ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Secure Energy oriented Multi-Objective Optimization technique for WSN

DR. JHUM SWAIN
Associate Professor, Department of CSE, Swami Vivekananda Institute of Technology, Secunderabad, Telangana, India.

Abstract
Wireless networks consist of several low-cost nodes, mostly with narrowly limited capacities for sensing, calculation, and communication. Data aggregation is the mechanism by which sensor data is summarized and combined to minimize data transfer in the network. Since wireless sensor networks are usually used to communicate sensitive information in remote and hostile environments, sensor nodes also are susceptible to different attack types. The packet drop attack is one such attack where the compromised sensor nodes drop the whole or selective packets intentionally. Hence, wireless sensor network protocols must be designed with security in mind. This paper introduces a secure and energy oriented mechanism named secure multi-objective Lion Optimization Algorithm (SMOLOA) which takes the advantage of the Lion optimization algorithm LOA. The network is divided as clusters based on k-means clustering for energy efficiency & easy data aggregation. SMOLOA evaluates the fitness function on the basis of key parameters such as packet drop, residual node energy, linked nodal density, cluster-distance average, and average transmission delay. The optimal route is based on LOA's proposed multi-target function. Compared to current schemes, the results from simulation demonstrated considerable improvements in safe data aggregation and energy usage.

Keywords: WSN, Data aggregation, Energy oriented routing mechanism, Lion optimization algorithm, Packet drop attack, Energy consumption.

I. Introduction

Wireless sensor networks (WSN), including medical monitoring, environmental monitoring, military monitoring and many others such as the Internet of Thing (IoT), have been implemented in many respects. [1]. The most important topic for WSNs has been energy conservation. However, energy is scarce and difficult to substitute for sensor nodes. Furthermore, nodes near the base station (also called the sink) are more energy consuming compared with other nodes as the nodes transmit the data gathered from sensors away from sink [2]. Thus, collected data from other sensors cannot be moved to the sink when these sensors close to the sink fail. The whole network would then be disconnected, although most nodes still have a great deal of capacity. The main task for WSNs is therefore to increase network life by reducing the energy consumption of sensor nodes.

A network of sensors includes a significant number both within and close to the device of highly-distributed low-cost multi-sensor nodes. These small nodes are made up of sensing, data processing and component communications. There should be no absolute location for those small nodes, which means not only that the sensor network protocols and their algorithms must have the capacity to organize themselves in inaccessible places. They must also be placed at random. However the energy supply and the bandwidth of nodes are limited, the low power consumption requirements are one of the most critical restrictions of sensor nodes. These limitations along with the specific use of a number of nodes presented many obstacles to the creation and management of networks. These problems require energy sensitivity at all network stack levels. In all types of sensing applications, there are common physical and connecting layer problems, and the focus of research is therefore on system knowledge, such as the dynamic voltage scale, hardware for radio communications, low-duty problems for cycles, system service and energy intense MAC protocols [3].

Cite this article as: Dr.Jhum Swain, "Secure Energy oriented Multi-Objective Optimization technique for WSN", International Journal of Research in Advanced Computer Science Engineering, (IJRACSE), Volume 7 Issue 8, January 2022, Page 1-10.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The main objective of the network layer is to find ways to build energiesparend routes and relay sensor nodes efficiently to a plinth to increase the durability of the network.

A network of sensors enables the ability to observe and respond to events in a given environment to be sensed, processed and communication. Tens to thousands of nodes is normally composed of WSN. This collects and communicates information collaboratively to a central site [4]. Figure 1 represent the Basic architecture of sensor network.

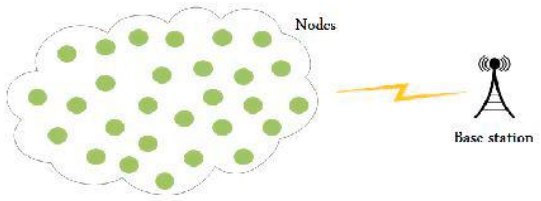

Fig. 1. Wireless sensor network

Compared with traditional networking technologies such as cost reduction, reliability, scalability, versatility, accuracy and ease-of-use, WSN technology provides numerous benefits. Sensors are being used for thousands of different applications as a result of the rapid technological advances. The areas of military, climate, health care and protection are some of their possible applications [5]." Many factors affect the nature of this network, such as: manufacturing failures, the operating environment, the topology of the sensor network, hardware's, media transmission and power consumption. These are the guidelines for protocols and algorithms designed to produce an efficient network of sensors [6-7-8].

