SURVEY ONPRIVACY PRESERVING PUBLIC AUDITING MECHANISM FOR SHARED DATA IN CLOUD COMPUTING ENVIRONMENT

Dr. SuvarnaNandyal[1], Suvarna L. Kattimani[2], Aniruddha A. Atwadkar[3]

[1]Prof &Head of Department of CSE, P. D. A. College of Engineering, Gulbarga, (India)

[2]Assistant Professor, [3]PG Scholar(MTech), Department of CSE, BLDEA's Dr.P.G.Halakatti College of Engineering &Technology, Vijaypur, (India)

ABSTRACT

In Cloud Computing Environment, data is stored and shared among multiple users. It is very important as well as very challenging job to maintain the integrity of the data. The data stored in the cloud is considered as subject of skepticism and scrutiny as the data is stored in the untrusted cloud. This survey, proposes the new mechanism for public auditing of shared data in the cloud computing environment. This mechanism takes advantage of the ring signatures to compute the signatures used by the users. the correctness of the data is audited using ring signatures and the identity of signer on each block is hidden from the third party auditor(TPA).this mechanism shows the effective auditing on various user's data, who are members of group. This survey shows effectiveness and coherence of auditing the data publicly.

Keywords: Cloud Environment, Dynamic Groups, Public Auditing, Privacy Preserving, Shared Data.

I. INTRODUCTION

1.1 Defining a Cloud Computing

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS).a Some vendors use terms such as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to describe their products.

1.2 Classes of Utility Computing

Any application needs a model of computation, a model of storage, and a model of communication. The statistical multiplexing necessary to achieve elasticity and the appearance of infinite capacity available on demand requires automatic allocation and management**.**

1.3 Cloud Storage Integrity

Cloud computing requires comprehensive security solutions based upon many aspects of a large and loosely integrated system. The application software and databases in cloud computing are moved to the centralized large data centers, where the management of the data and services may not be fully trustworthy.A data integrity

checking algorithm which eliminates the third party auditing, to protect static and dynamic data from unauthorized observation, modification, or interference.

1.4 Data Correctness in Cloud Environment

The traditional approach for checking data correctness in cloud includes two steps. The first step is to retrieve the entire data from the cloud, and the second step is to verify data integrity by checking the correctness of signatures by RSA or hash values by MD5 of the entire data. Advantage of this approach is able to successfully check the correctness of cloud data. The disadvantage of this approach is efficiency decreased while using this traditional approach on cloud data.

1.5 Cloud Computing Economics

There are two particularly compelling use cases that favor utility computing over conventional hosting. A first case is when demand for a service varies with time. For example, provisioning a data center for the peak load it must sustain a few days per month leads to under-utilization at other times. Instead, cloud computing lets an organization pay by the hour for computing resources, potentially leading to cost savings even if the hourly rate to rent a machine from a cloud provider is higher than the rate to own one. A second case is when demand is unknown in advance.

For example, a Web startup will need to support a spike in demand when it becomes popular.

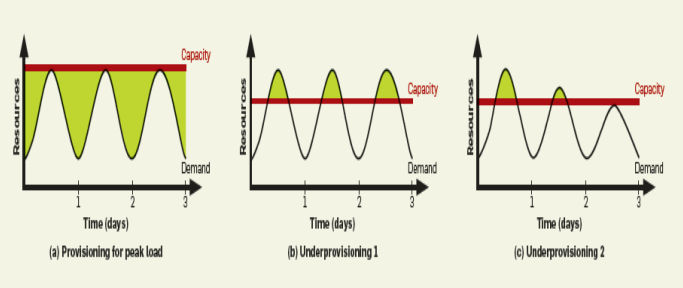


Fig. 1. (A) Waste of Resources Without Elasticity (B) Potential Revenue From Users Not Served. (C) Experiencing Poor Service.

1.6 Public Key Infrastructure

The shared file is divided into a number of small individual blocks, where each block is independently signed by one of the two users with Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing scheme. Once a block in this shared file is modified by a user, that particular user needs to sign the new block using his/her secret private key. Finally, different blocks are signed by various users due to the modification introduced by these different users. Then, in order to correctly audit the integrity or correctness of the entire data, a public verifier needs to choose the suitable public key for each block. Specifically, as shown in Fig. 2, after performing several auditing tasks, thethird party auditor can first learn that Alice may be a more important role in the group because most of the blocks in the shared file are always signed by Alice, on the other hand, this public verifier can also easily deduce that the eighth block may contain data of a higher value (e.g., a final bid in an auction), because this block is frequently modified by the two different users. In order to protect this confidential information, it is essential and critical to preserve identity privacy from third party auditor during public auditing.

As a result, thethird party auditor will inevitably learn the identity of the signer on each block due to the unique binding between an identity and a public key via digital certificates under public key infrastructure (PKI).

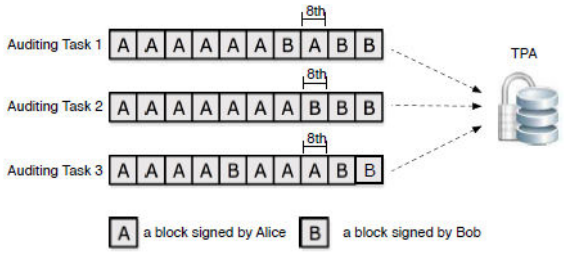


Fig. 2.Alice and Bob Share A File in the Cloud. the TPA Audits the Integrity of Shared Data With Existing Mechanisms.

II. EXISTING MECHANISM

In [1], thedescriptionis about framework for provable data possession. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs.Verifying the authenticity of data has emerged as a critical issue in storing data on untrustedservers. The client maintains a constant amount of metadata to verify the proof.The advantage of this scheme is the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public auditing.

Drawback

This mechanism is only suitable for auditing the integrity of personal data.

In [2], author describes about the security challenges cloud computing presents the burden of local data storage and maintenance. Public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor to check the integrity of shared data. The advantage of this mechanism is it eliminates the burden of cloud user from the tedious and possibly expensive auditing task.

Drawback

This mechanism only holds good for single user public auditing task.

In [3], author describes about a dynamic audit service for verifying the integrity of an untrusted and outsourced storage. The audit service is constructed based on the techniques,fragment structure, random sampling and index-hash table,supportingprovable updates to outsourced data, andtimely abnormal detection. Theresults not only validate the effectiveness of approaches, but also show audit system and verifies the integrity with lower computation overhead, requiring less extra storage for audit metadata.

Drawback

Less frequent activities may not detect in a timely manner.

In [4], the author describes about POR's scheme which is also able to check the correctness of data on an untrusted server. The original file is added with a set of randomly-valued check blocks called sentinels. The verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values. Sentinel Based POR protocol is amenable to real-world application.

Drawback

- **Integrity Threats**

First, an adversary may try to corrupt the integrity of shared data. Second, the cloud service provider may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors. Making matters worse, the cloud service provider is economically motivated, which means it may be unwilling to inform users about such corruption of data.

- **Privacy Threats**

The identity of the signer on each block in shared data is private and confidential to the group. During the process of auditing, a public verifier, who is only allowed to verify the correctness of shared data integrity, may try to reveal the identity of the signer on each block in shared data based on verification metadata.

In [5], author describes about an efficient PDP mechanism based on symmetric keys. This mechanism can support update and delete operations on data; however, insert operations are not available in this mechanism. It exploits symmetric keys to verify the integrity of data, it is not public verifiable.

Drawback

This scheme provides a user with a limited number of verification requests.

In [6], the author describes about leveraged homomorphic tokens to ensure the correctness of erasure codes-based data distributed on multiple servers. The major contribution of this mechanism is able support dynamic data, identify misbehaved servers.

Drawback

The leakage of identity privacy to public verifiers.

In [7], the author describes about a mechanism for auditing the correctness of data under the multi-server scenario, where these data are encoded by network coding instead of using erasure codes. This scheme minimizes communication overhead in the phase of data repair.

Drawback

This scheme requires bothBoneh–Lynn–Shacham (BLS) signatures and pseudo-random function.

In [8], the author describes about the problem of simultaneously achieving fine grainedness, scalability, and data confidentiality of access control. On one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents.

Drawback

This scheme has computing overhead complexity for cloud servers.

III. ARCHTECTURE

The architecture of proposed system is as shown in fig.3.

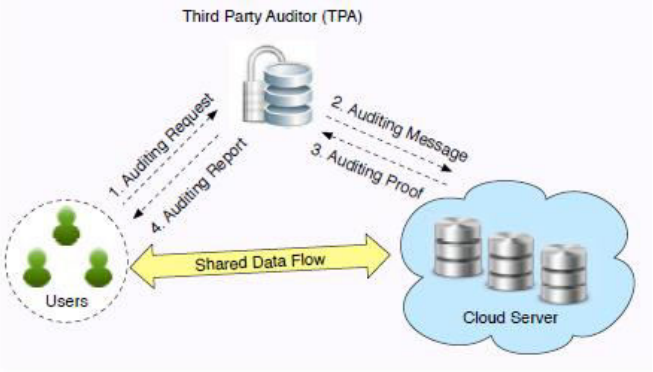


Fig. 3 Verification from TPA to Share the Data to Cloud Users

The proposed model architecture includes users, third party auditor(TPA), cloud server. The user requests for auditing the shared data in cloud by keeping the identity privacy to third party auditor.

The proposed system uses the HARS algorithm, which includes

KeyGen

Each user in the group generates his/her public key and private key.

RingSign

A user in the group is able to generate a signature on a block and its block identifier with his/her private key and all the group members public keys. A block identifier is a string that can distinguish the corresponding block from others.

RingVerify

A verifier is able to check whether a given block is signed by a group.

IV. SUMMARY OF CHARACTERISTICS BETWEENEXISTING SYSTEM AND PROPOSED SYSTEM.

SL. NO	METHODS	EXISTING (Privacy Preserving Public Auditing Scheme)	PROPOSED(ORUTA)
1	**Technique**	• Provable data possession (PDP) • Proofs of Retrievability (POR) • Dynamic Provable data possession (PDP)	ORUTA(One Ring to Rule Them All)
2	**Identity of signer**	Kept public to third party auditor	Kept private to third party auditor
3	**Auditing task**	Single auditing task	Multiple auditing task

V. CONCLUSION

In this paper, the proposed method is used to share data in the cloud. Privacy-preserving public auditing mechanism utilize ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data. The scheme cannot differentiate the signer on each block. Our mechanism is used to audit the dynamic groups. To improve the efficiency of verifying multiple auditing tasks.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” in Proc. ACM Conference on Computer and Communications Security(CCS), 2007, pp. 598–610.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[3] Y. Zhu, H.Wang, Z. Hu, G.-J.Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage inClouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

[4] A. Juels and B.S. Kaliski, "PORs, Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc. InternationalConference on Security and Privacy in Communication Networks(SecureComm), 2008.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[7] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

[8] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in Proc. International Conference on the Theory andApplication of Cryptology and Information Security (ASIACRYPT).Springer-Verlag, 2001, pp. 514–532.

A STUDY ON FINANCIAL LITERACY AMONG WORKING WOMEN IN EDUCATIONAL SECTOR OF JHANSI DISTRICT: WITH SPECIAL REFERENCE TO INVESTMENT AVENUE

Priyanka Agarwal[1], Dr. (Mohd) Shamim Ansari[2], Dr.Suman Yadav[3], Radhika Kureel[4]

[1,4]Research Scholar, Gautam Buddh Technical University, Lucknow Uttar Pradesh, (India)

[2]Senior Lecturer, Institute of Economics& Finance, Bundelkhand.University. Jhansi Uttar Pradesh,(India)

[3]Head & Lecturer Bundelkhand Institute of Engineering and Technology, Jhansi, Uttar Pradesh,(India)

ABSTRACT

Literacy is a key indicator of development. Today the people are more aware about the education but only literacy is not adequate. The awareness of financial literacy is now very essential. Financial literacy enable individuals to navigate the financial world make informed investment decision and minimize chances of being misled. Furthermore women should be knowledgeable especially about it since they are taking many household decision. However they are not interested in managing investment decision due to ignorance of Investment avenues. This paper therefore aims to analyze the investment decision of saving among respondents, it also study the knowledge about the investment avenue and analyze the investment pattern of both the teaching and non-teaching female staff in education sector of Jhansi District. The Major findings are that mostly working women are aware about the investment avenue and invest their saving in bank and post office fixed deposit.

Key Words: Financial Literacy, Investment Avenue, Women, Investment Decision

I. INTRODUCTION

Financial literacy has gained universal recognition all over the world .Even the fact that India is having a large population, a fast growing economy with a national focus on inclusive growth and an urgent need to develop a vibrant and stable financial system; it is all the more necessary to quickly formulate and implement the national strategy. Financial education or financial literacy has assumed greater importance in the recent years. Women traditionally were primarily responsible for the home and daily maintenance activities, which often include household budgeting and bill paying. Women's lack of knowledge and confidence with regard to money management and investment programs impacts their ability to reach their financial potential. The basic principles of investing are the same across all gender, but women do not look at financial matters in the same way as their counterpart does. Women who are empowered and educated must utilize tools and resources to reach their financial potential.

II. CONCEPT OF FINANCIAL LITERACY

Financial literacy is mainly used in connection with personal finance matters. Various dimensions of financial literacy are financial knowledge, financial behavior and financial attitude. Financial Literacy can broadly be defined as the capacity to have familiarity with and understanding of financial market products, especially rewards and risks in order to make informed choices. **According to OECD** defines "Financial Literacy as a combination of financial awareness, knowledge, skills, attitude and behavior necessary to make sound financial decisions and ultimately achieve individual financial well being. People achieve financial literacy through a process of financial education".

III. OBJECTIVES OF THE STUDY

1. To analyze the investment decision regarding saving of the working women in Education Sector in Jhansi District.
2. To study the knowledge about the investment avenue among working women in Jhansi District
3. To analyze the investment pattern of the working women in Jhansi District.

IV. METHODOLOGY OF THE STUDY

Sampling unit- Here "working women" in educational sector of Jhansi District are consider as sample unit. Here educational sector compose of primary, junior, secondary/higher secondary and under graduate/ bachelors degree education & higher education/post graduate level education. Women working at levels are considered for the study.

Sample size – since sample size depends on some constraint like budget, time, and information etc .here approximately 40 respondents has been considered for the effective study. 20 teaching and 20 non teaching respondents were considered for the study.

V. REVIEW OF THE EXTENSIVE STUDY

Lusardi, Annamaria .et.al (2010) examined financial literacy among the young, they showed that financial literacy is low, less than one-third of young adults possess basic knowledge of interest rates, inflation and risk diversification. Financial literacy was strongly related to socio demographic characteristics and family financial sophistication [1]. Willis, Lauren E (2011) stated that the final salvo of financial education promoters is usually that education is the only politically feasible path to improving consumers' financial lives. Once the true costs are considered, however, effective financial education looks much less politically palatable[2]Travnichek, Rebecca J.(2012) reviewed research that looked at college student's financial practices, credit usage behaviors, spending habits, and money attitudes. In addition, they identified future research opportunities, much of which needs to reflect the relationship between financial literacy and credit behavior, as well as longitudinal research to measure long-term effects of financial education on adult financial literacy[3]Thilakam,C.(2012) founded that the financial literacy is very important to make efficient decision on their finance. As compared to urban people the rural people have low level of awareness on finance matter. He also concluded that the government should literate the rural people financially through the camp, seminars, and conference then only the rural masses can make their investment in an efficient manner [4] Ramasawmy, Deerajen.et.al(2013) founded that overall,

management students at the University of Mauritius attach a sound level of importance to financial literacy to their subject of study., it was also founded that age, gender, language, race and income level do not have an impact on the level of financial literacy. They also recommended that financial literacy courses should be included in the curriculum so as to improve their level of knowledge and understanding in all financial matters [5].Shaari, Noor Aziah. et.al (2013) revealed that the spending habit and year of study have a significant positive relationship with the financial literacy, whereby the age and gender are negatively associated with the financial literacy [6] Taft, Marzieh Kalantarie, et.al (2013) founded that that age and education are positively correlated with financial literacy and financial wellbeing. Married people and men are more financially literate. Higher financial literacy leads to greater financial well-being and less financial concerns. Finally, financial wellbeing leads to less financial concern [7] GUPTA (2014) analyzed that micro entrepreneurs in district Kangra possess low financial skills. These are revealed by deficient record keeping practices, poor cash management, improper saving habits, and less awareness regarding different financial products and instruments. They concluded that to some extent micro entrepreneurs are lagging behind in the adoption of formal financial practices. The financial literacy programmes organized by the authorities should be directed to approach each sector of the society[8].Fatoki(2014) reviewed the extant literature on financial literacy in South Africa suggested that t here is the need for consistent publication of research findings on the levels of financial literacy by the government or private organizations involved in measuring financial literacy in South Africa[9] Prawitz, Aimee D(2014) examined whether financial education would influence financial behaviors that help people balance consumption and savings to maximize utility over the lifespan. Specifically, financial education participants and non-participants were compared on perceived financial wellness, savings ratios, frequency of negative financial behaviors, and the likelihood of performing specific financial activities, including budgeting, reviewing asset allocation strategies, retirement contributions, obtaining or updating life insurance plans, and obtaining or updating estate planning documents[10] very few studies for assessment of financial literacy have been carried out in India.

VI. ANALYSIS AND FINDINGS

One of the primary objectives of this paper has been to draw empirical evidence whether working women are investing their saving and they have knowledge about Investment Avenue. This paper attempted to analyze investment behavior of women working on education sector in India.

Table 1: Monthly Income of Family of Respondent

Job Profile in Education		Monthly income of family						Total
		10,000 - 20,001	20,001 - 30,000	30,001 - 40,000	40,001 - 50,000	50,001 - 1,00,000	1,00,000 & above	
Teaching	f	5	3	1	1	6	4	20
	%	*(25.0)*	*(15.0)*	*(5.0)*	*(5.0)*	*(30.0)*	*(20.0)*	
Non-Teaching	f	4	5	4	3	3	1	20
	%	*(20.0)*	*(25.0)*	*(20.0)*	*(15.0)*	*(15.0)*	*(5.0)*	
Total	**f**	**9**	**8**	**5**	**4**	**9**	**5**	**40**
	%	***(22.5)***	***(20.0)***	***(12.5)***	***(10.0)***	***(22.5)***	***(12.5)***	

(Source: Field Survey)

22.5% respondent have monthly income between Rs 10000 to 20,000. Another 22.5% have also reported that their family income is between Rs 50,000 to Rs 1, 00,000 (Table 1). Figure 1 given below reflects the family income of both teaching and non- teaching respondents.

Figure 1.Monthly Family Income

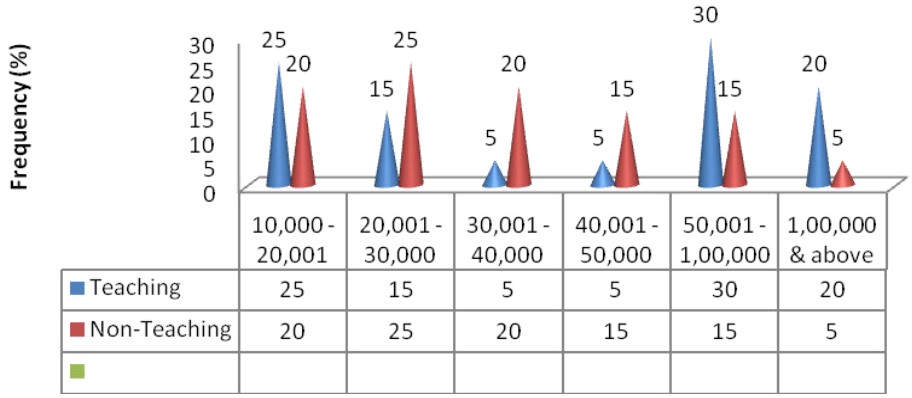


Table 2: Investment of saving by the Respondents

Respondents in Education Sector		Investment decision of saving among the Respondents		Total
		Yes	No	
Teaching	f	11	9	20
	%	*(55.0)*	*(45.0)*	
Non-Teaching	f	15	5	20
	%	*(75.0)*	*(25.0)*	
Total	**f**	**26**	**14**	**40**
	%	***(65.0)***	***(35.0)***	

(Source: Field Survey)

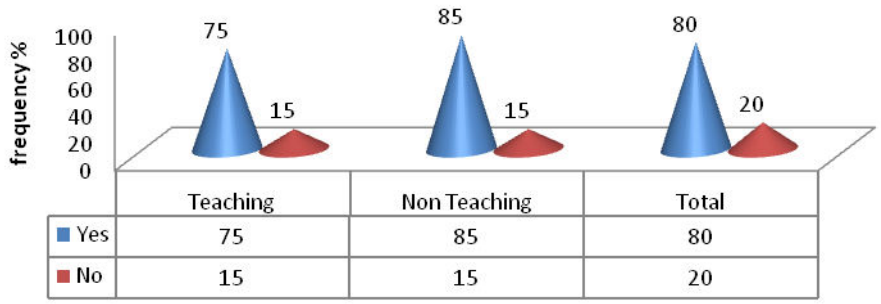
The Table-2 revealed that 65% respondent invests their savings where as 35% respondent do not invest their savings. However, it has been observed that non –teaching working women staff invests more as compared to non –teaching staff. 75% of the non-teaching respondent prefers to invest their savings while only 55% of the teaching staff prefers to invest. This may be because of teaching staff are able to save less than non-teaching staff.

Table: 3 Knowledge About the Investment Avenue of the Respondents

Respondents in Education Sector		Knowledge about the investment avenues		Total
		Yes	No	
Teaching	f	15	5	20
	%	*(75.0)*	*(25.0)*	
Non-Teaching	f	17	3	20
	%	*(85.0)*	*(15.0)*	
Total	f	32	8	40
	%	*(80.0)*	*(20.0)*	

(Source: Field Survey)

Figure 3: Knowledge about investment avenues of the respondents.



The tables-3 explained that out of the total respondents 80% respondent are aware about the investment avenues. The Fig: 3.1 revealed that in the teaching sector 75% respondents have knowledge about the investment avenues however 15% do not have knowledge about the investment avenues however in the non –teaching departments 85% respondent have knowledge of the investment avenues and 20% respondent are unaware about the investment avenues .

Table 4: Investment Pattern of the Respondents in Different Investment Avenue

Investment Avenues	Teaching (%)				Non Teaching (%)				TOTAL			
	Yes		No		Yes		No		Yes		No	
	F	%	F	%	F	%	F	%	F	%	F	%
Mutual fund	2	10	15	75	5	25	15	75	7	35	30	150
National savings certificate	1	5	16	80	9	45	11	55	10	50	27	135
Post office Fixed Deposit	7	35	10	50	7	35	13	65	14	70	23	115
Post office Recurring deposit	6	30	11	55	10	50	10	50	16	80	21	130
Bank Fixed Deposit	9	45	8	40	7	35	13	65	17	90	21	105

(Source: Field Survey)

Table 4 exhibit the investment pattern of the respondent in different avenues. In the teaching sector10% of the respondent invest in mutual funds and 75% respondent do not invest in mutual fund , 5% investment in National savings certificate , 80% do not invest in National savings certificate,35% respondent in post office

Fixed Deposit. ,50% respondent do not invest in post office F.D.,30% respondent invest in post office Recurring deposit., whereas55% respondent do not invest in post office Recurring deposit. 45% respondent invest in Bank F.D. whereas 40% respondent do not invest in Bank F.D. whereas in the non teaching sector. 25% of the respondent invest in mutual funds& 75% respondent do not invest in mutual fund., 45% investment in National savings certificate, 55% do not invest in National savings certificate, 35% respondent in post office Fixed .Deposit, 65% respondent do not invest in post office Fixed .Deposit., 50% respondent invest in post office Recurring deposit whereas50% respondent do not invest in post office Recurring deposit. 35% respondent invest in Bank Fixed .Deposit. Whereas 65% .respondent do not invest in Bank Fixed Deposit. .

