



# Improvement of Node Efficiency in the Radiation Affected Area of WSN

Asha K.R.<sup>1</sup>✉, Supriya M.C.<sup>2</sup>

<sup>1</sup>Research Scholar, SSAHE, Agalakote, Tumakuru, Karnataka, India - 572105

<sup>2</sup>Associate Professor, Dept. of Master of Computer Application, SSIT, Karnataka, India - 572105

✉ ashamanjunatha@yahoo.com

---

## Abstract

*Advancement of technologies in Wireless Sensor Network, cleverly performs effective sensing, monitoring and data transmission in inspired ways. Highly monitored area attacked by nuclear attackers or nodes hacked by hackers leads to different issues. Nuclear radiation accidents cause changes in behavior of nodes and nodes consume more energy and data loss will take place. In situation like this, monitoring of node behavior, energy consumption and data transfer process is essential. However, intrusion detection is used to detect unknown attacks and it is suitable for WSNs environment. The proposed system could monitor the influence of such attacks. In this paper, the capability to produce a desirable result to improve the nodes efficiency in terms of less consumption of energy, less packet loss and secure transformation of data are proposed. The method identifies the behavior of the nodes through intrusion detection agent, with the energy efficient clustering. The main objectives are to improve the efficiency of the node and achieve efficient security for the monitoring area by WSNs.*

**Keywords:** *Intrusion detections System, Wireless sensor Networks.*

---

## 1. INTRODUCTION

Real time applications of Wireless Sensor Network influence people to use advanced technologies in essential environments like military vigilance, war field, forest monitoring and security monitoring for cities in a better way [1,2]. A wireless sensor networks build with sensors, global positioning system, radio transceiver, power source, memory and processor. These resources are limited in capabilities [3]. Sensor nodes placed in the environment will senses the information and send to sink. Highly monitored area monitored by WSNs, attacked by radiation to disturb the communication and unknown attack to send malicious data. Identifying status or behavior of sensor nodes and network communication is very crucial. In that situation energy of the sensor nodes are

depleted, nodes fail to communicate with the neighbor nodes, loss of packet, failed to send the collected information to the base station and due to malicious activity wrong information can reach the base station. That is, nodes behave like transfaulty [4, 5]. In that situation changing energy source or continuous supply of energy is not possible. So energy efficiency should be followed on each node. Utilize available energy in an efficient way to improve its lifetime will reflect the life time of the entire network.

Securing the WSN by using cryptographically is not enough. To handle the radiation attacks or unknown attack in the specified area, efficient mechanisms are needed to improve the node efficiency by considering less utilization of energy, less data loss and more secured transformation of data. To get efficacy for the improvement of node efficiency in the radiation affected area of WSN will be achieved by identifying the behaviors of node during radiation attack through intrusion detection system. An Intrusion detection systems can be used to identify behavior of nodes inside the WSNs [6, 7]. Cluster based Wireless Sensor Network can decrease the load of each nodes and energy consumption of all the nodes [8-10].

Intrusion detections System is used for inscription of various types of security attacks in WSNs. An IDS is used for intrusion detection and are able to detect attacks but cannot prevent or respond. In order to identify the attack it uses three methodologies. Misused based, Anomaly based and Specification based detection. Misused based methods identify the behavior by comparing with known patterns. In Anomaly based detection normal behavior of nodes are observed. If any changes in normal behavior are consider to be abnormal behavior due to attacks by considering the established automated training examples. In specification based detection any changes in behavior of the nodes is identified by their deviation in the values due to different attacks and is compares with the specific constraints.

Here it is consider efficacy from IDS to improve node efficiency in radiation affected area of clustered based WSN. We proposed a co-operative, distributive and decentralized Intrusion detection system with energy efficient clustering and data reduction mechanisms. Co-operative nature in cluster based IDS are distributed in nature, here every node monitors its neighbor's activities and operations with respect to the malicious activity. In decentralized nature every node gives information to cluster head about malicious activity if it is found within the cluster. To secure and efficiently monitoring, keep tracking

energy consumption and data collections of nodes is considered for identifying behavior and traffic monitoring during radiation attack. Intrusion detection system agent is installed in each and every sensor nodes in WSNs. It will identify the behavior of the sensor nodes in WSNs, when an area is affected by radiation and if nodes contain error data then alert message is sent to the base station through cluster head. By considering the cluster, data reduction and data aggregation saves the each nodes energy in effective way.

Krontiris Ioannis et al. [11] proposed a distributed Intrusion detection system for Wireless sensor networks by considering localized information of node and observing the neighbor nodes for black hole and selective forwarding attacks. They are focused on secure routing to send the information to the sink. But they are not focused on authentication to the secure information and save energy of nodes in the WSNs. A. da Silva et al. [12] specifies that, for detecting intrusion decentralized approach will be used. Intrusion detectors were distributed in one-hop distance in entire network. In distributed manner information will be collected and processed. Authors claimed that their approach is robust and scalable than centralized approach. I. Krontiris et al. [13], proposed a solution in co-operative way. In WSNs the nodes were deployed with local detector modules. In a distributed way, identify the intruder in WSNs. whenever intrusion is suspected, detector modules is triggers. Authors provide suitable conditions and algorithm for identifying an attacker with respect to the general threat.

