Received: August 18, 2021. Revised: September 24, 2021. 596

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Security and Energy Aware Adaptive Routing using Cost Centric Cuckoo Search Algorithm

Sowmyashree Malligehalli Shivakumaraswamy[1]* **Chikkanayakanahalli sadashivaiah Mala[1]**

[1]*Department of Electronics and Telecommunication Engineering,*
BMS Institute of Technology and Management Bengaluru-56064, India
* Corresponding author's Email: Sowmyashree.m.s@bmsit.in

Abstract: In the previous few years, innovations in the Wireless Sensor Network (WSNs) domain have acquired momentum because of WSN's various applications in farming, mechanical assembling, military observation, ecological checking, clinical and medical care, debacle recuperation tasks and so forth. In WSN, the wireless sensor nodes are organized randomly to communicate with other nodes inside the network. Since the nodes are battery-powered, energy is one of the major constraints in WSN. Moreover, the nodes are affected by malicious attacks (ex. black hole attack) which leads to security issues in the network. In this paper, the Cost Centric Cuckoo Search Algorithm (CCCSA) is proposed to overcome the energy and security issues in WSN. Here, the clustering operation is performed using the K-means clustering algorithm followed by CCCSA is used to select the adaptive Cluster Head (CH) between the normal nodes in the cluster. Further, the CCCSA is integrated with Ad hoc On-Demand Distance Vector (AODV) routing protocol to generate the adaptive routing path. In CCCSA, the trust value is considered as primary cost value for accomplishing a secure communication in WSN. The Packet delivery rate of the CCCSA method is 95.91% and it is higher when compared to the existing Media access control Centralized Routing Protocol (MCRP), Secure Routing Protocol based on Multi-objective Ant-colony-optimization (SRPMA) method and Realisable Secure Aware Routing (RSAR) protocol.

Keywords: Ad hoc on-demand distance vector routing protocol, Cluster head selection, Cost centric cuckoo search algorithm, K-means clustering algorithm, Security, Wireless sensor network.

1. Introduction

WSN is a combination of various minuscule measured sensor hubs which carry out a bunch of activities such as detection, transmission and handling different remote communication assignments [1, 2]. The WSNs are classified into two categories known as structured WSN and unstructured WSN. The network in which the sensor hubs are deployed in an ad-hoc manner is called a structured WSN network. The network in which the sensor hubs are deployed in a preplanned way is called an unstructured WSN network [3]. The sensor hubs communicate between themselves by using the radio frequency through air medium [4]. These sensor hubs collect and store helpful data for additional important activities which are should be taken by the sink hub [5]. Hence, the sensor hubs need to be deployed either in a uniform or ad-hoc manner for smooth assortment and validation of data for various discrete occasions [6]. Because of its restricted battery limitation, power usage is a significant factor that needs consideration for effective data transmission in the network [7]. Hence, the clustering and routing approaches help in limiting the energy utilization and in reducing the processing overhead in the network. However, the path obtained to reach the destination node from source node by using the routing approach has several security issues [8, 9].

Recently, WSN has become vulnerable to several attacks which leads to an insecure environment for data transmission. Some of the attacks performed on the sensor hubs by the hackers are the black hole attack, DoS attack, Spoofing

attack and Sybil attack [10, 11]. Hence, the sensor nodes are easily affected by hackers and act as malignant nodes. The malignant nodes in the network cause insecurity to the entire network during data transmission [12]. The occurrence of unauthenticated data access becomes possible that results in loss of essential information stored in the nodes which is a matter of extreme concern [13-15]. As a result of this, a secured and energy-efficient routing protocol is an urgent requirement to extend the lifespan and to provide security to the network. While designing a protocol to obtain a secured communication over WSN, the following factors are to be taken into consideration: integrity, forward secrecy, backward secrecy, freshness, non-repudiation and availability [16]. Hence, a secure and energy aware adaptive routing using CCCSA is proposed for selecting an adaptive CH and routing path in the network. The selected adaptive CH and routing path are used to enhance the packet delivery ratio and energy consumption of the WSN. The main contributions of this research work are given as follows.

