International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 389 - 395, 2013, ISSN: 2319–8656

Multiple Downlink Fair Packet Scheduling Scheme in Wi-Max

Pooja Gupta
Lingaya's University
Faridabad,India

Brijesh Kumar
Lingaya's University
Faridabad,India

B.L. Raina
Lingaya's University
Faridabad,India

Abstract: IEEE 802.16 is standardization for a broadband wireless access in network metropolitan area network (MAN). IEEE 802.16 standard (Wi-Max) defines the concrete quality of service (QoS) requirement, a scheduling scheme and efficient packet scheduling scheme which is necessary to achieve the QoS requirement. In this paper, a novel waiting queue based on downlink bandwidth allocation architecture from a number of rtps schedule has been proposed to improve the performance of nrtPS services without any impaction to other services. This paper proposes an efficient QoS scheduling scheme that satisfies both throughput and delay guarantee to various real and non-real applications corresponding to different scheduling schemes for k=1,2,3,4. Simulation results show that proposed scheduling scheme can provide a tight QoS guarantee in terms of delay for all types of traffic as defined in WiMax standards. This process results in maintaining the fairness of allocation and helps to eliminate starvation of lower priority class services. The authors propose a new efficient and generalized scheduling schemes for IEEE 802.16 broadband wireless access system reflecting the delay requirements.

Keywords: QoS,IEEE 802.16,WiMax,rtps,nrtps,Fair Scheduling.

1. INTRODUCTION

IEEE 802.16 based wireless access scheme (commonly known as WiMAX) is considered as one of the most promising wireless broadband access for communication networks in metropolitan areas today. Since IEEE802.16 standard defines the concrete quality of service(QoS) requirement, a scheduling scheme is necessary to achieve the QoS requisite level. Many Scheduling schemes have earlier been proposed with the purpose of throughput optimization and fairness enhancement. However, few scheduling algorithm support the delay requirement. Here delay refers to unpredictably longer time for packets to reach the destination due to unavailability of network resources. IEEE802.16 has strict delay requirement, the lower the delay the better the QoS. To achieve the objective of providing a fair and efficient allocation of bandwidth to all the services without much of the delay different algorithms have been proposed by taking care of different parameters. Moreover, we have four service classes of IEEE802.16 which have different delay requirements for example for UGS service class cannot tolerate delay, while for BE service class is delay tolerable.

Sometime the priority of service classes leads to the starvation problem for lower priority service class. The priority goes from higher to lower like UGS>rtps>nrtps>BE respectively. In [1], the authors propose a hybrid of Earliest Due Date (EDD) and Weighted Fair Queue (WFQ). In EDD, all the arriving packets get a deadline stamp and are scheduled according to the increasing order of deadlines. The algorithm intends to serve the real time traffic first and only if real time buffer is empty will they consider BE traffic. This will certainly lead to starvation of lower priority requests. In [3], the authors consider two types of queues. The first type is used to schedule data grants for UGS and allocate request opportunities for rtPS and nrtPS. These grants are scheduled in a first in first out (FIFO) manner. Once the first queue type has been served, the scheduler will consider the second type leading to scarcity. The authors in [4] propose an architecture consisting of three schedulers. The first scheduler is concerned with UGS, rtPS and ertPS flows. The second scheduler is concerned with flows requiring a minimum bandwidth mainly nrtPS. The third scheduler is used for BE traffic that comes into picture only when the first two schedulers have become free. In [5], the authors suggest downlink bandwidth allocation algorithms based on flow type and strict priority from highest to lowest - UGS, rtPS, nrtPS and BE. Here an Opportunistic fair scheduling was used. Here BE traffic is served whenever an opportunity is available, but for most of the time BE starves for bandwidth. For guaranteeing the QoS for different service classes, priority based schemes could be used in WiMAX scheduler [6]. The priority order used in real time schedulers is: UGS, ertPS, rtPS, nrtPS and BE. Here the priority is maintained but the least priority ones starve for bandwidth. Delay based algorithm is specifically designed for both real time traffic and non real time traffic, where the delay tolerance is the primary QoS parameter. Earliest Due Date (EDD) is the basic algorithm for scheduler to serve the connection based on the deadline [7, 12]. However, this algorithm does not guarantee the throughput for higher priority service viz.UGS. So [13] proposed a scheduler that combines both EDD and priority for assuring nrtPS and BE better performance while trying to satisfy the other classes. Even though there are lots of conventional scheduling algorithms they are not meeting all

the required QoS parameters. The performance affecting parameters like fairness, bandwidth allocation, throughput, average delay and delay jitter are studied and found out that none of the algorithms perform effectively for delay requirement of nrtps service class connections with respect to other service classes.

2. SYSTEM MODEL

Point to Multi Point(PMP) mode and mesh mode are the two types of operating modes define for IEEE802.16. In the PMP mode SSs are geographically scattered around the BS. The performance of IEEE 802.16 in the PMP mode is verified in[8][9]. Our system model is based on a time-division-duplex (TDD) mode. The IEEE 802.16 frame structure is illustrated in Fig.1[2]. The downlink subframe starts with preamble followed by frame control header (FCH), downlink map (DL-MAP), uplink map (UL-MAP) messages and downlink burst data. The DLMAP message defines the start time, location, size and encoding type of the downlink burst data which will be transmitted to the SSs. Since the BS broadcasts the DLMAP message, every SS located within the service area decodes the DL-MAP message and searches the DL-MAP information elements (IEs) indicating the data bursts directed to that SS in the downlink subframe. After the transmit/receive transition gap (TTG), the uplink subframe follows the downlink subframe. IEEE 802.16 provides many advanced features like adaptive modulation coding (AMC), frame fragmentation and frame packing. In the current work, the focus is on the downlink scheduling scheme.

3. MULTI USER SCHEDULER OF THE MAC LAYER

In this section, a multiuser scheduler is designed at the medium access control (MAC) layer. Delay requirement is taken into account in the scheduler design. The AMC, packet fragmentation and packet packing have not been considered. In case of the UGS traffic, the required bandwidth is reserved in advance. Hence, only rtPS, nrtPS and BE connections are focused in the design.

3.1 Proportional Fair Scheduling

The proportional fair scheduling [10] has shown an impressive guideline in scheduler design because it maximizes the total sum of each SS's utility. In the proportional fair scheduling, the metric for each connection is defined as follows

$$\phi_i(t)=DRC_i(t)/R_i(t). \quad (1)$$

where DRC_i [12] is the rate requested by the SS_i and R_i is the average rate received by the SS_i over a window of the appropriate size Tc [2][12]. The average rate R_i is updated as

$$R_i(t+1)=(1-1/T_c)R_i(t)+1/T_c*\text{current transmission rate}. \quad (2)$$

where Tc is the window size to be used in the moving average. The proportional fair scheduler selects the connection that has the highest metric value.

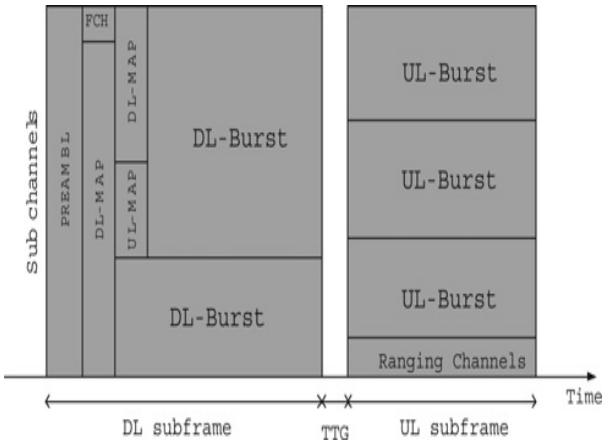


Fig. 1. IEEE 802.16[2] frame structure

3.2 Proposed Fair Scheduling(FS)

In the proportional fair scheduling, the strict fairness is guaranteed, however the QoS requirement is not reflected. To the knowledge of authors rtps connections for QoS have been discussed in the literature with regard to one specified nrtps connection ,Kim et. al.[2].Pooja gupta et al. [14]have generalized this concept by associating various parameters such as scheduling ratio xi of rtps class parameter associated to k number of nrtps class.Thus, the general scheduling scheme is being introduced that satisfies the delay requirement. In this paper we have generated a number of fair scheduling schemes corresponding to the parameter k so that the delay requirements are minimized with regard to corresponding nrtps schemes as mentioned below.

The metric value of the rtPS connections with the delay requirement should be increased as the queuing delay increases because the scheduler selects the connection with the highest metric value with nrtps connections, because nrtps connections are in the lowest priority. For the above mentioned conditions the equations for rtps and ,nrtps are proposed by the authors in paper [2].Here we are generalizing the above equation by proposing a new scheduling scheme based on the following metrics for rtPS, nrtPS and BE connections are given as :

$$\Phi_{rt,i}(t)= 1/R_{rt,i}(t)+C(1+2/\pi*\arctan(|d|)). \quad \text{if } q_i>0 \text{ and } d \geq d_{min}. \quad (3)$$

$=1/R_{rt,i}(t)+ C.$ if $q_i >0$ and $d< d_{min.}$

$=0$ if $q_i =0$

$\Phi_{nrt,i}(t)= 1/R_{nrt,i}(t)+ C.$ if $q_i >0$ (4)

$=0$ if $q_i =0$

$\Phi_{BE,i}(t)= 1/R_{BE,i}(t).$ if $q_i >0$ (5)

$=0$ if $q_i =0$

The parameter d is the queuing delay and C means the intensity of the delay requirement in the rtPS connection. The parameter dmin is the minimum delay that triggers the service differentiation between the rtPS connection and nrtPS connection, and q_i means the queue length of the connection i. Note that R_{rt}, R_{nrt} and R_{BE} are updated in the same manner as in the proportional fair scheduling, that is

$$R_{rt,i}(t+1)= (1-1/T_c)R_{rt,i}(t) + r/T_c \text{ if connection } i \text{ is scheduled.} \quad (6)$$

$$=(1-1/T_c)\, R_{rt,i}(t) \quad \text{otherwise}$$

where Tc is the window size to be used in the moving average and r is the current transmission rate requested by the SS. The long-term rate is the average sum of the previously scheduled transmission rates during the time window Tc, where the high Tc value means that the long-term rate changes slowly because the average is taken over many previous transmission rates. The long-term rate of a connection decreases exponentially before the connection is scheduled, and it increases when the connection is scheduled. We do not consider the AMC, so r is a constant. On every frame, the scheduler selects the connection that has the highest metric value. Owing to the delay requirement term in the rtPS metric, rtPS connections are served more frequently than other connections when the queuing delay increases.

3.3 Determination of Novel Parameters with Analysis

The scheduling ratio x as the average number of scheduling times for each of rtPS to k nrtPS connections where k<=x has been defined as given by the following two cases:

If rtPS and nrtPS connections are scheduled equally, the scheduling ratio x equals k, and if rtPS connection is scheduled more frequently than nrtPS connection, the scheduling ratio x becomes greater than k. Now the average scheduling interval in the rtPS connection is ((x+k)/x) frames because, on the average, k nrtPS schedule corresponding to x rtPS connections. As a result of this, the average scheduling interval in nrtPS connection is (k+x) frames. At the steady state, the average long-term rates of rtPS and nrtPS connections at the scheduling instance are as follows:

$\overline{R_{rt}} = \overline{R_{rt}}(1-(1/T_c))^{(k+x)/x} + (r/Tc)$, at the steady state, we obtain

$$\overline{R_{rt}}=(r/T_c)/ (1-(1-(1/T_c))^{(k+x)/x} \quad (7)$$

Analogously, Since $\overline{\overline{R_{nrt}}} = \overline{\overline{R_{nrt}}}(1-(1/T_c))^{(k+x)} + (r/Tc)$ at the steady state, we obtain

$$\overline{\overline{R_{nrt}}}=(r/T_c)/ (1-(1-(1/T_c))^{(k+x)} \quad (8)$$

We consider the same assumption as in [11] that the average metric value for each connection at the scheduling instance becomes similar to each other. Hence,

$$1/\overline{R_{rt}}(1-(1/T_c))^{(k+x)/x} + C(1+(2/\pi)\arctan(d)).$$
$$\approx 1/\overline{\overline{R_{nrt}}}(1-(1/T_c))^{(k+x)} + C. \quad (9)$$

From (7) and (8) , (9) can be written as

$$(1-(1-(1/T_c))^{(k+x)/x})*T_c/ (r*(1-(1/T_c))^{(k+x)/x}) + C(1+(2/\pi)\arctan(d)).$$
$$\approx (1-(1-(1/T_c))^{(k+x)})*T_c/(r*(1-(1/T_c))^{(k+x)}) + C. \quad (10)$$

Put $(1-1/T_c)=X$, $L=1+(2/\pi)\arctan(d)$, therefore from above equation we have

$$(1-(X)^{(k+x)/x})*T_c/(r*(X^{(k+x)/x}) + C*L$$

$$(1-(X)^{(k+x)})*Tc /(r*(X^{(k+x)}) + C$$

$$\text{i.e. } C*(L-1)=(Tc/r)*((1-(X)^{(k+x)}/X^{(k+x)} – (1-(X)^{(k+x)/x})/X^{(k+x)/x}))$$

$$C*(2/\pi)*\tan^{-1} d=(Tc/r)*((X^{(k+x)/x} – X^{(k+x)})/X^{((x*x+k*x+k+x)/x)}) \quad (11)$$

Now with the help of L and X as defined above and with little algebra, the set of values of delay represented by $d=d_i$ correspond to different sets of values of x,k and C, from equation (11) we have for $d\geq 0$,

$$d= \tan(((\pi*Tc)/(2*r*C)*[((1-1/Tc)^{(k+x)/x} – (1-1/Tc)^{(k+x)})]/(1-1/Tc)^{((x*x+k*x+k+x)/x)}] \quad (12)$$

Now generalizing the above equation if d_i represents the various delays for i iterations corresponding to the above parameters associated to number of rtps,nrtps and intensity such that $d\geq 0$.Thus we have the main result as :

$$d_i=\tan(((\pi*Tc)/(2*r*C)*[((1-1/Tc)^{(k+x)/x} – (1-1/Tc)^{(k+x)})]/(1-1/Tc)^{((x*x+k*x+k+x)/x)}], \text{ However } d_i\geq 0 \quad (13)$$

here $x_i=i, 0\leq i\leq 10$.However,d_i, C_j, k_t all will take real values under the investigation as given below:

Now we determined the solution set (d_i) corresponding to the various parameters C_j, x_i and k_t. As the parameter C_i

increases, the delay d_i decreases because d_i and C_i are inversely proportional to each other. For, k=1, we derive the delays d_i corresponding to different values of $C=C_i$ and plot the graph as given below.When we compare these with the ones derived by Kim et. al.[2], we notice here that our results turn out to be almost closer with their results.