Packet dropping attack

The transmission of data for both sensitive and non-sensitive applications can be damaged by a packet drop attack. Malicious nodes are like regular nodes in dropping attacks and dropping packets selectively [9]. The drop nodes which be randomly selected. It is very difficult and sometimes impossible to identify such attacks. A packet drop attack is a form of denial of service that attracts and selectively drops packets without being transferred. Take the scenario in Figure 1, for example. Node 1 is the source node, while Node 7 is the source node [10]. Nodes 2 to 6 are in the center. Node 5 is like the node of malice. If the source wants to send data packets, the first RREQ packets will be sent to the next nodes. The RREQ is also provided to malicious nodes which are part of the network. The source node transmits data packets after receiving the RREP from the destination. Since node 5 also forms part of the routing route, it sends and sends some data packets. The malicious nodes sound like a good node to make this form of attack is very tough to detect. The dropping of packets has a great negative effect on traditional protocol efficiency metrics. Figure 2 shows the packet drop attack.

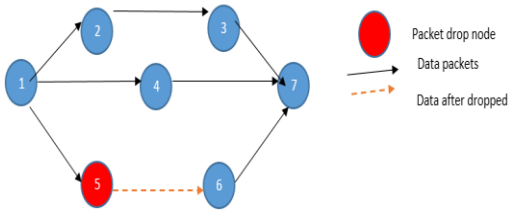

Fig2: Packet drop attack

II. Literature review

Kashif Saghar and David Kendali [11] have been able to use structured modeling to resolve the issue of block hole attacks and avoid attacks by developing the RAEED (Robust formally analyzed protocol for deployment of wireless sensor networks).

An analysis technique of a suggested Black Hole Attack is given and Black Hole Attack nodes are identified in the course the AODV routing Protocol is improved [12].

The authors of [13] have proposed a confidence model and the confidence between network nodes. The trustee is either unbelieved or trusted by a node, depending on faith. Since thruster disbelief prevents and removes black hole attackers from the road.

Manisha Rathee et al.[14] proposes QEBSR in addition to energy balance and ACO adapt to estimate the routing route for WSNs based on the security requirements and QoS requirements. In considering the packet generation rate and the packet drop rate, the

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

method has been based on an efficient confidence measurement mechanism. However, QEBSR is performing better than existing methods such as EENC and DEBR in terms of reduced delays, prolonged lifetime and data transfer through nodes.

SDARP for energy balance and security balancing ad hoc sensor networks was proposed by K. Vinoth Kumar et.al. [15]. Data gathering technology based on fuzzy was also used to collect data using a clustering model. The algorithm of data encryption and decryption reduces energy use and improves safety. The proposed method SDARP shows improved performance in increasing energy consumption, high data collection speed, less jitter, less delay and high network life in comparison with previous methods such as STEAR and FEEMCHSRP.

III. EXISTING SYSTEM

QoS aware and energy balancing secure routing (QEBSR) algorithm using ant colony optimization (ACO) [16]:

This QEBSR lists the major contributions as follows.

1) Simultaneous attention was paid to critical WSN concerns (balancing energy use, quotas and safety requirements)

2) For data generation and data communication to the sink node an event-based scenario is assumed and a source node selection framework is given for this.

3) Improved heuristics for the calculation of sensor node delay and trust, resulting in improved network efficiency, are proposed in this section.

A number of bio-inspired metaheuristic techniques, including Genetic algorithms (GA), ACO, PSO, bee optimization and Cuckoo Search (CS), to name a few, have been developed. Although these two methods can be used in WSN routing, ACO is better suited to and adaptable for the WSN routing problem.

Routing in WSNs is a discreet optimization problem and the previous continuous optimization techniques have, with the exception of ACO and GA, been mostly proposed. These methods must also be discretized if they are to be used for routing.