- The K-means clustering algorithm is utilized for accomplishing an effective over the nodes present in the network. Here, the K-means clustering is used because of its faster clustering operation and also it helps to minimize the energy consumption.
- The CCCSA is introduced for an adaptive CH selection. The CH selection process is performed based on the cost values such as node degree, distance, residual energy and trust value. Here, the adaptive CH selection is used to select an appropriate CH in various communication levels (e.g., high and low residual energy level of the nodes).
- Specifically, the trust value is considered as primary cost for avoiding the malicious nodes during the data transmission. Furthermore, the cuckoo search algorithm is integrated with the AODV routing protocol to find a secure and adaptive path for well-protected data transmission in the network.

The overall structure of the paper is given as follows: The related works are reviewed in Section 2. A detailed explanation of the CCCSA is provided in Section 3. The performance analysis of the CCCSA is explained in Section 4. Finally, Section 5 concludes the paper.

2. Literature review

Some of the recent techniques applied to get an effective and secure cluster-based routing protocol for WSN are reviewed in this section. The methodology, advantages and limitations of the existing methods are also being discussed.

Ahutu and El-Ocla [17] developed MAC Centralized Routing Protocol (MCRP). The implementation of centralized network intelligence was achieved by the developed MCRP. The MCRP operated in one component of the Base Station (BS) that reduces the power utilization while keeping the harmony between BS and sensor hubs to effectively identify the wormhole attacks. The performance of the WSN improved even if the number of nodes was maximized by the MCRP protocol. However, the MCRP needed further upgrading to improve the performance of WSN due to the less few of nodes. The results of the MCRP were evaluated in terms of frame delivery ratio, throughput, average measured time, energy consumption, packet loss rate and end-to-end delay.

Shi [18] developed a Reputation-Based Mechanism to Stimulate Cooperation (RBMSC) mode. The route for data transmission was obtained by the developed protocol. The developed protocol provided security from malicious attacks. The variant of the Dijkstra algorithm was enhanced by the developed method to produce a secure path for data transmission in WSNs. The developed RBMSC mode failed to calculate the time delay for each path during transmission. The results are evaluated in terms of the number of nodes, packet delivery ratio and packet loss rate.

Salari-Moghaddam [19] utilized the trust-based routing algorithm to enhance the quality of services in Dynamic Source Routing (DSR) protocol. The developed method prevented the malicious nodes in the routing path by using the trust-based DSR (TDSR). In the next step, Enhanced DSR (EDSR) was introduced which was used to improve the quality of services. Therefore, the DSR method achieved better performance in the packet delivery ratio and reduced the energy utilization in the network. However, the DSR and TDSR protocols provided lower performance in discovering the shortest path and sometimes it selected the longer path due to the higher energy consumption.

Sun [20] implemented the Secure Routing Protocol based on Multi-objective Ant-colony-algorithm (SRPMA) for WSN. Two objective functions were mainly considered in the developed method. The first objective function was about considering the typical residual energy of the routing path to minimize energy utilization. The second objective function was about considering the routing path's typical trust value which ensures the route nodes being secured. The SRPMA method

achieved better performance against black hole attacks in WSN. However, the routing path generation of SRPMA method was considered only the energy and trust value of node.

Yarde [21] developed an Adaptive Immune-Inspired Energy-Efficient Cross-Layer Routing (AIEECR) protocol. To enhance the area coverage and to reduce the coverage hole problems in the network, an adaptive sunflower optimization (ASFO) algorithm was introduced in this paper. An artificial immune-based routing protocol is utilized here for choosing an effective routing path for the data communication from CH to the BS. The quality of service of the network was unable to improve by the developed model due to the network overloads. The results obtained by the developed model are evaluated in the following terms such as packet delivery ratio, average energy consumption, jitter, throughput, and delay.

Basha [22] presented the Realisable Secure Aware Routing (RSAR) protocol for minimizing the control overhead of the network. The trust degree of each node was calculated by using the conditional tug of war optimisation in the RSAR protocol. Here, the energy consumption was optimized by using the cluster based data aggregation. But, the developed RSAR was considered only energy of the nodes, it failed to consider the distance and node degree of the nodes.

The limitations found from the literature review are generation of routing with high transmission distance and inappropriate selection of cost functions. The above limitations lead to the higher energy consumption and less packet delivery ratio. In order to overcome the aforementioned limitations, the proposed CCCSA is used to select an adaptive CH and routing path over the network. Therefore, an appropriate CH and routing path is selected, even when the network is operated under various communication levels such as high & low residual energy, high & low node degree, high & low transmission distance, and so on. This helps to improve the PDR of the CCCSA while minimizing the energy consumption of the network.

