ENHANCING THE SECURITY BY THE USE OF REDUNDANCY HANDLING MECHANISM AND DATA DISSEMINATION MECHANISM

Abhilasha Sharma
Mtech Scholar
SSIET,Pathankot

Vibha Dutta
Assistant Professor
SSIET. Pathankot

ABSTRACT

WSN will be the one in which data is transferred with the help of sensors. Sensors have limited energy so it cannot store large amount of data. The data transmission will be from one node to another. As the exposure of WSN increases to multiple users the security of data will be at stakes. So in the proposed paper we will be considering the security of data. The energy consumption is also minimized by the used of the proposed paper. The redundancy will be eliminated. Which means same data does not have to be transferred again and again. For this purpose the restricted access protocol will be proposed.

Keywords
WSN, Data, Restricted Access Protocol, Redundancy, energy

1. INTRODUCTION

The data which is transferred over WSN is exposed to wide variety of users. The data may be corrupted when it is transferred since data may be exposed to malicious users. The objective of this paper is to detect those malicious entries and rectify the problems if any. The data over WSN will be transferred in the form of packets. Each packet will have the sequence number associated with it. Once the data with the particular sequence number is transferred then same packet should not be transferred is the objective of this paper. The technique which is proposed is known as Selective data dissemination. The SDT will be used in combination with filtering in order to ensure that the data transferred is not corrupted. The data base of extension will be maintained. If the packet does not have the extension as contained within the database then the packet will be rejected. The specific area within the WSN is considered which MANET is. The properties of the WSN is as listed below

- Limited Energy can occur within the WSN
- There is a possibility that the point may be failed
- The nodes are wireless in nature
- Improvement in large wide geographical area will takes place
- The topologies are frequently changes
- It is relatively easy to use
- Self configurable
- Data redundancy is present

Sensor node is a small computer with limited energy, power, resources and radio transceiver. The supports stations are the main part of the WSN with huge memory, large computational power etc. All the operations are being performed by the use of this support station.

Now days the work towards the security of the data and redundancy is going on. The proposed paper is the extension of the existing work.

1.1 Architecture of the WSN

The architecture of the WSN is presented in the two ways: first is the architecture of the sensor nodes and second with the help of architecture of WSN.

1.1.1 Structure of Sensor Node

The structure of the sensor nodes will consists of four components: a sensor, a microprocessor, a radio and battery

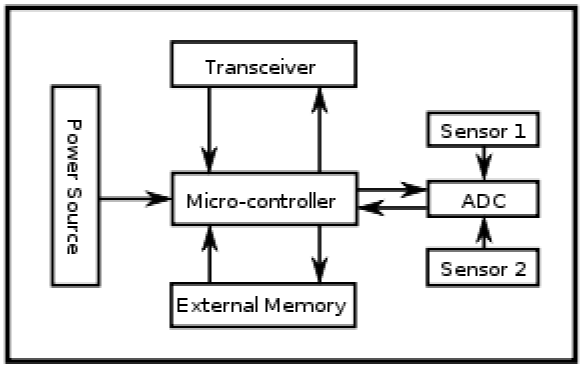


Fig 1 Showing Structure of Sensor Nodes

Sensor Unit: This unit consists of group of nodes which are used in order to transfer the data from the source to the destination. The transfer process will depend upon the conditions and environment presented. It also involve analog to digital converted which converts analog signals to digital form.

Power Source: Power source will have important role within the WSN. It contains the battery to drive the other components of the wireless system. The battery life is limited in nature.

Radio: It is a small range radio which is used for communication. The data will be transmitted with the help of radio channels. Radio transmitter and recover will exist in this case.

The Electronic Brain: The electronic brain will consist of processing using and few flash storage. The data which it receives will convert into the packet format. The packet will consist of header as well. The header will contain the information about the source and the destination. The set of microprocessors also exist in this case. The packet transfer will be efficient with the help of these microprocessors. The electronic brain will act as interface between the sensor nodes and the radio.

1.2 Network Structure

Large number of sensor nodes is deployed within the WSN. The source and destinations will exist within the WSN. The radio signals are transmitted by the sensor and if the signals intersect then the sensors are in range and data can be transmitted from the sensors in range.

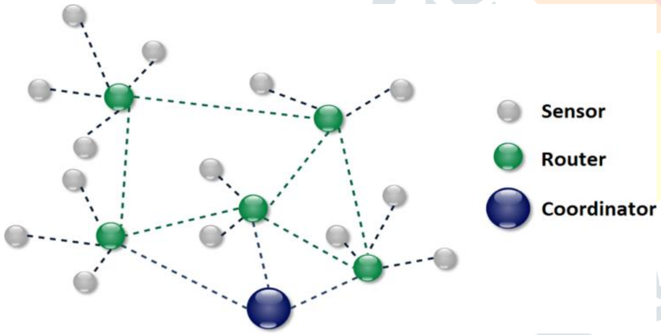


Fig 2 Structure of WSN

2. RELATED WORK

The work is being done toward the MANET. The data transmission is the prime focus of the present work. [1] In wireless ad hoc networks basic network operations are carried out through the cooperation of all available nodes. Due to the inherent lack of a managed infrastructure the nodes of an ad hoc network cannot be considered as trustworthy as in a dedicated infrastructure. Wireless ad hoc networks are thus vulnerable to various exposures threatening the basic network operations like routing and packet forwarding. This paper presents a survey of current research activities dealing with routing security, cooperation enforcement and key management in wireless ad hoc networks. Existing solutions seem to only partially address the threats and fall short of providing a comprehensive answer. Wireless security mechanisms in layer 2 that are often considered as part of the solution domain do not meet the specific requirements of wireless ad hoc networks. [2] the review of the various techniques used within the MANET will be used. The routing protocols such as AODV, DSR etc are considered in this case. [3] the review of various security aspects are considered in this case. The security aspect is important since WSN is exposed to large number of users. The users can be of malicious nature. So detection and prevention against such users is very important. [4] MANET security issues are considered in this case. The security will be accomplished by the use of AODV and DSR techniques. [5] Ad-hoc networks have lots of challenges than traditional networks. It has challenges like infrastructure less and self organizing networks. They don’t have any fixed infrastructure. In Manets there will be no centralized authority to manage the network. Nodes have to rely on other nodes to keep the network connected. As the ad-hoc network is dynamic and every transmission in these networks become vulnerable to many number of attacks and security becomes a major issue. In this survey paper we study the different security attacks to ad-hoc networks and also discussed available solutions. We try to provide a brief introduction to the types of attacks and possible counter measures to prevent the attacks. [6] the concept of routing protocols are considered in this case. The proactive reactive and hybrid routing protocols are considered. [7] In recent years mobile ad hoc networks have become very popular and lots of research is being done on different aspects of MANET. Mobile Ad Hoc Networks (MANET)-a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.). There are different aspects which are taken for research like routing, synchronization, power consumption, bandwidth considerations etc. This paper concentrates on routing techniques which is the most challenging issue due to the dynamic topology of ad hoc networks. There are different strategies proposed for efficient routing which claimed to provide improved performance. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions .This paper provides an overview of different routing protocols proposed in literature and also provides a comparison between them.

