WIRELESS CONNECTIVITY ISSUES

Project Report

Submitted in the partial fulfillment of the requirements for the award of the degree of **BCA (BACHELOR OF COMPUTER APPLICATIONS).**

Department of Computer Science

By

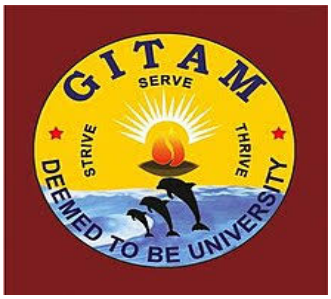
GDVS SANDEEP

(Regd. No: 121812501026)

Under the esteemed guidance of

Dr. M Sesha Shayee

Associate Professor



Department of Computer Science

GITAM Institute of Science

GITAM (Deemed to be University)

Visakhapatnam -530045, A.P

(ESTD. u/s 3 of the UGC Act. 1956)

(2018-21)

GITAM
(DEEMED TO BE UNIVERSITY)
VISAKHAPATNAM ❁ HYDERABAD ❁ BENGALURU

CERTIFICATE

This is to certify that the project entitled **"WIRELESS CONNECTIVITY ISSUES"** is a BONAFIDE record of the project work done by **GDVS SANDEEP**, Regd. No: 121812501026 during **January 2021** to **May 2021** in partial fulfillment of the requirement for the award of degree of **Bachelor of Computer Applications (BCA)** in the **Department of Computer Science, GITAM Institute of Science, GITAM (Deemed to be University), Visakhapatnam**.

Internal Guide

Dr. M.Sesha shayee

Associate Professor

Dept of Computer Science, GIS

GITAM

Head of the Department

Dr.Vedavathi Katneni

Professor

Dept of Computer Science, GIS

GITAM

DECLARATION

I, GDVS SANDEEP **Regd**. **No: 121812501026** hereby declare that the project entitled **"WIRELESS CONNECTIVITY ISSUES"** is an original work done in the partial fulfillment of the requirements for the award of degree of **Bachelor of Computer Applications (BCA)** in **GITAM Institute of Science, GITAM (Deemed to be University), Visakhapatnam.** I assure that this project work has not been submitted towards any other degree or diploma in any other colleges or universities.

GDVS SANDEEP

(Regd. No: 121812501026)

ACKNOWLEDGEMENT

It is my prime duty to express my sincere gratitude to all those who have helped me to successfully complete this project. I express respectful and sincere thanks to my project guide **Associate Professor, Dr.M.Sesha shayee, our AMC Ms. B. Satya Sai Vani, Associate professor, our HOD Dr. K. Vedavathi,** Distinguished **Professor & Principal Mr. M. Saratchandra Babu** and the faculty members of our department for the valuable cooperation, guidance and continuous support rendered by them on me throughout my project work. At last, I would like to thank all of my friends and my parents for giving needful advices and giving full support for completion of this project.

GDVS SANDEEP

(Regd. No: 121812501026)

ABSTRACT

Wireless networks is a quickly developing worldview having the capacity to change the physical association between the people and associations. Wireless networks organizes plans to trade "things" in a secure and dependable path through IT framework. This innova tion has discovered applications in various fields, for example, social insurance, learning, and preparing, asset the executives, data handling to give some examples. Be that as it may, viable acknowledgment of this innovation is met various security and p rotection concerns, which are to be alleviated for enormous scale effectively organization of Wireless networks innovation.

A counteractive action system is proposed to improve the digital security of Wireless networks gadgets and systems against DDOS(Denial of Service Attack) (Denial of service attack)assaults which devour the transfer speed he present day of (Wireless networks) gadgets. Since these systems are remote and self -designing and needn't bother with a prior framework and have huge unusual hub developments and association drop outs gets one of the most fundamental issues to be raised into the record. Wireless Sensor Network arrange (WSN) includes modest sensor hubs with constrained beginning vitality and is sent in detecting territory quite compelling to bring vital condition information and sending it back to end client throu gh a base station.

One of the significant issues in WSN (wireless sensor network)is vitality effective inclusion in which Significant objective of steering convention is to watch each conceivable physical space with no loss of information because of an absence of vitality or power in sensor hub. Such circumstances may happen due to over trouble on hubs when lopsided bunches are framed prompting additional correspondence overhead. LEACH conventions as far as Packet transmission, vitality dissemination and number of Nodes alive and steadiness period and we will examine the bit of leeway and burden of these conventions under different conditions.

INDEX

LIST OF FIGURES

-1

INTRODUCTION

1.1 Project Overview :

Internet of Things is creating worldwide patterns in the web -based information model encouraging the distribution of merchandise , enterprises in the worldwide storage network to arrange. Wireless networks is an application space coordinating different advancements and social fields have depicted Wireless networks as "A system of things, all of them inserted with remote sensors and associated through the internet". The main point is guarantee differing scope of things that can be associated and worked to such an extent that they can connect with themselves and clients. It is a functioning IT framework making them design capacity for building up interoperable correspo ndence conventions among the physical and the virtual characters of the things through keen interfaces in Wireless networks.

Wireless networks underpins respective ceaseless trade of detected information and data about the earth and naturally activating activities according to this present reality occasions One of the significant difficulties looked by Wireless networks world isn't extension however its security. As we as a whole realize conventional wired systems are generally more secure than their remote Wireless networks partners. Traditional foundation systems enable the traffic to go through various steering gadgets like switches, entryways and so forth which are frequently verified with profoundly designed firewalls and numerous other security the board procedures.

Remote Sensor systems are an assortment of sensor hubs whose fundamental usefulness is to screen the district where they are conveyed. The primary test issue in WSNs is how to plan conventions that would limit vitality utilization and draw out the system lifetime with required associated inclusion. These systems have been broadly utilized for checking of different physical or ecological conditions. Sensor sending can either be deterministic or irregular. In the deterministic arrangement, inclusion can be amplified because of the ideal position of sensor hubs. Arbitrary arrangements are favored when the area data isn't known apriority . At the point when sensor hubs are arbitrarily sent, barely any articles in the locale might be thickly secured and few might be meagerly secured. T he full network is one of the conditions for solid information transmission in WSNs because of its multi -bounce nature of the correspondence.

A system is considered as completely associated if each pair of hubs can correspondence and trade data with one another. This correspondence can be immediate or through different hubs Since the network is a basic capacity. Agreeable transmission and utilization of directional receiving wires are two of the most famous systems for expanding the transmission extend. A WSN can be organized or unstructured system. An unstructured WSN is one that is conveyed arbitrarily into the sensor field given a thick sensors region. Henceforth, issues, for example, identifying disappointments and network the executives turn out to be increasingly unpredictable. Availability scales the sufficiency with which the hubs can impart. Then again, the Coverage issue can be named either region inclusion issue or target inclusion issue. In the Area inclusion issue, the goal is to assemble data about a whole territory of intrigue. Then again, the objective inclusion issue worries about checking a lot of explicit areas .

1.2 The Coverage Issues :

The inclusion issues found in writing developed in three phases, to be specific, straightforward inclusion, k -inclusion, and Q -inclusion. With straightforward inclusion, each target ought to be observed by at any rate one sensor hub. Nonetheless, basic inc lusion was not adequate for remunerating hub disappointments or if there should be an occurrence of checking with more prominent precision. This made ready for k -inclusion, where each target must be observed by at any rate k sensor hubs, where k is a prede fined number consistent. Be that as it may, the k -inclusion issue appears to be unfit for applications where targets need not be observed by the very same number of sensor hubs. This prompts Q -inclusion were a lot of n targets signified by T = T1, T2, . . . , Tn ought to be observed by the number of sensor hubs indicated by Q = q1, q2, . . . , and with the end goal that targets Tj is observed by at least qj number of sensor hubs, where n is the number of targets and $1 \leq j \leq n$. The inclusion necessity relies upon the application. A few applications require total inclusion consistently, though the inclusion necessity can marginally be undermined for some different applications. In that capacity, it is basic to investigate the network part of WSN together with issues of inclusion .

1.3 Objectives:

The destinations of the task are

1. To beat the issue a crossbreed mix to improve the QoS administration is proposed in the examination paper to improve the looking through technique, a hereditary calculation is proposed

2. To improve the better quality in the transmission of parcels, he lpful getting is proposed and this methodology positively demonstrates worthier than the underlying variants of responsive conventions.

1.4 Organization of The Project

There are eight parts to this report. Albeit every part has been composed to act natura lly contained, every section expands on the after effects of going before part. The substance of every part is abridged underneath.

2: Literature Survey

Portrays about the review of the undertaking related papers. It likewise involves the benefits and disadvantages of those papers.

3: System Analysis

Depicts the current framework, its constraints, proposed framework, investigate commitment an d points of interest of the proposed framework.

4: Experimental Investigations

Depicts the test examinations and results.

5: Experimental Results

It portrays the exploratory outcomes.

6: Discussion of Results

Depicts execution and test results.

7: Conclusion

Depicts the finish of the undertaking.

8 : Bibliography

Depicts the book reference and references of the undertaking.

-2

LITERATURE SURVEY

Defense scheme to protect Wireless networks from cyberattacks using AI Principles :

Ahamad Ahanger, Tariq. (2018) International Journal o f Computer Communication and control. The proposed model for associated target k inclusion issues in heterogeneous remote sensor systems. They utilized two calculations in particular incorporated associated target k -inclusion calculation and appropriated a ssociated target k -inclusion calculation to give vitality proficient and inclusion of heterogeneous system. Their proposed model limited associated target k -inclusion with least k -dynamic sensor hubs. Their proposed model diminished the number of dynamic s ensor hubs and every hub can interface with sink hub to advance information. Coverage problem in wireless senor network deals with deploying sensor nodes with maximum coverage area by scheduling and analyzing sensor nodes. Connectivity in wireless sensor n etwork provides communication among sensor nodes through directly or indirectly to forward data to sink node.

Security and privacy for cloud based wireless networks : challenges :

J.Zhou, Z.cao, x.dong and A.V.Vasilakos, the proposed coverage issue in heterogeneous net work based on coverage and reach ability they formulated minimum coverage problem as intersection problem. Due et al., solved an issue for scalabilities and perform ing issues in the heterogeneous network by using differential coverage algorithms

An Overview:

K.Rose , S.Eldridge, and L.chapin, Understanding the issues and challenges of a more connected world, proposed stochastic coverage for het erogeneous network and they formulated minimum coverage problem as intersection problem. Due et al., solved an issue for scalabilities and performing issues in the heterogeneous network by using differential coverage algorithms.

An efficient algorithm to maintain discrete active sensor nodes :

et al., the proposed system is to cover all the available targets and provide connectivity among the network. They proposed an algorithm to schedule sensor nodes to increase the lifetime of network conne ctivity. The creator proposed advanced associated inclusion heuristic calculation to keep up the availability of the system with the most extreme system lifetime. Planning for sensor arrange inclusion incorporates territory inclusion and target inclusion. This creator understood objective inclusion issues in the remote sensor coordinate with streamlined associated inclusion calculation.

Linear programming and greedy based technique to solve coverage problem in sensor network :

Cardei . In their proposed work, the sensor nodes cover more than one coverage set and thus it increases the number of coverage set in the network. Greedy based target coverage algorithm was proposed to maximize the number of sensor coverage sets by maintaining and managing poorly target nodes. Based on cost function the authors proposed heuristic methodology to manage poorly connected targets and improve the lifetime of network.

Wireless networks : A comprehensive study of security issues and defensive mechanisms :

T.A. Ahanger and A. Aljumah . The proposed stochastic coverage for heterogeneous network and they formulated minimum coverage problem as intersection problem. Due et al., solved an issue for scalabilities and perform ing issues in the heterogeneous network by using di fferential coverage algorithms.