3. CCCSA method

This research paper proposes an adaptive CH selection and routing protocol to enhance the packet delivery of the WSN. The CCCSA method contains three phases that are clustering, Cluster Head (CH) selection and routing operations. The clustering is performed by using the K-means clustering algorithm. The CH selection and routing process are performed by using the CCCSA. An adaptive CH selection is performed based on the cost values considered in the proposed CCCSA method. The considered cost values are distance, node degree, residual energy and trust value. The trust value of the nodes is computed to prevent the network from Blackhole attacks. The malicious nodes are avoided during the CH selection process, thus it is called as an adaptive clustering and routing process. Since the CCCSA is referred as adaptive approach, because it is used to deliver better performances for different levels of communication. Specifically, the CCCSA selects the node as CH in the following categories: i) the candidate CH node with higher trust value, less distance to the BS, high energy, and less node degree, ii) the candidate CH node with medium distance, high energy, high node degree and higher trust value, iii) the candidate CH node with high distance, medium level of energy, high node degree and higher trust value and so on. In all of these cases, the CCCSA adaptively selects the authorized node, even in different communication level. Therefore, the developed CCCSA method is referred as adaptive approach which helps to improve the packet delivery.

The main aim of the CCCSA is to provide secured clustering and routing operation to improve the packet delivery ratio. The flowchart of the CCCSA is given in Fig. 1.

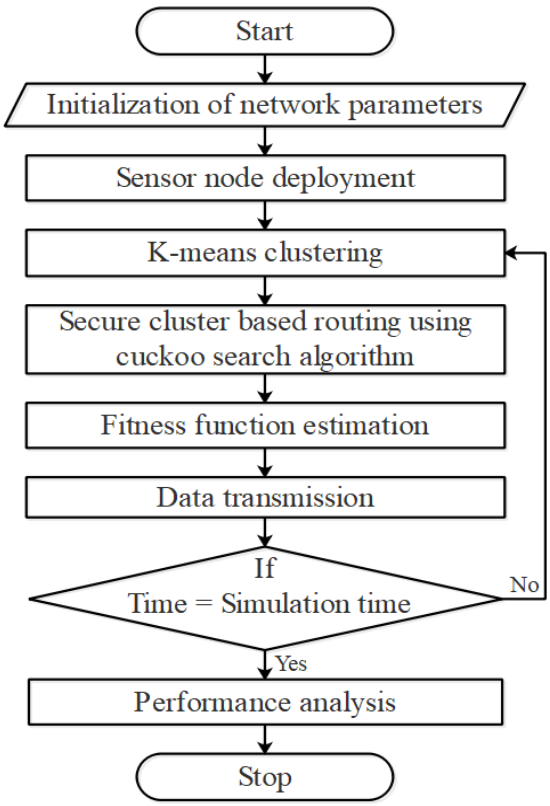

Figure. 1 Flow chart of the CCCSA method

3.1 Clustering using K-means algorithm

The K-mean algorithm is a partition-based classifying algorithm. In the K-mean algorithm, the n number of samples is divided into k number of subsets. These clustering subsets lead to high similarities inside the cluster. Initially, the k samples are selected randomly from the sets of data and the Euclidean distance between K centers and each sample is calculated. After that, the mean of the subsets is calculated which is referred to as the new clustering center. The K-means clustering algorithm is performed based on the above steps to generate the new cluster center.

3.2 Overview of a cuckoo search algorithm

The cuckoo search algorithm is a heuristic algorithm and it efficiently resolves the optimization issues by simulating the parasitic parenting and Levy flight of the cuckoo. The cuckoo bird does not nest during its breeding period. The cuckoo replaces its own egg with other birds to reproduce. After hatching the eggs, the cuckoo identifies its bird by comparing the similarities between them. The path to the new nest location for bird breeding is obtained by using the Eq. (1) as follows,

$$x_i^{(t+1)} = x_i^{(t)} + \alpha \oplus Levy(\lambda); i = 1,2, \dots \dots \dots, \quad (1)$$

where, $x_i^{(t)}$ represents the position of the nest of i^{th} bird in the t generation and α represents the step size control. $Levy(\lambda)$ represents Levi's random search path and it is obtained by the following Eq. (2).

$$Levy(\lambda) = t^{-\lambda}; 1 < \lambda < 3 \quad (2)$$

3.2.1. Adaptive cluster head selection using CCCSA

The CCCSA is utilized in this current research to select an adaptive sensor node as CH for each cluster. By selecting the adaptive CH node, the packet delivery of the network is improved in WSN. Since the CH responsibilities such as data aggregation and cluster management are increased, it is important to find a suitable node among all the cluster members. Here, the CH is selected based on the cost values such as distance, node degree, residual energy and trust value.