3. PROPOSED WORK

The proposed work will involve construction and evaluation of the system in which security is enhanced. The security will be achieved by deeply analyzing the contents of the files along with the extension present within the file. Redundancy elimination mechanism is also used so that file can be compressed and less memory will be consumed. The energy consumption is also minimized when the redundancy is reduced. First of all, Receive the data in the form of packets with different or same sequence numbers (e.g 1,2,3,4,1,2,3 etc) after receiving the packets store them in buffer. Buffer will be divided into slots (b1,b2-------,bn). When one packet is stored within the buffer then its sequence number can be compared against incoming packet sequence number. If the sequence number is same then the incoming packet will not be moved forward and system will go into sleep mode. Otherwise packet will be accepted. After receiving the packets nodes will be analyzed along with the path. If there is interference or node is down then sensor will detect some other path using Bellmen Ford Algorithm. Interference will be detected using Sphere Intersect Algorithm. By the above mechanism overall reliability, power management and efficiency will be increased.

In the existing system only SDT is achieved however in our project we have also done range detection and the sensor node having higher range will be selected for data transmission. There are two Parameters which are associated with it.

1. Selective data transmission
2. Path Management

SDT with Path Management

1. Receive the data in the form of packets with different or same sequence numbers (e.g 1,2,3,4,1,2,3 etc)
2. After Receiving the packets store them in buffer.
3. Buffer will be divided into slots(b1,b2-------,bn)
4. When one packet is stored within the buffer then its sequence number can be compared against incoming packet sequence number.
5. If the sequence number is same then the incoming packet will not be moved forward and system will go into sleep mode.
6. Otherwise packet will be accepted.
7. After receiving the packets nodes will be analyzed along with the path.
8. If there is interference or node is down then sensor will detect some other path using Range based Algorithm.
9. Interference will be detected using Sphere Intersect Algorithm.
10. By following the above mechanism overall reliability, power management and efficiency will be increased.

Concept of SDT with Path management is followed. First of all SDT will be achieved using the following Algorithm

```
SDT (A, B)

returns (Non_Redundant, Redundant)

    1. Input Packet Sequence (p1,p2,----------,pn)
    2. Initialize k=1
    3. Store the packets in Buffer slots (b1,b2,------------bn)
    4. Repeat the steps for i<=n
           a) Repeat the steps for j<=n
   a1)           if (pi=bi) then
```

```
a1.1)       k=2
            End of if
    a2)         j=j+1
            end of  Inner loop
        b)  if(k=1)
        c)    b1)          return Redundant
            else
    b2)         return non_Redundant
            end of if
     c)         i=i+1, k=1
            end of outer loop
```

In the given algorithm first of all we are going to Determine weather there is a collision in the transmission or not. Also interference will be detected with this algorithm.

sphere intersect(A, B)

returns (OVERLAP,DISJOINT)

```
1. l = c2 − c1
2.  Square of (d) = l.l
3. if (square of(d) < (r1 + r2)*(r1+r2))
4.  return (OVERLAP);
5.  Else
6.  return (DISJOINT);
```

If the interference is high then the signals do not intersect with each other and data will not be moved forward. Signals from two distinct sensors will intersect with each other only if distance between there centers c1 and c2 is less then sum of their radii r1 and r2. If the interference is present then either separate path will be followed to transmit the data.

The restricted access protocol will be use the properties of both the algorithms. In the proposed model restricted access protocol is used. The data when encrypted using some methodology like symmetric key algorithms or asymmetric key algorithms then the files which are encoded are not checked for accuracy. Also they are not checked in order to determine whether they contain malicious information or not. In the proposed system before encryption the authenticity of the file being transmitted is checked and then it is transmitted forward. The file when verified is encoded using encryption mechanism.

After performing the encryption data is transmitted toward the destination. At the destination end data will be decoded and received by the destination. By using the above mechanism the reliability will be increased. The proposed system hence will increase the performance of the existing system.

4. RESULT AND PERFORMANCE ANALYSIS

Following explanation shows to form an ad-hoc network of the wireless sensor nodes so that less power is needed for one node to transmit data to other node. Design and implement an algorithm that can intelligently take decisions by the data collected from the sensor network. To make sensors consume less power by designing integrated chip having all the required components on one single chip.

To re-design the logics required to perform smart switching of the nodes according to the information from the sensor part of it. To design a Scheme, that has in-built capability of implementing all the above mentioned objectives.

The key idea behind this is SDT with path management. When selective data is transmitted from source to destination then power is saved and efficiency is in increased. Duplicate packets are not transmitted. In our Project we have considered a storage capacity with each sensor nodes. When data is stored in the buffer of Nodes then that data will not be deleted until it is transmitted successfully to the destination. Which means the sender does not have to be invoked again if the packet is lost. The data can only be transmitted if there exist a path. In order to determine the path we have checked the centers and radius of the signal which is generated by the sensor node.

Sensors will have diameter if sensor network intersect with each other then we will check its range. Data will be transmitted along the path having higher range. By this we ensure that chances of data being lost is very less. Path Detection is dynamic in nature so path will be selected which have higher success rate. The Sleep Time in our project is (Total Number of Packet-Filtered Packet) and duty cycle is (Time Period per Signals*100/Total Unit). The overall power consumption is going to be reduced. The duty cycle will give the utilization of the CPU. Sleep time will give the time during which CPU sit idle. The intersection of the signals will be determined through the formula. There are chances that Sleep time could be high or memory requirement could be high.

First we will open the netbeans. Then we select the start button after that we will right click on the start button and then click on the run file. After that packet adaptive dissemination dialogue box will appear which is shown below:-