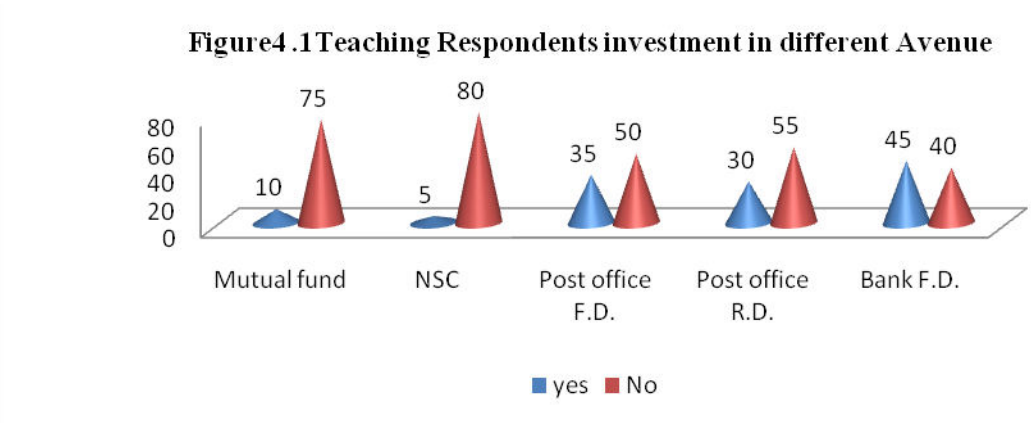


Figure: 4.1

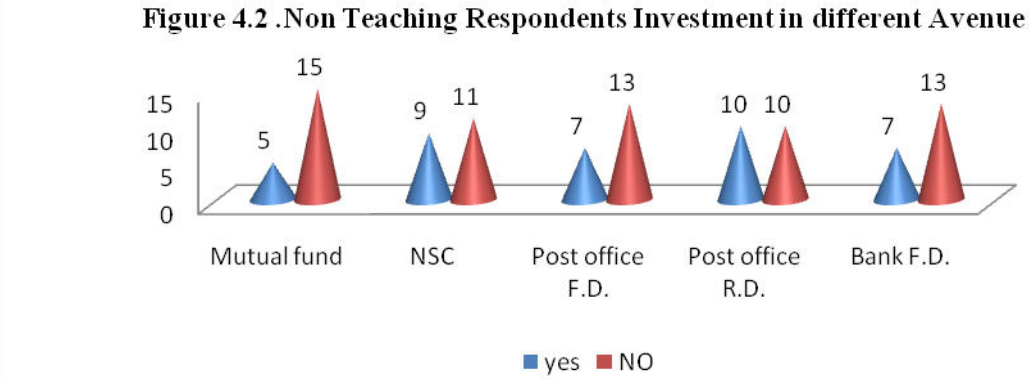
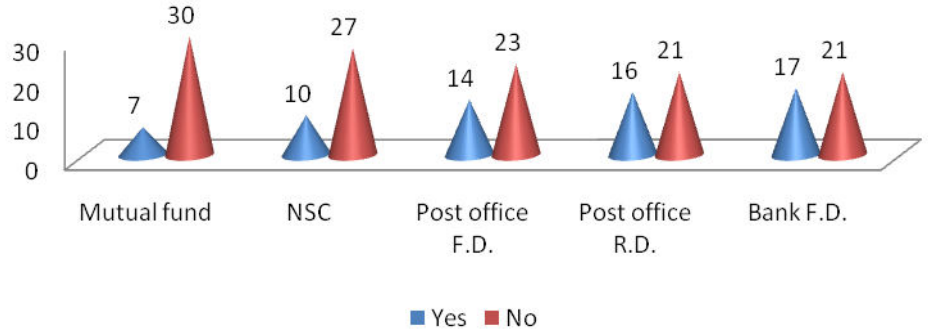


Figure: 4.2

Reveal that majority of the respondent invest in post office R.D. however only 5% of the respondent invest in mutual fund.

Figure 4.3Total Respondents Investment Avenues in DifferentTypes.



The Figure 4.3.showed total respondents of both teaching and non teaching levels of education sector. We find that majority of the investment is in Bank Fixed Deposit. and only 7% of the total respondent invests in mutual fund.

VII. CONCLUSION

Financial literacy is a foremost issue in today times, the people are more appealing to earn income but they are not serious about their investment decision and saving allocation. Through the financial literacy, they are able to take investment decision properly. The conclusion of this paper is that women should be more knowledgeable about the investment avenue since they are generally depends on their spouses or other family members. However they are focus on the some investment avenue viz: Bank and Post office Fixed Deposits only. Due to improper knowledge about the shares, Mutual Funds and other investment alternatives, they cannot able to take investment decision in such kind of alternatives confidently.

VIII. SUGGESTION

- As the majority is shown that 65% working women are take decision related to Investment Avenue. The percentage should be increase by awareness programme of Investment companies.
- Awareness Programme should be conducted for women by the Government to increase their Financial Literacy.
- Financial Education and training should be given to women for the financial well being of household.
- Established the separate financial institute for financial literacy to empower the investors.
- Awareness campaign should be organized by the Banks, NBFC and Investment companies to educate the investors.
- Time to time seminars should be conducted to increase the knowledge about the Investment alternatives.
- Financial Literacy Programmes should start at school level, as student and parents to be educated as early as possible.
- Methodology to assess existing financial literacy programme should be develop.
- Arrange financial behavior modification programme to the Investors with the support of the Government Projects.

REFERENCES

[1]. Lusardi, Annamaria.et al (2010) "Financial Literacy among the Young", The Journal of Consumer Affairs, Vol. 44, No. 2, 2010 ISSN 0022-0078 pp 358-380.

[2]. Willis Lauren E (2011) "The Financial Education Fallacy", American Economic Review: Papers and Proceedings 2011, pp429-434.

[3]. ravnichek.Rebecca J..(2012) "Student Financial Literacy: Campus-Based Program Development" Journal of Financial Counseling and Planning Vol 24 issue 2, 2013.pp 77-81.

[4]. Thilakam.C (2012) "Financial Literacy Among Rural Masses in India" The 2012 International Conference on Business and Management, pp204-217

[5]. Ramasawmy, Deerajen et al (2013) "A Study of the Level of Awareness of Financial Literacy among Management Undergraduates", Proceedings of 3rd Asia-Pacific Business Research Conference Kuala Lumpur, Malaysia, ISBN: 978-1-922069-19-1.

[6]. Shaari Noor Azizah et al (2013) "Financial Literacy: A Study among the university students" Interdisciplinary Journal of contemporary Research in Business, 2013 vol5.no 2 pp279-299.

[7] Taft.Marzieh Kalantarie et al (2013) "The Relation between Financial Literacy, Financial Wellbeing and Financial Concerns" International Journal of Business and Management; Vol. 8, No. 11; 2013 ISSN 1833-3850 E-ISSN 1833-8119 .

[8] Gupta.et al (2014) "A Study of Financial Literacy Among Micro Entrepreneurs in District Kangra" IMPACT: International Journal of Research I Business Management (IMPACT: IJRBM) ISSN(E): 2321-886X; ISSN(P): 2347-4572 Vol. 2, Issue 2, Feb 2014, 63-70.

[9] Fatoki Olawale & Olabanji Oni (2014) "Financial Literacy Studies in South Africa: Current Literature and Research Opportunities" Mediterranean Journal of Social Sciences, ISSN 2039-2117 (online),ISSN 2039-9340 (print) Vol 5 No 20 pp 409-414

[10] Prawitz Aimee.D (2014) "Workplace Financial Education Facilitates Improvement in Personal Financial Behaviors", Journal of Financial Counseling and Planning Volume 25, Issue 1, 2014, pp5-26.

AN EFFICIENT SPECTRUM DECISION MAKING FRAMEWORK FOR COGNITIVE RADIO NETWORKS

Bhagyashree Anil Dere[1], Prof. Sheetal Bhujade[2]

[1]*P.G. Student, Department of E &TC Engineering, Saraswati College of Engineering, (India)*

[2]*Asst. Professor, Saraswati College of Engineering, Navi Mumbai, Maharashtra, (India)*

ABSTRACT

This review paper is based on the spectrum decision framework for cognitive radio networks. Cognitive radio networks have been proposed as a solution to both spectrum inefficiency and spectrum scarcity problems. However, they face to a unique challenge based on the fluctuating nature of heterogeneous spectrum bands as well as the diverse service requirements of various applications. In this paper, a spectrum decision framework is proposed to determine a set of spectrum bands by considering the application requirements as well as the dynamic nature of spectrum bands. To this end, first, each spectrum is characterized by jointly considering primary user activity and spectrum sensing operations. Based on this, a minimum variance based spectrum decision is proposed for real-time applications, which minimizes the capacity variance of the decided spectrum bands subject to the capacity constraints. For best-effort applications, a maximum capacity-based spectrum decision is proposed where spectrum bands are decided to maximize the total network capacity.

I. INTRODUCTION

Today's wireless networks are characterized as a static spectrum assignment policy. Recently, because of the increase in spectrum demand, this policy is faced with spectrum scarcity at particular spectrum bands. On the contrary, a large portion of the assigned spectrum is still used sporadically leading to underutilization of the significant amount of spectrum [9]. Hence, dynamic spectrum access techniques have recently been proposed to solve these spectrum inefficiency problems. The key enabling technology for dynamic spectrum access techniques is the cognitive radio technology, which provides the capability to share the wireless channel with licensed users (or primary users) in an opportunistic manner [1]. Cognitive radio (CR) networks are envisioned to provide high bandwidth to mobile users via heterogeneous wireless architectures and dynamic spectrum access techniques. CR networks, however, impose unique challenges because of the high fluctuation in the available spectrum as well as the diverse quality-of-service (QoS) requirements of various applications. To address these challenges, first, CR networks are required to determine which portions of the spectrum are available, called spectrum sensing [2], [10]. Furthermore, how to coordinate multiple CR users to share the spectrum band, called spectrum sharing, is another important issue in CR networks [7], [16]. Although all these efforts enable CR users to exploit spectrum opportunities effectively, the heterogeneous spectrum environment introduces a new critical issue in CR networks. Generally, CR networks have multiple available spectrum bands over a wide frequency range that show different channel characteristics, and need to support applications with diverse service requirements. Therefore, once available spectrum bands are identified through spectrum sensing,

CR networks need to select the proper spectrum bands according to the application requirements. This process is referred to as spectrum decision, which constitutes an important but yet unexplored topic in CR networks. . To decide on spectrum bands properly, CR networks need to consider all available spectrum bands show different characteristics in the CR network. To select the proper spectrum, the CR network needs to characterize available spectrum bands by considering current radio conditions as well as the primary user (PU) activity. The CR network needs to provide a dynamic decision framework to consider all possible events that prevent reliable communications by closely interacting with other CR functionalities such as spectrum sensing and spectrum sharing. According to the PU activities, total capacity in CR networks varies over time, which makes it more difficult to decide on spectrum bands while maintaining the service quality of other CR users. Thus, the CR network should perform spectrum decision adaptively.

II. LITERATURE REVIEW

Most of the research on spectrum sharing in CR networks has mainly focused on how to efficiently allocate either spectrum or power among CR users subject to interference constraints. For spectrum allocation, a global optimization scheme is developed based on graph theory [17]. However, whenever the network topology changes according to the node mobility, the network needs to completely recomputed spectrum assignment leading to a higher computational and communication overhead. To solve this problem, a distributed spectrum allocation based on local bargaining is proposed in [4], where CR users negotiate spectrum assignment within local self-organized groups. For their source-constrained networks such as sensor and ad hoc networks, a rule-based spectrum management is proposed, where CR users access the spectrum independently according to both local observation and predetermined rules [5]. In [20], a dynamic channel selection scheme is developed for delay-sensitive applications based on a priority queuing analysis and a decentralized learning algorithm. Power allocation among CR users competing the same spectrum is another important issue in spectrum sharing. In [12], an optimal power allocation scheme is proposed to achieve ergodic and outage capacity of the fading channel under different types of power constraints and fading models. In [22], joint beam-forming and power allocation techniques are presented to maximize the user capacity while ensuring the QoS of primary users. Game theory provides an efficient distributed spectrum sharing scheme by describing the conflict and cooperation among CR users, and hence allowing each user to rationally decide on its be station. Thus, it has been widely exploited for both channel allocation [16] and for power allocation [7].

III. IMPLEMENTATION CHALLENGE IN SPECTRUM DECISION

All of the previous research explained above has mainly addressed spectrum sharing issues where all operations are performed within the same spectrum band or across contiguous channels. Furthermore, to adapt the fast time varying channels, they are generally designed as a short term operation, such as a packet-based or a time-slot based scheduling. However, CR networks necessitate an additional resource allocation capability when primary users are detected or CR users newly begin their sessions, which are relatively long-term events. Thus, this capability should consider longer-term channel characteristics, compared to spectrum sharing. In addition, since available spectrum bands are distributed over a wide frequency range, this function needs to be implemented as an inter- spectrum operation. However, this operation inevitably introduces an additional switching delay leading to service quality degradation. Thus, it is not desirable to extend existing spectrum sharing solutions

designed to adapt to the fast time-varying channel to the long-term inter-spectrum operation. This unique challenge in CR networks has not been addressed in previous research.

IV. PROPOSED SYSTEM MODEL

A novel capacity model is developed to describe unique characteristics in CR networks by considering PU activity as well as sensing capability. Accordingly, two different decision schemes are introduced. To satisfy the delay constraints in real-time applications, we propose a minimum variance-based spectrum decision (MVSD) scheme that selects spectrum bands to minimize capacity variation. For best-effort applications, we propose a maximum capacity-based spectrum decision (MCSD) scheme to maximize the total network capacity. Both decision schemes are controlled by a proposed resource management based on the current network condition. System Model in this paper, we consider an infrastructure-based CR network that has a centralized network entity, such as a base-station. The base-station exerts control over all CR users within its transmission range. CR users perform the observations and analysis on radio environments and feed them to the central base-station, which decides on spectrum availability and spectrum allocation. Each CR user has multiple software-defined radio (SDR) transceivers to exploit multiple spectrum bands over a wide frequency range by reconfiguring the operating frequency through software operations. Here, we assume frequency division duplex (FDD) systems where uplink and downlink channels are separated. Thus, the proposed decision scheme can be applied to each link independently. When primary users appear in the spectrum band, CR users need to move to a new available band, resulting in a temporary communication break. To solve this problem, we assume that multiple noncontiguous spectrum bands can be simultaneously used for the transmission in the CR network. This method can create a signal that is not only capable of high data throughput, but is also immune to the PU activity. Even if a primary user appears in one of the current spectrum bands, the rest of them will maintain current transmissions [1].The control channel plays an important role in exchanging information regarding sensing and resource allocation. Several methods are presented in [3], one of which is assumed to be used as the common control channel in our proposed method.

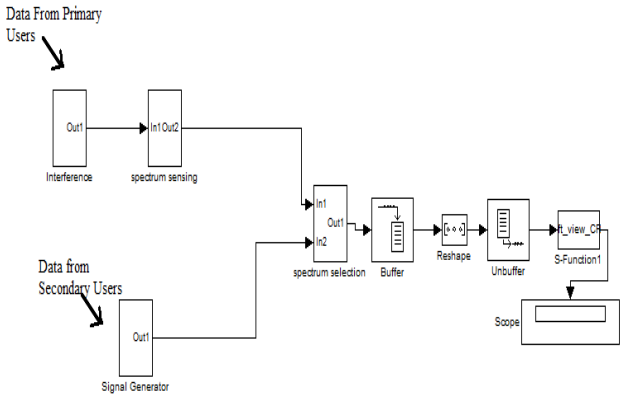


Fig 1 The Proposed Spectrum Decision Framework Model

V. DECISION FRAMEWORK OVERVIEW

The proposed spectrum decision framework model shown in Figure 1. consist of resource manager determines if the CR network accepts a new incoming CR user or not. If a new CR user is allowed to transmit, it is assigned to

the proper spectrum bands through spectrum decision. Since there may be multiple CR users competing the same spectrum, spectrum sharing coordinates those multiple accesses to prevent collisions, and accordingly to achieve the maximum capacity. In the event detection, current spectrum bands and users connections are monitored to detect decision events. The event detection consists of two main tasks: spectrum sensing and quality monitoring. When events are detected, the CR network reconfigures its resource allocation to maintain the service quality. In case of short-term channel variations such as fast fading, the CR network reallocates resources within the spectrum band through spectrum sharing. If a primary user is detected or the current spectrum band cannot provide the predetermined service quality any longer over a long-term period, the CR network switches the spectrum through the resource manager and the spectrum decision.

VI. PRIMARY USERS DETECTION IN A SPECTRUM

The main system for the detection of multiple primary users is shown above in fig. 2(a). in this system five different primary users are detected.

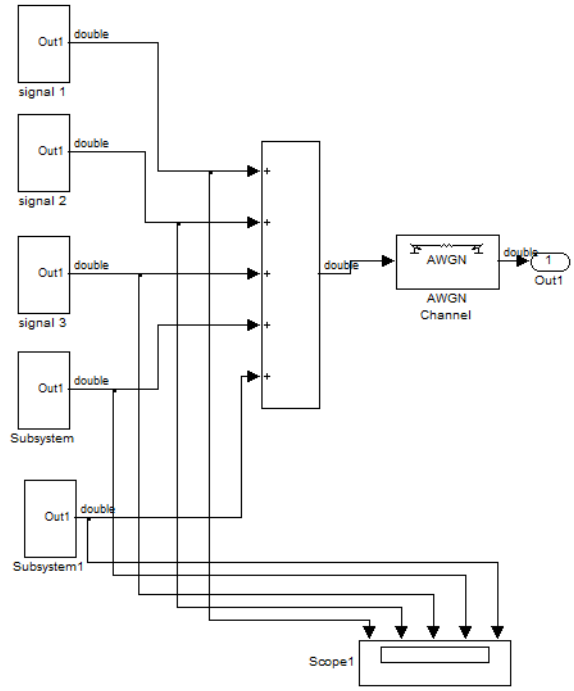


Figure 2(a) Primary Users Detected in a Spectrum

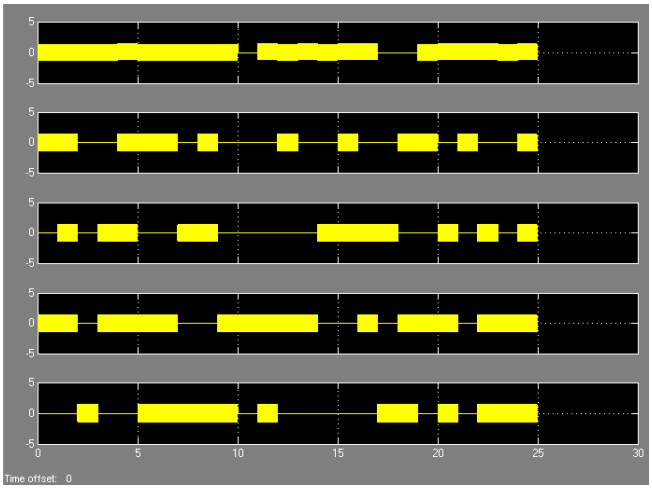


Fig 2 (b) Random Signals from Primary Users

Each user that is being detected generates random signals which are shown in the fig 2(b), further these five random signals are combined together and given to the workspace for comparing it with the Secondary Users or unlicensed users signal. Since these five combined signals are time-dependent signals they are further fed to the Fast Fourier transformation block in order to convert the time domain signals into frequency domain signals.

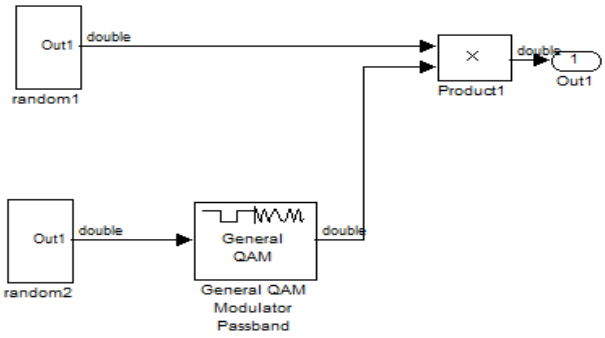


Fig 2(c) The Sub-System of Each Primary User

Each main system is divided into sub systems according to the number of users present in it as shown in fig 2(c). Random 1 and random 2 blocks generates random binary numbers. These digital signals are then combined with analog signal and their obtained product is obtained. Further the QAM modulator pass band block modulates the signal using double side-band amplitude modulation. The modulated signal is given to the main system as a Primary user signal.

VII. SPECTRUM SENSING MODEL

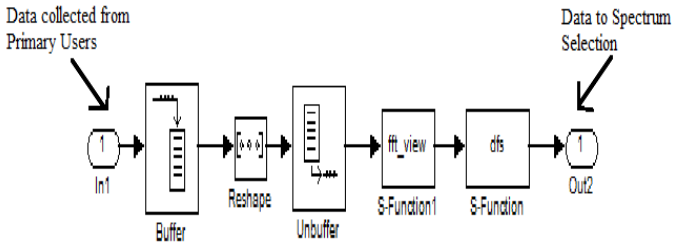


Fig 3(a) Spectrum Sensing Model

Data collected from multiple Primary Users is given to the spectrum sensing model as shown in fig.3 which consists of various blocks with different functions. The Buffer block redistributes the input samples to a new frame size. It collects the primary users' signals and sends the signals to the reshape block. The Reshape block changes the dimensionality of the input signal to a 2-D signal. The unbuffer block adjusts the output rate so that the sample period is the same at both the input and output. Further the sensed signals are fed to the frequency selection block.

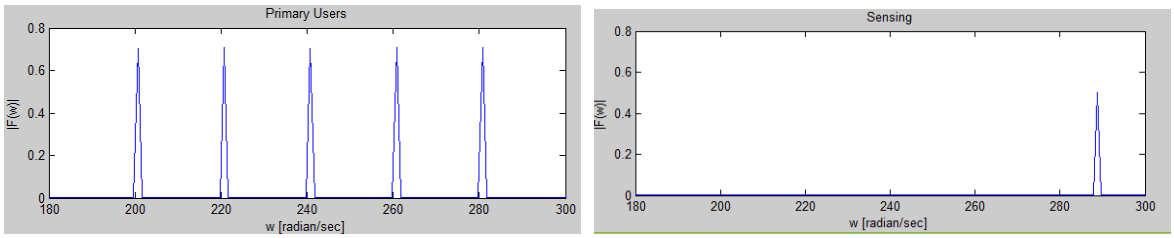


Fig 3(b) Response Generated by Sensing Model

VIII. SECONDARY USERS DETECTION IN A SPECTRUM

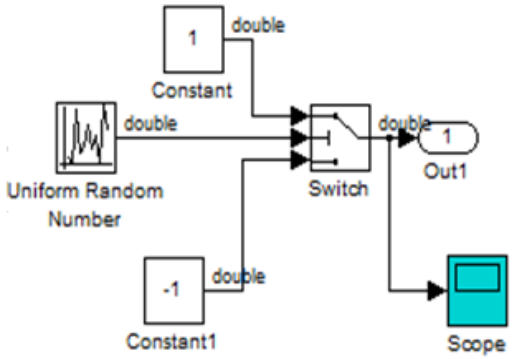


Fig 4(a) Secondary Users Detection in a Spectrum

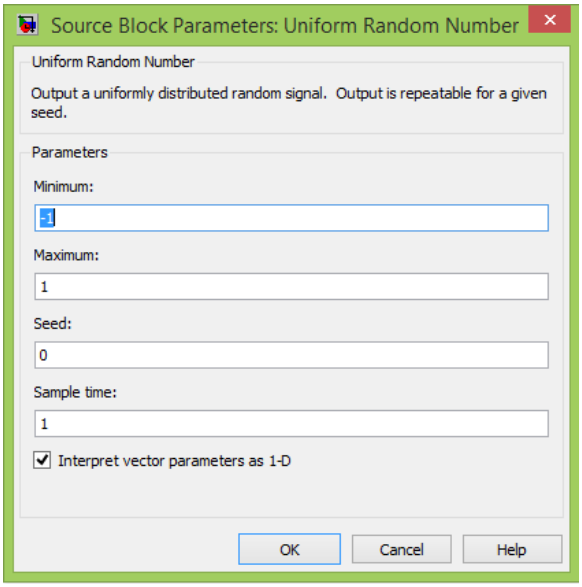


Fig 4(b) Parameters for Uniform Random Number Generator

Once the primary users are detected in spectrum, a random signal generator block generates random signals from the range -1 to 1. Seed is equal to 0 which indicates that the sequence is non-repeatable.

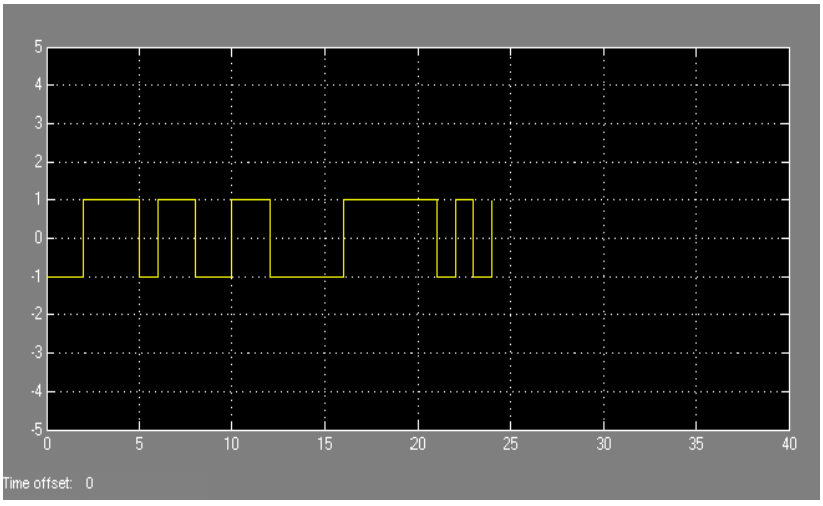


Fig 4(c) Random Signals from Secondary Users

IX. RESULTS AND DISCUSSION

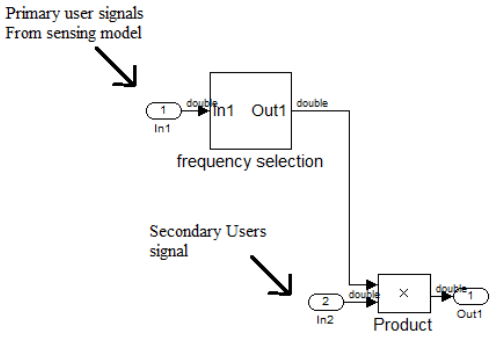


Fig 5(a) Frequency Selection Block

As shown in the above figure5(a) the Secondary Users signal and the Primary Users signals which are sensed in a sensing model are fed to the frequency selection block and further the product of Primary and Secondary Users is taken and Spectrum allocation is done as per the presence of users in a spectrum. The output of allocated spectrum is shown in the fig 5(b).

