VOLUME 1 ISSUE 1 JANUARY - JUNE 2020

JIR

SSAHE

JOURNAL OF INTERDISCIPLINARY RESEARCH

Exploring the unknown
Creating the new...

www.ssahe.in/jir

SRI SIDDHARTHA ACADEMY OF HIGHER EDUCATION

JOURNAL OF
INTERDISCIPLINARY
RESEARCH

VOLUME 1 ISSUE-1 JUNE 2020

Contents

Contact :

Dr. C. Rangaraj
SSAHE JIR, Editor
Professor, Sri Siddhartha Institute of Technology, Tumakuru – 572105.
E-mail: ssahe.jir@gmail.com
Ph. 9880824098 / 7019847477

Cover and article page design

Sri Siddhartha Center for Media Studies Tumkur

The SSAHE JIR is a unpaid and peer reviewed journal published two times a year

EDITORIAL

The giants of thought in yesteryears were indeed interdisciplinary since they recognized the world as one, whereas narrowing of scope by specialists frequently reinforced orthodoxy. The newer branches of engineering which we see today are the result of interdisciplinary research in the past.

In days gone by, research meant isolating important aspects of phenomena, reducing the variables so as keep the problem manageable. It also meant restricting the validity of conclusions to a range resulting from removal of the unmanageable complications. With the advent of information technology, attempts were made to solve more complex problems by modelling. More difficult problems usually were represented by a differentiated set of variables and hitherto insolvable problems were tackled. Also, uncertainty was included which, till then, was not practically possible to be integrated.With all these, the possibility of interdisciplinary research assumed importance.

Interdisciplinary research may help to reduce the exclusive focus on positive research. Positive results are undoubtedly important for progress of science but replication and null studies are equally important. In null studies, the results of the experiment contradict existing research findings. Further replication studies and null studies help in weeding out the bias that may creep into engineering and science, mainly due to its focus on positive results. Interdisciplinary researcher has to ascertain that solution devised for another domain is indeed suitable and cost effective. Interdisciplinary researchers should be aware of scale effects while obtaining solutions especially when the solution is referenced outside its scope. Complex, community level problems do exist which need a genuine interdisciplinary approach that ensures an immediate benefit. The subjective and objective inputs from two or more disciplines also help in advancing understanding of science itself.

The trend of research in Europe and India was within the discipline focus, whereas USA took a lead in interdisciplinary research. Such research articles might not exactly fit into the journals that are dedicated to the given discipline of study. The development of interdisciplinary research was crippled with very few journals catering to their useful research findings. There is a need for interdisciplinary research, as the particular field of investigation may be beyond the scope of researchers of each constituting discipline. In the above context, it is felt that there is dire need of a dedicated journal with the sole objective of providing a platform to address all the pressing and currently relevant issues raised above. Here is the sincere and all-out effort put in by the able team of SSAHE Journal, published by Sri Siddhartha Academy of Higher Education, a deemed to be University, at Tumakuru, Karnataka, India. This online biannual interdisciplinary journal is expected to bring researchers across the globe, to a single platform, enabling them to publish, exchange views/solutions and speedup the desired solutions so as to reach the stage of effective implementation.

Jacob's Syndrome - A rare Case Report

R. Lakshmi Prabha Subhash[1], Anupama D.[2]✉, Bindurani M. K.[3], Harshal K. L.[4], Jayarama S. Kadandale[5], Swathi Shetty[6], Meenakshi Bhat[7]

[1]Professor and HOD, [2] Professor, [3]Associate Professor, [4]Research Associate, [5]Cytogeneticist, [6]Molecular Biologist, [7]Genetic counselor,
Dept. of Anatomy, Sri Siddhartha Medical College, SSAHE, Agalakote, Tumakuru 572107, Karnataka, India

✉dranupama7373@gmail.com

Abstract

Jacob's or 47,XYY or XYY or YY syndrome is a male sex chromosomal disorder which is less common and this chromosomal anomaly is seen in 1/1000 live male births. It is characterized by the presence of an additional Y chromosome in a male. Normal male karyotype is 46, XY. In this syndrome, the chromosome pattern of the individual is 47, XYY which is a result of pre conception or post conception error in cell division. Most patients with 47, XYY karyotype have normal phenotype hence the diagnosis may be delayed or coincidental. Majority of them have an average or tall stature and usually have normal fertility, may also present with developmental delay, speech and behavioral problems. A rare case of 47,XYY syndrome associated with male infertility is reported here.

Keywords: *Chromosomal abnormality, Karyotype, Infertility, Developmental delay.*

1. INTRODUCTION

Jacob's or 47, XYY syndrome is the second common sex chromosomal disorder seen in males next to Kline Felter syndrome characterized by the presence of an extra Y chromosome in males. The parental origin of the extra Y chromosome in males with XYY is always paternal. It is also termed as XYY or YY or Jacob's syndrome. In 1961, the first case was described by a cytogeneticist Avery Sandberg and his associates which was a coincidental finding. This syndrome is seen as a result of non-disjunction during metaphase II of paternal meiosis during spermatogenesis with extra copy of chromosome Y which if involved in fertilization, the child will carry an additional Y chromosome in all the cells. In few cases, there might be an error in the post zygotic mitosis in early embryonic development which produces a mosaic 46, XY/47, XYY. Most of these patients present with anti-social behavior. Hence, the incidence is increased to 2-3% of males, who are in institutions because of learning and behavioral problems [1,2]. Although they show emotional

imbalance and impulsive behavior, fertility rates are normal[1], but there are some case reports which reveal that infertility can be associated with the extra copy of Y chromosome [3]. Physical appearance is normal and stature is usually average or above average. They may have mild developmental delay with sluggish motor activities and speech disturbances, excessive acne and multiple joint problems [1]. The first published report of a man with a 47, XYY karyotype was from Rosewell Park Memorial Institute (RPMI) in Buffalo, New York in 1961. It was an incidental observation in an apparently normal forty four year old male of average intelligence who was subjected to karyotyping, because he had a daughter with Down syndrome. In another large study of 315 male patients from the hospital for the developmentally disabled, XYY chromosomal pattern was seen in nine patients between 17 to 36 years with an average height of almost 6 feet and these were mischaracterized as aggressive and explosive criminals. All published XYY studies were usually based on height criteria in institutionalized XYY males. Men with this sex chromosomal abnormality usually have tall stature [4]. Sometimes it causes no unusual physical features. 47, XYY syndrome has normal production of the male sex hormone like testosterone and normal sexual development and they are usually fertile [2]. 47, XYY syndrome with fertility issue is relatively less common and syndrome can be missed clinically because of its variable clinical presentations [2]. Male infertility is seen more frequently associated with sex chromosome abnormalities[3].

2. CASE REPORT

A thirty year old male presented with h/o Infertility at Invitro Fertilization (IVF) Centre of Sri Siddhartha Medical College, Tumakuru. The patient was married two years back. He was born at full term with a normal birth weight and height to a consanguinous couple (first cousins) with birth order of 4 out of 13. Past history was not significant other than poor performance at school hence dropped out from school. He was a tea shop owner. The family history revealed another case of Infertility in the elder brother aged thirty four years, who was also found to be azoospermic. General physical examination revealed tall adult male moderately built and nourished with long, coarse facies, hypertelorism and marked philtrum with swelling and pain of left lower limb. Patient also had slurred slow speech and mild mental retardation. As history given by his spouse he was slow in all his activities. Routine blood investigations and semen analysis were done. Semen analysis revealed Azoospermia. Testosterone levels were found to be normal. Then, the case was referred for chromosome analysis and Y micro deletion study. Chromosome

studies with conventional cytogenetic technique revealed sex chromosomal abnormality. The Geimsa Banding Technique (GTG) revealed the abnormal non-mosaic 47, XYY karyotype in the peripheral blood cells from the patient as shown in Figure-1. Y micro deletion study indicated the presence of all 3 regions AZF a, AZF b and AZF c regions tested on the Y chromosome.

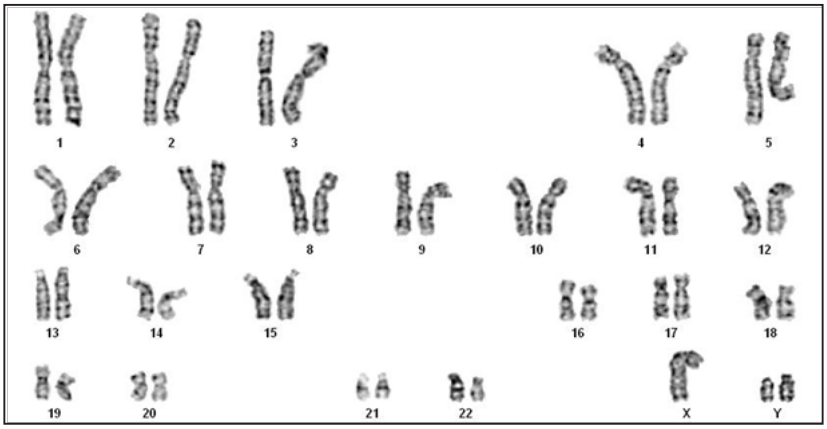


Figure-1 Male Karyotype showing 47, XYY Pattern

3. DISCUSSION

Accurate diagnosis of this syndrome is by subjecting the patient to chromosomal analysis which provides a valuable aid in counseling and early intervention of the patients who undergo fertility evaluation [3]. For this condition, how an extra Y chromosome can affect fertility in 47, remains unclear, thus many more detailed studies need to be conducted to carry out more evaluation of infertility in individuals with 47, XYY syndrome [3].

It is reported that the patient with 47, XYY karyotype has behavioral defects including delayed speech, language skills and motor development, slow performance and reduced interactive skills with high level prevalence of autism spectrum disorders. The additional Y chromosome in XYY is an active one, and over expression of all Y-linked genes because of double copy of Y chromosome in the XYY. Initially, the Y chromosome was thought to have sex-determining and testicular function genes, but is now understood that it contains additional genes. It is hypothesized that autistic behavioral features in XYY are based on excessive dosage of one or more of these Y-specific genes. Attention deficits are more common in boys to validate that screening for sex chromosomal abnormalities on the basis of this behavioral indication; however genetic evaluation should be indicated when Attention Deficit Hyperactivity

Disorder (ADHD) is associated with physical and language problems and testicular malformations [1].

Another study reported that the index patient presented with microcephaly who was the first child of healthy non consanguineous couple. Prenatal diagnosis (Amniocentesis) was suggested due to an increased nuchal fold and chromosomal analysis revealed 47, XYY [5].

Physical and laboratory examination in three cases with 47, XYY syndrome found during infertility evaluation revealed that greater prevalence of hyper haploid sperm results in greater prevalence of passing the additional Y chromosome to offspring. In these cases, the sperm count may vary from normal to azoospermia. It is found to have inhibitory effect on sperm count, maturity, and genetics as demonstrated by published case reports [3].

A Study reports that a five year old boy with the clinical feature of "DOWN SYNDROME" which is the most common human genetic syndrome revealed a mosaic pattern of down syndrome and XYY together. The karyotype was 47, XY + 21(19)/48 XYY +21(6). Treatment of Jacob's syndrome is always symptomatic and supportive which includes behavioral, speech and occupational therapy. If the condition is associated with Infertility and azoospermia then the option of sperm donation and IVF should be discussed during counseling.

REFERENCES

1. Judith L. Ross, David P. Roeltgenetal Behavioral and Social Phenotypes in Boys With 47, XYY Syndrome or 47, XXY Klinefelter Syndrome. *Pediatrics.* 2012, 129(4), pp.769–778.
2. Turnpenny Ellard, *Emery's Elements of Medical Genetics,*13th Ed., Churchill living Stone Edinburgh Ch.18, pp.273.
3. Ina W Kim, Arjun C Khadilkaretal. 47, XYY Syndrome and Male Infertility. *Rev Urol,* 2013, 15(14), pp.188-196.
4. Hanane Latrech and Imane Skikaretal, Disorder of Sexual Development and Congenital Heart Defect in 47, XYY: Clinical Disorder or Coincidence? Hindawi Publishing Corporation, *Case Reports in Endocrinology,* 2015, Article ID 802162, DOI: 10.1155/2015/802162.
5. S. Nguyen-Minh et al. Is Microcephaly a so-far Unrecognized feature of *XYY Syndrome*? *Meta Gene,* 2014, 2, pp.160-163.
6. Mayur Parihar and Beena Koshyetal, Mosaic Double Aneuploidy: Down Sydrome and XYY. *Indian J.Hum.Genet.,* 2013, 19(3), pp.346-348.

Improvement of Node Efficiency in the Radiation Affected Area of WSN

Asha K.R.[1]✉, Supriya M.C[2].

[1]*Research Scholar, SSAHE, Agalakote, Tumakuru, Karnataka, India - 572105*
[2]*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 cites 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 Anamoly 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. METHODLOGY

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.

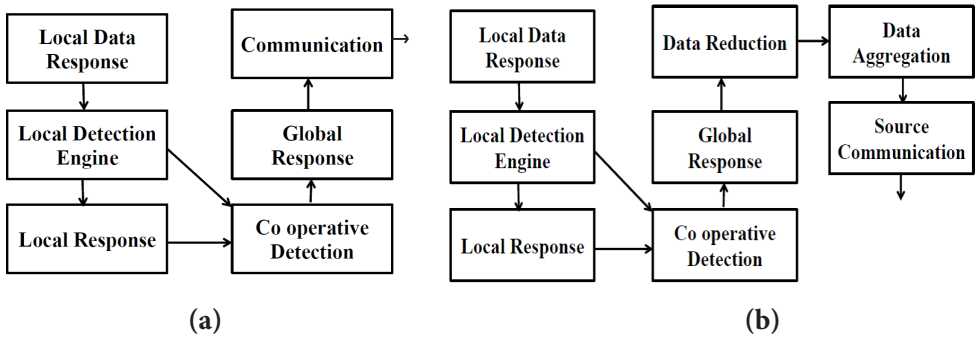


Figure-1 IDS running in a member node and cluster head (a) IDS running on the member nodes of a cluster (b) IDS running on the cluster head

IDS agent placed in each node in WSNs to detect attacks by observing the node's transfaulty behavior of affected sensor nodes. Due to transfaulty 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 is 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:

regy[i] =regy[i]-(dist [i, nei [i, j]]*egy_consumption) (2)

and average remaining energy is calculated by:

avg_rem_egy=total_of _regy/ tno_nodes. (3)

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

egy_consumption = (data_pk_t * k1) + (data_pk-r * k2) (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:

$$nd\_cov(x) = \sum_{1}^{ng\_nd(x)}((x,y) \in E/\ y \in ng\_nd(x))/\ |ng\_nd(x)| \quad (5)$$

Node Mobility of the sensor node, mb_nd (n) of the node is found out by:

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

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:

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

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:

pkt_dely_ratio= recd_pkt_size / sou_pkt_size (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:

pkt_drop_ratio= pkt_actly_frd/pkt_tobe_frd (11)

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

thr_put = tot_no_bits/tot_sim_time (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

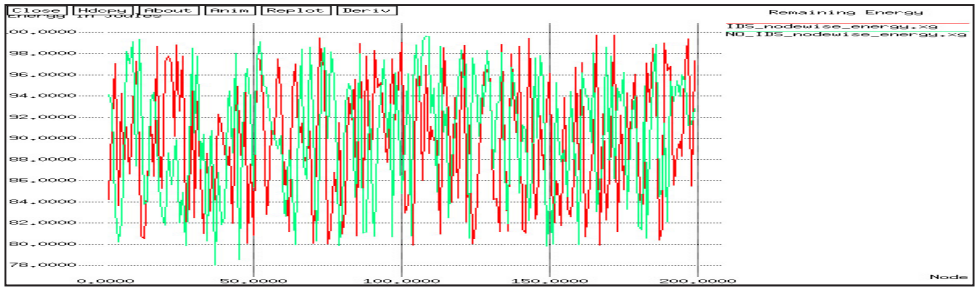


Figure-2 Comparison of node wise remaining energy in 50.100.150 and 200 nodes with IDS and without IDS in nodes

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.