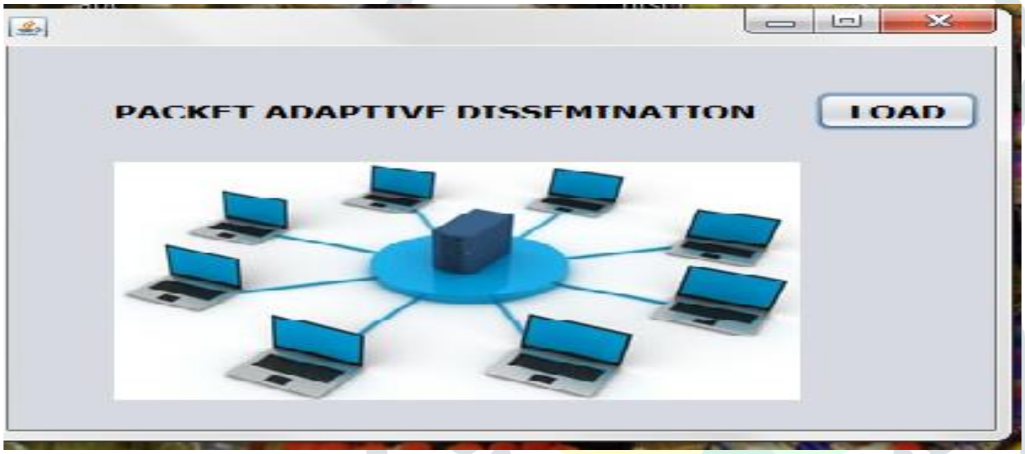
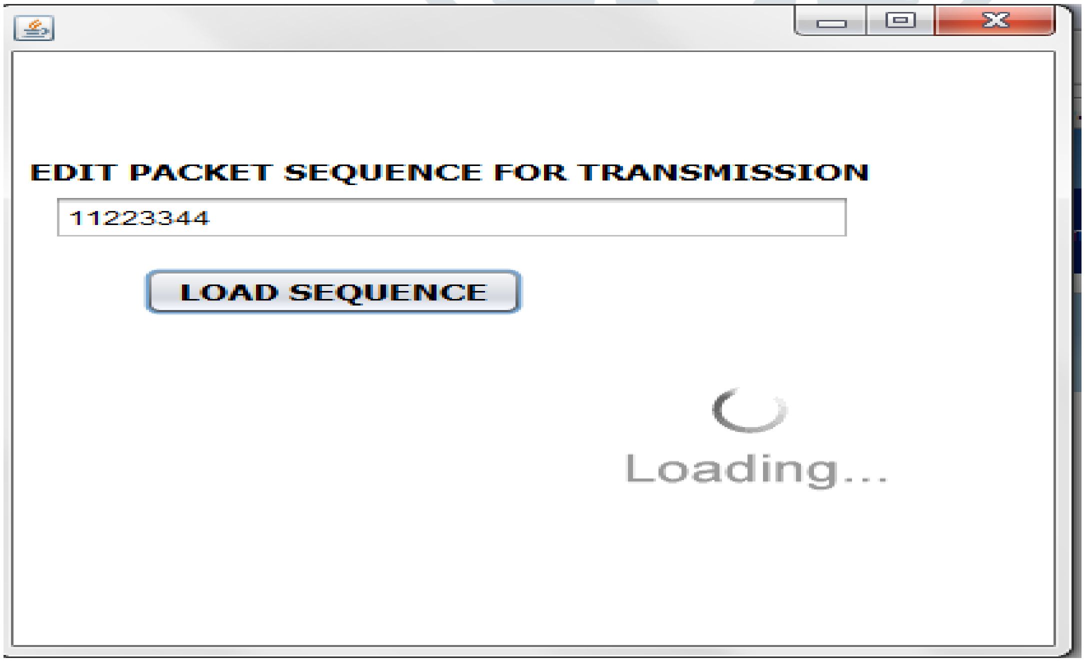


Figure 7. Shows Packet adaptive Dissemination.

Then we will click on load button a dialogue box will appear and we will give the input for the packet transmission.


EDIT PACKET SEQUENCE FOR TRANSMISSION

11223344

Figure 8. Shows Packet for transmission

After that we will click on the load sequence button. Then select system dialogue box will appear in which we can choose either old system or new system but here we choose old system.

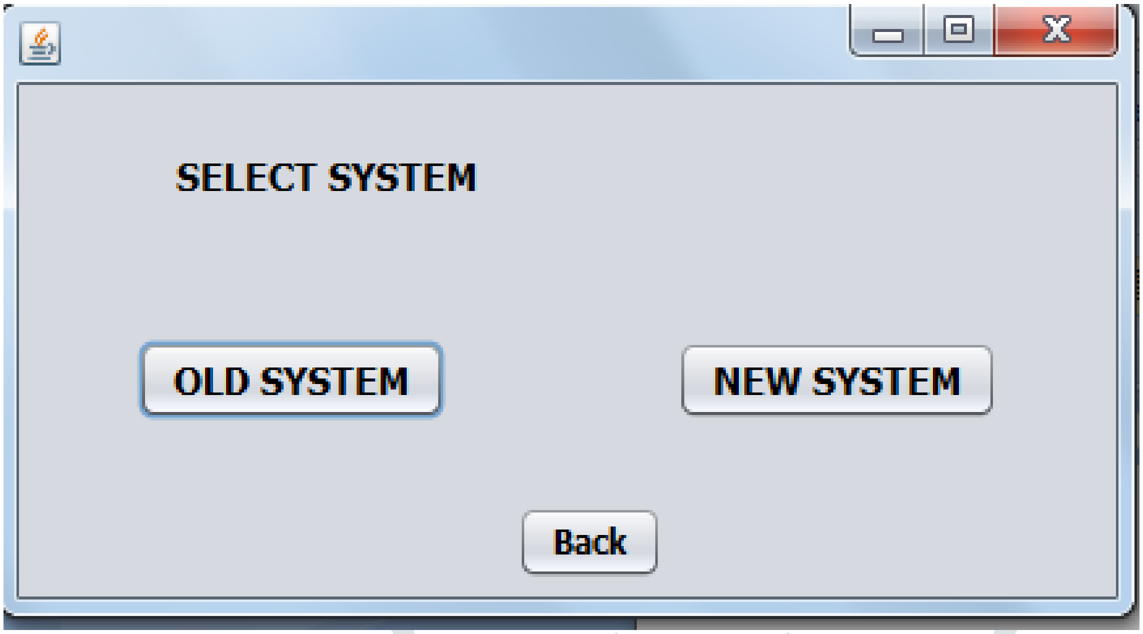


Figure 9. Shows Selection of System

After that we click on the transmit button packet will transfer from source to destination.

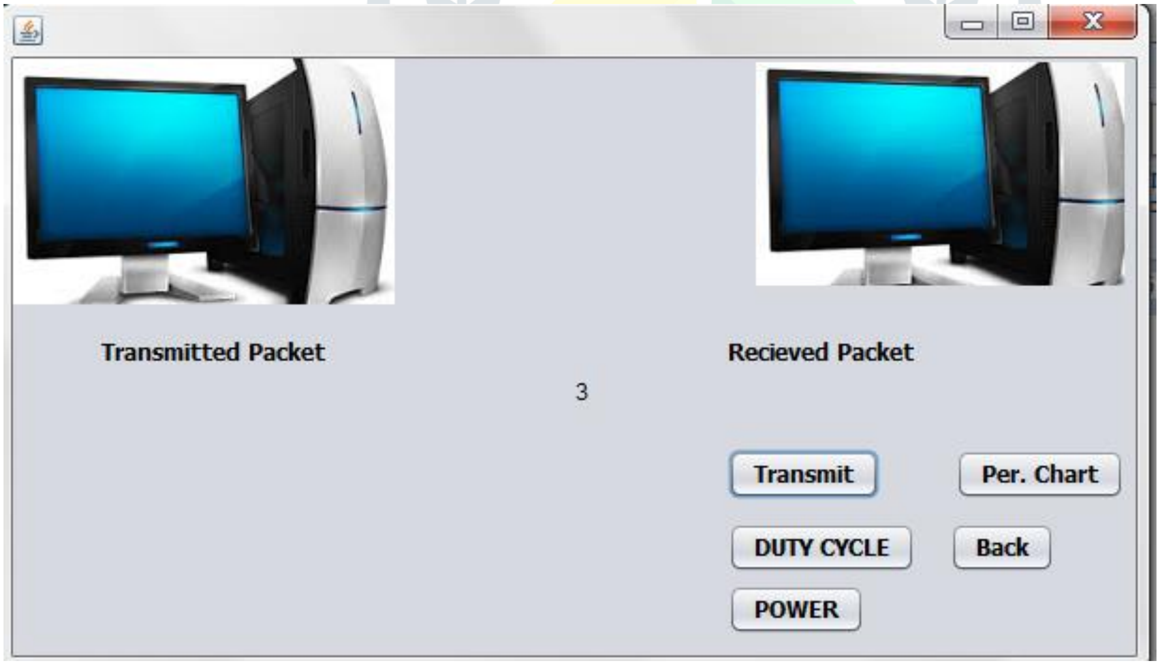


Figure 10. Shows Transmission of packet

Then we click on the duty cycle button to check the duty cycle of the old system.