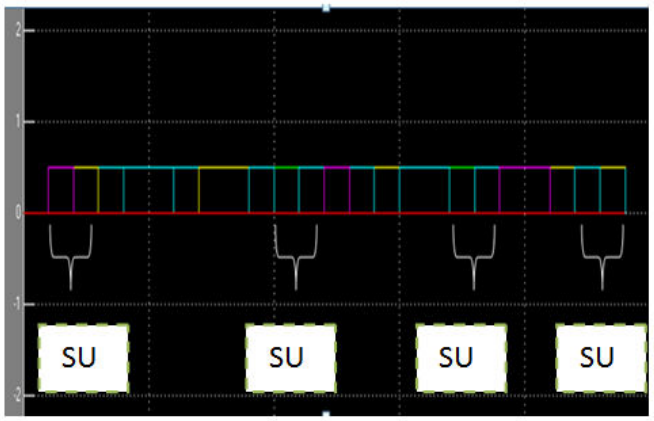


Fig 5(b) Spectrum Allocation to Secondary and Primary Users

X. CONCLUSION

In this review paper, we introduced a framework for spectrum decision to determine a set of spectrum bands by considering the channel dynamics in the CR network as well as application requirements. To this end, first, a novel spectrum capacity model is proposed that considers unique features in CR networks. Earlier cognitive model worked only for two Primary Users (PU) whereas this cognitive model works for five different Primary Users (PU).

Moreover, a dynamic resource management scheme is introduced to enable the CR network to coordinate spectrum decision adaptively dependent on the time-varying spectrum resources. Further the cognitive model for more than five licensed user is planned to be developed along with multiple unlicensed users or secondary used present in the same bandwidth.

XI. ACKNOWLEDGEMENTS

This work is based upon the spectrum decision framework paper by W.Y.Lee and I.F. Akyildiz.

REFERENCES

[1] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran, and S. Mohanty, "A Survey on Spectrum Management in Cognitive Radio Networks," IEEE Comm. Magazine, vol. 46, no. 4, pp. 40-48, Apr. 2008.

[2] D. Cabric, S.M. Mishra, and R.W. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios," Proc. IEEE Asilomar Conf. Signals, Systems and Computers, pp. 772-776, Nov. 2004.

[3] D. Cabric, S.M. Mishra, D. Willkomm, R. Brodersen, and A. Wolisz, "A Cognitive Radio Approach for Usage of Virtual Unlicensed Spectrum," Proc. 14th IST Mobile and Wireless Comm. Summit, June 2005.

[4] L. Cao and H. Zheng, "Distributed Spectrum Allocation via Local Bargaining," Proc. IEEE Sensor and Ad Hoc Comm. and Networks (SECON), pp. 475-486, Sept. 2005.

[5] L. Cao and H. Zheng, "Distributed Rule-Regulated Spectrum Sharing," IEEE J. Selected Areas in Comm., vol. 26, no. 1, pp. 130- 145, Jan. 2008.

[6] C. Chou, S. Shankar, H. Kim, and K.G. Shin, "What and How Much to Gain by Spectrum Agility?" IEEE J. Selected Areas in Comm., vol. 25, no. 3, pp. 576-588, Apr. 2007.

[7] R. Etkin, A. Parekh, and D. Tse, "Spectrum Sharing for Unlicensed Bands," IEEE J. Selected Areas in Comm., vol. 25, no. 3, pp. 517-528, Apr. 2007.

[8] J.R. Evans and E. Minieka, Optimization Algorithms for Networks and Graphs, second ed. CRC Press, 1992.

[9] FCC, ET Docket No 02-135, Spectrum Policy Task Force Report, Nov. 2002.

[10] M. Gandetto and C. Regazzoni, "Spectrum Sensing: A Distributed Approach for Cognitive Terminals," IEEE J. Selected Areas in Comm., vol. 25, no. 3, pp. 546-557, Apr. 2007.

[11] IEEE P802.22/D0.3.8.1, IEEE 802.22 WG, Draft Standard for Wireless Regional Area Networks Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands, IEEE, Sept. 2007.

[12] X. Kang, Y. Liang, A. Nallanathan, H. Garg, and R. Zhiang, "Optimal Power Allocation for Fading Channels in CR Networks: Ergodic Capacity and Outage Capacity," IEEE Trans. Wireless Comm., vol. 8, no. 2, pp. 940-950, Feb. 2009.

[13] W.-Y. Lee and I.F. Akyildiz, "Optimal Spectrum Sensing Framework for Cognitive Radio Networks," IEEE Trans. Wireless Comm., vol. 7, no. 10, pp. 3845-3857, Oct. 2008.

[14] W.-Y. Lee and I.F. Akyildiz, "Spectrum-Aware Mobility Management in Cognitive Radio Cellular Networks," to be published. [15] Y.C. Liang, Y. Zeng, E. Peh, and A.T. Hoang, "Sensing- Throughput Tradeoff for Cognitive Radio Networks," IEEE Trans. Wireless Comm., vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[16] N. Nie and C. Comaniciu, "Adaptive Channel Allocation Spectrum Etiquette for Cognitive Radio Networks," Proc.First IEEE Int'l Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05), pp. 269-278, Nov. 2005.

[17] C. Peng, H. Zheng, and B.Y. Zhao, "Utilization and Fairness in Spectrum Assignment for Opportunistic Spectrum Access," ACM Mobile Networks and Applications, vol. 11, no. 4, pp. 555-576, Aug. 2006.

[18] M.R. Chari, F. Ling, A. Mantravadi, R. Krishnamoorthi, R. Vijayan, G.K. Walker, and R. Chandhok, "FLO Physical Layer: An Overview," IEEE Trans. Broadcasting, vol. 53, no. 1, pp. 145-159, Mar. 2007.

[19] T. Rappaport, Wireless Communications: Principles and Practice, second ed. Prentice Hall, 2001.

[20] H. Shiang and M. Schaar, "Queuing-Based Dynamic Channel Selection for Heterogeneous Multimedia Applications over Cognitive Radio Networks," IEEE Trans. Multimedia, vol. 5, no. 10, pp. 896-909, Aug. 2008.

[21] K. Sriram and W. Whitt, "Characterizing Superposition Arrival Processes in Packet Multiplexers for Voice and Data," IEEE J. Selected Areas in Comm., vol. 4, no. 6, pp. 833-846, Sept. 1986.

[22] L. Zhang, Y. Liang, and Y. Xin, "Joint Beamforming and Power Allocation for Multiple Access Channels in Cognitive Radio Networks," IEEE J. Selected Areas in Comm., vol. 26, no. 1, pp. 38-51, Jan. 2008.

RESISTIVE TOUCHSCREEN BASED CHARACTER RECOGNITION SYSTEM

Meer Suri[1], Dr. Sukhwinder Singh[2]

[1]*Undergraduate Student, PEC University of Technology, Chandigarh, (India)*

[2]*Supervisor, Assistant Professor, PEC University of Technology, Chandigarh, (India)*

ABSTRACT

The project uses a 4 wire resistive touchscreen to acquire an input character from the user which is then processed in LabVIEW to compare with the database of stored characters and to display the closest match. The touchscreen produces an analog output that is converted to digital using the built in 10 bit ADC of the ATmega16 microcontroller and then sent serially to the computer equipped with LabVIEW.

Keywords: Character Recognition, LabVIEW

I. INTRODUCTION

Character or Handwriting recognition is used as an input method in mobile phones, PDAs, tablet PCs etc. The project aims to recognize a character drawn on the touchscreen which sent to a computer serially by an ATmega16 microcontroller. The digital version of the input produced by the microcontroller is processed by LabVIEW which compares it with the database of stored characters using statistics and then displays the closest match.

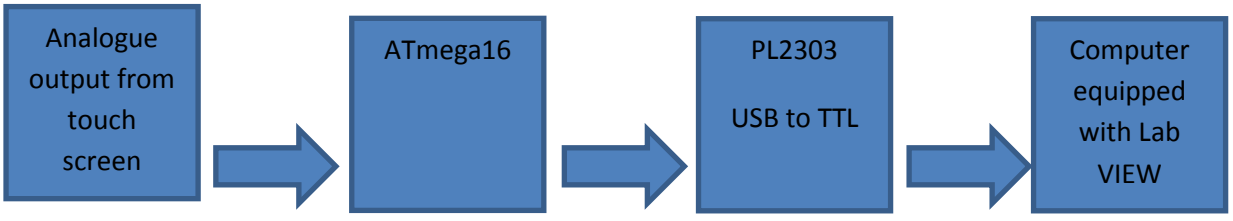
II. RELATED WORKS

Character or Handwriting recognition software has been in use in mobile phones, PDAs, tablet PCs for a long time. The first handwriting recognition system in a PDA came in 1993 in the Apple MessagePad[1]. Since then several sophisticated algorithms have been developed that con recognize words at a time and produce accurate results. In contrast this project uses a very simple algorithm based on statistics to do the recognition.

III. HARDWARE

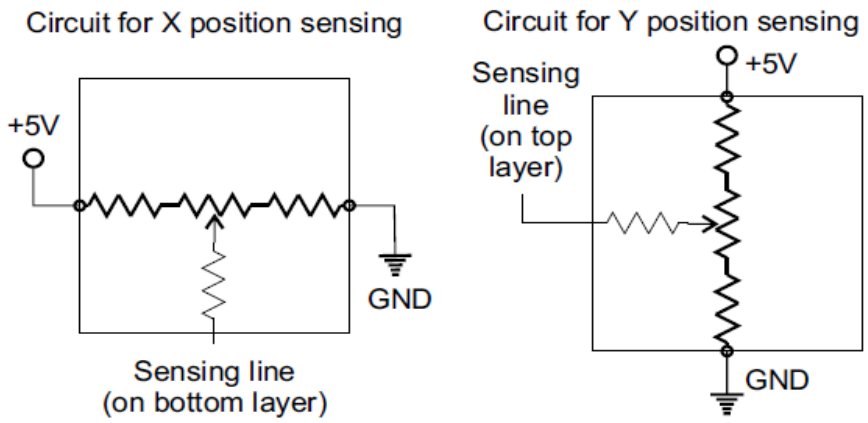
There are 4 components-

1. 4 wire analog resistive touchscreen
2. ATmega16 microcontroller
3. PL2303 USB to TTL converter
4. Computer equipped with LabVIEW



Resistive Touchscreen [2]

A 2- Dimensional sensing device that is constructed of 2 sheets of material separated slightly by spacers. A common construction is a sheet of glass providing a stable bottom layer and a sheet of Polyethylene (PET) as a flexible top layer .The 2 sheets are coated with a resistive substance, usually a metal compound called Indium Tin Oxide (ITO).When the PET film is pressed down, the two resistive surfaces meet. The position of a touch can be read by a touch screen microcontroller circuit.



ATmega16 microcontroller-

It has been used to acquire the input from the touchscreen and convert it to digital values using the built-in 10 bit Analog to Digital converter. It has been programmed to output digital coordinates of the touch in the format $x_1x_2x_3,y_1,y_2,y_3$ using full 10 bit resolution. Each digit of the coordinates is transmitted in one byte. These coordinates are sent serially to the computer through the USB to TTL converter.

IV. LABVIEW

It stands for Laboratory Virtual Instrument Engineering Workbench. It was developed to allow scientists and engineers to control instruments through computers using an easy to understand graphical programming language. LabVIEW has been used to serially acquire data using VISA libraries and then to plot and compare the input character with the database of characters.

V. MAIN VI

The main VI configures the serial port using controls setting the appropriate data bits, stop bits, baud rate and parity (not used). After the port has been configured it uses the VISA Read function to read data in every iteration of the while loop. In every iteration it reads one set of coordinates, uses the Match Pattern function to separate the X and Y coordinates and stores them in separate arrays. These arrays are then clustered together and sent for plotting to the XY Graph. Each set of coordinates is 8 bytes, 6 for the numbers, 1 for the comma and 1 for a new line character at the end, so 8 bytes are read every iteration.

When the user has finished entering the character, he may press the Recognize button on the front panel to do the character recognition and display the recognized character.

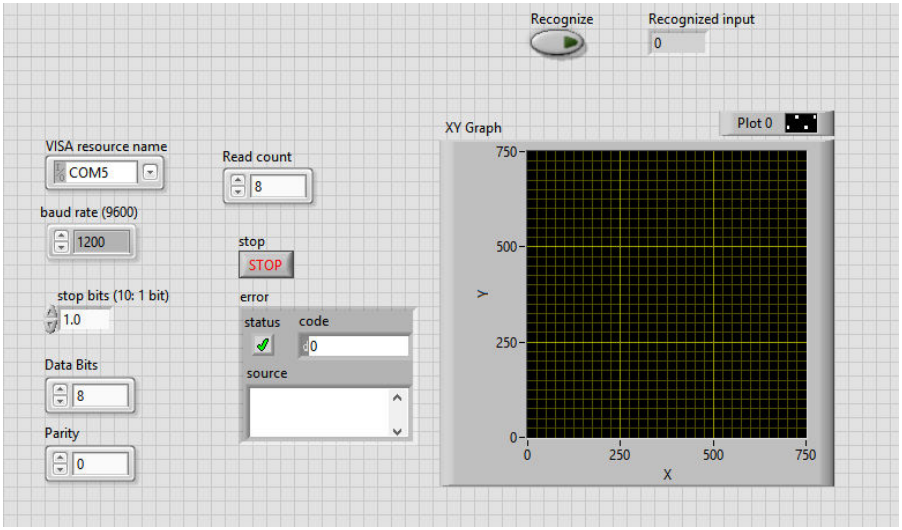


Figure 1 Front Panel of the Main VI

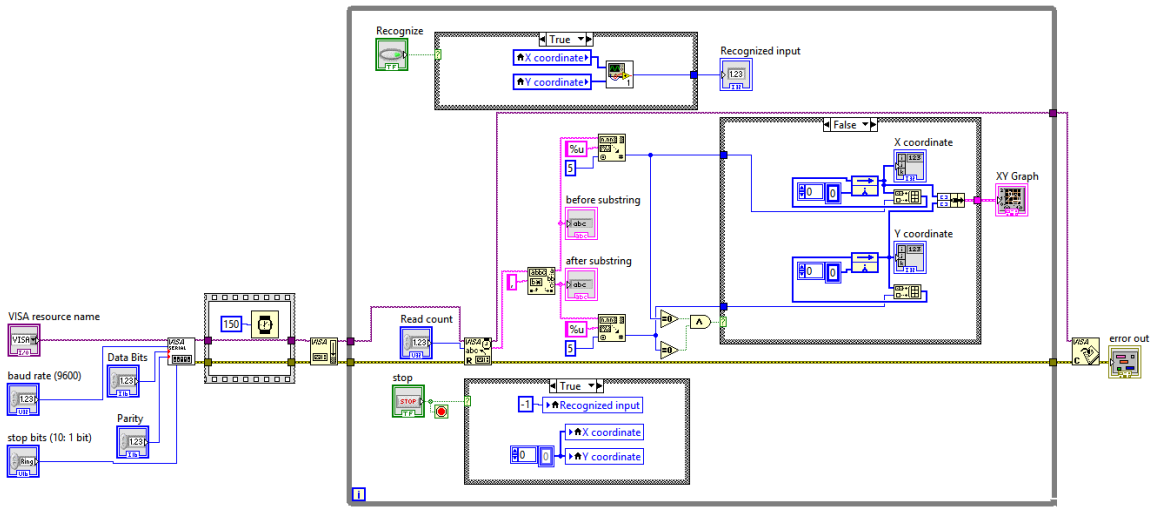


Figure 2 Block Diagram of the Main VI

After the user presses the Recognize button, the Compare subVI is passed the X and Y arrays of the input character. It does the recognition and displays the output.

VI. COMPARE SUBVI

The Compare subVI does the calculations for the recognition. It uses the Mean Absolute Deviation [3] function of Statistics for doing the comparisons. Mean Absolute Deviations of difference of input arrays and stored arrays calculated and compared. Mean Absolute Deviation of a data set tells us how far, on average, all values are from the mean value.

The mean absolute deviation of a set $\{x_1, x_2, ..., x_n\}$ is

$$\frac{1}{n}\sum_{i=1}^{n}|x_i - m(X)|.$$

$m(X)$ is the mean of the data set

It be zero for difference of 2 curves if they are identically drawn on the screen irrespective of their locations. It will be non-zero and will increase as the 2 curves being compared get more different from each other.

The subVI has access to the database of characters which consists of a text file for each character. Each text file contains the X and Y arrays of the character in the database, with which the input character's X and Y arrays will be compared. The subVI calculates the Mean Absolute Deviations of the difference of the input and stored characters and then compares these values iteratively in a Formula Node to find the character with least deviations compared to all others in the database. This is taken as the closest match and is displayed as the Recognized input on the Front Panel of the main VI

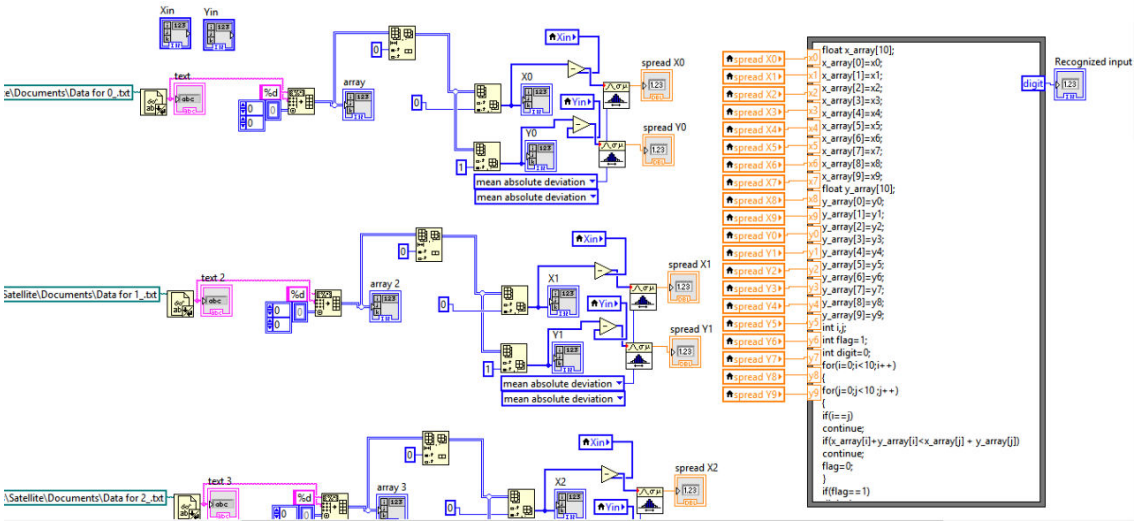


Figure 3 Block Diagram of the COMPARE subVI

VI. CONCLUSION

The accuracy of the character recognition system depends on the following:

1. The shape of the character in comparison to shape stored in the database. We got accurate results when the input was similar to the database. It was not a big constraint as characters did not have to be exactly the same for accurate results.
2. The speed at which the character was drawn when it was stored in the database. The speed has more influence on the accuracy as even if the same shape is drawn, but at a significantly different speed from the database, the result will be inaccurate.
3. While drawing on the touch screen, some points can appear randomly on the XY graph. If too many of these points appear, the accuracy will be decreased and results may not be as expected. These points may be due to noise in the ADC.
4. The baud rate plays a very significant role in deciding the error and speed of the data transmission.

So, if the speed at which the character is drawn and it's shape are similar to the character in the database, the results will be accurate most of the times.

VII. FUTURE SCOPE

This system is accurate enough to differentiate between similar characters provided the speed at which the character is drawn and its shape are similar to the ones in the database, so it would possible to include many more characters in the database without affecting accuracy.

A more advanced version could be made which would be able to recognize a word of writing at a time.

It could be used as pattern lock system for devices like mobile phones, PDAs, tablet PCs. A pattern to unlock the device would stored in the database and if the input would match with that, the device would unlock.

REFERENCES

[1] http://en.wikipedia.org/wiki/MessagePad

[2] https://www.sparkfun.com/datasheets/LCD/HOW%20DOES%20IT%20WORK.pdf

[3] http://en.wikipedia.org/wiki/Average_absolute_deviation

GESTURE CONTROLLED TOUCHSCREEN BASED AUTOMATION SYSTEM

Jatin Gaur

Department of Electronics and Communication Engineering, PEC University of Technology, Chandigarh, (India)

Mentored By: Dr. Sukhwinder Singh

ABSTRACT

In the proposed paper, graphical programming is used to create an automation system using a resistive touchscreen, basically a handy remote to control the electric and electronic appliances of the considered over apartment and office. A basic comparison algorithm is used to achieve the same. By means of serial communication, the above mentioned technology is implemented and Labview provides the GUI.

Keywords: Resistive, Touchscreen, Automation, Serial Communication, Labview, GUI.

I. INTRODUCTION

An enhanced, low-cost user interface using touch is a valuable feature for a variety of consumer, medical, automotive, and industrial devices. In many consumer applications, designers prefer expensive capacitive touch screens to resistive technologies because they can track a large number of fingers and seem to offer a friendlier interaction with the user. At present, low-cost resistive technologies fill a market niche where only a single touch is required, extremely accurate spatial resolution is obtained. Hence, through this project , our objective is to create a gesture recognition system and henceafter feeding it to a home automation system so as to match the increasing digitalization of the world.

II. EXISTING TECHNOLOGIES

Every work earlier was operated through switches that had to be turned on and off manually. As the technology grows, everything has gone embedded. To bring down the whole of the electrical system of a place, to a screen is an example of embedded system.

III. WORKING

3.1 Description

Basically the project converts the analog voltage coming from the resistive touch screen into a two co-ordinate integer value and sends it to the PC through the microcontroller. The processing code takes these co-ordinates as inputs and draws a white dot for each co-ordinate, on the output screen.

So when you write continuously on the touch screen, the dots would be plotted close enough to make it look like a line or curve.

3.2 ATMega16 Code Explanation

-Map the 4 pins of PORTA in the following way using "#define"

#define y1 PA1

#define x2 PA2

#define y2 PA3

#define x1 PA4

-Initialize the USART and ADC functions of the microcontroller.

-Enter into an infinite while loop

-Configure x1 (PA4) & x2 (PA2) as outputs. Set x1 (PA4) to high (+5V) state and x2 (PA2) to low (GND) state.

-Read the analog voltage at y2 (PA3) using ReadADC(3) command. Store the discrete value in the variable "x"

-Configure y1 (PA1) & y2 (PA3) as outputs. Set y1 (PA1) to high (+5V) state and y2 (PA3) to low (GND) state.

-Read the analog voltage at x1 (PA4) using ReadADC(4) command. Store the discrete value in the variable "y"

-Transmit the co-ordinates in "x, y" format to the PC using WrCoord(x,y) function.

A software 'Processing' was used to analyse the output when block diagrams in LabVIEW were in progress.

3.3 Processing Code Explanation

1. First we define the output screen size and also fill the background with some color using *size(width,height)* and *background(value)* functions.

Note: I have taken width=690 and height=540. You can take any values but make sure it's aspect ratio is same as that of the touch screen dimensions.

2. Next we need to create a serial connection, defining the COM port number where the board is connected and also the baud rate which is done by the following lines

Serial myport;

myport = new Serial(this,"COM9",57600);

COM9 is where my board is connected to and I have used baud rate=57600 bps since the program should keep up with my speed of writing.

3. Next we need to call a function whenever a data is available at the serial port. Then we need to read the data and store it in a string type variable.

void serialEvent(Serial p){

```
String stringData=myport.readStringUntil(10);
if(stringData!=null){
    stringData=trim(stringData);
    int data[]=int(split(stringData,','));
  if(data.length==2){
    x=data[0];
    y=data[1];
  }
```

Since our ATMega16 is programmed to continuously send the data (line after line), two set of co-ordinates may get into the "read" function same time causing errors. To avoid that we use "*readStringUntil(10)*" (where 10 is the ASCII value for a new line)instead of plain read. This is would help in setting a mark between two different co-ordinate by skipping every time after a new line occurs.

The *trim()* function is used to remove standard whitespace characters such as space, carriage return, and tab. Example:"1009,1024/r/n" will be converted into "1009,1024"

4. Next we split the string to extract the x and y co-ordinate separately. For this we use the *split(stringData,',')* function and store the co-ordinates in two different address locations of a integer type array.

Example: "1009,1024" is split into and stored as x=1009 and y=1024

5. Now that we have the raw co-ordinate value, we need to convert them into a sensible range of values corresponding to the screen size we are going to plot our sketch onto. For this we use the *map(value, start1, stop1, start2, stop2)* function. Where "value" is the incoming value to be converted

"start1" is the lower bound of the value's current range

"stop1" is the upper bound of the value's current range

"start2" is the lower bound of the value's target range

"stop2"is the upper bound of the value's target range

Then the converted co-ordinates are stored in variables "xcord" and "ycord".

6. Lastly we draw a solid circle (with small radius) at the co-ordinate given by xcord, ycord variables using *ellipse()* function.

7. At any point of time you can clear the drawing screen by pressing 'c' on the keyboard. This is achieved by using *keyPressed()* function.

3.4 Setup Instructions

1. You can either compile the code given using a suitable compiler like WINAVR with ATMEL STUDIO/AVR STUDIO or simply burn the "slate.hex" file given below.

2. Plug in the converter using an USB cable. If you are connecting it for the first time then get the drivers installed and note down the COM port to which the converter is connected. Go to System Properties> Device Manager and look out for the converter by its name to see the COM port number.