4. SIMULATION RESULTS OF FOUR FAIR SCHEDULING SCHEMES

We now compare the delays of rtPS and nrtPS corresponding to a number of scheduling schemes corresponding to k=1,2,3,4 and as such analysis has been done using Matlab for values of di (delays) corresponding to different prescribed values of x_i, k_t, and C_j. ,for $1\leq i \leq 10$,j=1,2,3,t=1,2,3,4.

CASE I a) x:k=1:1 that is number of rtps connections is equal to number of nrtps connections.In this case x=5,k=5.

Table 1. Delay requirement of rtps connections for k=1 corresponding to various values of $C=C_j$, $1\leq j \leq 3$

x	1	2	3	4	5	6	7	8	9	10	C_j
d_1	.0029	.0064	.0098	.0133	.0167	.0202	.0237	.0271	.0306	.0341	0.1
d_2	.0059	.0128	.0197	.0266	.0336	.0405	.0475	.0546	.0617	.0689	0.05
d_3	.0002	.03	.0635	.0877	.1139	.143	.1761	.215	.2622	.322	0.01

We now draw the graph for delay d_i , $1\leq i \leq 10$, for various values of x corresponding to one nrtps scheduling i.e. k=1 and compare these delays with the once obtained by Kim et. al.[2].The analysis follows as under:

Case I.1

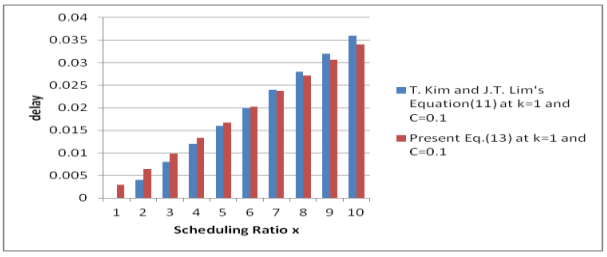


Fig 2. Delay against Scheduling ratio x when k=1 at C=0.1

Case I.2

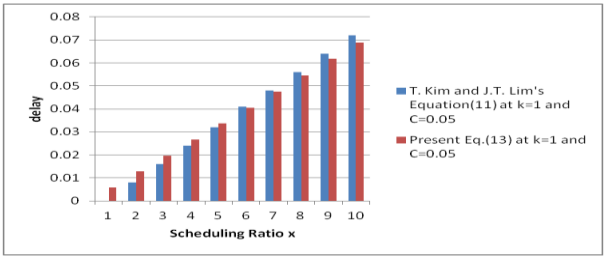


Fig 3. Delay against Scheduling ratio x when k=1 at C=0.05

Case I.3

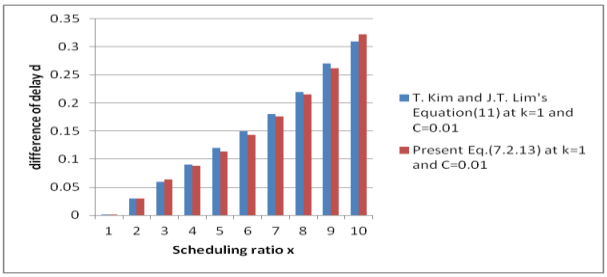


Fig 4. Delay against Scheduling ratio x when k=1 at C=0.01

From Fig. 2., Fig. 3. and Fig. 4,it has been observed that our Eq.(13) coincides with Kim et. al. equation[2]'s equation. Hence our equations proves to be correct for k=1 at C=0.1,0.05 and 0.01.However, it has been analysed that as x increases, the delays corresponding to each of five rtPS, five nrtPS increase. However, we notice that for first five values of x, respective delays of nrtPS.>rtPS and then there follows transition and for the next five values the delays reverse such that nrtPS<rtPS justifying doing away with the starvation of nrtps.

Case II:

Delay requirement of rtps connection for k=2,such that $k \leq x$.

Table 2. Delay requirement of rtps connections for k=2 corresponding to various values of $C=C_j$,$1\leq j \leq 3$

x	1	2	3	4	5	6	7	8	9	10	C_j
d_1	.0169	.0267	.0366	.0464	.0563	.0662	.0761	.0861	.0960	.1060	0.1
d_2	.0337	.0534	.0732	.0930	.1130	.1330	.1531	.1734	.1939	.2145	0.05
d_3	.1701	.2734	.3825	.5003	.6304	.7779	.9501	1.1583	1.4206	1.7693	0.01

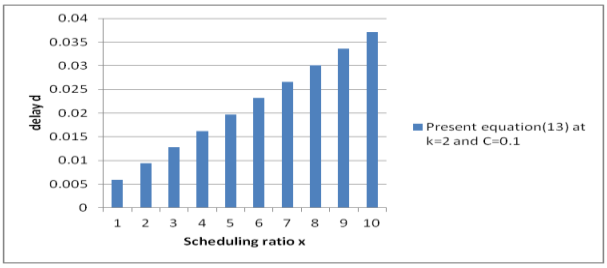


Fig 5. Delay against Scheduling ratio x when k=2 at C=0.1

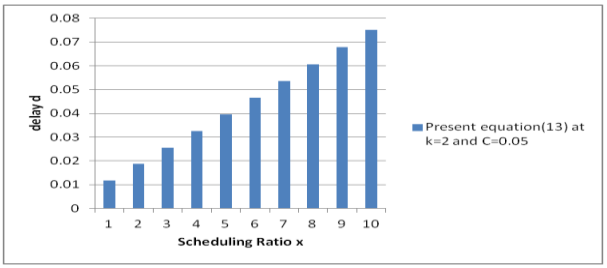


Fig 6. Delay against Scheduling ratio x when k=2 at C=0.05

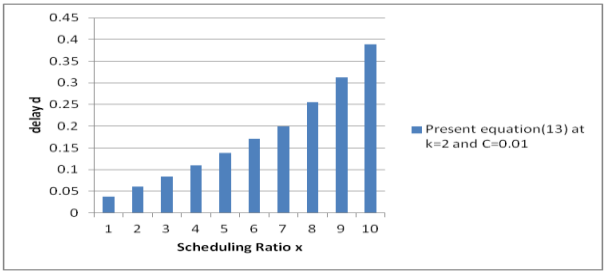


Fig 7. Delay against Scheduling ratio x when k=2 at C=0.01

Case III:

Delay requirement of rtps connection for k=3,such that k ≤ x.

Table 3. Delay requirement of rtps connections for k=3 corresponding to various values of $C=C_j$,$1\leq j \leq 3$

x	1	2	3	4	5	6	7	8	9	10	C_j
d_1	.0253	.0351	.0450	.0549	.0648	.0747	.0847	.0946	.1046	.1146	0.1
d_2	.0506	.0704	.0902	.1101	.1301	.1503	.1705	.1910	.2115	.2323	0.05
d_3	.2584	.3665	.4829	.6109	.7556	.9238	1.1259	1.3791	1.7127	2.1834	0.01

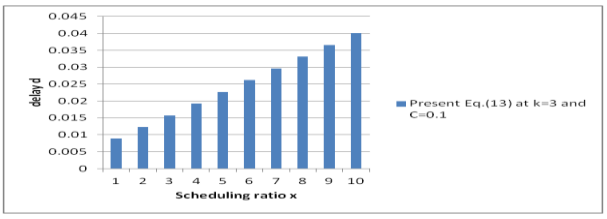


Fig 8. Delay against Scheduling ratio x when k=3 at C=0.1

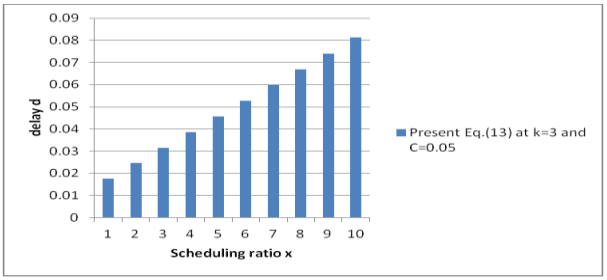


Fig 9. Delay against Scheduling ratio x when k=3 at C=0.05

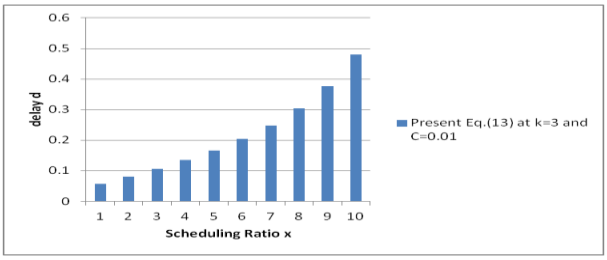


Fig 10. Delay against Scheduling ratio x when k=3 at C=0.01

Case IV:

Delay requirement of rtps connection for k=4,such that k ≤ x.

Table 4. Delay requirement of rtps connections for k=4 corresponding to various values of $C=C_j$,$1\leq j \leq 3$

x	1	2	3	4	5	6	7	8	9	10	C_j
d_1	0.0117	0.0152	0.0187	0.0221	0.0256	0.0291	0.0326	0.0361	0.0396	0.0431	0.1
d_2	0.0236	0.0305	0.0375	0.0445	0.0515	0.0586	0.0658	0.0728	0.0792	0.0876	0.05
d_3	0.0771	0.1024	0.1301	0.1614	0.1975	0.2408	0.2946	0.3649	0.4630	0.6131	0.01

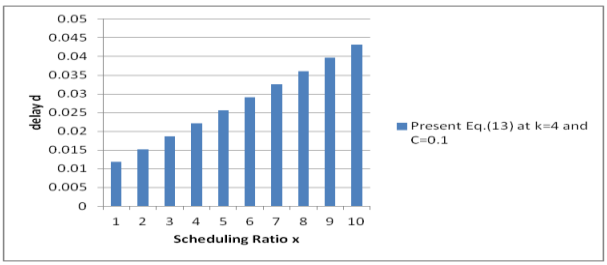


Fig 11. Delay against Scheduling ratio x when k=4 at C=0.1

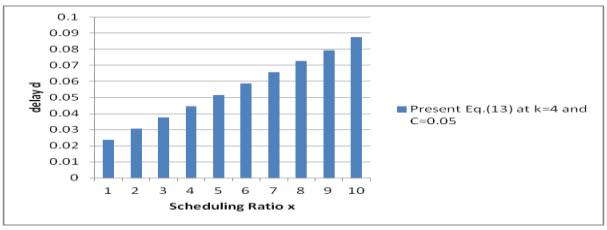


Fig 12. Delay against Scheduling ratio x when k=4 at C=0.05

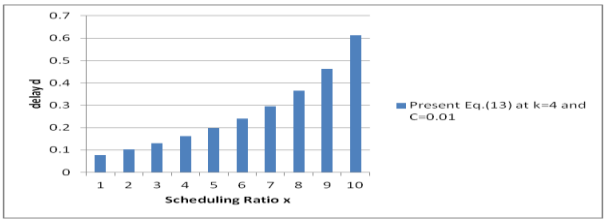


Fig 13. Delay against Scheduling ratio x when k=4 at C=0.01

Table 5. Simulation Information

Parameter	Value
Packet Size	1500 bytes
Number of nodes	10
Delay requirement	30ms

Table 6. represent the comparison of all the analysis that has been observed for Kim et. al.[2] value's at k=1.Our's at k=1,2,3,4 at different values of C corresponding to different values of x where $1 \le x \le 10$.

Table 6. Anaylsis of result of Kim et. al. at k=1,Our's at k=1 ,k=2, k=3 and k=4 at different values of C corresponding to different values of x where $1 \le x \le 10$.