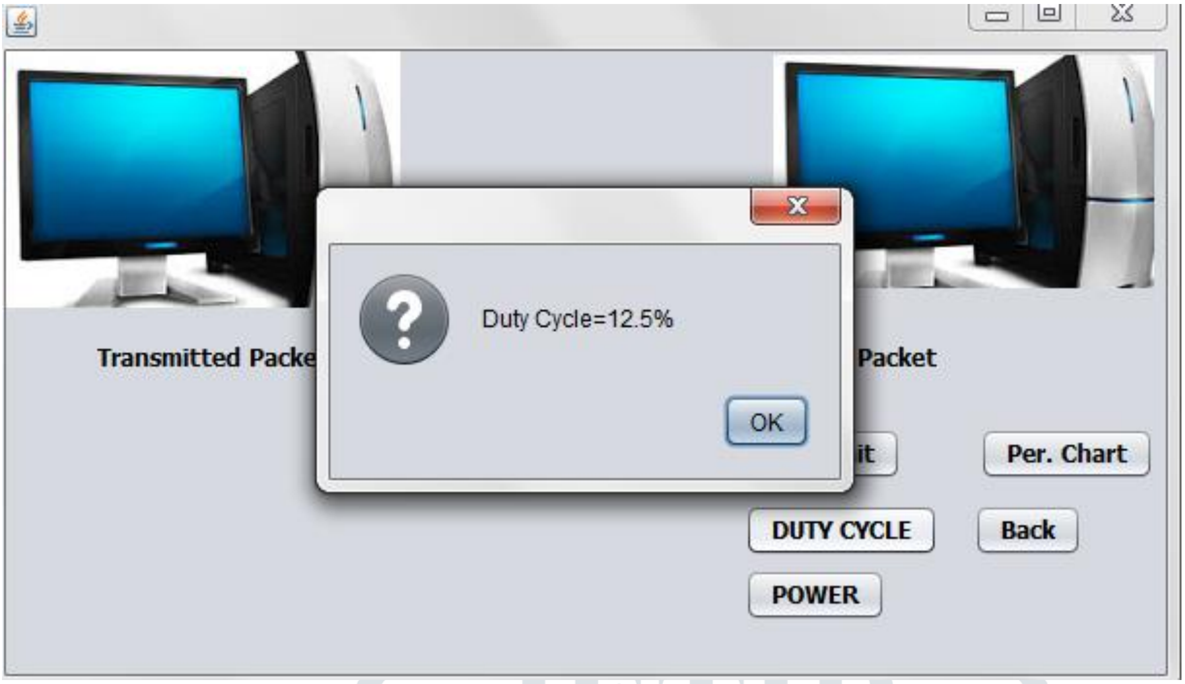

Duty Cycle=12.5%

Figure 11. Shows Duty Cycle of packet

Then we click on the Power button to check the power required for the old system.

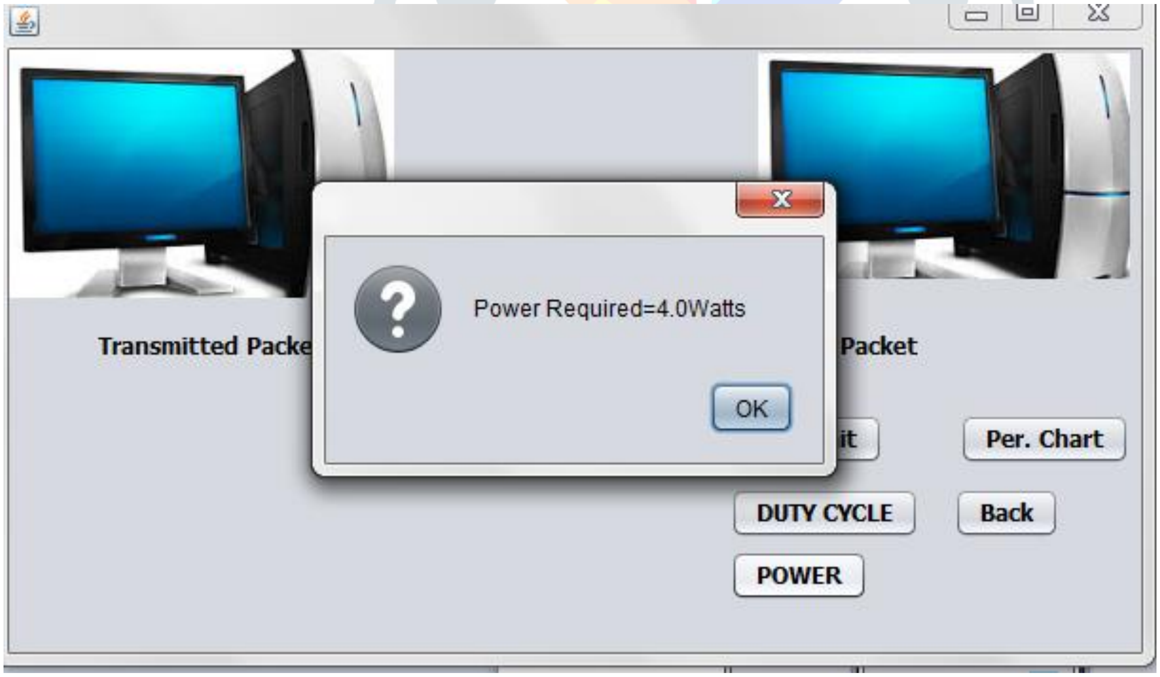

Power Required=4.0Watts

Figure 12. Shows Power use for packet transmission

After that we click on the back button the select system dialogue box will appear.

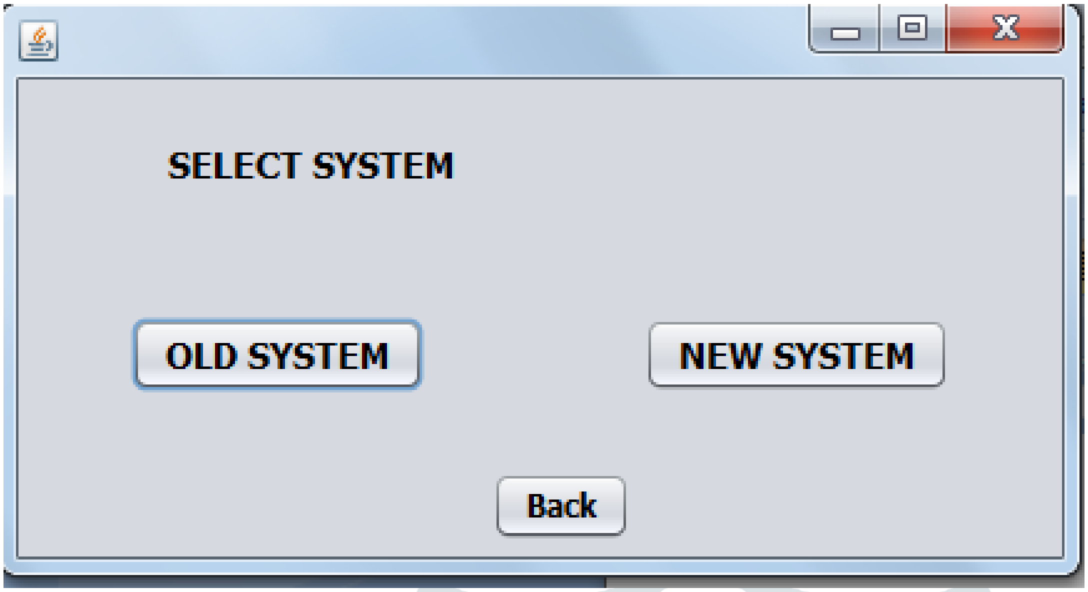


Figure 13. Shows Selection of System

After that we select the new system then new system will show which is shown as below:

