International Journal of Allied Practice, Research and Review

Website: www.ijaprr.com (ISSN 2350-1294)

Hybrid Approach of KNN and Euclidean Distance to Tackle Sybil Attack in the Network

Yasmeen and Nikita Bakshi
M-tech Scholar and Assistant Professor
Department of Computer Science and Engineering,
Universal Institute of Engineering and Technology, Lalru, Patiala, Punjab, India

Abstract - The wireless sensor network uses batteries which decay as data is being transmitted from source and destination. This decay in batteries requires to be minimised. Reasons for decay in batteries could be congestion and attacks. The attacks which are common in WSN is Sybil attack which is multiple identity attack. In such a situation, attacker node copies the identities of other nodes and data which is transmitted delivered to the wrong node causing threat to secure data. In order to solve the problem KNN mechanism is used in the proposed system. KNN is used in order to form clusters of the minimum distance nodes. These clusters then can be examined for similarity in terms of identities. In case similarity in terms of identities is found then Sybil attack is detected. The result is presented in terms of classification accuracy and mean square error. Classification accuracy is obtained by subtracting the actual value from the approximate value. The error rate is obtained by subtracting the classification accuracy from 100. The proposed approach uses Euclidean distance to determine the neighbouring nodes. The simulation of the proposed system is conducted in MATLAB 2017. The mechanism employed detects the Sybil attack with more precision. The result is improved by the margin of 10% proving worth of the study.

Keywords: - Wireless Sensor Network, Matlab, KNN and Euclidean algorithm

I. INTRODUCTION

The Sybil attack in computer security is an attack where in a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder.

A Sybil attack is a Multiple Identity Attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of Multiple Identity Attack attacks against a single target or multiple targets. With the rapid development of network technology in recent years, the attack traffic scale caused by Multiple Identity Attack attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as network bandwidth, the attack influence sphere has also become broader.

WSN (wireless sensor network) provides a wide range of computing resources from servers and storage to enterprise applications. WSN is a hosting environment that is immediate, flexible, scalable, secure and available. The computing resources from cloud can be easily and quickly accessed and released after use with very less management effort. The concept of WSN can be used in mobile applications running on SMDs (surface mounted device) to boost up their performance. With the integration and support of WSN into the complex mobile applications, the term Mobile WSN (MCC) arises.

The Sybil attack in computer security is an attack where in a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder.

A Sybil attack is a Multiple Identity Attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of Multiple Identity Attack attacks against a single target or multiple targets. With the rapid development of network technology in recent years, the attack traffic scale caused by Multiple Identity Attack attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as network bandwidth, the attack influence sphere has also become broader.

WSN (wireless sensor network) provides a wide range of computing resources from servers and storage to enterprise applications. WSN is a hosting environment that is immediate, flexible, scalable, secure and available. The computing resources from cloud can be easily and quickly accessed and released after use with very less management effort. The concept of WSN can be used in mobile applications running on SMDs (surface mounted device) to boost up their performance. With the integration and support of WSN into the complex mobile applications, the term Mobile WSN (MCC) arises.

The Sybil attack in computer security is an attack where in a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder.

A Sybil attack is a Multiple Identity Attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of Multiple Identity Attack attacks against a single target or multiple targets. With the rapid development of network technology in recent years, the attack traffic scale caused by Multiple Identity Attack attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as network bandwidth, the attack influence sphere has also become broader.

WSN (wireless sensor network) provides a wide range of computing resources from servers and storage to enterprise applications. WSN is a hosting environment that is immediate, flexible, scalable, secure and available. The computing resources from cloud can be easily and quickly accessed and released after use with very less management effort. The concept of WSN can be used in mobile applications running on SMDs (surface mounted device) to boost up their performance. With the integration and support of WSN into the complex mobile applications, the term Mobile WSN (MCC) arises.