X	⟶	1	2	3	4	5	6	7	8	9	10
C_1=0.1	Tim's value at k=1	0	.004	.008	.012	.016	.02	.024	.028	.032	.036
	Present value at k=1	.0029	.0064	.0098	.0133	.0167	.0202	.0237	.0271	.0306	.0341
	K=2	.0059	.0093	.0128	.0162	.0197	.0231	.0266	.0301	.0336	.0371
	K=3	.0088	.0122	.0157	.0192	.0226	.0261	.0296	.0331	.0366	.0401
	K=4	0.0117	0.0152	0.0187	0.0221	0.0256	0.0291	0.0326	0.0361	0.0396	0.0431
C_2=0.05	Tim's value at k=1	0	.008	.016	.024	.032	.041	.0481	.056	.064	.072
	Present value at k=1	.0059	.0128	.0197	.0266	.0336	.0405	.0475	.0546	.0617	.0689
	K=2	.0117	.0186	.0256	.0325	.0395	.0465	.0535	.0606	.0678	.0750
	K=3	.0177	.0246	.0315	.0385	.0455	.0526	.0596	.0668	.0740	.0813
	K=4	0.0236	0.0305	0.0375	0.0445	0.0515	0.0586	0.0658	0.0728	0.0792	0.0876
C_3=0.01	Tim's value at k=1	.0002	.03	.0635	.0877	.1139	.143	.1761	.215	.2622	.322
	Present value at k=1	.0002	.03	.0635	.0877	.1139	.143	.1761	.215	.2622	.322
	K=2	.0374	.0601	.0841	.1100	.1386	.1711	.1991	.2548	.3125	.3892
	K=3	.0568	.0806	.1062	.1343	.1662	.2032	.2476	.3034	.3767	.4803
	K=4	0.0771	0.1024	0.1301	0.1614	0.1975	0.2408	0.2946	0.3649	0.4630	0.6131

5. ANALYSIS OF DELAYS OF rtps and nrtps SERVICE CLASSES

Now in particular, we give the comparison of delay of different classes with regard to the 10 nodes for the cases C= 0.1,C=.05 and C=0.01 Kim et. al.[2] at k=1 with our's Equation(13) and analyze the comparison of the downlink services within rtPS, nrtPS, as given below:

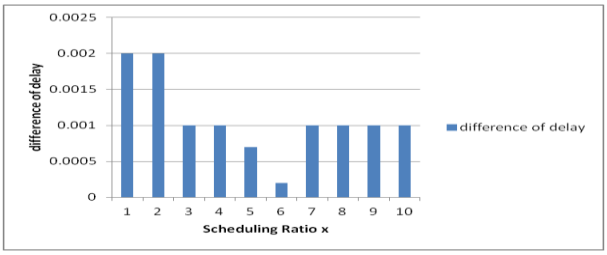


Fig. 14. Difference of delay d of Kim et. al.[2] with our's Equation(13) when k=1 and C=0.1

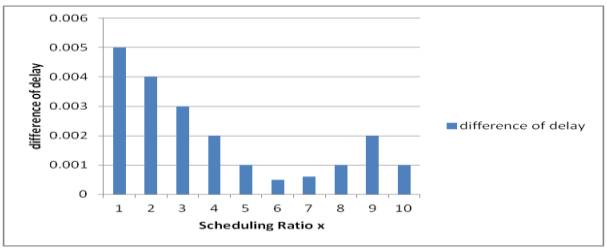


Fig. 15. Difference of delay d of Kim et. al.[2] with our's Equation(13) when k=1 and C=0.05

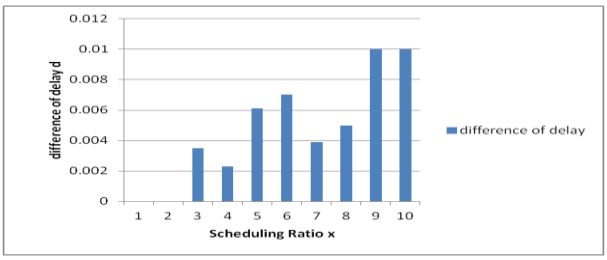


Fig. 16. Difference of delay d of Kim et. al.[2] with our's Equation(13) when k=1 and C=0.01

From Fig. 14, it has been observed that the difference of delay when k=1 and C=.1 first decreases till sixth value of x and then become steady. The value of difference of delay is approx. 0.001 which is quite less. Similarly, from Fig. 15 it has been observed that the difference of delay when k=1 and C=0.05 first decreases till sixth value of x then increases and decreases at 10 but again the value of difference of delay is quite less. From Fig. 16 it has been observed that the difference of delay when k=1 and C=.01 is showing the variation of increase and decrease but that will not not effect much because of the lesser difference.

6. CONCLUSION

In this paper, an effort has been done to remove the starvation problem and improvise the proportional fair scheduling scheme by managing the value of k. The suggested model has been simulated using Matlab and the results have

been discussed. To support the QoS requirement the delay requirement term in the proportional fair scheduling scheme has been added. The main contribution of this paper is that a method has been proposed which will generalize the delay requirement by associating various parameters of x_i defined as (various) rtps connections to the parameter k_i associated to the (various) nrtps connections. The suggested general scheduling scheme satisfies the delay requirement. One can find the appropriate parameter C according to the traffic condition of the networks. After fine tuning of the operating parameter, the delay requirement can be satisfied without excessive sacrifice in the nrtps connection performance.

7. REFERENCES

[1]. Guojun D., Dai J., (March 2007), "*An Improved Handover Algorithm for Scheduling Services in IEEE802.16e*", Published in Mobile WiMAX Symposium,Orlando,FL, IEEE,pp 38-42.

[2]. Kim T., Lim J.T.,"*Quality of service supporting downlink scheduling scheme in worldwide interoperability for microwave access wireless access systems*", Published in IET.Communications, Vol. 4, Iss. 1, pp. 32–38,2010.

[3]. Howon L. , Taesoo K. and Dong-Ho Cho, (Sept. 2004), "*An efficient uplink scheduling algorithm for VoIP services in IEEE 802.16 BWA systems*", 60th IEEE Vehicular Technology Conference, vol.5, pp. 3070 – 3074.

[4]. Kun y., Jie z. and Hsiao-hwa c., (March-April2007), "*A Flexible QoS aware service Gateway for heterogeneous wireless networks*",Published in IEEE NETWORK, vol. 21,issue 2,pp 6-12 .

[5]. Mehrjoo M.,Dianati M., Shen X. and Naik K.,(2006), "*Opportunistic Fair Scheduling for the Downlink of IEEE 802.16Wireless Metropolitan Area Networks*", Published in Proceeding Qshine'06 proceedings of the 3rd International Conference on QoS in heterogenous Wired /Wireless Networks, vol.191.

[6]. Wang Y., et al., (May 2008), "*Priority-Based Fair scheduling for Multimedia WiMAX Uplink Traffic*", Proc. of IEEE International Conference on Communication, China.

[7]. Perumalraja R., et al., (2006), "*Multimedia Supported Uplink Scheduling for IEEE 8021.6d OFDMA Networks*", Proceedings of Annual India Conference.

[8]. Kumar S.,"Hybrid scheduling For QoS in WiMAX",Master Thesis , Thapar University,Patiala,June 2009.

[9]. "IEEE Standard for Local and metropolitan area networks", Part 16: Air Interface for Broadband Wireless Access Systems.

[10]. CDMA-HDR a high efficiency-high data rate personal communication wireless system'. Proc. IEEE Vehicle Technology Conf., Tokyo, May 2000, vol. 3,pp. 1854–1858.

[11]. HOU F., HO P., SHEN X., CHEN A. "A novel QoS scheduling scheme in IEEE 802.16 networks". Proc. IEEE WCNC, Hong Kong, March 2007, pp. 2457–2462.

[12]. Wongthavarawat K., and Ganz A., (2003), "*Packet Scheduling for QoS Support in IEEE 802.16 Broadband Wireless Access Systems*", International Conference. on Journal of Commn. Systems., pp.81-86.

[13]. Perumalraja R., et al., (Sept. 2010), "*QoS Assured Uplink Scheduler for WiMAX Networks*", Published in Vehicular Technology Conference Fall,IEEE 72nd,pp-1-5.

[14]. Gupta P., Kumar B., Raina B.L.,"*QoS Support downlink for WiMAX Network*", Published in QSHINE 2013,LNICST(Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering) Springer 115 proceeding ,pp- 989-997.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 396 - 399, 2013, ISSN: 2319–8656

Secure Communication Using Generalized Digital Certificate

Bismin V Sherif
Viswajyothi College of Engineering and Technology, Kerala, India

Andrews Jose
Viswajyothi College of Engineering and Technology, Kerala, India

Abstract:- A digital certificate is the combination of a statement and a signature of the statement, signed by a trusted certification authority. This work proposes using generalized digital certificate (GDC), for user authentication and key agreement for efficient secure communication. A GDC contains user's public information, such as the information of user's digital driver's license, digital birth certificate, etc., and a digital signature of public information signed by a trusted certificate authority(CA). In GDC, user does not have any public and private key pairs, therefore key management in using GDC is much simpler than public key digital certificate. The digital signature component of GDC is used as the secret token of each user that will never be exposed to any verifier. Instead, the owner proves to the verifier that he has the knowledge of the signature by correctly responding to the verifier's challenge. The session key established using proposed approach can be used for secure communication between the entities.

Keywords: Generalized Digital Certificate; User Authentication; Key Establishment; Certification Authority; Secure Communication

1. INTRODUCTION

Digital certificate is a form of an electronic credential for the Internet. Similar to driver's license, employee ID card etc, a digital certificate is issued by a trusted third party to establish the identity of the certificate holder. The trusted third party who issues the Digital Certificate is called as the Certification Authority (CA). Digital certificate is actually the combination of a statement and a digital signature of the statement. X.509 public-key digital certificate has been widely used to provide authentication on the user's public key contained in the certificate. In X.509 public key digital certificate, the statement normally contains the public key along with some general information's , which is signed by trusted certification authority. The user is authenticated if he is able to prove that he has the knowledge of the private key corresponding to the public key contained in the X.509 public-key digital certificate. However, the public key digital certificate itself cannot be used to authenticate a user since a public-key digital certificate contains only public information and can be easily recorded and played back once it has been revealed to verifier. A new form of digital certificate is introduced in the paper[1]. The approach mentioned in the above paper enables a user to be authenticated and a shared secret session key to be established with his communication partner using any general form of digital certificates. This general form of digital certificates can be anything like a digital driver's license, a digital birth certificate or a digital ID, etc, which can be called as *generalized digital certificate (GDC).* A GDC contains user's public information and a digital signature of this public information signed by a trusted Certification Authority. This digital signature will never be revealed to the verifier directly. Therefore, the digital signature of a GDC becomes a security factor which can be used for user authentication.

In GDC, the public information does not contain any user's public key. Since user does not have any private and public key pair, this type of digital certificate is easier to manage than the X.509 public-key digital certificates. The digital signature of the GDC is used as the secret token of each user. The owner of this kind of digital certificate never reveals signature of GDC to a verifier in plaintext. Instead, the owner computes a response to the verifier's challenge to prove that he has the knowledge of the digital signature of GDC. Thus, owning a GDC can provide user authentication in a digital world.

In addition, a secret session key can be established between the verifier and the certificate owner during this interaction. And the two parties can be further communicate by encrypting the messages using this secret session key. But the same key is used between the participants for encrypting the whole messages in that session. From this it is clear that a hacker who continuously monitor their communication can easily decrypt the messages, which compromises the secrecy of the information. This approach also has the disadvantage, what symmetric key encryption concepts undergoes. So an innovative approach which can overcome the above mentioned problem is presented in this paper. And with the proposed method digital certificate can be efficiently generated and the participants can be securely communicated.

2. RELATED WORKS

The two fundamental services in secure communication are user authentication and key establishment. Wide researches have been conducted on both of these areas. But most of the works have been carried on public key digital certificate. A number of signature schemes for generating signatures have also been developed over years.

The most widely using digital certificate is X509 public key digital certificate[2]. In cryptography, a public key digital or identity certificate is an electronic document that uses a digital signature to bind a public key with an identity information such as the name of a person or organization, their address, etc. This certificate can be used to verify that a public key

belongs to an individual. The problem with public key digital certificate approach is it can be easily recorded and played back once it has been completely revealed to the verifier. Since it deals with public and private key pairs, key management with public key digital certificate is difficult.

This proposed scheme is related to the Identity based cryptography[3]. In ID based system, each user must register at a private key generator(PKG). If the user is accepted, PKG will generate a private key for the user. The identity like name or email ID can be consider as user's public key. In ID-based system, it is assumed that each user already knows the identity of his communication partner. Based on this assumption, there is no need, to authenticate the identity, which can be consider as the its main advantage. Due to this assumption, ID-based cryptography is only limited to applications that communication parties know each other prior to communication. But in the GDC concept, the user does not need to know any information of his communication partner. The public information of a GDC, such as user's identity, can be transmitted through the network and verified by each communication entity. That is GDC schemes support general PKI applications, such as Internet e-commence, that communication entities do not need to know each other prior to the communication.

3. PROPOSED APPROACH

The entities involved in the digital certificate application are:

a) Certificate Authority (CA): CA is the person or organization that digitally signs a statement. The X.509 public-key digital certificate contains a statement, including the user's public key, and a digital signature of the statement. The difference between the GDC and the existing public-key digital certificate is that in a GDC, the public information does not contain any user's public key, which helps the easier management of the certificate.

b) Owner of a GDC: The owner of the GDC is the person who receives the certificate from a trusted CA over a secure channel. The owner needs to compute a valid response to the verifier's challenge in order to be authenticated and establish a secret session key.

c) Verifier: The verifier is the person who challenges the owner of a GDC and validates the answer using the owner's public information.