3.2.1.1. Cost estimation for cluster head selection

The cost value estimation is performed to improve the packet delivery by selecting an optimal CH among the nodes present in each cluster. The cost values involved in the CH selection are distance, node degree, residual energy and trust value. The definition and the derivation of the cost values are given below,

3.2.1.1.1. Residual energy

The CH in each cluster performs operations such as data aggregation and cluster management inside the cluster. Due to the high responsibility of the CH, the selected CH must have high residual energy to balance energy consumption inside the cluster. The node residual energy is calculated by using the Eq. (3) as follows,

$$F_1 = \sum_{i=1}^{m} \frac{1}{RE_{CH_i}} \quad (3)$$

where the node residual energy is represented as RE_{CH} and the number of nodes is represented as m.

3.2.1.1.2. Node degree

The number of hops connected to the respective node is defined as node degree which is the important factor to be considered in the next-hop selection. If the next-hop is selected with a low node degree, then the respective node lasts for a longer duration. The node degree calculation is performed by using Eq. (4).

$$F_2 = \sum_{i=1}^{m} |CM_i| \quad (4)$$

Where the quantity of the cluster nodes in the i^{th} cluster is represented as CM_i.

3.2.1.1.3. Distance

The distance between the CH and each of the cluster members in the cluster is calculated by using the Eq. (5). The distance calculation inside the cluster is performed to help improve the link quality between the nodes.

$$F_3 = \sum_{j=1}^{m} \left[\frac{\sum_{i=1}^{|CM_j|} d(CH_j, CM_i)}{|CM_j|} \right] \quad (5)$$

Where, the Euclidean distance between the CH of the j^{th} cluster and CM of the j^{th} cluster is represented a $d(CH_j, CM_i)$.

3.2.1.1.4. Trust value

The trust value calculation is an important factor while designing a secure system. In WSN, the trust

value calculation is applied for access control, trust routing and node authentication. The trust value of the nodes is calculated based on the behavior as given in Eq. (6).

$$F_4 = \frac{DS_{i,j}(t)}{DR_{i,j}(t)} \quad (6)$$

Where, $DS_{i,j}(t)$ refers the interval taken for the sender node to send the data and $DR_{i,j}(t)$ represents the time taken by the receiver node to receive the data.

3.2.1.2. Initialization

During the initialization phase, the cost values of each node are calculated by using the respective equations. The trust values are considered to avoid malicious nodes from getting selecting as CH. If the trust value is not taken into consideration, the nodes in the network have a high chance of getting affected by a black hole attack. Based on the cost values, the sensor nodes are listed in descending order. From that sort listed of nodes, only the top 20% of the nodes are selected as the most eligible CH candidates. Here, the clusters are referred to as host nests and the sensor nodes in them are referred to as eggs. After the initialization phase, the CCCSA iterative process is initiated.

3.2.1.3. Iterative process

Initially, the network has H host nests and m number of cluster members in each host nest. The selected most eligible CH candidates are present in all the host nests. In one cluster, there is a possibility of having more than one of the most eligible CH candidates. The cost value of the CH candidates is compared with other CH candidates in the same host nest to select an optimal CH for that cluster. This iterative process is repeated until an optimal CH is determined for all the host nests present in the network.

3.2.2. CCCSA based adaptive routing algorithm

The cost values used for the route discovery process are residual energy, node degree, trust value and distance of the nodes. The adaptive routing path for data transmission is selected by using a CCCSA. Similar to the CH selection, the routing path generation also adaptively works in different communication levels. The trust value calculation of the nodes is performed to prevent the nodes from black hole attack. By avoiding the malicious nodes during the path selection process, the chances of link failure are reduced.

3.2.2.1. Initialization

Here, the clusters are referred to as host nests and the sensor nodes in it are referred to as eggs. Initially, the dimension of each egg is equal to the quantity of CHs. Each egg position is initialized with a random node_id between 1 and n. Let, $E_i = (E_i^1, E_i^2 \dots \dots \dots E_i^m)$ be the i^{th} egg. Where each egg position $E_i^d, 1 \leq d \leq m$ represents node_id between 1 and n in the network. The possible path from source to the destination is figured out. The cost values of each node involved in the possible path is calculated. After completing the initialization phase, the iterative process is initiated.