-3

SYSTEM ANALYSIS

3.1 Existing System:

In the ongoing time, with the colossal development of web and system innovation, interruption identification, counteractive action, and barrier strategies have accomplished an incredible speed. The fundamental reason for an Intrusion Detection Systems to recognize and stipulate plausible securit ies issues and many breakdown in the framework. Intrusion Detection System overview report was referenced in and there is a portion of the chose that have I ntrusion Detection System t heir base on scientific investigation. The first and most significant supposition of this exploration is to have a current, Intrusion Detection System is Flexible Wireless networks Intrusion Detection System . The utilization of broke down measurable log information and satisfactory reportage is the foundation of an adaptable Wireless networks interruption discovery framework.

Two classifications of the hubs are accepted by in the proposed typical Wireless networks hubs and Intrusion

location hubs where the current Wireless networks framework is utilized by these I ntrusion Detection System

hubs to make the administration arrange. After a characterized sift hold time all the chose I ntrusion Detection System hubs to send the gathered data parcels to the primary Intrusion Detection System station that is identified with the system exercises. Following this method, the consolidated log document information is controlled utilizing criminological investigation an d a report created. Information data is contained in these of the log documents of parcel -level like bundle size, parcel type, hub ID, occasion type, steering convention information, and time stamps. The algo utilized for criminological examination utilises end technique where the outcomes are recovered as Intrusion Detection System redundancy's utilizing a pool of sequential log search systems. Along these lines, in light of such existing Intrusion Detection System models, I have endeavored to improve the functionalit y and arranged an aversion strategy for DDOS(Denial of Service Attack) assaults. A mapping of

Intrusion Detection System investigation is given by report and these could be only an occurrence of things to come of the general evaluation for a particular timeframe of the system security. A set 'R' is keeping up the rundown of recognized pernicious hubs, their assault portrayal that thus give the assault data like sort of assault, cooperation classification the identified assailants rundown and

it is effectively conceivable to produce an APD after measurably examining the event and conduct of the aggressor hubs. This profile database can give a factual examination of the qualities of each malignant hub for a longer period. These outcomes produce the likelihood to get to the fundamental data to counteract the future comparable assaults. Intrusion Detection System DDOS(Denial of Service Attack) assaults

principle point is to diminish the exhibition of the system explicitly administration and asset openness and utilizing APD, it can get composed evidence of the hubs being malevolent and the extent of the assault and a report will be created after each id cycle. Boycott table hubs are considered with a higher probability of being malevolent. As a guarded computing , the framework's reactive plan, the usefu lness of these chose hubs will be diminished and named as dishonest and will be confined from having any job in making any influence of the system course and in some basic conditions these hubs pronounced as inept and those are segregated from a system completely. Since the exact report produced from the interruption discovery framework understands the likelihood to get the data of the action of certain hubs, these hubs are set apart in the boycott table and their usefulness and exercises are observed and assessed as an individual from the group and as a group too.

FLOW CHART FOR EXISTING SYSTEM

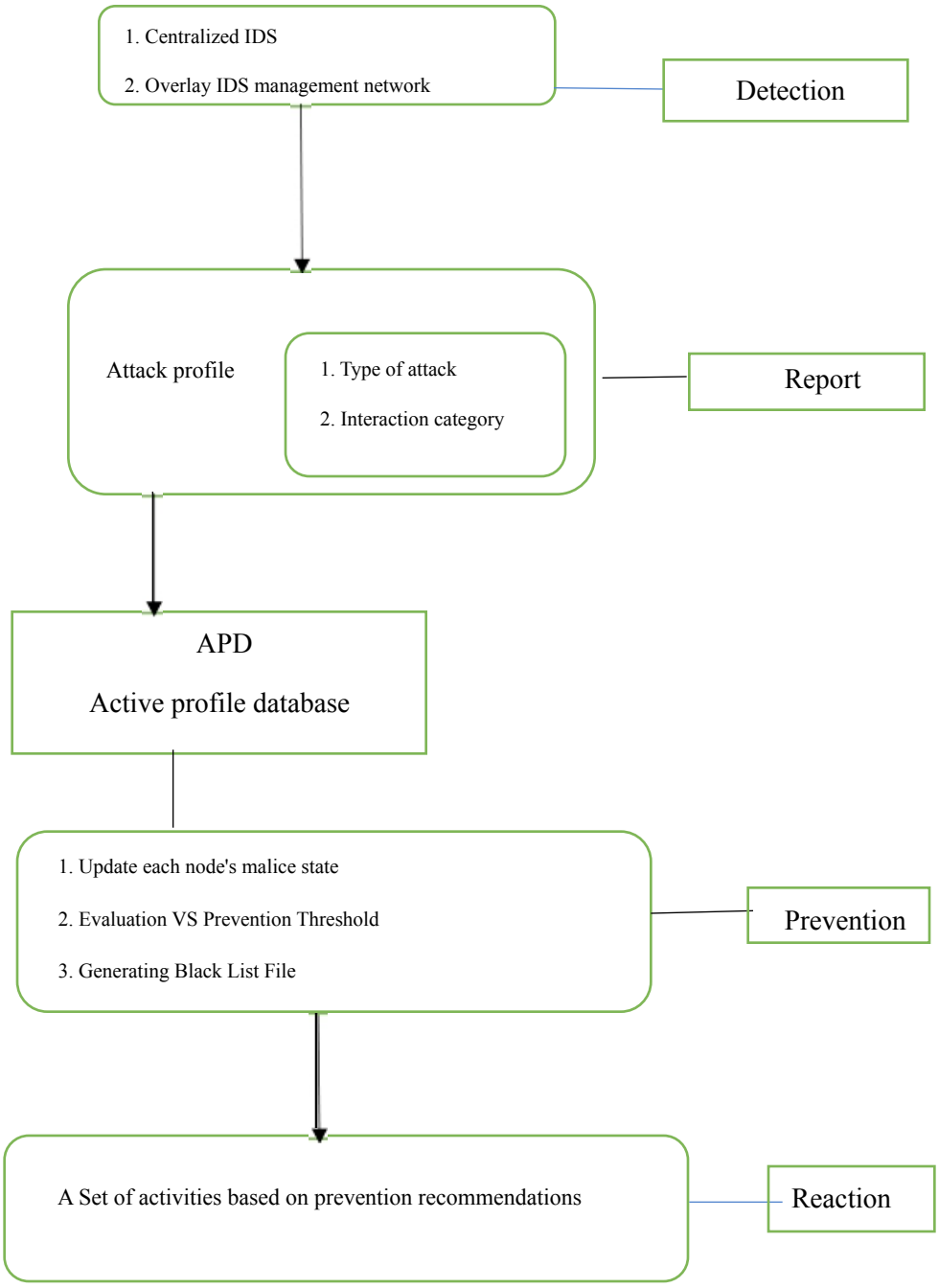


Figure 3.1 : Proposed security system overview

The above flow chart is the proposed security system for intrusion prevention detection algorithm in Wireless networks. The main purpose of an IDS to identify and stipulate probable security issues and breakdowns in the system. An IDS survey report is mentioned in and there are some of the selected IDS that have their base on forensic analysis . Two classifications of the hubs are accepted by in the proposed IPAM (interruption Prevention Algorithm in Wireless networks): ordinary Wireless networks hub s and Intrusion location hubs where the current Wireless networks framework is utilized by these IDS hubs to make the administration arrange. After a characterized sift hold time all the chose IDS hubs send the gathered data parcels to the principle IDS station that is identified with the system exercises. Following this strategy, the consolidated log document information is controlled utilizing legal investigation and a report is produced. The information data is contained in these log documents of bundle level like par cel size, bundle type, hub ID, occasion type, steering convention information and time stamps. The measurable investigation utilizes disposal strategy where the outcomes are recovered as IDS reiteration's utilizing a pool of back to back log search methods . Along these lines, in light of such existing IDS models, I have made an endeavor to improve its functionalities and arranged an anticipation system for DDOS(Denial of Service Attack) assaults. After that the reaction at last is a set of activities based on prevention recommendati ons.

ALGORITHM FOR EXISTING SYSTEM

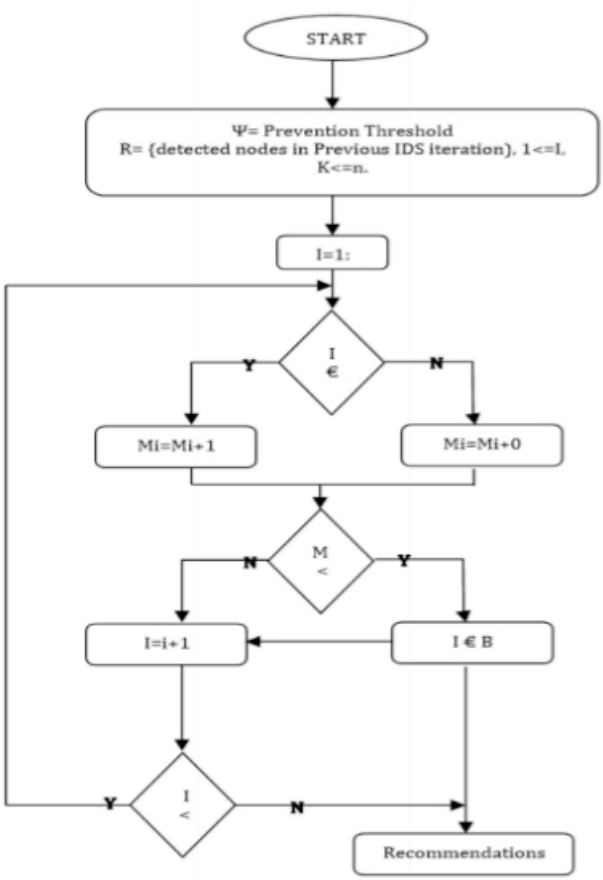


Fig. 2: Proposed IPAM algorithm flowchart

Fig3.2 -Proposed IPAM algorithm flowchart

The above flowchart is the proposed IPAM flowchart in intrusion detection technique in wireless networks. T he proposed IPAM (interruption Prevention Algorithm in Wireless networks): ordinary Wireless networks

hubs and Intrusion location hubs where the current Wireless networks foundation is utilized by these IDS hubs to make the administration organize.

3.2 Limitations :

The most generally referred to confinements of system Intrusion Prevention System are as per the following:

· The organize Intrusion Prevention System could require master tuning for adjust ing the sensor to the system and host and application conditions.

· Intrusion Prevention System sensor can't investigate traffic in appli cation layer , when the traffics load was encoded either with Intrusion Prevention System.

· The organize Intrusion Prevention System could be over-burden by arranging traffic if it is not appropriately estimated. In this way, the Intrusion Prevention System can without much stretch neglect to react to constant occasions

conveniently if it is estimated inappropriately.

· The organize Intrusion Prevention System may translate traffic inappropriately, which can prompt bogus in
negatives. This was regularly consequence of the sensor's seeing the traffic uniquely in contrast to how t o end framework or else target sees the traffic with in it .

3.3 Proposed System:

Remote Sensor organizes (WSN) include modest sensor hubs with constrained introductory vitality and are sent in detecting zone specifically compelling to bring essential condition information and sending it back to end client through a base station. One of the significant issues in WSN is vitality productive inclusion in which the significant objective of steering convention is to watch each conceivable physical space with no loss of information because of the absence of vitality or power in sensor hub. Such circumstances may happen due to over trouble on hubs when uneven bunches are framed prompting additional correspondence overhead. In this paper we are talking about the LEACH conventions regarding Packet transmission, vitality dissemination and number of Nodes alive and steadiness period and we will examine the bit of leeway and disservice of these conventions under different conditions.