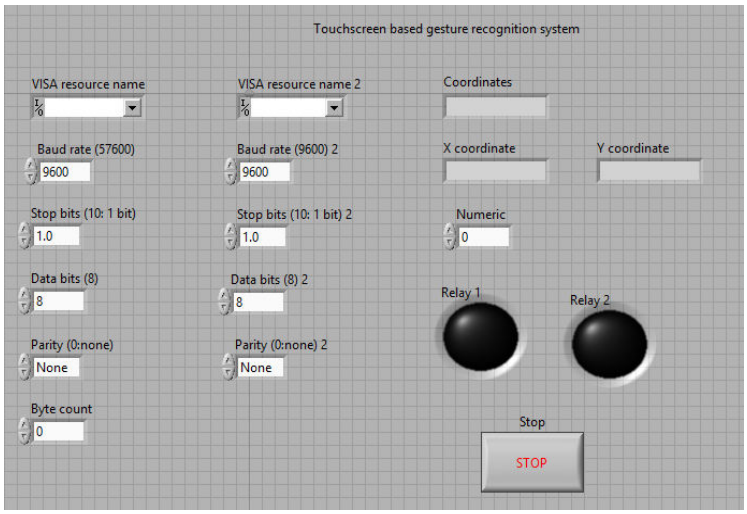
3. Open the processing software and copy paste the code given below. Remember to edit the COM port number.

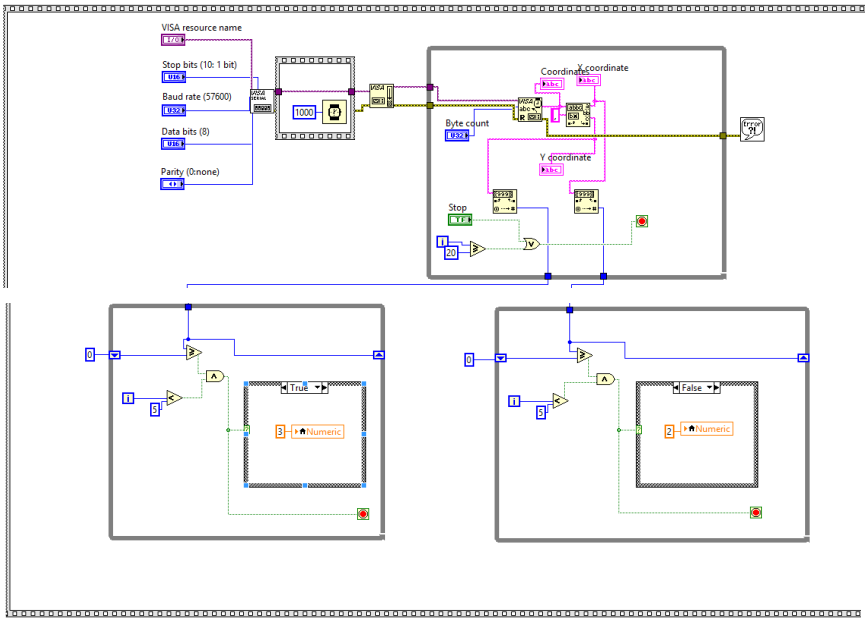
4. Click on the  button and also turn ON the development board.

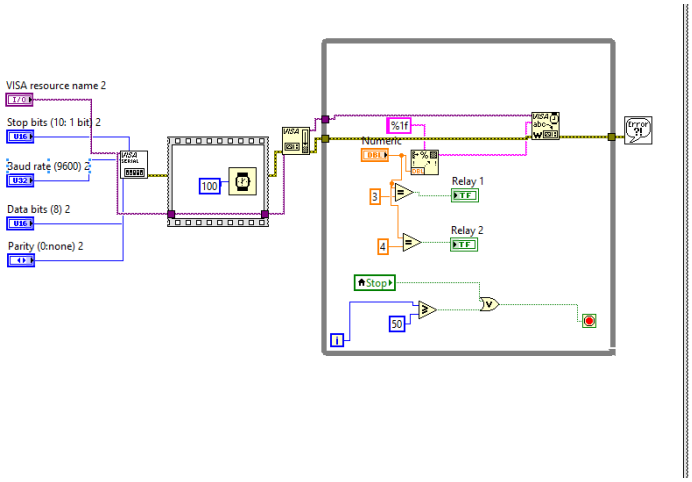
5. Now using your finger or a stylus, try drawing something onto the touch screen. If everything is done

properly then you should see something on the output screen window of the processing.The data can in the same way is fed to Labview and henceafter another controller to supply the power to the appliance.

IV. INTERFACING







V. CONCLUSION

The conclusion hence obtained is that the resistive touchscreen on interfacing with the ADC ports of a microcontroller can serve as a input to any software of our choice and henceafter be modified according to application of requirement.

VI. FUTURE SCOPE AND APPLICATIONS

1. Proper tactile feedback once established would increase sensitivity of touchscreen enormously making its applications suitable in security systems and biometric systems.
2. Technology will become a more organic and natural part of our daily lives, beginning through eyewear, in which we are already seeing in development or eventually, through our bodies becoming more intertwined with technology and hence the widened application in medical field.
3. Interaction with a host of touch sensors wrapped around the body of the phone.
4. interactions will be through the use of voice, gaze, gesture, or spatio-temporal intelligence — the device will know what user wants, before you even have the inkling that one wants to know it.

REFERENCES

[1]. http://www.engr.sjsu.edu/bjfurman/courses/ME106/ME106pdf/A2D_ATmega16.pdf
[2]. http://extremeelectronics.co.in/avr-tutorials/rs232-communication-the-basics/
[3]. http://files.spogel.com/abstracts/p-9385--smart-home-labview.pdf
[4]. http://www.atmel.com/devices/atmega16.aspx

REVİEW ON DİSTRİBUTED DENİAL OF SERVİCE ATTACKS AND THEİR DEFENSE

Madhavi Dhingra

Amity University Madhya Pradesh, Gwalior

ABSTRACT

Distributed Denial of Service attack (DDoS) attack has affected a large number of networks all over the world. It is not a single kinkd of attack; instead it comprises variety of attacks which occur at protocol level as well as application level. These attacks are reviewed in this paper. With attacks, defense comes naturally. Defense approaches regarding DDOS employ several methods and architectures, which are studied in this paper.

Keywords- DDoS Review, DDoS Attacks, DDoS Defense

I. INTRODUCTİON

Denial of Service (DoS) attack is the most popular and emerging threat for the past few years in the world of internet. A denial-of-service attack (DoS attack) denies the intended user to make use of the required resource by making it unavailable. The major goals of attackers are high profile web servers. With the increasing use of internet on every device, these attacks are spreading on a very large scale in numerous forms by many methods. Rather than relying on a single server, attackers could now take advantage of some hundred, thousand, even tens of thousands or more victim machines to launch the distributed version of the DoS attack. A distributed denial of service attack (DDoS attack) is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet [1].

The first well-publicized DDoS attack in the public domain was in February 2000. On February 7, Yahoo was the victim of a DDoS during which its Internet portal was inaccessible for three hours. Analysts estimated that during the three hours Yahoo was down, it suffered a loss of e-commerce and advertising revenue that amounted to about $500,000.

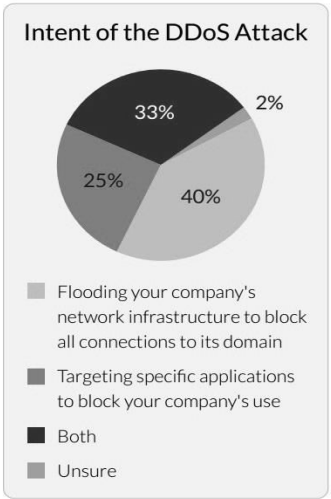


Fig.1 Intent of the DDoS Attack [2]

The impact of this attack was pervasive scale, and therefore network devices and servers are now making greater plans to secure and prevent them from such attacks. According to a survey conducted by incapsula, the intent of DDos attacks were flooding networks infrastructure to block all connections to organization's domain.[2]

II. DDOS ATTACKS

DDoS attacks can be broadly divided into three types:-

2.1 Volume Based Attacks

The attacks make use of large volumes of spoofed packets to flood the network and so as to consume the network bandwidth. Therefore its magnitude is measured in bits per second. It includes UDP floods, ICMP floods, and other spoofed-packet floods.

UDP Flood - This DDoS attack leverages the User Datagram Protocol (UDP), a session less networking protocol. This type of attack floods random ports on a remote host with numerous UDP packets, causing the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP Destination Unreachable packet. This process saps host resources, and can ultimately lead to inaccessibility.

ICMP (Ping) Flood - Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, which results in a significant overall system slowdown.

2.2 Protocol Attacks

Protocol attacks invade at the protocol level. They include SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. Its main goal is to exhaust actual resources such as firewalls and load balancers. The magnitude of Protocol attacks is measured in terms of packets per second.

SYN Flood - A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the "three-way handshake"), wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

Ping of Death - A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size - for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535

bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

2.3 Application Layer Attacks

Application layer attacks target the web servers with the intent to crash them. They target Windows, Apache or other software's. These include Slowloris, Zero-day DDoS attacks. It is measured in requests per second.

Slowloris - Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

HTTP Flood - In HTTP flood DDoS attack, the attacker exploits seemingly legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request.

Zero-day DDoS Attacks - "Zero-day" is simply unknown or new attacks, exploiting vulnerabilities for which no patch has yet been released. The term is well-known amongst the members of the hacker community, where the practice of trading Zero-day vulnerabilities has become a popular activity.

III. DDOS DEFENSE

The implementation of defense system is done either on an autonomous system or distributed system. Autonomous system uses a single node for detection of an attack and responding to an attack. While a distributed defense uses number of systems interconnected over the network which can be implemented anywhere on the network.

Defense regarding DDoS are performed in terms of prevention and detection and response.

Thus DDoS defense mechanisms are categorized into following three types [1] –

3.1 Survival Mechanisms

The goal of survival mechanisms is to limit the effect of DDoS attacks by inclusion of increased resources. Special load balancing techniques are used to maintain and increase the system capacity and performance. But it's not a foolproof approach as attackers can make thousands of zombies to attack multiple resources.

3.2 Proactive Techniques

These techniques aim to detect the attack before they occur. Once attack is detected, the attack lessening approach is followed.

3.3 Reactive Mechanisms

Reactive techniques are performed after an attack occurs on the services of the victim. In this technique, a detection and mitigation process is called to determine the source of the attack and filter the traffic from the

attack. They respond to attack by controlling the stream of attack or by finding out the location of the zombie machines and react to that either by controlling attack streams, or by attempting to locate agent machines and invoking human action. There have been numerous proposals and partial solutions available today for react to the DDoS attack. These mechanisms are further classified into spoofing based and non-spoofing based techniques involving ingress filtering, traceback etc.

Attack is detected following patterns or anomalies. In pattern detection, the identification pattern of known attacks is stored in database. Signatures are used as identification. Anomaly detection makes a model of normal system behavior. It compares the current system features with the expected normal system model. Anomaly detection procedure can also detect unknown attacks.

IV. DEFENSE ARCHİTECTURES

There are four primary factors involved in defense.

1. Agent Identification – This is the procedure that determines the attacking machines and provides their information to the victim machines.
2. Rate limiting – These mechanisms set the limit on the stream of data that can be treated as malicious.
3. Filtering - These mechanisms filter out the attack streams based on the characteristics set by the detection mechanism.
4. Reconfiguration – These mechanisms change the configuration of network by changing the topology of the victim machine or add more resources to isolate the attacks.

Depending on the deployment locations, three kinds of defense architectures are in use [4].

4.1 Source-End Defense Mechanisms

A generic architecture of source-end defense schemes is shown in Figure 2. The choking component imposes rate of outgoing connections. The Detection engine is used for comparing each incoming and outgoing traffic statistics based on predefined profiles. It detects as well as stops DDoS attack at the source and thereby prevents the flooding towards the whole network. The limitation of this approach is that it is not capable of detecting stack when sources are distributed in a wide area.

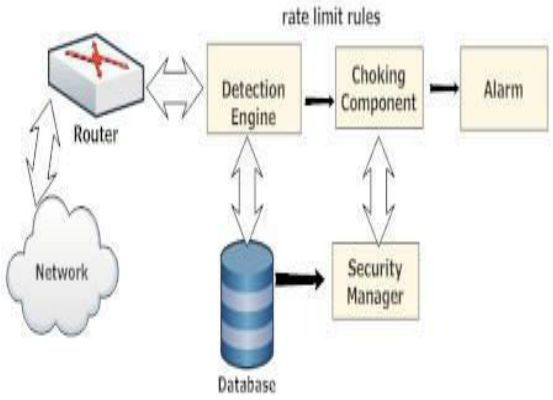


Fig. 2 Architecture for source-end DDoS Mechanism [4]

4.2 Victim-End Defense Mechanisms

This defense is implemented on the routers of victim networks. When resource utilization increases at routers, these routers are designated as victim. Thus it is essential to secure the network resources used by web servers. The only drawback of this approach is that the attack can be detected only after it attacks victim.

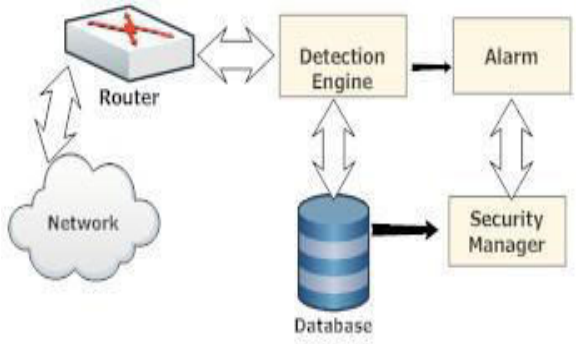


Fig. 3 Architecture for Source-End DDoS Mechanism [4]

4.3 Intermediate Network Defense Mechanisms

The intermediate network defense scheme balances the trade-offs between detection accuracy and attack bandwidth consumption, the main issues in source-end and victim-end detection approaches. Figure 3 shows a generic architecture of the intermediate network defense scheme which can be used in any network router. Such a scheme is usually cooperative in nature and also the routers share their observations with other routers. Like a source-end scheme, these schemes also impose rate limits on connections passing by the router when scrutiny with hold on normal profiles.

In this approach, detection and traceback of attack sources are simple because of cooperative operation. Routers can form an overlay mesh to share their observations. One main drawback of this approach is ability of deployment. All other routers on the network need to employ this detection scheme in order to achieve full detection accuracy. Obviously, full practical implementation of this scheme is extremely tough by reconfiguring all the routers on the Internet.

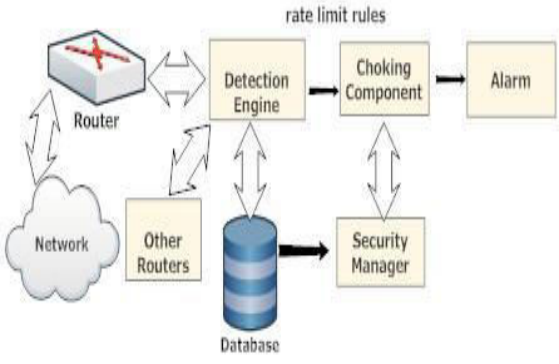


Fig. 4 Architecture for Intermediate Network Based DDoS Mechanism [4]

V. ATTACK DETECTION METHODS REVIEW

The work done on DDoS attack detection mechanism is classified under three basic methods [4].

5.1 Statistical Methods

Statistical properties of normal and attack patterns could be exploited for detection of DDoS attacks. A statistical inference test is applied to see whether any new instance belong to statistical model of normal traffic. Most common DDoS defense scheme is D-WARD [7]. A DWARD system is installed on source router that acts as gateway between the source network and the internet. It identifies an attack based on continuous watching of two way traffic between the two networks. Some other schemes are also proposed based on this method.

5.2 Knowledge based Methods

In this type of method, attack events are checked against predefined patterns of attack. These approaches make use of expert system. Examples of these approaches embody self-organizing maps and state transition analysis.

5.3 Soft Computing Methods

Soft computing comprises processing techniques that bear with imprecision and uncertainty.

Several methods are proposed that detect the network status and guard network servers, routers and client hosts. Zhong and Yue [8] present a DDoS attack detection model which extracts a network traffic model and a network packet protocol status model and sets the limit for the detection model. Captured network traffic values are clustered based on the k-means clustering algorithm to build initial threshold values for network traffic. All captured packets are used to build the packet protocol status model using the Apriori and FCM algorithms [9].

VI. CHALLENGES WITH PRESENT TECHNOLOGY

Many problems exist while implementing defense mechanisms. They are [10]-

(a) Large number of unwitting participants,

(b) No common characteristics of DDoS streams,

(c) Use of legitimate traffic models by attackers,

(d) No administrative domain cooperation,

(e) Automated tools,

(f) Hidden identity of participants,

(g) Persistent security holes on the Internet,

(h) Lack of attack information and

(i) Absence of standardized evaluation and testing approaches.

VII. CONCLUSION

DDoS attacks are increasing by leaps and bounds consequently. Their defense approaches are also refined periodically. After studying number of architectures and methods of defense, it is understood that attacks have their own features and in accordance with that, preventive techniques are used. However, success of defense techniques depends on the nature of attack and its level and implementation of defense method, especially in terms of unknown attack. Several methods and tools exist today for preventing the networks against these attacks. The need for modification occurs when some new kind of attack comes in the network.

REFERENCES

[1] A Survey on Solutions to Distributed Denial of Service Attacks, Shibiao Lin Tzi-cker Chiueh, Department of Computer Science, Stony Brook University, Stony Brook, NY-11794

[2] Incapsula Survey:What DDoS Attacks really Costs Business- DDoS Impact Survey

[3] Survey on DDoS Attacks and its Detection & Defence Approaches, Nisha H. Bhandari, International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1, Issue-3, February 2013, pp. 67-71

[4] Dileep Kumar, Dr CV Guru Rao, Dr Manoj Kumar Singh, Dr Satyanarayana, A Survey on Defense Mechanisms countering DDoS Attacks in the Network, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2013

[5] Ms. Anuja R. Zade, Dr. Suhas .H. Patil, A Survey On Various Defense Mechanisms Against Application Layer Distributed Denial Of Service Attack, International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397 Vol. 3 No. 11 November 2011, pp.3558-3563

[6] S.Karthik, Dr. V.P. Arunachalam, Dr.T.Ravichandran , An Analysis Of DDoS Attack Methods, Threats, Tools And Defense Mechanisms, IJERIA-An Analysis of DDoS Attack Methods Threats Tools and Defense Mechanisms

[7] Mirkoviac, J., Prier, G., and Reiher, P. (2002) Attacking DDoS at the source. Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEE CS.

[8] Zhong, R. and Yue, G. (2010) DDoS detection system based on data mining. Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, pp. 062–065. Academy Publisher.

[9] Agrawal, R. and Srikant, R. (1994) Fast algorithms for mining association rules in large databases. Proceedings of the 20th International Conference on Very Large Data Bases, Santiago de Chile, Chile, 12-15 September, pp. 487–499. Morgan Kaufmann.

[10] B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 pp.1793-8163

[11] Akamai‘s Prolexic Quarterly Global DDoS Attack Report Quarter 1 of 2014

[12] Arbor’s ninth Annual Worldwide Infrastructure Security Report (WISR), released march,2014, mim.umd.edu/wp-content/uploads/2012/10/arbor_networks_issue2-2.pdf

DESIGN OF MICROSTRIP PATCH ANTENNA WITH ENHANCED BANDWIDTH

Sabita Yadav[1], Amninder Kaur[2], Prof. (Dr.) K. K. Saini[3]

[1,2,3]*Dronacharya College of Engineering, Gurgaon, Haryana (India)*

ABSTRACT

In this work microstrip feed rectangular microstrip patch antenna for 5.2GHz IEEE 802.11 applications is proposed. The antenna is designed on Roger R03003 substrate with dielectric constant. The antenna parameters such as return loss, VSWR, gain and directivity are simulated and optimized using commercial computer simulation technology microwave studio (CST MWS). Latest optimization tools are used for desirable results. The main advantage of this antenna is that the designed structure is very simple compared to other proposed WLAN antennas and the cost for making this antenna is also low. In this work there is lot of scope for future research. As new parameters depending on applications can be added & correspondingly results will be analyzed.

Keywords: Microstrip Antenna, Monolithic Microwave Integrated Circuits, Wireless local Area Network.

I. INTRODUCTION

With rapid development of wireless communication the demand for devices that can operate in different bands is increased. However, multifrequency antennas have the advantages of surveying multiple frequencies with one antenna but the crosstalk from the neighbor bands makes them a weak choice [1]. The principal disadvantages of microstrip patch antenna are narrow bandwidth, low efficiency and small size [2]. Many researchers have been performed to enhance the bandwidth of printed antennas. To overcome this difficulty many methods and techniques are raised in the literature. The miniaturization of antenna and improvement in bandwidth can be obtained by adjusting to cut the slot in ground (DGS) and patch of microstrip antenna of proper length and width [3-5]. WLAN is a flexible data communication system which is implemented as an alternative to wired LAN. WLANs are becoming popular in a number of vertical markets such as retail, health, care, warehousing, manufacturing and academia which have profited from use of handheld terminal for real time information transmission to centralized hosts for processing [6]. WLAN are also being widely recognized as a reliable, cost effective solution for wireless high speed data connectivity.

There are three operation bands in the IEEE 802.11 WLAN standards:

- IEEE 802.11b/g (2.4 - 2.484GHz)
- IEEE 802.11a (5.15 – 5.35GHz)
- IEEE 802.11a (5.725 – 5.825GHz) [7]

- IEEE 802.11a employs the higher frequency bands and these bands are mostly used in business network due to its higher cost. Slot antennas are the very good choice for WLAN because of the ability of various frequencies ease of fabrication and compatibility with monolithic microwave integrated circuits (MMIC).

A number of WLAN antennas have been recently proposed and reported in literature [7]. For designing compact sized WLAN antennas different and interesting methodologies are used few of them are as:

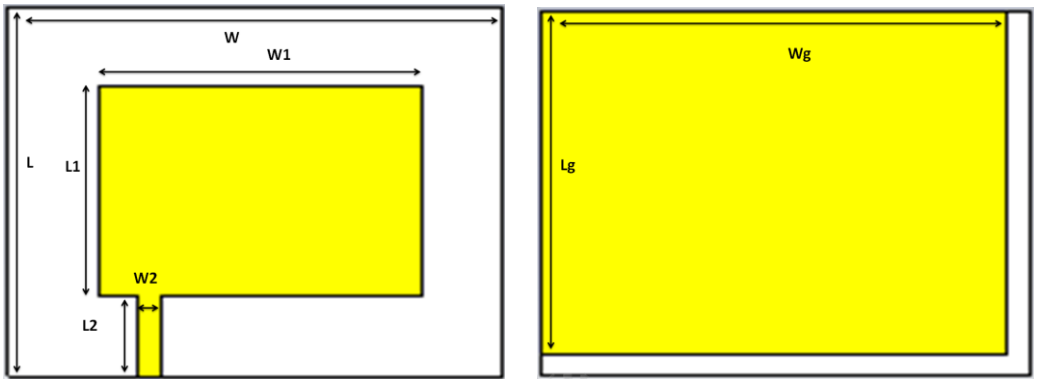
- Bending the monopole to different shapes has been used in [8]-[13].
- Effective size reduction techniques are the use of an inverted-F structure [14]-[17]. By inverted F structure achieving a compact size is a design challenge this challenge has been tackled in [18].
- The direct feed PIFA proposed in [19] was combined with parasitic element was used to generate the 5.8 GHz band.

This paper proposes a compact and simple Microstrip patch antenna. Designed antenna is operating in 5.2GHz IEEE 802.11 band. The main advantage of this antenna is this designing structure is very simple and compact as compared to other designed antennas [8]-[16]. And its bandwidth is improved using the DGS technique. As due to its simple design structure it can be easily designed and fabricated so it reduces cost and time of manufacturing this antenna and as the 5.2GHz WLAN antenna have indoor applications so the reduced cost can promote its applications in other areas too where the budget is not much high. The substrate used for designing this antenna is Roger R03003 which is good substrate material for better results.

In this paper there are three sections. The antenna design is explained in second section. In third section simulated results are mentioned of designed antenna, in results we are including the return loss, bandwidth, VSWR, gain, directivity and current distribution of proposed antenna. And in final section paper is concluded.

II. ANTENNA DESIGN

Roger R03003 substrate with the dimension of 22.18 × 23.35 mm and the thickness of 1.6 mm is used for designing this antenna the dielectric constant of this substrate is 3.5. For designing this antenna firstly we designed a simple rectangular patch antenna with patch dimensions 17.5 X 12.3 X 0.035. The microstrip feeding is used with dimension L2 = 4.8mm and W2 = 1.19mm for providing feed to this antenna as shown in Fig.1. Mcrostrip feedline is adjusted to the point on patch where best results are obtained.