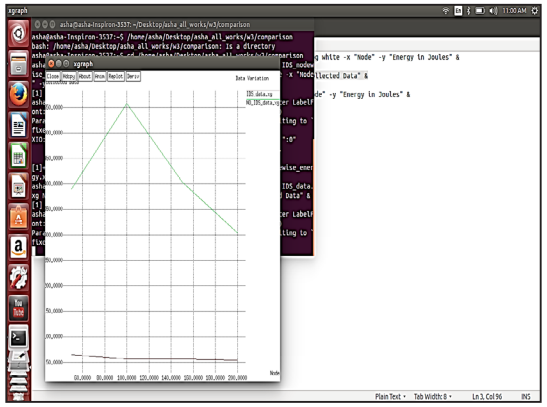


Figure-3 Data variation 50,100,150 and 200 with IDS

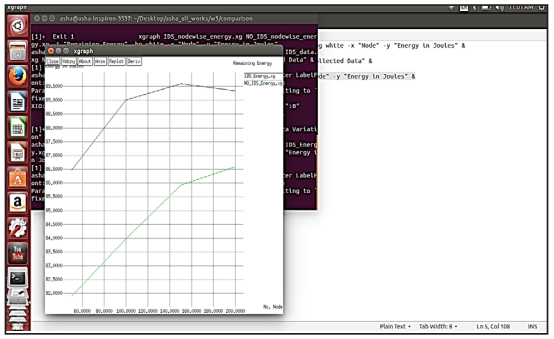


Figure- 4 Remaining energy for of 50,100,150 and 200 without IDS

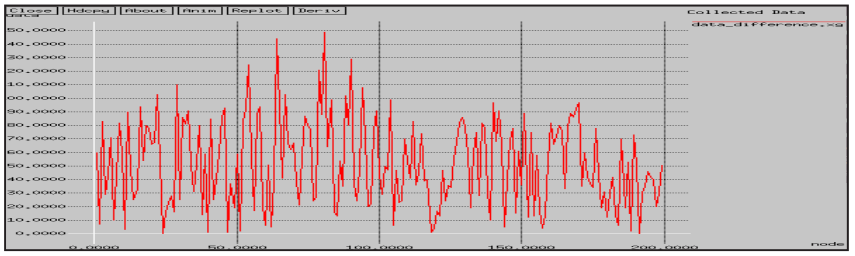


Figure-5 Data collected in 50,100,150 and 200 nodes with IDS

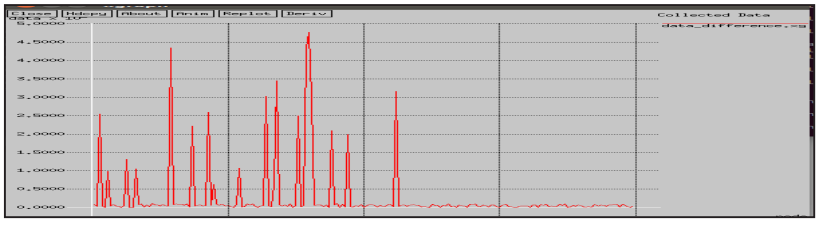


Figure-6 Data collected in 50,100,150 and 200 nodes without IDS

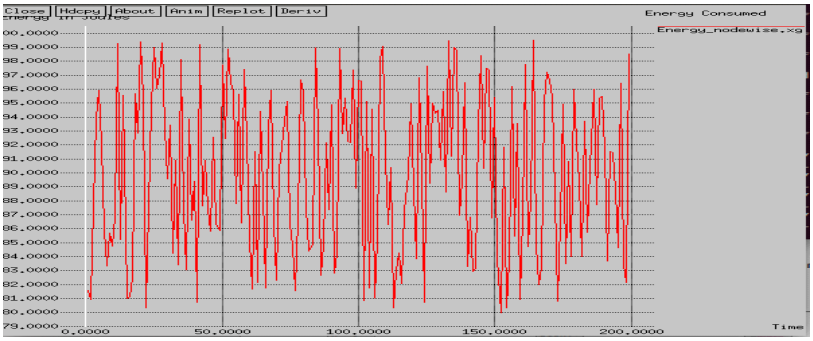


Figure-7 Energy consumed in 50,100,150 and 200 with IDS

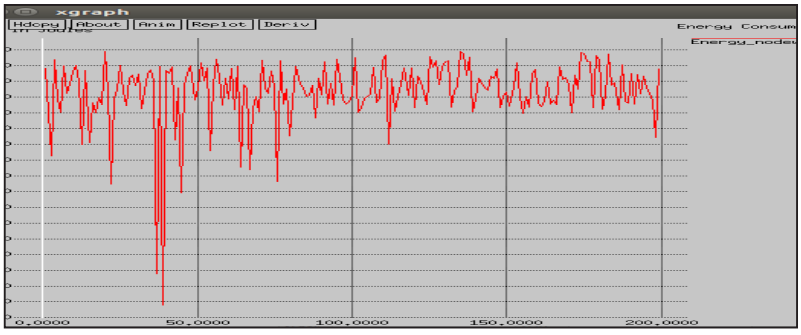


Figure-8 Energy consumed in 50,100,150 and 200 nodes without IDS

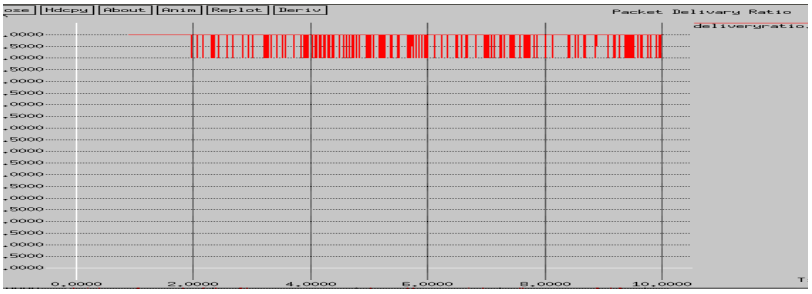


Figure-9 Packet delivery ratio in 200 nodes with IDS

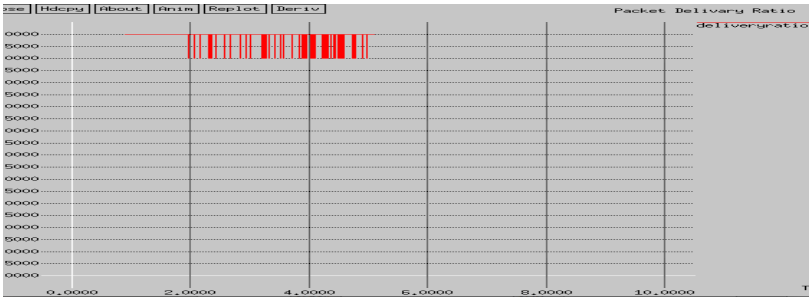


Figure-10 Packet delivery ratio in 200 nodes without IDS

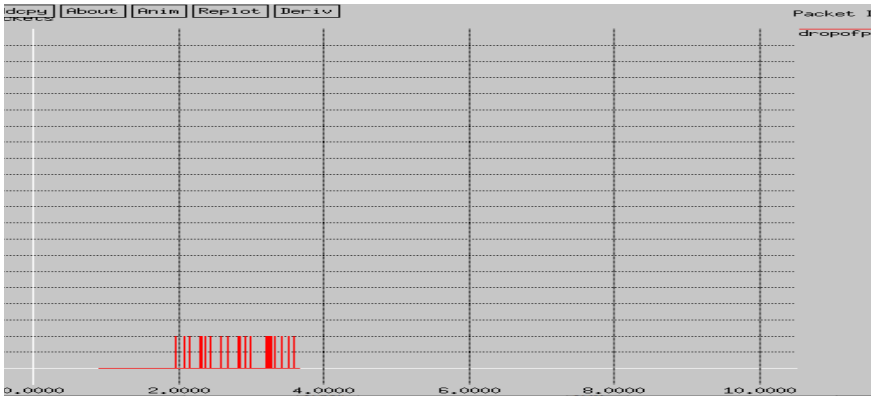


Figure-11 Packet drop in 200 nodes with IDS

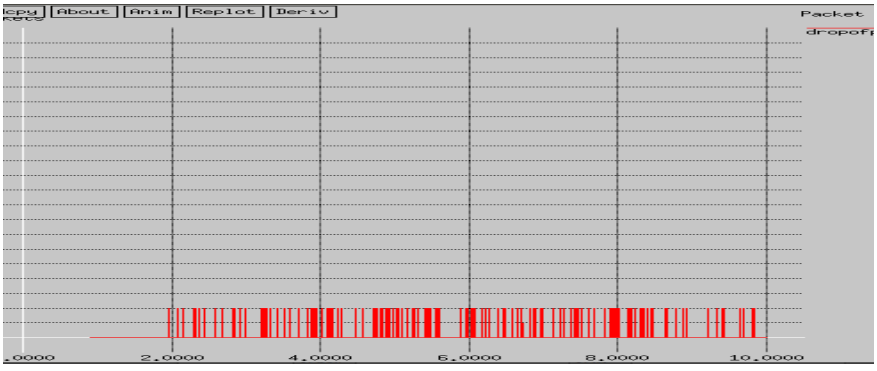


Figure-12 Packet drop in 200 nodes without IDS

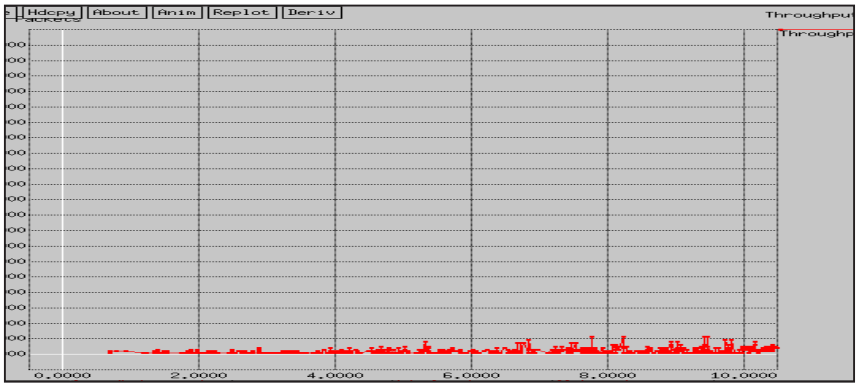


Figure-13 Throughput in 200 nodes with IDS

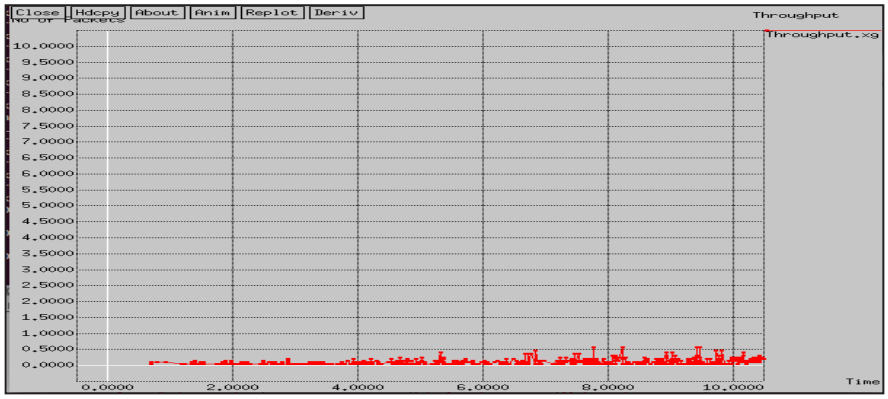


Figure-14 Throughput in 200 nodes without IDS

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.

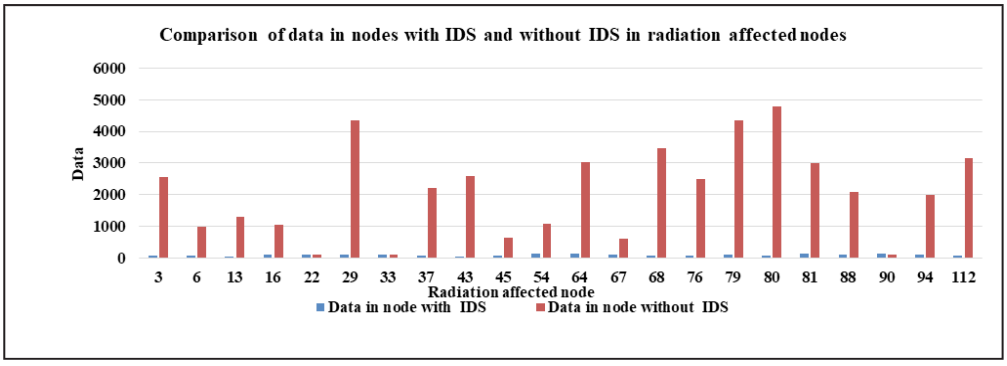


Figure-15 Comparison of data in nodes with IDS and without IDS in radiation affected nodes out of 200 nodes.

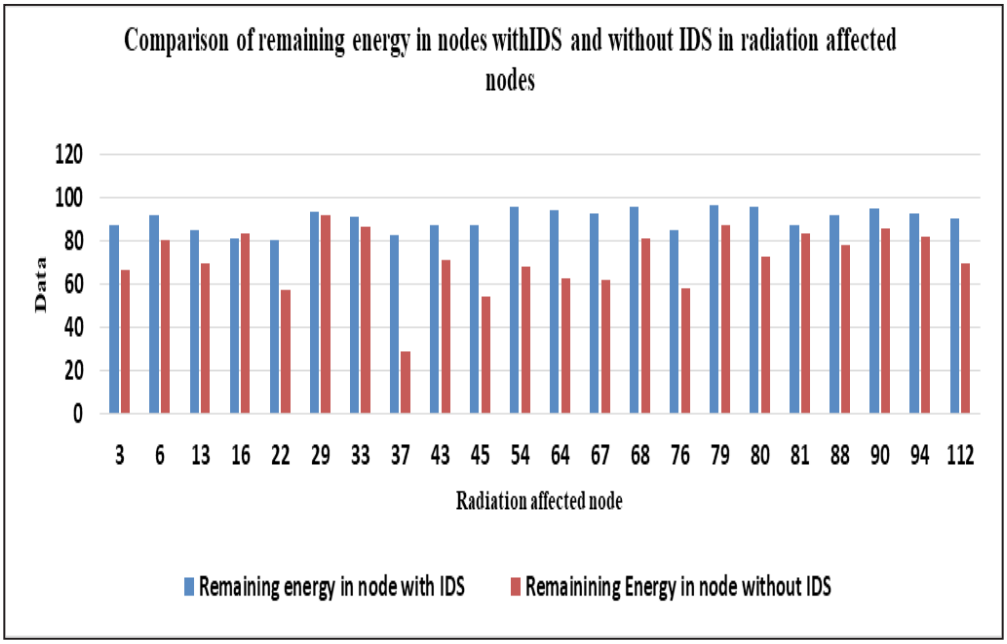


Figure-16 Comparison of remaining energy in nodes with IDS and without IDS in radiation affected nodes out of 200 nodes.

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 with out 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 Sheme 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. Giannetsos, F. Freiling, and T. Dimitriou, Cooperative Intrusion Detection in Wireless Sensor Networks. Conference on *Wireless Sensor Networks,* 2009, 5432, pp.263–278.

Static and Vibration Analysis of Bridge Deck Slabs

Roopa M.[1]✉, Venugopal H.[2], Nischay T. G.[3]

[1]Research Scholar, SSAHE, Agalakote, Tumakuru, Karnataka, India - 572105
[2]Professor ,Dept. of Civil Engg., SSIT, Tumakuru, Karnataka-572105,
[3]Engineer – Design, Bureau Veritas (India) Pvt. Ltd., # 1030, 13th Cross, Banashankari 2nd Stage, Bangalore 560070
✉roopacivil11@gmail.com

Abstract

Bridge deck slabs are the most important structures commonly supported at the two edges. Such supports are generally orthogonal to the traffic course. However, once in a while they may not be orthogonal to the traffic route necessitated by many reasons. Such bridge decks are defined as skew bridge decks. Very little research work is reported on static and vibration behavior of skew slab bridges. Subsequently, in this study an attempt has been made to evaluate the static and vibration behavior of skew slab bridge decks and the usage of finite element analysis. Static analyses are done for distinctive skew angles and for defferent aspect ratios, loading situations together with dead load, Indian Road Congress (IRC) class A loading and also for the cases of deck slab with out and with edge stiffening beams. Similarly, parametric studies on bridge deck having 30° skew angle and aspect ratio of 0.4 are done to assess the impact on area stiffening, bearing flexibility at the static behavior. Vibration analysis of simply supported skew slab bridges of various skew angles and aspect ratios are also performed.

Keywords: *Skew bridge decks, Skew angles, Edge stiffening, Bearing flexibility.*

1. INTRODUCTION

The structures are generally analyzed by static and dynamic methods. Selection of an appropriate method depends upon the several factors such factors includes importance of analysis, importance of structure, type of the structures and its surrounding soil conditions. Structures are designed in such way that it should carry self-weight, live loads, super imposed loads and wind loads. These loads are considered as maximum load taken by the structure and they are static in nature [1-5]. In some of studies it includes static and dynamic loads also [6]. The analysis of dynamic loading are evaluated by equivalent static method, or by an impact factor, or by a modification of the factor of safety etc. The finite element evaluation performs an essential function for any complex analysis.

It is very beneficial in which difficulty of Geometrical conditions, material properties, boundary situations and loading are involved.

2. METHODOLOGY

2.1 Details of Finite Elements used

The finite element approach has turn out to be a powerful computational tool, which allows complex analyses of the structures to be completed in a recurring fashion. There are various finite element software applications along with STAAD pro, SAP 2000, ATENA, ABAQUS, ANSYS, E-TABS, etc. STAAD pro (Structural analysis and design) is used for the present observation. Bridge deck slabs are modeled using Plate/Shell detail. Area stiffening beams are modeled using beam element and support elastomeric bearings is modeled using solid elements.

2.2 Material Properties and Load Modeling

Properties for Deck slab is taken as $E = 25 \times 10^6$ kN/m^2; $\mu = 0.2$; $\rho = 25$ kN/m^3 The dead load contains of self-weight of the whole structure. This is accounted through geometrical properties of sections and unit weight of materials used. The primary live load on Highway Bridge is of the cars moving on it. Indian Roads Congress (IRC) recommends different kinds of widespread hypothetical vehicular loading systems in IRC 6:2000, for which a bridge is to be designed. The vehicular live load consists of a set wheel loads which can be distributed over small areas of contacts of wheels and form patch loads and dealt with as concentrated loads acting at centers of contact areas. This will acquire the maximum response resultants for the layout, different positions of every type of loading system as per IRC 6:2000 is tried at the bridge deck. The load is moved longitudinally and transversely in small steps to occupy a large number of various positions on the deck. The largest force reaction is obtained at each node. As per IRC 6:2000 Table-2, lane of class A or one lane of class 70R should be considered to get most response under hypothetical vehicular loading systems.

2.3 Support Conditions

For simply supported case, the nodes must be constrained in the vertical direction (Y direction). A single line of nodes on the plate along the supported width are constrained in vertical direction (Y course). For the evaluation to run, small spring stiffening of 1 kN/m is provided all along the supported width of plate in Z direction. The simple support is shown in the Figure-1.

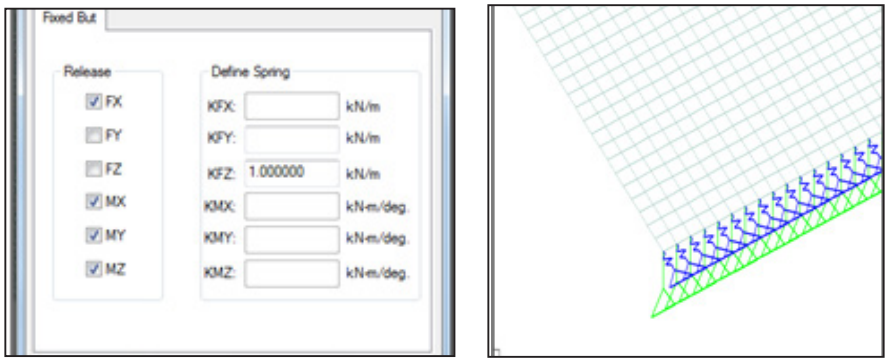


Figure- 1 Details of simply supported condition

3. STATIC ANALYSIS

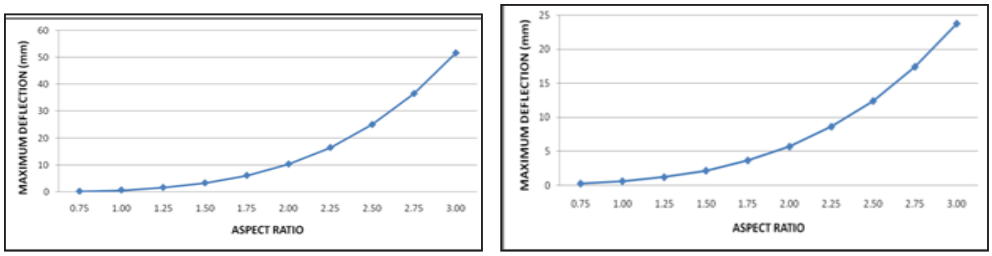
Typical simply supported two- lane bridge study cases are considered in this study. Ten aspect ratios 0.75, 1.0, 1.25, 1.50, 1.75, 2.00, 2.25, 2.50, 2.75 and 3.00 are considered as parameters of deck slab of 0.75m thickness. The aspect ratios considered for analysis are shown in Table-1.

Table-1 Different aspect ratios for deck slab

Span in m	Right widthin m	Aspect ratio (L/B)
5.25	7	0.75
7.00	7	1.00
8.75	7	1.25
10.50	7	1.50
12.25	7	1.75
14.00	7	2.00
15.75	7	2.25
17.50	7	2.50
19.25m	7	2.75
21.00m	7	3.00

It is observed that the deflection increase with the increase in span to width ratio (Aspect ratio). Variation of deflection under dead load and IRC Class A load is shown in the Figure-2 (a) and (b) respectively.

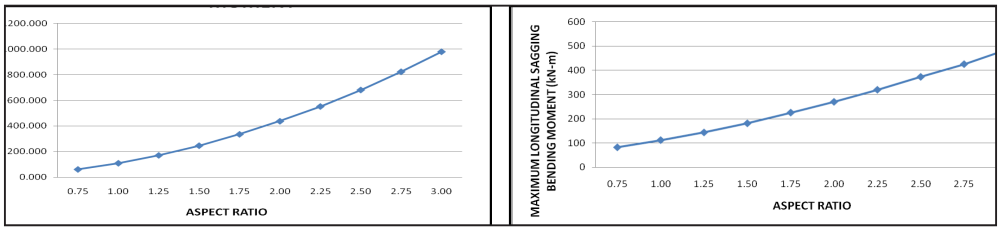
3.1 Variation of Deflection



(a) **(b)**

Figure-2 Variation of deflection

3.2 Variation of Longitudinal Sagging Bending Moment

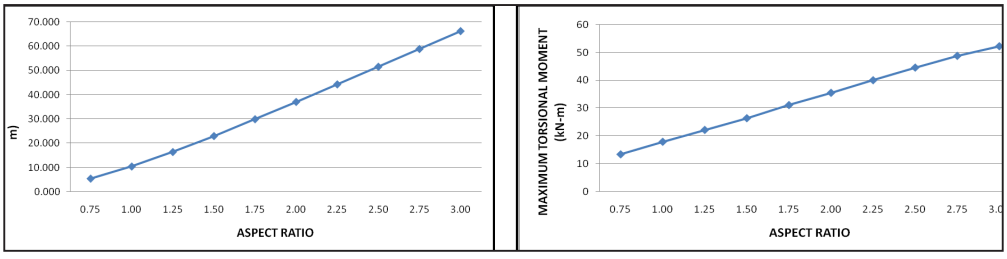


(a) **(b)**

Figure-3 Variation of longitudinal sagging bending moment

It is observed that longitudinal sagging bending moment increases with increase in aspect ratio. And the effect under dead load and IRC Class A load is shown in the Figure-3(a) and 3(b) respectively

3.3 Variation of Torsional Moment



(a) **(b)**

Figure-4 Variation of torsional moment

The variation of torsional moment with respect to Aspect ratio for dead load and IRC Class A load is shown in the Figure-4.