The plan of WSN is im pacted by numerous variables, for example, starting vitality, versatility, creation costs, detecting condition, and system topology and power utilization of sensor hubs. Thusly structuring remote sensor organize is a difficult undertaking when inclusion al ongside arranges lifetime is considered. There leave a tradeoff among inclusion and system lifetime provided that we consider full inclusion at that point organize lifetime get diminished and on the off chance that we attempt to build arrange lifetime, at that point inclusion gets decreased.

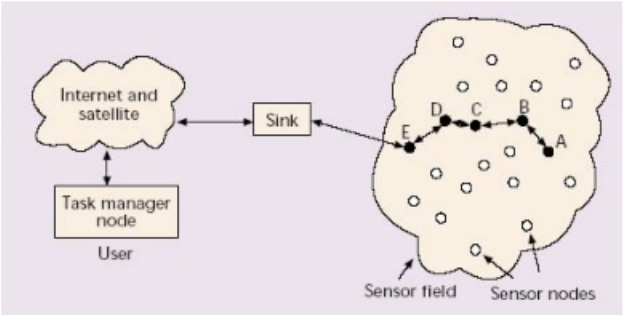


Figure 3 . 3 : Information flow in wireless sensor network

In any network, sensor node consists of the internet and satellite and task manager node as the user and it through the sink it will goes to sensor field and the sensor nodes and the connection of the nodes establishes there in the closed network.

3.4 Advantages :

The drain is appropriated. The drain doesn't require the control data from the base station, and the hubs do es not require the information on worldwide system s with the end goal for L each to work.

Filter decreases vitality by multiple times as the contrast with direct transmission and least transmission vitality steering.

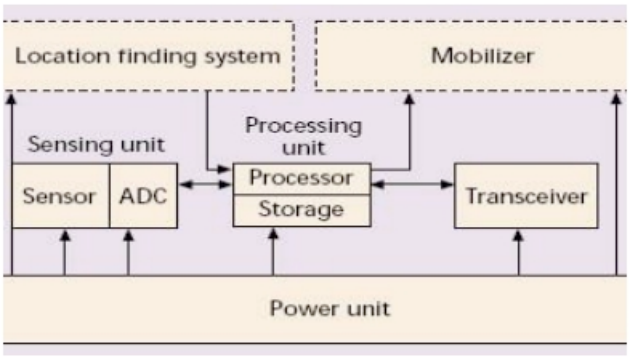


Figure 3 . 4 : The components of a wireless sensor node

In any network, sensor node consists of four basic components, as shown i n the following Figure 3.4 , a sensing unit, a processing unit, a transceiver unit, and a power unit. They may also have additional application dependent components such as a location finding system, power generator and mobilize.

Interruption Detection is an exceptionally dynamic and significant research region in Security writing. We won't endeavor to study or classify the exploration around there, however, we note that the birthplace of the issue is frequently credited to and a few scientific classifications and study examine be found, for example. Regularly all methods in known interruption recognition frameworks are falling under two significant standards: abnormality disco very, as indicated by which traffics unique in relation to typical ones could be deciphered liable to be an assault, and mark detection as per traffic significantly like referred to assault traffic could be translated prone to be a similar assault. The two sta ndards offer focal points and impediments, and numerous ongoing frameworks join the two standards, instead of specifically picking one of them. In spite of the enormous measure of research around there, no settled basic structure exists for the plan and inv estigation of interruption discovery frameworks. A normal inquire about a paper in the area proceeds describing some new ideas for detecting and justifies their legitimacy by depicting a specific execution experience where both the pace of 'bogus positives' and the pace of 'bogus negatives' are low. An eminent special case is a fundamental paper of, which provides various substantial and formal rules for the design and tools for the analysis of intrusion d escry systems..

-4

EXPERIMENTAL INVESTIGATION

4.1 TOOLS USED:

4.1.1 Mat lab:

MATLAB is composed to give access the to the framework programming is created by the LINPACK and the EISPACK ventures, which both speak to the edge programming for grid calculation s . MATLAB was developed by the contributions from so many clients .

4.1.2 Cisco Packet Tracer :

Bundle Tracer is the visual reenactment instrument by Cisco Systems that enables clients to make and organize topologies and the impersonate current PC systems. The product enables the clients to recreate the Cisco switches and the switches utilizing mimicked direction line interface. The product enables the clients to recreate the Cisco switches and switches utilizing a mimicked direction line interface . Beforehand under studies took the crack at a CCN A program could uninhibitedly download s and utilize s the instrument s for nothing out of pocket for instructive use only.

4.1.3 Clustering:

The open -source grouping programming accessible here actualize the most regularly utilized bunching strategies for quality articulation information investigation. Bunching strategies can be utilized in a few different ways. Group 3.0 gives a Graphical User Interface to access to the bunching schedules. It is accessible for Windows, Mac OS X, and Linux/Unix. Python clients can get to the grouping schedules by utilizing Pycluster, which is an augmentation module to Python. Individuals that need to utilize the grouping calculations in their very own C, C++, or Fortran projects can download the source code of the C Clustering Librar y.

Step 1: The distinct confines are set for Shortest Path route.

Step 2: Casual values are produced among confines.

Step 3: The values of produced routes have put into function of object

Step 4: The fitness evaluation will be completed for the numerous routes fmax (n, 1) = max (fx (n, 1))

fmin(n,1) = min(fx(n,1) for i=1:z ft(i,1) = (fmax(n,1) - fmin(n,1)) - fx(n,1); end ftb = mean (ft); for

i=1:z rl (i, 1) = ft (i, 1)/ftb; end

Step 5: The best fit will be estimated rely on above formula.

Step 6: Assortment based on roulette wheel thought will be completed, the values offering the best fit

being provided a high percentage on wheel re gion so that values giving a best fit have high probability

of generating an offspring.

Step 7: Crossover will executed on strings utilizing midpoint crossover.

Crossover offers integration of extra features in off springs formed.

Step 8: Mutation will be completed whether consecutive iteration values have the similar.

Step 9: The novel routes, which satisfy the minimization object, & associated factors have plotted.

Where: fx be the fitness value; ft=normalized fx

Sample Code:

```
function LEACH()

n=200;
%Initial Energy
Eo=0.1;
xm=100;
ym=100;

%x and y Coordinates of the Sink
sink.x=1.5*xm;
sink.y=0.5*ym;

%Optimal Election Probability of a node
%to become cluster head
p=0.2;

%Eelec=Etx=Erx
ETX=50*0.000000001;
ERX=50*0.000000001;
%Transmit Amplifier types
```

```
Efs=10*0.000000000001;
Emp=0.0013*0.000000000001;
%Data Aggregation Energy
EDA=5*0.000000001;

%Values for Hetereogeneity
%Percentage of nodes than are advanced
m=0.5;
%\alpha
a=1;

%maximum number of rounds
%rmax=input('enter the number of iterations you want to run : ');
rmax=50;

%%%%%%%%%%%%%%%%%%%%%%%%%%%% END OF PARAMETERS %%%%%%%%%%%%%%%%%%%%%%%%%%%%

%Computation of do
do=sqrt(Efs/Emp);

%Creation of the random Sensor Network
figure,
hold off;
for i=1:1:n
    S(i).xd=rand(1,1)*xm;
    XR(i)=S(i).xd;
    S(i).yd=rand(1,1)*ym;
    YR(i)=S(i).yd;
    S(i).G=0;
    %initially there are no cluster heads only nodes
    S(i).type='N';
```

```
    temp_rnd0=i;
    %Random Election of Normal Nodes
    if (temp_rnd0>=m*n+1)
        S(i).E=Eo;
        S(i).ENERGY=0;
       plot(S(i).xd,S(i).yd,'o-r');
        hold on;
    end
    %Random Election of Advanced Nodes
    if (temp_rnd0<m*n+1)
        S(i).E=Eo*(1+a);
        S(i).ENERGY=1;
       plot(S(i).xd,S(i).yd,'+');
        hold on;
    end
end

S(n+1).xd=sink.x;
S(n+1).yd=sink.y;
plot(S(n+1).xd,S(n+1).yd,'o', 'MarkerSize', 12, 'MarkerFaceColor', 'r');
figure(1);
% figure(1)
%  plot(o1,o2,'^','LineWidth',1, 'MarkerEdgeColor','k', 'MarkerFaceColor','y', 'MarkerSize',12);
%    hold on
%First Iteration
%counter for CHs
countCHs=0;
%counter for CHs per round
rcountCHs=0;
cluster=1;
```

```
countCHs;
rcountCHs=rcountCHs+countCHs;
flag_first_dead=0;

for r=0:1:rmax
   r;

  %Operation for epoch
  if(mod(r, round(1/p) )==0)
    for i=1:1:n
       S(i).G=0;
       S(i).cl=0;
    end
  end

hold off;

%Number of dead nodes
dead=0;
%Number of dead Advanced Nodes
dead_a=0;
%Number of dead Normal Nodes
dead_n=0;

%counter for bit transmitted to Bases Station and to Cluster Heads
packets_TO_BS=0;
packets_TO_CH=0;
%counter for bit transmitted to Bases Station and to Cluster Heads
%per round
PACKETS_TO_CH(r+1)=0;
PACKETS_TO_BS(r+1)=0;
```

```
figure(1);

for i=1:1:n
   %checking if there is a dead node
   if (S(i).E<=0)
      plot(S(i).xd,S(i).yd,'^','LineWidth',1, 'MarkerEdgeColor','k', 'MarkerFaceColor','y', 'MarkerSiz
8);
       dead=dead+1;
       if(S(i).ENERGY==1)
          dead_a=dead_a+1;
       end
       if(S(i).ENERGY==0)
          dead_n=dead_n+1;
       end
       hold on;
   end
   if S(i).E>0
       S(i).type='N';
       if (S(i).ENERGY==0)
    plot(S(i).xd,S(i).yd,'o','LineWidth',1, 'MarkerEdgeColor','k', 'MarkerFaceColor','g', 'MarkerSize
8);
       end
       if (S(i).ENERGY==1)
       plot(S(i).xd,S(i).yd,'+','LineWidth',3, 'MarkerEdgeColor','k', 'MarkerFaceColor','r',
'MarkerSize',8);
       end
       hold on;
   end
end
```

```
plot(S(n+1).xd,S(n+1).yd,'x','LineWidth',1, 'MarkerEdgeColor','k', 'MarkerFaceColor','r', 'MarkerSize',8);


STATISTICS(r+1).DEAD=dead;
DEAD(r+1)=dead;
DEAD_N(r+1)=dead_n;
DEAD_A(r+1)=dead_a;
%          plot(S(n+1).xd,S(n+1).yd,'o', 'MarkerSize', 12, 'MarkerFaceColor', 'r');
%          plot(S(n+1).xd,S(n+1).yd,'x','LineWidth',1, 'MarkerEdgeColor','k', 'MarkerFaceColor','r', 'MarkerSize',8);
%When the first node dies
if (dead==1)
   if(flag_first_dead==0)
      first_dead=r;
      flag_first_dead=1;
   end
end

countCHs=0;
cluster=1;
for i=1:1:n
  if(S(i).E>0)
  temp_rand=rand;
  if ( (S(i).G)<=0)

 %Election of Cluster Heads
 if(temp_rand<= (p/(1-p*mod(r,round(1/p)))))
          countCHs=countCHs+1;
          packets_TO_BS=packets_TO_BS+1;
          PACKETS_TO_BS(r+1)=packets_TO_BS;
```