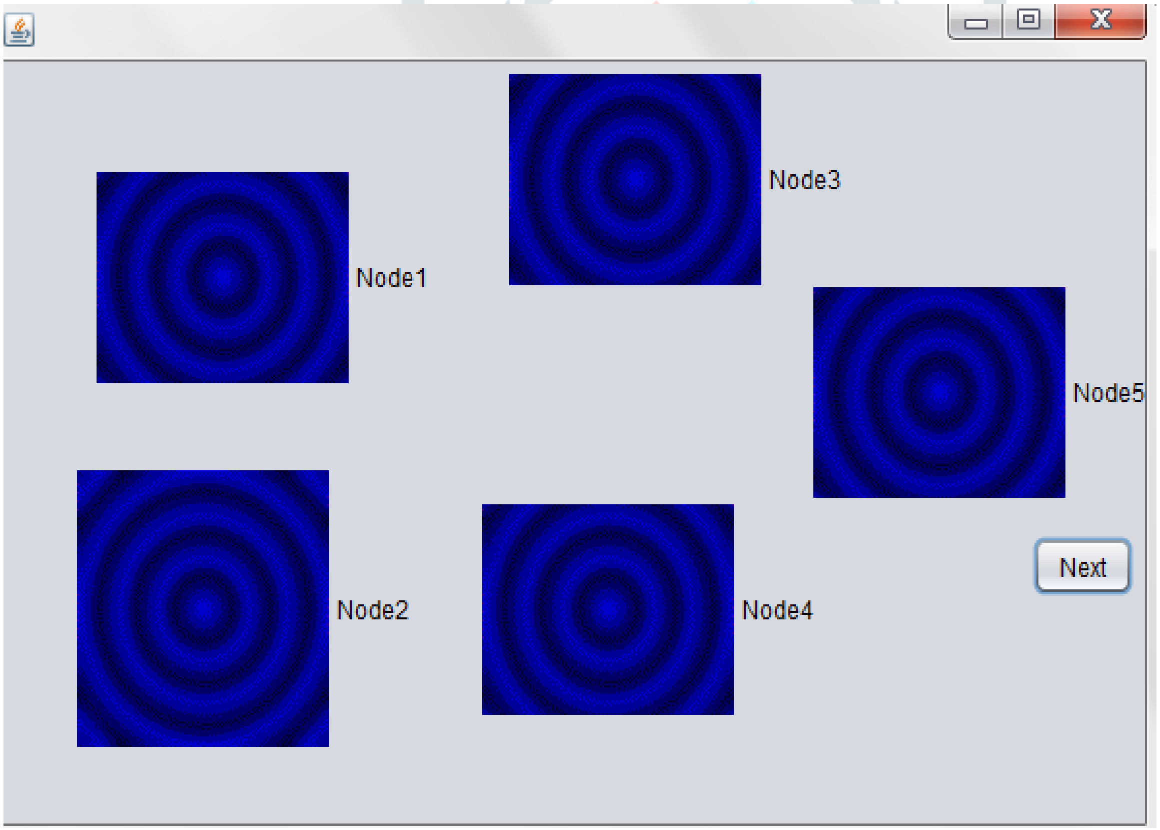
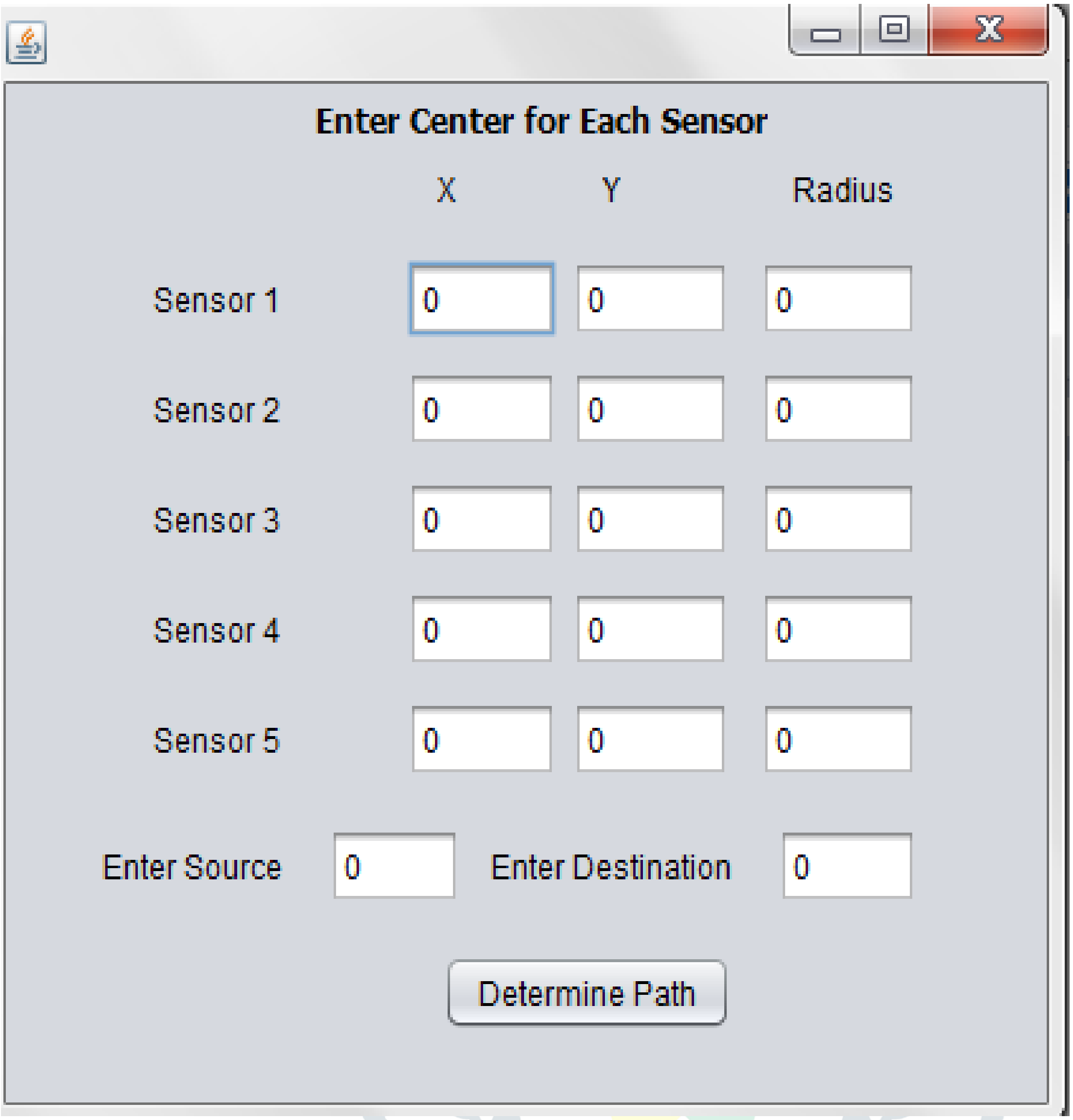


Figure 14. Shows Sensor Nodes

Then click on next button. Then next dialogue box will appear in which we will give the inputs to the sensor nodes.