(a) (b)

Fig .1. Proposed Antenna (a) Front View (b) Back view

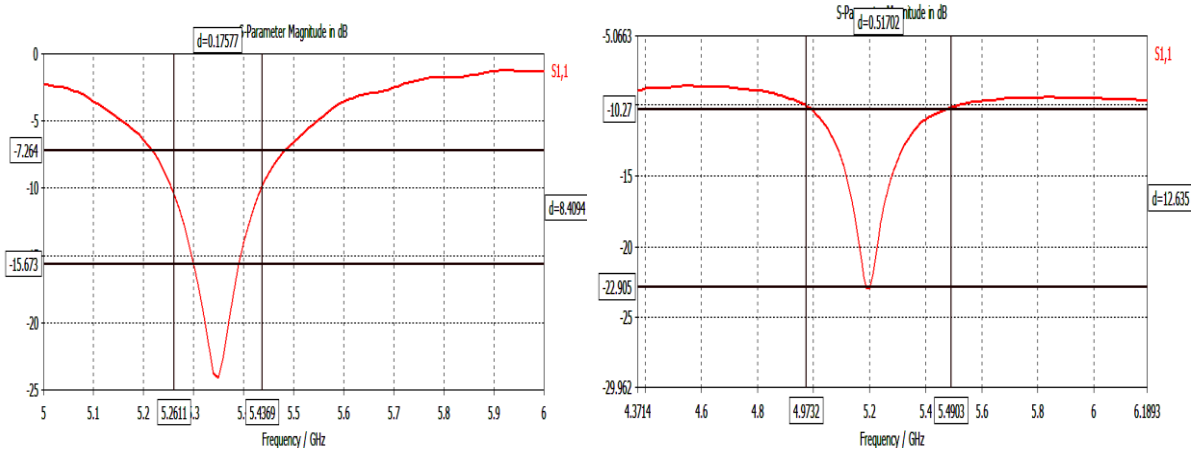
Table I Dimensions of Proposed Antenna

Antenna parameter	Value	Antenna parameter	Value
L	22 mm	W	26.4 mm
L1	12.5 mm	W1	17.3 mm
L2	4.8 mm	W2	1.2 mm
Lg	20.9 mm	Wg	25.1

By simulating the designed structure without changes in ground it is working for some band for the 5.35 GHz with bandwidth of 175MHz for IEEE802.11a WLAN band. Then its bandwidth is enhanced by making changes in ground and now its resonant frequency is 5.2GHz with bandwidth of 517MHz. Hence using DGS approx 350MHz bandwidth is increased. The geometry of the designed antenna is shown in Fig.1 and the dimensions of this antenna are listed in TABLE I.

III. RESULT AND DISCUSSION

Fig.2 (a) shows the simulated return loss of the antenna without DGS. The return loss gives the band from 5.26 to 5.43 GHz is less than -10 dB and -24.5 dB for the resonant frequency 5.35GHz. Then for enhancing the bandwidth of antenna [20], designed antenna is shown in Fig.1. Now the return loss is shown in Fig.2.(b), resonant frequency is 5.2GHz with band from 4.9 to 5.5 GHz its bandwidth is approx 520 MHz as shown in Fig.2.(b) and it under IEEE802.11 WLAN standards and it is used in indoor applications.



(a) **(b)**

Fig.2.Simulated Results for Return loss (a) without DGS (b) with DGS

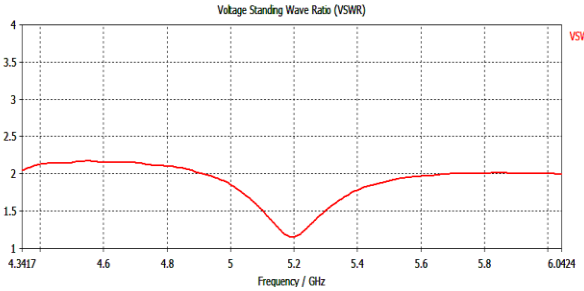


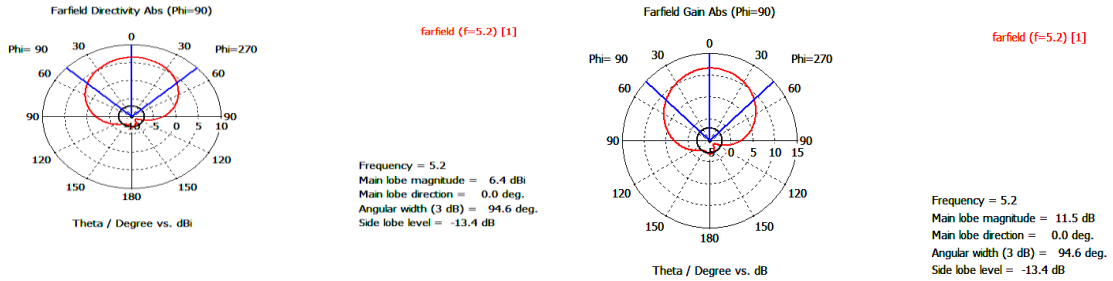
Fig.3.VSWR of Proposed Antenna

Fig.3 shows the simulated VSWR results of the proposed antenna. For microstrip antenna acceptable value of VSWR for resonant frequency should be less than or equal to 2. For this antenna VSWR at resonant frequency (5.2 GHz) is 1.19.

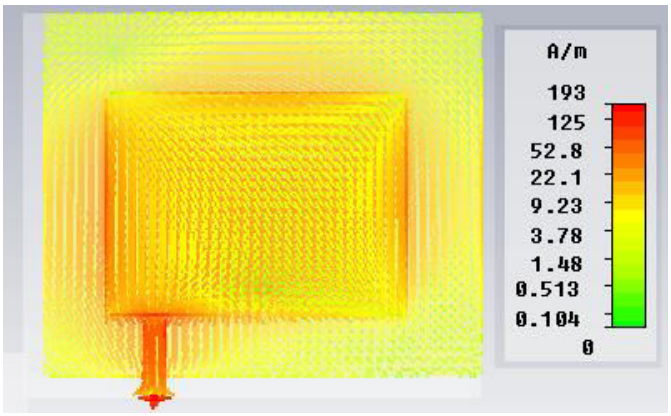
Fig.4 (a-b) shows the radiation pattern of this rectangular patch antenna at resonant frequency 5.2GHz. The antenna is representing the radiation in desired direction. The different parameters we get from radiation pattern are as follows:

- Angular width(3dB) = 94.6 Degree
- Gain(dB) = 11.5 dB
- Directivity = 6.5 dBi
- Side lobe magnitude = -13.4 dB

Fig.4 (c) is showing the current distribution of this antenna and as we can see that current distribution is maximum on the edges of rectangular patch.



(a) **(b)**



(c)

Fig.4. Simulated Results of Proposed Antenna

(a) Gain at 5.2GHz (b) Directivity at 5.2GHz (c) Current Distribution at 5.2 GHz

IV. CONCLUSIONS

In this paper a low cost compact sized microstrip patch antenna with improved bandwidth for 5.2 GHz IEEE802.11 WLAN applications is demonstrated. For designing this antenna Roger R03003 material is used. For improving the bandwidth and other parameters of antenna DGS is introduced. The designed antenna is working for the frequency band 4.9 to 5.5 GHz with resonant frequency 5.2GHz. At the resonant frequency the

return loss = -23dB, VSWR = 1.19 and gain = 11.5 dB. The simulated results are good and its simple planar geometry makes it suitable for microwave integrated circuits. In future this antenna can be converted for multiple bands so that the single antenna can be used for different wireless applications. Also this antenna can be converted to reconfigurable antenna using RF and MEMS switches.

In this field lot of research can be carried by varying the input & output parameters depending upon the the area of applications.

REFERENCES

[1]. Alireza Pourghorban Saghati, Mohammadnaghi Azarmanesh, and Reza Zaker, *Member, IEEE*, "A Novel Switchable Single- and Multifrequency Triple-Slot Antenna for 2.4-GHz Bluetooth, 3.5-GHz WiMax, and 5.8 GHz WLAN, " IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS, VOL. 9, 2010

[2]. K. Kiminami, H. Akimasa, and S. Toshiyuki, "Double-sided printed bow-tie antenna for UWB communications." *IEEE Antennas and Wireless Propagation Letters*, vol. 3, no. 1, pp. 152-153, 2004.

[3]. T. S. See and Z.N. Chen, "An electromagnetically coupled UWB plate antenna," IEEE Trans. Antennas Propag, vol. 56, no. 5, pp. 1476-1479, 2008.

[4]. M. R. I. Faruque, M. T. Islam and N. Misran, "Evaluation of specific absorption rate (SAR) reduction for PIFA antenna using metamaterials," *Frequenz*, vol. 64, no. 7-8, pp.144-149, 2010.

[5]. J. X. Xiao, M. F. Wang, and G. J. Li, "A ring monopole antenna forUWB application," *Microw. Opt. Technol. Lett.*, vol. 52, no. 1, pp. 179-182, 2010

[6]. Peshal B. Nayak, Ramu Endluri, Sudhanshu Verma and Preetam Kumar., "Compact Dual-Band Antenna for WLAN Applications" 2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications

[7]. Song, X.D.; Fu, J.M.; Wang, W., "Small CPW-fed microstrip monopole antenna for WLAN applications," *Microwave Conference, 2008. APMC 2008. Asia-Pacific* , vol., no., pp.1,4, 16-20 Dec. 2008

[8]. Y. Cao, C. Lu, and Y. Zhang, "A compact dual band miniaturized antenna forWLANoperation," *in Proc. ICMMT*, Apr. 2008, pp. 416419.

[9]. T. N. Chang and J. J. Jiang, "Meandered T-shaped monopole antenna,"*IEEE Trans. Antennas Propag.*, vol. 57, no. 12, pp. 39763978, Dec. 2009.

[10]. Q. X. Chu and L. H. Ye, "Design of compact dual-wideband antenna with assembled monopoles," *IEEE Trans. Antennas Propag.*, vol. 58, no.12, pp. 40634066, Dec. 2010.

[11]. S. H. Yeh and K. L.Wong, "Dual-band F-shaped monopole antenna for 2.4/5.2 GHz WLAN application," *in IEEE Antenna Propag. Soc. Int. Symp. Dig.*, 2002, vol. 4, pp. 7275.

[12]. T. H. Kim and D. C. Park, "CPW-fed compact monopole antenna for dual-band WLAN applications," *Electron. Lett.*, vol. 41, pp. 291293,2005.

[13]. B. S. Yildirim, "Low-profile and planar antenna suitable for WLAN/ Bluetooth and UWB applications," *IEEE Antenna Wireless Propag. Lett.*, vol. 5, pp. 438441, 2006.

[14]. M. Z. Azad and M. Ali, "A miniature implanted inverted-F antenna for GPS application," *IEEE Trans. Antennas Propag.*, vol. 57, no. 6, pp. 18541858, Jun. 2009.

[15]. M. Gallo, O. Losito, V. Dimiccoli, D. Barletta, and M. Bozzetti, "Design of an inverted F antenna by using a transmission line model," *in Proc. 5th Eur. Conf. Antennas Propag.*, 2011, pp. 635638.

[16]. D. X. Liu and B. Gaucher, "The inverted-F antenna height effects on bandwidth," *Proc. IEEE Antennas Propag. Soc. Int. Symp.*, vol. 2A, pp. 367370, 2005.

[17]. T. H. Jiang, D. L. Su, K. J. Ding, G. Y. Wang, and Y. Zhou, "Design of the low-profile inverted-F antenna with multiparasitic elements," in Proc. 7th Int. Symp. Antennas, Propag. EM Theory, 2006, pp. 14.

[18]. A. R. Razali andM. E. Bialkowski, "Coplanar inverted-F antenna with open-end ground slots for multiband operation," *IEEE Antenna Wireless Propag. Lett.*, vol. 8, pp. 10291032, 2009.

[19]. H. Y. Wang and M. Zheng, "An internal triple-band WLAN antenna,"*IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 569572, 2011.

[20]. Vinay Jhariya, Prof. Prashant Jain "Designing of Rectangular Microstrip Patch Antenna for C-Band Application" IJMER ISSN: 2249–6645 Vol. 4 Iss.10 Oct. 2014 15

NIBLACK METHOD BASED SEGMENTATION FOR MICROSCOPIC IMAGERY

Ramudu.K[1], Krishna Reddy.V.V[2], Abdul Rahim.B[3]

[1]Assistant Professor, [2]PG Scholar, [3]H.O.D & Associate Professor, Dept of ECE,
Annamacharya Institute of Technology & Sciences, Rajampeta, Kadapa, A.P, (India)

ABSTRACT

The main objective of Niblack image segmentation is to extract and characterize anatomical structures with respect to some input features or expert knowledge. In this paper, we present a sliding window based local thresholding technique 'Niblack' and given a detailed comparison of some existing thresholding algorithms with this method. The Niblack thresholding method aims at achieving better results, specifically, for microscopic images. It is a local thresholding algorithm that adapts the threshold according to the local mean and the local standard deviation over a specific window size around each pixel location. It exhibits its robustness and effectiveness when evaluated on microscopic images.

Keywords: Thresholding, Niblack, Otsu, Iterative Triclass Segmentation

I. INTRODUCTION

The gray levels of pixels belonging to the object are entirely different from the gray levels of the pixels belonging to the background, in many applications of image processing. Thresholding becomes then a simple but effective tool to separate those foreground objects from the background. We can divide the pixels in the image into two major groups, according to their gray-level. These gray levels may serve as "detectors" to distinguish between background and objects is considering as foreground in the image [1]. Select a gray-level between those two major gray-level groups, which will serve as a threshold to distinguish the two groups (objects and background). Image segmentation is performed by such as boundary detection or region dependent techniques. But the thresholding techniques are more perfect, simple and widely used [2]. Different binarization methods have been performed to evaluate for different types of data. The locally adaptive binarization method is used in gray scale images with low contrast, Varity of background intensity and presence of noise. Niblack's method was found for better thresholding in gray scale image [3].

In this work the input image is segmented using Niblack thresholding algorithm later we are applying edge detection and morphological operations to improve segmentation.

II. THRESHOLDING

Simply the basic function [5] for thresholding creates the binary image from gray level ones by turning all pixels below some threshold to zero and all pixels above that threshold to one [1],[5]. If *g(x, y)* is a threshold version of *f(x, y)* at some global threshold *T*. g is equal to 1 if *f(x, y) T* and zero otherwise [1].

$$g(x,y) = \begin{cases} 0 & if\ f(x,y) < T \\ 1 & if\ f(x,y) \geq T \end{cases}$$

Thresholding techniques can be classified generally into two categories like Global thresholding and Local thresholding. Global thresholding methods consider a single intensity threshold value. Local thresholding methods compute a threshold for each pixel in the image on the basis of the content in its neighborhood. It considers presences of all intensity level in the image. So the local thresholding methods generally perform better for low quality images [3]. We categorize the thresholding methods in groups according to the information they are exploiting. Histogram shape-based methods, this method used the peaks, valleys and curvatures of the smoothed histogram are analyzed. Clustering-based methods perform where the gray-level samples are clustered in two parts as background and foreground (object). Entropy-based methods result in algorithms that use the cross-entropy between the original and binarized image, the entropy of the foreground and background regions [3], [4]. Object attribute-based methods; search a similarity measure between the gray-level and the binarized images, such as edge coincidence, fuzzy shape similarity. The spatial methods use correlation between pixels and/or higher-order probability distribution. Local methods adapt the threshold value on each pixel to the local image characteristics [4].

III. OTSU'S THRESHOLDING METHOD

Otsu's method is used to automatically perform clustering-based image thresholding or the reduction of a gray level image to a binary image. The algorithm assumes that the image to be threshold contains two classes of pixels or bi-modal histogram (e.g. foreground and background) then calculates the optimum threshold separating those two classes so that their combined spread (intra-class variance) is minimal.

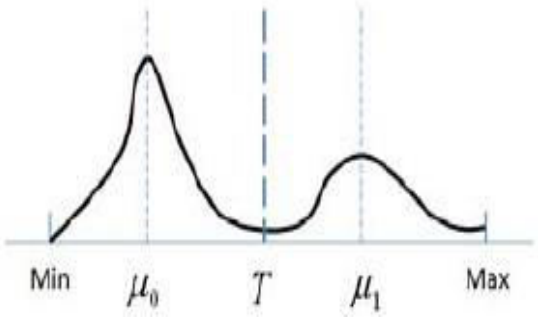


Fig 1: Otsu's Method Binarizes an Image to Two Classes Based on Threshold *T* by Minimizing the Within-Class Variances

The threshold is that which minimizes the weighted within-class variance which in turns out to be the same as maximizing the between-class variance Operates directly on the gray level histogram. Some of the Otsu's assumptions which can be defined are Histogram (and the image) is bimodal. No use of spatial coherence, or any other notion of object structure. This Assumes stationary statistics, but can be modified to be locally adaptive. One more Assumption is uniform illumination so the bimodal brightness behavior arises from object appearance differences only. The weighted within-class variance is

$$\sigma_w^2(t) = q_1(t)\sigma_1^2(t) + q_2(t)\sigma_2^2(t)$$

Where the class probabilities are estimated as:

$$q_1(t) = \sum_{i=1}^{t} P(i) \qquad q_2(t) = \sum_{i=t+1}^{I} P(i)$$

And the class means are given by:

$$\mu_1(t) = \sum_{i=1}^{t} \frac{iP(i)}{q_1(t)} \qquad \mu_2(t) = \sum_{i=t+1}^{I} \frac{iP(i)}{q_2(t)}$$

Finally, the individual class variances are:

$$\sigma_1^2(t) = \sum_{i=1}^{t} [i - \mu_1(t)]^2 \frac{P(i)}{q_1(t)}$$

$$\sigma_2^2(t) = \sum_{i=t+1}^{I} [i - \mu_2(t)]^2 \frac{P(i)}{q_2(t)}$$

All it is need to do is just run through the full range of values [1,256] and pick the value that minimizes. But the relationship between the within-class and between-class variances can be exploited to generate recursion relation that permits a much faster calculation.

Total variance is

$$\sigma^2 = \sigma_w^2(t) + q_1(t)[1 - q_1(t)][\mu_1(t) - \mu_2(t)]^2$$

The basic idea is that the total variance does not depend on threshold (obviously). For any given threshold, the total variance is the sum of the within-class variances (weighted) and the between class variance, which is the sum of weighted squared distances between the class means and the grand mean. After some algebra, we can express the total variance as since the total is constant and independent of t, the effect of changing the threshold is merely to move the contributions of the two terms back and forth. So, minimizing the within-class variance is the same as maximizing the between-class variance. The nice thing about this is that we can compute the quantities in recursively as we run through the range of t values.

IV. ITERATIVE TRICLASS METHOD

The idea of dividing an image's histogram iteratively into three classes is illustrated at the bottom of Fig. 2.

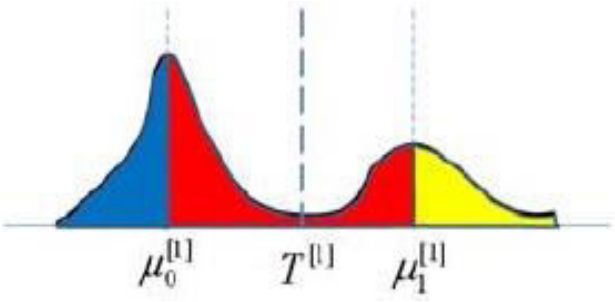


Fig 2: Iterative method we classify the histogram into three classes, namely the foreground region with pixel values greater than μ_1 (shown in yellow), the background region with pixel values less than μ_0 in blue, and the third region, called TBD, in red. The superscript denotes the number of iteration in our new algorithm.

For an image u, at the first iteration, Otsu's method is applied to find a threshold $T^{[1]}$ where the superscript denotes the number of iteration. We then find and denote the means of the two classes separated by $T^{[1]}$ as $\mu_0^{[1]}$ and $\mu_1^{[1]}$ for the background and foreground, respectively. Then we classify regions whose pixel values are greater than $\mu_1^{[1]}$ as foreground $F^{[1]}$ and regions whose pixel values are less than $\mu_0^{[1]}$ as background $B^{[1]}$. For the remaining pixels u(x, y) such that $\mu_0^{[1]} \le u(x, y) \le \mu_1^{[1]}$ we denote them as the TBD class $\Omega^{[1]}$. So our iterative process assumes that the pixels that are greater than the mean of the "tentatively" determined

foreground are the true foreground. Similarly, pixels with values less than μ_0 are for certain the background. But the pixels in the TBD class, which are the ones that typically cause miss-classifications in the standard Otsu's method, are not decided at once and will be further processed. By our definition, we have

$$U = F^{[1]} \cup B^{[1]} \cup \Omega^{[1]}$$

Where ∪ is the logical union operation. At the second iteration, we apply Otsu's method to find threshold $T^{[2]}$ on region $\Omega^{[1]}$ only. We then calculate the two class means in $\Omega^{[1]}$ separated by $T^{[2]}$ as $\mu_0^{[2]}$ and $\mu_1^{[2]}$. Similarly, the second iteration will generate a new $F^{[2]}$, $B^{[2]}$, and $\Omega^{[2]}$ such that

$$\Omega^{[1]} = F^{[2]} \cup B^{[2]} \cup \Omega^{[2]}$$

where $F^{[2]}$ is defined as the region in $\Omega^{[1]}$ with pixel values greater than $\mu_1^{[2]}$, $B^{[2]}$ as the region in $\Omega^{[1]}$ with pixel values less than $\mu_0^{[2]}$, and Ω [2] are the new TBD region. The iteration stops when the difference between two consecutive threshold $|T^{[n+1]} - T^{[n]}|$ is less than a preset threshold. At the last iteration [n +1], $\Omega^{[n+1]}$ is separated into two instead of three classes, i.e., foreground $F^{[n+1]}$ is defined as the region of $\Omega^{[n]}$ that is greater than $T^{[n+1]}$ instead of $\mu_1^{[n+1]}$ and background $B^{[n+1]}$ is defined as the regions with pixel value less than $T^{[n+1]}$.

Segmented image=$F^{[1]} \cup F^{[2]} \ldots \cup F^{[n+1]} \cup B^{[1]} \cup B^{[2]} \ldots \cup B^{[n+1]} \cup \Omega^{[1]} \cup \Omega^{[2]} \ldots \cup \Omega^{[n]}$

The method is to iteratively define the TBD regions to gain a high distance ratio, which will result in better segmentation by applying Otsu's method. But it will take more time because iterations depend on type of image.

V. LOCAL ADAPTIVE THERSHOLDING

The local thresholding method is partitioned the original image into smaller sub images and a threshold value is determined for each of the sub images [6], [3]. This yields some discontinuities in gray level due to a different gray level of two different sub images. The threshold of a region can be calculated by the point-dependent method or the region-dependent method. A smoothing technique is then applied to eliminate the discontinuities of gray level between the sub images [6]. A threshold value is calculated at each pixel, which depends on some local statistics like variance, range, or surface-fitting parameters of the pixel neighborhood [4]. The threshold value is indicated as a function *T (i, j)* and the coordinates *(i, j)* at each pixel. If this is not possible, the object / background decisions are indicated by the logical variable *B (i, j)* [4]. Niblack and Sauvola methods are used the local image property variance and standard deviation values. The neighborhood size should be small, it enough to preserve local details, but at the same time large enough to suppress noise [3].

5.1. Smoothing

The local thresholding method is partition the original image into smaller group of pixels or sub images. A threshold value is determined for each of the sub images [6].

This yields some discontinuities in gray level due to a different gray level of two different sub images [3], [9]. The threshold of a region can be calculated by the point dependent method or the region-dependent method. A smoothing technique is then applied to eliminate the discontinuities of gray level between the sub images [6].

5.2. Niblack Thresholding Algorithm

Niblack's algorithm determines a threshold value to each pixel-wise by sliding a rectangular window over the gray level image [7]. The size of the rectangle window may differ. The threshold is calculated based on the local mean m and the standard deviation S of all the pixels in the window and is given by the following derivation [7], [8].

$$T_{Niblack} = m + k * s$$

$$T_{Niblack} = m + k\sqrt{\frac{1}{NP}\sum(p_i - m)^2}$$

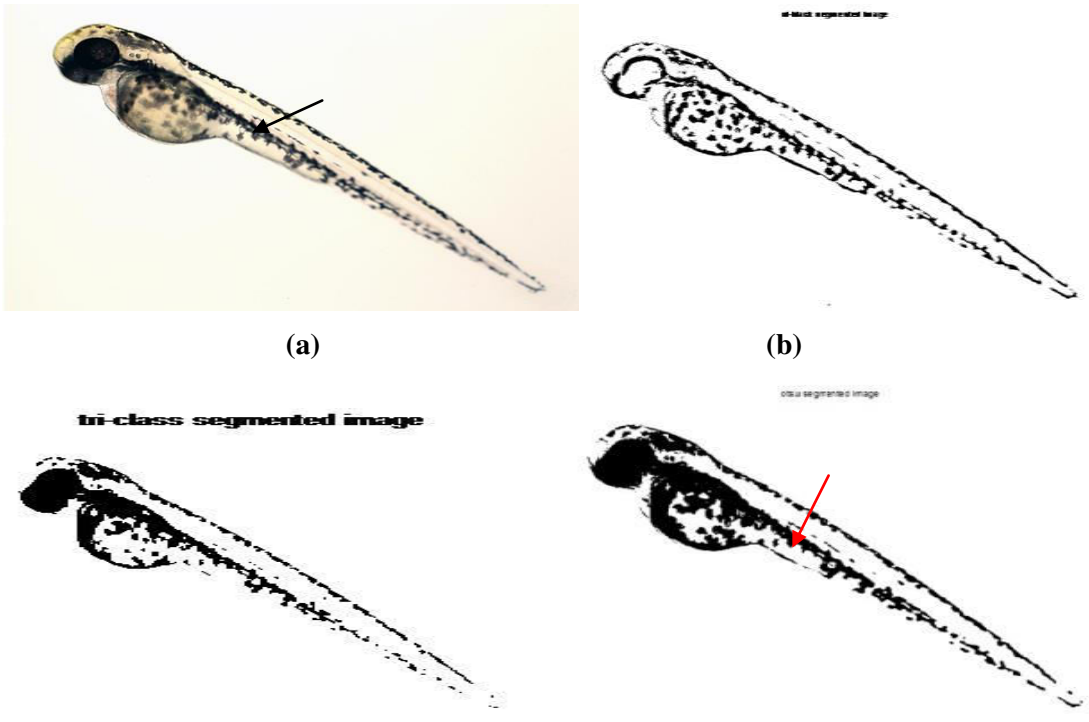
$$= m + k\sqrt{\frac{\sum p_i^2}{NP} - m^2} = m + k\sqrt{B}$$

Where NP is the total number of pixels presents in the gray image [7], [8], [9], *T* represent the threshold value, *m* is the average value of the pixels *pi*, and *k* is fixed depends upon the noise still live on the background it may be -0.1 or -0.2 [9].

