Indo-Iranian Journal of Scientific Research (IIJSR)
Peer-Reviewed Quarterly International Journal, Volume 2, Issue 2, Pages 67-75, April-June 2018

Estimation of Harvested Energy from the Traffic Patterns Associated with Nodes

T.Augusty Chandija Lincy[1] and Mrs D.Regi Timna[2]

[1]PG Scholar, Department of Electronics and Communication Engineering, Francis Xavier Engineering College, Tirunelveli, India.
[2]Assistant Professor, Department of Electronics and Communication Engineering, Francis Xavier Engineering College, Tirunelveli, India.
Email: lincythavasiraj@gmail.com[1] and regitimna@gmail.com[2]

Article Received: 30 December 2017 *Article Accepted: 29 March 2018* *Article Published: 31 May 2018*

ABSTRACT

Collaborative spectrum sensing (CSS) was visualize to improve the reliability of spectrum sensing in centralized cognitive radio networks (CRNs). A popular attack in Collaborative Spectrum Sensing is the called spectrum sensing data falsification (SSDF) attack. There will be a punishment strategy which is present to see the reputation method, in which the honour factor and the retribution factor are introduced to give SUs to given in positive and honest sensing activities. There will be a punishment strategy which is present to see the reputation method, in which the honour factor and the retribution factor are introduced to give SUs to given in positive and honest sensing activities. Harvesting energy from ubiquitous radio frequency (RF) signals in urban area is environmentally friendly and self-sustaining. Here Proposed a threshold-based framework for optimal spectral access strategy and show that the threshold is optimal and traffic-dependent. The proposed threshold-based strategy takes into account both the spectral access and energy harvesting opportunities provided by a particular traffic application. Also an iterative algorithm is used that selects a threshold which maximizes the SU transmission opportunity subject to the overall harvested energy budget. Further, we illustrate the effects of different Harvesting energy for the Primary users and the illerate algorithm is used here.

Keywords: Collaborative spectrum sensing, spectrum sensing data falsification, Fusion centre, Malicious Users, Secondary Users, Radio frequency.

1. INTRODUCTION

Cognitive Radio networks can change its parameters by the sensing of the spectrum. It determines the vacant bands, and makes use of these available bands in an opportunistic manner, improving the overall spectrum utilization. With these capabilities, cognitive radio can operate in licensed as well as unlicensed bands. In licensed bands wireless users with a specific license to communicate over the allocated band (PUs) [1], have the priority to access the channel. In the Cognitive Radio Network Sensing-based Spectrum sharing is used but there are many types of radio network. In the Spectrum Sensing that there will be a First the Primary users detect the licensed spectrum and the time allocated for the licensed spectrum. There is also a another positive approach that during the spectrum analysis there will be energy harvested during the transformation of spectrum from one node to another.

Section 2, the Identification of problems formulation related to the existing methods. Section 3 presents detailed description of proposed techniques for solving plant related issue. Experiment results and discussions are described in Section 4. Finally, the conclusion and further enhanced are given in Section 5.

PROBLEM DESCRIPTION AND PREVIOUS WORK

In the DSA Networks paper the cooperative spectrum sensing is used in a distributed DSA network under SSDF attack. In the proposed system. The trust models used here is Beta distribution and Dirichlet distribution. Beta distribution which assigns the trust values to the neighbor nodes at in a different time slots. Dirichlet distribution is able to incorporate uncertainty in the trust values. But It is not linearly separable. In the DSS network the only efficient spectrum is used here [2-12]. In this models is to share their licensed spectrum or is to reallocate other spectrum in the allotted bands. In the Adaptive modulation schemes is to enable coexistence, interference mitigation, Frequency, space, time cognizant protocols But It Should embrace more dynamic models of spectrum sharing. A Bayesian inference model based on propose of two reliability models: an optimistic one for a normal system and a conservative one for a mission critical system.