With this scheme, the owner of a GDC never needs to reveal the digital signature of the GDC in plaintext to the verifier under any circumstances. Instead, the owner proves that he has knowledge of the digital signature by generating the correct response to the verifier's challenge.

The proposed protocol should satisfy the following security requirements.

1) **Unforgeability**: A valid response can only be generated by the certificate owner who knows the digital signature of the Gneralized Digital Certificate.

2) **One-wayness**: No other person can derive the digital signature of the certificate based on any interaction.

3) **Nontransferrability**: A response to a verifier's challenge cannot be transferred into a response to another verifier's challenge, which would otherwise create impersonation of the user.

This work specifies the method for using this concept in discrete logarithm based protocol, with mechanism for efficient secure communication. This is built on the combination of traditional DL-based protocol and Diffie – Hellman Assumption. The proposed approach has mainly three phases :Registration phase, User Authentication phase and Key Establishment Phase.

3.1 Registration phase

Let A be the certificate owner and B be the verifier. To obtain a GDC, A needs to register at a CA. The CA uses the ElGamal Signature[4] concept to generate the signature for user A's message. The ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms. . It helps the verifier to confirm the authenticity of a message m sent by the signer to him over an insecure channel.

The user sends the information from any one of digital certificates like birth certificate, digital Identity cards etc to the CA and CA generates the digital certificate using ElGamal Signature scheme. In ElGamal scheme, a large prime p and a generator g in the order of $p-1$ are supposed to be shared by all the users. The signer selects a random private key $x \in [1, p-2]$ and computes the corresponding public key

$$y = g^x \bmod p$$

The signer randomly selects a secret parameter $k \in [1, p-1]$ with $\gcd(k, p-1) = 1$ and computes

$$r = g^k \bmod p$$

Then, s is solved by knowing the signer's secrets, x and k, as

$$m = ks + rx \bmod p - 1$$

where m represents the message digest of the message m'. (r, s) is defined as the digital signature of the message m'. The signature component s is a function of the statement. Each owner needs to keep it secret from the verifier in the authentication process. The signature (r, s) can be verified by checking whether the equation

$$g^m = y^r r^s \bmod p$$

holds true.

3.2 User authentication phase

If user wants to obtain service from any service provider, provider must ensure that the user is the right one. For this, in user authentication phase the following operations are performed.

Step 1: User will not directly reveal the signature component s to the verifier.

The user A passes his user information m'_A and parameters (r, S) to the verifier B, where

$$S = r^s \bmod p$$

Step 2: After receiving m'_A and (r, S), the verifier checks whether

$$g^{mA} = y^r S \bmod p$$

where y is the public key of the CA. If this equality holds true, the verifier B randomly selects an integer $vB \in [1, p-2]$ and computes a challenge

$$c_B = r^{vB} \mod p$$

and send c_B to the user A. Otherwise, the user authentication fails and the protocol is stopped.

Step 3: The user A first uses his secret s to compute the Diffie-Hellman secret key

$$K_{A,B} = C_B{}^{s} \mod p$$
$$K'_{A,B} = D(K_{A,B})$$

where $D(K_{A,B})$ represents a key derivation procedure with $K_{A,B}$ as an input. This key derivation procedure also enforce security to the authentication process. Then user A randomly selects an integer $v_A \in [1, p-2]$ and computes

$$C_A = r^{vA} \mod p.$$

After that the response is calculated as

$$Ack = h(K'_{A,B}\ C_B \| C_A),$$

where $h(K'_{A,B}\ C_B \| C_A)$ represents a one-way hash function using the key $K'_{A,B}$. The user A sends Ack and C_A back to B and waits for the response from verifier.

Step 4: After receiving the Ack and C_A from the user A, the verifier B uses his secret v_B to compute the secret key using the Diffie-Hellman concept.

$$K_{B,A} = S^{VB} \mod p$$

And this key is given as input to the key derivation procedure and computes $K'_{B,A}$ as

$$K'_{B,A} = D(K_{B,A})$$

then computes

$$h(K'_{B,A}\ C_B \| C_A)$$

and checks whether $h(K'_{B,A}\ C_B \| C_A)$= Ack is true. If this condition holds, verifier confirms that user is authenticated. Then user and verifier enters into the key establishment phase.

3.3 Key establishment phase

In this phase, user and verifier establishes symmetric secret key for securing further communication. On the user side, the key established is:

$$K_1 = C_B{}^{vA} \mod p$$

where vA is the secret of user A and C_B is the challenge from verifier B. On the verifier side, the key established is:

$$K_2 = C_A{}^{vB} \mod p$$

where vB is the secret of Verifier B and C_A is the challenge from User A. The established secret key on both side are symmetric:

$$K_1 = C_B{}^{vA} \mod p = r_A{}^{vAvB} \mod p$$
$$K_2 = C_A{}^{vB} \mod p = r_A{}^{vBvA} \mod p = K_1$$

For the further communication between the parties this established secret key is used for encryption and decryption of the message. But if same key is used for encrypting the whole messages in the session, attacker who continuously monitor the system may got an idea about the secret key established between the partners. So for communicating the highly confidential messages, the key can be changed for each messages as follows.

For encrypting the first message, the established key itself is used. For the second message, the key is generated by XORing the first required bits of previous message with first same number of bits of the previous key. Similarly keys for all further communication can be generated.

$$K1 = r_A{}^{vAvB} \mod p$$
$$K2 = K1 \text{ XOR } m1$$
$$K3 = K2 \text{ XOR } m2$$

where k1,k2etc represents first 16 bits of corresponding key and m1,m2 represents first 16 bitsof message.This concepts guarantees high security to the communication between the partners.

3.4 Security analysis and discussions

In this section, the unforgeability, one-wayness and nontransferability of the proposed user authentication and key establishment protocol is analysed. To perform a forgery attack, the attacker needs to send a valid pair (r, S) in step 1) and the corresponding Ack in step 3) in order to impersonate the certificate owner effectively. A valid pair (r, S) alone in step 1) cannot be used to authenticate the certificate owner since this pair of parameters can be easily solved by the attacker from the following equation

$$g^{mA} = y^r S \mod p$$

But, it is computationally infeasible for the attacker to find the discrete logarithm of because of the security of ElGamal signature scheme. Therefore, it is computationally infeasible for the attacker to get a pair (r, s) to satisfy

$$g^{mA} = y^r r_A \mod p$$

Due to the Diffie-Helman Assumption, without knowing the secret exponent of S, it would be infeasible for the attacker to compute the key K_A, and forge a valid response Ack in step 3.But, the certificate owner obtains the secret exponent of S from CA during the registration phase and the certificate owner can be authenticated successfully in step 3). In summary, the security of the unforgeability of the proposed protocol is provided through the security of ElGamal signature scheme and the DHA. So, the proposed protocol is secure against forgery attacks. The computation of s from S is infeasible since it is a discrete logarithm problem.In step 3, the user uses the secret to compute the Diffie-Hellman key $K_{A,B}$. Although the verifier knows the Diffie-Hellman key K_A; but due to the DHA, the verifier will never obtain the secret s. Therefore, the proposed protocol satisfies the one-wayness property. A valid response Ack can only be generated by the certificate owner, who knows the secret signature component s.But the digital signature of GDC is never passed to the

verifier, the verifier cannot pass the complete GDC to any third party, whether which is possible with X509 public key digital certificate. So, a valid response *Ack* cannot be transferred into a response of another verifier's challenge. Therefore, the proposed protocol ensures non-transferability. Since the secret key established between the communication parties can be changed for each message, using the proposed method confidential messages can be securely communicated through the network.

4. CONCLUSION

The concept of GDC that can be used to provide user authentication and key agreement is proposed. A GDC contains user's public information, such as the information from user's digital driver's license, passport, digital birth certificate, etc., and a digital signature of the public information signed by a trusted certificate authority(CA). Since GDC does not contain any user's public key, it is easier to manage than X509 public key digital certificate. The digital signature of the GDC is used as secret token of each user that will never revealed to any verifier in any context. Instead, the owner proves to the verifier that he has the knowledge of the signature by responding with valid acknowledgement to the verifier's challenge. The secret key established during these communication can be used for securely transmitting the further messages.

5. REFERENCES

[1] L. Harn and J. Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", IEEE trans. on Wireless Communications, vol.10, pp. 2372-2379, 2011.

[2] Network Working Group, "Internet X.509 public key infrastructure certificate and crl profile, RFC: 2459," Jan. 1999.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology: Proc. Crypto'84, Lecture Notes in Computer Science vol. 196, (Berlin), pp. 47- 53, Springer-Verlag, 1985.

[4] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete loarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469-472, 1985.

[5] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discret logarithm," Electron. Lett., vol. 30, no. 24, pp. 2025-2026, 1994.

[6] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. Assoc. Comp. March., vol. 21, no. 2, pp. 120-126, 1978.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 400 - 408, 2013, ISSN: 2319–8656

M Payment Prototype for Mobile Bill Payment System

Jimoh, R. G.
Dept. of Computer Science
University of Ilorin, Nigeria

COCO, K. B
Dept. of Computer Science
University of Ilorin, Nigeria

OLUOBO, Abdel, M. F. O.
Department of Computer Science
University of Ilorin

Abdulsalam, S. O
Dept. of Computer, Library & Info. Science
Kwara State University, Malete, Nigeria

Isiaka, R. M.
Dept. of Computer, Library & Info. Science
Kwara State University, Malete, Nigeria

Abstract: Mobile devices and wireless technologies have come to make a great impact on our lives. Mobile devices have been widely used in the last few years which have led to the e-revolution. This suggests the electronic mode of payment in sustaining the new innovations. The manual payment system has been revealed to be associated with a numbers of problems such as fatigue of standing in long queue, human error, forgery and lots more. This made a number of authors to have suggested electronic payment system with proven advantage in terms of accuracy, speed, cost and security. The Electricity Holding Company of Benin Republic (EHCB) is currently facing a lot of challenges using manual payment system which has made the stakeholders in company to suggest mobile payment system as an alternative. This informs the aim of the researcher to develop an m-payment prototype for EHCB and confirm its usability. The prototype was developed based on prototyping model using WINDEV while the usability was tested using an adapted survey questionnaire with ten metrics. It was discovered that the developed m-payment prototype for Electricity Holding Company of Benin Republic is usable.

Key words*: WINDEV, M-payment, E-revolution, Prototype and EHCB.*

1. INTRODUCTION

A mobile payment or m-payment may be defined as any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services [1]. Mobile devices may include mobile phones, PDAs, wireless tablets and any other device that connect to mobile telecommunication network and make it possible for payments to be made [3].

In recent years, mobile and wireless technologies have been a hot topic [9]. Many mobile and wireless applications developments are still going on [8]. Instead of paying with cash, cheque or credit cards, a consumer can use a mobile phone to pay for a wide range of services. Consumers and mobile industry representatives are looking forward to the third generation (3G) of mobile phones, one that promises higher quality services to consumers. There are already more than 6 billion mobile subscribers worldwide [2]. This rapid growth has made a mobile phone to provide extra functions and services like bill payment. Consumers are using their mobile phones not only as voice communication tools but also as multi-function tools that can send SMS, play games, and perform other functions.
Mobile payment represents another opportunity for the mobile industry and financial service companies [6]. Perhaps, in the near future, it will be a service that is demanded by consumers [6]. Imagine it is the last date of bill payment and you are stuck in an unavoidable meeting; imagine standing in long queues when you could be having fun with friends and family**.** By sending an SMS your bills are paid and payment is really just a click away.

This research work is particularly to achieve electricity bill payment system via mobile phone. The responsibility of EHCB is to supply electricity to their numerous customers. It is desirable in this work to examine the potential technologies for mobile payments systems and to also identify the opportunities and issues for mobile payments with respect to EHCB.

2. PROBLEM STATEMENT

There are a number of challenges facing the manual payment system. This approach is not effective in solving the perennial problem like bill distribution, billing and cash collection [4]. According to the source, the following could be identified as major shortcomings of a manual payment system:

1. Time consuming
2. Lack of real time information storage
3. Lack of prompt updating
4. Possibility of human error
5. Lack of accurate and prompt reports
6. Possibility of data duplication

The aforementioned shortcomings among others serve as the justification for migrating from manual bill payment system to the proposed mobile bill payment system in

Electricity Holding Company of Benin Republic (EHCB). It is equally revealed that, it is not all about developing mobile payment system but also ensuring the usability of such a system [3]. The need for m-payment system at EHCB was equally revealed by the stakeholders of the company [7].

3. RESEARCH QUESTIONS AND OBJECTIVES

In addressing the research problem, the following research questions are required to be answered:

1. How can mobile bill payment prototype for EHCB be developed?
2. What is the usability of the developed mobile bill payment prototype for EHCB?