WSN Security

In spite of its popularity, however, WSN has raised a range of significant security and privacy concerns which hinder its adoption in sensitive environments. The transition to WSN model exacerbate security and privacy challenges, mainly due to its dynamic nature and the fact that in this model hardware and software components of a single service span multiple trust domains. In the cloud, data and services are not restricted within a single organization's perimeter. This dynamism of data introduces more risk and complicates the problem of access control.

Therefore, compared with the traditional models, in WSN model ensuring confidentiality and integrity of the end-users' data is far more challenging. Moreover, cloud services are usually multi-tenancy services, meaning that a single infrastructure, platform, or software provides its services to multiple mutually untrusted parties simultaneously. Therefore, confidentiality of these parties' data need to protected against each other. However, in some cases these parties may want to collaborate and share some data with each other in a controlled manner and thus there should be a mechanism that allows them to collaborate. Layered architecture of WSN requires different levels of security considerations. In this work we are mainly concerned with the problem of identity management and access control in application and service level. We introduce a set of multi-party protocols specifically designed for cross-domain integrated cloud services. The main objective of these protocols is to provide more visibility and control to the end-user and close the gap between capabilities of existing solutions and new requirements of cloud based requirements.

Even though, the virtualization and WSN delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of WSN. Some of the security issues in the Cloud are discussed below:

1. **Integrity**: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location.

2. **Availability**: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP‟s) in order for their systems to have redundancy.

3. **Confidentiality**: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren't encrypting their communication.

II. Problem Formulation

During the last few years, there has been a sharp increase in the number of network-based computer attacks. This has lead many researchers to study this field in great depth in order to develop novel methods that are capable of eliminating this threat from today's computer networks. This chapter presents a summary of some of the most recent work on the mitigation techniques of common identity based attacks like Sybil and spoofing. The work that is summarized in this chapter deals primarily with attacks on the transport layer, attacks on the network layer, and a thorough introduction to the concept of the mitigation technique known as client puzzles. It is very difficult to secure data from intruders. Now in our proposed system we detect the malicious nodes as well as correct them.

III. OBJECTIVE OF STUDY

The proposed work deals with the mobility of nodes along with the static nodes to reduce the identity based attacks in the cloud like networks. The objectives are listed as follows

1. Increasing the lifetime of the network.

2. Reduce the energy consumption within the network.

3. Reduce the packet drop ratio.

4. Increase reliability and reduce bandwidth consumption of the network.

IV. METHODOLOGY

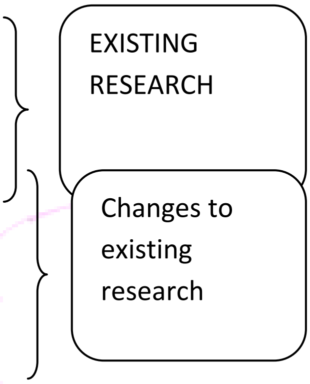
The methodology to achieve the objectives is listed as follows

```
1.    Input the number of nodes in the networks.

2.    Enter the threshold coverage area (Ct) associated with node.

3.    Initialize count=0

4.    Check the neighborhood of nodes in terms of coverage area(Ci)
4.1   if Ct>Ci then
Count=count+1
End of if
5.    if count=1 then
5.1   Apply Euclidean distance to determine location of attacking node
5.2   If Ct>Ci then
5.3   Declare Sybil attack along with its location
End of if
6.    Repeat the above steps for all the nodes
7.    Calculate lifetime, packet drop ratio and energy consumed
8.    Stop
```



EXISTING RESEARCH

Changes to existing research

V. Tools Used

In order to perform the simulation of the existing and proposed system MATLAB is used. The MATLAB is a mathematical tool which is used in order to build the environment in which this simulation can take place. The research methodology which is utilize in this case will involve all the tools which are utilize in the name of gathered the enlightenment around the obstacle. This enlightenment will be utilize in the name of solve the obstacle which is considered.