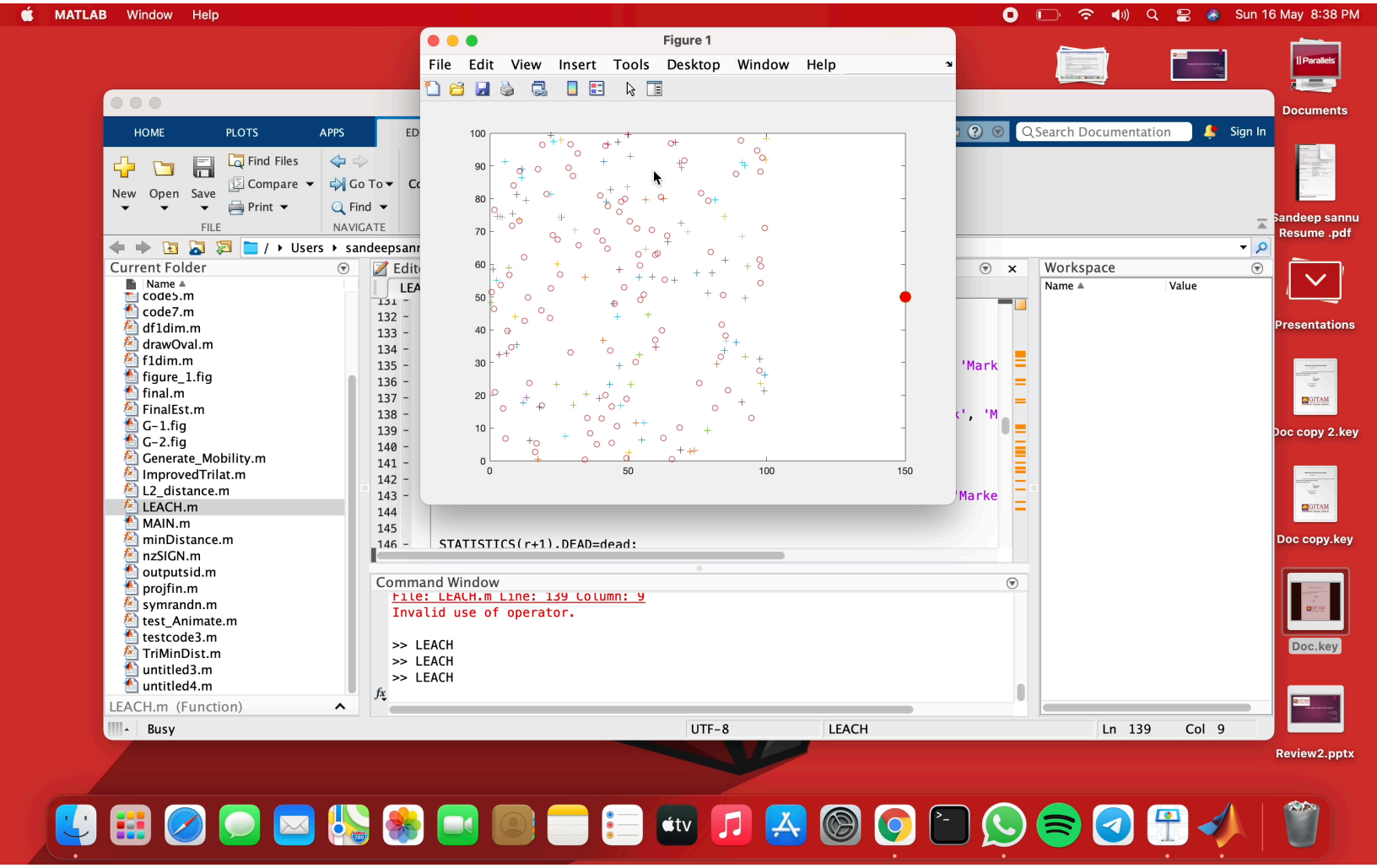
```
        S(i).type='C';
        S(i).G=round(1/p)-1;
        C(cluster).xd=S(i).xd;
        C(cluster).yd=S(i).yd;
         plot(S(i).xd,S(i).yd,'k*');

        distance=sqrt( (S(i).xd-(S(n+1).xd) )^2 + (S(i).yd-(S(n+1).yd) )^2 );
        C(cluster).distance=distance;
        C(cluster).id=i;
        X(cluster)=S(i).xd;
        Y(cluster)=S(i).yd;
        cluster=cluster+1;

        %Calculation of Energy dissipated
        distance;
        if (distance>do)
            S(i).E=S(i).E- ( (ETX+EDA)*(4000) + Emp*4000*( distance*distance*distance*distance ));
        %S(i).E=S(i).E- ( (ETX+EDA)*(4000) + Emp*4000*( distance*distance*distance*distance ));
        end
        if (distance<=do)
            S(i).E=S(i).E- ( (ETX+EDA)*(4000)  + Efs*4000*( distance * distance ));
        %S(i).E=S(i).E- ( (ETX+EDA)*(4000)  + Efs*4000*( distance * distance ));
        end
        Energy_disp(r+1) =  S(i).E;
    end

  end
 end
end
```

```
STATISTICS(r+1).CLUSTERHEADS=cluster-1;
CLUSTERHS(r+1)=cluster-1;

%Election of Associated Cluster Head for Normal Nodes
for i=1:1:n
  if ( S(i).type=='N' && S(i).E>0 )
    if(cluster-1>=1)
      min_dis=sqrt( (S(i).xd-S(n+1).xd)^2 + (S(i).yd-S(n+1).yd)^2 );
      min_dis_cluster=1;
      for c=1:1:cluster-1
         temp=min(min_dis,sqrt( (S(i).xd-C(c).xd)^2 + (S(i).yd-C(c).yd)^2 ) );
         if ( temp<min_dis )
            min_dis=temp;
            min_dis_cluster=c;
         end
      end

      %Energy dissipated by associated Cluster Head
          min_dis;
          if (min_dis>do)
             S(i).E=S(i).E- ( ETX*(4000) + Emp*4000*( min_dis * min_dis * min_dis * min_dis));
          end
          if (min_dis<=do)
             S(i).E=S(i).E- ( ETX*(4000) + Efs*4000*( min_dis * min_dis));
          end
       %Energy dissipated
       if(min_dis>0)
        distance=sqrt( (S(C(min_dis_cluster).id).xd-(S(n+1).xd) )^2 + (S(C(min_dis_cluster).id).yd-(S(n+1).yd) )^2 );
         S(C(min_dis_cluster).id).E = S(C(min_dis_cluster).id).E- ( (ERX + EDA)*4000 );
if (distance>do)
             S(C(min_dis_cluster).id).E=S(C(min_dis_cluster).id).E- ( (ETX+EDA)*(4000) +
Emp*4000*( distance*distance*distance*distance ));
          end
```

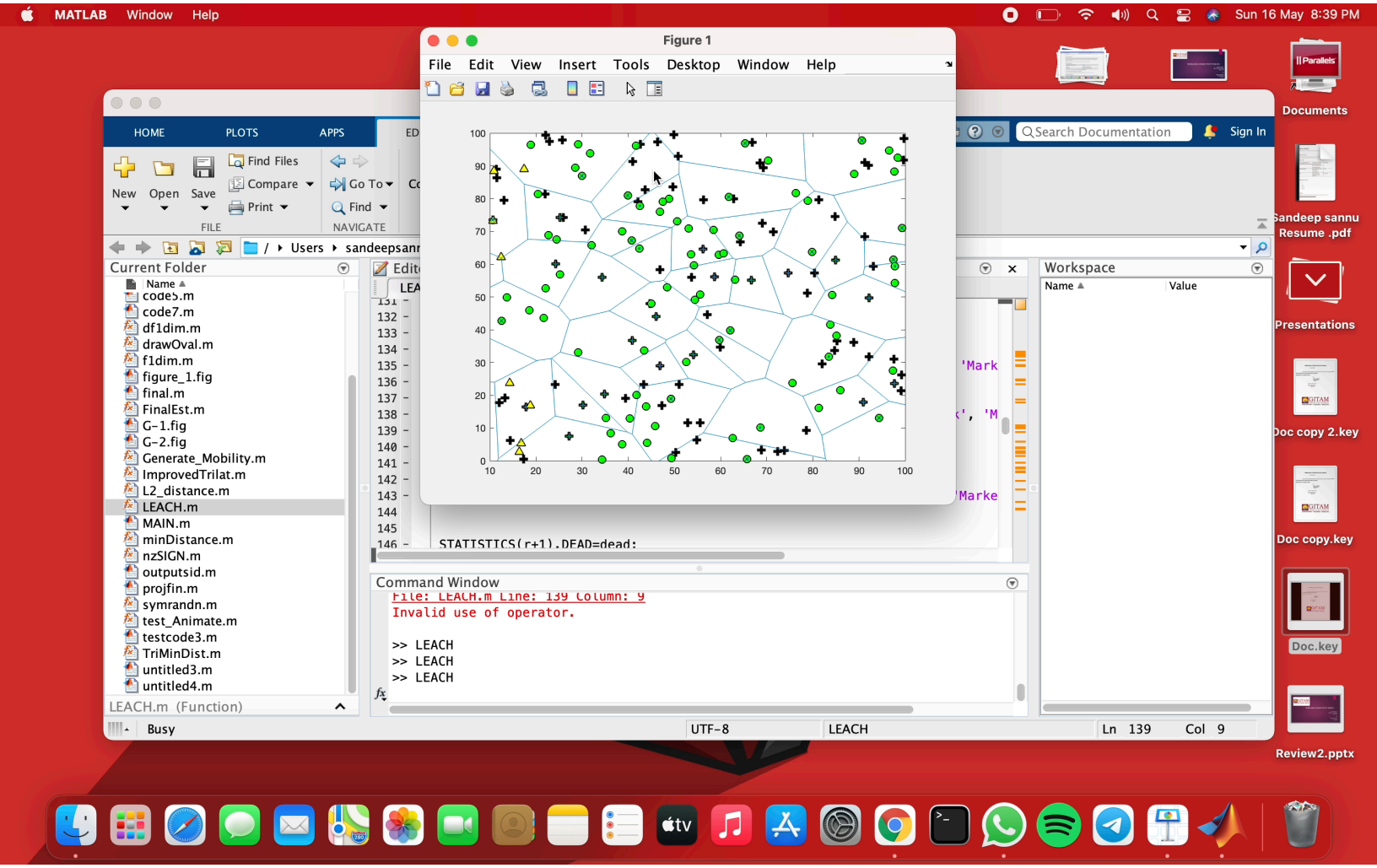
```
 if (distance<=do)
              S(C(min_dis_cluster).id).E=S(C(min_dis_cluster).id).E- ( (ETX+EDA)*(4000)  +
Efs*4000*( distance * distance ));
           end
          PACKETS_TO_CH(r+1)=n-dead-cluster+1;
        end

       S(i).min_dis=min_dis;
       S(i).min_dis_cluster=min_dis_cluster;

    end
 end
end
hold on;

countCHs;
rcountCHs=rcountCHs+countCHs;
sum=0;
for i=1:1:n
if(S(i).E>0)
    sum=sum+S(i).E;
end
end
avg=sum/n;
STATISTICS(r+1).AVG=avg;
sum;
```