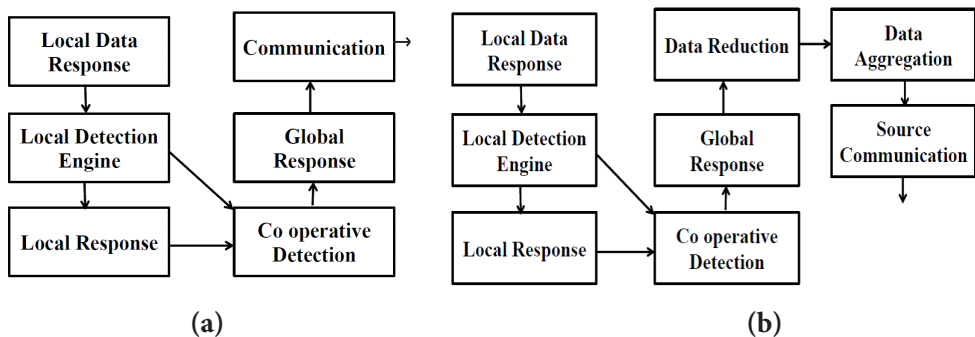
Rest of the paper is organized such that: Section II has discussed about the proposed work Section III, provides result from simulation of the proposed work and finally Section IV reveals conclusion and future works.

## **2. METHODOLOGY**

Radiological attack will radiate the energy in wave's pattern, which will affect the network communication and cause node outage problem. Services of WSN's components will be stopped. Nodes will exhibit the transfaulty behavior. Nodes sense the information properly but are unable to communicate with neighboring nodes, energy of sensor nodes is drained and reduces the life time of network. But this problem is temporary because in affected nodes the effect of radiation is decreases after some duration then the communication can occur between the sensor nodes. But delay in packet sending, loss of packets and consumption of more energy is taken with in the nodes.

In this proposed work, it will be consider Wireless sensor network monitors a specified area which is attacked by radiation along with malicious activity and distributive, co-operative, decentralized IDS will be considering in the network. Figure-1(a) shows the IDS agent running on the member nodes of a cluster. Figure-1(b) shows the IDS agent running on the cluster head.

To make the method simple and efficient, each and every node in a cluster monitors the activity occurred in the monitoring area. IDS in each node will do its work as shown in the Figure-1(a) then information about the activity will be given to the cluster head. In cluster head, reduction of sensed data will be taking place by the data reduction module and aggregation of varied data by considering data aggregation method. Activities will be shown in the Figure-1(b). In our method, we avoid unnecessary computation in cluster to select the different roles of the nodes. Each node is distributed with IDS, cooperative with each other and with cluster head and each nodes report the information to the cluster head in decentralized way. That is, each node is independent to inform about malicious activity. This leads better monitoring of radiation affected area with malicious activity.



**Figure-1** IDS running in a member node and cluster head (a) IDS running on the member nodes of a cluster (b) IDS running on the cluster head

IDS agent placed in each node in WSNs to detect attacks by observing the node's transfaultry behavior of affected sensor nodes. Due to transfaultry behavior, affected node consumes more energy. Node is unable to communicate with the neighbor. IDS agent of the affected node identifies higher consumption of energy then alarm message is generated to intimate its neighbor. IDS agent update the firmware and key of the node.

To work in the radiation prone environment it will be consider as

communication mode transfer mechanism of our previous work to continue the communication between nodes which shows transfaulty behavior due to radiation attack. Communication mode of node is changing from RF mode to acoustic mode to work in radiation affected environment. Acoustic communication mode is not affected by radiation.

In WSNs, consider three tracks. Nodes fall in the respective track depending upon the latitude, longitude and neighborhood information about the nodes. Inside the track unequal number of clusters is created by considering each nodes information and track details of neighbors. For transferring the sensed information from nodes to the base station cluster head will be selected to save energy of each node. For the selection of head node, the node having highest remaining energy, highest node coverage and lowest mobility is considered for selection of cluster head. By applying this mechanism, we can avoid more consumption of energy in the routing process and minimizes work load of members in cluster.

Along with the cluster mechanism, the author has used reduction technique of previous work to reduce the continuous transaction of sensed data to base station. By that we can find less energy utilization in data routing process. Current Sensed data is compared with the previous round data to find the difference. If the difference value is more than threshold value 10 then this indicates that change in environment due to radiation. Next finding how much difference will occur between the current data and previous data are identified. If the difference is greater than the data threshold value then it is to be considered has deviated member. Threshold value to identify data deviation is taken has 10. To find out maximum changes in the environment, we are going to find out deviation ratio.by considering total number of deviated member with respect to total number of member in the cluster. After finding deviation percentage, it is compare with member threshold 50. If it is greater than 50 then in that situation there is needs to send data for data aggregation queue. In this way we find route with less consume energy to reach base station.

Distance between the neighbor nodes is calculated by:

$$\text{distance [inn, jnn]} = \text{sqrt } (((x2-x1) ^2) + ((y2-y1) ^2))) \quad (1)$$

Each node broadcasting its energy detail  $egy[i]$  to its neighbor and waits for getting energy details from its neighbor. Energy of each node is found out by calculating remaining energy of each node in the process.

At the current instance of time the amount of energy left out in a sensor node is called Remaining energy and is calculated by:

$$\text{regy}[i] = \text{regy}[i] - (\text{dist}[i, \text{nei}[i, j]] * \text{egy\_consumption}) \quad (2)$$

and average remaining energy is calculated by:

$$\text{avg\_rem\_egy} = \text{total\_of\_regy} / \text{tno\_nodes}. \quad (3)$$

Energy consumption is the energy utilized by the sensor node after the time 't' and it is calculated by:

$$\text{egy\_consumption} = (\text{data\_pk\_t} * k1) + (\text{data\_pk-r} * k2) \quad (4)$$

After sharing the energy between the nodes in cluster of respective track, after that cluster head node will be selected by considering the node which is having greater remaining energy and maximum node coverage and less mobility. Node satisfying all these will be selected as head node with respect to each cluster present in each track or zone. Other nodes withdraw itself from the competition process.