The main advantage is Reliability may be caused by temporal But it has no strict convergence on the decision reliability is achieved. In the spectrum sharing, a spatial separation region is defined around primary users to protect them from secondary user induced interference [13-28]. This protection region called as an exclusion zone or a protection zone . EZs are the primary ex-ante spectrum enforcement method used by regulators to protect the incumbents from SU-induced interference. The concept of Multitiered Incumbent Protection Zones

2. PROBLEM IDENTIFICATION AND SOLUTION

2.1. Introduction

Keeping in mind the end goal to recognize and shield against the confused assault conduct of vindictive clients all the more successfully and quickly [29-33], this paper proposes a novel notoriety based security instrument. In the instrument, each SU is assigned a persistently refreshed thorough notoriety (CR) esteem by the FC as per its announced detecting information.

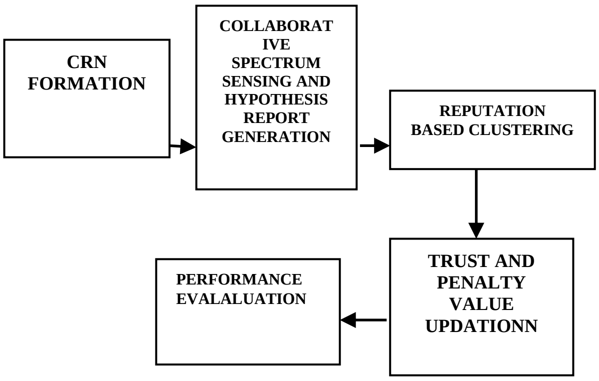

CRN FORMATION
COLLABORATIVE SPECTRUM SENSING AND HYPOTHESIS REPORT GENERATION
REPUTATION BASED CLUSTERING
TRUST AND PENALTY VALUE UPDATIONN
PERFORMANCE EVALALUATION

Fig 1. Block diagram of proposed work

The CR esteem assesses the unwavering quality and accuracy of the individual client's detecting information sent to the FC. Higher notoriety implies that the client's detecting information in the past are more helpful for the FC to settle on the privilege worldwide choices. The CR esteem is an imperative reference in the following detecting round. The far reaching notoriety fundamentally considers four affecting components of client dependability, including current unwavering quality, authentic notoriety, remunerate factor and discipline factor. A malevolent client gets low notoriety and combination weight because of submitting distorted detecting information, and the FC debilitates its unsafe impact during the time spent information combination or straightforwardly disregards its detecting comes about. The far reaching notoriety sufficiently measures and mirrors the unwavering quality of individual detecting comes about for subjective clients in a suitable time scale and is always showed signs of change and refreshed.

2.2. Historical reputation

The notoriety is the subjective likelihood forecast of the subject concerning whether the question can finish a specific cooperative movement accurately and non-devastatingly, and recorded detecting conduct mirrors the dependability variety of intellectual clients. With a specific end goal to feature the recorded conduct of SUs in the part of notoriety assessment, we present the chronicled notoriety.

2.3. Punishment Strategy

Since security has assumed a noteworthy part in CRNs, various research works have chiefly centered around assault identification in view of discovery likelihood, yet few of them took the punishment of assaults into thought and dismissed how to execute successful correctional methodologies against assailants

2.4. Penalty factor

The punishment scheme follows a habit of human society, that is the initial criminal punishment is light, and the cumulative crime will be punished heavily. Therefore, the greater the threat is, the more serious of a punishment should be imposed.

2.5. Harvested energy budget

We accept that SU shrewdly gets to a PU channel. Other than conventional data decoder (ID), each SU is furnished with a RF vitality gatherer (EH) that can separate DC control from the got electromagnetic waves

3. RESULT AND DISCUSSION

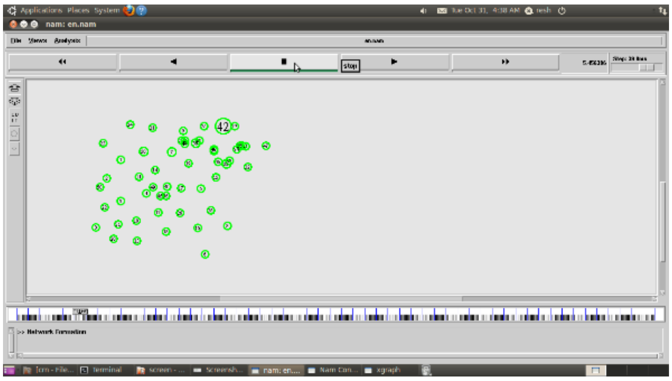
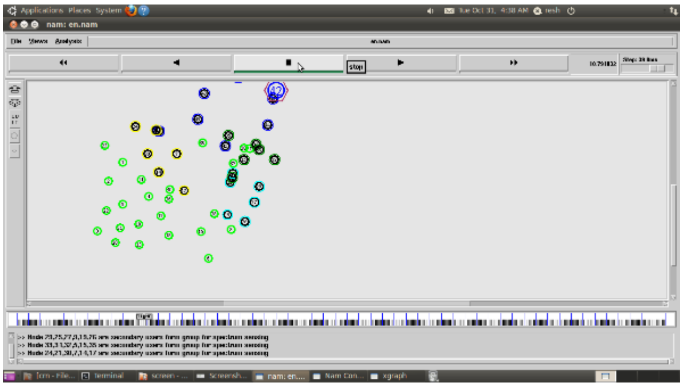