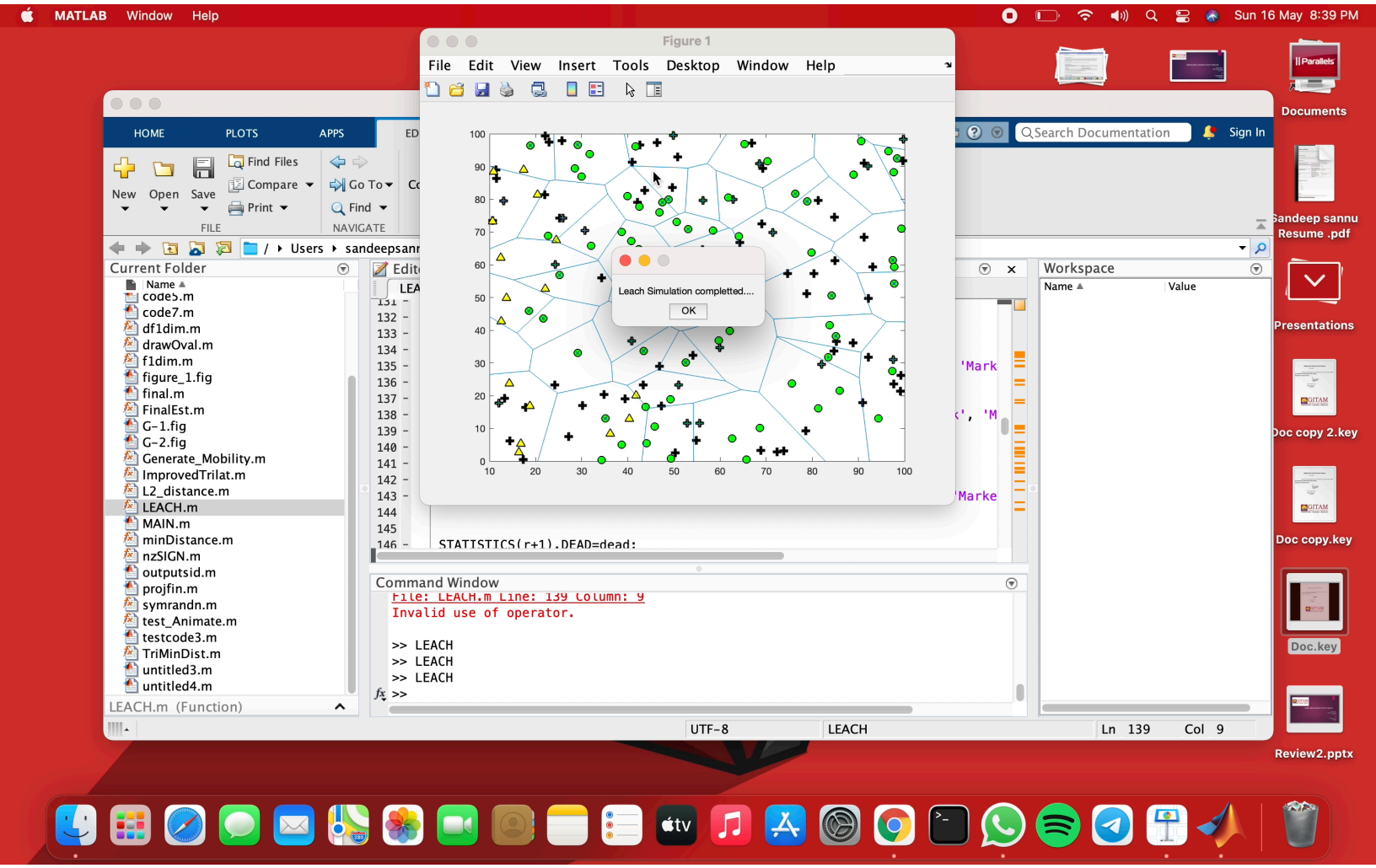
```
%Code for Voronoi Cells
%Unfortynately if there is a small
%number of cells, Matlab's voronoi
%procedure has some problems
warning('OFF');
[vx,vy]=voronoi(X(:),Y(:));
plot(X,Y,'g+',vx,vy,'m-');
hold on;
voronoi(X,Y);
axis([10 xm 0 ym]);

end
msgbox('Leach Simulation completted....');
end
```

Before Leach simulation completed:



During Leach simulation:





After Leach simulation completed.

-5

EXPERIMENTAL RESULTS

Figure 5.1: Number of nodes in the connection

The above figure represents the number of nodes in the connection . The number of nodes we want we can access those number of nodes and those nodes are represented in red color and the unknown are the minimum number of nodes taken. The horizontal area and the vertical area represent the number of nodes in the connection. The figure5.1 represents the number of nodes in the connection.

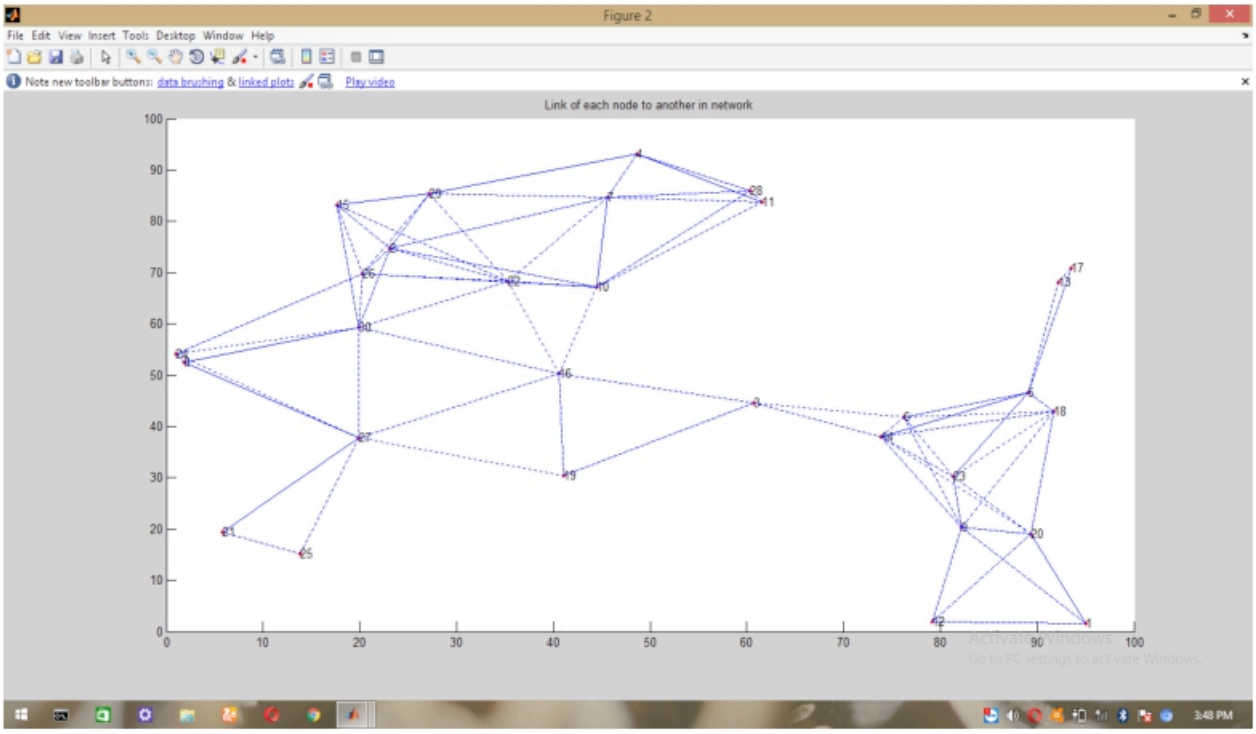


Figure 5.2: T he connection between nodes

The above figure represents the connection between the nodes . The link of each node to another in the network connection is shown here. From one node to another node the connection is raised and it is represented in the dotted blue lines and the connection is between the nodes. The figure 5.2 represents the link of each node to another node.

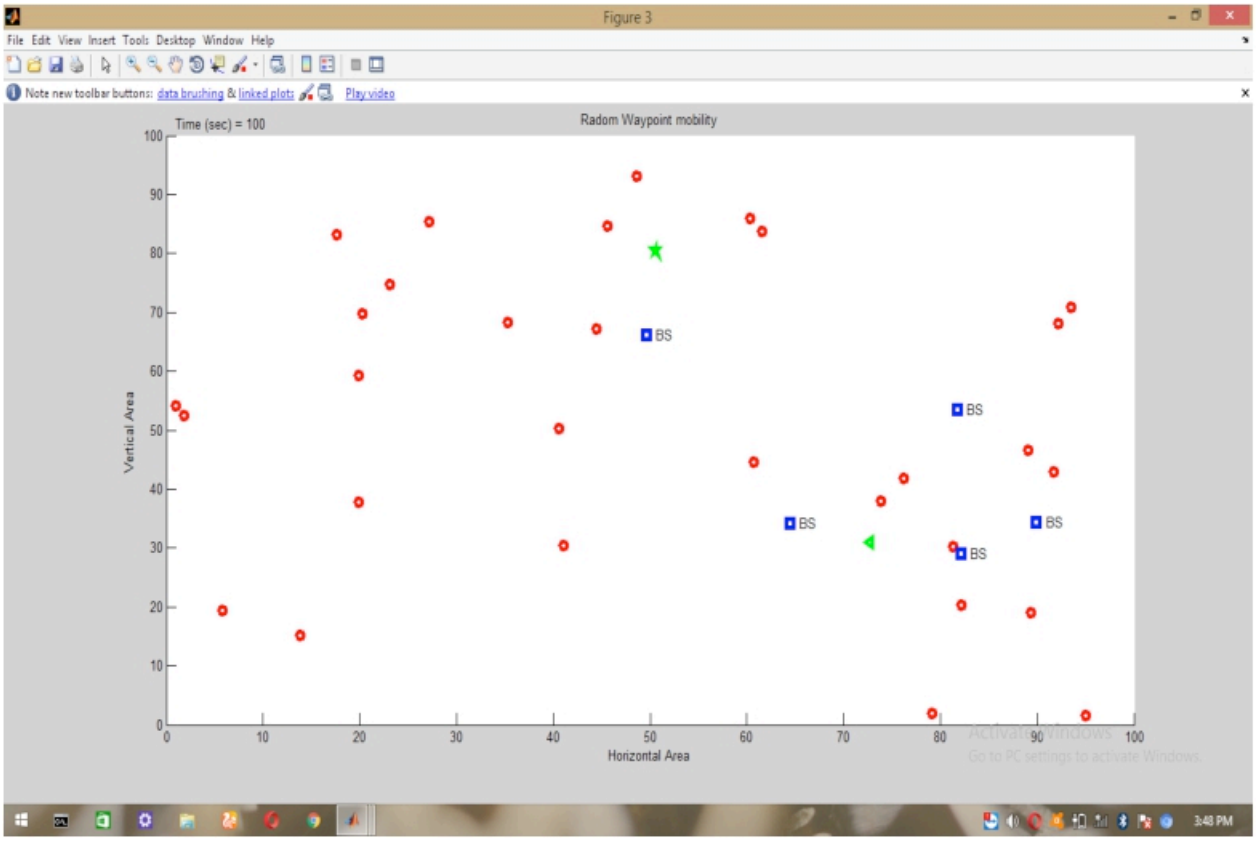


Figure 5.3: Random waypoint mobility

The above figure represents the random waypoint mobility of the nodes in the connection. The nodes mobility and the time required the mobility is done from one node to another node the mobility is done by the random waypoint mobility. The figure 5. 3 represents the random waypoint mobility of nodes in the connection.