The main objective of this study is to develop mobile billing application that will allow registered customers of Electricity Holding Company of Benin Republic (EHCB) to pay their bill. In achieving this main objective; the following specific objectives are thereby formulated:

1. To develop a mobile bill payment prototype for EHCB
2. To evaluate the usability of the prototype developed.

A mobile phone user communicates with a merchant and makes an economic transaction. The merchant obtains the phone number of the customer and initiates the m-payment transaction request stating the amount for which payment is required. The customer confirms the request and authorizes payment. The Mobile Application Service Provider (MASP) receives the authorization and verifies the authenticity of the customer. The MASP then debits the customer account and credits the merchant account by interacting with the bank. Once the electronic funds transfer is successful a confirmation message is sent to the customer and the merchant advising them of the debit and credit respectively. The Certifying Authority shown in Figure 1 supplies digital certificates for the users in the system to provide security. This model can be extended to handle the interaction between the MASP and the financial system taking into account inter-bank payments and settlement. This study is guided by the generic Model for M-Payments Application Service Provider as described in Figure 1.

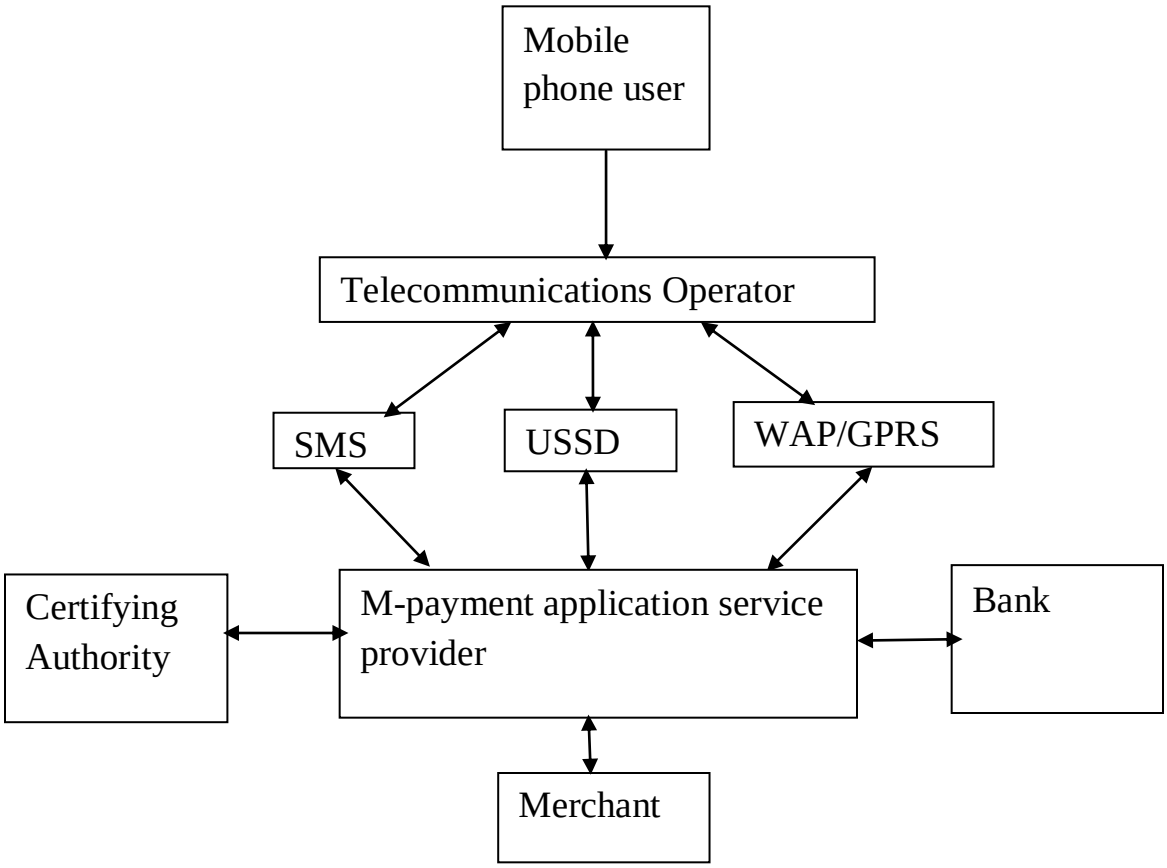


Figure 1: A Generic Model for M-Payments Application Service Provider

Prototyping approach is employed in this study due to its many advantages as follows:

1. **Reduced time and costs**: Prototyping can improve the quality of requirements and specifications provided to developers. Because changes cost exponentially more to implement as they are detected later in development, the early determination of what the user really wants can result in faster and less expensive software.

2. **Improved and increased user involvement**: Prototyping requires user involvement and allows them to see and interact with a prototype allowing them to provide better and more complete feedback and specifications. The presence of the prototype being examined by the user prevents many misunderstandings and miscommunications that occur when each side believe the other understands what they said. Since users know the problem domain better than anyone on the development team does, increased interaction can result in final product that has greater tangible and intangible quality. The final product is more likely to satisfy the users desire for look, feel and performance.

4. UML DIAGRAMS OF THE PROPOSED SYSTEM

The Class Diagram shows the class definition and relations, also depicts interfaces within the design of your system as described in Figure 2. Customer can possess one or more meters, nevertheless more than one customer cannot be linked with the same meter. In the same vein, the account of a meter can be detailed in more than one bill; however, one bill cannot detail the account of two meters. Figure 3 describes the Use Cases Diagram of the system. An Activity Diagram depicts the detailed behavior inside a single functional requirement; it shows an elaboration of the behavior of the system as shown in Figure 4. A Sequence Diagram depicts the detailed behavior over time within one path or scenario of a single functional requirement. It is useful for understanding the flow of messages between elements of the system; it shows object interactions over time as shown with Figure 5.