Ratio of average distance with its neighbor's gives the node coverage and it is calculated by:

$$\text{nd\_cov}(x) = \frac{\sum_1^{ng\_nd(x)} ((x, y) \in E / y \in ng\_nd(x))}{|ng\_nd(x)|} \quad (5)$$

Node Mobility of the sensor node, mb\_nd (n) of the node is found out by:

$$\text{mb\_nd}(n) = 1/T \sqrt{\sum_{t=1} (x_{co_t} - x_{co_{t-1}})^2 + (y_{co_t} - y_{co_{t-1}})^2} \quad (6)$$

Selected head nodes will send advertisement to its each cluster's node, whenever area monitored by WSN is affected by radiation. Some the nodes are affected by radiation and behaves like transfaulty, in that situation nodes energy consumption is more. Suppose, IDS agent of the node identifies higher consumption of energy then IDS agent of that particular node generates alarm message to intimate its neighbor. Head node verifies alarm from the IDS agent of the respective node, if abnormal activity is found on that particular member. Head node initiate data balancing process of all the affected nodes then IDS agent update the firmware and key of the node. Along with that Head Computed

Average data of member nodes present in its control area. To see the variation in data collected by the sensor nodes due to radiation affection and also to avoid the unnecessary transferring of data to the base station, if there is no changes in the environment. First, it calculates the average data of the cluster members by using the equation (7)

Cluster head calculates average of the data collected by cluster members,  $avg\_dt\_cul(c)$  by:

$$avg\_dt\_cul(c) = \frac{\sum_{i=1}^{M(c)} dt\_node(i)}{|tl\_mem\_cul(c)|} \quad (7)$$

After finding the average data it checks for variation in that environment by finding difference between the current data and previous data of the cluster by:

$$difference = avg\_dt\_cul - dt [nn] \quad (8)$$

Then difference of data is compared with data threshold value to find out how much data members are deviated by greater than data threshold value 10. Again percentage of deviated members is calculated by:

$$dv\_per\_clu = (dv\_meb\_clu(C) / |tl\_mem\_cul(c)|) * 100 \quad (9)$$

This deviated percentage is compared with the member threshold value 50 to take the decision to sending aggregated data of particular cluster in track to base station. When deviated percentage is greater than member threshold then data send to base station otherwise there is no need to send.

The proposed method with IDS agent associated with more computations to identify behavior of nodes, network communication, and energy of sensor nodes to enhance the activity time of network during radiation attack with more accuracy. Also, here we are considering comparison of proposed method with IDS and without IDS, to know how efficiently the proposed method with IDS will work. As a result we will get the better result.

The performance of our proposed method depends on number of various metrics. This plays vital role in analytical examination of our method. Some of the essential criterion considered to study the performance of our method in simulation study.

Packet delivery ratio is described as the ratio of data packets received by the destinations to those packets generated by the sources is calculated by:

$$\text{pkt\_dely\_ratio} = \text{recd\_pkt\_size} / \text{sou\_pkt\_size} \quad (10)$$

Packet Drop (Loss) Ratio, Packet loss appears due to, some of the data packets fail to reach their targeted node in a network and is given by:

$$\text{pkt\_drop\_ratio} = \text{pkt\_actly\_frd} / \text{pkt\_tobe\_frd} \quad (11)$$

Throughput, defined as the total number of packets reached over the total simulation time. thr-put can be calculated by:

$$\text{thr\_put} = \text{tot\_no\_bits} / \text{tot\_sim\_time} \quad (12)$$

### 3. SIMULATION ANALYSIS

In this research paper proposed method is tested by simulating wireless sensor network by using NS2 version 2.35 with parameters which is mentioned in Table-1. AWK scripting language is used to write an algorithm to perform radiation attack, broadcasting energy details between the nodes, creation of track, and cluster, packet drop, energy, path, data reduction and send the aggregated data to base station by finding abnormal activities within the network. AWK script to extract the needed statistical data of trace file. The simulation work of proposed method has been checked for 50, 100, 150 and 200 nodes deployed in the 3000×2500 simulation area along with the IDS agent included in all the nodes. Here we consider proposed method with IDS and without IDS and with 10, 21, 22, 22 radiation affected nodes in 50, 100, 150 and 200 respectively. To identify the data and remaining energy in the radiation affected node with IDS and without IDS agent in our proposed method concerned to the 200, 150, 100 and 50 nodes. To know about transfaulty behavior of node, by considering variation in data and remaining energy in the affected node, we observe lot difference in the values.

Communication between nodes can be achieved using UDP communication protocol and CBR traffic model to handle the traffic in wireless sensor network. To get the radio waves using two-ray ground, Omni directional antenna is used to collect the signal from each node. Our algorithms for improvement of node efficiency in the radiation affected area are achieved in the application layer of wireless sensor network.

The proposed method works better to get efficacy for the improvement of node efficiency in the radiation affected area with malicious activity in WSNs. Assesses by considers, lessen the energy consumption in each node in better way for improvement of life time activity of the entire network by installing IDS agent in each node in the network. In the simulation outputs, we can observe better result in proposed method with IDS concerned to packet delivery ratio, packet loss, and throughput, comparison of energy and data of nodes than the method without the IDS agent in the nodes. The particular metrics are used in our proposed method to find out, comparison of remaining energy and data variation in node wise with and without IDS, comparison of average remaining energy ,average data variation ,and energy consumption in nodes 50,100,150 and 200 with and without IDS, data collected in 50,100,150 and 200 nodes with and without IDS, packet delivery ratio, packet drop, and through put in 200 nodes with and without IDS, and comparison of remaining energy and data in nodes with and without IDS in radiation affected nodes out of 200 ,150,100,50 nodes.