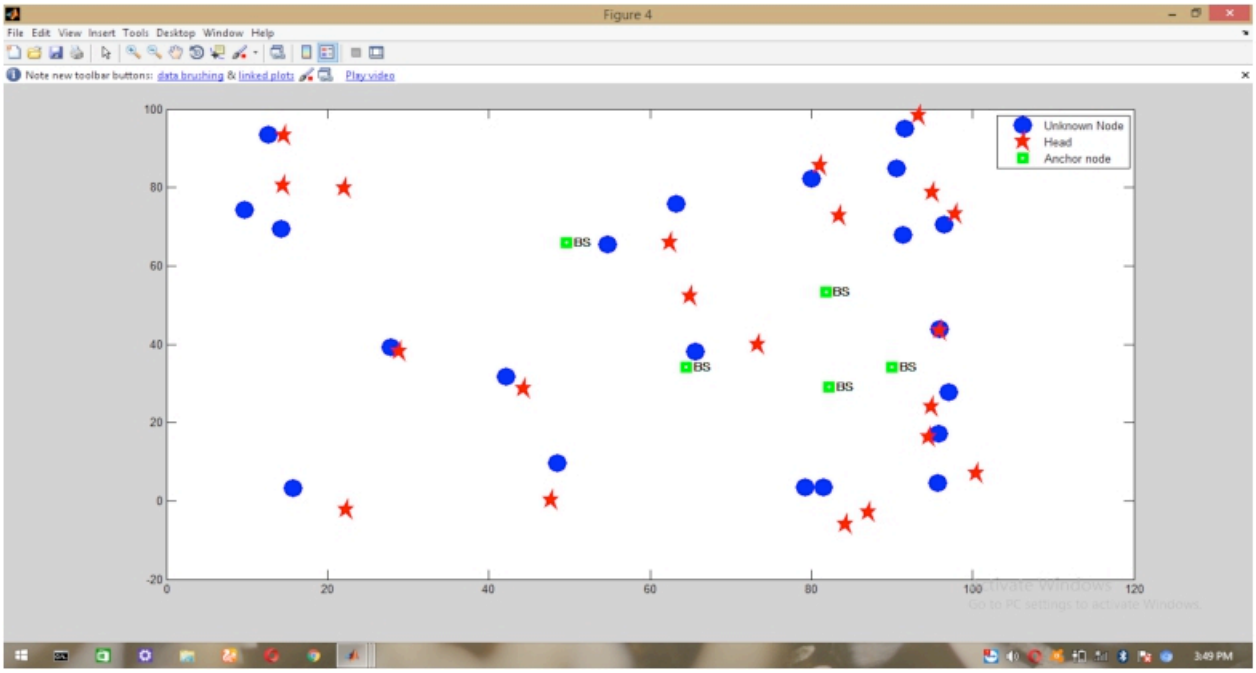


Figure 5.4: Raising a connection using the leach protocol

The above figure represents the raising a connection using the leach in the connection. The unknown node and the head and the anchor node represent here the mobility is made by the heads and the anchor nodes in the wireless connections. The figure 5.4 represents the connection raising between the nodes using leach protocol.

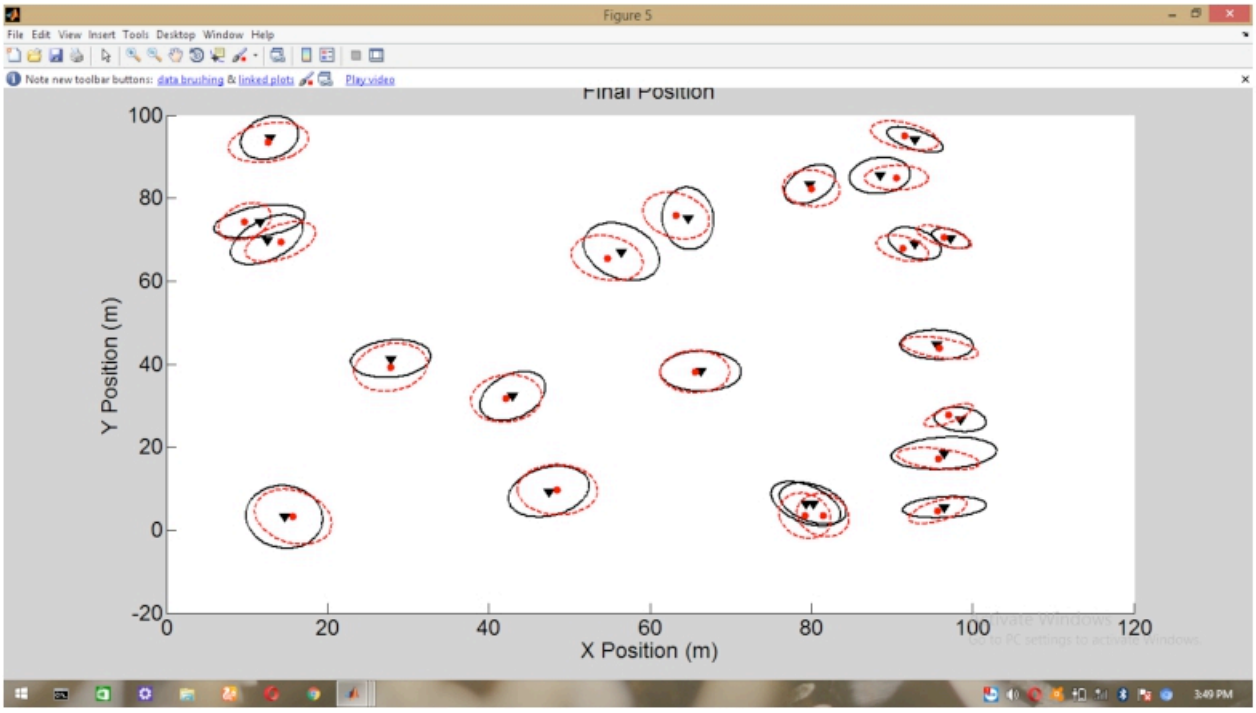


Figure 5.5 : Position of the nodes

The above figure represents final position of the nodes in a connection . The position of the nodes is represented here by the red dotted circles in the connection of the X and Y position. The nodes and mobility are done here by the connection by doing clustering. The figure 5.5 represents the final postion of nodes in the connection.

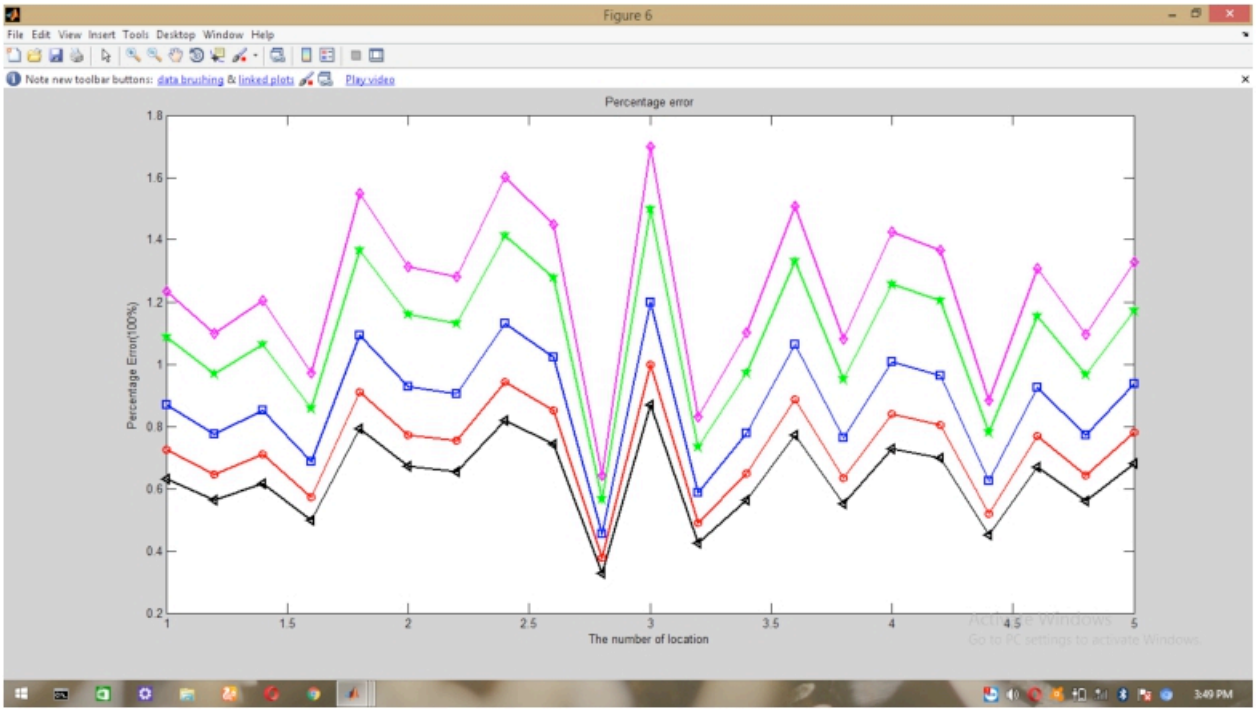


Figure 5.6: Graph of nodes location and percentage error

The above figure represents the graph of the node location and the percentage error . The number of nodes we want we can access those number of nodes and those nodes are represented in red color and the unknown are the minimum number of nodes taken. The horizontal area and the vertical area represent the number of nodes in the connection. The figure 5.6 represents the graph of the node location and the percentage error.

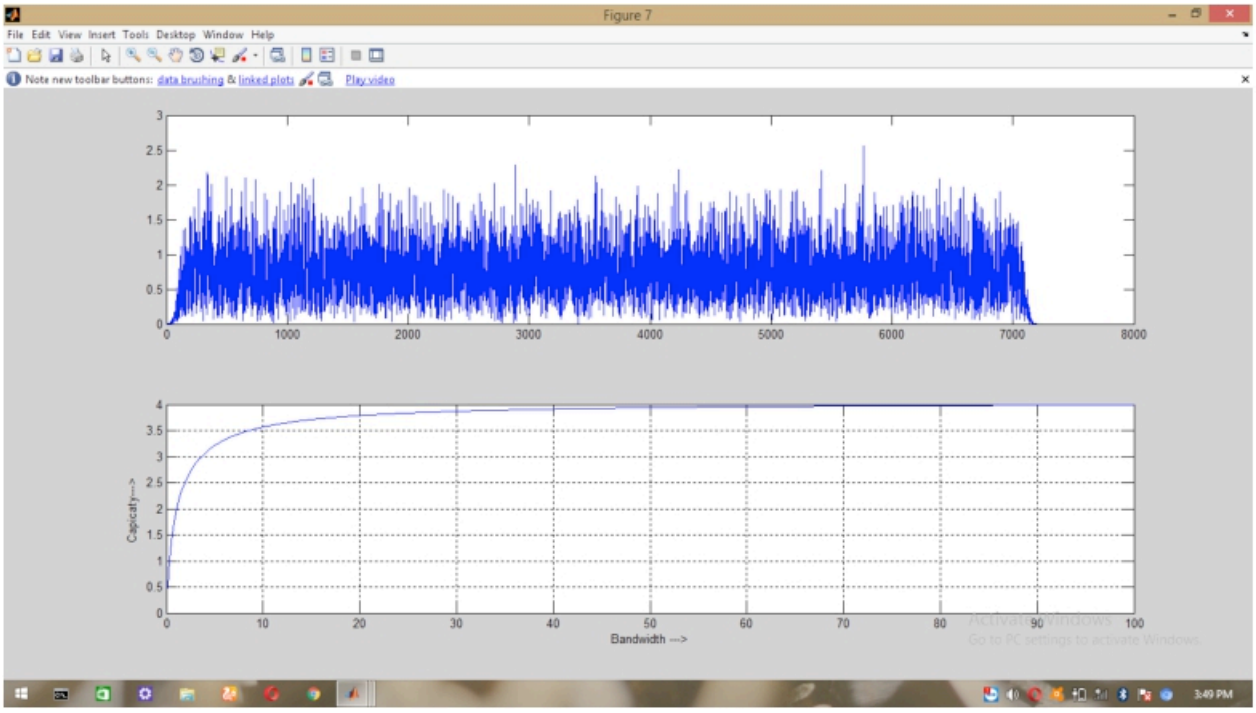


Figure 5.7: Graph of nodes bandwidth and capacity

The above figure represents the graph of the node bandwidth and capacity . The number of nodes we want we can access those number of nodes and those nodes are represented in red color and the unknown are the minimum number of nodes taken. The horizontal area and the vertical area represent the number of nodes in the connection. The figure 5. 7 represents the graph of the node bandwidth and capacity.