4. VIBRATIONAL ANALYSIS

Natural frequencies are obtained by carrying out vibration analysis of different cases mentioned in previous sections. Figure-5 and 6 shows variation in natural frequencies of bridge deck with respect to the varying aspect ratios

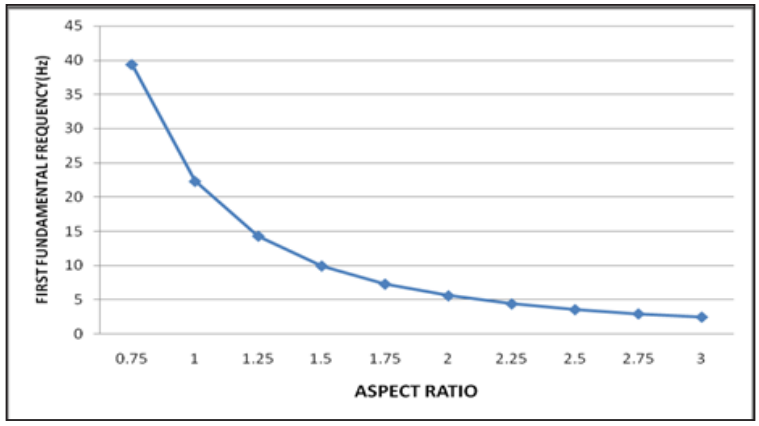
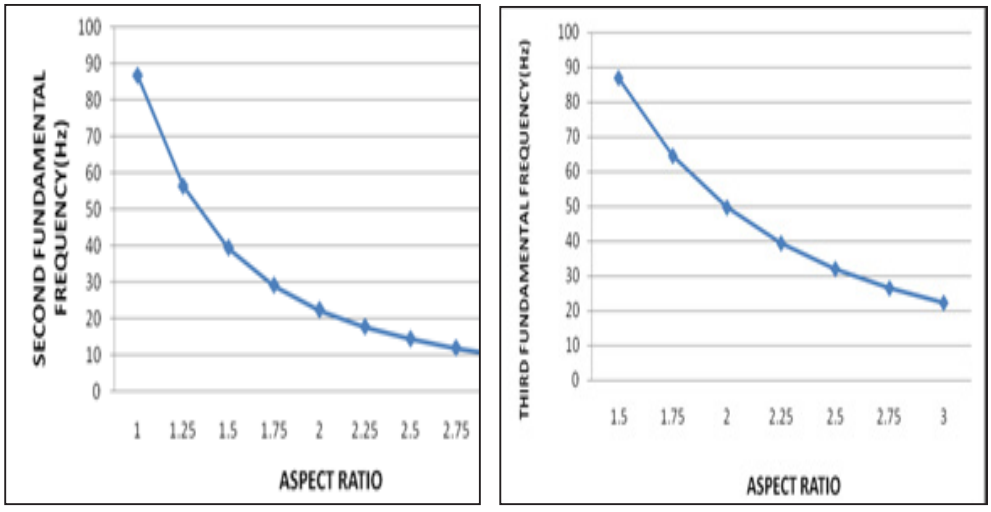


Figure-5 Variation of first fundamental frequency of bridge deck slab with aspect ratio



(a) **(b)**

Figure-6 Variation of second and third fundamental frequency bridge deck slab with aspect ratio

4.1 Mode Shapes

First three Mode shapes for the aspect ratio 1.0 are shown in Figure-7(a),7(b) and 7(c) respectively.

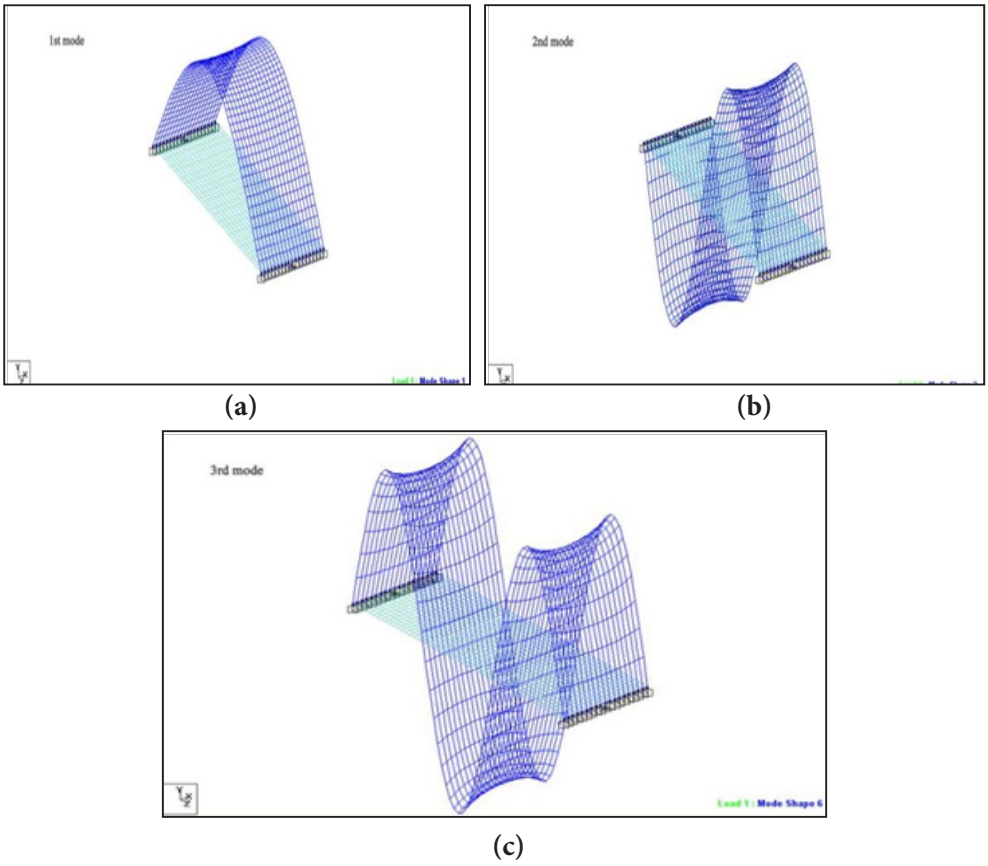


Figure-7 First three mode shapes for 1.0 aspect ratio of bridge deck slab.

5. CONCLUSIONS

Based on the Static evaluation and vibrational evaluation of Bridge deck slab, the following conclusions are drawn.

- The maximum deflection for the deck slabs increases with increase in aspect ratios for all loading situations.
- The maximum longitudinal sagging bending moment for the deck slabs increase with increase in aspect ratios for all loading conditions.
- The maximum torsional moments increase with increase in aspect ratios for all loading situations.
- As aspect ratio will increase first fundamental frequency decreases.
- As aspect ratio increases second fundamental frequency decreases.
- As aspect ratio will increase third essential frequency decreases.

Legend

μ	=	Poisson's Ratio
ρ	=	Density
B	=	Right Width in m
E	=	Modulus of Elasticity
L	=	Span Length in m

REFERENCES

1. Lingkunchen Lizhong Jiang and Liping Wang, Research on Seismic Response and Damping Effect for High-Speed Railway Seismic Isolated Bridge *Journal of Structural Engineering ASCE,* 2011, 1(5), pp. 163-167.
2. Zhang Yuling, Xin Xuezhong and Cui Xin , Updating Fatigue Damage Coefficient in Railway Bridge Design Code in China *Journal of Structural Engineering ASCE, 2012,* 17 (5), pp. 788–793.
3. Rongqiao Xu and Binleishao, A New Beam Element for Incremental Launching of Bridges, *Journal of Bridge Engineering ASCE,* 2012, 17 (5), pp 822-826.
4. Yiqiang Xiang and Zhengwei Ye, Methods of Calculating Wind Loads on Long-Span Girder Bridges with Tall Piers and Comparison *Journal of Structural Engineering ASCE.*2012, 17, (5), pp. 813-821.
5. Ardalan Sherafati, Reza Farimani and Atrod Azizinamini., Effect of Concrete Slab on Shear Capacity of Composite Plate Girders Under Positive Moment *Journal of Bridge Engineering ASCE,* 2013, 18 (2), pp. 89-98.
6. Gongkang Fu, Lang Liu and Mark D., Multiple presence factor for truck load on highway bridges, *Journal of Bridge Engineering ASCE,* 2013 18 (3), pp. 240-249.

A solution to Energy-Balanced Routing and Data Aggregation based on Artificial Bee Colony and Ant Lion Optimization for LEACH Protocol

Devika G.[1]✉, Ramesh D.[2], Asha Gowda Karegowda[3]

[1]Research Scholar,SSAHE,Agalakote,B.H.Road, Tumakuru572107,Karnataka, India
[2] Dept. of CSE, SSIT, Tumakuru 572105,Karnataka, India
[3] Dept. of MCA, SIT, Tumakuru 572103, Karnataka, India
✉devika@gmail.com

Abstract

One among most influenced technology in the digital era is Wireless Sensor Networks (WSN). It is a collection with numerous homogeneous or heterogeneous low cost low power sensors basically meant to garner information from any geographical location. WSNs are constrained to limited battery power, henceforth there is a dire need to optimally utilize WSNs energy so as to enhance network life span. In this context, cluster based routing algorithm is suitable solution. Furthermore, the computational bio-intelligence algorithm can be applied in an effective way for routing algorithm. This research paper is presenting optimizing LEACH clustering algorithm using meta-heuristic algorithm, Ant Lion Optimization (ALO) to enhance network life and compares with another implemented clustering algorithm Artificial Bee Colony (ABC). Both ABC and ALO have been applied separately for selection of both Cluster Head (CH) and Vice Cluster Head (VCH). VCH will replace CH if energy level drops beneath the user specified threshold value, hence avoids frequent reconstruction of clusters in WSN finally to extend the lifespan of WSN. The performance of proposed work is assessed through consumption of energy, throughput and retained alive sensor nodes. The simulation work confirms that ALO optimized LEACH outperforms ABC optimized LEACH.

Keywords: *Energy Optimization, LEACH, WSN, Artificial Bee Colony,Ant Lion Optimization*

1. INTRODUCTION

Research advancements in an embedded technology have led to advancement in devices used for sensing in different application in terms of capacity, size, and range of access for environment. Sensors sense data and communicate to

either nearby nodes or directly to Base Station (BS). The sensors in a large collection of test bed forming groups of sensors as depicted in Figure-1. In order to avoid redundancy, data aggregation is performed before transmitting data to BS. The increasing size of Wireless Sensor Networks (WSN) demands for an efficient deployment and routing. The detailed survey of proposed few methods on various routing algorithms are included in [1]. Among the various routing algorithms based on clustering LEACH. is the most predominant one and is applicable for linear selection of clusters with energy uniform distribution among sensor [2]. Further the uniform energy distribution leads to earlier death of few sensors in network.

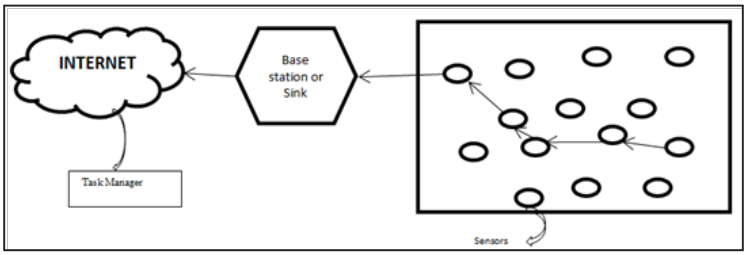


Figure-1 Typical WSN architecture

Henceforth, many works are proposed to enhance LEACH in terms of (i) optimal selection of cluster head and (ii) formation of cluster [3, 4, 5]. The selection of Cluster Head (CH) is recognized as NP problem [6], at this juncture meta heuristic algorithm are found to be promising one from literature survey [7]. Solution of bio inspired algorithms can be grouped into swarm intelligence (based on bio inspired agents such as ant, bee, wolf, cuckoo, ant, lion etc.,) and evolutionary computing (using genetic algorithm) [8, 9, 10].

In cluster based routing algorithms based WSN, the selection of CH is one of the major issue to balance energy consumption in the network. However, avoiding frequent selection of CH minimizes requirement of resources as it is of major issue in context to energy imbalance and minimized network lifetime. Most of the work do not provide stability among exploitation and exploration. Henceforth, the application of meta-heuristic algorithms shows potential use in maintaining the degree of balance between current exploitation and exploration. In this paper, two meta-heuristic algorithms Artificial Bee Colony (ABC) and Ant Lion Optimization (ALO) have been applied for improving LEACH performance so as to achieve enhanced network lifespan. ABC optimization is identified to be a popular method over the recent years with an added capability of introducing effectiveness during the task of identification of

CH nodes to generate predominant results. Ant Lions are associated to family of myrmeleontidae and well known as doodlebug in larval stages, during this state antlions construct funnel-shaped mines in sand. It digs and hides itself at the bottom to consume its prey. This special smart behavior of antlions inspired in formulation of meta-heuristic to solve many optimization related problems

The main objective of this work, is to propose a selection of both Vice Cluster Head (VCH) and CH for LEACH algorithm using ABC and ALO algorithms. The VCH are identified to replace CH in situations where CH's energy level falls below specified value and henceforth avoids frequent task of CH selection and cluster formation, which inturn leads to increased network lifespan. Among the two meta-heuristic methods, the ALO based LEACH operates good compared with ABC based LEACH.

The remaining sections includes design challenges in section 2, reviews of similar works are briefed in section 3, section 4 gives details of proposed algorithms Vice Artificial Bee Colony (VABC) LEACH and Vice Ant Lion Optimization (VALO) LEACH followed by results and discussion in section 5 and conclusion in section 6.

2. WIRELESS SENSOR NETWORKS DESIGN CHALLENGES

Mobile ad-hoc networks and WSN exists with similarities in terms of few features such as collection of nodes, communication requirement, mode of operations and others; there are also distinct features among them which include: traffic pattern, memory, power supply, functions to resources, operating bandwidth range, magnitude of data, need of data aggregation, detect information, and remove excess amount data. Major challenges of WSN are discussed in brief below.

Calculations and storage requirements: Each sensor nodes has CPUs prepared with tiny low processing power along with memory limitation. Hence there is a need to develop routing algorithms with minimal processing to achieve maximum functionalities of WSN.

Automaticity and self-organization: Since WSN is natured by dynamic capability, few nodes become non-operational in many operational phases. Hence the routing algorithms must be proactive in nature to adapt enough to continue data collection for a longer period with the remaining active nodes.

Energy efficiency: The major critical part of sensor is efficient utilization of power in critical aspects of operative period of WSN is to support longer network lifespan. Therefore there is need to develop routing protocols which consume minimum energy for both data transmission as well as for finding optimal route. Energy usage needs to be in balance with the functionalities design.

Scalability and reliability of network: In WSN thousands of sensors will be deployed normally for time critical applications. In this direction routing protocols design should consider for Quality Of Service (QOS) parameters such as, scalability and reliability. Multi-hop WSN will minimize interference in communication and also avoids unexpected failures.

Information security of network: The inadequate network with security measures may lead to violations negotiations of QOS. So, secured data transmission is vital service of WSN. The physical design of WSN is supported for broadcast way of communication which is inherently insecure, hence demanding secured routing algorithms.

3. LEACH BASED EXISTING BIO-INSPIRED ALGORITHMS

The Author have elaborated concerning few of WSN bio-inspired, efficient for routing and data aggregation in terms of energy related works carried by research fraternity discussed in this section. LEACH [11] a state-of-art protocol of WSN by many researchers. In many research works LEACH proved a hierarchical method which conserves energy to minimize problems in traditional techniques to provide equilibrium for energy to carry on all operations of WSN. The data being transmitted is also reduced by data aggregation/data fusion leading to minimum energy consumption. The selection of CH is dynamic for all intervals and CH is considered to be having more resources (eg: energy, processing power) among all its neighbors and on its previous history of operating as CH with frequency [12].

In LEACH function threshold T(n) is computed using P/1-P(r mod 1/P) by eligible nodes, other wise 0 will be assigned. In the function given 'N' represents number of nodes, P indicates probable rate of node getting select as 'CH', 'R' specifies round number, and nodes which are not being selected as CH till will be in NN for the last 1/P rounds count. The nodes will get assigned values between 0-1, hence the nodes getting selected as CH will normally have value between 0-1 and the chance of getting selected as CH will be more for T(n) being less then sum of all nodes. Further, node identified as CH starts to

send message to all nearby nodes, so as to take decision to join a particular cluster. In order to avoid collisions during message transmission, Carrier Sense Multiple Access (CSMA) is applied. CH introduces and transmits a Time Division Multiple Access (TDMA) in corresponding schedule of transmission to broadcast to respective clusters in allotted time schedule of TDMA [13].

The merit of using TDMA is its capability to move to idle state whenever nodes are futile. The clusters are formed applying dispersed procedure as node to become CH will be originally selected value of 'P' and remaining nodes determine to join to particular cluster based in minimal energy to communicate. The CH role will be handed over to other eligible nodes at regular intervals [14]. Many works have been carried on from then to optimize usage of energy within WSN using LEACH as summarized in [3]. Currently bio-inspired or computational intelligence algorithms are being used in identification of efficient nodes as CH with in each cluster [15]. Swarm intelligence based Particle Swarm Optimization (PSO) algorithm has been devised in construction process of clusters for WSN in [16].

ABC based CH selection process to improve efficiency with estimation of multi-objective fitness function utilized in [13]. ABC-based least hop count for the purpose of provisioning potential data transmission was proposed for enhancing the rate of data and energy dissipation in an efficient way [17]. The distance and energy parameters considered in selection of CH using multi-dimensional features of sensor nodes to evaluate CH based on PSO model proposed in [18]. Selection of CH based on residual energy, inter-distance between sensor nodes and intra-distance between each sensor node and the base station based on Cuckoo and Harmony Search-based Cluster Head Selection Scheme (CHS-CHSS) was proposed for balancing the node energy in [19]. In [20], the Discrete Ant Lion Optimization (DALO) algorithm functionalities have been engaged in gathering of data by sink, sink operates by moving to place of sensors.

4. ARTIFICIAL BEE COLONY AND ANT LION OPTIMIZATION

This section briefs on Artificial Bee Colony and Ant Lion Optimization.

4.1 Artificial Bee Colony Algorithm

ABC is a meta-heuristic algorithm impersonator of foraging behavior of bees. ABC involves three types of agents to perform its tasks: i) scout, ii) onlooker and iii) employee bees. ABC being used to work in network to work in phases of operations, such as i) initialization, ii) employee, iii) onlooker and iv) scout phases. The ABC population will be initialized in initialization phase. Based

on solutions of previous stages the fitness of each agent will be calculated in employee phase. In onlooker phase, agents assigned with highest eligible value will be nominated as cluster head and finally in scout phase decision is taken to enter next iteration or not. The ABC flow chart is shown in Figure-2(a).