3.2.2.2. Iterative process

The calculated cost values of the nodes are updated to the iterative process to find an optimal route for data transmission. The distance between the nodes is calculated in the cost values which leads to minimized link breaks during communication. Thus, the packet delivery ratio of the network is increased. Based on the cost values calculated in the CCCSA, optimal nodes in the network are selected. As discussed in section 3.2.1.1 the cost values for routing are calculated.

3.2.2.3. AODV based routing

The AODV routing protocol is integrated with a CCCSA in the research study. The source node broadcasts the route_request message throughout the network with its node_id and cost values. While receiving the route_request message, the optimal nodes existing in the path to the destination node return the route_reply message to the source node. The source node selects the better path by comparing their cost values attached with their route_reply message.

The developed CCCSA method is used to accomplish the adaptive CH selection and routing in the WSN. This CCCSA is used to select an optimal CH and to generate the routing path over the network. In this adaptive CH selection, the node which has the best trust value, high energy, less distance and less node degree is selected as secure adaptive CH. In that cost values, trust value is considered as an important cost value which is used for an effective detection and prevention of the malicious nodes in the network. Moreover, the CCCSA based routing generates a secure routing path over the network. Therefore, the developed

Table 1. Parameter specifications

Parameters	Values
MAC protocol	Mac/802.11
Antenna pattern	OmniAntenna
Communication radius	250 m
Data flow speed	448 kbit/s
Initial energy	50 J
Wireless propagation protocol	TwoRayGround
Interface type of the network	WirlessPhy
Queue type	PriQueue
Size of packets	210 Bytes
Number of connections	20
Simulation time	100 s

CCCSA is used to minimize the packet loss, while minimizing the energy consumption of the network.

4. Simulation results and discussion

The Network Simulator (NS) 2.34 platform is utilized for obtaining the simulation results and 100 nodes are randomly arranged in the area of 1200m × 1200m to simulate the CCCSA method. In this research, the simulation results of CCCSA method with the presence of black hole attack are analyzed. Various nodes are presented as malignant nodes, to simulate a black hole attack. The sink node's energy is limitless and the starter energy of every sensor node is steady. Table1 shows the details of the parameter settings of the CCCSA.

4.1 Performance evaluation

The performances of the CCCSA method are analyzed in terms of packet loss rate, end-to-end delay, packet delivery rate, average energy consumption, and routing load. The performance of the CCCSA is compared with three existing methods namely MCRP [17], SRPMA [20] and RSAR [22]. These existing methods are designed and simulated by using the same specifications mentioned in the Table 1. The aforementioned parameters are described as follows:

4.1.1. End to End Delay

The End to End Delay (EED) is referred to as the time taken by a receiver for the transmission of the packets to the number of packets received by the receiver. The EED is calculated by using the Eq. (7) as follows,

$$EED = \frac{total\ time\ taken\ by\ the\ receiver\ for\ packet\ transmission}{The\ number\ of\ packets\ received\ by\ the\ receiver} \quad (7)$$

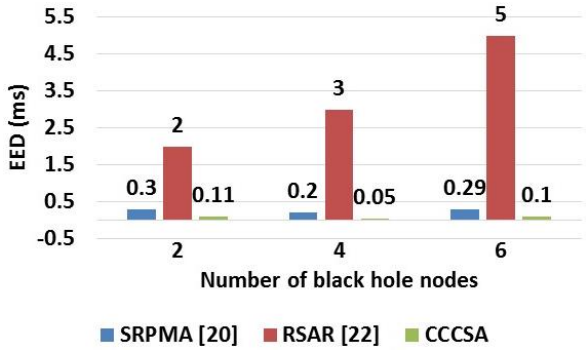

Figure. 2 End to end delay

The EED comparison of the CCCSA method with the SRPMA [20] and RSAR [22] is shown in Fig. 2. The EED of the CCCSA method is lesser than the EED of the existing SRPMA [20] and RSAR [22]. The distances between the nodes are calculated in the cost values to identify the shortest path for data transmission. Hence, the EED is minimized in the proposed method.

4.1.2. Packet Delivery Rate

The Packet Delivery Rate (PDR) is the ratio of the number of delivered packets to the number of packets sent during the data transmission. The PDR is computed by using the Eq. (8) as follows,

$$PDR = \frac{T_{ND}}{T_{NS}} \quad (8)$$

where, the number of delivered packets is represented as T_{ND} and the number of sent packets is referred as T_{NS} .