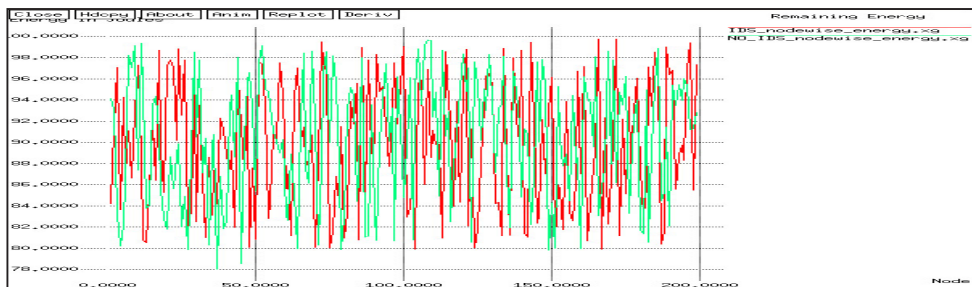
**Table-1** Parameters used for the simulation purpose

Channel	Wireless
Simulation Time	50 ms
Nodes	50,100,150,200
Topography area	3000x2500 m
Connection	UDP
Source traffic	CBR
Routing Protocol	DSR
MAC type	802_11
Transmission range	250m
Network Interface	WirelessPH
Initial energy	100 Joules
Energy consumption	0.0001 J/m
Node mobility	random
Area affected by radiation	1000-2000 X-axis 750-1500 y-axis
Range of sensing	30 m
RF mode communication range	90 m
Acoustic mode Communication range	70 m
Carrier sense threshold	10000.21756e-11

Receive power threshold	10000.4613e-10
Radio frequency signal speed in air	3*108 m/s
Ultrasonic sound Speed through air	330m/s

**Table-2** Average remaining energy and average data variation of without and with IDS 50,100,150 and 200 nodes

Nodes	Average remaining energy without IDS in J	Average remaining energy with IDS in J	Average Data variation without IDS in J	Average Data variation with IDS in J
50	81.8948	86.4732 J	390.200	65.4200
100	83.9758	89.0167	557.990	56.3700
150	85.9292	89.5999	403.747	57.1533
200	86.5920	89.3445	303.280	54.5300



**Figure-2** Comparison of node wise remaining energy in 50.100.150 and 200 nodes with IDS and without IDS in nodes

Figure-2 shows the comparison of each node's remaining energy among 50,100,150 and 200 nodes by considering proposed method with and without IDS.

Table-2 shows average data variation and average remaining energy comparisons of our method with and without IDS in the nodes. In our method with IDS shows 65.42, 56.37, 57.1533 and 54.53 data variation in 50, 100,150 and 200 nodes in WSNs with 10, 21,22and 22 radiation affected node respectively. Also in our method with IDS shows 86.4732, 89.0167, 89.5999 and 89.3445 J remaining energy in 50, 100,150 and 200 nodes in WSNs with 10, 21, 22and 22 radiation affected nodes respectively. Data variation comparison between the methods and remaining energy comparison between the methods is plotted graphically in Figure-3 and Figure- 4 respectively.

In Figure-5, the proposed method with IDS shows the normal variation in data collected in 50,100,150 and 200 nodes in radiation affected WSNs environment and with 10, 21, 22 and 22 affected nodes respectively. In the Figure-6 a lot of variation can be observed in the collected data of nodes without IDS in the radiation affected environment. Hence, in this proposed method, sensor nodes with IDS if with any abnormal activity is found on that particular member. Head node initiate data balancing process of all the affected nodes.

In Figure-7, the proposed method with IDS shows less energy consumption in 50,100,150 and 200 nodes in radiation affected WSNs environment and with 10, 21, 22 and 22 affected nodes respectively. In the Figure-8 more energy consumption can be observed in the nodes without IDS in the radiation affected environment.

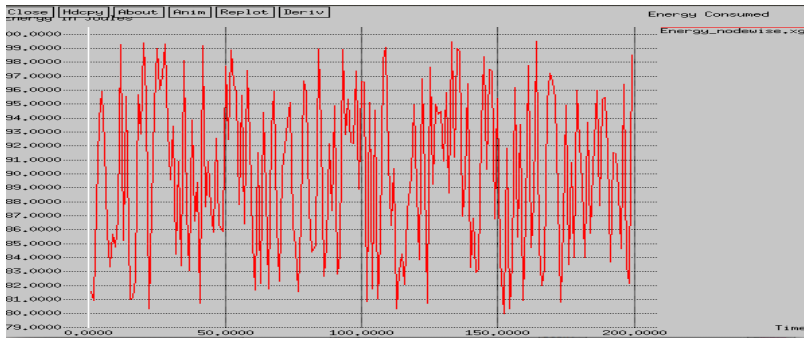
Figure-9 and 10 show packet delivery in 200 nodes with IDS and without IDS of WSNs affected by radiation. The above proposed method with IDS Shows that highest packets delivered to destination is more successfully compared with the method without IDS. Concerned to the total number of data packets generated to the destination by the source with the presence of 22 radiation affected nodes

Figure-11 and 12 show packet drops in 200 nodes with IDS and without IDS of WSNs affected by radiation. This proposed method with IDS shows that less Packet drop compare to the method without IDS in presence of 22 radiation affected nodes

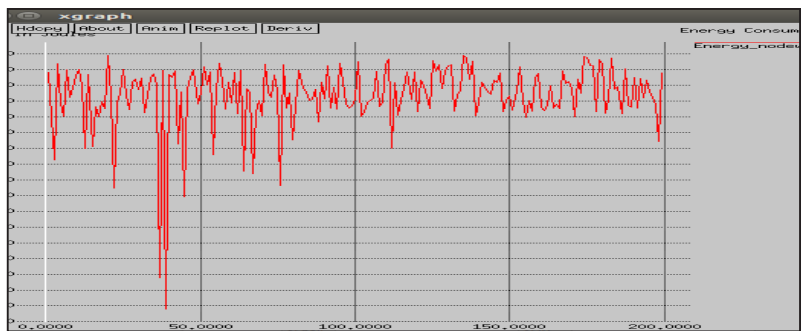
Figure-13 and 14 show throughput in 200 nodes with IDS and without IDS of WSNs affected by radiation. In this research paper nodes with IDS shows the high through put compare to the nodes without IDS in the presence of 22 radiation affected nodes.