4.2 Ant Lion Optimization Algorithm

ALO is a meta-heuristic algorithm impersonator of hunting ant lions. The random walk of ants will be affected because of antlion in a network. Fitness

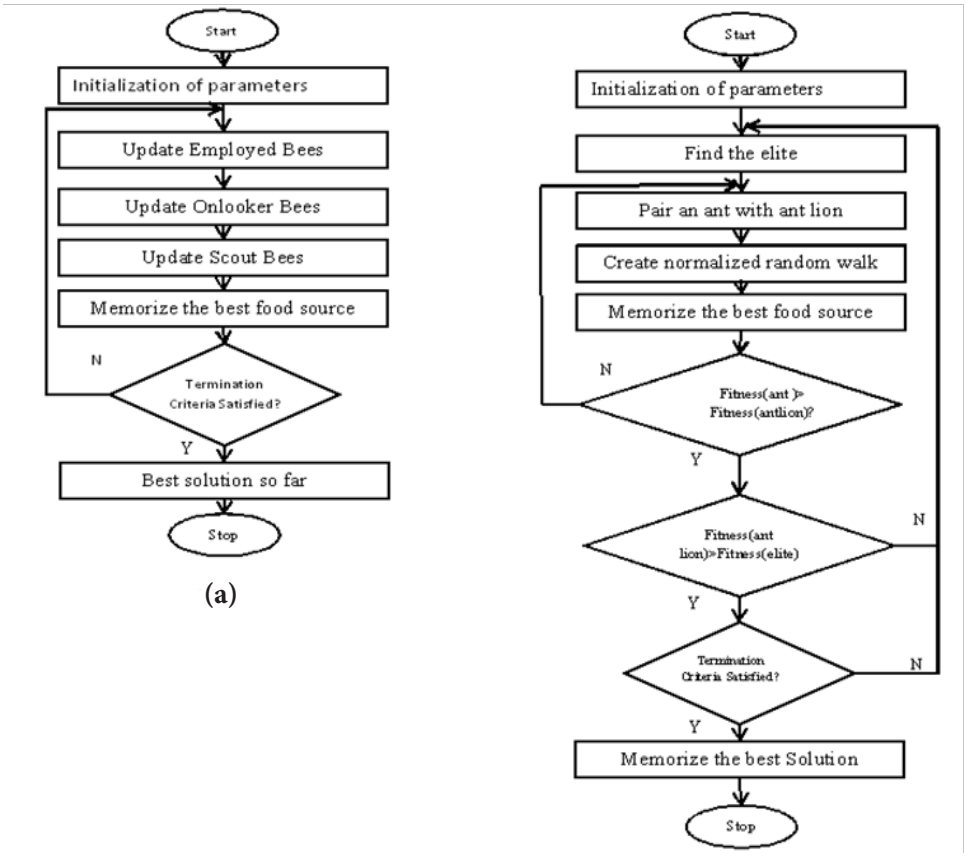


Figure-2 Flow chart of (a) ABC (b) ALO

of each ant lion will decide effectiveness of agent trap with the use of elitism as cluster head. ALO optimization algorithm consists of phases such as initialization and catching followed by rebuilding of trap. During initialization phase trap will be built to identify highest fit agent. In next catching and rebuilding phase, the decision will be taken to build new trap or not. The flow chart of ALO is shown in Figure-2(b).

5. PROPOSED WORK

In order to analyze VABC and VALO algorithm for WSN few reasonable assumptions were made in network and energy model are briefed. WSN network topology will be static and connected. The transmission distance between neighboring nodes will be symmetric with restriction on transmission length. According to requirements of network data aggregation functions will be initiated to operate as of requirement.

Network Model: WSN is assumed to work similar to graph: G(V,E) with 'V' indicates number of sensors and 'E' represents communication link from node to node as an undirected graph. In proposed work, placement of sensors is randomly spaced in the square shaped monitored regions. 'n' number of source nodes are considered with base station(BS) positioned at (0,0) for purpose of simulation. The data are generally transmitted from sensor at threshold value $d_0 = \sqrt{\frac{E_{FS}}{E_{MP}}}$ in the equation E_{fs} specify consumption of energy required to transmit one bit in free space and for multipath is denoted in E_{mp}.

Energy Model: The key issue of WSN is energy consumption. Normally sensors are battery operated and recharging is difficult in most of applications once depleted. The required energy for communication between sensor nodes to BS is normally more. Operations such as transmission, reception, sensing and aggregation shares more consumption of energy. Model of Shiozaki [13] assumed for energy, the radio communication assumed to consume E_{elec} = 50nJ/bit to transmit or receive in a circuit. Assumed value for amplifier E_{amp} = 100pJ/bit/m^2 for transmitting amplifier. Energy loss of d^2 is assumed in a network where'd' indicates detachment from sender to receiver,E_{elec} indicates other signal related operations and E_{amp} relay on receiver location. The transmission of message length of k-bit with 'd' length between nodes assumed in the model, consisting of three type of sensor nodes and is computed using equation (1)

$$E_{Tx}(k,d) = \begin{cases} E_{elec} * k + E_{amp} * k * d^2 \\ E_{elec} * k + E_{amp} * k * d^4 \\ E_{elec} * k + E_{amp} * k * d^6 \end{cases} \quad (1)$$

.

The channel for communication is assumed to be symmetric radio channel in transmitting signal. The energy consumption for receiving message is computed using equation (2). The data aggregation energy requirement is

computed using equation (3). The required amplification is computed by using equation (4). In addition energy in idle state and sensing are also considered.

$$E_{RX}(N; d) = E_{ele}N \tag{2}$$

$$Eelec = E_{TX} + E_{RX} \tag{3}$$

$$E_{amp} = \begin{cases} E_{fs}d^2 \\ E_{fs}d^4 \\ E_{fs}d^6 \end{cases} \tag{4}$$

5.1 Working Principle of VABC LEACH Protocol

Artificial Bee Colony is a bio-inspired meta-heuristic algorithm which simulates bees foraging comportment. ABC consists of agents who can be categorized as scout, onlooker and employee bees. The network works in different phases of operations such as initialization, employee, onlooker and scout phases. The ABC population will be initialized in initialization phase. Based on solutions of previous stages the fitness of each agent will be calculated in employee phase.

In onlooker phase, agent with highest fitness value among agents will be selected as cluster head and finally in scout phase decision is taken to enter next iteration or not. The proposed novel VABC algorithm is an optimization technique designed as of conventional ABC technique and concentrates mainly on selection of CH and VCH in an energy efficient manner. VABC involves classes of bees to perform its functions employed, onlooker and scout bees.

VABC works with two operational phases as of LEACH; (i) set-up and (ii) steady. CH and VCH identification and formation of clusters are performed in set-up phase. The current status of every sensor will be collected considering as ABC's employee, formation of clusters with selection of CH and VCH as in ABC's onlooker bee and finally, steady phase data sensing, transmission and aggregation of steady phase actions are similar to ABC's scout bee.

The CH will be replaced by VCH once CHs energy falls below threshold value or sensor goes off. Working process of VABC LEACH protocol is presented step by step in Algorithm 1.

Algorithm 1: Pseudocode of proposed VABC LEACH algorithm

Input: set of nodes X={x1,x2….xN}//for number of nodes N, and initial resource values of all sensors
Output: CH and VCH node identification//for number of clusters S

Step 1: Initialize the parameter values to the Number of CHs &VCH, No. of bees
Step 2: Initialize the positions of agent//sensor
Step 3: Evaluate the nectar amount of the food sources// Objective function
Step 4: Deploy sensor nodes within the prescribed layout using rand() function and place BS at (0,0) co-ordinate.
Step 5: Compute the distance between the all the sensor nodes, distance to BS.
Step 6: For each employee bee
Calculate the fitness value of bees
End for
Step 7: Apply the greedy selection process
For each onlooker bee
Choose a solution xi depending on distance to BS
Produce new solutions CH
Calculate the fitness
End for
Apply the greedy selection process other than CH nodes
For each onlooker bee
Choose a solution xi depending on distance to BS
Produce new solutions VCH
Calculate the fitness
End for
Step 8: Sort nodes other than CH and VCH in each CH to form cluster
Step 9: Perform steady phase functions
Step 10: If N>N_threshold,
t=t+1, goto step 2
End if
Step 11: Stop

5.2 Working Principle of VALO LEACH Protocol

Ant lion optimization algorithm is a computational meta-heuristic intelligence algorithm, which impersonates the comportment of hunting ant lions [20]. Larvae (hunting prey usually ants) and adult (3-5 weeks used for reproduction) are the two major stages in the lifespan of antlion. Ants perform a random search, antlions can hunt ants using right traps to hold on. The random search of ants benefits the antlions to achieve global optimization solution. Fitness of each ant lion will decide effectiveness of agent trap with the use of elitism (best fit antlion) as cluster head. ALO optimization algorithm consists of phases such as initialization and catching followed by rebuilding of trap. During initialization phase, trap will be built to identify highest fit agent. In next catching and rebuilding phase, the decision will be taken regarding to build new trap or not.

From reviewed research work, the conventional ABC possess low convergence rate and higher latency and ALO also retain the same problem in WSN as it requires frequent reformation of cluster. Hence, in the proposed work, VCH strategy is applied to resolve problem and to extend lifetime of ALO based WSN. The proposed VALO algorithm is a novel optimization technique based on conventional ALO technique mainly meant for selection of CH and VCH in an energy efficient manner.

In proposed VALO LEACH algorithm, after sensor node deployment is done within the specified network, each sensor is considered as antlion/ant. Energy of sensor, existence of node within radio coverage, distance between sensor and neighbors and distance to BS parameters are taken into consideration in identification of CH and VCH on fitness value. The algorithm works similar to basic LEACH. The identification of CH and VCH, and formation of cluster is based on ALO. Algorithm-2 provides complete operational steps of VALO LEACH algorithm.

6. EXPERIMENTAL RESULTS

The results of proposed VABC LEACH and VALO LEACH algorithms implementation details are briefed in this section. The simulation detail of network consisting of 100 nodes is summarized in Table-1. The proposed algorithms are compared with traditional LEACH, Meta heuristic ABC LEACH (for only selecting CH and no VCH) and ALO LEACH (for selecting only CH and no VCH) protocols. The investigation of algorithms analyzed using alive nodes count, throughput (terms of packets sent) and energy consumption.

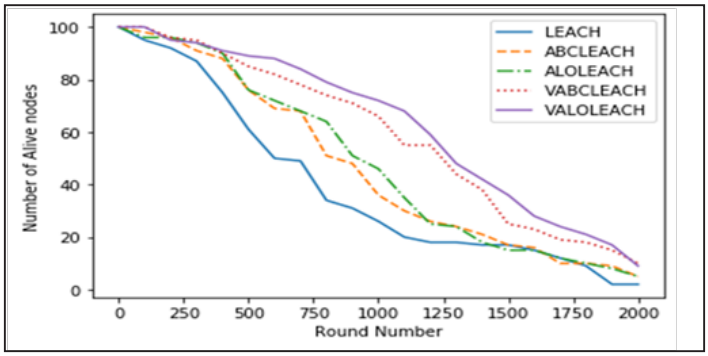


Figure-3 Plot of number of alive nodes

Figure-3 depicts simulation of five methods for alive nodes number in different rounds. The number of alive nodes was almost same during initial 200 rounds for all five methods. The alive nodes are nearly same in ABC and ALO LEACH protocols in almost all rounds. Overall performance of VALO LEACH is best compared to LEACH, ABCLEACH (with only ABC used for selection of only CH and not VCH), as well as ALOLEACH(with ALO used for selection of only CH and not VCH).

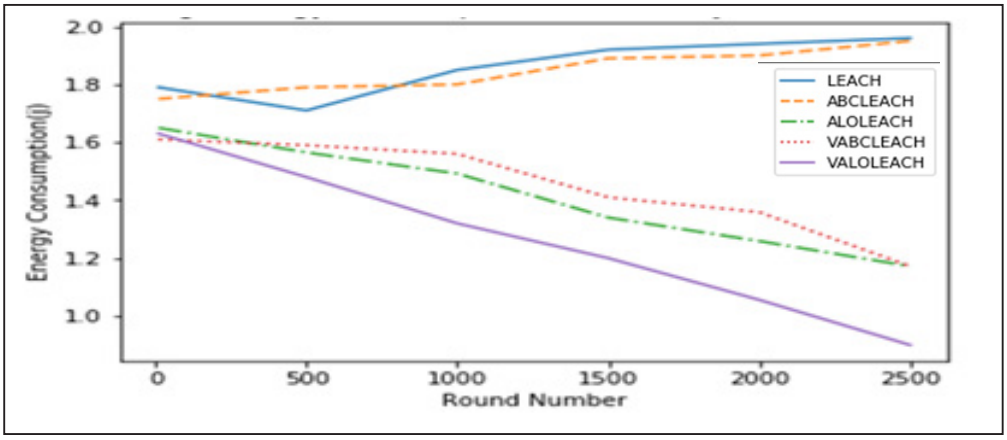


Figure-4 Plot of average energy consumption of proposed conventional protocols

Figure-4 indicates remaining energy round wise of a network for all algorithms. The initial energy consumption is almost same by all protocols only about 5% of performance improvement can be viewed in proposed algorithms. The graph clearly indicates a VALO LEACH method is losing energy at slower rate compared to conventional LEACH and ABCLEACH. Among all simulated algorithms proposed methods VALO LEACH shows better performance with very low energy consumption on the later rounds.

Table-1 Network simulation parameters

Parameter used	Value Set
Region of sensor fields	200m x 200m
Base Station	Base Station
Total Number Of Sensor Nodes(TSN)	100
Maximum number of rounds(Max Rounds)	2500
Initial energy of the sensor nodes	0.5 J
Packet size	4000 bits
Factor of Scaling(8)	0.5
Receiver energy	$5*10^{-9}$ J
Transmitter energy	5*10 J
Amplifier energy consumption for smaller distance	103pJ/bit/m^4
Amplifier energy consumption for larger distance	103pJ/bit/m^4
Cluster head probability	5%=0.05
Control message size	32 bits
Ratio of advanced nodes adv	0.1
Energy factor for advanced nodes	0.5-1

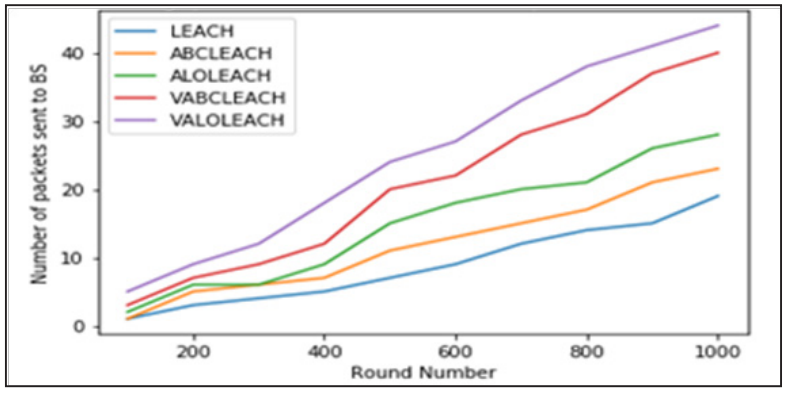


Figure-5 Plot of throuput of proposed and conventional protocols

Figure-5 depicts the performance of the five methods for work done through packets transferred to BS from CH nodes for different rounds. Comparison of throughput is over all measurement of information being forwarded to BS as packets. It can be noticed that VALOLEACH shows improved performance as round number increases. It is observed that ABC and ALO based LEACH showed better results when used for selection of both CH and VCH when compared to in absence of VCH.

6. CONCLUSIONS

This paper presents and compares two energy efficient routing protocol designed using hybrid bio-inspired computational intelligence algorithms. The VABC LEACH algorithm designed based on ABC and VALO LEACH algorithm based on principles of ALO. Among proposed methods VALO LEACH shows a remarkable improvement over VABC LEACH as well as other protocol for concert parameters such as throughput, low consumption of energy and alive nodes presence in network. The results confirm the significant role of VCH for the enhanced performance of proposed VABCLEACH and VALOLEACH when compared ABC and ALO used for only CH. VCH increases reliability and minimize energy consumption avoiding frequent reformation of clusters. In addition, the results prove that the meta-heuristic methods have enhanced the performance of conventional LEACH. As part of further research work, authors would like to explore many more bio-inspired computation intelligence algorithms with special interest on evolutionary based algorithms for improving performance of LEACH both in terms of throughput and overall network lifespan. Furthermore, author has planed to develop protocols which avoids computational load on BS by making WSN self -configurable and curative.

Legend

d	=	Transmission distance
E_{fs}	=	Specify consumption of energy required to transmit one bit in free space
E_{mp}	=	Specify consumption of energy required to transmit one bit for multipath
E_{elec}	=	Energy consumed to transmit or receive data
E_{ch}	=	Average energy of cluster
E_{thr}	=	Threshold energy
E_{amp}	=	Energy required for amplification
N	=	Number of nodes
$N_{threshold}$	=	Number of nodes set for threshold limit

REFERENCES

1. Devika G and Asha Gowda, Survey of WSN Routing Protocols, *International Journal on Applied Engineering Computing,* 2019, 11(1), pp.34-46.
2. Krishna M.B. and Doja M.N. Swarm Intelligence-based Topology Maintenance Protocol for Wireless Sensor Networks. *IET Wireless Sens. Syst.* 2011,1(4), pp.181–190.
3. Devika G and Asha Gowda Karegowda, A Pragmatic Study of LEACH and its descendant Routing Protocols in WSN. *International Journal of Computing Intelligence and Informatics,* 2015,4 (4), pp.300-307.
4. M.Ezhilarasi and V.Krishnaveni, A Survey on Wireless Sensor Network :Energy and Lifetime Perspective. *Taga Journal,* 2018, 14(6), pp.41-48.
5. Lucia Keledile., Ketshabetswe and Boyce sigweni, Communication Protocols for Wireless Sensor Networks: A Survey and Comparison. *Science Direct,* 2019, 5(5), pp.65-77.
6. Bharathy M.V. and Rao K.K.C, One-leap Fuzzy enabled Clustering Technique for under Water Wireless Sensor Networks to improve the Stability and Energy Exhation Rate of the Nodes .*J. Phys. Conf. Ser.* 2019, 1172, pp.08-12.
7. Devika G., Premasudha B G and Asha Gowda., A Comparative Study of Energy Efficient Hierarchical Wireless Sensor Network Protocols, *International Journal of Applied Research on Information Technology and Computing,* 2015,6(3), pp.173-179.
8. Adnan., Razzaque., Ahmed I. and Isnin I.F. Bio-Mimic Optimization Strategies in Wireless Sensor Networks. *Sensors,* 2013, 14(1), pp.299-308.
9. Asha Gowda Karegowda, Devika G and B. G Premsudha. A Pragmatic Study of Evolutionary Techniques Based Energy Efficient Hierarchical Routing Protocols - LEACH And PEGASIS. *International Journal of Applied Engineering Research,* 2016, 10(5), pp.274-285.
10. Domnguez-Medina C. and Cruz-Cortes, N. Routing Algorithms for Wireless Sensor Networks Using Ant Colony Optimization. *In: G. Sidorov, A. Hernandez Aguirre, C. Reyes(eds.) Advances in Soft Computing, Lecture Notes in Computer Science,Springer Berlin Heidelberg,* 2010, 6438, pp. 337-348.
11. W. B. Heinzelman., Application-Specific Protocol Architectures for Wireless Networks. *IEEE Transactions on Wireless Communications,* 2002, 1(4), pp.660-670.
12. Shankar T and Shanmugavel S. PSO Algorithm for Energy Efficient Cluster Head Selection in Wireless Sensor Networks, *Journal of Engineering Science and Technology,* 2014, 9, pp.246 - 260.
13. Mann, P.S. and Singh S. Artificial Bee Colony Metaheuristic for Energy-Efficient Clustering and Routing in Wireless Sensor Networks. *Soft. Comput.* 2016, 21 (22), pp.6699–6712.
14. Abdulsalam, Hanady M. and Layla K. Kamel.W-LEACH: Weighted Low Energy Adaptive Clustering Hierarchy Aggregation Algorithm for Data Streams in

Wireless Sensor Networks. *In: Data Mining Workshops (ICDMW), IEEE International Conference,* 2010.
15. Wang, X., Wang, S., and Ma, J. J. An Improved Co-Evolutionary Particle Swarm Optimization for Wireless Sensor Networks with Dynamic Deployment. *Sensors.* 2007, 7, pp.354–370.
16. S. Mirjalili. The Ant Lion Optimizer. *Elsevier Advances in Engineering Software,* 2015, 83, pp.80-98.
17. Kaur, S. and Mahajan, R. Hybrid Meta-Heuristic Optimization based Energy Efficient Protocol for Wireless Sensor Networks. *Egypt. Inf. J.* 2019,19 (3), pp.145–150.
18. Vijayalakshmi and P. Anandan. A Multi Objective Tabu Particle Swarm Optimization for Effective Cluster Head Selection in WSN. *Cluster Computing, Cluster Computing Springer,*2018, 5, pp.352-365.
19. Gupta G.P. and Jha S. Integrated Clustering and Routing Protocol for Wireless Sensor Networks using Cuckoo and Harmony Search based Metaheuristi Techniques. *Eng. Appl. Artif. Intell,* 2018, 68, pp. 101–109.
20. Yan and B. Wang, An Adaptive WSN Clustering Scheme based on neighbor hood Energy Level . *IEEE 3rd Information Technology and Mechatronics Engineering Conference (ITOEC),* 2017, pp.1170–1173.