Fig 2: CRN FORMATION

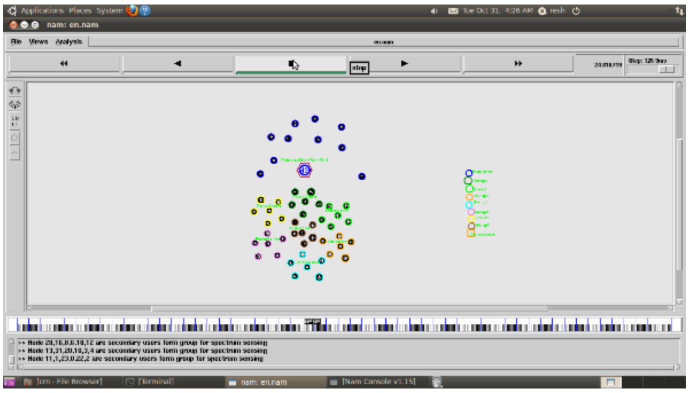
Fig 2 Node Deployment: shows that 71 nodes were created and node deployed at the area of 1700 1700 which has simulation time of 55 seconds. Thus network was created in cognitive radios.



```
>> Node 29,25,27,0,19,26 are secondary users form group for spectrum sensing
>> Node 33,31,37,5,15,35 are secondary users form group for spectrum sensing
>> Node 24,21,30,7,14,17 are secondary users form group for spectrum sensing
```

Fig 3: Separation of primary users and secondary users

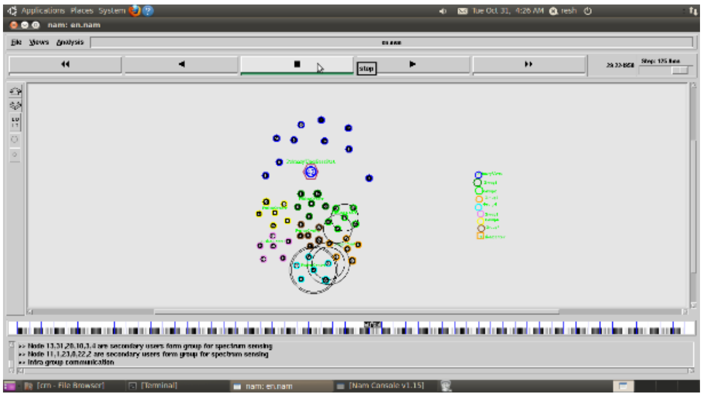
Fig 3 shows that node 42 represents the fusion centre which decides the availability of spectrum in accordance with the free bands in both primary and secondary users. In this dark blue color nodes comprises a single group of primary users. The remaining nodes forms seven individual group of secondary users.



```
>> Node 28,16,8,6,18,12 are secondary users form group for spectrum sensing
>> Node 13,31,20,10,3,4 are secondary users form group for spectrum sensing
>> Node 11,1,23,0,22,2 are secondary users form group for spectrum sensing
```