IV. Proposed Framework

In this paper, we introduces a secure and energy aware routing algorithm named secure multi-objective Lion Optimization Algorithm (SMOLOA) which takes the advantage of the Lion optimization algorithm LOA. The network is divided as clusters based on k-means clustering for energy efficiency & easy data aggregation. Based on important parameters such as packet drop, elected residual energy node, connected node density, average cluster distance, mean time and traffic rate, SMOLOA evaluates fitness function. Based on the proposed multi-objective feature of LOA, the optimal routing is defined.

Proposed algorithm overview

The network is divided into clusters based on k-means of energy efficiency clustering and simple data aggregation during the proposed work. SMOLOA assesses the fitness function on average cluster distances and average transmission & traffic speeds based upon important parameters including packet drop value, residual energy in the node chosen, associated node densities. Based on the proposed multi-objective feature of LOA, the optimal routing is defined.

K-means algorithm

K-means-algorithm mainly depends on Euclid distances, and the selection of the cluster head depends on the residual node capacity. Therefore, from all nodes about the node id, location and residual energy, the central node collects and stores data. The clustering algorithm starts after it's obtained from all nodes (k-mean).

Algorithm

- Take "k" number of centroids at random locations at first for the number of clusters of 'k.'
- Calculate the distance from each Euclidean node to all centers and allocate the center closest to them. The first clusters are created with this "k"

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Suppose there are n nodes are given such that each one of them belongs to $\boldsymbol{R_d}$. The problem with the discovery of the minimal variance classification of k nodes is that the k centroids can be found as $\{\boldsymbol{m_j}\}^{\boldsymbol{k}}$ in $\boldsymbol{R_d}$ such that,

$$\left(\frac{\mathbf{1}}{\boldsymbol{n}}\right) \boldsymbol{x} \sum \left(\boldsymbol{mid}\, \boldsymbol{d^2}\left(\boldsymbol{X_i}, \boldsymbol{m_j}\right)\right), \quad \boldsymbol{for\ i = 1\ to\ n}$$

Eq (1)

Where $\boldsymbol{d(X_i, m_j)}$ denotes the Euclidean distance between $\boldsymbol{X_i}$ and m_j.

1. Recalculate the centroid positions in each cluster and verify the location changes from the previous.

2. If the location of a centroid changes then go to STEP 2 otherwise the clusters will be completed and the operation of the cluster will end.

As each node takes part in clustering decisions, the clustering method is distributed. Each node here receives information required to cluster all other nodes. The algorithm clusters all nodes and selects the cluster head based on this information.

Finding secure optimal routing path using multi-objective LOA

The selection of the optimal routing path with multi-target LOA is discussed in this section. The SMOLOA algorithm proposed determines the suitable forwarder nodes based on the multi-target parameters. With the proposed multi-target fitness, the fitness of each node is determined. For fitness assessment a number of goals are considered, including packet drop value, elected node residual energy, connection node density, mean cluster distance, average transmission & traffic delay.

Multi-objective Fitness function

This article provides the role of optimizing fitness based on various goals: average dropping time and transport rate, residual node energy and connected node density. The fitness function is per node the highest value to pick the node as the best node. The following is briefly clarified for all these parameters:

Packet drop value (PDV): This metric is the number of packets dropped during transmission of data by the sensor node. If the node is to be selected as the perfect forwarder, the packet drop value should be minimum.

Residual energy of elected Node (RE): Present energy node left. Residual energy is one of the main considerations. Furthermore, the residual power of a node is its transmission.

Node density (ND): The number of nodes in a cluster is the node density. The ND is also growing with the number of cluster members. In addition, node density would be more the overhead network interaction.