A Novel Cost-effective Real Time Technique for Breathing Rate Monitoring in New Born Babies for Neonatal Care

Purnima P. S.[1]✉ and Suresh M.[2]

[1]*Research Scholar, SSAHE, Agalakote, B.H. Road, Tumakuru 572107, Karnataka, India*
[2]*Professor, Dept. of ECE, SSIT, Tumakuru-572105, Karnataka, India*
✉purnima.p.s.2015@gmail.com

Abstract

A healthy baby is a sign of a developed society, country or economy; it is very much important to keep a close watch on the health conditions of a newborn. The factor of abnormal breathing rate in a newborn can lead to a breathing disorder during sleep which is also termed as sleep apnea and is usually more common in premature babies. The primary cause of this abnormal breathing rate during sleep can be an immature nervous system, lung problems, heart or blood vessel problems etc. Hence, continuous and intense monitoring of breathing rate of newborn is very much needed. Thus, this paper presents a real-time and low-cost method that will monitor a newborn for detecting abnormal breathing rate. In this non-invasive method, a simple microphone is kept near the nostrils of the child and breathing rate is monitored. Here the microphone senses the breathing signal from the neonate. Next, the noises present in the audio signal are removed by specialized software. Finally the breathing rate is counted within specific time intervals for the purpose of detecting any abnormality in the newborn baby. This application has been implemented in MATLAB software. A large number of breathing samples have been collected from neonatal care units of various hospitals and clinics. This low cost, and real time application can be incorporated in neonatal care units of various hospitals and clinics which can prove to be very effective in detecting abnormal breath rate in newborn babies.

Keywords: *Neonatal Care, Baby Monitoring, Breath Sensor.*

1. INTRODUCTION

According to World Health Organization(WHO), yearly 41% of newborn babies die in first 28 days of their birth. The scene is worse in developing countries where newborn babies are deprived in receiving proper care just after their birth. If proper healthcare facilities can be provided to newborn babies in first

seven days of their life, a great amount of newborn mortality can be prevented. As a developing country Neonatal Mortality Rate (NMR) is a burning issue in the Indian context. Though the rate of infant mortality has been slowed down by a good amount from 2008 to 2018, still it remains a matter of great concern in Indian context. A statistic fromFigure-1 shows that in India the infant mortality rate of 49.4 per thousand live births in 2008 has been reduced to 29.9 per thousand live births in 2018.

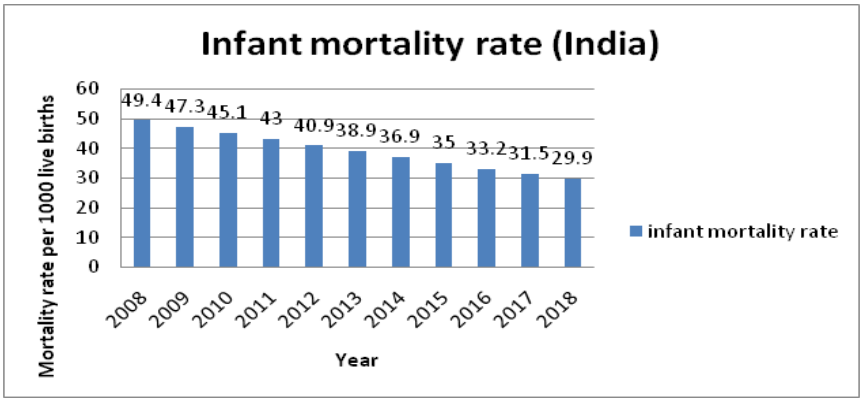


Figure-1 Infant mortality rate in India from 2008 to 2018

A neonate or a newborn baby is actually a baby whose age is under 28 days. This is a crucial period of newborns life because this is a high-risk time when a child's death is highly possible. There are three major causes behind neonatal death that has been observed worldwide. They are infections in different organs of the infant contributing to 36% of neonatal death, premature birth contributing to 28% of neonatal death and birth asphyxia contributing to 23% infant death worldwide. In Indian context, 78% of newborn death allover India are caused due to premature birth and inadequate weight at birth, infections in the newborn and birth asphyxia and trauma [1].

The lack of breathing in a newborn can gives rise to apnea symptoms in the infant. It is a medical condition observed in newborns where the incident of stoppage of breathing for some period of time occurs in the newborn, it is more common in premature newborns. Pausing of breathing process during sleep of an infant is termed as sleep apnea. It is a serious medical condition as it can lead to poor development of the baby and abnormal heart rate. Partial pausing of breathing process is termed as "hypopneas" and complete pausing is apnea. Thus, a close and consistent watch to the infant's health is very much mandatory.

There are different methods for detecting apnea in infants but constant monitoring of the breathing rate is one of the important ways for detecting sleep apnea. In general, the normal breathing rate of a neonate is 30 to 60 breaths in minute and 20 breaths per minute during sleep. In 20 seconds, duration, if there is three or more effortless breaths, then it is normal breathing for neonates. But if there are symptoms of cessation of normal breathing process for more than 20 seconds then it can be a symptom of apnea.

The neonates having less than 34 weeks of gestation duration must be constantly monitored for abnormality in breathing for a minimum of seven days. In general, an apnea monitoring device contains an alarm which indicates an emergency condition like cessation of breathing process for a long duration. The neonate's sleep apnea monitoring devices can be classified into three categories: invasive and non-invasive sleep apnea detection devices, impedance-dependent devices and polysomnography devices [2]. The most primary non-invasive form of estimating the respiratory rate of a neonate is video imaging technique. In a non-contact method, a simple camera has been used along with an embedded application [3]. The video captured by the camera examines the up-down movement of the newborn's rib cage and determines the rate of respiration. Another similar video imaging method for neonatal respiratory rate detection uses magnification of infant's respiratory motion from chest movement along with filtering technique with respect to frequency [4]. For recognizing presence of apnea, cessation of breathing is detected by the aid of dynamic thresholding process. In a polysomnography acquisition of neonatal Respiration Rate (RR) estimation, video image has been aggregated [5]. Video enlarging is employed to magnify breathing movements followed by capturing of breathing signal by the aid of optical flow. After enhancement of signal quality, the breathing rate is estimated using Fourier Transform[6].

A different imaging technique has been proposed by the researchers, Here the thermography imaging technique has been employed and examined[7]. They have used the technique of image analysis and breathing pattern from an image has been detected by the use of continuous wavelet transformation method.

In addition, other non-invasive device, is a pressure sensitive mat (PSM),[8]. Analysis of PSM captured data has been carried out with respect to time and frequency domain and the researchers have demonstrated that

frequency domain operation gives more accurate result in estimating RR. The same authors have made an extension of their previous work where they have designed a neonatal RR analysis algorithm by considering uncertainty analysis which is vital in determining physiological parameters [9].

A contactless and real time newborn RR monitoring technique has been proposed, which uses ultra-wideband radar [10]. The radar captures respiratory signals from chest rib movements of the infant, a periodic location finding technique has been employed and apnea has been recognized by processing the RR signal captured. A wireless technique using Radio Frequency Identification (RFID) tag has been employed for monitoring RR of newborns by the researchers [11]. The RR is calculated by capturing the difference in strengths of the received respiratory signals corresponding to inhale and exhale. In a recent research work the researchers have evaluated the accuracy of impulse radio ultra-wide band radar for monitoring respiratory rate of the newborns [12]. though the infant movement can affect accuracy of the radar. A plethysmographic signal acquiring color camera has been employed for RR estimation of neonates [13]. The camera direction is to the rib cages of the neonate and captures the diaphragm image of the neonate. In another machine vision-based approach more than one digital vision and depth sensors have been employed for capturing breathing movement signals of the infant [14]. The authors have established the fact that accuracy of RR estimation enhances with increasing number of sensors used.A different non-invasive system has been developed for neonatal RR monitoring using white noise [15]. The smart speakers behaving as white noise machine which also allows comfortable sleep to the infant without interruption. The white noise emitted from the smart speakers is reflected by the newborn's body and received signals are analyzed for chest movement of the infant. From the above discussion it is concluded that various non-invasive, non-contact methods exist which monitor neonatal RR. But the primary importance should be given on designing and developing a method that is cost effective in implementation and can provide results in real time. Therefore, this paper focuses on designing and developing a very low-cost device for monitoring sleep apnea of infants that operates in real time.

2. METHODOLOGY

Figure-2 illustrates the overview of the system. A low cost and easily available microphone (headset) have been employed which is connected to a computer running MATLAB software as well as a specialized audio processing software. The microphone here acts as a sensor which detects the

breath of the baby as a 1D audio signal. Further, this microphone is directly connected to the laptop which has an audio recorder as well as specialized audio processing software which reduces the noise recorded during the process of sensing the respiratory audio signal. The algorithm in Fig-3has two major phases: removing noise from the captured neonatal audio signal for clear and distinct respiratory signal and counting breadth rate of the infant.

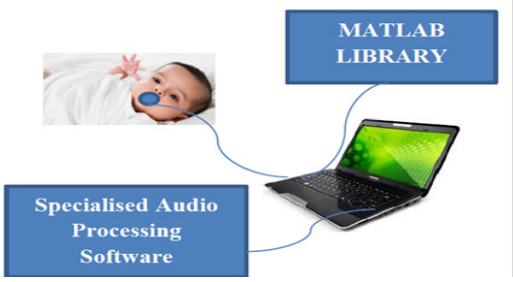


Figure-2 Proposed system model for neonatal RR estimation

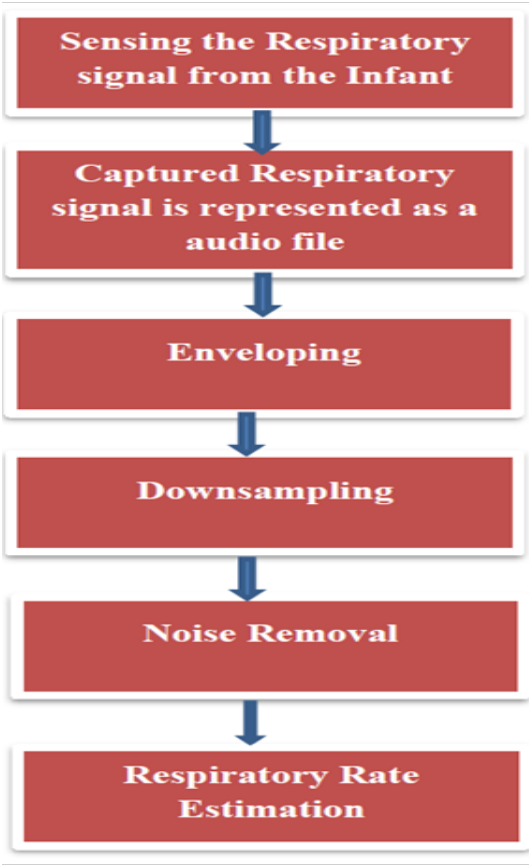


Figure-3 The neonatal RR estimation algorithm.

Step 1: Reading audio file of the captured neonatal RR signal

The user is asked to select the audio file corresponding to respiratory signal sensed using selector prompt. A function called "audio read" from MATLAB has been used to read audio file. One captured audio signal corresponding to a subject has been displayed below.

Step 2: **Enveloping**

Envelope is created around audio signal using peaks. For this purpose, 'envelope' function from MATLAB has been used.

Step 3: **Down sampling**

At this stage the number of data points in the signal is very large which will increase computation requirement and computation time. So algorithm will not be executed in real time. So down sampling is carried out to reduce unnecessary computations. As a result, the number of data points is reduced to an optimum level. Figure-4 and Figure-5 respectively shows the various forms of the signal after enveloping and down sampling processes being carried out.

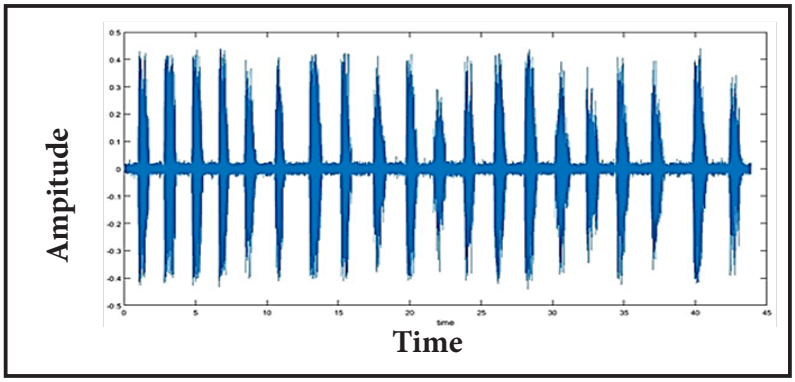


Figure-4 Audio Signal

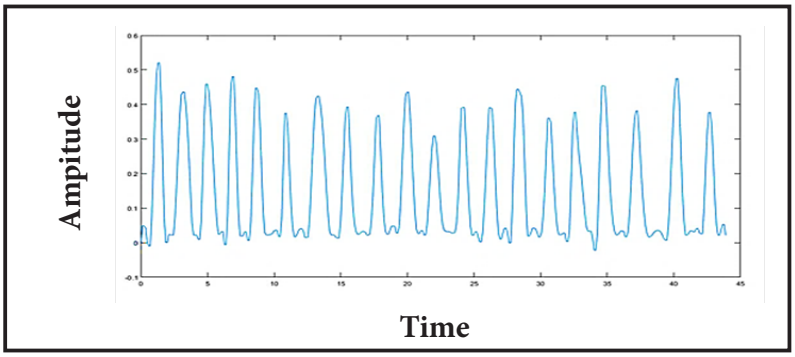


Figure-5 Form of the signal after enveloping and down sampling

Step 4: Noise removal

At this stage, strength of noise in the signal is very low in comparison to respiratory signal due to breathing. Hence, median filter technique has been applied to remove noise.

Step 5: RR estimation

Fast Fourier Transform is used to convert the signal from time domain to frequency domain. And frequency corresponding to highest peak in the signal indicates breath per second. Finally it is converted to breath per minute. In the Figure-6, the highest peak indicates the corresponding RR.

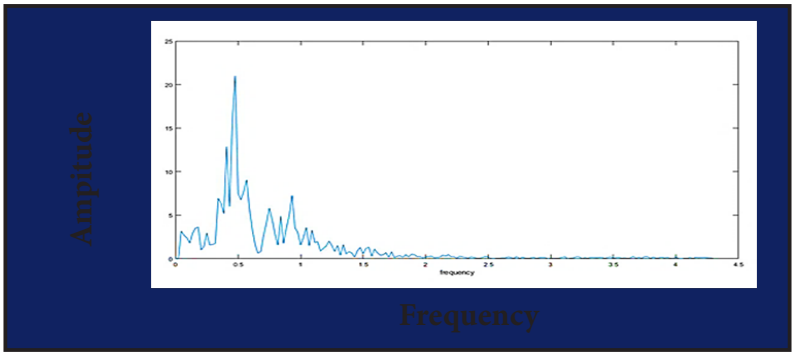


Figure-6 Respiratory rate corresponds to the highest peak

3.RESULTS AND DISCUSSION

A. Experimental setup

MATLAB version 2013 has been used to implement the proposed algorithm.

B. Dataset

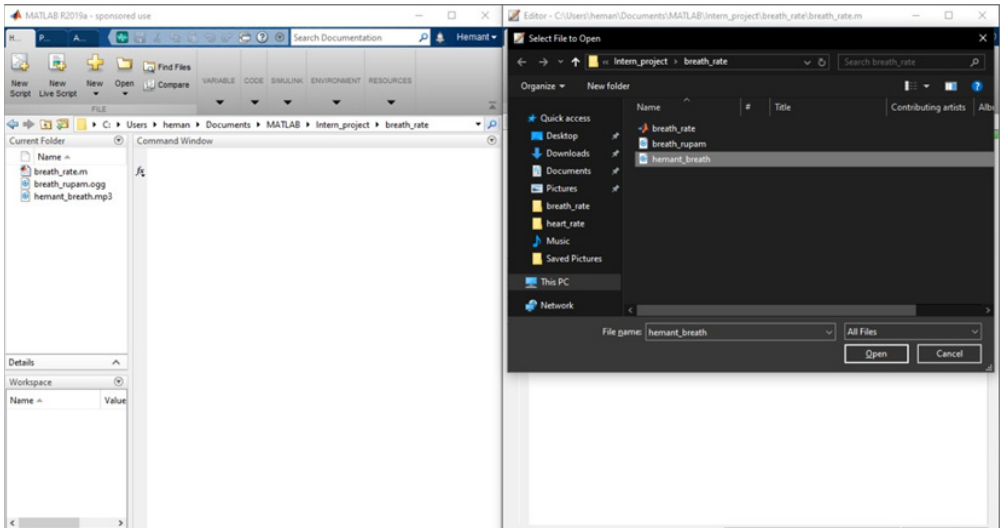
Breathing samples of five subjects have been collected from the neonates in different neonatal care units at different hospitals in Tumakuru and Bengaluru regions in Karnataka, India.

C. Demonstration

Demonstration of the running application has been depicted in the Figure-7 and Figure-8. The first screenshot indicates that the application is asking for real time respiratory signal data. The Fig-7 displays the respiratory rate determined by the application and Fig-8 shows, a sample of neonate RR result displayed which is 28.6352 times per minute.

D. Result 1: Comparison result of actual RR and counted RR.

TheTable- 1 illustrates the comparison result between actual RR and application counted RR with respect to five neonatal subjects.



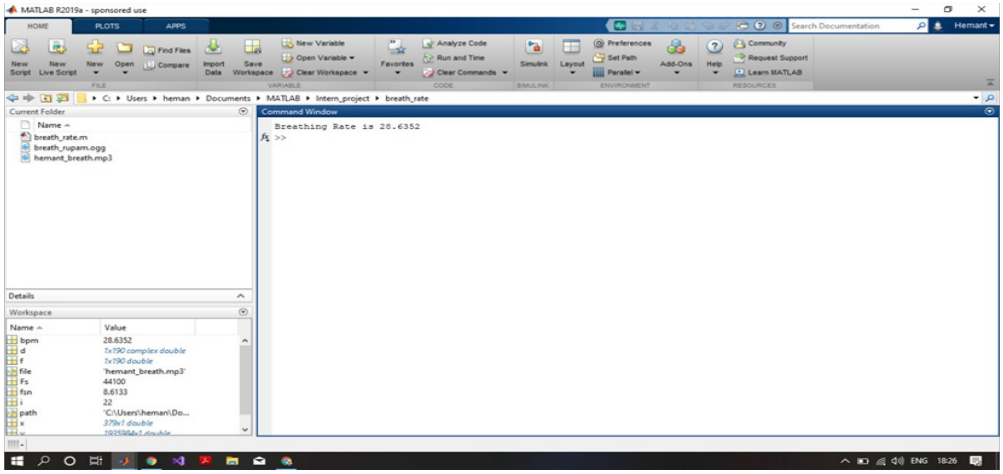


Figure-8 Application displaying captured RR of the neonate

Table-1 Comparison result of actual RR and counted RR

Sample Number	Counted Breath	Actual Breath	Accuracy Percentage
1	28.8	30	96.00
2	32.6	34	95.88
3	40.7	42	96.90
4	29	29	100
5	32	32	100

From Table-1 it can be observed that there are very low differences between application counted RR and actual RR. So, it can be concluded that the proposed method is very much accurate. The corresponding graph has been shown in Figure-9.