VI. EXPERIMENTAL RESULTS

The improved Niblack segmentation shows better performance compared with different thresholding techniques like Otsu and iterative triclass thresholding techniques .The zebra fish embryo (fig.3) is first converted into normalized gray level values then we apply Otsu, Iterative and Niblack method.

In this we have taken two test cases, we applied the modified Niblack method on real microscopic images. For the first type of images we applied the Niblack method on *in vivo* zebra fish images acquired by a bright-field microscope. Fig. 3(a) shows a raw image of a zebra fish embryo. Because zebra fish embryos are transparent we can directly observe many anatomic structures without fixing and staining. For example the spinal cord of the embryo is visible in Fig. 3(a). The segmentation result of Otsu's method is shown in Fig. 3(b). Though the standard Otsu's method can segment the major structure of the embryo it misses detailed anatomic structure such as the spinal cord.



(a) **(b)**

(c) **(d)**

Fig. 3 Experiments on a zebra fish microscopic image. (a) A raw zebra fish embryo image acquired by a bright-field microscope. Its spinal cord is pointed by the arrow. (b) The result given by Otsu's method. (c)The result

given by the triclass iterative method (d) In the final result, the spinal cord of the zebra fish embryo, pointed by the red arrow, is fully segmented by Niblack method.

For comparison, Fig. 3(c) show the result generated by the iterative triclass method a. We can observe that some weak objects are missing. In particularly, the Niblack algorithm is able to accurately segment the spinal cord (pointed by the arrow), as shown in Fig. 3(d).

As the second example, we tested the iterative method on zebra fish images obtained in a different experiment where zebra fish embryos developed pericardial edema.

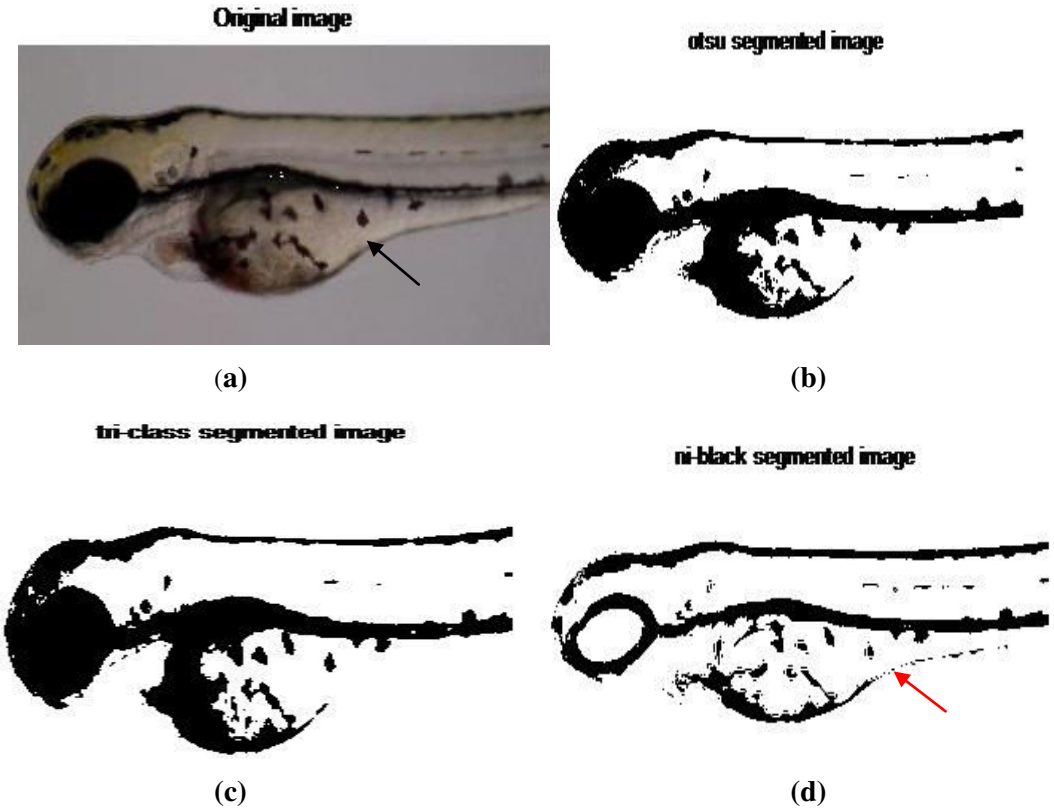


Fig. 4 (a) A test image showing a zebra fish embryo acquired by a bright field microscope. The arrow points to pericardial edema. (b) The result given by the standard Otsu's method. (c) The result given by the triclass iterative method. (d) The result of the Niblack method, which detects the spherical boundary of the pericardial edema (pointed by the arrow) while it is missed by the standard Otsu's method and iterative method.

An original image is shown in Fig. 4(a) and its standard Otsu's result and iterative triclass result is shown in Fig. 4(b) and 4(c) respectively, which does not segment the half spherical boundary of the edema. The results of applying the Niblack method are shown in Fig. 4(d). From the result we can observe that the algorithm is able to segment the half spherical boundary of the pericardial edema.

6.1 Statistical Results

Table: Comparison Between Iterative and Niblack Method

IMAGE	ITERATIVE TRICLASS METHOD			NIBLACK METHOD		
parameter	MSE	PSNR(dB)	EXECUTION TIME(Sec)	MSE	PSNR(dB)	EXECUTION TIME(Sec)
IMAGE 1	2.2680e+05	30.0347	12.315902	0.0408	62.0207	6.759054

IMAGE 2	5.8414e+04	24.1434	11.967807	2.1683	44.7697	6.475221
IMAGE 3	1.5684e+05	28.4328	13.571967	0.1232	57.2236	6.030193

VII. CONCLUSION

As Otsu's method is widely used as a pre-processing step to segment images for further processing, it is important to achieve a high accuracy. However, since Otsu's threshold is biased towards the class with a large variance, it tends to miss weak objects or fine details in images. Though the iterative method is give better result than Otsu but it is also missing some weak objects or fine structures. For example in biomedical images, nuclei and axons may be imaged with very different intensities due to uneven staining or imperfect lightening conditions, raising difficulty for algorithms like Otsu's method to successfully segment them. Without a robust segmentation results, more sophisticated processing such as tracking and feature analysis become highly challenging.

In order to overcome the limitations of Otsu and iterative triclass we used Niblack thresholding technique for segmentation later we applied edge detection and morphological operations for better segmentation. In this the threshold values are spatially varied and determined based on the local content of the target image. In comparison with global techniques, local thresholding techniques have better performance against noise and error especially when dealing with information near texts or objects. Testing results show that the Niblack method can achieve better performance in challenging cases. Though targeted here for microscopic image analysis only, it will be a good candidate for other kinds of applications as well like MRI image processing, scene processing and image segmentation.

REFERENCES

[1] Nir Milstein, "Image Segmentation by Adaptive Thresholding", Spring 1998.

[2] Sang uk lee, seok yoon chung and Rae hong park, "A Comparative Performance Study of Several Global Thresholding Techniques for Segmentation", Computer Vision Graphics And Image Processing 52, 171-190, 1990

[3] Graham Leedham, Chen Yan, Kalyan Takru, Joie Hadi Nata Tan and Li Mian, "Comparison of Some Thresholding Algorithms for Text/Background Segmentation in Difficult Document Images", Proceedings of the Seventh International Conference on Document Analysis and Recognition , 2003.

[4] Rafael C. Gonzalez, Richard E. Woods, Steven L. Eddins, "Digital Image Processing Using MATLAB", 2nd edition, Tata McGraw Hill Education Private Limited, 2010.

[5] Mehmet Sezgin and Bulent Sankur, "Survey over image thresholding techniques and quantitative performance evaluation", Journal of Electronic Imaging 13(1), 146–165, January 2004.

[6] P. K. Sahoo, S. Soltani, A. K. C. Wong and Y. C. Chbn, "A Survey of Thresholding Techniques", Computer Vision, Graphics, and Image Processing 41, 233-260, 1988.

[7] P.Subashini and N.Sridevi, "An Optimal Binarization Algorithm Based on Particle Swarm Optimization", International Journal of Soft Computing and Engineering (IJSCE),Volume-1, Issue-4, September 2011.

[8] Naveed Bin Rais , M. Shehzad Hanif and rmtiaz A. Taj, "Adaptive Thresholding Technique for Document Image Analysis", International Multi-Topic Conference IEEE, 61 – 66, Dec. 2004.

[9] Er.Nirpjeet kaur and Er Rajpreet kaur, "A review on various methods of image thresholding", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 3441-3443, 10 October 2011.

ANALYSIS OF SHADING INFLUENCE ON MODELING OF STANDALONE PV ARRAY SYSTEM FOR OPTIMAL POWER OUTPUT

L Navinkumar Rao[1], S Gairola[2]

[1]*Assistant Professor, Dept. of Electrical Engg, I.T.S. Engineering College, Greater Noida, (India)*

[2]*Professor, Dept. of Electrical Engg, Noida Institute of Engineering and Technology, Greater Noida, (India)*

ABSTRACT

A photovoltaic power system exhibits non linear characteristics and the maximum power point tracking (MPPT) operation is essential for best performance. The P-V array characteristics for partial shading condition (when some panels are under shadow) show multiple maxima points and normal operation fails to locate global maximum power point. In this paper, shading effect on PV array system of low rating is investigated and its characteristics under different shading conditions are studied. A small PV system consisting of nine 50 W PV modules connected in series and parallel configurations, is investigated for different shading conditions. The analysis is carried out for PV panel connection reconfiguration to increase power output. A new model is also proposed for the PV modules during partial shading and the results are validated by simulations using Matlab/Simulink software platform.

Index Terms: Photovoltaic (PV) Module, Global Maximum Power Point (GMPP), Partial Shading, Standard Test Condition (STC), Sine Model

I. INTRODUCTION

The demand for electrical energy is globally increasing day by day and the use of renewable energy is the only alternative to meet this demand as the fossil fuel stock on earth is limited. Considering the environmental and technical constraints, the solar energy is becoming popular due to its advantages like absence of moving parts, ease of control and no air and noise-pollution. The major drawback with solar power generation is that it is available only during day time, however, there are applications like farming (water pumping, winnowing, etc), office work, certain industries which may require power only during day time. Moreover, PV generated power can also be fed to the grid and each watt of power fed helps in meeting the demand.

A PV generation system generally consists of solar panel connected to load through a DC-DC converter that may be buck, boost or buck-boost type. Such an arrangement with Boost DC-DC converter is shown in Fig. 1 to be employed in this paper. In PV generation systems, generally a large number of PV modules are connected in series and parallel combinations and obviously PV generation gets affected by shading phenomenon. This shading may be there due to change in earth's inclination with seasons and presence of tall structures close to the PV modules. If a PV panel in a array is shaded, then the panel will be damaged due to formation of hot spots and the effect is avoided by connecting bypass diodes in parallel with the PV modules which prevent reverse

current flow through shaded panel. In PV generation system, the insolation is not uniform throughout the day, moreover, some panels may be under shadow during the day time because of obstruction from long trees, tall buildings, cloudy conditions, poles, etc. present near the panel layout. This shading causes a mismatch in generation of modules output in each string and affects the overall efficiency of PV generation. The loss in generation due to shading can be found to be proportional to shaded area and location of PV module in a given array. A single PV panel has low voltage and current rating and its single diode model is shown in Fig. 2 for 50W ratings. Its I-V and P-V characteristics are shown in Fig. 3 under standard test conditions (STC) that depicts its non linear behavior. The modeling and parameter identification for PV systems is described by various researchers [1-2]

J.S. Ramos et.al. [3] has shown that at well depth of 100 m the pumping of water cost about 1.07 €/m^3 where the required pump power is of 154 W and a solar array of 195 W-peak (W_p) is used. When a 720 W-p PV array is connected to a permanent magnet DC (PMDC) motor coupled with centrifugal pump at 5-8 m water head 20 to 840 lit/min can be drawn depending on the solar intensity. This means 38000 l volume of water can be pumped for the water head of 5 m with 9 hours of operation [4]. Several types of pumps and motors are available in the markets which are based on the PV pumping technology. If such PV based water pumping is used in villages or fields, the shading influence shall hamper the performance and therefore the investigation becomes important.

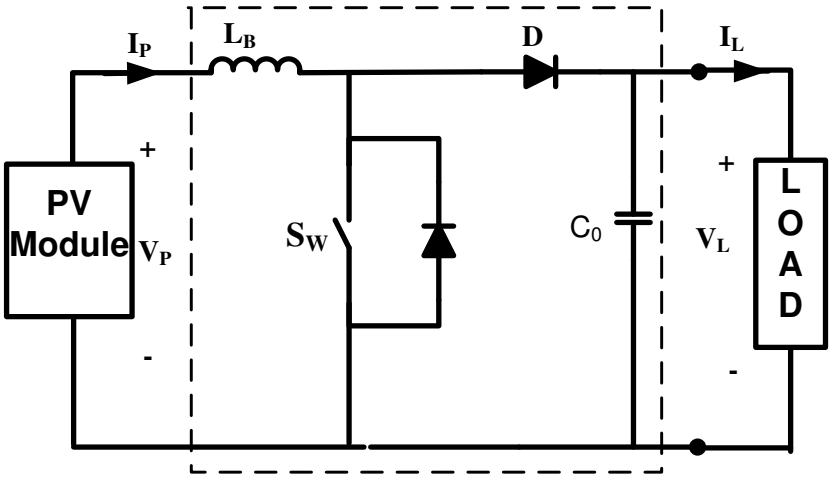


Fig.1 Circuit Diagram of Boost Converter for Effective Load Matching

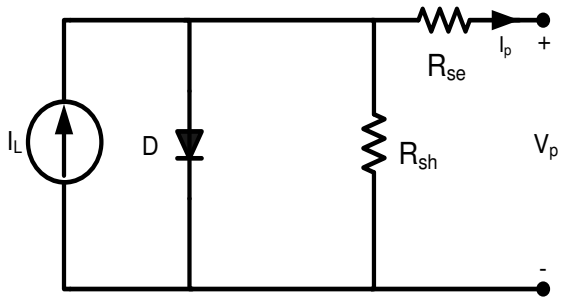


Fig.2 Single Diode Equivalent Circuit of PV Panel Representing Model Parameters

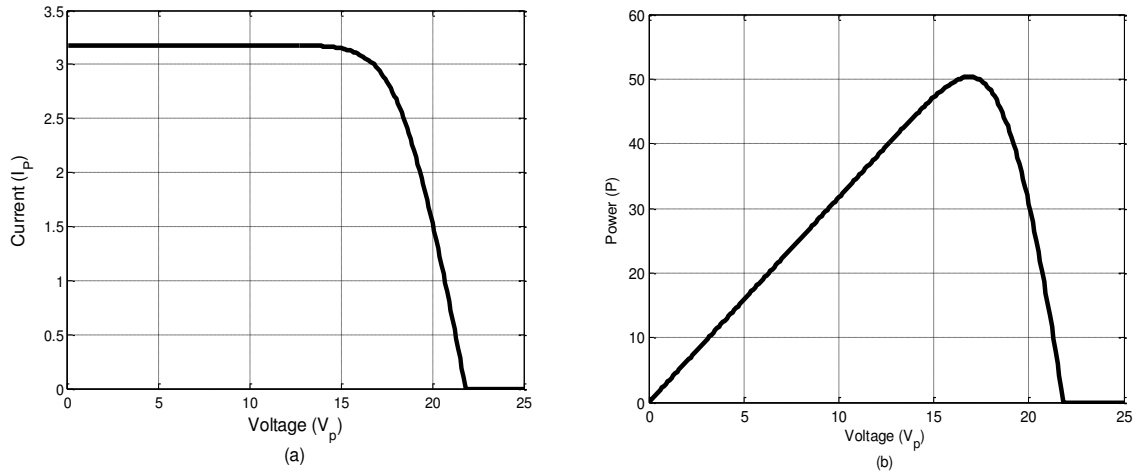


Fig. 3 I-V and P-V Characteristics of a 50W Solar Panel at Insolation of 1000W/m^2 at 25^{0}C

During Standard test conditions (STC), normally all the panels in PV array are subjected to same temperature and insolation and P-V characteristics has only one peak as shown in Fig. 3 (b). However, it is reported in literature [5-8] that the PV system shows multiple peaks in PV characteristics under partial shading conditions. The presence of multiple maxima points makes it difficult to operate PV system at Global Maximum Power Point (GMPP). The controller should be accordingly designed otherwise operating point may work stably on local maximum power point rather than GMPP. Some techniques and algorithms for tracking global maxima have been given by [6] and [7], however, in the presence of shading influence the controllers also need improvement. Patel. H et.al. [9]-[10] has given the various shading pattern for non uniform insolation and proposes the method for tracking the global peak under partial shaded conditions. It is observed that none of researchers have given representation of these PV characteristics that shall facilitate the investigation of such system under shading. This paper investigates the shading effect in a small PV system comprising of nine PV modules connected in an 3×3 array as shown in Fig. 4. The detailed characteristics, analysis and representation are presented here in a novel way that shall be highly beneficial for flexible controller development including shading conditions.

Table I. BP-PV Panel Specifications

S. No.	Electrical Characteristics of Panel	BP-350
1	Maximum power point (P_{max})	50 W
2	Voltage at P_{max} (V_{mp})	17.3 V
3	Current at P_{max} (I_{mp})	2.89 A
4	Short circuit current I_{sc}	3.17 A
5	Open circuit voltage V_{oc}	21.8 V

II. SYSTEM MODELLING

2.1 Model of PV Cell

A PV array consists of number of PV panel connected in series and parallel. The 50 W PV panel BP350, also described in [1], is used for PV array and analysis purpose. A PV panel is modeled as a current source

connected in parallel with diode with shunt and series resistance and the current equation that governs panel voltage and current [1-2] is given by

$$I = I_L - I_0\left(e^{\frac{V+IR_{se}}{b}} - 1\right) - \frac{V + IR_{se}}{R_{sh}} \qquad (1)$$

where $b = \dfrac{N_s \gamma KT}{q}$ (2)

I_L is light generated current,

D is diode

q is electron charge 1.6×10^{-19} C

K is Boltzmann's constant. 1.38×10^{-23} J/K

γ is the photovoltaic single cell ideal factor (value for which varies within 1-2).

N_S is the number of cells in series

T is the PV panel temperature in K.

I_0 is diode reverse saturation current

R_{se} and R_{sh} are the resistance shown in Fig. 2

The electrical power output delivered by a photovoltaic panel depends upon solar insolation, cell temperature, sun's incidence angle and load resistance. The PV module manufacturer typically provides operational data for photovoltaic panels at STC. The data provided is the open circuit voltage (Voc), the short circuit current (I_{sc}), the maximum power point voltage (V_{mpp}) and maximum power point current (I_{mpp}), the temperature drift coefficients at open circuit voltage and short circuit current. The specification for the 50 W PV panel employed is given in Table I [1]. It is worth mentioning here that Eqn. (1) is a mixed equation that is difficult to solve moreover, it is for STC and not for partial shading. It can be solved only with iterative methods by making certain assumptions.

2.2 Series and Parallel Configuration of PV array

A 3×3 PV array (450 W) is formed by connecting PV panels in series and parallel arrangement for investigation, as shown in Fig 4 (CASE-1). In this arrangement, three strings are connected in parallel and each string consists of three PV panels connected in series. Each panel has characteristics as given in Fig. 3. The 3x3 array of these panels has P-V characteristics given in Fig. 4(b) for STC. However during partial shading condition, multiple peak points are formed in P-V characteristics as shown in Fig. 5(a)-5(e) for some cases (CASE 2-6). Therefore, for best utilization of PV system, it is necessary to operate PV generator at global maximum power point and whole of generated power may be fed to the power grid or loads where varying power can be supplied. This matching of load to PV source is possible by employing the intermediate DC-DC converter, which continuously controls the voltage and current levels thereby moving the operating point as described by some researchers [6-8].

The investigation for analysis of partial shading influence on PV system is carried out under non-uniform insolation (at 1000 W/m^2 and 500 W/m^2) and standard operating temperature (25^{0}C) and kept under following six cases:

CASE 1: All nine panels are working under normal insolation condition, without any shading as shown in Fig. 4(a). The P-V characteristics obtained for this case is also shown at 100 % insolation level (1000 W/m^2)

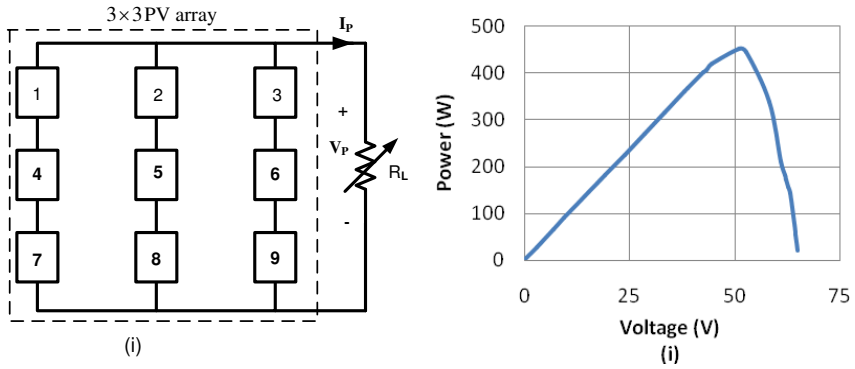


Fig. 4 3×3 PV Array Configuration Having Nine Panels Connected in Series-Parallel Arrangement. (CASE 1 All Panels are Receiving Insolation of 1000 W/m^2 at 25° C)

CASE 2: A single panel (No. 7) in the corner of 3×3 PV array is shaded due to obstruction while other 8 panels are working under normal insolation condition. The P-V characteristics obtained is as shown in Fig. 5(a). The characteristic shows two peak power points.

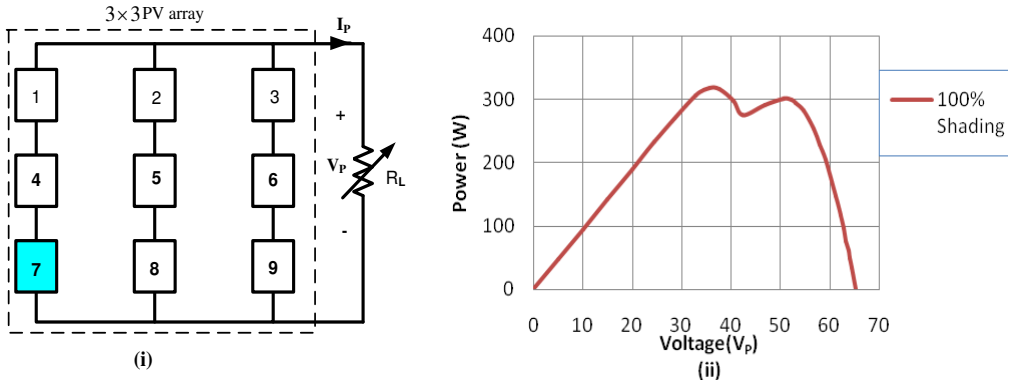


Fig. 5 (A) A 3×3 PV Array Configuration Having Nine Panels Connected In Series-Parallel Arrangement With One Panel Shaded (CASE 2). PV Characteristic Is Shown For 100% Shading On Panel 7.

CASE 3: When two panels (No. 7 and 8) in a corner of the 3×3 array are shaded while other seven panels are working under normal insolation condition as shown in Fig. 5(b). The characteristic shows two peak power points.

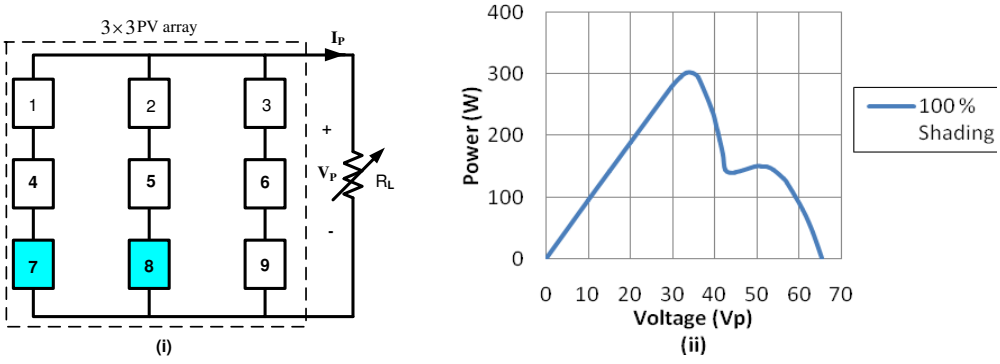


Fig. 5 (B) A 3×3 PV Array Configuration Having Nine Panels Connected in Series-Parallel Arrangement with Two Panels Shaded (CASE 3). PV Characteristic is Shown for 100%, Shading on Panel 7 & 8.

CASE 4: When two panels (No. 4 and 7) in a corner of the 3×3 array are shaded while other seven panels are working under normal insolation condition as shown in Fig. 5(c). The characteristic shows multiple peak points.