Average cluster distance (ACD): The distance from other nodes in their cluster is measured first, then the sum of the distances is calculated. Take S as a group of cluster nodes such as S {S1, S2 ...SN }. Let I and j be two nodes of S, . (i, j) ∈ S, and distance can be calculated as:

$$\boldsymbol{Dist} = \sqrt{(\boldsymbol{i_x} - \boldsymbol{j_x})^2 + \left(\boldsymbol{i_y} - \boldsymbol{j_y}\right)^2} \quad \text{Eq (2)}$$

Then the mean cluster distance value will be for node I

$$\boldsymbol{ACD} = \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{Dist}\,(\boldsymbol{i}, \boldsymbol{S_i}) \quad \text{Eq (3)}$$

Average delay in transmission (ADT): The time required to pass all packet bits to the wire is the time required to move them. The length of the packet and rate of the bit are determined. This means the packet size-to-link transmission rate ratio. ADT should be minimum for timely data transmission.

$$\boldsymbol{ADT} = \frac{\boldsymbol{Packet_{size}}}{\boldsymbol{link\ transmitting\ rate}} \quad \text{Eq (4)}$$

Traffic rate (TR): The last objective parameter is traffic density for the derivation of the fitness function. For improved communication, the amount of traffic has the minimum value. The following is the volume of traffic

$$\boldsymbol{TR} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \frac{\boldsymbol{F_{(i)}(t)}}{\boldsymbol{max}\,|\boldsymbol{F_{(i)}(t)}|} \quad \text{Eq (5)}$$

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Where, the term $\boldsymbol{F_{(i)}(t)}$ indicates the flow rate of the ith node and $\mathbf{max}\ \boldsymbol{F_{(i)}(t)}$ indicates the maximum flow rate.

The fitness function is determined by combining all these factors:

$$\boldsymbol{fitness\ (f) = \frac{PDV*RE}{ND*ACD*ATD*TR}} \qquad \text{Eq (6)}$$

Construction of the proposed SMOLOA algorithm

The SMOLOA algorithm proposed determines the perfect path. The current LOA algorithm uses three lions to solve the optimisation problem. He's a lion, a lion, a nomad lion. Selecting optimal sensor nodes from the different sensor nodes is the issue of optimization. Three lions used in the proposed SMOLOA reflect the sensor nodes. The process of optimization ensures that nomadic nodes are eliminated from the routing zone. Figure 3 represent the block diagram of proposed system.

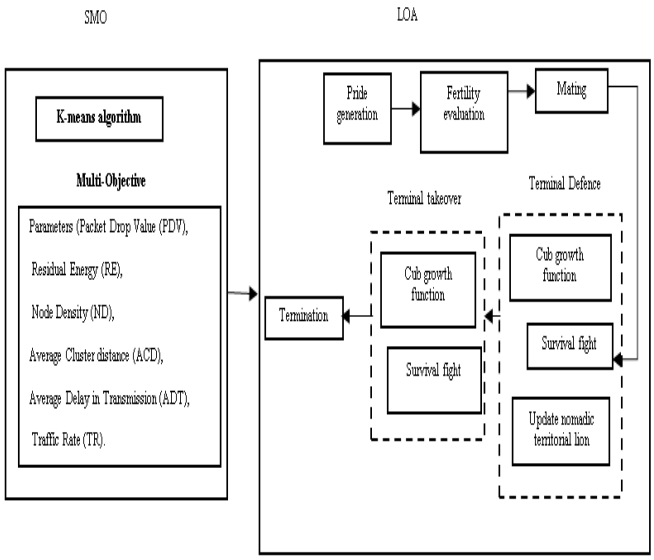

Fig3: Block diagram of Proposed SMOLOA

the SMOLOA algorithm proposed ensures the following conditions,

- The male lion is fit to optimize the issue more effectively.
- The SMOLOA proposal provides a multi-objective fitness function for the ideal sensor node from existing sensor nodes.
- There is a trajectory between the sensor nodes and the ideal cluster.