Table-3 shows data of 22, 22, 21 and 10 nodes affected by radiation along with malicious activity, out of 200,150,100, and 50 nodes in WSNs respectively. In the proposed method, nodes are included with IDS agent. Radiation affected nodes in the proposed method with IDS will show the actual data. Node with IDS will monitors its neighbor's nodes activities and operation. If any malicious activity is found then cluster head is informed. Head node verifies alarm from the IDS agent of the respective node. If abnormal activity is found on the member then head node initiates data balancing process.

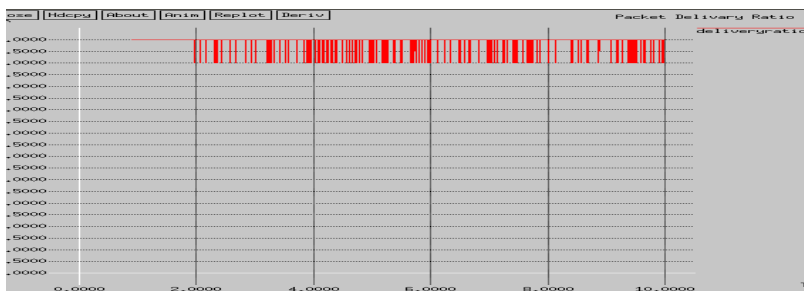




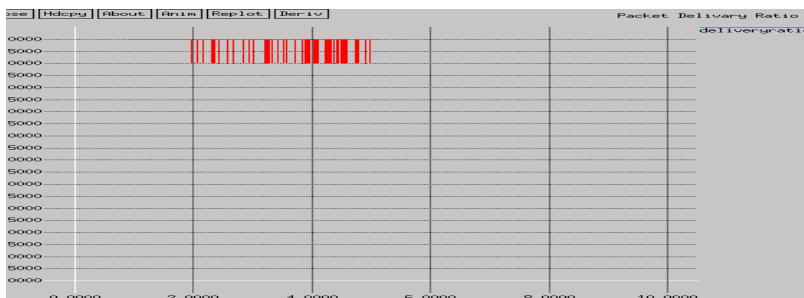
**Figure-7** Energy consumed in 50,100,150 and 200 with IDS



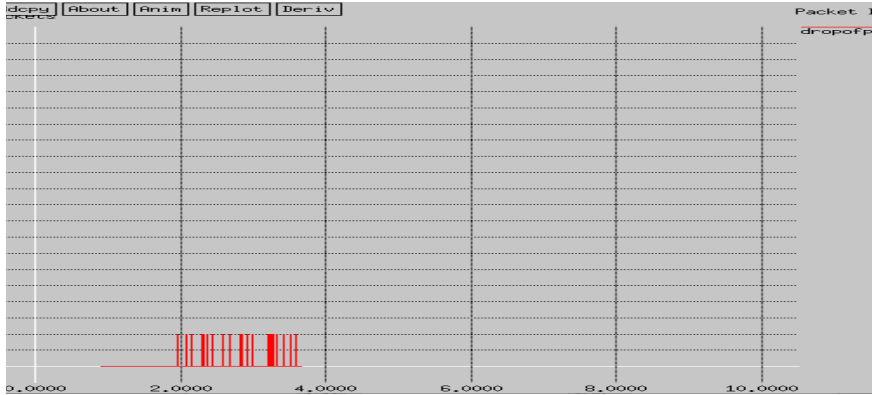
**Figure-8** Energy consumed in 50,100,150 and 200 nodes without IDS



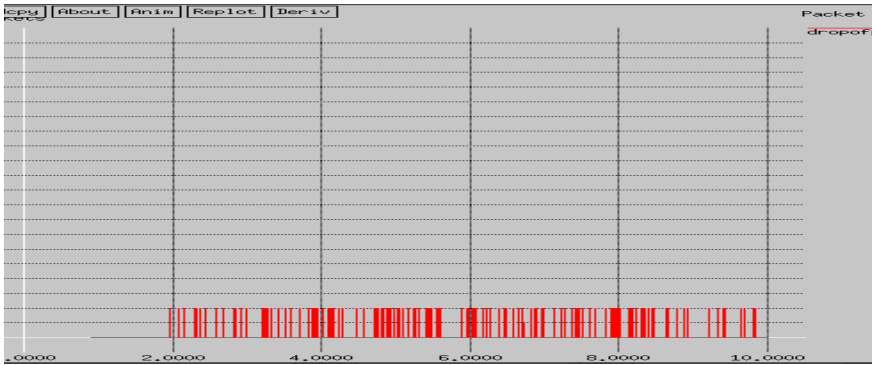
**Figure-9** Packet delivery ratio in 200 nodes with IDS