Fig 4: Initialization of trust value

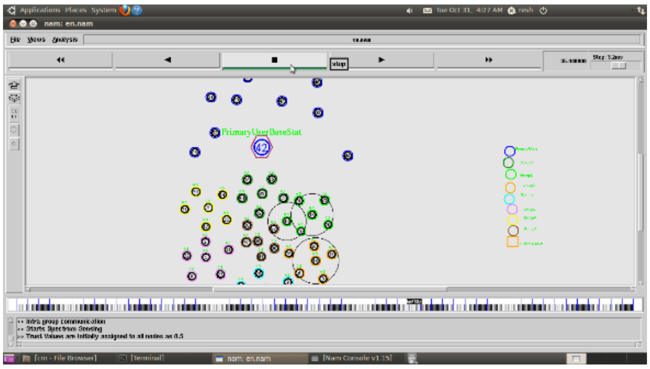
Fig 4. This shows that the trust value is set to be 0.5. The nodes which have this trust value forms a group which belongs to the fusion centre. Rather nodes will be considered as a malicious users.



```
>> Node 13,31,20,10,3,4 are secondary users form group for spectrum sensing
>> Node 11,1,23,0,22,2 are secondary users form group for spectrum sensing
>> Intra group communication
```

Fig 5: Intragroup communication

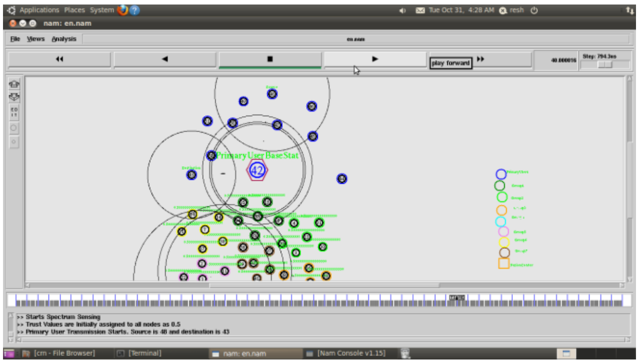
Fig 5 Based on the grouping of nodes there will be a colouring occurs. So that there will be a intragroup Communication Occurs and there will be a fusion centre act as a base station. So that there will be a Communication occurs between the nodes.



```
>> Intra group communication
>> Starts Spectrum Sensing
>> Trust Values are initially assigned to all nodes as 0.5
```

Fig 6: Starts spectrum sensing

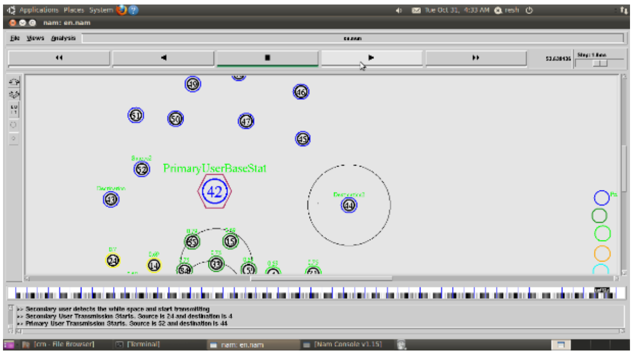
Fig 6 shows that trust values are assigned to all the nodes as 0.5; Intragroup communication has been done between the users and starts spectrum sensing.



```
>> Starts Spectrum Sensing
>> Trust Values are initially assigned to all nodes as 0.5
>> Primary User Transmission Starts. Source is 48 and destination is 43
```

Fig 7 : Assigning source and destination

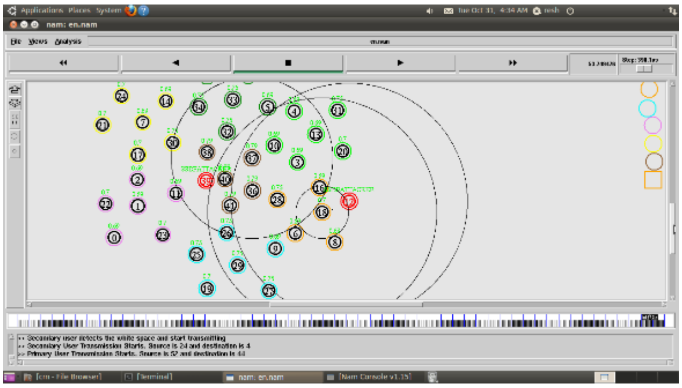
Fig 7 shows that the transmission starts between primary users thereby assigning source node as 48 and destination node as 43 and it is changeable for each and every primary users in order to data transmit. At the same time secondary users sends its spectrum sensing to the fusion centre.



```
>> Secondary user detects the white space and start transmitting
>> Secondary User Transmission Starts. Source is 24 and destination is 4
>> Primary User Transmission Starts. Source is 52 and destination is 44
```