Different steps are explained in the proposed SMOLOA algorithm,

Step 1: Pride generation: The first phase in the SMOLOA algorithm is the production of pride. The cluster nodes are the pride of the cluster's head node. The term $\boldsymbol{Y^U}$ indicates the male lion, the term $\boldsymbol{Y^V}$ indicates the female lion, and the term $\boldsymbol{Y^{W1}}$ indicates the nomadic lions in the WSN. $\boldsymbol{Y^{W1}}$And $\boldsymbol{Y^{W2}}$ are the two nomadic lions, in which $\boldsymbol{Y^{W1}}$ is initialized in pride generation and $\boldsymbol{Y^{W2}}$ is initialized in territorial defense. The various elements of the male lion $\boldsymbol{Y^U}$, female lion $\boldsymbol{Y^V}$, and nomadic lion $\boldsymbol{Y^W}$ are expressed as follows,

$$\boldsymbol{Y^U(p) = \{Y^U(1), Y^U(2) \dots\dots\dots\dots\dots Y^U(p)\};\quad p = 1, 2, 3, \dots\dots P}$$

$$\boldsymbol{Y^V(p) = \{Y^V(1), Y^V(2) \dots\dots\dots\dots\dots Y^V(p)\};\quad p = 1, 2, 3, \dots\dots P}$$

$$\boldsymbol{Y^W(p) = \{Y^W(1), Y^W(2) \dots\dots\dots\dots\dots Y^W(p)\};\quad p = 1, 2, 3, \dots\dots P}$$

Where, the population size is indicated by P.

Step 2: Multi-objective test proposed Fitness

Every node fitness via Equation 6 is established with the proposed SMOLOA algorithm. For node selection between sensor nodes, a threshold is established. The optimisation method calculates the fitness of each lion as a problem of maximisation.

Step 3: Fertility evaluation

The next step is the assessment of fertility in the proposed SMOLOA algorithm. It is now settled on the fertility between the male lion and the female lion. The proposed SMOLOA algorithm prevents the convergence of the local Optima algorithm. The evaluation of lion fertility depends on the wellbeing of each lion. In the assessment of fertility: the modified

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

lion of the girl, health of comparison, ratings, sterility rate, number of females updating and number of females are considered. The algorithm selects a f_{thres} reference fitness for the assessment process. If the fitness of the lion knots is greater than the fitness of the comparison, it changes the laggardness rate. Failure to do this would re-establish the health of the male lion and the laggard rates. The female lion's fertility assessment is given as,

$$Y_q^V = \begin{Bmatrix} Y_P^V; & if\ q = p \\ Y_q^V; & otherwise \end{Bmatrix}$$

$$Y_p^V = min\left[Y_q^{max},\ max\ (Y_P^{min}, \nabla p)\right] \quad \text{Eq (7)}$$

Where, the terms Y_q^V , and Y_p^V indicates the qth and the pth vector elements of the female lion Y^V. The term p indicates the random integer between the values 0 to P. The term ∇p indicates the female lion update function. The formulation of the lion update function ∇p is defined in the following equation.

$$\nabla p = \left[Y_P^V(t) + (0.1a_2 - 0.05)(Y_P^U(t) - a1YPVt)\right] \quad \text{Eq (8)}$$

Where, a_1 and a_2 ranges between 0 and 1.

Step 4: Mating of the nodes

The next move is to combine the algorithm proposed. The method involves crossover and transmutation operators to effectively generate the lion's cubes. The pairing is performed accordingly,

$$Y^{(cub)}(r) = L_r\, o\, Y^U + L1_r\, o\, Y^V \quad \text{Eq (9)}$$

◦ is a result of Hadamard and the word "Lr" means mask length crossover (F). The set value ranges between one and four values. The mating of the male lion and the female lion efficiently produces four cub lions $Y^K(r)$.

Step 5: Cub growth formation

The cub growth formation depends on the mutation of the both the male cub Y^{U_cub} and the female cub Y^{V_cub}. The mutation rate for cubic growth is below 0.2. The mutated cube of man and female replaces the male cub and female cub if their health value is higher.

Step 6: Territorial defence

For the proposed SMOLOA algorithm the territorial defense relies on the Nomad coalition, survival, pride updates and updates to the nomad. The Nomad coalition between the two nomad lions Y^{W1} and the Y^{W2} results in one of the winning nomad lion Y^{WIN_W} . The survival fight between the lions depends on the winning nomad lion Y^{WIN_W} . The following equations indicate the conditions for the nomad Lion to win the survival fight:

$$fitness\left(Y^{WIN\_W}\right) > fitness(Y^U)$$

$$fitness\left(Y^{WIN\_W}\right) > fitness(Y^{U\_cub})$$

$$fitness\left(Y^{WIN\_W}\right) > fitness(Y^{V\_cub})$$

The pride update is done when the male lion Y^U is defeated by the winning nomad lion Y^{WIN_W}.