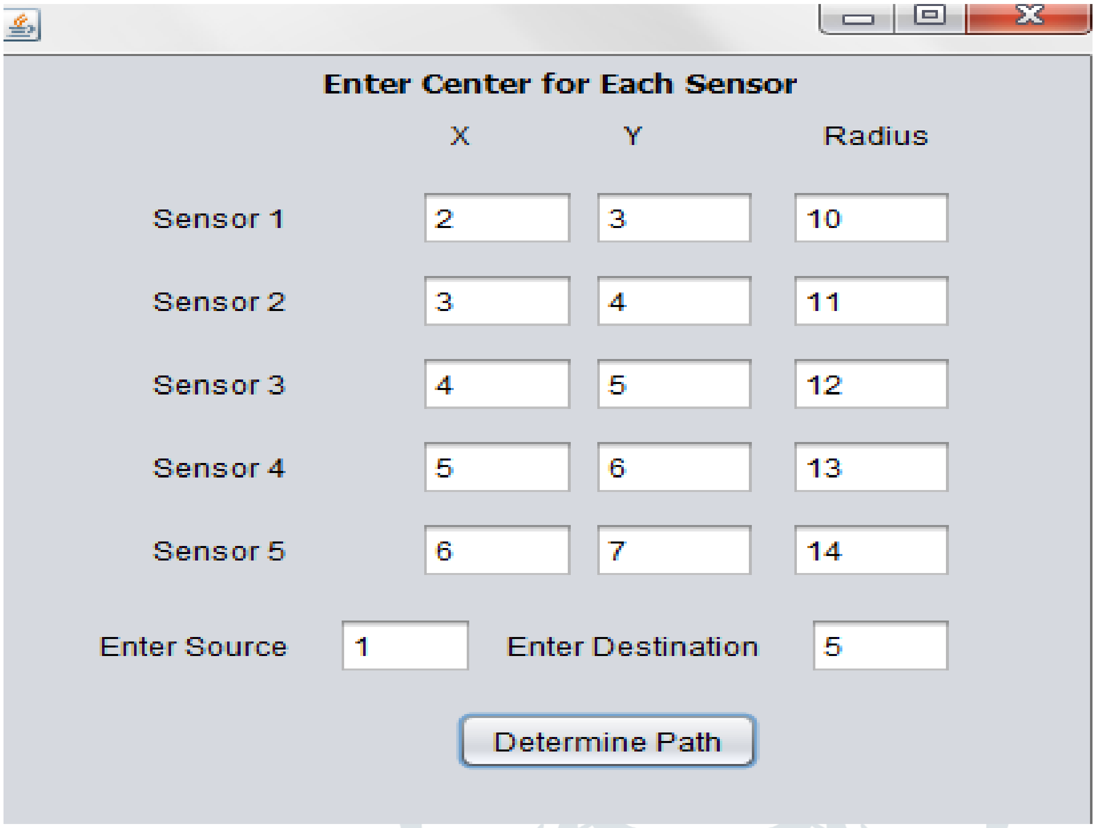
Enter Center for Each Sensor

	X	Y	Radius
Sensor 1	0	0	0
Sensor 2	0	0	0
Sensor 3	0	0	0
Sensor 4	0	0	0
Sensor 5	0	0	0

Enter Source 0 Enter Destination 0

Figure 15. Shows path Determine Dialogue Box

In above Dialogue box if we cannot give any input then it shows the message “no path” which means there is no path to transmit packet. We can give the input and give source and destination and click on determine path to determine the path for transmission



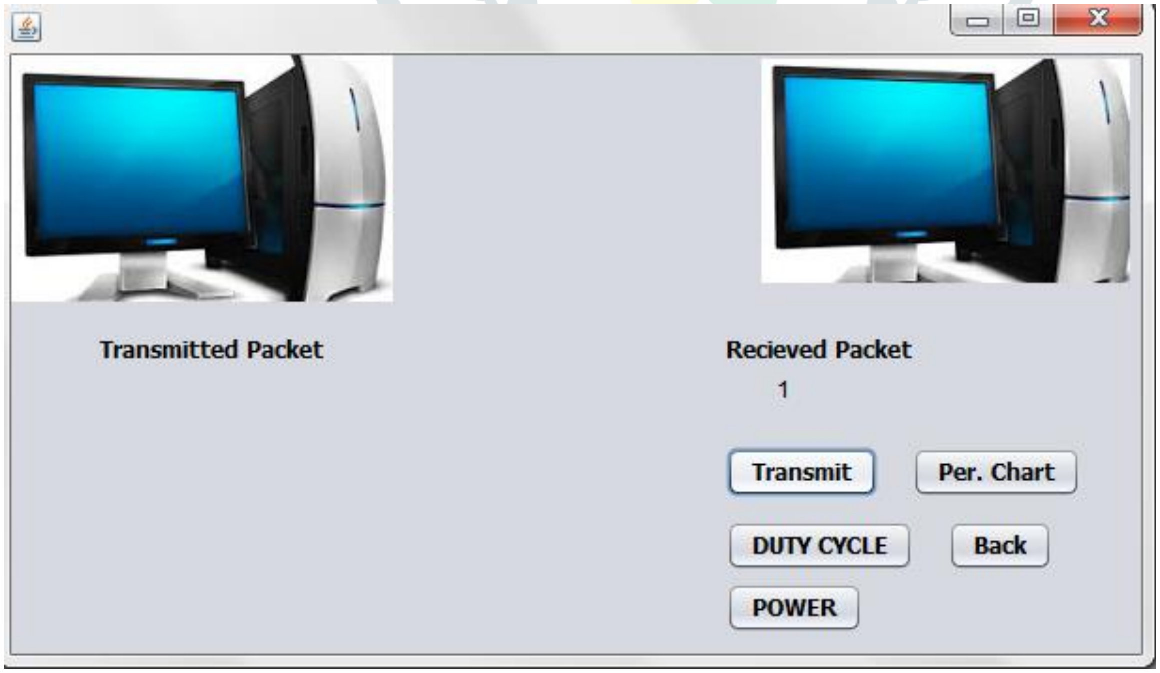
Enter Center for Each Sensor

	X	Y	Radius
Sensor 1	2	3	10
Sensor 2	3	4	11
Sensor 3	4	5	12
Sensor 4	5	6	13
Sensor 5	6	7	14