-6

DISCUSSION OF RESULTS

6.1 Cisco Security Agent :

The Cisco HIntrusion Prevention System is a Cisco Security Agent (CSA), which supplements the Cisco Intrusion Prevention System,

guaranteeing the dependability of uses and working systems. Pernicious activity is hindered before hurt is done by using conduct -based development that screens request rehearses. CSA guarantees against known and a new/darken attack . Living in between the piece and request s , CSA engages the most extraordinary application detectable quality with little impact on the presentation and robustness of the essential working structure. Several of the different framework security benefits CSA offers are according to the accompanying :

- Zero-update assurance lessens crisis fixing in light of powerlessness declarations, limiting patch-related personal time and IT costs.
- Visibility and control of delicate information shield against misfortune from both client activities and focused on ma lware.
- Predefined consistency and adequate use strategies permit productive administration, revealing, and inspecting of exercises.
- The framework is ensured consistently, in any event, when clients are not associated with the corporate system or do n ot have the most recent patches. This is frequently alluded to as "constantly watchful" security.
- Predefined consistency and worthy use arrangements permit effective administration, detailing, and examining of exercises.
- The framework is ensured cons istently, in any event, when clients are not associated with the corporate system or come up short on the most recent patches. This is regularly alluded to as "constantly watchful" security.
- Visibility and control of touchy information shield against mi sfortune from both client activities and focused on malware.

· The Cisco HIntrusion Prevention System is a Cisco Security Agent, of which supplements the Cisco NInt
Prevention System, ensuring
the uprightness of utilizations and working frameworks. Malignant action is obstructed before
harm is finished

6.2 Cisco results :

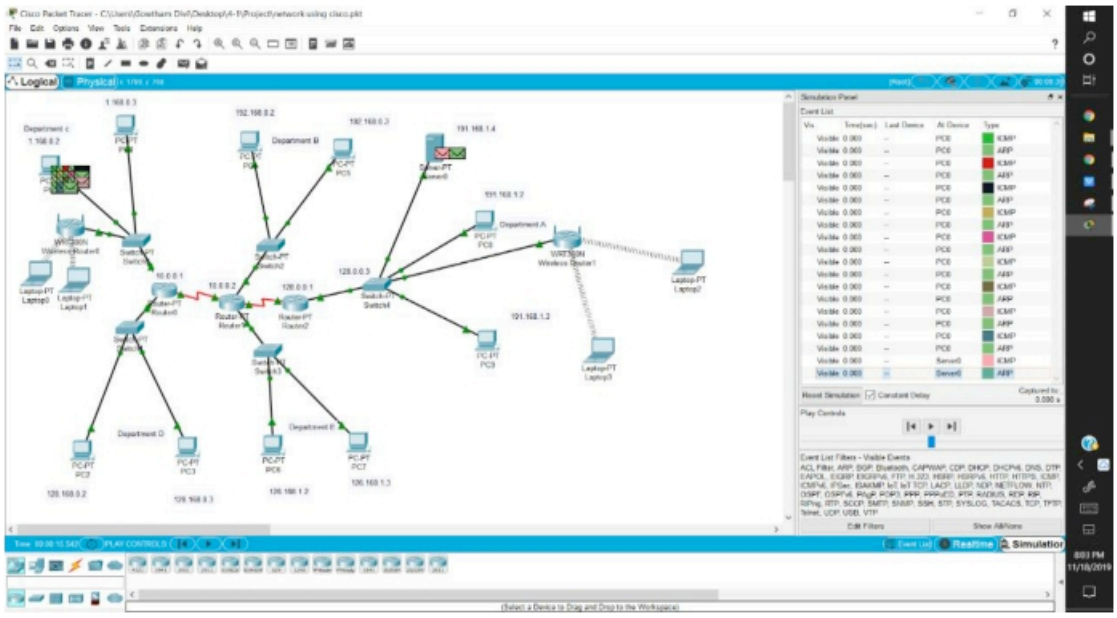


Figure 6.1: cisco network when the messages are sent

The above figure represents the cisco network when the messages are sending. When the messages are sending from one network to other by the cisco packet the packets flowing connection is seen here. The figure 6.1 represents the cisco network when the messages are sending from network to another.

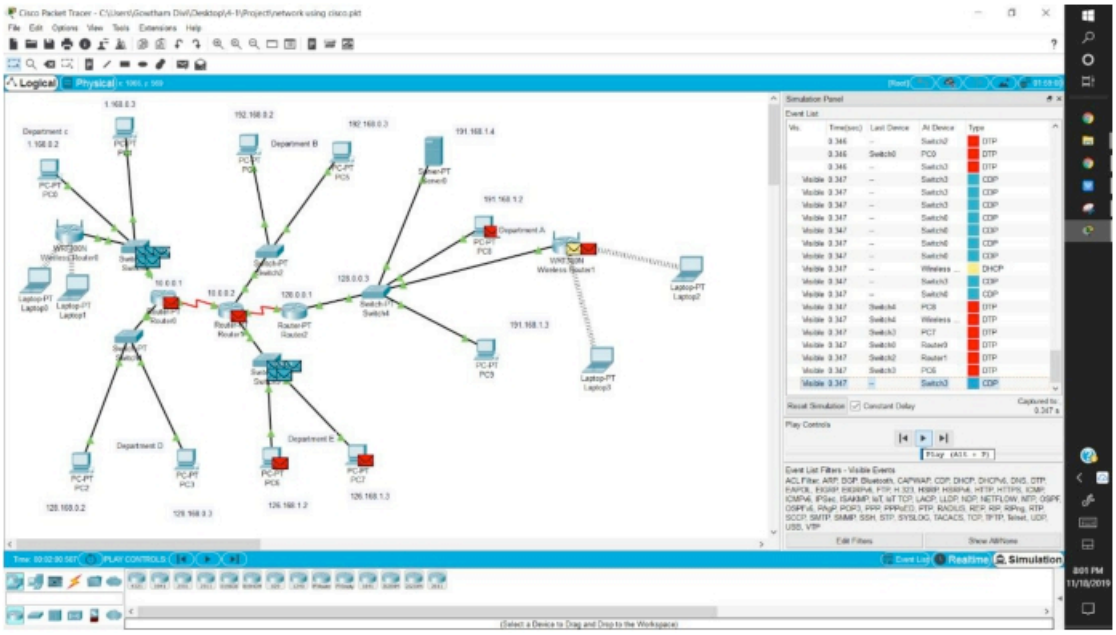


Figure 6. 2 : cisco network when the messages are drop out

The above figure represents the cisco network when the messages are drop out in the connection. When the messages are sending from one network to other by the cisco packet the packets flowing connection is seen hand some of the messages are drop out due to the connection loss in the network. The figure 6.2 represents the cisco network when the messages are drop out in the network while transferring.

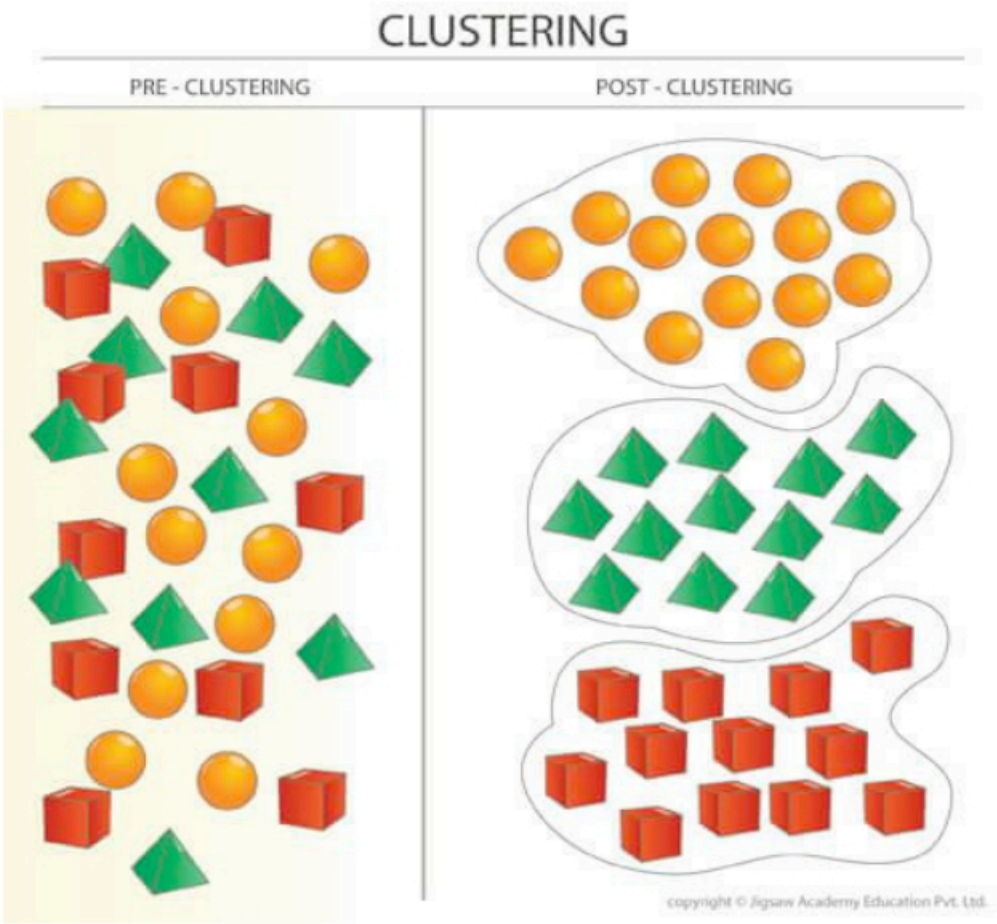


Figure 6.3: pre clustering and post clustering

Bunching is especially significant as it decides the inborn gathering among the unlabeled information present. There are no criteria for good bunching. It relies upon the client, what is the criteria they may utilize which fulfill their needs. For example, we can be keen on finding agents for homogeneous meetings (information decrease), in discovering "common bunches" and portray their unclear properties ("normal" statistics types), in finding helpful and reasonable grou pings ("valuable" statistics classes) or in finding abnormal data objects (exception recognition). This calculation must make a few presumptions which establish the closeness of focuses and every supposition make unique and similarly legitimate bunches.

Step 1: The distinct confines are set for Shortest Path route.

Step 2: Casual values are produced among confines.

Step 3: The values of produced routes have put into function of object

Step 4: The fitness evaluation will be completed for the numerous route s fmax (n, 1) = max (fx (n, 1))

fmin(n,1) = min(fx(n,1) for i=1:z ft(i,1) = (fmax(n,1) - fmin(n,1)) - fx(n,1); end ftb = mean (ft); for

i=1:z rl (i, 1) = ft (i, 1)/ftb; end

Step 5: The best fit will be estimated rely on above formula.

Step 6: Assortment based on roulette wheel thought will be completed, the values offering the best fit

being provided a high percentage on wheel region so that values giving a best fit have high probability

of generating an offspring.

Step 7: Crossover will executed on strings utilizing midpoint crossover.

Crossover offers integration of extra features in off springs formed.

Step 8: Mutation will be completed whether consecutive iteration values have the similar.

Step 9: The novel routes, which satisfy the minimization object, & associated factors have plotted.