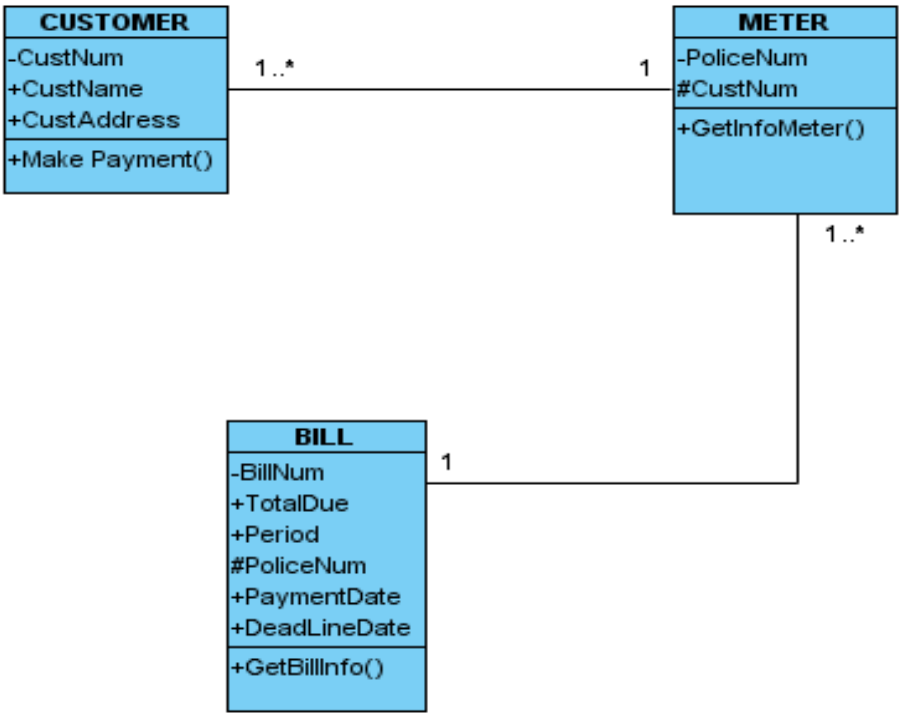


Figure 2: Class Diagram of the Proposed System

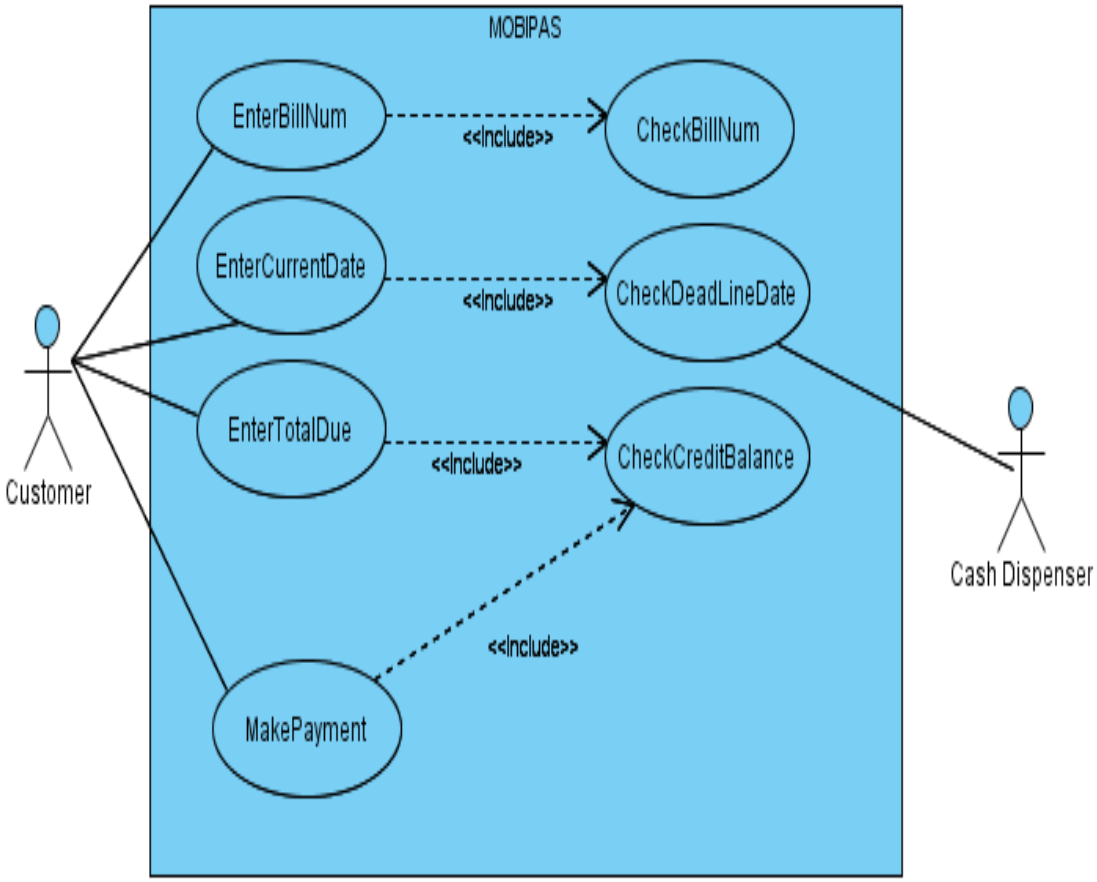


Figure 3: Use Case Diagram of the Proposed System

Volume 2– Issue 4, 400 – 408, 2013, ISSN: 2319–8656

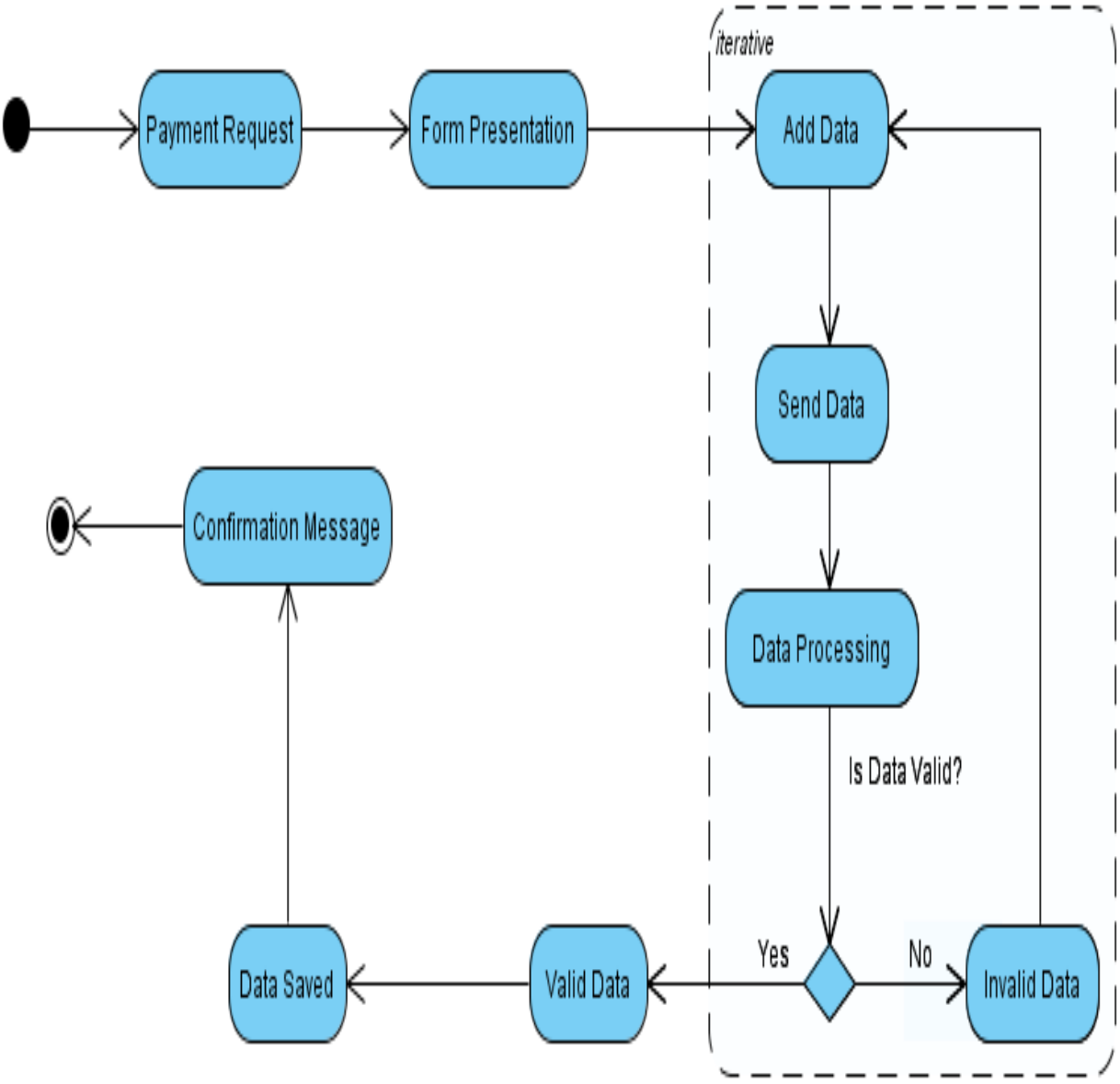


Figure 4: Activity Diagram of the Proposed System

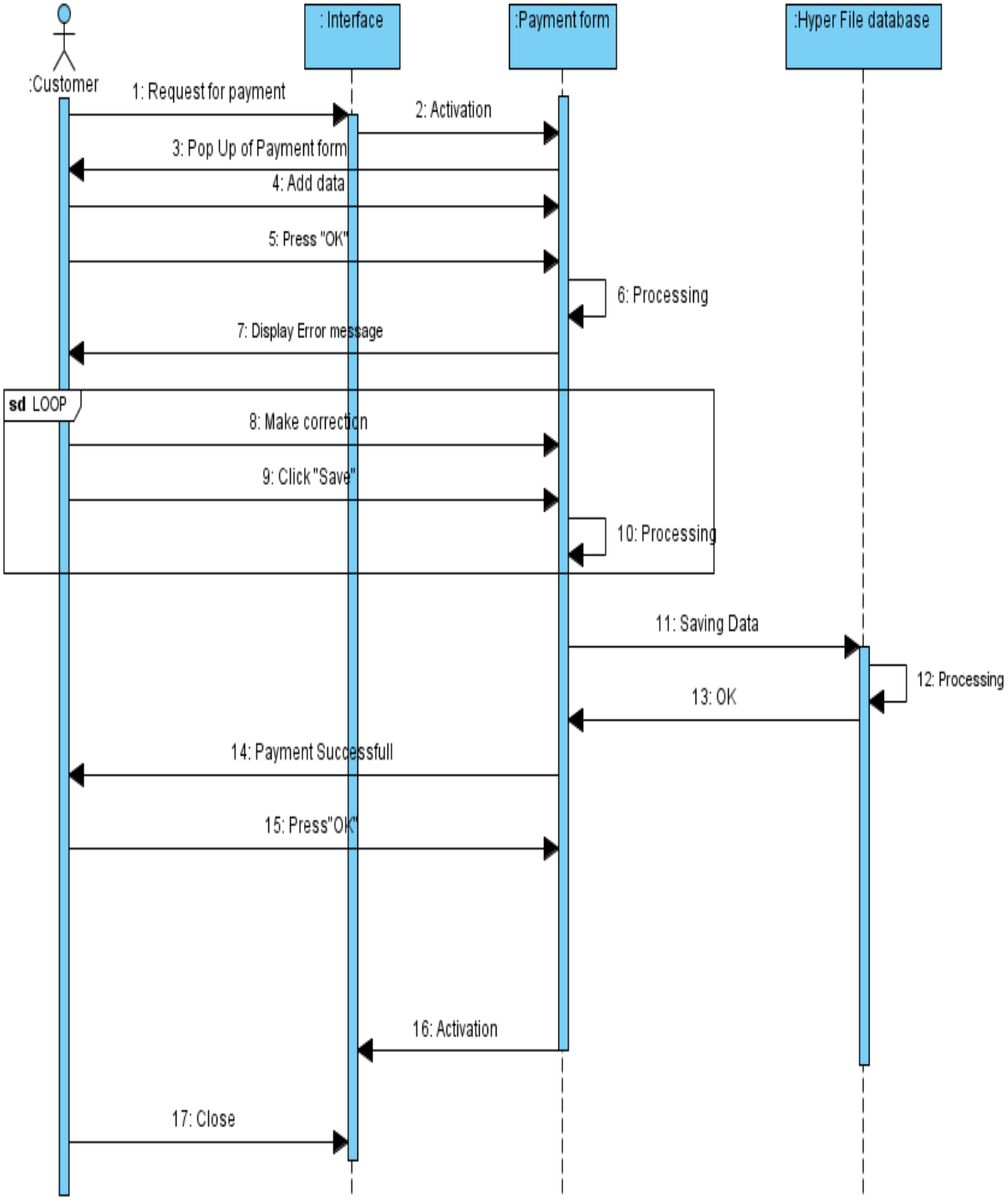


Figure 5: Sequence Diagram of the Proposed System

5. USABILITY TESTING

The usability of the developed prototype is evaluated using the items from the usability evaluation questionnaire developed by [5] which was adopted in this study. The questionnaire consists of 10 questions which covers software system metrics like simplicity of dialogue, clarity of language, memory load, consistency, feedback mechanism, clear point of exit, shortcut facilities, clear error messages, minimal error, adequate help and documentation. The items contained in the questionnaire are described in Tables 1 to 10 as follows:

6. USABILITY RESULT

Table 1: MPUQ1 (Simplicity of Dialogue)

		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	1	100,0%	5	62,5%	4	36,4%
	2	0	,0%	3	37,5%	7	63,6%
	Combined	1	100,0%	8	100,0%	11	100,0%

The result of usability testing shows that the language used is clear and unambiguous as shown in Table 2 with more 80% of respondents agreeing to the fact that the dialogue of the prototype is simple.

Table 2: MPUQ2 (Clarity of Language)

		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	1	100,0%	7	58,3%	2	28,6%
	2	0	,0%	5	41,7%	5	71,4%
	Combined	1	100,0%	12	100,0%	7	100,0%

The usability testing reveals that the prototype is of acceptable memory load as can be seen from Table 3.

Based on the metrics used to measure system reliability which include simplicity of dialogue, clarity of language, memory load, consistency, feedback mechanism, clear point of exit, shortcut facilities, clear error messages, minimal error, adequate help and documentation, analysis of data collected from users of the prototype gives the following results. The results as shown from Tables 1 to 10 show that positive indication of all observed metrics as majority of the respondents fall between Agree and Strongly Agree. The result of the usability testing shows that the prototype is perceived simple to use with more than 90% of sample respondent on the agreement side as shown in Table 1.

Table 3: MPUQ3 (Memory Load)

		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	3	100,0%	5	38,5%	2	50,0%
	2	0	,0%	8	61,5%	2	50,0%
	Combined	3	100,0%	13	100,0%	4	100,0%

The developed prototype is perceived to be consistent with over 70% of respondents on the agreement side as shown in Table 4.

Table 4: MPUQ4 (Consistency)

		Strongly Disagree		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	2	100,0%	3	100,0%	3	23,1%	2	100,0%
	2	0	,0%	0	,0%	10	76,9%	0	,0%
	Combined	2	100,0%	3	100,0%	13	100,0%	2	100,0%

The result of the usability testing shows that the feedback mechanism in the prototype is acceptable with 50% of the sample respondent on the agreement side of the Table 5.

Table 5: MPUQ5 (Feedback Mechanism)

		Strongly Disagree		Disagree		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	3	100,0%	3	100,0%	3	75,0%	1	11,1%	0	,0%
	2	0	,0%	0	,0%	1	25,0%	8	88,9%	1	100,0%
	Combined	3	100,0%	3	100,0%	4	100,0%	9	100,0%	1	100,0%

The developed prototype is perceived to have a clear point of exit with more than 75% of the sample respondents on the agreement side as shown in Table 6.

Table 6: MPUQ6 (Clear point of exit)

		Disagree		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	0	,0%	1	25,0%	5	100,0%	4	40,0%
	2	1	100,0%	3	75,0%	0	,0%	6	60,0%
	Combined	1	100,0%	4	100,0%	5	100,0%	10	100,0%

The result of the usability testing shows that the sample respondents perceive the shortcut facilities with more than 50% of the respondents on the agreement side as shown in Table 7.

Table 7: MPUQ7 (Shortcut Facilities)

		Strongly Disagree		Disagree		Undicided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	1	100,0%	5	71,4%	0	,0%	2	100,0%	2	100,0%
	2	0	,0%	2	28,6%	8	100,0%	0	,0%	0	,0%
	Combined	1	100,0%	2	100,0%	3	100,0%	8	100,0%	6	100,0%

The developed prototype is perceived to have a good error trap system with more than 80% of the respondents on the agreement side as shown in Table 8.

Table 8: MPUQ8 (Clear error message)

		Disagree		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	1	100,0%	2	100,0%	1	12,5%	6	66,7%
	2	0	,0%	0	,0%	7	87,5%	3	33,3%
	Combined	1	100,0%	2	100,0%	8	100,0%	9	100,0%

The developed prototype is perceived to have minimal error with the 50% of the sample respondents on the agreement side depicted in Table 9.

Table 9: MPUQ9 (Minimal error)

		Disagree		Undecided		Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	3	100,0%	1	14,3%	6	60,0%
	2	0	,0%	6	85,7%	4	40,0%
	Combined	3	100,0%	7	100,0%	10	100,0%

The developed prototype is perceived to have an average help and documentation facility with 60% of the sample respondents on the agreement side as can be seen on Table 10

Table 10: MPUQ10 (Help and documentation)

		Strongly Disagree		Disagree		Undecided		Agree		Strongly Agree	
		Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Cluster	1	2	33,3%	4	66,7%	0	,0%	1	100,0%	3	100,0%
	2	4	66,7%	2	33,3%	4	100,0%	0	,0%	0	,0%
	Combined	6	100,0%	6	100,0%	4	100,0%	1	100,0%	3	100,0%

7. DISCUSSION

There is no doubt that the beauty of Information Technology has brought about electronic revolution in virtually all aspects of human endeavor. Electronic payment system is not left out in this regard. This study

aimed at suggesting a usable m-payment prototype for Electricity Holding Company of Benin Republic having identified the need for such innovation both locally and globally. In achieving the goal of the study, extensive literature review was carried out to justify the required research effort. Various software development methodologies were also reviewed. It was discovered that, prototyping model is more suitable for this work. The system requirement was specified using use case diagram and class diagram. The usability of the prototype was tested using the survey questionnaire of [5] with ten software usability metrics which includes simplicity of dialogue, clarity of language, memory load, consistency, feedback mechanism, clear point of exit, shortcut facilities, clear error messages, minimal error, adequate help and documentation. The results show that the developed prototype is perceived to be usable based on these metrics.

8. CONCLUSION

The introduction of Information Technology (IT) has introduced ubiquitous way of transacting businesses. This cannot be achieved without making the payment system also ubiquitous. Since mobile payments services provide an attractive, simple and rapid payment channel for users, it is therefore concluded that such payment medium poses a promising future for the emerging ICT-driven transactions. but still lack the proper regulations and standardization with associated are numerous challenges to be overcome. Network operator, businesses, and consumers have to come forward and make value-producing investments for a successful implementation of mobile payments to be widely accepted as a mode of payment. If all these are properly provided, it can be concluded that m-payment system will deliver in Electricity Holding Company of Benin Republic. It is advised to test this application in other different domains.

9. REFERENCES

[1] An, B., & Papavassiliou, S. (2001). A mobility-based clustering approach to support mobility management and multicast routing in mobile ad-hoc wireless networks. International Journal of Network Management, 11 (6), 387-395.

[2] ITU (2011). Global mobile statistic 2011 part A. Retrieved February 02, 2012 from mobilethinking.mobi/mobile-marketing-tools/latest-stats/a#subscribers

[3] Karnouskos, S., & Fokus, F. (2004). Mobile Payment: a journey through existing procedures and standardization initiatives. IEEE Communications Surveys and Tutorials, 6(4), 44-66.

[4] Mansi, C. ,Namita, K. , & Avanish, C. (2009). Hospital Management System project (Masters dissertation Rajasthan Technical University, Kota, 2009). Retrieved April, 10, 2012 from http://www.paombomghealthcare.googlecode.com?

[5] Nelson, J. (1993). Usability Engineering Academic press Chapter 5, p 115. NFC Adoption Will Be Slower Than Expected.(n.d). About NFC Adoption. Retrieved October 5, 2011 from http://www.rfidupdate.com/articles/index.php?id=1554

[6] Senn, J. A. (2000). The Emergence of M-commerce. Computer, 33(12), 148-150.

[7] Société Bénioise d'Energie Electrique (2011). Retrieved January 10, 2012 from www.africa-oil-gas/sbee_(societe_beninoise_d'energie_electrique)-1278-1-2-art.html

[8] Varshney, U. , & Vetter, R.(2000). Emerging mobile and wireless networks. Communications of the ACM, 43 (6), 73-81.