Fig 8: Transmission between primary users

Fig 8 shows that the primary user detects the free space and assign the source and destination for the second time for 52 and 44 nodes.



```
>> Secondary user detects the white space and start transmitting
>> Secondary User Transmission Starts. Source is 24 and destination is 4
>> Primary User Transmission Starts. Source is 52 and destination is 44
```

Fig 9: SSDF attacker

Fig 9 shows that the trust value updation for every node and based on the updation the reward and penalty factor is assigned. Based on the penalty factor the SSDF attacker node is identified

3.1. SIMULATION GRAPHS

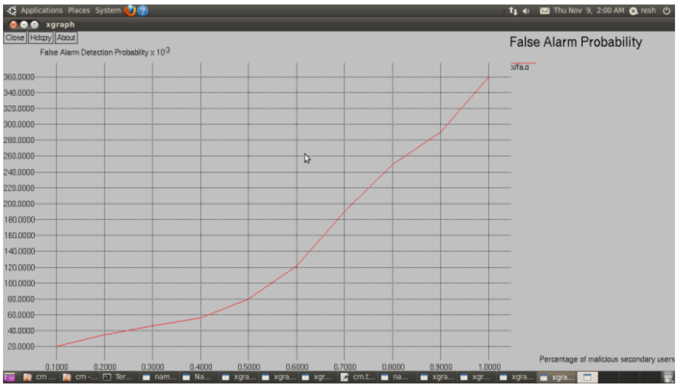


Fig 10: False alarm probability

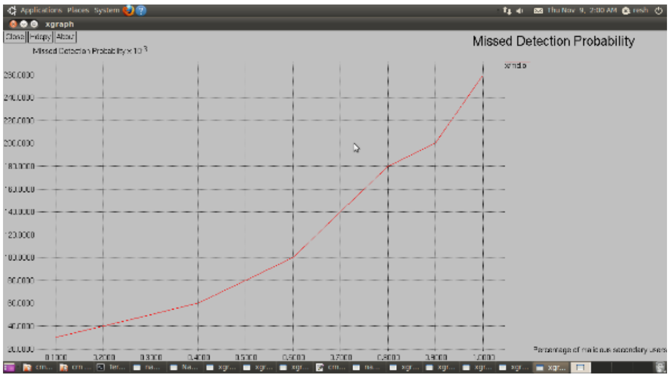


Fig 11: detection performance

Fig 10 shows the false alarm probability. The always opposite attack strategy refers to the attack mode that MUs report after reversing the local decision result. Figures present the cooperative sensing performance under SSDF attack. The horizontal axis accounts for the proportion of malicious users. The vertical axis in Figure represents the global false alarm probability Qf , and the vertical axis in Figure represents the global misdetection probability Qm. It can be seen from the Figures, when there is no malicious users in the network, the optimal sensing performance can be achieved if K cognitive users are reliable nodes.

Fig 11 shows the detection performance. The detection performance , in which K - N0 RNs participate in the collaboration, is inferior. The detection performance of the scheme with no reputation mechanism dropped dramatically under the AO attack pattern, which means it is indispensable for CRNs to adopt a necessary and effective security mechanism to defend against various types of spiteful attack behaviors. When the number of MUs exceeds half of all cognitive users, the sensing performance is even worse than that of random guessing. The proposed system achieve the equivalent performance of K - N0 reliable nodes, meaning that they can availably identify the malicious SUs and eliminate their harmful effects via only using reliable reported results for fusion decision making.

4. CONCLUSION

Generally trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors. That is, the trust value is used to reflect whether a sensor node is willing and able to act normally in WSNs. In this paper, a trust value ranges from 0 to 1. A value of 1 means completely trustworthy and 0 means the opposite. In future we will consider recommendation trust, direct trust and indirect trust models for further calculating SSDF attack efficiently. Direct trust is a kind of trust calculated based on the direct communication behaviors. It reflects the trust relationship between two neighbor nodes. Recommendation trust is defined as the calculation of trust based on recommendations from neighbor nodes. An efficient mechanism is used to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust. The indirect trust value is gained based on the recommendations from other nodes.