The packet delivery rate comparison of the CCCSA method with the existing SRPMA [20] and RSAR [22] is illustrated in Fig. 3. The CCCSA method shows the highest packet delivery rate when compared to the existing SRPMA [20] and RSAR [22]. The cost value includes the trust value of the nodes which minimizes the link failure during communication. Thus, the pack delivery rate of the CCCSA method is improved.

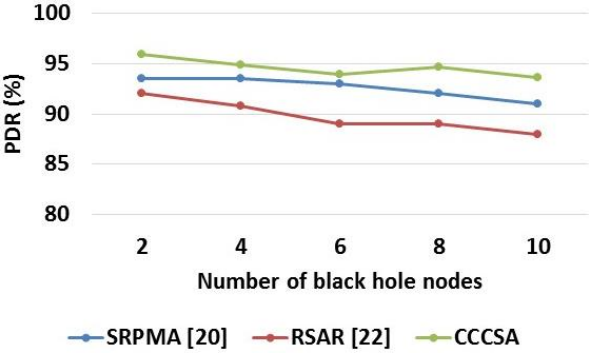

Figure. 3 Graphical comparison of PDR

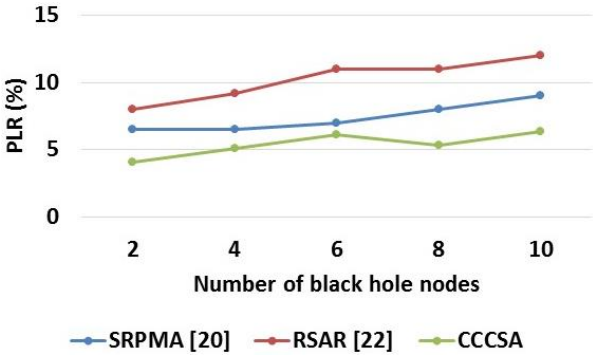

Figure. 4 Packet loss rate

4.1.3. Packet Loss Rate

The Packet Loss Rate (PLR) is obtained by the number of transmitted data packets from the source nodes and the number of received data packets by the sink in the simulation process. The packet loss rate is calculated by using Eq. (9).

$$Packet\ loss\ rate = 1 - \frac{No.of\ received\ data\ packets\ from\ the\ sink}{No.of\ sent\ data\ packets\ by\ the\ source\ node} \quad (9)$$

Fig. 4 illustrates the comparison between the CCCSA method and the existing SRPMA [20] and RSAR [22] in terms of packet loss rate. The packet loss rate of the CCCSA method is lesser when compared to the SRPMA [20] and RSAR [22]. The distance and trust values used in the cost value calculation reduces the link failure. In case of a link break during transmission, an alternative path is selected by using AODV routing protocol. Hence, the packet loss rate of the CCCSA method is minimized.

4.1.4. Routing Load

The Routing Load (RL) is referred to as the ratio of the number of transmitted data packets to the number of delivered data packets. The routing load is calculated by the Eq. (10) as follows,

$$Routing\ load = \frac{\delta}{\chi} \quad (10)$$

where, the quantity of transferred data packets is represented as δ and the quantity of delivered data packets is represented as χ .

The routing load comparison of the CCCSA method with the existing SRPMA [20] and RSAR [22] is given in Fig. 5. The routing load of the CCCSA method is minimized by reducing the control messages during the path selection process. The control messages are effectively reduced by using the AODV routing protocol. The CCCSA