Step 7: Territorial takeover

When wellbeing is met, territory is taken by the substitution of old lions with cubic lions. The male lion shall be replaced by the following criteria:

$$Y^U = \begin{Bmatrix} Y^{U\_cub}; & if\ \left(fitness(Y^U) < fitness(Y^{U\_cub})\right) \\ Y^U; & else \end{Bmatrix}$$

Eq (9)

The substitution of the female lion is performed on the basis of:

$$Y^V = \begin{Bmatrix} Y^{V\_cub}; & if\ \left(fitness(Y^V) < fitness(Y^{V\_cub})\right) \\ Y^V; & else \end{Bmatrix}$$

Eq (10)

Step 8: Termination

This is the last phase in the method of optimisation. When the termination condition is not met, the algorithm is repeated from step 3. The algorithm

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

terminates until the T_{max} iteration is reached as far as possible.

V. Results and Discussion

Experimental setup

The scenario below is used to assess the approach proposed and compare with the methods already in place. The sensor nodes are randomly deployed and the sensor nodes are spread across the network area within an area of 1000x1000m. The location of the node is still. The size of the network varies between 50 and 250. The sensor nodes have an initial energy of 100joules. CBR communication is allowed and the sensor nodes will send the packet at the constant bit rate speed. The size of the database is 1024bytes. The network has been simulated for 100ms.

Table1: Simulation Parameter table

PARAMETER	VALUE
Application traffic	CBR
Transmission rate	1024 bytes/ 0.5ms
Radio range	250m
Packet length	1024 bytes
Routing Protocol	AODV
Simulation time	100s
Number of nodes	50, 100, 150, 200, 250
Area	1000 x1000
Transmission Protocol	UDP
Initial Energy	100j

Fig4: End to end delay

The above results figure 4 display the experimental results of the implementation of the methods in 50 to 250 different Network Sizes, both current and proposed. Time and time a data packet takes to the destination shall be determined by the delay between the end to end. Improper selection of the forwarder node and a high hop count affect the data packet delay at the end. In the proposed way, the transmission of data is achieved using the proposed multipurpose fitness function, energy-efficient transmission nodes. Therefore, there is relatively less delay in the proposed process than in the previous ones.

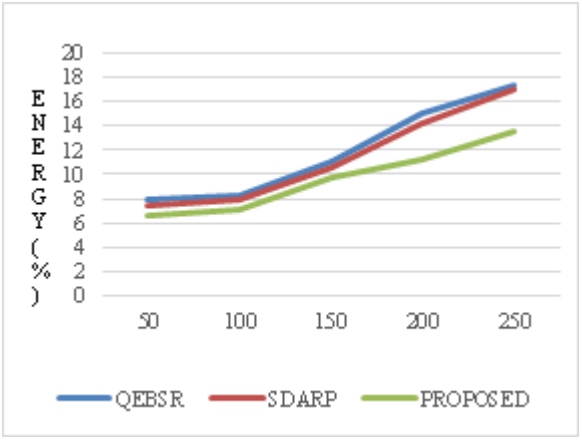

Fig5: Energy consumption

Energy is the sensor network's critical parameter. The initial energy is provided for each node of the network. The first energy was 100joules in our simulation. For network operations, the sensor nodes consume resources. In order to last longer, energy consumption should be optimized. The choice of the energy-efficient routing route through the proposed fitness calculation multi-objective algorithm optimizes the energy use of the sensor node and improves network life. Therefore, energy conservation was not taken into account by the current approaches in a way that the energy consumption was comparatively superior. The proposed method's average energy consumption rate was 13j for 250 node networks with a maximum of 17j in previous methods. Figure 5 represent the graphical view of energy consumption.