[9] Varshney, U. , & Vetter, R. (2002). Mobile commerce: framework, application and networking support. Mobile Networks and Applications, 7(3), 185-198.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 409 - 414, 2013, ISSN: 2319–8656

DESIGN OF MOBILE SHORT MESSAGE SERVICE (SMS) ACROSS A COMPUTER NETWORK FOR ORGANISATIONAL COMMUNICATION

Jimoh, R. G.
Dept. of Computer Science
University of Ilorin, Nigeria

COCO, K. B
Dept. of Computer Science
University of Ilorin, Nigeria

OLUOBO, Abdel, M. F. O.
Department of Computer Science
University of Ilorin

Abdulsalam, S. O
Dept. of Computer, Library & Info. Science
Kwara State University, Malete, Nigeria

Isiaka, R. M.
Dept. of Computer, Library & Info. Science
Kwara State University, Malete, Nigeria

Abstract: Short Message Service (SMS) is the most powerful tool in terms of communication especially for mobile users. It does not limit anyone regardless of high- or low-end mobile phones for as long as they can receive and send messages anytime, anywhere. It was revealed that, lack of adequate communication technology in an organization leads to a number of issues that make such organization to perform less. In order to fully utilize the mobile phones, this study has come up with a fast way where users can get information quickly without spending more. This study aimed to promote access to such information through the use of Short Message Service (SMS) and improve transparency, reliability, usability of the information for organization. The proposed SMS application will provide multi level local authentication to the SMS gateway service. The application was developed based on the Unified Software Development Process or in short, the Unified Process being a components-based system. The programming languages used are PHP and JAVA. The resulting SMS application is found to be usable and economical.

Keywords: SMS, SMS gateway, Transparency, Reliability, Usability.

1. INTRODUCTION

The Short Message Service (SMS) allows textual messages to be delivered between SMS enabled and digital cell phones from a computer network. These messages travel on the network in tandem with voice call signaling traffic. The service is extremely popular in Europe and Asia, generating tens of billions of messages a month. A number of factors hindered initial SMS acceptance in the United States, but traffic has grown remarkably in the last two years, and this trend is expected to continue [3]. SMS has also demonstrated to be a reliable alternative to voice communications, during the terrorist attacks on September 11, 2001. High traffic volumes made it extremely difficult to connect people on calls; however, SMS text messaging continued to operate and provide communication means for people who understand how to use it [3].

The conflux of these events raises the question: given that SMS shares the network, that popularity and awareness of SMS are increasing rapidly, and that SMS might be a person's means of communications during another crisis, how would the wireless network handle the surge in short messaging traffic? [7]. This question was answered by wireless network reliability, capacity and congestion handling, security and vulnerability, priority services, and new SMS-related developments. It was then concluded that networks are theoretically capable of continued operation and service (including NS/EP service) during a crisis [7]. However, it may be possible for extremely high volumes of SMS traffic, when combined with high numbers of voice call attempts, to interfere with a wireless network's performance. The absence of a definitive conclusion is due to the unavailability of key information: the network configuration details (known only by the network operator), the congestion handling algorithms (known only by the equipment manufacturers). Organizations today are facing several unique communication challenges: the proliferation of electronic messages across their enterprise; the need to provide employees, customers, and partners with consistent information; the desire to better equip information workers with meaningful information to drive informed decisions; and the mandate to control costs without sacrificing application availability, security, or reliability [5]. Popularity, will impact the future load on SS7 [3]. This Technical Information Bulletin (TIB) addresses two major SMS Markets; the United States and Europe. In Great Britain alone, over 68 million short messages were sent on Valentine's Day, 2003. In Europe, 10 billion messages are sent each month. In the United States, SMS traffic has increased tremendously to today where hundreds of millions of short messages are sent each month. The goal TIB is to:

1. Perform an analysis of the vulnerability of SS7 to a huge increase in Short Messaging Service (SMS) traffic.

2. Examine the state-of-the-art of SMS applications in the PSN environment.
3. Examine the security aspects of employing SMS in an NS/EP environment.
4. Provide an analysis of future developments in SMS and transmission media other than PSN.

TIB includes:

- A description of the SMS technology.
- Capacity and load analysis for high traffic volume situations.
- Security issues of using SMS in the PSN and other media.

All these features among others are captured in this work.

2. PROBLEM STATEMENT

It is generally believed that information is power. At the same time, useful information cannot be gathered without effective communication. Efforts on effective communication strategy should therefore be continuous. SMS has become an alternative to voice communication as it has been revealed by previous authors that, a number of factors can hinder effectiveness of the voice communication method [7]. It was revealed that, lack of adequate communication technology in an organization leads to a number of issues that make such organization to perform less [5]. The researcher is interested in filling this gap by proposing a usable mobile SMS for organizational communication.

3. RESEARCH QUESTIONS AND OBJECTIVES

1. What are the previous SMS-based communication strategies?
2. How can a mobile SMS-based communication prototype be developed?

The aim of this research work is to produce a useful program that takes care of mobile short message service (SMS) for organizational communication. In achieving this central objective, the following specific objectives are formulated:

1. To review existing SMS communication strategies
2. To design and develop SMS approach as a means of communication in an organization

4. SOFTWARE DEVELOPMENT APPROACH USED

The software development approach used in this research work is the Unified Software Development Process or simply put, the Unified Process (USDP). USDP was used because it is a component-based process which allows various components making up the system to be linked together through a well defined interface. Information systems are embedded in an organizational context. As the organization surrounding the system evolves, new requirements emerge. The implementation of a new system can also transform the usage context and therefore new requirements arise [2].The evolutionary prototyping approach results in the gradual development of systems and allows for, or adapts to, changes that take place within an organization as a result of either the operationalisation of the system, or externally induced changes to the organization [4].In contexts of high uncertainty (and unlike contexts with high certainty where waterfall models are employed), the evolutionary prototyping approach dynamically responds to changes in user needs and accommodates subsequent unpredictable changes in requirements, as the development process progresses [6].

[2] identifies incremental development and evolutionary system development as two distinct approaches that employ prototypes. During incremental development the system evolves gradually in partial increments against the backdrop of an overall long range development strategy. The fundamental difference between evolutionary development and incremental development is in system design; while software design evolves in evolutionary development, there are no changes to the design during incremental development [4]. Whilst incremental development assumes that most user needs are known at the beginning, in evolutionary system development, the prototype is built in an area where overall the requirements are not well understood [1]. Initial development, however, starts in an area where the requirements are known. USDP allows all this components making up a system to be well represented using a Unified Modeling Language. In fact, The Unified Process uses Unified Modeling Language (UML) in preparation of blueprints for the software.

Unified Process is more than a single process; it is a generic process framework that can be used for a very large class of software systems, for different application areas, different types of organizations, different competence levels and different project sizes. The Unified Process is component-based which implies that the software system being built is made up of software components interconnected via well-defined interfaces as described in Figure 1.

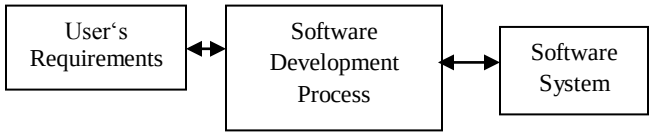


Figure 1: Software Development Process.

5. SYSTEM ARCHITECTURE

Figure 2 describes the system architecture of the proposed SMS system. The components developed by team members are in the rectangular with dash line.

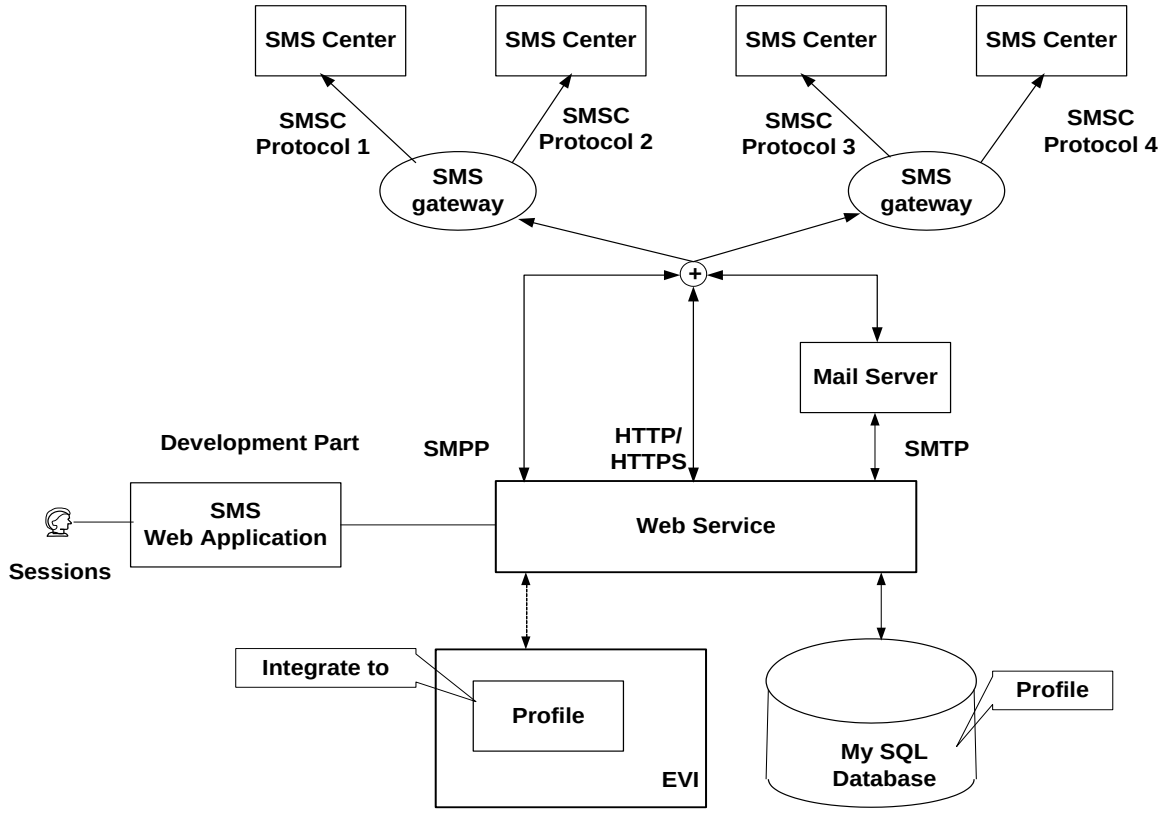


Figure 2: SMS Spot Application Architecture

The application contains seven main components. Its functions are described as follows:

1. Web Browser: Running on client-side, it allows users log in and send SMS messages.
2. Web Service: Provide the service for gateway and SMS application to send and receive SMS messages under JAXWS
3. EVI (Enterprise Voice Integration) profile: contain the information of customers. Based on this information, the web application can determine the route and protocol for transferring a message.
4. Web Application: Running in the server-side, it handles requests from SMS users for sending and receiving SMS message. Beside, the web application can get the information from EVI profile or database, and then it decides the route and the protocol that it uses to send the SMS message. This is the server side component to be built by the project.
5. SMS Gateway: an SMS gateway can be set up to handle the connections to the SMSCs. To connect to an SMS gateway, an SMSC protocol is used such as SMPP, HTTP/HTTPS, email to SMS, etc.
6. SMS Center: A SMS center (SMSC) is responsible for handling the SMS operations of a wireless network. When an SMS message is sent from a mobile phone, it will reach an SMS center first. The SMS center then forwards the SMS message towards the destination.
7. Mail Server: Provide SMTP service to send SMS messages to the mail system of the mobile phone carriers and a mailbox to receive the SMS message sent from mobile phones.