Enter Source 1 Enter Destination 5

Figure 16. Shows Source and Destination for Packet Transmission

Then we will click on the determine path button for the nearest path selection

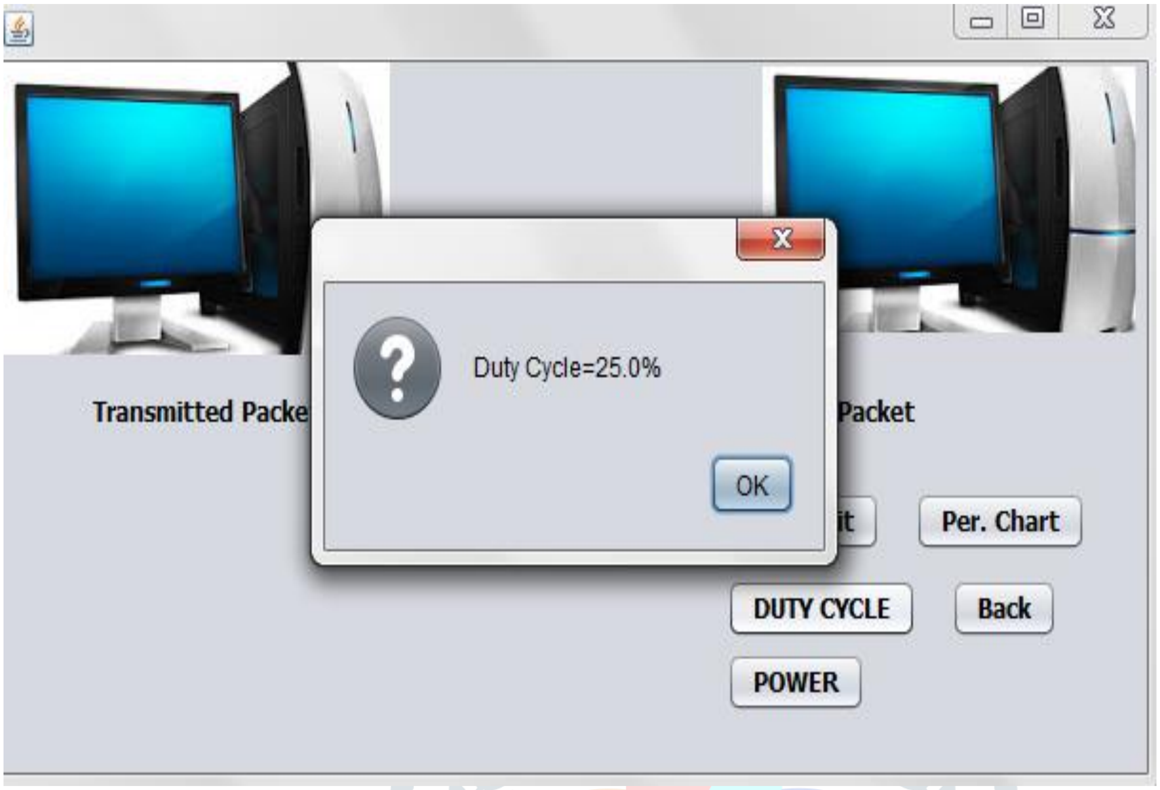


Transmitted Packet

Recieved Packet
1

Figure 17. Shows Packet Transmission in New System

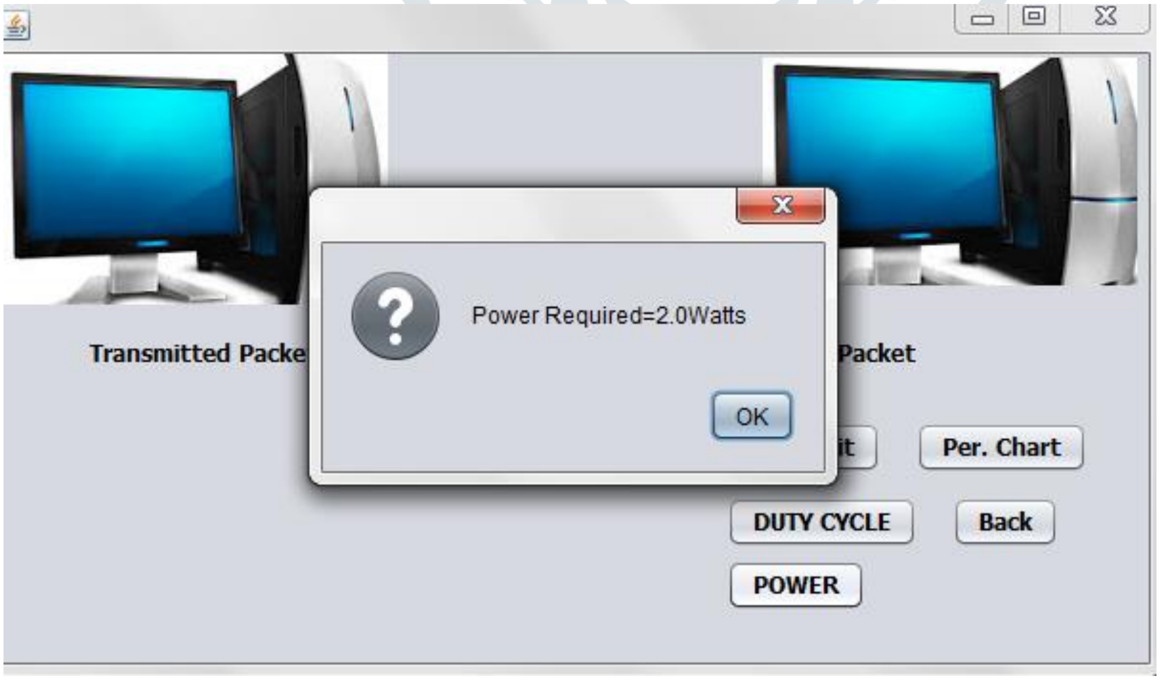
After that transmission process will be start. Then again click on duty cycle button to check the duty cycle result will show.