ACKNOLEDGEMENT

This work was supported in part by Department of Science & Technology (DST), FIST Program at Francis Xavier Engineering College, Tirunelveli, Tamilnadu, India.

REFERENCES

[1] Muthukumaran. N and Ravi. R, 'Hardware Implementation of Architecture Techniques for Fast Efficient loss less Image Compression System', Wireless Personal Communications, Volume. 90, No. 3, pp. 1291-1315, October 2016, SPRINGER.

[2] Muthukumaran. N and Ravi. R, 'The Performance Analysis of Fast Efficient Lossless Satellite Image Compression and Decompression for Wavelet Based Algorithm', Wireless Personal Communications, Volume. 81, No. 2, pp. 839-859, March 2015, SPRINGER.

[3] K. Khoshelham, C. Nardinocchi, E. Frontoni, A. Mancini, and P. Zingaretti, "Performance evaluation of automated approaches to building detection in multi-source aerial data," ISPRS Int. J. Photogramm. RemoteSens., vol. 65, no. 2010, pp. 123–133, Jan. 2010.

[4] Muthukumaran. N and Ravi. R, 'VLSI Implementations of Compressive Image Acquisition using Block Based Compression Algorithm', The International Arab Journal of Information Technology, vol. 12, no. 4, pp. 333-339, July 2015.

[5] Anil Lamba, "Uses Of Cluster Computing Techniques To Perform Big Data Analytics For Smart Grid Automation System", International Journal for Technological Research in Engineering, Volume 1 Issue 7, pp.5804-5808, 2014.

[6] Anil Lamba, "Uses Of Different Cyber Security Service To Prevent Attack On Smart Home Infrastructure", International Journal for Technological Research in Engineering, Volume 1, Issue 11, pp.5809-5813, 2014.

[7] Anil Lamba, "A Role Of Data Mining Analysis To Identify Suspicious Activity Alert System", International Journal for Technological Research in Engineering, Volume 2 Issue 3, pp.5814-5825, 2014.

[8] Anil Lamba, "To Classify Cyber-Security Threats In Automotive Doming Using Different Assessment Methodologies", International Journal for Technological Research in Engineering, Volume 3, Issue 3, pp.5831-5836, 2015.

[9] Anil Lamba, "A Study Paper On Security Related Issue Before Adopting Cloud Computing Service Model", International Journal for Technological Research in Engineering, Volume 3, Issue 4, pp.5837-5840, 2015.

[10] Muthukumaran. N and Ravi. R, 'Simulation Based VLSI Implementation of Fast Efficient Lossless Image Compression System using Simplified Adjusted Binary Code & Golumb Rice Code', World Academy of Science, Engineering and Technology, Volume. 8, No. 9, pp.1603-1606, 2014.

[11] Ruban Kingston. M,Muthukumaran. and N, Ravi. R, 'A Novel Scheme of CMOS VCO Design with reduce number of Transistors using 180nm CAD Tool', International Journal of Applied Engineering Research, Volume. 10, No. 14, pp. 11934-11938, 2015.

[12] Muthukumaran. N and Ravi. R, 'Design and analysis of VLSI based FELICS Algorithm for lossless Image Compression', International Journal of Advanced Research in Technology, Vol. 2, No. 3, pp. 115-119, March 2012.

[13] Manoj Kumar. B and Muthukumaran. N, 'Design of Low power high Speed CASCADED Double Tail Comparator', International Journal of Advanced Research in Biology Engineering Science and Technology, Vol. 2, No. 4, pp.18-22, June 2016.

[14] Anil Lamba, "Uses Of Artificial Intelligent Techniques To Build Accurate Models For Intrusion Detection System", International Journal for Technological Research in Engineering, Volume 2, Issue 12, pp.5826-5830, 2015.

[15] Anil Lamba, "Mitigating Zero-Day Attacks In IOT Using A Strategic Framework", International Journal for Technological Research in Engineering, Volume 4, Issue 1, pp.5711-5714, 2016.

[16] Anil Lamba, "Identifying & Mitigating Cyber Security Threats In Vehicular Technologies", International Journal for Technological Research in Engineering, Volume 3, Issue 7, pp.5703-5706, 2016.