VI. Results

Sybil attack will be the one in which one node takes the identity of other node. The overall performance goes down by the application of Sybil attack. In order to resolve the problem Euclidean distance mechanism is merged along with KNN approach. KNN used to find the neighbours of the node being analyzed. In, case their exist only one neighbour of current node then Sybil attack is detected the Euclidean distance is used to check the location of the Sybil node. The overall time consumption of simulation is achieved to be better as compare to existing approach. This is shown as under

Table: Showing time consumption of existing and proposed system

PROPOSED KNN+EUCLIDEAN	EXISTING KNN
12.5357	22.4715
36.6243	44.4277
48.6805	64.4345
46.7414	60.4107
73.0829	98.9666
101.205	113.473

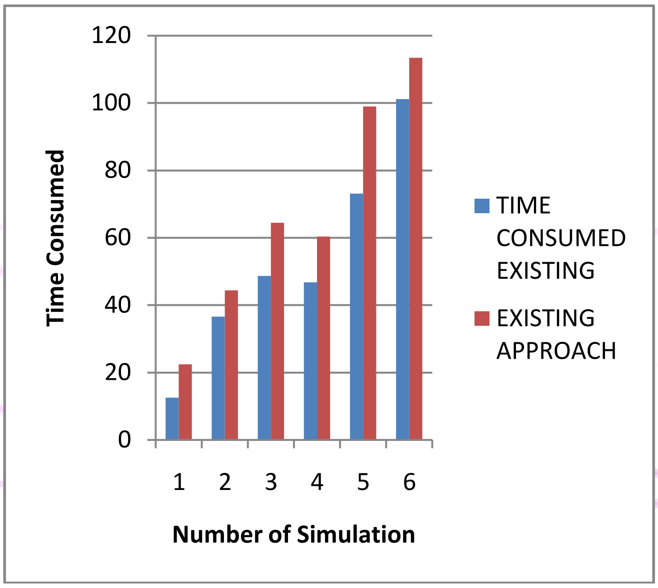


Figure : Showing time consumption of existing and proposed system

The simulation is conducted in matlab and Sybil nodes are recorded the number of nodes are varied from 100 to 200 and result is recorded. The snapshot generated from proposed system is as under