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

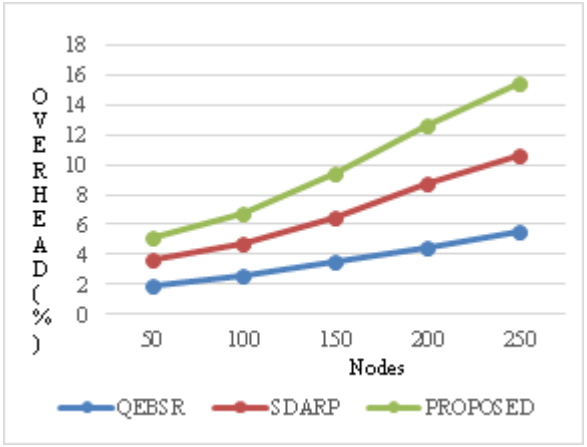

Fig6: Overhead

The overhead parameter is associated with the overhead often occurring in the network by the method/ algorithm implemented. The algorithm/method needs resources for completing the given task related to the sum of additional control packages. The route loss because of the wrong selection of the forwarder node calls for transmission completion. To save the undesirable energy consumption, this should be avoided. The multi-objective fitness estimate algorithm was checked in the approach proposed, selecting energy-efficient paths. The successful network clustering also enhances the aggregation of data. In the proposed system, therefore, the overhead was regulated when the current methods failed. Figure 6 shows the graphical representation of overhead.

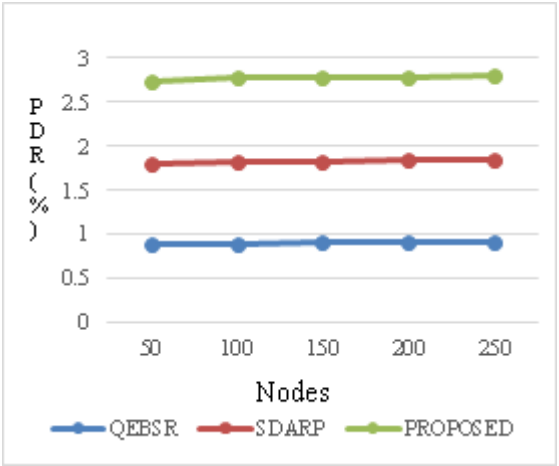

Fig7: Packet delivery ratio

A Packet Diffusion Ration, PDR, determines the ratio of the total number of packets sent to the destination node from the source node to the number of packets sent. The failure of the route and congestion are the major factors affecting the PDR rate. The successful data aggregation by cluster heads and energy-efficient path selection by means of the multi-target fitness feature ensure that data packets are transmitted smoothly to their own destination through energy-efficient pathways. Therefore, in the system suggested, the PDR of the current methods was as low as 91% while the PDR was as high as 95%. Figure 7 shows the graphical view of packet delivery ratio.

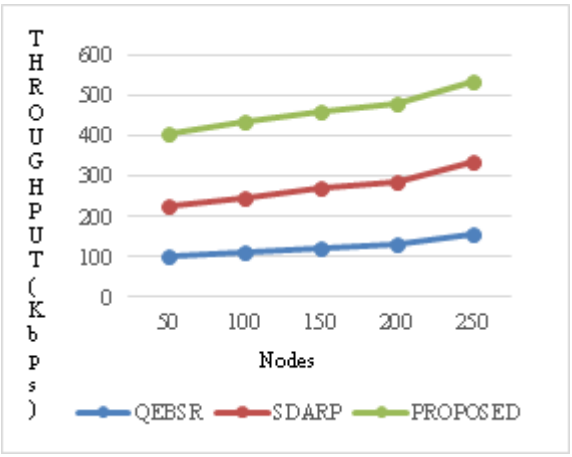

Fig8: Throughput

The Throughput refers to the amount of data that can be transmitted in a certain time from one sensor to the other. The efficient rate of transmission of the network is described throughput. In the network performance, the presence of congestion in the routing path. The effective path selection strategy of the MOA and the data aggregation of the proposed algorithm maintains high fitness efficiency. The highest throughput rate achieved in our execution was 198 kbps, compared to 156 kbps for existing methods. Figure 8 represents the graphical view of throughput.