Duty Cycle=25.0%

Figure 18. Shows Duty Cycle in New System

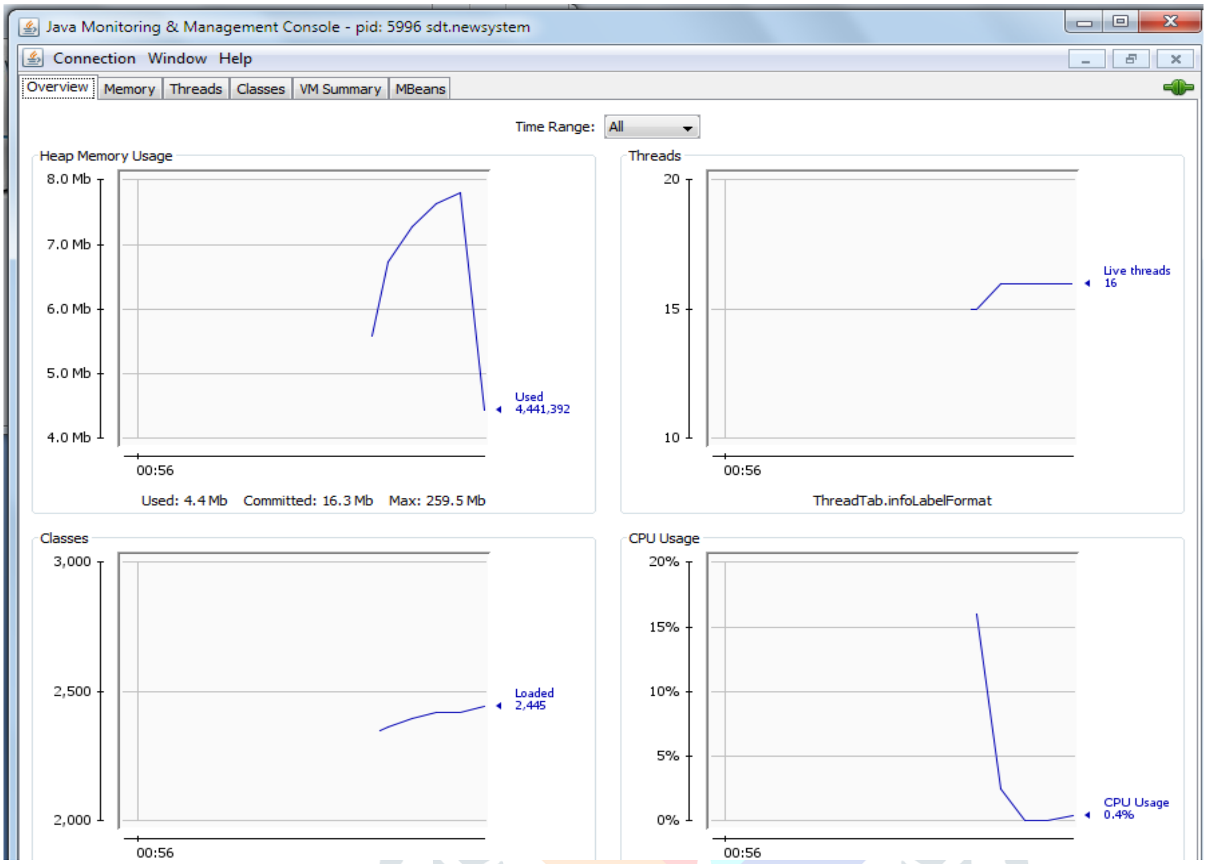
Then again click on Power button to check the Power result will show.



Power Required=2.0Watts

Figure 19. Shows Power used in New System.

Then click on the performance chart button by which we can compare the performance of old system and new system.



Time Range: All

Used: 4.4 Mb Committed: 16.3 Mb Max: 259.5 Mb

ThreadTab.infoLabelFormat

Figure 20. Shows Performance Graphs.

This said there remains much to be done to reduce the power consumption thereby increasing the efficiency of the network. Any network needs a long lasting power source for operation. The still remains a great deal to de improved in this area. Power sources can be re-designed to last longer. Smart wireless sensors can be implemented that can take switching decisions themselves. This would reduce the transfer cost of data from centralized network to nodes thus reducing power consumption. The protocol can be enhanced to increase power efficiency.

In our algorithm we will use the concept of signal strength. If strength of the signal is high then that path will be selected because of this there is less chances of data loss. The data when deliver to the destination acknowledgment will be generated. Since there is less number of passes hence, less time will be consumed for data transmission coordinates of two sensors (x_1, y_1) and (x_2, y_2) and radius $r_{1,}$ $r_{2.}$

$D_1=\sqrt{}\ (y_2, y_1)^2 +(x_2, x_2)^2$

$R=\sqrt{r_1}+\sqrt{r_2}$

If ($R>D_1$) then

Sensor has a range and data will be transmitted.

5. CONCLUSION AND FUTURE WORK

The proposed work ensures that the security of the existing system should be enhanced. The security will be enhanced by the use of the concept of redundancy elimination and encryption. The energy consumption will be significantly reduced. The future work will involve reducing the complexity of the proposed algorithm and to ensure the security in terms of the random key rather than plan key.

6. REFERENCES

[1]–[23]

[1] H. Zhao, “Security in Ad Hoc Networks,” *Security*, pp. 756–775, 2003.

[2] A. K. Gupta, H. Sadawarti, and A. K. Verma, “Review of Various Routing Protocols for MANETs,” *Int. J. Inf. Electron. Eng.*, vol. 1, no. 3, pp. 251–259, 2011.

[3] P. Rai and S. Singh, “A Review of ‘ MANET ’ s Security Aspects and Challenges ’,” *IJCA Spec. Issue “Mobile Ad-Hoc Network”, MANETs*, pp. 162–166, 2010.

[4] N. Garg, “MANET Security Issues,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 8, pp. 241–246, 2009.

[5] J. G. Ponsam and R. Srinivasan, “A Survey on MANET Security Challenges,, Attacks and its Countermeasures,” *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 1, pp. 274–279, 2014.

[6] H. Kaur, V. Sahni, and M. Bala, “A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review,” *Network*, vol. 4, no. 3, pp. 498–500, 2013.

[7] D. S. S. D. A. P. Dr.S.S.Dhenakaran, “An Overview of Routing Protocols in Mobile Ad-Hoc Network,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 2, pp. 251 – 259, 2013.

[8] M. A. Ali, “Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions,” no. March, 2011.

[9] D. Djenouri and L. Khelladi, “A survey of security issues in mobile ad hoc networks,” *IEEE Commun. Surv.*, vol. 11, no. 02, pp. 129–137, 2005.

[10] A. Dorri and S. R. Kamel, “Security Challenges in Mobile Ad Hoc Networks: A Survey,” *Int. J. Comput. Sci. Eng. Surv.*, vol. 6, no. 1, pp. 15–29, 2015.

[11] M. Fasanghari and G. A. Montazer, “Design and implementation of fuzzy expert system for Tehran Stock Exchange portfolio recommendation,” *Expert Syst. Appl.*, vol. 37, no. 9, pp. 6138–6147, 2010.

[12] Gagandeep, Aashima, and P. Kumar, “Analysis of different security attacks in MANETs on protocol stack a-review,” *Int. J. Eng. Adv. Technol.*, vol. 1, no. 5, pp. 269–275, 2012.

[13] W. Li and A. Joshi, “Security Issues in Mobile Ad Hoc Networks-A Survey,” *Dep. Comput. Sci. Electr. …*, pp. 1–23, 2008.

[14] T. Mamatha, “Network Security for MANETS,” no. 2, pp. 65–68, 2012.

[15] H. Paul and P. Das, “Performance Evaluation of MANET Routing Protocols,” *Int. J. Comput. Sci. Issues*, vol.

9, no. 4, pp. 449–456, 2012.

[16] A. Shrivastava and A. Shanmogavel, “Overview of Routing Protocols in MANET’s and Enhancements in Reactive Protocols,” ... *Comput. Sci.* ..., 2005.

[17] V. Ulnerabilities and T. Chou, “S Ecurity T Hreats on C Loud C Omputing,” vol. 5, no. 3, pp. 79–88, 2013.

[18] P. Veeraraghavan and V. Limaye, “Security Threats in Mobile Ad Hoc Networks,” *2007 IEEE Int. Conf. Telecommun. Malaysia Int. Conf. Commun.*, vol. 1, pp. 1–22, 2007.