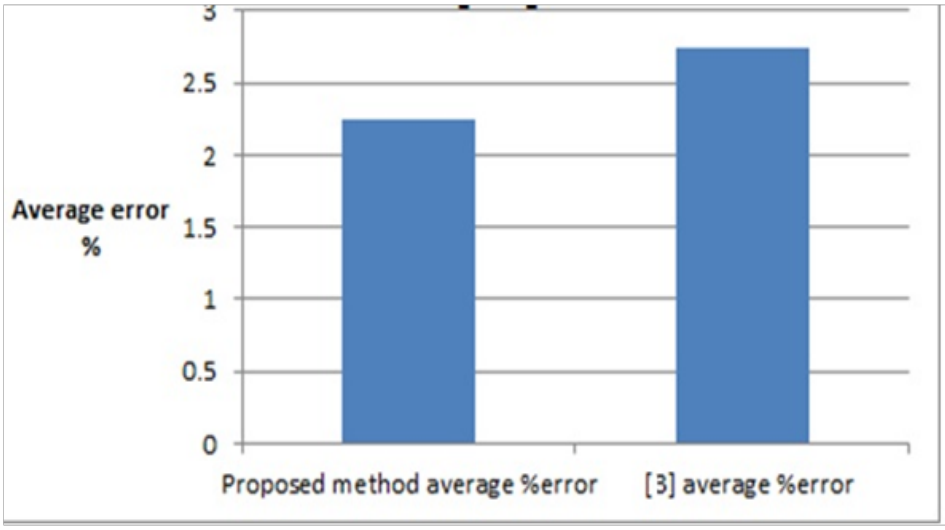


Figure-9 RR comparison chart between application counted RR and actual RR

The accuracy graph with respect to five neonatal subjects has been shown in Figure-10.

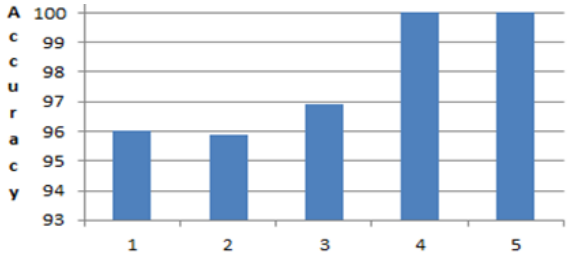


Figure-10 RR detection accuracy of the proposed method w.r.t. the subjects

E. Result 2: Comparison of the proposed method with other existing methods

The performance of the proposed method has been compared with the method mentioned in [3]. For five subjects in each method their average RR is determined and compared.

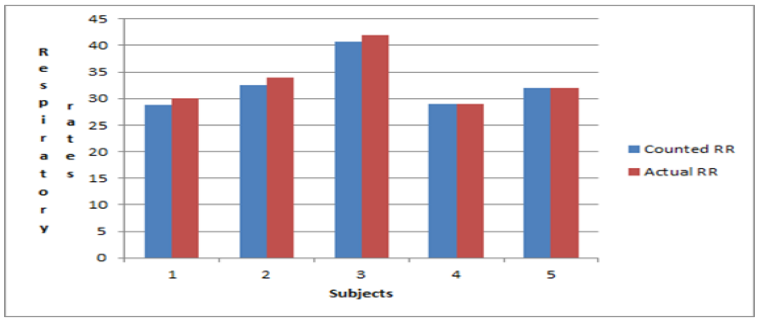


Figure-11 Comparison of the proposed method with another method

It can be observed that though the proposed method that average percentage error of the proposed method is less than its counterpart in [3]. Hence, it can be concluded that the propsed method is more accurate and outperforms the method mentioned in [3].

4. CONCLUSIONS

One of the most important factors for recognizing sleep apnea of a newborn is to monitor the baby's respiratory rate. There are various devices, both invasive and non-invasive, available for estimating neonatal RR. but, a non-invasive and low-cost device is preferable. which can operate in real time. In this research work, a simple and low-cost microphone has been used to sense the respiratory signals of the newborn. A MATLAB based application has been developed which detects the RR. The captured signal is represented as an audio file. Then enveloping is carried out to get the signal waveform. Data points optimization is carried out using down sampling technique. Finally, noise from the signal is removed by applying medial filter and RR is estimated by Fast Fourier Transform. It has been found from the experimental results that the system performs with nearly 100% accuracy and outperforms its counterpart with respect to average percentage error. In future, our goal is to improve this present system with the objective of estimating respiratory rate as well as heart rate of a neonatal from video images of the newborn. The system can be further improved by applying a combination of audio respiratory signal and video respiratory images for neonatal RR and heart rate estimation.

REFERENCES

1. Diego G Bassani, Rajesh Kumar, Shally Awasthi, Shaun K Morris, Vinod K Paul, Anita Shet, Usha Ram, Michelle F Gaffey, Robert E Black and Jha, Causes of neonatal and child mortality in India: nationally representative mortality survey, *Lancet*, 2010, 376, pp. 1853–1860.

2. Salvatore Pullano, I Mahbub, M. G. Bianco, S. Shamsir and S. K. Islam, Medical Devices for Apnea Monitoring and Therapy: Past and New Trends, *IEEE Reviews in Biomedical Engineering,* 2017, 10, pp. 199-212.
3. Juvenal Rodriguez Diana and David Santoyo López , Noninvasive Monitoring System for Early Detection of Apnea in Newborns and Infants, *IEEE EMBS Conference on Biomedical Engineering and Sciences* (IECBES), 2016, 26, pp. 414-418.
4. Sourya Bhattacharyya, Shashan Sharma, Jayanta Mukherjee, Parimal Kumar Purkait, Arunava Biswas and Alok Kanti Deb, Automated detection of newborn sleep apnea using video monitoring system, *Eighth International Conference on Advances in Pattern Recognition* (ICAPR), IEEE, 2015.
5. Ninah Koolen, Olivier Decroupet, Anneleen Dereymaeker and Katrien Jansen, Automated Respiration Detection from Neonatal Video Data, *4th International conference on Pattern Recognition Applications and Methods,* 2015.
6. Mauricio Villarreal, , Sitthichok Chaichulee, João Jorge, Sara Davis, Gabrielle Green, Carlos Arteta, Andrew Zisserman, Kenny McCormick, Peter Watkinson and Lionel, Non-contact physiological monitoring of preterm infants in the Neonatal Intensive Care. *Lancet*, Article no. 128, 2019.
7. Abbas K Abbas, Konrad Heimann, Katri Jergus, Thorsten Orlikowsky and Leonhardt, Neonatal non-contact respiratory monitoring based on real-time infrared thermography, *Biomedical Engineering Online,* Article no. 93, 2011.
8. Shermeen Nizami, Comparing time and frequency domain estimation of neonatal respiratory rate using pressure-sensitive mats, *IEEE International Symposium on Medical Measurements and Applications* (MeMeA), 2017.
9. S. Nizami, A. Bekele, M. Hozayen, K. Greenwood, J. Harrold and J. R. Green, Measuring uncertainty during respiratory rate estimation using pressure-sensitive mats, *IEEE Transactions on Instrumentation and Measurement*, 2018, Vol. 67, pp. 1535 – 1542.
10. Xinming Huang, Ling Sun, Tia, Zeyan Huang and Edward Clancy, Real-Time Non-Contact Infant Respiratory Monitoring Using UWB Radar, *Proceedings of ICCT*, 2015.
11. Shrenik A. Vora, Endla, Anday, Kapil R. Dandekar, Genevieve Dion, Adam K. and Fontecchi, On Implementing an Unconventional Infant Vital Signs Monitor with Passive RFID Tags, *IEEE International Conference on RFID* (RFID), 2017.
12. Jong Deok Kim,Won Hyuk Lee, Yonggu Lee, Hyun Ju Lee, Teahyen Cha, Seung Hyun KimKi-Min Song, Young-Hyo Lim, Seok Hyun Cho, Sung Ho Cho and Hyun-Kyung Park, Non-contact respiration monitoring using impulse radio ultra-wideband radar in neonates, *Royal Society Open Science*, 2019, 6, pp. 42-48.
13. Juan-Carlos, Cobos-Torres, M. Abderrahim and J. Martínez-Orgado, Non-Contact, Simple Neonatal Monitoring by Photo plethysmography, *Noninvasive biometric sensors*,2018, 18, pp. 1-14.
14. Luca Cattani, Davide Alinovi, Gianluigi Ferrari, Riccardo Raheli, Elena Pavlidis, Carlotta Spagnoli and Francesco Pisani, Monitoring infants by automatic video processing: A unified approach to motion

analysis, *Computers in Biology and Medicine*, 2017, 80, pp. 158-165.
15. Anran Wang, Jacob, E. S. Sunshine and Shyamnath Gollakota, Contactless Infant Monitoring using White Noise, The *25th Annual International Conference on Mobile Computing and Networking*, Article no. 52, 2019.

Novel approach for Securing Virtual Machines in Cloud Environment

Naveen Kumar A. N.[1] ✉, Udayakumar N. L.[2]

[1]Research Scholar, SSAHE, Agalakote, B.H.Road, Tumakuru -572107, Karnataka, India
[2]Assistant Professor, Dept. of CSE, SSIT, Tumakuru – 572 105, Karnataka, India
✉anenaveen@gmail.com

Abstract

Cloud computing is the system of imparting IT associated computing skills on demand, primarily based on Pay as you use system. Since Virtualization is the fundamental aspect of Cloud Services, it is important to have protection mechanism to avoid attacks, intrusions and device exploitations in Virtual Machines(VMs). Virtualization allows the creation of VMs (instances) and lead them to run concurrently by way of having exclusive Operating Systems(OS) with well suited applications over existing physical sources, thereby reducing the cost of funding for Cloud Service Providers. A method to offer the safety for the VMs and their required sources by allowing them to work generally without problems and making use of the available underlying physical assets is proposed.

Keywords: *Cloud Services, Hypervisor, Security, Vulnerability, Virtual Machine.*

1. INTRODUCTION

Computational power, server capacity, applications, platforms, software's etc are IT assets, which are to be had to customers all the time they needed, from cloud service providers through the internet. The Virtualization logically partitions these computational assets to create a pool of logical resources to lessen the investment and to increase the utilization.

Hypervisor plays a crucial function in each of the models in creation of logical versions of existing physical resources. Cloud computing has become a new manner of computing, which performs a major role in each IT industries and academics. Though the use of virtualization in cloud computing has many benefits, its components are affected by security problems, while sharing the logical resources. In addition information protection is the largest issue in cloud computing. It is necessary to have the perfect security mechanisms to shield both logical and physical resources.

2. HOW VIRTUALIZATION WORKS?

Virtualization is the process of isolating the logical sources from physical resources there by satisfy the needs of service users based on their demands. For example, the use of logical memory, the processes can allocate greater memory than available physical memory with the help of exchanging the data and information from primary to secondary and vice-versa, though the physical resources are partitioned and allotted to distinct users, every user has a feel that they've their own useful resource and work like as though they work with physical resource. This method also works with numerous layers of assets like networks, server, desktop, platform and application.

2.1 Security Risks in Cloud Virtualization

The device where the Hypervisor is running is the one, who acts as central controlling device for the purpose of allocating the resources to the virtual machines created earlier, then processing and de-allocating the same resources from those machines after the processing is over, there by releasing virtual instances. Since it is fair in the role of creating, allocating and de-allocating of VMs, it can be vulnerable to threats and attacks. As shown in Figure-1, the VMM (Virtual Machine Monitor) become the weak factor. The virtual instances of a few other physical devices may try to get resources from this VMM and it could attempt to inject the assaults to the VMs working environment with the aid of breaching the security measures.

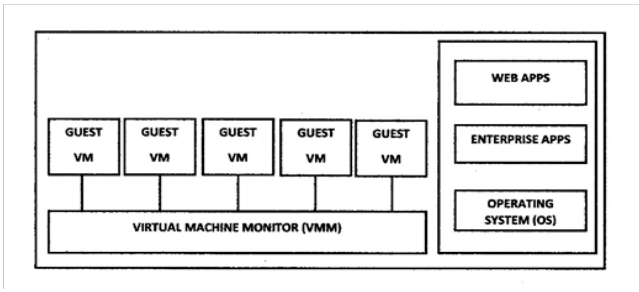


Figure-1 Virtualization vulnerabilities

2.1.1 Authorized Users and Accesses

The authorized users have extra rights than the ordinary users. The probabilities of injecting the attacks and involving in elaborate get right of entry to the resources are commonly happening with the authorized customers only, due to the fact the normal users are typically avoided at the fundamental degree of protection thereby heading off the serious assaults at the preliminary level itself.

2.1.2 Service Secrecy

The cloud users requests for the specified computational resources which includes software, applications, infrastructures, systems or memory from the cloud providers. In this state of affairs the consumer has to engage with the cloud provider company and their cloud offerings. During this interaction, alternate of statistics and confidential statistics with recognize to cloud offerings will be passed off using community transactions [1,2]. In this situation, it is essential to maintain customer's information and their confidential data effectively and securely. The restricted customers can try to hack consumer's confidential data. This may also create serious troubles to customers. In addition, while many clients are sharing the common resources among them, it is important to avoid each patron from the use of or knowing the usage or fame of other clients to keep away from the problems. This is the limitation of cloud computing.

3. PROPOSED APPROACH

This research work proposes an approach where three components are introduced in the Cloud services virtual environment which is shown in Figure-2. A Memory Monitor [MM], a Processor Monitor [PM] and an I/O Monitor [I/OM] shown in Figure-2. MM maintains all the logs related to memory consumption by the processes running in the each VMseparately. It regularly monitors each VM memory consumption and calculates the average memory consumption of each VM separately at regular intervals. If there is any huge variation in consumption of memory by any VM, it can be identified by MM and it is intimated to Security Supervisor (SS). At the same time processor monitor maintains all the logs related to processor usage by applications running in each VM. It regularly monitors processor utilization by each VM and calculates average processor utilization by each VM at regular intervals. If there is any huge variation in processor utilization rate, it will be intimated to SS.

The I/O Monitor maintains the logs related to I/O operations. In these cases, the SS checks normal consumption level of Memory, Processor and I/O of the VMs which are maintained at Memory, Processor and I/OM components. If there is any huge variation in consumption of resources when compared to normal average level, then it applies some security mechanisms to identify the infected VMs and the reasons for it. If possible, it tries to debug the problems and allow the VMs to work normally; otherwise, the details of the infected VM will be given to Hypervisor. Then the Hypervisor will get back all the computing resources which are allocated to infected VM and release that VM. This method will provide security to Cloud Virtual resources by stopping infected VMs.

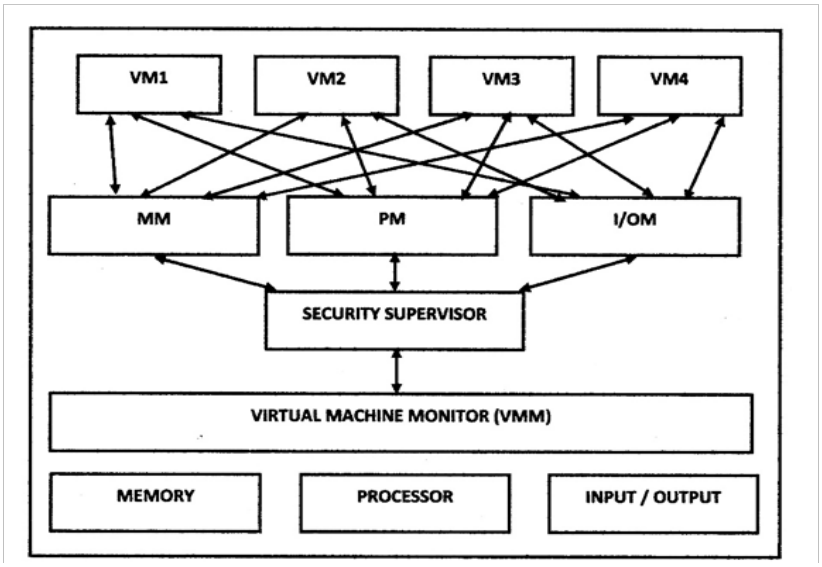


Figure-2 Virtual Machines with Security Supervisor [SS] and Logs Monitors

3.1 Algorithm (shows the function of Security Supervisor [SS])

1. VMs are created using the required resources from the pool of available physical resources.
2. Interacting with Virtual Machine Manager [VMM] to get started processing with required computing resources.
3. MM maintains logs of each VM, which gives information about memory consumption of the processes running in each VM.
4. PM maintains logs of each VM, which gives information about Processor utilization by the applications running in each VM.
5. IOM maintains logs of each VM, which gives information about Input and Output utilization during processing.
6. MMs, PMs and I/OMs calculate average consumption of memory, processor and I/O by each VM at regular intervals.
7. If there is any abnormal variation in consumption of memory, processor and I/O, send notification to SS.
8. SS identifies the infected VM and try to bring it back to normal function level. If it is not possible to avoid such problems by SS, then send notification to Hypervisor.
9. Hypervisor get back all the computing resources from infected VM and release the infected VM.

Different sorts of safety mechanisms, trouble identity functions, hassle correction strategies, heading off restricted customers and accesses, system

of hiding the originality of records mechanisms, strategies of identifying and heading off intruders, attackers, malwares, viruses ought to be protected in SS. In addition, it may comprise some updates and patches required by way of the VMs and softwares. It has to have the power of inclusive of the latest strategies and other solutions which may go thoroughly in future. It ought to have the habit of redesigning its methods and answers and keep updating at normal intervals in order that it ought to always contain latest, adequate and powerful security solutions. Some security solutions are privileged to work directly on VMs to provide the secured working environment. During adaptation of such safety and security approaches inside the SS, the users may face performance degradation.This approach is simulated using Cloudsim simulator; the analysis part is shown below.

3.1.1 Result-1

In the first analysis, no security supervisor and monitors is applied in cloud environment; all VMs are in normal working condition is as shown in Figure-3.

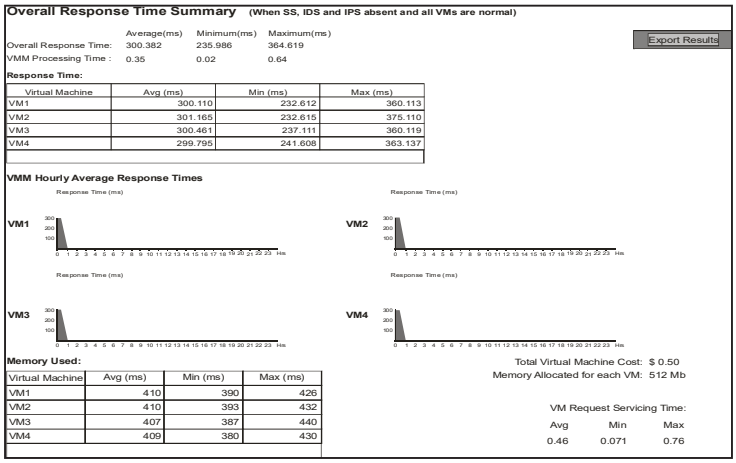


Figure-3 VMs are in normal working

3.1.2 Result-2

In the second analysis sheet [Figure-4], The SS is introduced with Intrusion Detection System [IDS] /Introduction Provision System [IPS]and three monitors are allowed to maintain the logs. In this case all VMs are working in normal condition(Figure-4).