Conclusion

This work implemented a WSN routing mechanism which is safe & energy conscious. In this paper, proposes a Lion optimizing algorithm based on the SMOLOA algorithm. The work proposed used the multi-target fitness function to pick the best sensor

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

nodes for the routing. The SMOLOA proposal takes various factors into consideration: packet drop value, elected residual energy, related node density, average cluster distance, average fitness transmission and traffic delays. The proposed model is simulated by a difference in population size and WSN nodes. The comparative study of the current models, including QEBSR and SDARP, is carried out. Even for dense sensor networks, the proposed algorithm has increased standardized grid energy.

References:

[1]. Jaladi, Aarti Rao, Karishma Khithani, Pankaja Pawar, Kiran Malvi, and Gauri Sahoo. "Environmental monitoring using wireless sensor networks (WSN) based on IOT." Int. Res. J. Eng. Technol 4, no. 1 (2017): 1371-1378.

[2]. Amin, Ruhul, SK Hafizul Islam, G. P. Biswas, and Mohammad S. Obaidat. "A robust mutual authentication protocol for WSN with multiple base-stations." Ad Hoc Networks 75 (2018): 1-18.

[3]. Yu, Qingyao, Guangming Li, Xiaojie Hang, and Kun Fu. "An energy efficient MAC protocol for wireless passive sensor networks." Future Internet 9, no. 2 (2017): 14.

[4] Filippini, Massimo, and Lester C. Hunt. (2011) "Energy demand and energy efficiency in the OECD countries: a stochastic demand frontier approach." *Energy Journal***32** (**2**): 59–80.

[5] Rawat, P., Singh, K. D., Chaouchi, H., and Bonnin, J. M.(2014)"Wireless sensor networks: a survey on recent developments and potential synergies." The Journal of supercomputing 68(1): 1–48.

[6] Kalkha, H., Satori, H., and Satori, K.(2016) "Performance Evaluation of AODV and LEACH Routing Protocol." Advances in Information Technology: Theory and Application.

[7] Kalkha, H., Satori, H., and Satori, K. (2017)"A Dynamic Clustering Approach for Maximizing Scalability in Wireless Sensor Network." Transactions on Machine Learning and Artificial Intelligence

[8] Akyildiz, I. F., Su, W., S Sankarasubramaniam, Y., and Cayirci, E. (2002) "Wireless sensor networks: a survey." Computer networks, 38(4):393–422.

[9] Rmayti, Mohammad, Rida Khatoun, Youcef Begriche, Lyes Khoukhi, and Dominique Gaiti. "A stochastic approach for packet dropping attacks detection in mobile Ad hoc networks." *Computer Networks* 121 (2017): 53-64.

[10] Vanitha, K., and AMJ Zubair Rahaman. "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol." *Cluster Computing* 22, no. 6 (2019): 13453-13461.

[11] Saghar, K., Kendall, D., and Bouridane, A. (2014, January) "Application of formal modeling to detect black hole attacks in wireless sensornetwork routing protocols."InApplied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference. IEEE.191–194.

[12] Wazid, M., Katal, A., Sachan, R. S., Goudar, R. H., and Singh, D. P.(2013, April)."Detection and prevention mechanism for blackholeattack in wireless sensor network."InCommunications and Signal Processing (ICCSP), 2013 International Conference.IEEE.576–581.

[13] Gondwal, N., and Diwaker, C.(2013) "Detecting blackhole attack in WSN by check agent using multiple base stations."AmericanInternational Journal ofResearch in Science, Technology, Engineering & Mathematics,3(2), 149–152.

[14] Rathee, Manisha, Sushil Kumar, Amir H. Gandomi, Kumar Dilip, Balamurugan Balusamy, and Rizwan Patan. "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks." *IEEE Transactions on Engineering Management* 68, no. 1 (2019): 170-182.

[15] Kumar, K. Vinoth, T. Jayasankar, V. Eswaramoorthy, and V. Nivedhitha. "SDARP: Security based Data Aware Routing Protocol for ad

ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

hoc sensor networks." *International Journal of Intelligent Networks* 1 (2020): 36-42.

[16] Rathee, Manisha, Sushil Kumar, Amir H. Gandomi, Kumar Dilip, Balamurugan Balusamy, and Rizwan Patan. "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks." *IEEE Transactions on Engineering Management* 68, no. 1 (2019): 170-182.