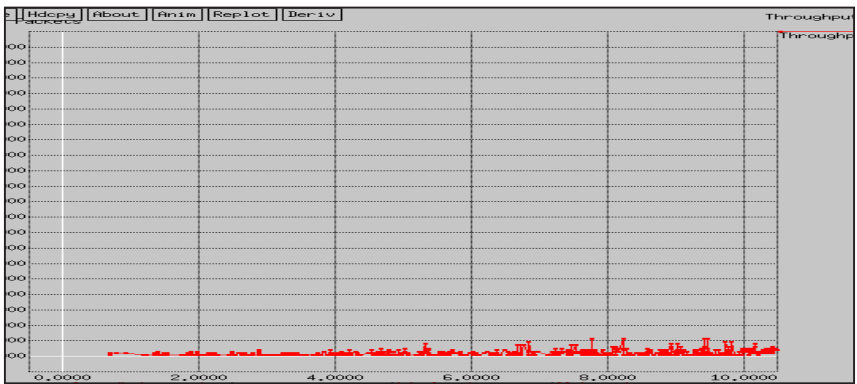
**Figure-10** Packet delivery ratio in 200 nodes without IDS



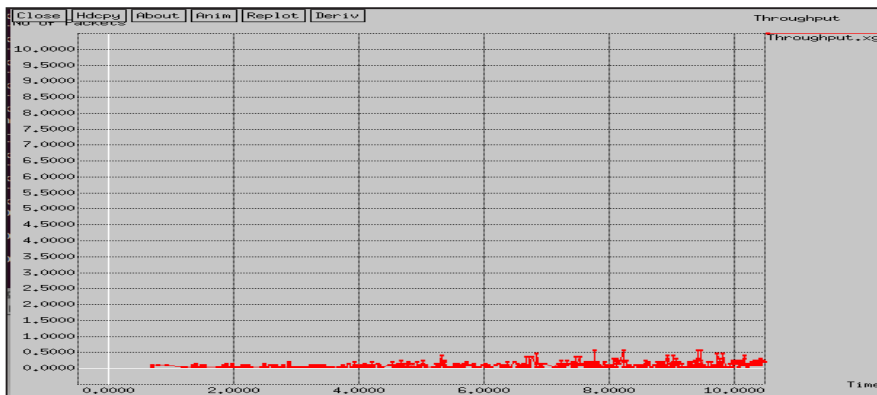
**Figure-11** Packet drop in 200 nodes with IDS



**Figure-12** Packet drop in 200 nodes without IDS



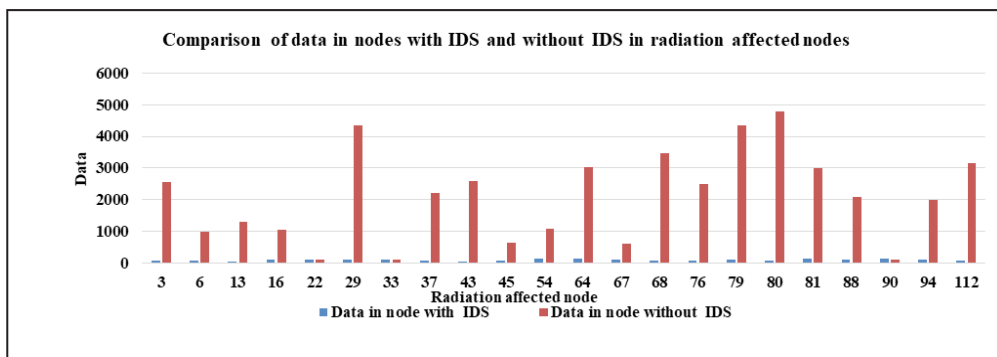
**Figure-13** Throughput in 200 nodes with IDS



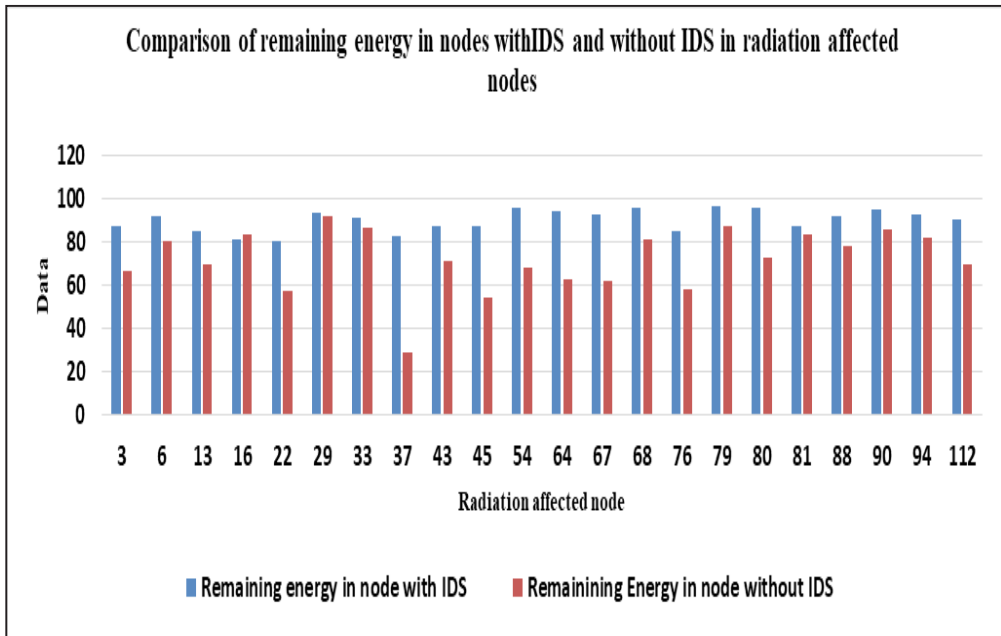
**Figure-14** Throughput in 200 nodes without IDS

But this is not in case of nodes without IDS. It shows more variation in the data in case of malicious activity. In the table we can observe more variation data in nodes without IDS.