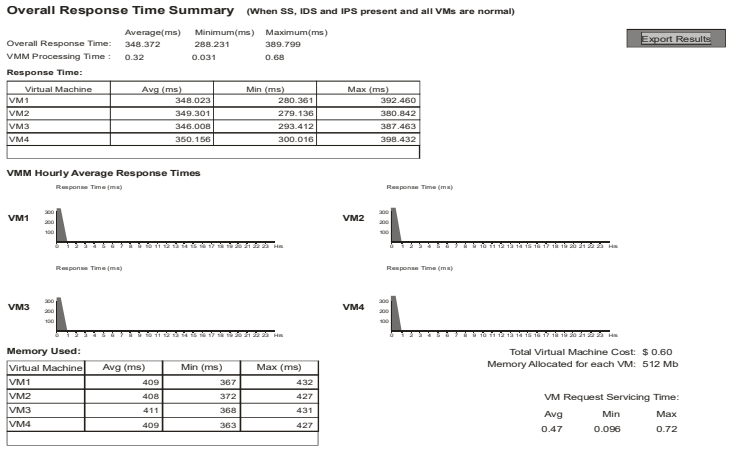


Figure-4 VMs are in normal working with IDS/IPS system

3.1.3 Result-3

In the third analysis sheet indicated in Figure-5, VM1 is infected and it infects VM3. SS tried to bring VM1 to normal condition, but it was not possible, it is stopped by Hypervisor by getting back all the allocated computing resources. It is shown with the help of Response time and Memory usage (Figure-5).

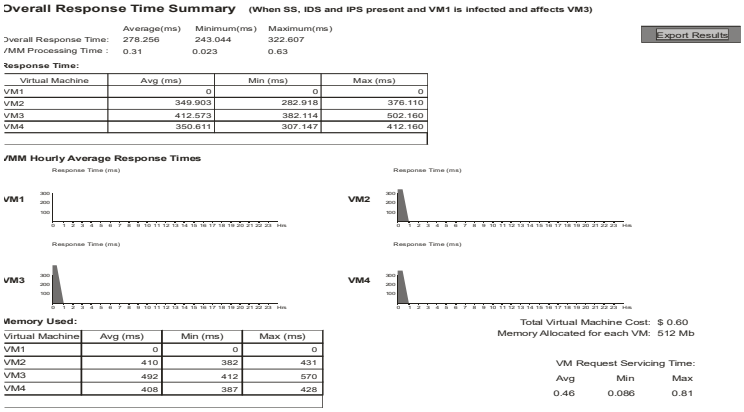


Figure-5 VM1 is infected and it infects VM3

4. CONCLUSIONS

In this research work, an approach is proposed to identify the infected VMs and bring back them to normal condition, otherwise stop them from working. The above solution is proposed which may not affect the performance of the virtual resources working in Cloud environment. It separates infected VM from other VMs and try to make it to work normally, if not possible then stops it's functioning by releasing the computing resources allocated to it. It is an advice

to the software industries that, they specifically concentrate on introducing secured virtualization mechanisms because same kind of challenges may be present among both virtual and physical working environments. Combining the proposed security solution with existing solutions (Which are already using in Cloud environment), this system implementation can guarantee that desired degree of security to all the VMs and at the same time not using overheads and creating problems.

REFERENCES

1. Gunnar Peterson, A Security Architecture Stack for the Cloud, *IEEE Security & Privacy,* 2010, 10(5), pp.83-86.
2. Udayakumar N.L. and Siddappa M., Multi-level Security for Virtualization in Cloud Services, *PARIPEX- Indian Journal of Research,* 2017, 6(5), pp.78-80.

Image Security Implementation and Cryptanalysis using ECC Cryptography, LSB-Watermarking Steganography

Y. Manjula[1]✉, K. B. Shivakumar[2]

[1]*Assistant Professor, Dept. of ECE, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.*

[2]*HOD, Dept. of TCE, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India*

✉manju.yerva@gmail.com

Abstract

Transferring data over a network is undoubtedly an important major security issue in today's world. To analyze secret data there are many attacks available. Attacks mainly focus on destroying secret data or only to know secret data. In both cases, security of data is lost. If secret data is destroyed then attack will be known to the sender and recipient otherwise attack is unknown. Lifetime of secrecy of the Secret data can be increased using steganography technique, where. secret image is hidden in any media. Cryptography technique is combined to increase confidentiality of data in communication channel. The term authentication can be still improved by adding a watermark to combination of above mentioned techniques. Usage of watermarking technique can give more authentication to secret data like image, audio, video etc. Therefore present paper is a blend of steganography, cryptography and watermarking techniques to provide a balance between necessary parameters of data transmission in network such as integrity, authentication and confidentiality. Secret image is converted by using cryptographic technique, i.e., Elliptic curve cryptography (ECC) combined with stenographic technique. Steganography technique which is used is least significant bit (LSB) method for embedding. This cover image is authenticated by embedding a logo or a water mark. Characteristics of image are analyzed by selecting the bit to embed the logo, which eases normal usability to provide strong security to data.

Keywords: *Cryptography, ECC, Logo, Robustness, Steganography.*

1. INTRODUCTION

Primary concern of real time society is security, for a given Data transmission in network. Secrecy is main parameter in field of communication. Different

type of coding techniques are used for giving security to the data, which has to be transmitted in network. People in earlier days used different techniques like invisible ink, hidden tattoos, candle writing for conveying messages. Algorithms which are used for transmission of unpublicized information should offers services likeConfidentiality, authentication, and integrity. Crucial issue in digital world is to develop such algorithms. Therefore demand of such algorithms with effective coding techniques for securing the confidential information is increasing. Cryptographic techniques and stegonographic techniques can be used to meet requirements.

Cryptographic algorithms change the characteristics of data and data becomes uncorrelated to third party. Therefore by implying encryption techniques security is increased.

By using Steganography techniques, existence of message between itself is concealedtwo parties by hiding message in a cover message (public data). Common algorithms such as injection and least significant bit embedding techniques are considered for hiding information in image video or audio. By using watermarking techniques the integrity of the sender as well as originality of information is realized. A simple logo image is embedded as watermark and integrity can be achieved.

The proposed algorithm clearly employs the identified parameters of the above discussed techniques and tries to give justice to the parameters for information security by blending techniques.

Hemanth Kumar Mohana et al. [1] presented a paper on LSB steganography, in which Point addition ECC is used. Message is compressed by wavelet transform and converted in to ASCII and then again it is converted in to binary value. This binary value is encoded by control NOT gate. These encoded values are then embedded.Yamunesh Goswami et al. [2] implemented a technique on DES-RSA and LSB photo steganography, in this technique a photograph is taken as input data and is verified for uniqueness by using canny edge detection. Encryption is applied to verify photograph. After encryption this data is embedded by using LSB technique.Kamal Deep Joshi et al. [3] surveyed on different stenographic techniques. A comparative analysis is made considering the parameters such as confidentiality, robustness, authentication, and indetectibility.Hyder YahyanAtown [4] proposed a method of hiding finger print using transposition cipher and also considered the parameters such as capacity, security and robustness. Lizhi et al. [5] analyzed the various methods and evaluating parameters of watermarking for the authentication

of the information. Authentication is one of primary services which has to be provided in the information transmission world. M.Mohhammad Sathik et al. [6] furnished a system and the systems low frequency components subband of wavelets domain and the resized version of original image are used in constructing the watermark and the rest are used for embedding the information.Chaudhari and Gunjal [7] inferred a method where a gray scale image is converted and 'Y' components of the images are divided into different small size blocks for two level decomposition.

Kamaldeep Joshi and Ravikumar Yadav [15] wrote a paper in which vernem cipher is used as encryption technique and to hide LSB technique. Cover image pixel values are converted into binary form and last four LSB bits are considered for encrypting the binary converted secret data using left circular shifting after each insertion with EX-OR operation.

Md. Khalid Imam Rahmani et al. [16] published a paper in which gradient energies are considered for several types of flipping rates taking 512*512 images.

In Gradient energy flipping rate detection, the variations in the energies are analyzed in spatial LSB technique for detection of secret messages. Nadiya et al. [17] wrote a paper on double stegging. DWT transform is used to decompose the cover image. First encrypted secret data is hidden in the second level decomposed detail coefficients then this stego image area is embedded in first level detail coefficients.

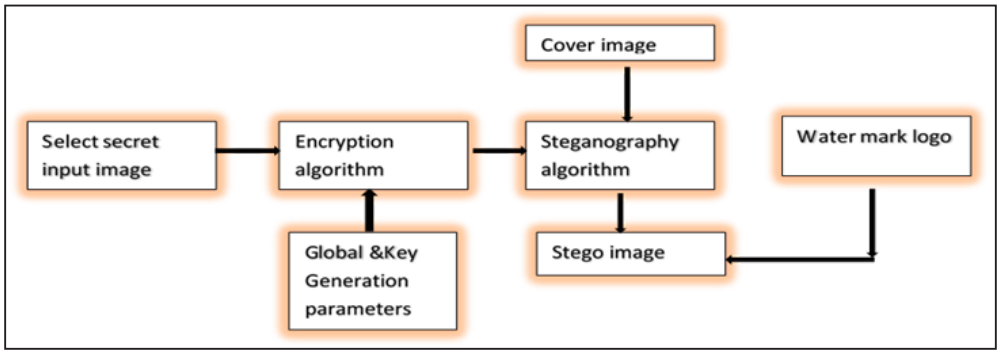
Andiksetyono et al. [18] proposed a paper on OTP encryption and 3 DWT. On applying 3 DWT we get subbands in which LL3 is considered for hiding. There after once again DWT applied to get HH4. The secret image is XOR-ed with OTP secret key to this encrypted values. These values are then embedded in HH4.

2. METHODOLOGY

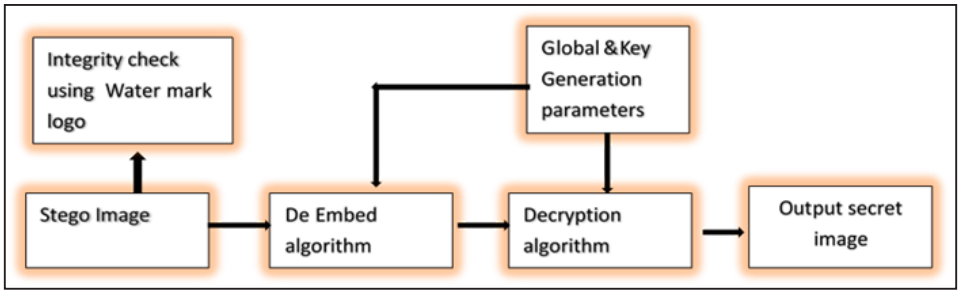
The present system uses all identified dominant advantages of cryptography, steganography and watermarking techniques. The blend of these techniques maintains a balance between the parameters such as payload capacity, similarity ratio, peak to signal noise ratio. Therefore this algorithm not only hides the high amount of data but also limits the difference occurred while comparing the cover image and stego image more efficiently. Adding watermark improves the integrity of the information by authenticating the originality of the sender.

Proposed technique shown in figure-1 is explained in the following steps.

a) Select the image for secure transfer.
b)Using ECC Encrypt the image.
c)Using LSB embed the coded secret image.
d)Embed water mark logo.
e)Watermarked stego is transferred.
f)De-embed the logo.
g)De-embed the coded image.
h)Decrypt the secret image.



(a)



(b)

Figure-1 Proposed block diagram
(a) Proposed method: Sender side (b) Proposed method: Receiver side

Select the image for secure transfer: Select the secret image which has to be transfered in communication channel.

Using ECC encrypt an image: The secret image is converted into bit format. A curve is considered as a parameter and all the points in a curve are generated. Then bit format message is substituted in a position of curve points through mapping table. Encryption is done using ECC technique.

Using LSB technique embed the coded secret message: The coded message is considered in a stream of bits. These bits are substituted by considering the LSB of cover image for embedding process and this is done by substituting the least significant bit of the cover image to get the stego image. The beauty of LSB technique is its simplicity in implementation.

Embed the watermark logo: Using bit replacement method by choosing the position of bit, embed the logo image. Here the image of SSIT is taken as the watermark logo.

3. SYSTEM IMPLEMENTATION

The public key cryptographic technique called 'Elliptic Curve' cryptography is used for encrypting secret image in present paper. Over infinite number of fields in numbers, elliptic curves are considered. The beauty of ECC algorithm lies in reducing complexity of multiplication of two points by considering addition operation. In addition to that the amount of security given by RSA with larger size numbers can be achieved by ECC with smaller numbers itself. Several factorization algorithms also use elliptic curves that have applications in cryptography. Point multiplication computing is the basic principle on which the security of ECC is depended upon. The curve size determines the strength of ECC technique. ECC is preferred when compared to other public key algorithms because of its smaller key size, effective storage capacity and transmission requirements. The complexity of the problem is directly proportional to the size of the elliptic curve. The elliptic curve considered for the cryptosystem is given in equation (1). It is a plane curve which has the number of points in it to encrypt.

$$y^2=x^3+ax+b \bmod p \quad (1)$$

The domain parameters which determine selected ECC curve are to be decided by both parties i.e., the sender and the receiver in the communication channel. P is a prime case is defined in the field. The constants a and b are used to define the elliptic curve selected. The generator point G defines the cyclic subgroup, nG =0 condition is used to choose the generator point G which is a prime number for small value of n.

Among steganography methods LSB method of embedding secret image is selected for cover image. This method is effective for human eye perception. The cover image is selected first and all least significant bits are zeroed using the software. The coded secret image in the bit form is then streamed in the zeroed values of the covered image.

Normally if a cover size is of 512*512 then the 8 bit format can have storage capacity of 512*512*8(2097152) bits. If one bit has to be replaced then 262144 bits i.e., 256KB is the embedded capacity of cover image. Similarly variations in cover size maybe considered for improving embedded capacity. The human perception is not effected by replacing the LSB bit. The functionality of the algorithm is as follows:

3.1 Encoding

LSB method allows large amount of secret data to be embedded in a cover image. Image file contains set of bytes which can be used for embedding. Cover images may contain several bytes depending on their sizes. The following steps are used during the encoding stage:

- The message is encrypted using public key of the receiver.
- The cover image is converted into bit stream.
- The input image is converted into bit stream.
- Make all the LSB bits of cover image to zero.
- Replace the LSB bit of the cover image with the LSB bit of character in the message to hide. GUI of encryption is shown in Figure-2

3.2 Decoding

In this stage, the embedded image is decoded to get a hidden message. Then message is decoded first and then decrypted by the private key that is known only by the authorized receivers or users of the proposed system.

An invisible watermarked logo which signifies source ownership and authentication has been used. The aim of logo is to permanently mark the digital data make it unalterable and also make it invisible to the unauthorized access and make only recipient knows the data (logo) which is watermarked on the cover image. The watermarked data is inserted into the choice of bit which can be selected in bit of the stream using bit plane substitution method.

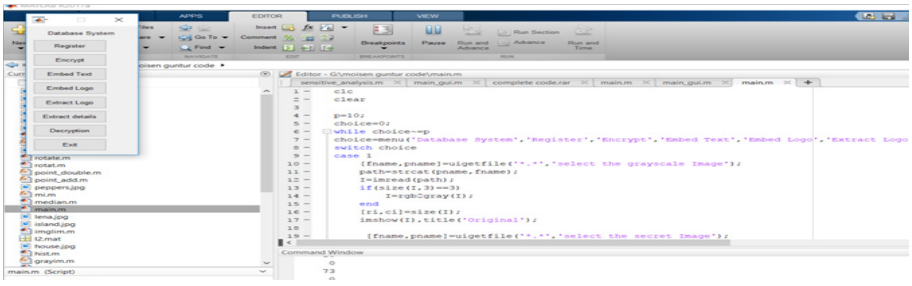


Figure-2 The Output Result of ECC Encryption

4. EXPERIMENTAL RESULTS

MATLAB software is used for the implementation of the proposed method. The identification of points is done by ECC for encryption. The parameter MSE calculation formula is

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{[OI(i,j) - DI(i,j)]^2}{M*N} \quad (2)$$

Invisible watermarking is used for ownership of the data and the sender. The motto of the logo is to permanently mark the digital data and make the information unalterable. The watermark insertion is made by choice of insertion bit. The receiver's private key is used for decryption. If that is the case the secrecy of the input message is maintained by the algorithm.

The quality of the image is evaluated by Peak to signal noise ratio. Size of the image considered for calculating PSNR is M*N gray scale image.

$$PSNR = 10log_{10} \frac{255^2}{MSE} \quad (3)$$

Figure-3 shows the result of steganography method in which each cameraman cover image is embedded with different bits considered for substitution. The Figure-4 shows the different cover images. Table-1 and Tabel 2 refer PSNR, SR and MSE of the stego images.Figure-5 shows the stego Images with the PSNR, SR and MSE values shown in Table -1.

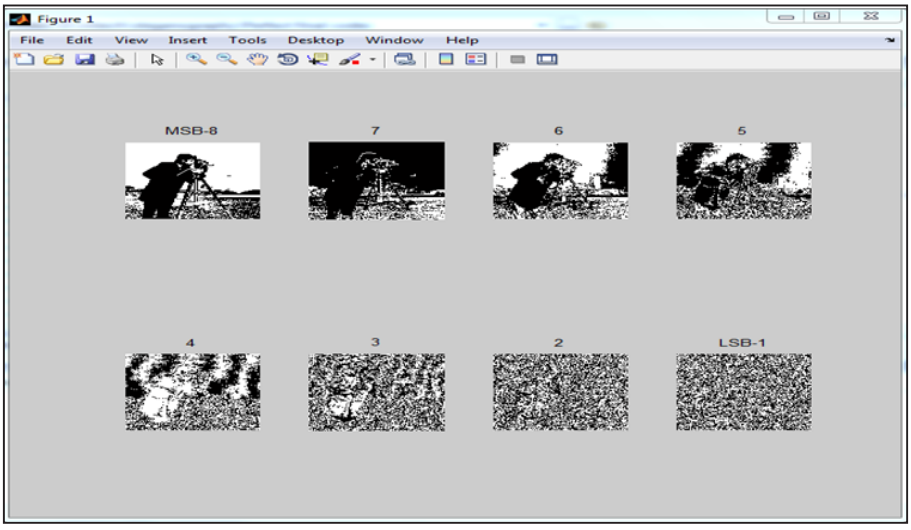


Figure-3 Image is embedded in different Bit positions

Figure- 4 Selected four cover images (512*512)

Figure-5 Four Stego Images

Table-1 Evaluation of the embedding scheme by considering different cover images for same secret image.

Stego images	SR	PSNR	MSE
Camera man	0.9836	56.212	0.1555
Lena	0.9923	56.2012	0.1559
Peppers	0.99898	56.1979	0.1563
Baboon	0.9897	56.1926	0.1563

Table-2 Evaluation of the algorithm by single cover image with variant secret image sizes. Image (sun) with different input image size

Secret image size	SR	PSNR values	MSE
16*16	0.9784	66.812	0.0135
32*32	0.9630	61.5759	0.0452
64*64	0.9346	56.1433	0.158
101*35	0.9366	56.8466	0.1344
152*35	0.9205	55.1359	0.1993
190*60	0.8547	51.9122	0.8547
200*33	0.9110	54.2341	0.2453

The rows and columns of the images are considered in this technique have same value. The watermark embedded is also a square matrix image. Size 512*512 is considered for testing. The original cameraman image (a), stego image with water mark (b) and watermark logo (c) used in the algorithm are shown in Figure-6. The visual difference between the camera man original and water marked stego image is minimum.

(a) (b) (c)

Figure- 6 Result of proposed method **(a)** Original cover image (b) Stego Image and (c) logo

PSNR is calculated for analyzing visual quality of the watermarked stego image and the value is 51.3225, which means the deterioration in the quality of the cover image is less when compared with watermarked stego image after applying the algorithm. Similarity ratio value is also near to 1 which indicates the strength of the algorithm. The similarity ratio equation considered is

$$SR=S/(S+D) \quad (4)$$

Similarity ratio evaluated using equation (4) between stego and cover images shown in Table-1 and similarity ratio between stego and watermarked stego is shown in Table-3. Authentication is preserved because the matching pixels are high in number.