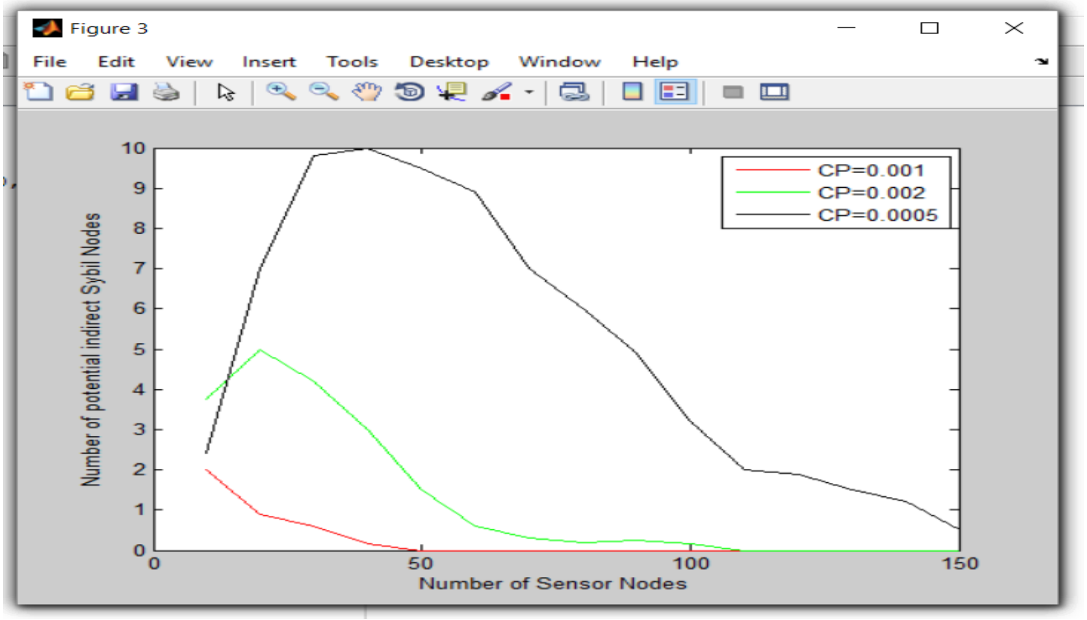


Figure: Number of potential Sybil attack nodes

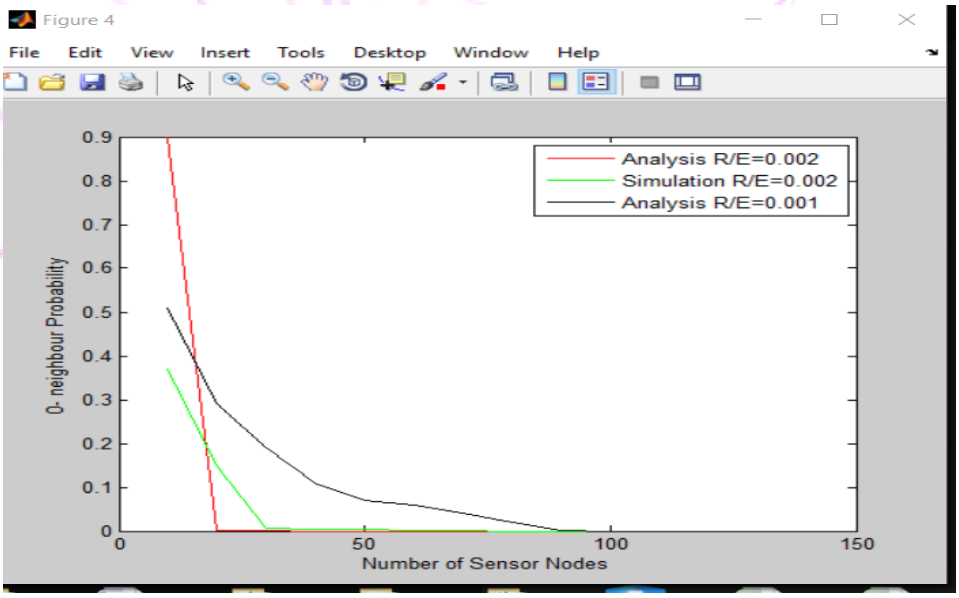


Figure: Nodes having 0 neighbours are indicated through the proposed system.