Table-4 shows remaining energy of 22, 22, 21, 10 nodes affected by radiation along with malicious activity in 200,150,100 and 50 nodes in WSNs respectively. In proposed method, nodes are included with IDS agent. Radiation affected nodes in proposed method with IDS will show less consumption of energy, i.e. maximum remaining energy. IDS agent of the respective node identifies higher consumption of energy. So an alarm message is generated to intimate its neighbor. IDS agent updates the firmware and key of the node. But this is not in the case of node without IDS. It shows more consumption of energy in radiation affected node with malicious activity. It shows more variation in the remaining energy of nodes without IDS.



**Figure-15** Comparison of data in nodes with IDS and without IDS in radiation affected nodes out of 200 nodes.



**Figure-16** Comparison of remaining energy in nodes with IDS and without IDS in radiation affected nodes out of 200 nodes.

Figure-15 shows comparison of data in nodes with and without IDS in radiation affected nodes out of 200 nodes. Figure-16 shows comparison of remaining energy in nodes with and without IDS in radiation affected nodes out of 200 nodes and results are similar for 150,100 and 50 nodes.

#### 4. CONCLUSIONS

Advanced ideas and thoughts in the field of research will help to get a better result in our work. Our methods with IDS support us to improve the node efficiency in the radiation affected area of WSN with malicious activity by identifying the transfaulty behavior of nodes in that context. In simulation results the author has observed that each node with IDS agent shows less energy compare to the node without IDS. Reduction of energy consumption, maximum delivery of packet, minimum packet loss and through put of method with IDS is better than the method without IDS. In future work, it is planned to consider more parameters in cluster mechanism to achieve less consumption of energy in nodes.

**Table-3** Data in radiation affected node with IDS and without IDS in 200,150,100 and 50 nodes.

Radiation affected nodes with malicious activity in 200, 150, 100, 50.	200 nodes in WSNs		150 nodes in WSNs		100 nodes in WSNs		50 nodes in WSNs	
	Data in Node with IDS	Data in Node without IDS	Data in Node with IDS	Data in Node without IDS	Data in Node with IDS	Data in Node without IDS	Data in Node with IDS	Data in Node without IDS
3	0083	2543	0080	3231	0084	2057	0104	3208
6	0071	0981	0069	1479	0058	0240	0089	0203
13	0048	1313	0129	1558	0131	1166	0067	3547
16	0094	1053	0097	0383	0073	3373	0071	2647
22	00103	0105	0060	1482	0042	4632	0112	2005
29	0110	4349	0148	0299	0126	1849	0037	4497
33	0091	0092	0023	2926	0104	2524	0104	4322
37	0080	2221	0047	0574	0099	4256	0141	1000
43	0040	2593	0113	2227	0099	4772	0040	0781
45	0086	0626	0146	4243	0076	0411	0094	1893
54	0125	1076	0072	1961	0101	1196	-	-
64	0144	3025	0061	4839	0107	4666	-	-
67	0103	0618	0066	2288	0134	2122	-	-
68	0067	3455	0075	4697	4697	3857	-	-
76	0077	2496	0064	3112	3112	2245	-	-
79	0121	4336	0102	3111	3111	2683	-	-
80	0088	4775	0080	1624	1624	4856	-	-
81	0149	2985	0176	1071	1071	3153	-	-
88	0102	2089	0155	2314	2314	3011	-	-
90	0129	0113	0158	0865	0865	2698	-	-
94	0108	1983	0128	2971	2971	0197	-	-
112	0083	3162	0057	4772	-	-	-	-

**Table-4** Remaining energy in radiation affected node with IDS and without IDS in 200,150,100 and 50 nodes.

Radiation affected nodes with malicious activity In 200, 150, 100, 50	200 nodes in WSNs		150 nodes in WSNs		100 nodes in WSNs		50 nodes in WSNs	
	Remaining energy in nodes with IDS	Remaining energy in nodes Without IDS	Remaining energy in nodes with IDS	Remaining energy in nodes without IDS	Remaining energy in nodes with IDS	Remaining energy in nodes without IDS	Remaining energy in nodes with IDS	Remaining energy in nodes without IDS
3	87.7103	66.3058	89.3477	49.4445	97.8098	84.1653	95.4659	68.8627
6	92.0724	80.1674	95.2365	79.9183	84.7368	75.8076	92.3818	78.8269
13	85.2094	69.8646	89.7037	73.4098	90.5005	69.4491	83.5783	66.4147
16	81.1325	83.2655	87.2839	73.4738	96.0287	73.5817	91.9139	45.0828
22	80.3189	57.3708	92.1819	66.0998	80.8346	78.7999	82.7601	67.2913
29	93.2065	92.0172	94.7686	96.9269	99.1843	80.3468	96.8672	89.4710
33	90.9297	86.9620	90.1039	72.4788	92.6276	51.0450	99.1796	85.0921
37	83.0549	28.8262	90.8599	78.8008	81.6199	26.4563	94.4780	98.6290
43	87.6164	71.2986	85.5342	70.8361	97.1337	66.6702	92.6090	74.2630
45	87.4358	54.5921	81.6870	67.9247	98.8374	64.4879	99.0696	70.9469
54	95.8062	67.9452	93.4071	72.2204	93.3663	80.3277	-	-
64	94.4115	62.6759	84.4985	73.5942	80.2659	62.5186	-	-
67	93.1513	61.8954	97.4457	96.3756	96.8721	98.9139	-	-
68	95.9149	81.2927	85.2201	58.8303	88.1759	77.1026	-	-
76	84.7369	58.1926	82.4098	77.8639	85.6686	57.3466	-	-
79	96.6761	87.6353	96.3951	91.0029	98.2917	86.3060	-	-
80	95.7303	72.7099	88.6765	71.3829	83.8145	81.0167	-	-
81	87.6045	83.4903	80.6993	76.7300	98.7261	75.8471	-	-
88	92.1591	78.2644	86.1469	70.9163	92.0140	75.5825	-	-
90	94.9096	85.6857	86.5414	84.8929	81.4900	88.9942	-	-
94	92.7929	82.3614	92.4646	79.5960	86.9623	77.4669	-	-
-112	90.4156	69.9928	99.2537	71.8535	-	-	-	-