Table-3 Quality evaluation of watermarking technique, Water mark logo of size 64*64

Parameters Used	Values
PSNR	51.3225
SR	0.9086

Table-4 PSNR values of the watermarked output image

Bit allocation	PSNR (dB)	
	Method [19]	Proposed
1st bit	65.7059	51.1626
2nd bit	59.7120	45.1552
3rd bit	53.7899	39.1227
4th bit	47.5984	32.7568
5th bit	41.2750	27.7444
6th bit	35.4789	20.9238
7th bit	29.5223	19.5847
8th bit	23.9433	8.2153

Table-4 listed out the comparison between existing and proposed method interms of PSNR value. The existing method is combination of LSB and maximum entropy, whereas the proposed method hides the logo inside stego image using bit substitution technique. From these results, proposed method has good results compared to existing one. Hence. the robustness of image is best.

Table-5 SR values of each bit allocation

Bit Allocation	SR values
1st Bit	0.5000
2nd Bit	0.5000
3rd Bit	0.5065
4th Bit	0.5132
5th Bit	0.5270
6th Bit	0.5000
7th Bit	0.5000
8th Bit	0.8478

Table-5 describes the Similarity Ratio values of 1st bit to 8th bit allocation and it can see that LSB bit allocation is good in the watermarking technique compare to MSB bit allocation

Table-6 Assessment of PSNR under Attacks

Attacks	Values	PSNR (dB)	
		Method [20]	Proposed
Adding Gaussian Noise (mean and variance)	0.01 and 0	38.3272	38.5890
	0 and 0.001	30.0997	30.0817
Adding Salt & Pepper Noise	0.002	32.1381	32.2121
Median filtering	3x3	29.5727	18.1470
Linear filtering	3x3	27.7761	32.4576
Histogram Equalization	-	19.0944	18.9616
Image Adjustment	-	18.5312	17.8628

The imperceptibility of watermark in the proposed method has been evaluated against incidental attacks by using the metric PSNR and is compared against the existing method [20]. A comparative study shown in Table-6 reveals

the fact that the quality of watermarked image under various incidental image processing operations is more or less similar in both methods.

Robustness of the proposed method under the common image processing operations has been identified with the help of Similarity Ratio and is compared against the existing method [20]. Table-7 shows the experimental results. The simulation results of both methods in case of additive Gaussian noises show that robustness of watermark in this attack is high with constant variance 0. An increase in variance slightly affects the robustness in both cases. The watermarked image is attacked with salt & pepper noise with density 0.002 and the results obtained shows that both techniques are highly robust.

Table-7 Assessment of SR under Attacks

Attacks	Values	Similarity Ratio	
		Method [20]	Proposed
Adding Gaussian Noise (mean and variance)	0.01 and 0	0.8371	0.4952
	0 and 0.001	0.5042	0.4685
Adding Salt & Pepper Noise	0.002	0.8370	0.5000
Median filtering	3x3	0.6629	0.5000
Linear filtering	3x3	0.6696	0.6903
Histogram Equalization		0.7598	0.4968
Image Adjustment		0.8435	0.4444

Watermarked image is smoothed with a 3x3 linear filter. Experimental results show that the proposed technique is more robust than the technique in the existing method [20] under filtering operation. Experimental results against Image adjustment and Histogram equalization attacks reveal that robustness of watermark is high.

5. CONCLUSIONS

The strength of the proposed method is clearly evaluated with parameters. The use of private key for decryption in ECC gives confidentiality and use of water mark gives an authentication to the sender. The technique ECC uses receiver's public key for encryption which is known to many. This drawback is cleared by blending ECC with watermarking technique. The encryption and steganography techniques are evaluated by calculating PSNR and MSE. The authentication strength of watermark is derived with help of similarity index. The watermark authentication has been be evaluated by adding the noises. The comparisons are made to verify robustness of the algorithm, which is achieved.

Legend

D	=	Number of different pixels
DI	=	distorted image
MSE	=	Mean square error between OI and DI.
OI	=	Original image
PSNR	=	Peak signal to noise ratio
S	=	Number of matching pixels
SR	=	Similarity Ratio

REFERENCES

1. Hemanta Kumar and Mohanta M, Secure Data Hiding Using Elliptical Curve Cryptography and Steganography, *International Journal of Computer Applications* (0975 – 8887) , December 2014 , 108, pp.3.
2. Yamunesh Goswami, Anuj Bhargava and Prashant Badal ,Improved Method For A Secure Image Cryptography Based On RSA and DES Algorithm and LSB Steganography Technique, *International Journal of Advance Engineering and Research Development,* 2017, 4 (11), pp. 731-737.
3. Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, A Crypto-Steganography: A Survey, (IJACSA) *International Journal of Advanced Computer Science and Applications,* 2014, 5 (7), pp.149.
4. Hyder Yahya Atown, Hide and Encryption Fingerprint Image by Using LSB and Transposition Pixel by Spiral Method, *International Journal of Computer Science and Mobile Computing,* 2014, 3 (12), pp. 624-632.
5. Rdharani and M.L. Valarmathi,A Study on Watermarking Schemes for Image Authentication, *International Journal of Computer Applications,* Vol.2, 2010, pp.24-32.
6. M. Mohamed Sathik and S.S. Sujatha,An Improved Invisible Watermarking Technique for Image Authentication, *International Journal of Advanced Science and Technology,* 2010, 24, pp. 61-73.
7. Chandhari and B.L. Gunjal, Image Watermarking Algorithm in DWT Domain, *International Journal of Modern Engineering Research*, 2012, 2, pp.1940-1943.
8. Ashadeep Kaur, Rakesh Kumar and Kamaljeet Kainth, Review Paper on Image Steganography. *International Journal of Advanced Research in Computer Science and Software Engineering,* 2016, 6 (6), pp. 499-502.
9. Anil Kumar,A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique, *IJARCSSE,* 2013, 3 (7), pp. 363-372.
10. Ankita Gangwar and Vishal Srivastava. Improved RGB -LSB Steganography Using Secret Key, *International Journal of Computer Trends and Technology* (IJCTT), 2013, 4, pp. 85-89
11. Abikoye Oluwakemi, AdewoleKayode S and OladipupoAyotunde J, Efficient Data Hiding System using Cryptography and Steganography, *International Journal of*

Applied Information Systems (IJAIS), 2012, 4, pp.6-11.
12. Galam Santosh Reddy, V. Madhu Viswanatham, PotluriJagadeesh and Mothe Dinesh Reddy, An Improved Authentication Scheme for Passport Verification Using Watermarking Technique, *International Journal of Computer Science Issues* (IJCSI), 2012, 9, pp.106-112.
13. C.M. Wang, N.I. Wu, C.S. Tsai and M.S. Hwang,A High Quality Steganography Method with Pixel-Value Differencing and Modulus Function, *Journals of Systems and Software,* 2008, 81, pp. 150-158.
14. Galam Santosh Reddy, V. MadhuViswanatham, PotluriJagadeesh and Mothe Dinesh Reddy,An Improved Authentication Scheme for Passport Verification Using Watermarking Technique, *International Journal of Computer Science Issues* (IJCSI), 2012, 9, pp.106-112.
15. Kamaldeep Joshi and Rajkumar Yadav, A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication, 978-1-5090-0148-4/15/$31.00© 2015 *IEEE.*
16. Li Zlii and Suiaefen, A LSB Steganography Detection Algorithm , The 14th IEEE 2003 *International Symposium on Personal,* lndoor and Mobile Radio Communication Proceedings.
17. Nadiya P V and B Mohammed lmran, Image Steganography in DWT Domain using Double-stegging with RSA Encryption ,2013 *International Conference on Signal Processing, Image Processing and Pattern Recognition* [ICSIPRj] 978-1-4673-4862-1/13/$31.00 ©2013 IEEE.
18. Andik Setyono, De Rosal Ignatius Moses Setiadi and Muljono, Stego Crypt Method Using Wavelet Transform and One-Time Pad for Secret Image Delivery, Proc. of 2017 *4th Int. Conf. on Information Tech., Computer, and Electrical Engineering* (ICITACEE), Oct 18-19, 2017, Semarang, Indonesia.
19. D.C. Wu and W.H. Tsai, A Steganographic Method for Images by Pixel-Value Differencing, Pattern Recognition Letters, Vol.24, .2003, Page no:1613-1626.
20. V. Madhu Viswanatham, Galam Santosh Reddy and Potluri Jagadeesh, A Hybrid Digital Watermarking Algorithm for Colour Images based on DWT and DCT, Annals. *Computer Science Series,* 2012, 10, pp.27-33.

SSAHE Journal of Interdiciplinary Research
Instructions to the Authors

It is requested to use the template attached at the end of this instruction to prepare the article for submission to SSAHE - JIR.

1. Aims and Scope

SSAHE Journal of Interdisciplinary Research (SSAHE-JIR) publishes research results dealing with all aspects of Engineering and Technology, Science, Dental, Medical and related domains. JIR is in English language and includes reviews and research articles.

2. Submission of Manuscripts

Manuscript should be prepared in MS Word format or Latex and must be converted into a single file (preferably within 10 to 12 pages) before submission. Paper need to be submitted via email to: ssahe.jir@gmail.com.

3. Manuscript Preparation

Formatting/Style

A4 paper format, the printing area is 17.5 cm x 26.2 cm (Single Column). The margins should be 1.75 cm on each side of the paper (All four sides). The paper style of SSAHE - JIR should be followed with respect to the kind size and type of font (Times New Roman, 12 fonts). Send files with docx extention only.

Authors List and Affiliation Format

The Authors' full first and last names must be provided. A corresponding author must be designated. The complete address including city, code, state, country, and email ID should be included.

Abstract and Keywords

The abstract should be prepared as a paragraph (100 to 250 words). A list of four to eight keywords must be given, and placed after the Abstract.

Figures, Schemes and Tables

Authors are encouraged to prepare figures, schemes and tables in color. Figure, schemes and tables must be numbered (Figure-1, Scheme-1, Table-1, etc.) and an explanatory title must be added. All table columns should have an explanatory heading. Provide legend for all equations, figures, schemes and tables. The legends should be prepared as a separate paragraph of the main text and placed in the main text after the conclusion. It is to be ensured that equations are written clearly and legibly with proper editors. Figures and tables, included are to be with proper indentation. Please supply all

figures as separate graphics files (in addition to the figures being embedded in text). We accept Images in the TIFF and JPEG formats. Tables should be prepared in MS Word (Scanned images of tables are not allowed)..

Reference Preparation

Ensure that every reference cited in the text, also exists in the reference list (and vice versa). In the text, refer to the author's name (without initials) and year of publication. For one are two authors all authors had to be listed. If there are more than two authors, the format first author, et al. should be used throughout the text. The list of references should be arranged alphabetically by authors' names and should list all authors. The manuscript should be carefully verified to ensure that the spelling of authors' names and dates are exactly the same in the text as in the reference list.

4. Review/Referees

The contributions will be peer-reviewed on the criteria of originality and quality. To aid in the peer review, authors can provide the names, address and e-mail ID of up to 5 potential referees, although the editor will not necessarily contact them.

5. Revised Manuscripts

In revised manuscripts, the areas containing the major required changes should be marked and the script color changed. Upon acceptance of the manuscript, the final uploaded version will be taken as the basis for subsequent production process, and papers are subjected to editorial changes. Responsibility for the factual accuracy of a paper relies entirely on the author . All the required corrections are to be implemented by author to the satisfaction of editorial board

6. Proofs and Reprints

Before publication, the corresponding author will receive page proofs via e-mail. The proofs should be corrected cautiously. In particular, authors should answer any editing queries. Authors may freely download the PDF file from which they can print unlimited copies of their articles.

7. Copyright/Open Access

The authors vouch that the work have not been published elsewhere, and the manuscript have not been submitted to another journal. The publishing

misconduct, such as plagiarism and data fabrication, will result in rejection/ retraction of the manuscript. Please note that if you are submitting material which has been already published elsewhere, you must also send the permission in writing that this material may be reprinted in SSAHE - JIR to the Editorial

Office, and the authors are expected to carry any costs arising from the permission. When the manuscript is accepted for publication, the authors agree for automatic transfer of the copyright. The Articles published in SSAHE - JIR will be open-access articles.

8. Fee and Charges

The SSAHE - JIR will be published free of cost, online and biannually through a standard blind review procedure.

9. Guidelines for Prepration of Manuscript

The various guidelins in detail have been prepared in the form of an article given next.

Format for the Manuscript Preparation

SSAHE Journal of Interdisciplinary Research www.sahe.in/jir ISSN: (Times New Roman, 10pt,)

Title of the Paper (Times New Roman, 18pt, Bold)

Original Research, Case Study, Discussion Paper, Methods (type of paper)

First name Last name[1] ✉. First name Last name[2], First name Last name[3*]
(Times New Roman, 12pt, Bold,)
[1]Full Affiliation/Address (Times New Roman, 10pt, Italic)
[2]Full Affiliation/Address

Example: [1]Assoc.Prof., Dept. of Physics, SSIT, Tumakuru-572105, India
[2]Research Scholar, SSAHE, Agalakote, B.H.Road, Tumakuru – 5720107
[3]Prof., Dept. of ECE, SSIT, Tumakuru-572105, India
✉Corresponding author: Email id (Times New Roman, 10pt)

Abstract (Times New Roman, 12pt, bold)

In the abstract author should emphasize on what has been done in the research. How they did it? What did they get it? With maximum of 250- words

(Times New Roman, 12pt, italic).

Key Words: *(Times New Roman, 12pt, bold, italic): Maximum 6-keywords separated by comma, ending in full stopand with no 'and' (Times New Roman, 12pt, Italic)*

1. INTRODUCTION (Times New Roman, 12pt, bold)

In the introduction (i.e., the initial section of a scientific paper) it is mandatory to present the topic of the research and state the background and relative rationale (if applied). In this section the authors should also explain the aim and novelty of the research work [1-5]. It is not necessary, except for review papers, to describe the full history and challenges of the specific research topic. The cited literature should be relevant and up-to-date [6]. (Times New Roman, 12pt).

The second paragraph in each section should start with an indent of 0.29"

2. ANALYSIS AND/OR DESIGNS (Times New Roman, 12pt, bold)

Theoretical methodology used in the paper is to be detailed here. Equations should be on separate line, to be numbered and positioned on the same line and in the standard format according to Latex/ Microsoft equation editor.

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos \frac{n\pi x}{L} + b_n \sin \frac{n\pi x}{L} \right) \quad (1)$$

All notations used need to be defined in the legend section after conclusions.

3. EXPERIMENTAL SECTION (Times New Roman, 12pt, bold)

Depending on the topic, the experimental section should include synthesis procedures, characterization techniques etc and specification of the instruments. If it is simulation, author will have to mention the type simulation software with specifications [3, 7]. Mention the importance of that software used relevant to research work carried out. (Times New Roman, 12pt)

3.1 Subsection head format (Times New Roman, 12pt, bold)

Accompanying Text (Times New Roman, 12pt)

4. RESULTS AND DISCUSSION (Times New Roman, 12pt, bold)

In this section, it includes the detailed discussion on different parameter values which are plotted in graph and mentioned in a table. Precise analysis of graphs and tables is needed [8-12].

Finally author has to mention how it has excelled in obtaining results in comparison with previous research works. Method of citing the reference numbers in the manuscript are shown in the above text. (Times New Roman, 12pt).

4.1 Subsection head format (Times New Roman, 12pt, bold)
Text (Times New Roman, 12pt)
The images or graphs should be clearly visible. In the graphs x and y axis should be clearly mentioned with relevant units. Refer given example of image or graph with caption format. Figure-1 is

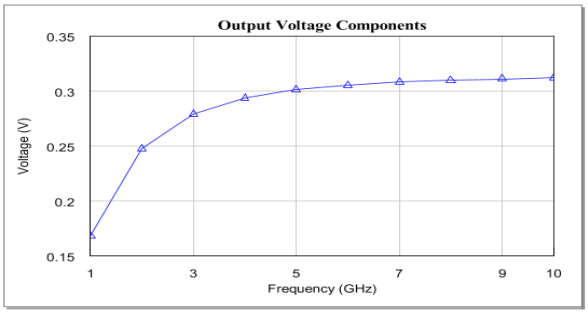


Figure-1 (Times New Roman, 11pt, bold) Photo-current and substrate temperature of the device (Times New Roman, 11pt)

(a) **(b)**

(c) **(d)**

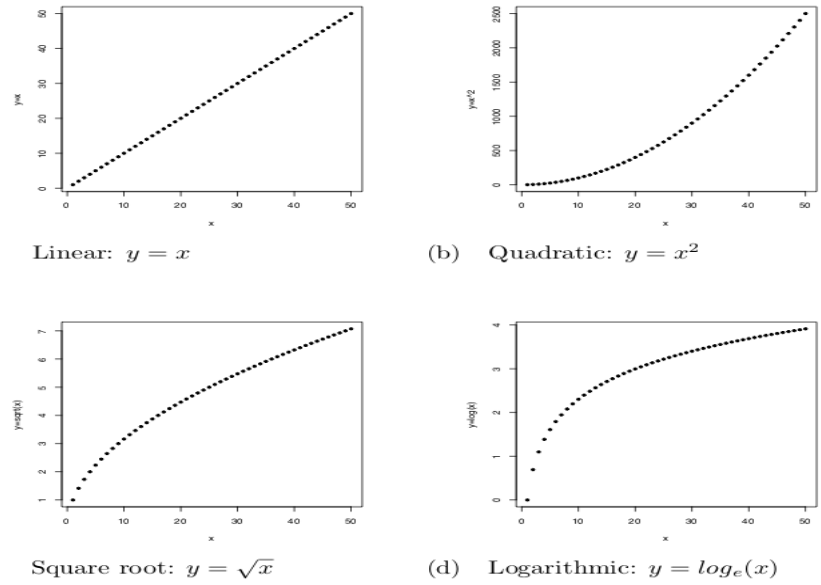


Figure-2 (Times New Roman, 11pt, bold) Basic mathematical functions (Times New Roman, 11pt) (a) linear y=x (b)Quadratic $y=x^2$ (c)Square root $y=\sqrt{x}$ (d)Logarithmic y=ln x

Table format is to be as follows:

Table-1 (Times New Roman, 10pt, table heads is to be bold) Kinematic parameter table of the developed robot(Times New Roman, 11pt)

Type	Θ_k	$\mathbf{d_k}$	$\mathbf{a_k}$	α_k	**SHP**
Base	Θ_1	d_1	0	90^0	0
Shoulder	Θ_2	0	a_2	0	90^0
Elbow	Θ_3	0	a_3	0	$\pi/2$
Tool pitch	Θ_4	0	a_4	90^0	-
Tool roll	Θ_5	d_5	0	0	90^0

5. CONCLUSIONS (Times New Roman, 12pt, bold)

The conclusion of a research paper need to summarize the research work

carried out and mentions the applications and future scope of the research work. (Times New Roman, 12pt).

Legend (Times New Roman, 12pt, bold)
No symbol which is used in the paper should be left undefined, and should be listed here. Greek symbols should come first and small letters first and capital symbols last. All should be in Times New Roman,12 pt. Please don't use spaces but use tabs for alignment. Above should include all symbols used in equations, figures and tables.

Γ	=	Cumulative error in measurement
Ω	=	Potential
β	=	Angle made with respect to vertical
θ	=	Angle made with respect to horizontal
k	=	Hydraulic Conductivity
kx	=	Hydraulic Conductivity in horizontal direction
n	=	Manning's coefficient
H	=	Depth of water upstream of dam
H1	=	Height of dam

.

6. ACKNOWLEDGEMENT (Times New Roman, 12pt, bold)
Acknowledgement is to be given to a person/institution where research facilities are used and also to the funding agency (if fund is obtained to carry out this research work) (Times New Roman, 10pt). Example: The authors thank the Department of Science and Technology (DST), Govt. of India for financial support and Centre for Nanoscience and Technology, Indian Institute of Science, Bangalore for the SEM measurements.

REFERENCES (Times New Roman, 12pt, bold)
The reference for various types should strictly be made in the mentioned format. In the paper the reference should appear in ascending order.

For Weblinks
(Do not list reference to website, thesis and patents)

Example - don't just refer URL like https://nptel.ac.in, but refer in detail as mentioned below https://nptel.ac.in/courses/102/108/102108078/

For Journal articles
1. Udayakumar N. L. and Siddappa M., Multi-level Security for Virtualization