Where: fx be the fitness value; ft=normalized fx

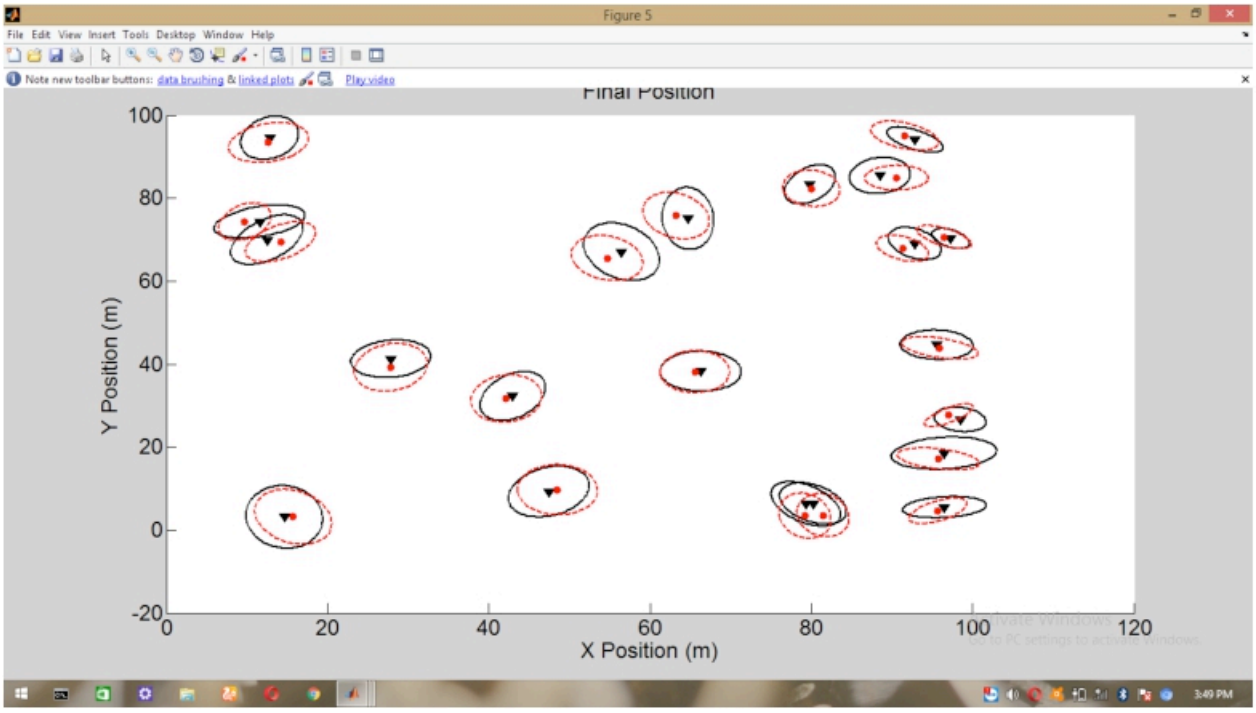


Figure 6 . 4 : Graph of nodes location and percentage error

The above figure represents the graph of the node location and the percentage error . The number of nodes we want we can access those number of nodes and those nodes are represented in red color and the unknown are the minimum number of nodes taken. The horizontal area and the vertical area represent the number of nodes in the connection. T he figure 6.4 represents the graph of the node location and the percentage error.

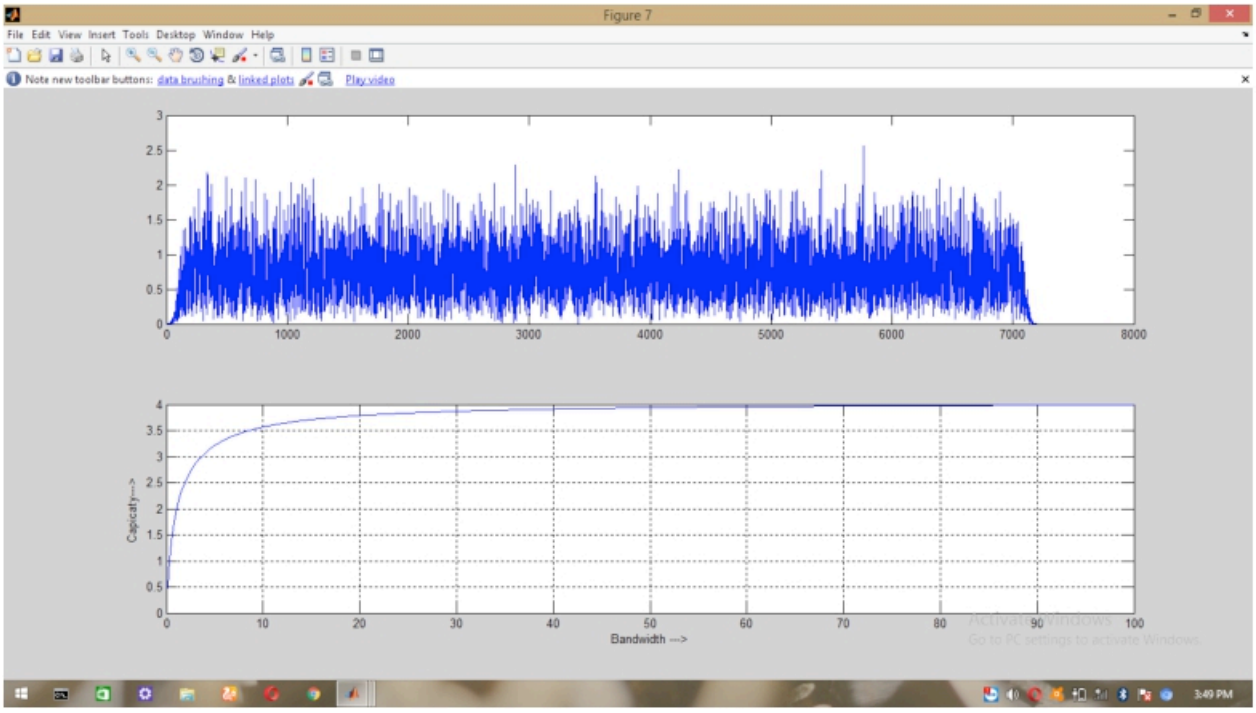


Figure 6.5 : Graph of nodes bandwidth and capacity

The above figure represents the graph of the node bandwidth and capacity . The number of nodes we want we can access those number of nodes and those nodes are represented in red color and the unknown are the minimum number of nodes taken. The horizontal area and the vertical area represent the number of nodes in the connection. The figure 6.5 represents the graph of the node bandwidth and capacity.

-7

CONCLUSION

The Magnitude of DDOS(Denial of Service Attack) and in this manner hurt as heightened with the consideration of different distinctive assault sources and along these lines making the appropriate conditions for hurting the security and execution of the Wireless networks innovation. The impact of assault and its recurrence can additionally intensify the system execution and counteract the genuine clients of the system from getting to the system administrations. This worries in conceivable securit ies procedure and proposed by an aversion plot that is good to be applied in systems that defenseless against DDOS(Denial of Service Attack) assaults. In light of the essential structure and elements of existing Intrusion Detection System , we have sued the results in proposed algo rithm in a way relating to time. Proposed algo rithm is a multiway versatile authoritatively and in fact for different security needs and is likewise customizable as indicated by the current data all the while updatable boycott table. Following this can prompt produce a proposal for response module and hence drawing closer to guarantee the system execution, security, and survivability at the hour of assault event.

FUTURE SCOPE:

The wireless networks is spreading widely and the security issues will be more so in concern of privacy in wireless connections many technologies are coming. The dropouts of the packets in wireless connections also will rectified by the leach protocol so there will be no drop outs and the connectivity issues in future. So in future there will be high secured connection packets transmitting from one network to another network with high security and high privacy so there will be no privacy and security conce rns in wireless wireless networks in future.

-8

BIBLIOGRAPHY

[1] Ahamad Ahanger, Tariq. Defense scheme to protect Wireless networks from cyber attacks using AI Principles. International Journal Of Computer Communication and control. 13. 915 - 926.10.15837/ijccc. 2018.6.3356. 2018

[2] J.Zhou, Z.C ao, X. Dong and A.V.Vasilakos, "security and privacy for cloud based wireless networks : challenges, "IEEE Commun. Mag., vol.55,no.1,pp.26 -33, jan.2017.

[3] K.Rose , S.Eldridge, and L.chapin," THE Wireless networks: AN OVERVIEW, Understanding the issues and challenges of a more connected world,"2015.

[4] L.catarinucci et al., "An Wireless networks aware architecture for smart health care systems,"IEEE,2015.

[5] R.H. Weber ."Wireless networks - new security and privacy challenges,"comput. law s ecure .rev., vol .26,pp.23 -30,2010

[6] T.A. Ahanger and A. Aljumah "wireless networks : A comprehensive study of security issues and defensive mechanisms," in IEEE access . doi:10.1109./ACCESS.2018.2876939 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnum ber=8519613&isnumber=6514899

[7] IEEE ,"towards a definition of the wireless networks (wireless networks),"2015.

[8] F. Wu, Y. Gui, Z. Wang, X. Gao, and G. Chen, "A survey on barrier coverage with sensors," Frontiers of Computer Science, vol. 10, no. 6, pp. 968 – 984, 2016.

[9] D. Tao and T. Y. Wu, "A survey on barrier coverage problem in directional sensor networks," IEEE Sensors Journal, vol. 15, pp. 876 – 885, Feb 2015.

[10] M. Li, Z. Li, and A. V. Vasilakos, "A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues," Proceedings of the IEEE, vol. 101, pp. 2538 – 2557, Dec 2013.

[11] N. Yeasmin, "k -coverage problems and solutions in wireless sensor networks: A survey," International Journal of Computer Applications, vol. 100, no. 17, 2014.

[12] P. Musilek, P. Krömer, and T. Barton, “Review of nature -inspired meth - ˇ ods for wake - up scheduling in wireless sensor networks,” Swarm and Evolutionary Computation, vol. 25, pp. 100 – 118, 2015.

[13] F. Aznoli and N. J. Navimipour, “Deployment strategies in the wireless sensor networks: Systematic literature review, classification, and current trends,” Wir eless Personal Communications, pp. 1 –28, 2016.

[14] A. Saipulla, B. Liu, and J. Wang, “Barrier coverage with airdropped wireless sensors,” in MILCOM 2008 - 2008 IEEE Military Communications Conference, pp. 1 – 7, Nov 2008.

[15] Z. Fei, B. Li, S. Yang, C. X ing, H. Chen, and L. Hanzo, “A survey of multi -objective optimization in wireless sensor networks: Metrics, algorithms and open problems,” IEEE Communications Surveys Tutorials, vol. PP, no. 99, pp. 1 – 1, 2016.

[16] M. Khalesian and M. R. Delavar, “Wireles s sensors deployment optimization using a constrained pareto -based multi - objective evolutionary approach,” Engineering Applications of Artificial Intelligence, vol. 53, pp. 126 – 139, 2016.

[17] S. K. Gupta, P. Kuila, and P. K. Jana, “Genetic algorithm a pproach for kcoverage and m - connected node placement in target based wireless sensor networks,” Computers and Electrical Engineering, pp. – , 2015.

[18] M. Xi, K. Wu, Y. Qi, J. Zhao, Y. Liu, and M. Li, “Run to potential: Sweep coverage in wireless sensor n etworks,” in 2009 International Conference on Parallel Processing, pp. 50 – 57, Sept 2009.

[19] B.Gorain and P. S. Mandal, “Approximation algorithms for sweep coverage in wireless sensor networks,” Journal of Parallel and Distributed Computing, vol. 74, no. 8, pp. 2699 – 2707, 2014.

[20] M. Li, W. Cheng, K. Liu, Y. He, X. Li, and X. Liao, “Sweep coverage with mobile sensors,” IEEE Transactions on Mobile Computing, vol. 10, pp. 1534 – 1545, Nov 2011.

CONNECTIVITY ISSUES

ORIGINALITY REPORT

12%	6%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Abdulaziz Aldaej. "Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)", IEEE Access, 2019 Publication	4%
2	www.ijrte.org Internet Source	3%
3	www.ciscopress.com Internet Source	1%
4	ijana.in Internet Source	1%
5	Submitted to International University of Malaya-Wales Student Paper	1%
6	Submitted to University of Dammam Student Paper	1%
7	Submitted to University of Hertfordshire Student Paper	1%
	Submitted to Higher Education Commission	

8	Pakistan Student Paper	<1%
9	Submitted to CSU, San Jose State University Student Paper	<1%
10	link.springer.com Internet Source	<1%

Exclude quotes	On	Exclude matches	< 14 words
Exclude bibliography	On		