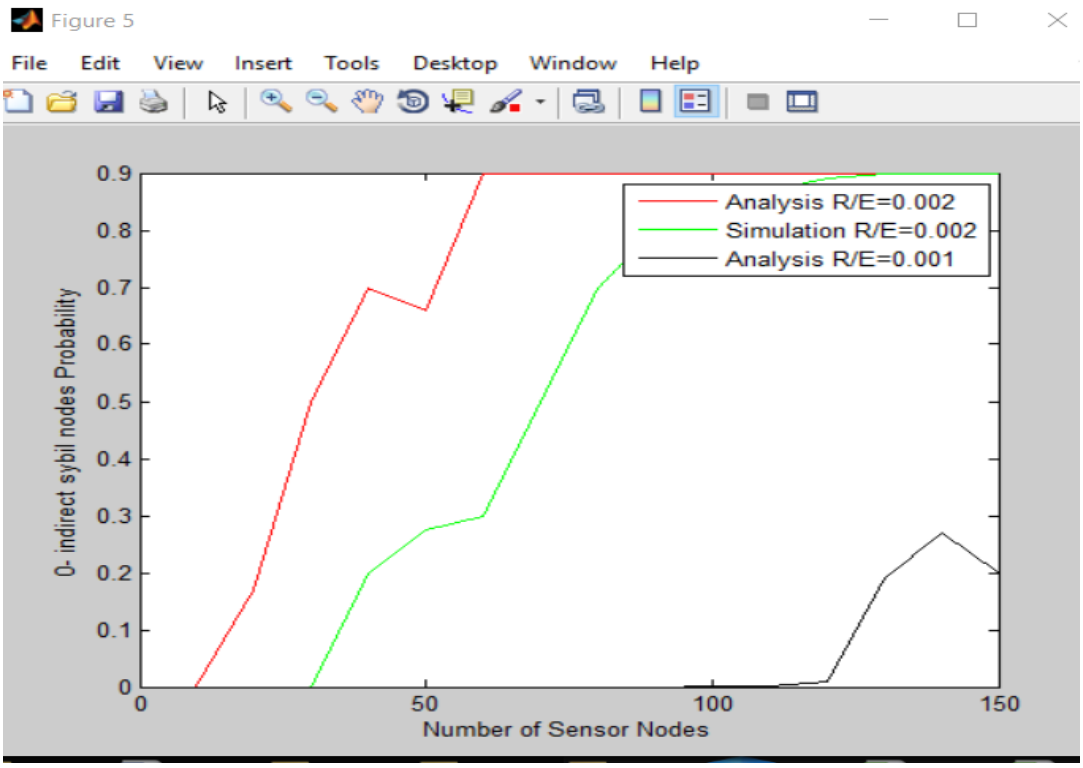


Figure: O probability neighbour node attacks are predicted through this graphs.

As the detection is more accurate hence less chances of attack and indirect attack probability decreases.

The result obtained from matlab simulation is given as under

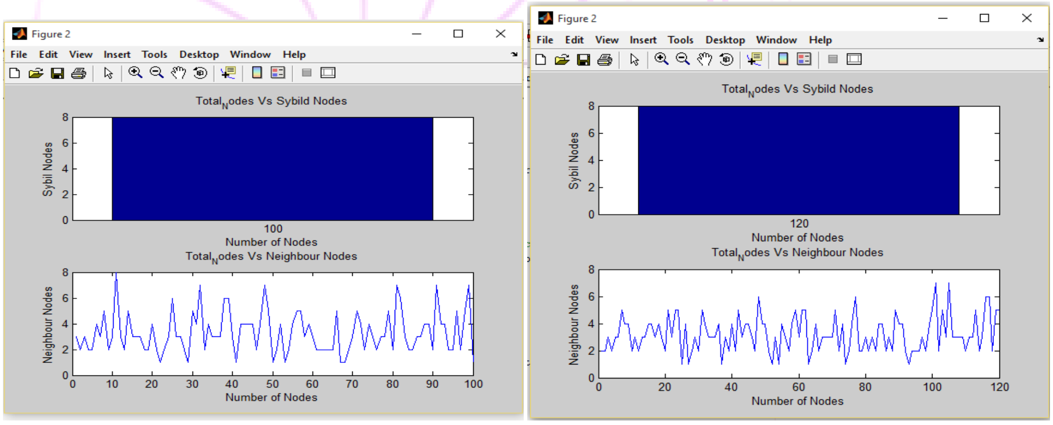


Figure 2
File Edit View Insert Tools Desktop Window Help
Total$_N$odes Vs Sybild Nodes
Sybil Nodes
8
6
4
2
0
100
Number of Nodes
Total$_N$odes Vs Neighbour Nodes
Neighbour Nodes
0
10
20
30
40
50
60
70
80
90
100
Number of Nodes
Figure 2
File Edit View Insert Tools Desktop Window Help
Total$_N$odes Vs Sybild Nodes
Sybil Nodes
120
Number of Nodes
Total$_N$odes Vs Neighbour Nodes
Neighbour Nodes
0
20
40
60
80
100
120
Number of Nodes