## Legend

distance [inn, jnn]	=	Distance between ith node and jth node
inn	=	ith node
jnn	=	jth node
x1	=	X coordinate value
x2	=	X coordinate value
y1	=	Y coordinate value
y2	=	Y coordinate value
regy[i]	=	Remaining energy of ith node
dist [i, nei [i, j]]	=	Distance between the node[i] and neighbor node nei [i. j] at particular time t
avg_rem_egy	=	Average remaining energy of all the nodes in a cluster
total_of_regy	=	Sum of remaining energy in all the nodes of a cluster
tno_nodes	=	Total number of nodes in a cluster
egy_consumption	=	Energy consumption of node at particular time t
data_pk_t	=	Number of transmitted packets
data_pk-r	=	Number of received data packets
k1, k2	=	Constants in the range (0,1)
nd_cov(x)	=	Node coverage of node x
ng_nd(x)	=	Neighbors node x
ng_nd(x)	=	Number of neighbors node x
E	=	Number of edges in a cluster of network Graph G (V, E)
V	=	Number of vertices in a cluster of network Graph G (V, E)
mb_nd (n)	=	Node Mobility of the node n
x_cot	=	X coordinate positions of node at time t
y_cot	=	Y coordinate positions of node at time t
x_cot-1	=	X coordinate positions of node at time t-1
y_cot-1	=	Y coordinate positions of node at time t-1
avg_dt_cul(c)	=	Average data collected by cluster members of cluster c
M(c)	=	Members count in a cluster c
dt_node(i)	=	Data of ith node
tl_mem_cul(c)	=	Total number of members in a cluster
difference	=	Difference between the current data and previous data

avg_dt_cul	=	Average data of a cluster
dt [nn]	=	Sensed data of previous round
dv_per_clu	=	Deviated members per cluster
dv_meb_clu(C)	=	Total number of data members deviated by greater than data threshold value
tl_mem_cul(c)	=	Number of nodes in the cluster
pkt_dely_ratio	=	Packet delivery ratio
recd_pkt_size	=	Sum of data packets received by the each receiver node
sou_pkt_size	=	Sum of data packets generated by the each sender node
pkt_drop_ratio	=	Packet Drop (Loss) Ratio
pkt_actly_frd	=	Packets reached the destination
pkt_tobe_frd	=	Actual packets send from source in a particular time `t`
thr_put	=	Throughput
tot_no_bits	=	The number of bits received successfully by all receiver
tot_sim_time	=	Total simulation time

## REFERENCES

1. I.F. Akyildipuz, W. Su, Y. Sankara subramaniam and E. Cayirci, Wireless Sensor Networks: *A Survey*. *Computer Networks*, 2002, 38, pp.393–422.
2. N. Marriwala and P. Rathee, An Approach to Increase the Wireless Sensor Network lifetime. *World Congress on Information and Communication Technologies, IEEE, Trivandrum, India*, 2012, pp.495–499.
3. V. C. Gungor, B. Lu, and G. P. Hancke, Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Transactions on Industrial Electronics*, 2010, 57, pp. 3557-3564.
4. S. S. McClure, Radiation Effects in Micro-Electromechanical Systems (MEMS): RF Relays. *IEEE Trans. Nucl. Sci.*, 2002, 49, pp.3197-3202.
5. H.R. Shea, Radiation Sensitivity of Micro Electromechanical System Devices. *Journal of Micro/ Nanolithography, MEMS and MOEMS*, 2009, 8(3), pp.1–11.
6. M. A. Rassam, M. A. Maarof, and A. Zainal, A Survey of Intrusion Detection Schemes in Wireless Sensor Networks. *American Journal of Applied Sciences*, 2012, 9(10), pp.1636–1652.
7. I. Butun, S. D. Morgera, and R. Sankar, A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*, 2014, 16, pp.266-282.
8. A. Mehmood, M. M. Umar, and H. Song, ICMDs: Secure Intercluster Multiple-Key Distribution Scheme for Wireless Sensor Networks. *Ad Hoc Netw.* 2017, 55,

pp.97-106.

9. Suma G. and M. Siddappa, Life Time Improvement with Hybrid Clustering in Mobile Sensor Networks. *International Journal of Computer Sciences and Engineering*, 2017, 5(11), pp.57-63.
10. V. Patel and J. Gheewala, An Efficient Session Key Management Scheme for Cluster Based Wireless Sensor Networks. *IEEE International Advance Computing Conference*. 2015 pp.963-967.
11. I.Krontiris, T. Dimitriou and F.C. Freiling, Towards Intrusion Detection in Wireless Sensor Networks. *Proc.13th European Wireless Conference*, 2007, pp.1-10.
12. A.da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, Decentralized Intrusion Detection in Wireless Sensor Networks. *1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks*. 2005, pp.16-23.
13. I.Krontiris, Z. Benenson, T. Giannetos, F. Freiling, and T. Dimitriou, Cooperative Intrusion Detection in Wireless Sensor Networks. *Conference on Wireless Sensor Networks*, 2009, 5432, pp.263–278.