*, vol. 8, no. 68, pp. 11565–11576, 2019.

[3] C. F. Wang, Y. P. Chiou and G. H. Liaw, "Nexthop selection mechanism for nodes with heterogeneous transmission range in VANETs," *Computer Communications*, vol. 1, no. 55, pp. 22–31, 2015.

[4] W. Y. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. C. Liang *et al.,* "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 22, pp. 2031–2063, 2019.

[5] Z. Lidong and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[6] M. Haenggi, "Routing in ad hoc networks – a wireless perspective," in *First Int. Conf. on Broadband Networks*, DC, USA, pp. 652–660, 2004.

[7] V. Karpijoki, "Security in ad hoc networks," in *Proc. of the Helsinki University of Technology, Seminars on Network Security*, Helsinki, Finland, pp. 1–14, 2000.

[8] N. Krishnaraj and S. Sangeetha, "A study of data privacy in internet of things using privacy preserving techniques with its management," *International Journal of Engineering Trends and Technology*, vol. 70, no. 2, pp. 43–52, 2022.

[9] C. Yu, B. Lee and Y. H. Yong, "Energy efficient routing protocols for mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 3, pp. 959–973, 2003.

[10] S. Kulkarni, S. Ambaji and G. Raghavendra Rao, "A performance analysis of energy efficient routing in mobile ad hoc network," *International Journal of Simulations–Systems, Science and Technology–IJSSST*, vol. 10, no. 1–A, pp. 1–9, 2010.

[11] Y. Xu, H. Johnand and E. Deborah, "Geography-informed energy conservation for ad hoc routing," in *Proc. of the 7th Annual Int. Conf. on Mobile Computing and Networking*, Rome, Italy, pp. 70–84, 2001.

[12] A. Spyropoulos and C. S. Raghavendra, "Energy efficient communications in ad hoc networks using directional antennas," in *Proc. Twenty-First Annual Joint Conf. of the IEEE Computer and Communications Societies*, BC, Canada, vol. 1, pp. 220–228, 2002.

[13] M. V. S. S. Nagendranth, M. R. Khanna, N. Krishnaraj, M. Y. Sikkandar, M. A. Aboamer *et al.,* "Type II fuzzy-based clustering with improved ant colony optimization-based routing (T2FCATR) protocol for secured data transmission in manet," *The Journal of Supercomputing*, vol. First Online, pp. 1–22, 2022.

[14] R. Zheng and R. Kravets, "On-demand power management for ad hoc networks," in *Proc. IEEE INFOCOM 2003. Twenty-second Annual Joint Conf. of the IEEE Computer and Communications Societies*, BC, Canada, vol. 1, pp. 481–491, 2003.

[15] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta *et al.,* "A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing," *Wireless Personal Communications*, vol. First Online, pp. 1–24, 2021.

[16] G. Priyanka, V. Parmar and R. Rishi, "Manet: Vulnerabilities, challenges, attacks, application," *IJCEM International Journal of Computational Engineering & Management*, vol. 11, no. 1, pp. 32–37, 2011.

[17] P. Rajamohan and W. C. Kong, "Performance analysis and special security issues of secure routing protocols in ad-hoc networks," *International Journal of Scientific Engineering and Technology*, vol. 3, no. 8, pp. 1094–1099, 2014.

[18] A. Waqas, H. Mahmood and N. Saeed, "Interference aware cooperative routing for edge computing-enabled 5G networks," *IEEE Sensors Journal*, vol. 12, no. 5, pp. 325–336, 2022.