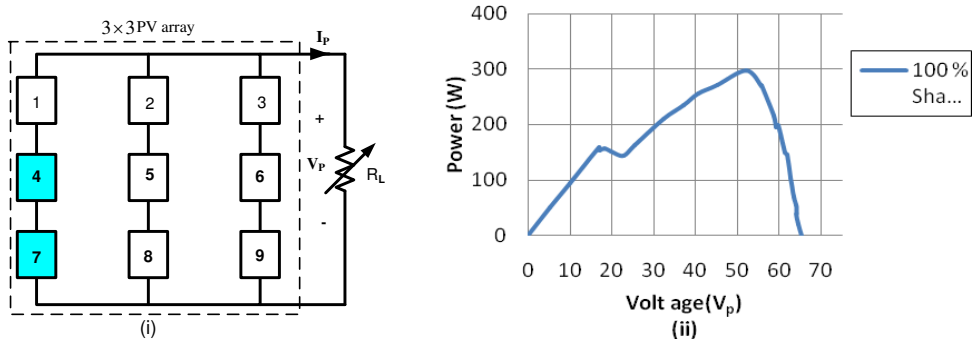


Fig. 5 (C) A 3×3 PV Array Showing Configurations Having Nine Panels Connected In Series-Parallel Arrangement with Two Panels in Series are Shaded (CASE-4). PV Characteristic is Shown for 100% Shading On Panel 4 & 7.

CASE 5: The three panels (No. 4, 7 and 8) in a corner of the 3×3 array are shaded (two from first string and one from second string) due to obstruction, while other 6 panels are working under normal insolations as shown in Fig. 5(d). The characteristic shows three peak points.

CASE 6: The three panels numbered as 4, 7 and 8 of an 3×3 array are shaded due to obstruction are reconfigured (one from each string) and other 6 panels are working under normal insolations condition as shown in Fig. 5(e). A four pole double throw (FPDT) switch is employed (Fig 5(e)) for reconfiguration of PV panels. The characteristics shows single peak point and output power is more than that obtained from case 5 when insolation on shaded PV panels is zero. The characteristics obtained for case 2 to 6 cannot be represented simply by exponential equation like Eqn. (1) and needs the mathematical expression for analysis and control. The representation is detailed in following section.

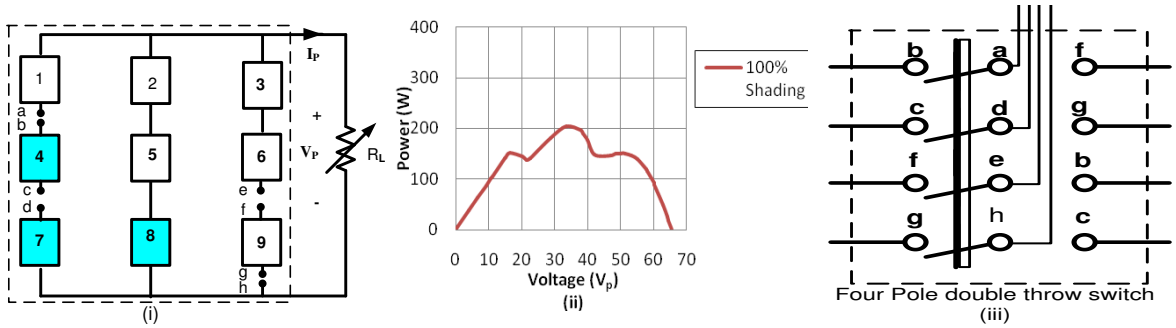


Fig. 5 (D) 3×3 PV Array Showing Configuration Having Nine Panels Connected in Series-Parallel Arrangement with Three Panels (Panel 4, 7 & 8) Shaded (CASE 5). the PV Characteristic is Shown for 100% Shading on Panel 4, 7 & 8.

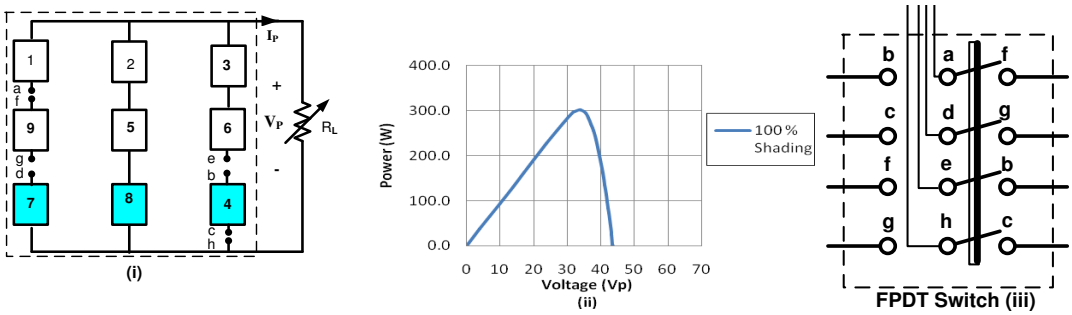


Fig. 5 (E) 3×3 PV Array Showing Configuration Having Nine Panels Connected in Series-Parallel Arrangement with Three Panels (Panel 7, 8 & 4) Shaded (Reconfigured) (CASE 6). The PV Characteristic is Shown for This Case For 100%, Shading on Three Panels.

Table II Design Parameters of Boost Converter

S. No.	Input voltage	V_i	10-70 V
1	Output voltage	V_o	10-150 [V]
2	Switching frequency	f_S	10 [kHz]
3	Main inductor	L_B	10 [m H]
4	Output capacitor	C_0	470 [μ F]
5	Input capacitor	C_i	50 [μ F]
6	Power	P	450 W

III. PROPOSED MODEL

For panels with or without partial shading of photovoltaic system as shown in CASES 1-6, the relationship between P and V is proposed have as follows:

$$P=\left\{\begin{matrix} a_1\sin\left(b_1V+c_1\right)+a_2\sin\left(b_2V+c_2\right)+a_3\sin\left(b_3V+c_3\right) \\ +a_4\sin\left(b_4V+c_4\right)+a_5\sin\left(b_5V+c_5\right)+a_6\sin\left(b_6V+c_6\right) \end{matrix}\right\}\left\{u\left(V\right)-u\left(V-V_{\max}\right)\right\} \quad (3)$$

Where

V is the panel output voltage of 3x3 PV array;

P is the power output of 3x3 PV array;

V_{max} is the maximum possible voltage generated by PV system.

a_1, a_2, a_3, a_4, a_5 and a_6 are constants having dimensions of power.

b_1, b_2, b_3, b_4, b_5 and b_6 are constants having dimensions of radians/volt

c_1, c_2, c_3, c_4, c_5 and c_6 are constants having dimensions of radian.

This representation is called sine model for PV array in this paper and it is suitable for PV system with or without shading provided the coefficients a_x, b_x and c_x are correctly known. The power P, the voltage V and current I are directly related, therefore a similar equation between I and V can also be written and may represent its model. This form of equation has advantage over Eqn. 1 which is mixed equation and difficult to solve. The

sine model shall also reduce the solving time for iterative control algorithms such as PSO technique used by some researchers [8].

IV. SIMULATION OF A PV ARRAY

Using MATLAB/Simulink software the PV array system is simulated. Fig. 6 shows the schematic diagram of complete system, while Fig. 7(a) represents the simulation of complete PV system along with boost converter connected to load. Fig 7(b) shows the schematic diagram of subsystem for simulation of BP-350 photovoltaic panel which employs parameters like series resistance, shunt resistance and reverse saturation current obtained from [1]. Fig.7 (c) shows the schematic diagram of subsystem for simulation of boost converter which employs parameters obtained from Table II. DC-DC boost converter act as interface between PV generating system and load.

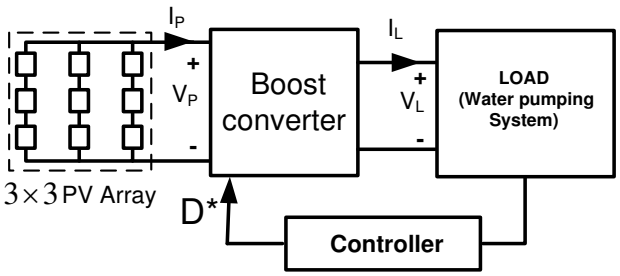


Fig. 6 Block Diagram Showing PV Array Connected to Load Through Boost Converter

The operating point of PV array at different load conditions is controlled by DC-DC converter. By varying the duty ratio of the converter, the load matching is obtained. Fig. 3 shows the circuit of boost converter used for changing operating point on P-V characteristics. TABLE II shows the design specifications of boost converter and parameters which are employed for simulation. The output voltage of boost converter is function of duty ratio of switching signal. The output voltage of boost converter is given by equation

$$V_{op} = \frac{1}{1-D} V_{ip} \qquad (4)$$

Where

D is duty ratio.

V_{ip} is input voltage for converter

V_{op} is output voltage for converter

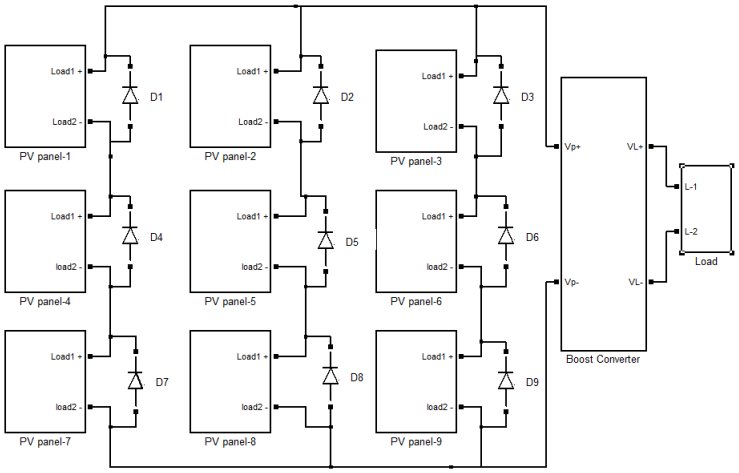


Fig. 7(A) Simulation Model of 3×3 PV Array Connected in Series Parallel Arrangement and Connected to Load Through Boost Converter

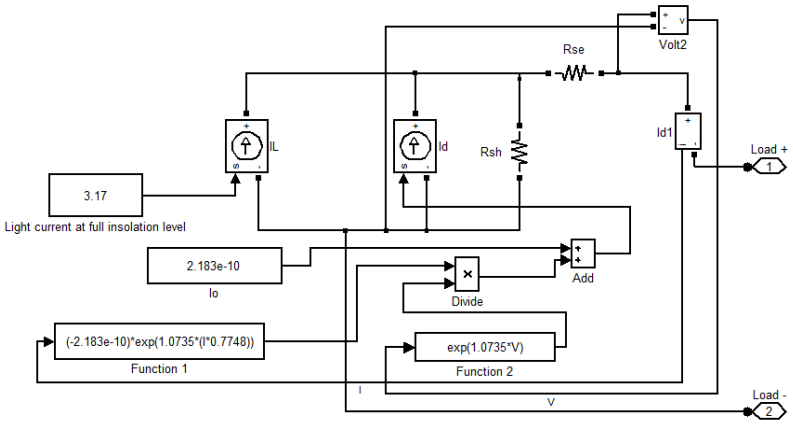


Fig. 7(B) Simulation Model of One PV Panel Fed From Constant Insolation

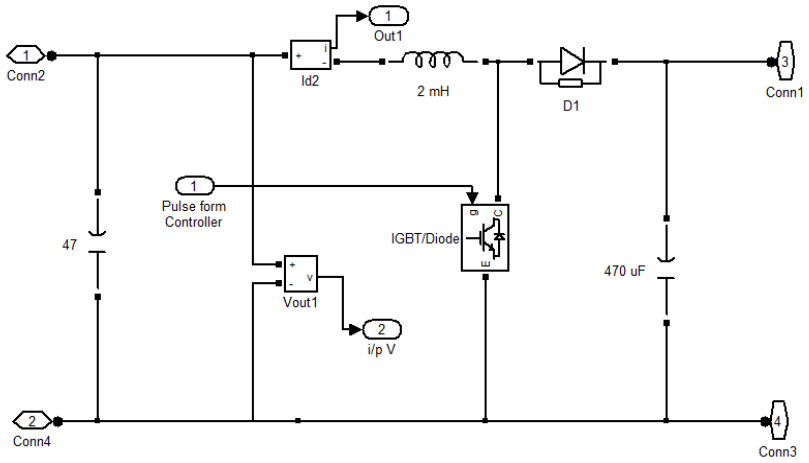


Fig. 7(C) Simulation Model of Boost Converter Employed in The PV Based System

4.1 Simulation of Proposed Model

From the values of constants shown in Table V, Eqn. 3 is employed as proposed sine model for the shading condition of CASE V. This model of 3×3 PV array connected in series parallel arrangement during shaded condition is connected to load through boost converter. Fig. 8(a) shows the schematic diagram for simulation of

proposed model of 3×3 PV array connected in series parallel arrangement when three panels are shaded (CASE V). Fig. 8(b) shows the schematic diagram of subsystem for simulation of Eqn. 3 employing parameter from Table V (a). The proposed model is simulated and P-V curve is plotted as shown in Fig. 9 and compared with PV curve obtained from actual model.

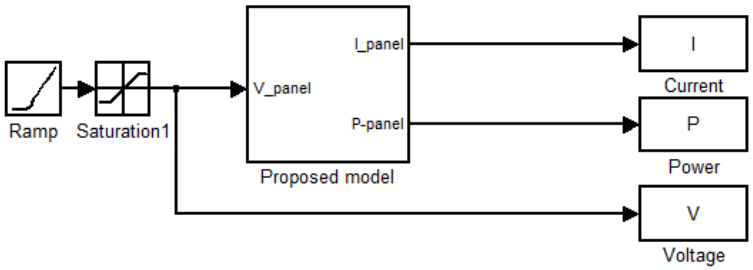


Fig. 8(A) Simulation of Proposed Model of 3×3 PV Array Connected in Series Parallel Arrangement When Three Panels are Shaded

V. RESULTS AND DISCUSSION

Fig. 3 has shown the I-V and P-V characteristics of 50 W single PV panel given by manufacturer for constant temperature 25^0C and constant insolation 1000 W/m^2 operation. The electrical characteristics is non linear as given by Eqn. 1. Fig. 4 shows the 3×3 PV panel array connected in series-parallel arrangement. The PV array is subjected to 100% shading condition and its characteristics is explained by considering different cases as shown in Fig 5(a) to Fig. 5(e). The P-V curves shows that the multiple peak points are formed for different shading cases and it becomes more complex to control the operating point. The MPPT techniques fail to track GMPP with normal perturbation and observation method. The operating point may become stable at local MPP which shall reduce the overall efficiency of PV system. To resolve the said problem, the sine model is proposed as shown in Eqn. 3, for predicting the GMPP. The parameters of proposed model and the observed root mean square error (RMSE) for each shading case in comparison with detailed simulation are shown in Table IV (a) and IV (b).

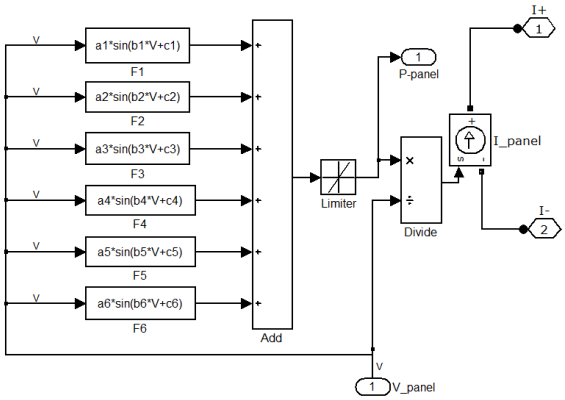


Fig. 8 (B) Simulation of Proposed Model of 3×3 PV Array (CASE 5) Employing Eqn. 3 and Constant Parameters From Table V (A)

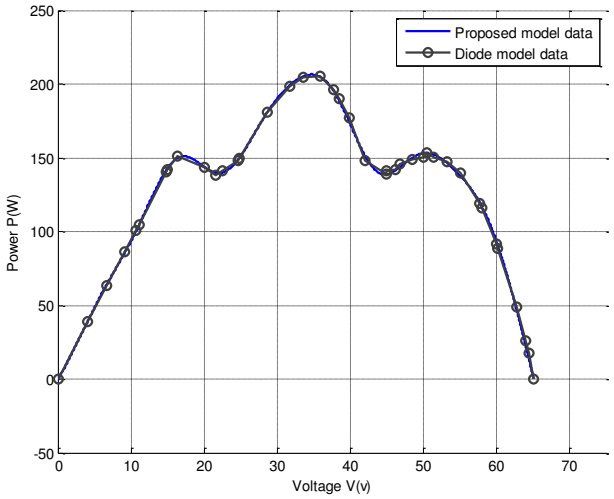


Fig. 9 The P-V Characteristic Obtained From Single Diode Model and Proposed Model for The Case When Three Panels are Shaded as Shown in Fig. 5(D)

Table III. Table Showing Values Of Voltage, Current And Power At Different Load Conditions for PV Array with Different-Panels 100% Shaded.

No Shading (CASE 1)			1-Panel Shaded (CASE 2)			2-Panels Shaded (CASE 3)			2-Panels Shaded (CASE 4)			3-Panels Shaded (CASE 5)			3-Panels Shaded(CASE-6)		
V_P	I_P	P	V_P	I_P	P	V_P	I_P	P	V_P	I_P	P	V_P	I_P	P	V_P	I_P	P
0	9.51	0	0	9.506	0	0	9.51	0	0	9.5	0	0	9.51	0	0	9.51	0
3	9.51	28.53	5	9.506	47.53	10	9.51	95.1	5.23	9.51	49.737	4.009	9.62	38.55	4	9.51	38
7	9.51	66.57	10	9.506	95.06	15	9.51	142.65	10	9.45	94.5	6.683	9.51	63.55	7	9.51	66.6
9.51	9.51	90.44	15	9.506	142.59	20	9.51	190.2	16.82	9.45	158.94	9.161	9.424	86.33	10	9.51	95.1
19.02	9.51	180.88	20	9.506	190.12	29.64	9.435	279.65	17.01	9.007	153.2	10.68	9.401	100.4	13.76	9.51	130.9
23.75	9.501	225.64	24.52	9.506	233.08	31.78	9.29	295.23	18.2	8.572	156.01	14.85	9.453	140.37	17.13	9.51	162.9
28.52	9.507	271.13	32.89	9.312	306.27	33.2	9.087	301.68	19.93	7.582	151.1	16.34	9.263	151.35	17.16	9.499	163
33.28	9.508	316.42	35.75	8.894	317.96	34.78	8.663	301.29	22.73	6.35	144.33	20.07	7.167	143.84	23.84	9.507	226.6
38.02	9.502	361.26	37.75	8.36	315.59	36	8.17	294.12	25.42	6.4	162.68	21.6	6.386	137.93	29.35	9.447	277.3
38.84	9.474	367.97	40.5	7.341	297.31	39.24	6.19	242.89	32.44	6.492	210.6	22.48	6.28	141.17	31.8	9.284	295.2
42.5	9.444	401.37	42.44	6.48	275.01	40.31	5.348	215.57	37.19	6.323	235.15	28.66	6.319	181.1	32.11	9.247	296.9
43.26	9.408	406.99	46.85	6.215	291.17	41.07	4.712	193.52	40.56	6.34	257.15	33.63	6.072	204.2	34.05	8.846	301.2
44.45	9.432	419.25	50.76	5.935	301.26	41.82	4.049	169.32	45	6	270	37.73	5.199	196.15	35.41	8.322	294.7
50.86	8.878	451.53	53.11	5.549	294.7	42.52	3.411	145.03	52.04	5.715	297.4	39.85	4.44	176.93	36.39	7.782	283.2
52.72	8.426	444.21	54.68	5.163	282.31	44.91	3.142	141.1	55.67	4.842	269.55	42	3.519	147.79	37.17	7.252	269.6
58.23	5.823	339.07	56.74	4.486	254.53	49.25	3.046	150.01	58.7	3.669	215.37	48.43	3.079	149.11	38.54	6.092	234.8
60.83	3.464	210.71	58.1	3.936	228.68	50.87	2.963	150.72	59.3	3.302	195.8	50.07	3.011	150.76	40.53	3.981	161.3
62.02	2.928	181.59	59.17	3.455	204.43	52.32	2.853	149.26	59.6	3.33	198.46	51.44	2.927	150.56	41.12	3.27	134.5
62.14	2.767	171.94	61.24	2.417	148.01	53.78	2.695	144.93	61.74	2.366	146.07	55.06	2.532	139.41	41.88	2.31	96.7
62.58	2.519	157.63	62.2	1.892	117.68	56.25	2.331	131.11	62.72	1.662	104.24	57.74	2.058	118.82	42.14	1.979	83.4
63.07	2.273	143.35	62.82	1.541	96.8	57.08	2.177	124.26	63.3	1.1	69.63	58.01	1.994	115.67	42.34	1.714	72.6
64.4	0.918	59.11	63.38	1.214	76.94	60.84	1.315	80	64.03	0.8373	53.61	60.21	1.476	88.86	43.11	0.67	28.94
64.46	0.8595	55.4	63.81	0.9621	61.39	63.11	0.6864	43.31	64.08	0.6	38.44	62.79	0.7791	48.91	43.19	0.55	23.97
65.04	0.3252	21.15	64.54	0.5247	33.86	65.3	0.035	2.28	64.5	0.3	19.35	64.081	0.4026	25.79	43.55	0.05	2.3
65.32	0.06532	4.26	65.4	0	0	65.35	0	0	65.2	0	0	64.51	0.2757	17.78	43.56	0	0

Table IV (A) Sine Model Parameters for P-V Characteristics for Different Cases (1-6)

Sine model parameters	CASES					
	CASE 1	CASE 2	CASE 3	CASE 4	CASE 5	CASE 6
a_1	442.5	316.8	254.1	257.5	360.7	340
b_1	0.057	0.045	0.0501	0.046	0.064	0.094
c_1	-0.408	-0.152	-0.079	-0.157	0.011	-0.515
a_2	529.6	43.46	37.38	74.23	448.9	1027
b_2	0.142	0.219	0.195	0.179	0.096	0.192
c_2	-2.058	4.786	2.093	-2.779	2.891	1.338
a_3	3.393	-1295	24.47	54.53	277.9	886
b_3	0.427	0.305	0.305	0.294	0.115	0.199
c_3	-1.85	-0.564	-2.701	-3.023	5.751	-1.918
a_4	669.9	1252	14.57	35.44	29.78	1.704
b_4	0.132	0.305	0.49	0.306	0.201	0.888
c_4	1.3	5.7	-3.731	-0.392	0.683	-5.85
a_5	0	105.4	7.619	1.995	15.53	0
b_5	0	0.251	0.722	0.454	0.343	0
c_5	0	0.742	-1.169	-0.435	8.717	0
a_6	0	3.172	5.379	111	3.946	0
b_6	0	0.664	0.993	0.145	0.586	0
c_6	0	-0.123	-6.845	1.012	-0.196	0
RMSE	8.007	17.3	3.163	10.53	4.03	1.293

Table IV (B) Sine Model Parameters for I-V Characteristics for Different Cases

Sine model parameters	CASES					
	CASE 1	CASE 2	CASE 3	CASE 4	CASE 5	CASE 6
a_1	16	11.79	7.418	8.996	9.752	15.67
b_1	0.0482	0.04209	0.029	0.027	0.032	0.071
c_1	0.411	0.6053	0.787	1.26	1.284	0.457
a_2	0.433	2.46	3.351	1.051	2.051	0.535
b_2	0.183	0.089	0.061	0.137	0.084	0.262
c_2	3.424	2.296	0.919	7.086	2.459	3.701
a_3	6.887	0.278	1.059)	0.521	0.875	0.0822
b_3	0.0845	0.343	0.216	0.081	0.287	0.545
c_3	2.676	-4.034	1.164	2.851	-3.361	1.956
a_4	0.542	0.137	0.478	0.341	0.627	0.0615
b_4	0.394	0.501	0.35	0.478	0.304	0.607
c_4	1.074	-4.291	-4.374	0.219	4.703	4.053
a_5	0.5143	0.669	0.201	34.43	0.192	6.667
b_5	0.405	0.209	0.498	0.734	0.539	0.128
c_5	3.92	1.676	-4.074	1.775	-0.858	2.7
a_6	0	0.074	0	0.476	0.093	0.0021
b_6	0	0.709	0	0.293	0.626	1.329
c_6	0	5.472	0	-2.526	-2.262	7.303
RMSE	0.1396	0.03754	0.1549	0.1699	0.08378	0.01165

t is observed from the obtained characteristics that the total maximum power output with shading is less than the actual power capacity of PV array. This difference of power is because of shading loss. This shading loss is also proportional to the position of shaded panel in an array. Fig. 5(e) shows that by changing switch position of FPDT switch from *b-f-c-g* to *f-g-b-c*, the position of shaded PV panels is changed and the PV characteristics shows only single peak. This reconfiguration of panels makes it suitable for MPPT with P &O method.

VI. CONCLUSIONS

This paper has discussed the performance of a 3×3 PV array at different shading conditions. It has considered the six different cases (I to VI) of shading of a 3×3 PV array and the P-V characteristics are plotted at for these shading conditions. The shading loss due to shading effect can be easily determined. Considering the case V (shown in Fig 5(d)), it is revealed that the power output of PV array can be improved by reconfiguration of PV panels connection, as shown in Fig 5(e). The paper has also proposed the model given by Eqn. 3. When different panels are shaded the characteristic is compared from model and detailed simulation of PV array system. The simulation result is shown in Fig. 9 which indicates that the proposed model PV characteristic is matching with the diode model based PV array for shading condition in case 5. The same is also validated for all cases and RMSE is obtained. Hence proposed model can be used to predict the position of local and global peak power points for maximum power point operation thereby simplifying the control algorithm in real time.