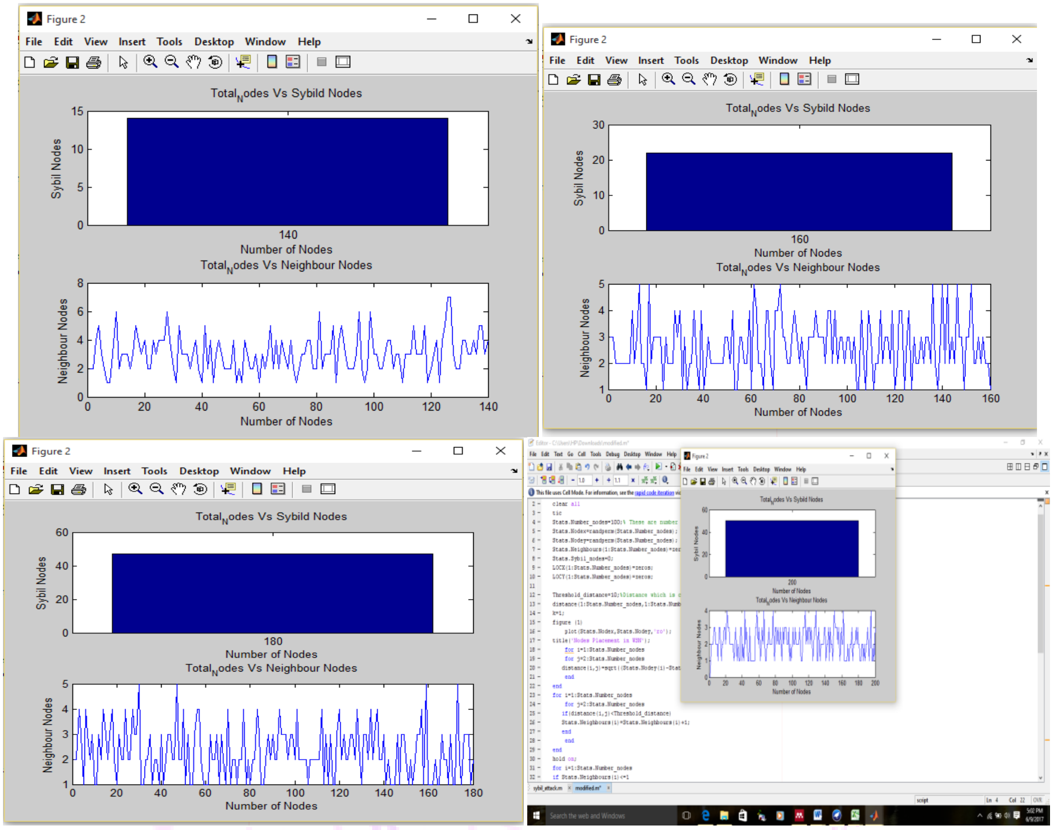


Figure 2
File Edit View Insert Tools Desktop Window Help
Total_Nodes Vs Sybild Nodes
Sybil Nodes
Number of Nodes
140
160
180
200
Total_Nodes Vs Neighbour Nodes
Neighbour Nodes
Number of Nodes
0 20 40 60 80 100 120 140
0 20 40 60 80 100 120 140 160
0 20 40 60 80 100 120 140 160 180
Editor - C:\Users\HP\Downloads\modified.m*
File Edit Text Go Cell Tools Debug Desktop Window Help
sybil_attack.m
modified.m*
Search the web and Windows