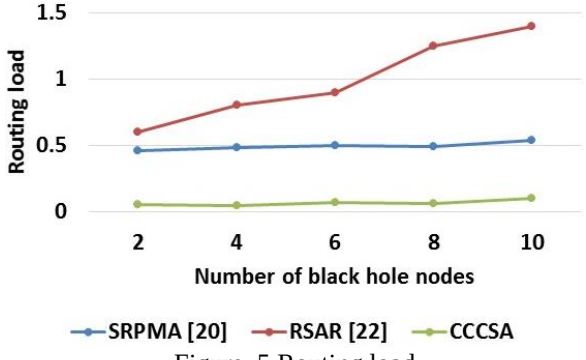

Figure. 5 Routing load

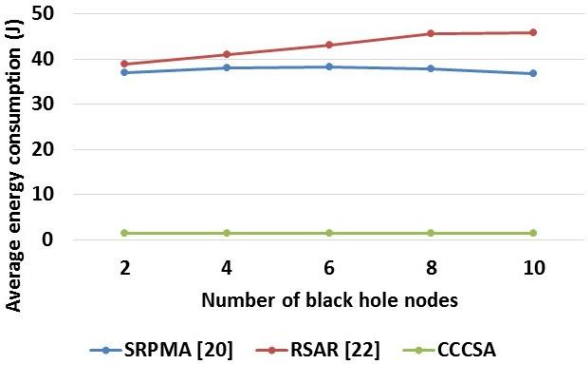

Figure. 6 Average energy consumption

method provides lesser routing load when compared to the SRPMA [20] and RSAR [22].

4.1.5. Average energy consumption

The average energy consumption is referred to as the sum of the receiving energy of each node and the transmitted energy. The average energy consumption is calculated by using the Eq. (11) as follows,

$$Average\ energy\ consumption = (E_{RX} \times number\ of\ nodes) + E_{TX} \quad (11)$$

Where the receiving energy and transmitted energy of the nodes are represented as E_{RX} and E_{TX}.

Fig. 6 illustrates the comparison between the CCCSA method and the existing SRPMA [20] and RSAR [22] in terms of average energy consumption. The CCCSA method shows a higher difference in energy consumption compared to the SRPMA [20] and RSAR [22]. During the path discovery process, the distance value is calculated to obtain the nearest node to transfer the data. Hence, the energy consumption of the nodes is reduced. The average energy consumption of the CCCSA method is lower when compared with the existing SRPMA [20] and RSAR [22].

Table 2 and Table 3 provides the comparative analysis of the CCCSA method with MCRP [17],

Table 2. Comparative analysis of average energy consumption, end-to-end delay and packet loss rate for CCCSA method

Number of black hole nodes	Average energy consumption (J)				EED (ms)				PLR (%)		
	MCRP [17]	SRPMA [20]	RSAR [22]	CCCSA	MCRP [17]	SRPMA [20]	RSAR [22]	CCCSA	SRPMA [20]	RSAR [22]	CCCSA
2	2.4	37	39	1.47	1.5	0.3	2	0.11	6.5	8	4.08
4	NA	38	41	1.38	NA	0.2	3	0.05	6.5	9.2	5.1
6	NA	38.2	43.08	1.33	NA	0.29	5	0.1	7	11	6.12
8	NA	37.9	45.71	1.34	NA	0.25	8	0.05	8	11	5.35
10	NA	36.8	45.8	1.5	NA	0.21	12	0.05	9	12	6.37

Table 3. Comparative analysis routing load and packet delivery rate for CCCSA method

Number of black hole nodes	RL			PDR (%)			
	SRPMA [20]	RSAR [22]	CCCSA	MCRP [17]	SRPMA [20]	RSAR [22]	CCCSA
2	0.46	0.6	0.052	75	93.5	92	95.91
4	0.48	0.8	0.043	NA	93.5	90.8	94.89
6	0.5	0.9	0.066	NA	93	89	93.87
8	0.49	1.25	0.059	NA	92	89	94.64
10	0.54	1.4	0.101	NA	91	88	93.62

SRPMA [20] & RSAR [22], where the term NA represents the parameters which are Not Available for the respective existing method. From the performance analysis, it is concluded that the performances of the CCCSA is better when compared to the MCRP [17], SRPMA [20] and RSAR [22]. The performance of MCRP [17], SRPMA [20] and RSAR [22] is less, because of its inappropriate selection of the cost values. The CCCSA considers four optimal cost values such as residual energy, node degree, distance and trust value. Specifically, the trust value considered in the CCCSA method is used to avoid the malicious nodes which leads to reduce the packet loss. However, the secure adaptive clustering and routing performed by the CCCSA is used to improve the PDR and average energy consumption of the network.

5. Conclusion

In this research paper, the K-means clustering algorithm is utilized to perform the clustering operation of the nodes present in WSN. The CCCSA algorithm is proposed to select an adaptive CH from the clusters and it is integrated with the AODV routing protocol to find an adaptive routing path for data transmission. The CH selection and routing operations are performed based on four different cost values such as are residual energy, node degree, distance and trust value. An adaptive CH selection and routing performed by the CCCSA is used to avoid malicious nodes in various communication levels i.e., the node with high and low residual energy. The nodes are prevented from the black hole attack by calculating the trust value. Hence, the CCCSA method provides secured data transmission in the network. The simulation results of the CCCSA method are much better when compared to the results of the existing SRPMA and RSAR. The energy consumption of the CCCSA method is 1.34 J for 8 black hole nodes and it is lesser when compared to the SRPMA and RSAR. The hybrid optimization approach will be used to improve the WSN's performance in future projects.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] K. Guleria and A. K. Verma, "Meta-heuristic ant colony optimization based unequal clustering for wireless sensor network", *Wireless Personal Communications*, Vol. 105, No. 3, pp. 891-911, 2019.