REFERENCES

[1] L. N. Rao and S. Gairola, "Modeling and Constant Power Operation of Photovoltaic (PV) Panel Employing PSO," International Conference on Electrical, Electronics, Signals, Communication and Optimization EESCO, Jan. 24th & 25th 2015. Visakhapatnam, India, paper no OR203

[2] D. Dondi, D Brunelli, L. Benini, P. Pavan and L. Larcher, " Photovoltaic cell modeling for solar energy powered sensor networks," IWASI, International workshop on Advances on sensors and interface. 2007. 26th -27th June, 2007, Bari, Italy.

[3] J.S. Ramos, H. M Ramos, " Solar powered pumps to supply water for rular or isolated zones: A case study," ELSEVIER, Science direct Energy for sustainable Development 13, pp. 151-158, 2009.

[4] M. Kolhe, J.C. Joshi and D.P. Kothari, " Performance analysis of a directly coupled photovoltaic water pumping system," IEEE Transactions on energy conversion vol. 19, no.3, pp. 613-618, Sep 2004

[5] M. A. S. Masoum, H. Dehbonei, and E. F. Fuchs, "Theoretical and experimental analyses of photovoltaic systems with voltage and current-based maximum power-point tracking," IEEE Trans. Energy Conversion., vol. 17, no. 4, pp. 514–522, Dec. 2002.

[6] L. Gao, R.A. Dougal, S. Liu and A. P. Iotova, "Parallel-connected solar PV system to address partial and rapidly fluctuating shadow conditions," IEEE Trans. Industrial electronics., vol. 56, no. 5, pp. 1548–1556, May. 2009.

[7] W. Xiao, N. Ozog and W. G. Dunford "Topology study of Photovoltaic interface for maximum power point tracking" IEEE Transactions on Industrial Electronics, vol. 54, no. 3, pp. 1696–1703. Jun. 2007.

[8] M. Abdulkadir, A. H. M. Yatim, and S T. Yusuf, "An improved PSO-Based MPPT control strategy for photovoltaic systems," International journal of photoenergy Hindawi Publishing Corporation, vol. 2014. http://dx.doi.org/10.1155/2014/818232

[9] Patel. H and Agarwal V. "MATLAB-Based Modeling to Study the Effects of Partial Shading on PV Array Characteristics," IEEE Transactions on Energy Conversion, vol. 23, no.1, pp.302-310, March 2008

[10] Patel. H and Agarwal. V. "Maximum Power Point Tracking Scheme for PV Systems Operating Under Partially Shaded Conditions,", IEEE Transactions on Industrial Electronics, vol. 55, no.4, pp.1689-1698, April 2008

AN EFFİCİENT APPROACH USİNG DİFFİE - HELLMAN KEY EXCHANGE TO PROTECT CLOUD FROM INTERNET ATTACKS

Lokashree S[1], Lokana S[2]

[1,2]*PG Student, Rajeev Institute of Technology, Hassan*

ABSTRACT

Because of rising threat of internet attacks especially denial-of-service attacks traceback problem is often relevant to internet security. It is a problem that involves identifying the source of the attack packets. Because of the dynamic nature of cloud there is a new area of research called cloud forensics. The cloud forensics is the branch of forensics that applies computer science knowledge to prove digital artifacts. The Distributed Denial of Service (DDOS) is a widely used attack in cloud environment. Web services can get exposed to denial of services or xml denial of services attack that hamper web services by crashing the service providers and their services. To perform forensics of DDOS if it is identified using possible detection and prevention mechanisms then it would result in cloud forensics solutions and evidence collection and segregation. In order to address the problem of kinds of internet attacks against cloud web services there is a need to differentiate the legitimate and illegitimate messages. Proposed work has been used to not only trace DDoS attacking packets but it also enhances filtering attacking traffic. We have used three types of filters namely MATCH, MARK, MAKE OVER and DUMP[13]. Then we use DIFFIE-HELLMAN KEY EXCHANGE algorithm to protect the genuine/legitimate data. The DIFFIE-HELLMAN KEY EXCHANGE algorithm will encrypt the plaintext data into cipher text and then hides the message being exposed to the attacker. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. It focuses of three major security concerns: authentication, key generation and encryption of data.

Keywords: Traceback, Xdos Attack, Ddos Attack, Filters, DIFFIE- HELLMAN KEY EXCHANGE Algorithm.

I. INTRODUCTİON

In recent days Internet is being widely used for various activities, because it provides relevant information and important services in almost all fields such as educational, commercial , business, finance, hospitality, retail, entertainment, telecommunication, etc. Hence, it is very necessary to provide security to the internet users about their information and service provider, who provides service to them for their request in Cloud environment. Due to the interruption of service provided by service provider, inconvenience is caused to the cloud users. These interruption activities are due to Denial of service (DoS) \ XML denial of service (XDoS) attacks which done by the attacker for the material gain access or popularity or personal reasons [20]. Since the DDoS and XDoS attackers spoof the source address, tracing them is very difficult. DDoS attacks actually hamper web

services by crashing the service provider and its services. The proposed approach is very simple to implement, scalable enough and helps rescue from DDoS attacks more effectively since these attacks can only be detected and cannot be prevented. This approach uses DIFFIE-HELLMAN KEY EXCHANGE algorithm to encrypt/hide the original data being exposed to the attacker and establishes a shared secret key that can be used for secret communications while exchanging data over a public network. It uses two keys: one secret and other private key. If Sender wants to communicate with the receiver, he encrypts the message with his private key and senders' public key[21].

1.1 Characteristics of Cloud

● Individual use on request: A user can use his desired resources at any place and at any time through the global network without any conflict.

●Wide range of network accessing capacity: Capacities of the system are available to customers via a network and it can be accessed from various devices such as desktop, laptops, mobile phones, tablets, etc.

●Resource allocation: Simultaneous users can access the cloud resources at any time without any conflict. Cloud solutions have right to chose where the users data will be stored and processed.

●Elasticity and flexibility: Cloud dynamically allocates necessary resources, and resources are automatically restored to its original condition. The user is free to purchase additional resources and opportunities in any quantity and at any time.

●Pay per use: Cloud services are measurable and their usage is transparent, both for the service provider and clients.

1.2 Security Concerns

Trustworthiness is one of the key concerns of the cloud service provider. Organizations are carefully deceiving both their sensitive and insensitive data to cloud to fetch required services. Cloud works on pay per use basis. Suppose a DoS attacker intentionally sends numerous requests to cloud then the owner of that particular cloud will have to process more requests at a time. Meanwhile, if other genuine users sends request to the server on cloud, their service will be denied since the server will be busy serving the DoS attacker. The other worst case is DDoS attack, where the attacker compromises some more hosts to send the flood request.

1.3 Denial-Of-Service Attack/ Distributed Denial-Of-Service Attack

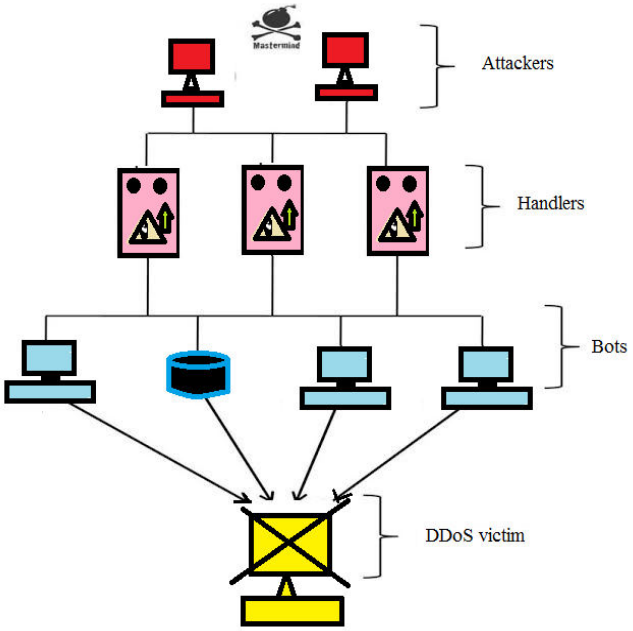
A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. This attack hamper web services by crashing the service provider and its services.

1.4 Modes of Attack

In a denial-of-service attack, the attacker makes an explicit attempt to prevent legitimate users of a service from using that service.

Two common forms of DoS attacks are:

1. those that crash services and
2. those that flood services.



II. RELATED WORK

In a Cloud computing environment, cloud servers that provide requested cloud services, may sometime crash after they receive huge amount of request [16]. This situation is called Denial Of service attack. Cloud Computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. Cloud Computing is changing the IT delivery model to provide on-demand self-service access to a shared pool of computing resources (physical and virtual) via broad network access to offer reduced costs, capacity utilization, higher efficiencies and mobility. Recently Distributed Denial of Service (DDoS) attacks on clouds has become one of the serious threats to this buzzing technology. Distributed Denial of Service (DDoS) attacks continue to plague the Internet. Distributed Denial-of-Service (DDoS) attacks are a significant problem because they are very hard to detect, there is no comprehensive solution and it can shut an organization off from the Internet. The primary goal of an attack is to deny the victim's access to a particular resource. In this paper, we want to review the current DoS and DDoS detection and defence mechanism.

The main problem faced in a cloud environment is the Distributed denial of service (DDoS) [17]. During such a DDoS attack all consumers will get affected at the same time and will not be able to access the resources on the cloud. All client users send their request in the form of XML messages and they generally make use of the HTTP protocol. So the threat coming from distributed REST attacks are more and easy to implement by the attacker, but such attacks are generally difficult to detect and resolve by the administrator. So to resolve these attacks we introduce a specific approach to providing security based on various filters. We make use of five different filters which are used to detect and resolve XML and HTTP DDoS attack. This allows the security expert to detect the attack before it occurs and block or remove the suspicious client.

Pushback is a mechanism for defending against distributed denial-of-service (DDoS) attacks [18]. DDoS attacks are treated as a congestion-control problem, but because most such congestion is caused by malicious hosts not

obeying traditional end-to-end congestion control, the problem must be handled by the routers. Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack.

Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the router's resources be used to route legitimate traffic. In this paper we present an architecture for Pushback, its implementation under FreeBSD, and suggestions for how such a system can be implemented in core routers.

Cloud Computing is an emerging area nowadays. Researchers are working on all aspects of cloud viz [19]. cloud network architecture, scheduling policies, virtualization, hypervisor performance scalability, I/O efficiency, data integrity and data confidentiality of data intensive applications. The dynamic nature of cloud presents researchers new area of research that is cloud forensics. Cloud Forensics is the branch of forensics for applying computer science knowledge to prove digital artifacts. The DDOS is the widely used attack in cloud environment. To do the forensics of DDOS if it is identified a possible detection and prevention mechanisms would aid in cloud forensics solutions and evidence collection and segregation. This paper presents different types of DDOS attack at the different layers of OSI model with increasing complexity in performing attack and focuses more on prevention and detection of DDOS at different layer of OSI and effect of DDOS in cloud computing.

The theoretical background of our proposed work is taken from reference [13]. We are giving security to the confidential data by using DIFFIE- HELLMAN KEY EXCHANGE algorithm. Diffie-Hellman key exchange approach uses two types keys: one is secret key and the other is private key. Sender communicates with the receiver by encrypting the message with his private key and senders' public key.

III. PROPOSED WORK

Flaws either in users' implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched. Of the kinds of network attacks, denial-of-service flood attacks have caused the most severe impact. Cloud computing suffers from major security threat problem by HTTP and XML Denial of Service (DoS) attacks. The combination of HTTP and XML messages that are intentionally sent to flood and destroy the communication channel of the cloud service provider is called as HX-DoS attack. To address this issue, there is a need to differentiate the genuine or legitimate message and illegitimate message.

HX-DoS attack involves an attacker who compromises a client having an account to access the cloud service provider server. Therefore, the attacker gets direct connection through the system. Then the attacker will install HX-DoS attack program at the user end and initiates it. The XDoS attack can take place in few ways: First, a network can be flooded with XML messages (instead of packets), in order to prevent legitimate users to network communication. Next, if the attacker floods the web server with XML requests, it will affect the availability of these web services. Finally, attackers manipulate the message content, so that the result web server gets crash. In order to differentiate them, the first method adopts Intrusion Detection System (IDS) by using a decision tree classification system called as MATCH filter. MATCH filter is located one hop away from host. The rule set of MATCH filter has been built up over time to identify the known HDoS and X-DoS messages. The well known HX-DoS attack is XML injection or XML Payload Overload, MATCH filter is trained and tested to identify these known attacks. After the detection of HX-DoS message, MATCH filter drops the packet which matches the rule set. The packets are subjected to marking after they are examined by the MATCH filter. The DIFFIE-

HELLMAN KEY EXCHANGE algorithm is used to convert the plaintext data into corresponding cipher text so that the attacker cannot view the original data being transmitted. Diffie–Hellman key exchange technique is accomplished by two parties who have no prior knowledge about each other to together establish a shared secret key over a channel.

IV. DESIGN CONSIDERATIONS

Consider two legitimate users and an attacker. User sends data through three filters namely, MATCH filter, MARK filter and MAKE OVER and DUMP filter to the server.

The message will be identified and if it is from an attacker then that message will be dropped before it reaches the server.

Modulo packet marking consists of two routers:

1. Edge router
2. Core router

On the victim side, by the time the victim starts collecting marked packets, all routers in the network will already have invoked the packet marking procedure. In extension, the victim does not have any knowledge about the real network or the attack graph. But the victim only knows the marking probability that the routers use.

It is appareled with the ability to mark packets as in the original Probabilistic Packet Marking(PPM) algorithm where each router shares the same marking probability. In specific, a router can either be a transit router or a leaf router. A transit router is a router that forwards traffic from upstream routers to its downstream routers or to the victim, whereas a leaf router is a router whose upstream router is connected to client computers and not to routers and forwards the clients' traffic to its downstream routers or to the victim. Assuredly, the clients are mixed with genuine as well as malicious parties. Likewise, every router will be having only one outgoing route toward the victim named "outgoing route toward the victim" and this can be further justified by the fact that modern routing algorithms favor the construction of routing trees.The plaintext data inside the packet will be converted into cipher text data using DIFFIE- HELLMAN KEY EXCHANGE algorithm so that when an attacker tries to get the data, he will be unable to read the original plain text data.

4.1 Goals

The denial-of-service (DDoS) attacks are addressed, where they try to suspend services of a host connected to the internet. The major goal of this project is to filter the genuine message from the message and pass that genuine message to the server, so that only genuine user can get resources of Cloud server. And the DIFFIE-HELLMAN KEY EXCHANGE algorithm is used so that the raw data is encrypted and is converted to cipher text so as to make it difficult the attacker to identify the message.

4.1.1 Cryptographic Explanation of Diffie-Hellman Key Exchange Algorithm [29]

The simplest and the original implementation of the protocol uses the multiplicative group of integers modulo p, where p is prime, and g is a primitive root modulo p. Here is an example of the protocol, with non-secret values, and secret values[29].

1. Alice and Bob agree to use a prime number $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $\boldsymbol{a = 6}$, then sends Bob $A = g^a \bmod p$

- $A = 5^{6} \bmod 23 = 8$

3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^{b} \bmod p$
   - $B = 5^{15} \bmod 23 = 19$
4. Alice computes $s = B^{a} \bmod p$
   - $s = 19^{6} \bmod 23 = \mathbf{2}$
5. Bob computes $s = A^{b} \bmod p$
   - $s = 8^{15} \bmod 23 = \mathbf{2}$
6. Alice and Bob now share a secret (the number **2**).

4.2 Modules

In a DDoS attack, an attacker compromises a client who has an account to access the cloud service provider server. By this way they get a direct connection through the system. The attacker then installs the DoS attack program at the user end and initiates it. To differentiate them, the first method adopts Intrusion Detection System (IDS) by using a decision tree classification system called as MATCH. MATCH filter is located one hop away from host. MATCH's rule set has been built up over time to identify the known DDoS messages. With the help of known DDoS attacks like XML injection or XML Payload Overload, MATCH filter is able to be trained and tested to identify these known attributes. Upon detection of DDoS message, MATCH filter drops the packet which matches the rule set. After MATCH examines all the packets, they are subjected to marking.

Next marking scheme is the Mark algorithm. As the packets travel via network, they are marked with router information using modulo technique. Upon trace-back request, reverse modulo is used to make over the path traversed by the packets. The marking is done on both edge and core routers. When an edge router decides to mark an incoming packet, it fetches the code to be marked that corresponds to physical address of the host from the lookup table and encodes it into the packet. The edge router requires one bit for indicating whether the packet is marked or not and few bits for marking code and it maintains a lookup table called MAC to ID table, which has physical address of the hosts attached to the network and equivalent numeric code for each of the physical addresses.

The core router marks the packet only if that packet has been already marked by the edge router. Else, it would simply forward the packets. Core router maintains a table called MAC to Interface which contains the physical addresses of all of its hardware input interfaces and link numbers assigned to each of these interfaces.

When a router decides to mark, it consults the table to find the link number assigned to the inbound interface. The core router uses the modulo technique for marking is calculated as in Equation 1,

New marking information= current marking information × number of interfaces on the router + the link number (1)

Make over and Dump filter, which is built from the IDP and its location is one hop back from the victim. Specifically, the host follows the same path (shortest path) across the routers for sending the packet to its destination. Make Over and Dump component maintains the information about each host and its equivalent packet marking value. If the marking value matches the stored value, it forwards the packet to respective host. During the time of the attack, when host spoofs the IP address of another host, the packet marking value differs from the value stored in the Make Over and Dump filter. This happens because: For marking, MATCH filter uses MAC address instead of the IP address. Therefore, the packets are dumped at the victim side and Make Over and Dump requests for the trace-back.

4.3 The Dıffıe- Hellman Key Exchange Algorithm Takes Place İn Following Steps [29]

1. Alice and Bob, using insecure communication, agree on a huge prime p and a generator g. They don't care if someone listens in.
2. Alice chooses some large random integer $x_A < p$ and keeps it secret. Likewise Bob chooses $x_B < p$ and keeps it secret. These are their "private keys".
3. Alice computes her "public key" $y_A \equiv g^{x}{}_A \pmod p$ and sends it to Bob using insecure communication. Bob computes his public key $y_B \equiv g^{x}{}_B$ and sends it to Alice. Here $0 < y_A < p$, $0 < y_B < p$. As already mentioned, sending these public keys with insecure communication is safe because it would be too hard for someone to compute x_A from y_A or x_B from y_B, just like the powers of 2 above.
4. Alice computes $z_A \equiv y_B{}^{x}{}_A \pmod p$ and Bob computes $z_B \equiv y_A{}^{x}{}_B \pmod p$. Here $z_A < p$, $z_B < p$. But $z_A = z_B$, since $z_A \equiv y_B{}^{x}{}_A \equiv (g^{x}{}_B)^{x}{}_A = g^{(x}{}_A{}^{x}{}_B{}^{)} \pmod p$ and similarly $z_B \equiv (g^{x}{}_A)^{x}{}_B = g^{(x}{}_A{}^{x}{}_B{}^{)} \pmod p$. So this value is their shared secret key.

V. CONCLUSION

HTTP or XML-Based DoS attacks are one of the most serious threats to cloud computing. Detection of these attacks can be effectively done by using marking approach based on packets on the attacker side and the detected packets are filtered by dropping the marked packets on the victim side. Therefore, the packet marking overhead and the false positive rate of DoS attacks are effectively reduced. DDoS attack detection scenario is improved by replacing the Cloud Protector with Make Over and Dump on the victim side and the introduction of MATCH filter and MARK filter at the source side. By this, enhancement of the reduction of the false positive rate is done and increase in the detection and filtering of DDoS attacks is possible. By the use of DIFFIE-HELLMAN KEY EXCHANGE algorithm, the victim can never be able to access the original text..

REFERENCES

[1] A.Belenky and N.Ansari (2003), 'Tracing Multiple Attackers with Deterministic Packet Marking (DPM)', Proceedings of IEEE Pacific Rim conference on communications, computers and signal processing, Vol. 1, pp. 49–52.

[2] A.Chonka W. Zhou and Y.Xiang (2008a), 'Protecting Web Services with Service Oriented Traceback Architecture', Proceedings of the IEEE eighth international conference on computer and information technology, pp. 706-711.

[3] A.Chonka, W.Zhou and Y.Xiang (2008b), 'Protecting Web Services from DDoS Attacks by SOTA', Proceedings of the IEEE fifth interna-tional conference on information technology and applications, pp. 1-6.

[4] A.Chonka, W.Zhou, J.Singh and Y.Xiang (2008c), 'Detecting and Tracing DDoS Attacks by Intelligent Decision Prototype', Proceedings of the IEEE International Conference on Pervasive Computing and Communications, pp. 578-583.

[5] A.Chonka, W.Zhou and Y.Xiang (2009a), 'Defending Grid Web services from X-DoS Attacks by SOTA', Proceedings of the third IEEE international workshop on web and pervasive security (WPS 2009), pp. 1-6.

[6] A.Chonka, W.Zhou and J.Singh (2009b), 'Chaos Theory Based Detec-tion against Network Mimicking DDoS Attacks', Journals of IEEE Communications Letters, Vol. 13, No. 9, pp. 717-719.

[7] A.Chonka, Y.Xiang, W.Zhou and A.Bonti (2011), 'Cloud Security Defence to Protect Cloud Computing against HTTP-DoS and XML-DoS attacks', Jour-nal of Network and Computer Applications, Vol. 34, No. 4, pp. 1097-1107.

[8] D.Dean (2002), 'An algebraic Approach to IP traceback', Journal ACM Transactions on Information and System Security', Vol. 5, No. 2, pp.119-137.

[9] S.Savage, D.Wetherall, A.Karlin and T.Anderson (2000), 'Practical Network Support for IP traceback', Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Com-puter Communication, pp. 295-306.

[10] H.Shabeeb, N.Jeyanthi and S.N.Iyengar (2012), 'A Study on Security Threats in Clouds', Journal of Cloud Computing and Services Sci-ence, Vol. 1, No. 3, pp. 84-88.

[11] X.Xiang, W.Zhou and M.Guo (2009), 'Flexible Deterministic Packet Marking: an IP Traceback System to Find The Real Source of At-tacks', Journal of IEEE Transactions on Parallel and Distributed Sys-tems, Vol. 20, No. 4, pp. 567-580.

[12] K.H.Choi and H.K.Dai (2004), 'A Marking Scheme using Huffman Codes for IP Traceback', Proceeding of 7th International Symposium on Parallel Architectures, Algorithms and Networks (SPAN'04).

[13] E.Anitha and Dr.S.Malliga (2014), 'A Packet Marking Approach To Protect Cloud Environment Against DDoS' Computer Science and Engineering Department, Kongu Engineering College Perundurai, India mallisenthil@kongu.ac.in.

[14] A.Parvathi and G.L.N.JayaPradha (2011), 'An IP Trace back System to Find the Real Source of Attacks', International Journal of Computer Trends and Technology- volume 2 Issue 1.

[15] K.Santhi, (2013), 'A Defense Mechanism to Protect Cloud Computing Against Distributed Denail of Service Attacks, volume 2, Issue 5, May 2013.

[16] Nisha H. bhandari (2013), 'Survey on DDoS Attacks and its Detection & Defence Approaches' IJISME.

[17] R. Vivek, R. Vignesh & V. Hema (2013), 'An Innovative Approach to Provide Security in Cloud by Prevention of XML and HTTP DDoS Attacks' ISSN(PRINT : 2320-8945, volume-1,Issue-1,2013.

[18] John Ioannidis, Steven M. Bellovin (2010) 'Implementing Pushback: Router-Based Defense Against DDoS Attacks' .

[19] J.J. Shah, Dr. L.G. Malik (2013), 'Impact of DDOS Attacks on Cloud Environment', Communication Technology, vol 2, Issue 7, July-2013.

[20] Amit Vinayakrao, Narendra Shekokar, Mahesh Maurya (2014) 'The Countering the XDoS Attack for Securing the Web Services', (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,3907-3911.

[21] Neha Tirthani, Ganesan R, 'Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography', School of computing Sciences and Engineering, M. tech–Computer Science, Associate Professor (CSE), VIT, Chennai campus.

[22] A.J.Han Vinck, University of Duisburg-Essen SVG version: Flugaal ,'Introduction to public key cryptography', p. 16.

[23] Merkle, Ralph C (April 1978). "Secure Communications Over Insecure Channels". Communications of the ACM 21 (4): 294–299. doi :10.1145/359460.359473. Received August, 1975; revised September 1977.

[24] Diffie, W. ; Hellman, M. (1976). " New directions in cryptography" (PDF). IEEE Transactions on Information Theory 22 (6): 644–654. doi :10.1109/TIT.1976.1055638.

[25] Ellis, J. H. (January 1970). "The possibility of Non-Secret digital encryption".

[26] Martin E. Hellman, Bailey W. Diffie, and Ralph C. Merkle, "Cryptographic apparatus and method", issued 29 April 1980.

[27] A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic," Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé, Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science, Volume 8441, 2014, pp 1-16.

[28] C. Kaufman (Microsoft) (December 2005). "RFC 4306 Internet Key Exchange (IKEv2) Protocol". Internet Engineering Task Force (IETF).

[29] http://www.google.com .