This file uses Cell Mode. For information, see the rapid code iteration

```
clear all
tic
Stats.Number_nodes=100;% These are number
Stats.Nodex=randperm(Stats.Number_nodes);
Stats.Nodey=randperm(Stats.Number_nodes);
Stats.Neighbours(1:Stats.Number_nodes)=zer
Stats.Sybil_nodes=0;
LOCX(1:Stats.Number_nodes)=zeros;
LOCY(1:Stats.Number_nodes)=zeros;

Threshold_distance=10;%Distance which is c
distance(1:Stats.Number_nodes,1:Stats.Numb
k=1;
figure (1)
    plot(Stats.Nodex,Stats.Nodey,'ro');
title('Nodes Placement in WSN');
    for i=1:Stats.Number_nodes
    for j=2:Stats.Number_nodes
   distance(i,j)=sqrt((Stats.Nodey(i)-Stat
    end
end
for i=1:Stats.Number_nodes
    for j=2:Stats.Number_nodes
   if(distance(i,j)<Threshold_distance)
   Stats.Neighbours(i)=Stats.Neighbours(i)+1;
   end
    end
end
hold on;
for i=1:Stats.Number_nodes
if Stats.Neighbours(i)<=1
```

Detection results in terms of 100,120,140,160,180 and 200 Nodes

As the number of nodes increases sybil attack is also enhanced. The detection process shows time consumption is greatly reduced in determining location of sybil nodes.

VII. REFERENCES

1. Advisor, D. & Committee, D., 2007. Communication Security in Wireless Sensor.

2. Almuzaini, K.K., 2010. Range-Based Localization in Wireless Networks Using Density-Based Outlier Detection. Wireless Sensor Network, 02(11), pp.807–814.

3. Analysis, A.L.B., Accuracy of Range-Based Cooperative Localization in Wireless Sensor Networks : , pp.1–11.

4. Anwar, R.W. et al., 2014. Security Issues and Attacks in Wireless Sensor Network. World Applied Sciences Journal, 30(10), pp.1224–1227.

5. Avila-Vazquez, D. et al., 2014. Geospatial recommender system for the location of health services. In 2014 9th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, pp. 1–4. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6877023 [Accessed January 13, 2016].

6. Bachrach, J. & Taylor, C., Localization in Sensor Networks.

7. Badshah, G. et al., 2015. Importance of Watermark Lossless Compression in Digital Medical Image Watermarking. , 4(3), pp.75–79.

8. Boudhir, A.A. & Mohamed, B.A., 2010. New Technique of Wireless Sensor Networks Localization based on Energy Consumption. International Journal of Computer Application, 9(12), pp.25–28.

9. C. Wu et al., 2013. WILL: Wireless Indoor Localization without Site Survey. IEEE Transactions on Parallel and Distributed Systems, 24(4), pp.839–848. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6216368 [Accessed January 12, 2016].

10. Chandrasekhar, V.R. & Seah, W.K.G., Range-free Area Localization Scheme for Wireless Sensor Networks.

11. Corke, P. et al., 2010. Environmental wireless sensor networks. Proceedings of the IEEE, 98(11), pp.1903–1917.

12. Demigha, O., LEACH-SC : A Spatial Correlation-Based Protocol for Energy-Efficient Data Collection in Wireless Sensor Networks.

13. Handa, P., Singh Sohi, B. & Kumar, N., 2016. Energy efficient hybrid routing protocol for underwater acoustic sensor network. 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp.2573–2578.

14. He, T. et al., 2003. Range-Free Localization Schemes for Large Scale Sensor Networks 1.

15. Kalita, H.K. & Kar, A., 2009. W s n s a. , 1(1), pp.1–10.

16. Kamath, H.S., 2013. Energy Efficient Routing Protocol for Wireless Sensor Networks. International Journal of Advanced Computer Research, 3(2), pp.95–100.

17. Kaur, A. & Kaur, J., 2012. Comparision of Dct and Dwt of Image Compression Techniques. , 1(4), pp.49–52.

18. Khalid, K. et al., 2016. An Energy-Efficient Routing Protocol for Infrastructure-Less Opportunistic Networks. 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp.237–244.

19. Kumar, A. et al., 2011. Range Free Localization Schemes for Wireless Sensor Networks. International journal of Computer Networks & Communications, 3(6), pp.115–129. Available at: http://www.airccse.org/journal/cnc/1111cnc07.pdf.