[17] Anil Lamba, "S4: A Novel & Secure Method For Enforcing Privacy In Cloud Data Warehouses", International Journal for Technological Research in Engineering, Volume 3, Issue 8, pp.5707-5710, 2016.

[18] Anil Lamba, "Cyber Attack Prevention Using VAPT Tools (Vulnerability Assessment & Penetration Testing)", Cikitusi Journal for Multidisciplinary Research, Volume 1, Issue 2, July - December, pp.64-71, 2014.

[19] N. Muthukumaran, 'Analyzing Throughput of MANET with Reduced Packet Loss', Wireless Personal Communications, Vol. 97, No. 1, pp. 565-578, November 2017, SPRINGER.

[20] P.Venkateswari, E.Jebitha Steffy, Dr. N. Muthukumaran, 'License Plate cognizance by Ocular Character Perception', International Research Journal of Engineering and Technology, Vol. 5, No. 2, pp. 536-542, February 2018.

[21] N. Muthukumaran, Mrs R.Sonya, Dr.Rajashekhara and Chitra V, 'Computation of Optimum ATC Using Generator Participation Factor in Deregulated System', International Journal of Advanced Research Trends in Engineering and Technology, Vol. 4, No. 1, pp. 8-11, January 2017.

[22] Ms. A. Aruna, Ms.Y.Bibisha Mol, Ms.G.Delcy, Dr. N. Muthukumaran, 'Arduino Powered Obstacles Avoidance for Visually Impaired Person', Asian Journal of Applied Science and Technology, Vol. 2, No. 2, pp. 101-106, April 2018.

[23] Mrs. S. Murine Sharmili, Dr. N. Muthukumaran, 'Performance Analysis of Elevation & Building Contours Image using K-Mean Clustering with Mathematical Morphology and SVM', Asian Journal of Applied Science and Technology, Vol. 2, No. 2, pp. 80-85, April 2018.

[24] Keziah. J, Muthukumaran. N, 'Design of K Band Transmitting Antenna for Harbor Surveillance Radar Application', International Journal on Applications in Electrical and Electronics Engineering, Vol. 2, No. 5, pp. 16-20, May 2016.

[25] B.Renuka, B.Sivaranjani, A.Maha Lakshmi, Dr. N. Muthukumaran, 'Automatic Enemy Detecting Defense Robot by using Face Detection Technique', Asian Journal of Applied Science and Technology, Vol. 2, No. 2, pp. 495-501, April 2018.

[26] Ms.Mary Varsha Peter, Ms.V.Priya, Ms.H.Petchammal, Dr. N. Muthukumaran, 'Finger Print Based Smart Voting System', Asian Journal of Applied Science and Technology, Vol. 2, No. 2, pp. 357-361, April 2018.

[27] Anil Lamba, "A Through Analysis on Protecting Cyber Threats and Attacks on CPS Embedded Subsystems", International Journal of Current Engineering and Scientific Research (IJCESR), Volume-1, Issue-3, pp.48-55, 2014.

[28] Anil Lamba, "Analysing Sanitization Technique of Reverse Proxy Framework for Enhancing Database-Security", International Journal of Information and Computing Science, Volume 1, Issue 1, pp.30-44, 2014.

[29] Anil Lamba, "Enhancing Awareness of Cyber-Security and Cloud Computing using Principles of Game Theory", International Journal of Advanced in Management, Technology and Engineering Sciences, Volume III, Issue I, pp.71-82, 2013.

[30] Anil Lamba, "Resolve Security Policies Conflicts Through Semantics Matching Alignment", International Journal of Scientific Research and Review, Volume 2, Issue 2, pp.43-58, 2013.

[31] Anil Lamba, "A Detailed Analysis of Data Security in a cloud Environment", SURAJ PUNJ Journal for Multidisciplinary Research, Volume 3, Issue 2, pp.43-51, 2013.

[32] Muthukumaran. N and Ravi. R, 'Quad Tree Decomposition based Analysis of Compressed Image Data Communication for Lossy and Lossless using WSN', World Academy of Science, Engineering and Technology, Volume. 8, No. 9, pp. 1543-1549, 2014.

[33] O. Ok, "Automated detection of buildings from single VHR multi spectral images using shadow information and graph cuts," ISPRS Int. J.Photogram. Remote Sens., vol. 86, no. 12, pp. 21–40, Sep. 2013.