[2] N. Mittal, "Moth flame optimization-based energy efficient stable clustered routing

approach for wireless sensor networks", *Wireless Personal Communications*, Vol. 104, No. 2, pp. 677-694, 2019.

[3] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah, and A. Kannan, "An energy-aware trust based secure routing algorithm for effective communication in wireless sensor networks", *Wireless Personal Communications*, Vol. 105, No. 4, pp. 1475-1490, 2019.

[4] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks", *Wireless Personal Communications*, Vol. 110, No. 4, pp. 1637-1658, 2020.

[5] R. Sharma, V. Vashisht, and U. Singh, "Fuzzy modelling based energy aware clustering in wireless sensor networks using modified invasive weed optimization", *Journal of King Saud University-Computer and Information Sciences*, 2019.

[6] R. Sharma, V. Vashisht, and U. Singh, "eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks", *Telecommunication Systems*, pp. 1-16, 2020.

[7] B. M. Sahoo, T. Amgoth, and H. M. Pandey, "Particle swarm optimization based energy efficient clustering and sink mobility in heterogeneous wireless sensor network", *Ad Hoc Networks*, Vol. 106, p. 102237, 2020.

[8] S. Famila and A. A. Jawahar, "Improved artificial bee Colony optimization-based clustering technique for WSNs", *Wireless Personal Communications*, Vol. 110, No. 4, pp. 2195-2212, 2020.

[9] V. B. Christopher and J. Jasper, "Jellyfish dynamic routing protocol with mobile sink for location privacy and congestion avoidance in wireless sensor networks", *Journal of Systems Architecture*, Vol. 112, p. 101840, 2021.

[10] T. Khan, K. Singh, M. A. Basset, H. V. Long, S. P. Singh, and M. Manjul, "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks", *IEEE Access*, Vol. 7, pp. 58221-58240, 2019.

[11] G. Dhand and S. S. Tyagi, "SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks", *Wireless Personal Communications*, Vol. 105, No. 1, pp. 17-35, 2019.

[12] S. I. Guddappa and R. M. Hegde, "Priority Aware Frequency Domain Polling Protocol in Cyber Physical Systems to Ejection of Malicious Node Attack", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 3, pp. 580-588, 2021

[13] W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks", *Digital Communications and Networks*, 2021.

[14] N. Mittal, S. Singh, U. Singh, and R. Salgotra, "Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Modified cuckoo search optimization algorithm for wireless sensor networks", *Wireless Networks*, Vol. 27, pp. 151-174, 2021.

[15] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks", *Applied Soft Computing*, Vol. 77, pp. 366-375, 2019.

[16] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, pp. 547-566, 2021.

[17] O. R. Ahutu and H. E. Ocla, "Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks", *IEEE Access*, Vol. 8, pp. 63270-63282, 2020.

[18] Q. Shi, L. Qin, Y. Ding, B. Xie, J. Zheng, and L. Song, "Information-Aware Secure Routing in Wireless Sensor Networks", *Sensors*, Vol. 20, No. 1, pp. 165, 2020.

[19] S. S. Moghaddam, H. Taheri, and A. Karimi, "Trust based routing algorithm to improve quality of service in DSR protocol", *Wireless Personal Communications*, Vol. 109, No. 1, pp. 1-16, 2019.

[20] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure Routing Protocol based on Multi-Objective Ant-colony-optimization for wireless sensor networks", *Applied Soft Computing*, Vol. 77, pp. 366-375, 2019.

[21] P. Yarde, S. Srivastava, and K. Garg, "Adaptive immune-inspired energy-efficient and high coverage cross-layer routing protocol for wireless sensor networks", *IET Communications*, Vol. 14, No. 15, pp. 2592-2600, 2020.

[22] A. R. Basha, "Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network", *IET Wireless Sensor Systems*, Vol. 10, No. 4, pp. 166-174, 2020.