20. La, V.H. & Cavalli, A., 2014. S Ecurity Attacks and Solutions in V Ehicular a D Hoc N Etworks : a S Urvey. , 4(2), pp.1–20.

21. Midasala, V., 2016. Performance Analysis of LEACH Protocol for D2D Communication in LTE-Advanced Network. , pp.2–4.

22. Muhammad, S., Hussain, S. & Yousaf, M., 2015. Neighbor Node Trust Based Intrusion Detection System for WSN. Procedia - Procedia Computer Science, 63, pp.183–188. Available at: http://dx.doi.org/10.1016/j.procs.2015.08.331.

23. Pal, S. & Sharma, S.C., 2015. Range Free Localization Techniques in Wireless Sensor Networks : A Review. Procedia - Procedia Computer Science, 57(i), pp.7–16. Available at: http://dx.doi.org/10.1016/j.procs.2015.07.357.

24. Pathan, a. S.K., Lee, H.-W.L.H.-W. & Hong, C.S.H.C.S., 2006. Security in wireless sensor networks: issues and challenges. 2006 8th International Conference Advanced Communication Technology, 2, p.6 pp.–1048. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1625756.

25. Patil, K.J., Chopda, M.Z. & Mahajan, R.T., 2011. Lipase biodiversity. Indian Journal of Science and Technology, 4(8), pp.971–982. Available at: http://www.indjst.org.

26. Purushothaman, D. & Abburu, S., 2012. An Approach for Data Storage Security in Cloud Computing. , 9(1), pp.100–105.

27. Ruj, S. et al., 2011. On Data-Centric Misbehavior Detection in VANETs. 2011 IEEE Vehicular Technology Conference VTC Fall, 35(2), pp.1–5. Available at: http://arxiv.org/abs/1103.2404.

28. Science, C. & Studies, M., 2014. Securing user data on cloud using Fog computing and Decoy technique. , 7782, pp.104–110.

29. Si, W. & Selvakennedy, S., 2008. A Position-Based Deployment and Routing Approach for Directional Wireless Mesh Networks. 2008 Proceedings of 17th International Conference on Computer Communications and Networks, pp.1–8. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4674234.

30. Stoleru, R., He, T. & Stankovic, J.A., 2007. Range-free localization. Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks, pp.3–31.

31. Walters, J. & Liang, Z., 2007. Wireless sensor network security: A survey. Security in distributed, …, pp.1–50. Available at: http://books.google.com/books?hl=en&lr=&id=KhxxsN3vJuYC&oi=fnd&pg=PA367&dq=Wireless+Sensor+Network+Se

curity+:+A+Survey&ots=R4RpHtOLGz&sig=Z_PWgD18TATEHDJK6qLCzP4CsTk.

32. Wang, C. et al., 2009. Ensuring Data Storage Security in Cloud Computing. Iwqos: 2009 Ieee 17th International Workshop on Quality of Service, pp.37–45\n302. Available at: <Go to ISI>://000274551300005.

33. Yang, S.-H., 2014. WSN Security. , pp.187–215. Available at: http://link.springer.com/chapter/10.1007/978-1-4471-5505-8_9.

34. Yu, Y., Prasanna, V. & Krishnamachari, B., 2006. Energy Minimization for Real-Time Data Gathering in Wireless Sensor Networks. IEEE Transactions on Wireless Communications, 5(10), pp.3087–3096.

35. Zheng, J. & Dehghani, A., 2012. Range-Free Localization in Wireless Sensor Networks with Neural Network Ensembles. Journal of Sensor and Actuator Networks, 1(3), pp.254–271. Available at: http://www.mdpi.com/2224-2708/1/3/254/.

36. Zhong, Z., 2009. Achieving Range-free Localization Beyond Connectivity. Sensys, pp.281–294.

37. Zhou, Z. et al., 2016. E-CARP: An Energy Efficient Routing Protocol for UWSNs in the Internet of Underwater Things. IEEE Sensors Journal, 16(11), pp.4072–4082.