6. USE CASE DIAGRAM OF THE PROPOSED SYSTEM

Use Case diagram of the application is shown in Figure 3. It contains three actors which are User, Administrator and Mobile and the functions performed by these actors

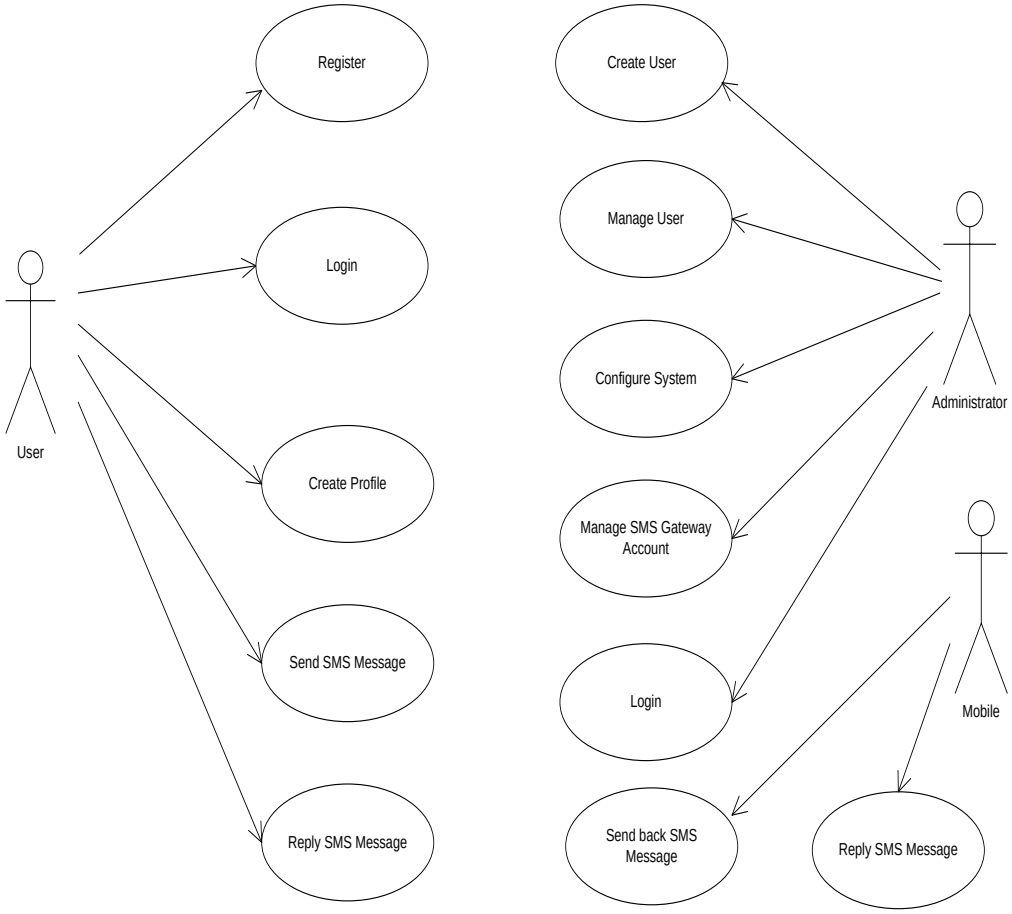


Figure 3 SMS Live Spot Use Case Diagram

7. CLASS DIAGRAM OF THE PROPOSED SYSTEM

The Database includes four tables which are Message, Contact, Group and GroupDetail to provide complete information to users and they are stored in MySQL database management system as shown in Figure 4. Message table: is identified by MessageID and contains information such as messagetype, subject, content, sender, date and userID. This table is used to store all the messages sent back and forth by users. Contact table is identified by UserID and contains information such as Username, password, firstname, lastname, address, homephone, cellphone and servprovider. This table is used to store the contact or recipient information that user want to send messages to. Group table is identified by userID, groupID and contains information such as group name, description. This table is used to store group of contact or recipient information that user want to send messages to. GroupDetail table is identified by userID, groupID. This table is used to provide detail information of the corresponding group.

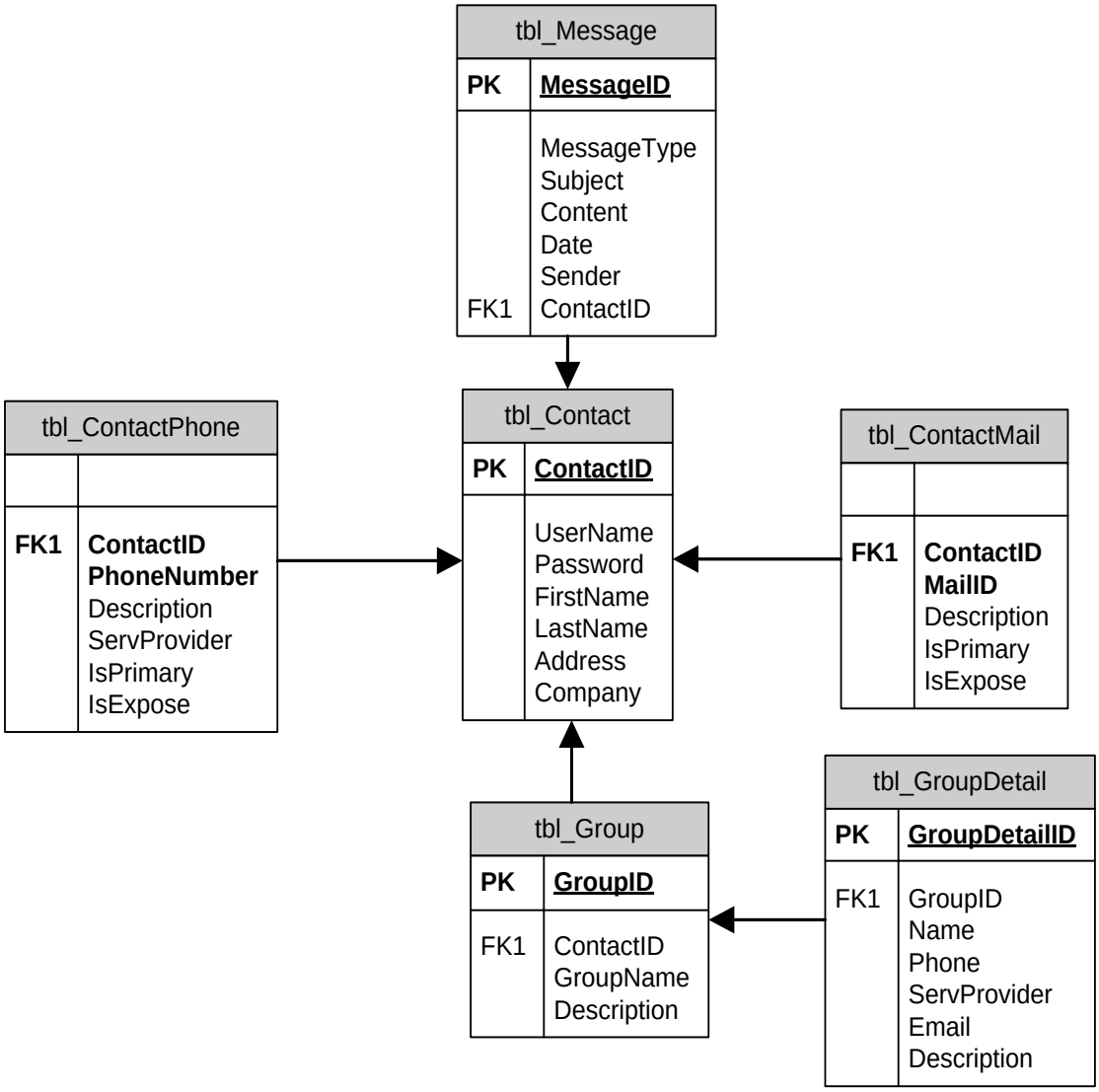


Figure 4: Class Diagram

8. DISCUSSION

The following prototype is developed based on the design described earlier and the usability of the developed prototype was also confirmed. Communication is very essential in virtually every organization. The emerging knowledge-driven organization places communication more prominently in achieving the objectives of such organization. Communication takes place at every stage in an organization. Various efforts have been made in making communication experience within an organization an interesting one. This work is contributing in this direction by proposing a mobile SMS across a computer network for a communication platform and also provides such service at almost free rate since it is across the network. The proposed communication medium is devoid of all barriers associated with communication using ICT as long as the mobile phone is on. This will assist the emerging knowledge-driven organizations in achieving their objectives with prompt and easy access to information.

9. CONCLUSION

Communication has become the life wire of any organization, most especially in this information age. Effectiveness of this communication depends on the reliability of the medium used. With due consideration to all design issues of a typical SMS services, the proposed SMS system has been validated to be reliable in terms of its capacity, Signaling Network Reliability, Signaling Path Reliability, Cost, Security and Privacy. It can therefore be concluded that the SMS system is capable of delivering effective communication within the organization. It is one thing to propose a communication medium, it is another thing for it to be affordable enough in terms of the cost since most organizations have the business initiative of saving cost. The proposed system is found to be suitable in this regards. From the past literature reviewed, it can be seen that, research efforts on inexpensive means of communication without compromising reliability should be encouraged. It is recommended that future researchers should concentrate on ways of preventing the likely vulnerabilities to the proposed communication approach.

10. REFERENCES

[1] Davis, A., Bersoff, E.H. & Comer, E.R. (1988). A Strategy for Comparing Alternative Software Development Life Cycle Models. IEEE Transactions on Software Engineering, 14, 1453-1461.

[2] Floyd, C. (1984) .A Systematic Look at Prototyping, in: Budde, R.,Kuhlenkamp, K., Mathiassen, L. & Zullighoven, H. (Eds.) Approaches to Prototyping, Heidelberg: Springer-Verlag, 1-17.

[3] Government of Canada Office of Critical Infrastructure Protection and Emergency Preparedness. (2002). Incident Analysis: The September 11, 2001 Terrorist Attacks – Critical Infrastructure Protection Lessons Learned. Quebec: Canada Government

[4] Ince, D.C. & Hekmatpour, S. (1987) .Software Prototyping: Progress and Prospects. Information and Software Technology, 29(1), 8-14.

[5] Product Guide.(2006). Retrieved March 16, 2006, from http://www.ozeki.hu/attachement/185/Product guide 2006.03.16.pdf /ms6. p185.

[6] Pape, T.C. & Thoresen, K. (1992) .Evolutionary Prototyping in a Change Perspective. Information Technology and People, 6, 2-4.

[7] SMS over SS7-NCS. Technical Information Bulletin: National Communication System. (2003). Retrieved April 25, 2012. From http://www.ncs.gov/library/tech.../2003/tib_03-02.pdf

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 415 - 421, 2013

Stability behavior of second order neutral impulsive stochastic differential equations with delay

S. Karunanithi
Department of Mathematics,
Kongunadu Arts and Science College (Autonomous),
Coimbatore – 641 029, Tamilnadu, India

R .Maheswari
Department of Mathematics,
Sri Eshwar College of Engineering,
Coimbatore – 642 109, Tamilnadu, India

Abstract: In this article, we study the existence and asymptotic stability in pth moment of mild solutions to second order neutral stochastic partial differential equations with delay. Our method of investigating the stability of solutions is based on fixed point theorem and Lipchitz conditions being imposed.
Keywords: Stochastic, neutral, impulse, asymptotic stability, mild solution

1. INTRODUCTION

Stochastic partial differential equations have received much attention in many areas of science including physics, biology, medicine and engineering. The existence, uniqueness and asymptotic behavior of solutions of the first order stochastic partial differential equations have been considered by several authors [3, 4, 11, 12, 15, 26]. Moreover many dynamical systems not only depend on present and past states but also involve derivatives with delays. Deterministic neutral functional differential equations, which was originally introduced by Hale and Lunel [9], are of great interest in theoretical and practical applications. Kolmanovskii and Myshkis [13] introduced neutral stochastic functional differential equations and gave its applications in chemical engineering and aero elasticity considering environmental disturbances into account.

Caraballo et al. [5] have considered the exponential stability of neutral stochastic delay partial differential equations by the Lyapunov functional approach. In [7], Dauer and Mahmudov have analyzed the existence of mild solutions to semilinear neutral evolutions with nonlocal conditions by using the fractional power of operators and Kransnoselski-Schaefer type fixed point theorem. In [10], Hu and Ren have established the existence results for impulsive neutral stochastic functional integrodifferential equations with infinite delays. It is well known that classical technique applied in the study of stability is based on a stochastic version of the Lyapunov direct method. However the Lyapunov direct method has some difficulty with the theory and application to specific problems when discussing the asymptotic behaviour of solutions in stochastic differential equations [16]. It seems that new methods are required to address those difficulties.

Appleby [1] studied the almost sure stability of stochastic differential equations with fixed point approach. Luo [18, 17] have successfully applied fixed point principle to investigate the stability of mild solution of various stochastic equations. Luo and Taniguchi [19], have studied the asymptotic stability of neutral stochastic partial differential equations with infinite delay by using the fixed point theorem. The impulsive effects exists widely in many evolution processes in which states are changed abruptly of certain moments of time, involving such fields as finance, economics, mechanics, electronics and telecommunications, etc [25]. The theory of impulsive differential equations have been studied extensively in [21, 22]. However in addition to impulsive effects, stochastic effects likewise exist in real systems. It is well known that a lot of dynamical systems have variable structures subjects to stochastic abrupt changes, which may result from abrupt phenomena such as stochastic failures and repairs of the components, changes in the interconnections of subsystems, sudden environment changes, etc.

Even though there are many valuable results about neutral stochastic partial differential equations, they are mainly concerned with first-order case. In many cases it is advantageous to treat the second order stochastic differential equations rather than to convert them to first-order systems. The second-order stochastic differential equations are the right model in continuous time to account for integrated processes than can be made stationary. For instance, it is useful for engineers to model mechanical vibrations or charge on a capacitor or condenser subjected to white noise excitation through a second-order stochastic differential equations. The studies of the qualitative properties about abstract deterministic second order evolution equation governed by the generator of a strongly continuous cosine family was proposed in [8,27]. Mahmudov and McKibben [20] established results concerning the global existence and approximate controllability of mild solutions for a class of second order stochastic evolution equations. Moreover, Ren and Sun [23] established the existence, uniqueness and stability of the second-order neutral impulsive stochastic evolution equations with delay with some non-Lipschitz conditions. Balasubramaniam and Muthukumar [2] also discussed the approximate controllability of second-order neutral stochastic distributed implicit functional differential equations with infinite delay. Sakthivel et al. [24] have studied the asymptotic stability of second-order neutral stochastic differential equations by a fixed point theorem. Lei Zhang et al. [14] have studied the controllability of second-order semilinear impulsive stochastic neutral functional evolution equations. Inspired by this consideration, the main objective of this paper is to study the asymptotic stability of the second-order neutral impulsive stochastic delay differential equations**.**

2. PRELIMINARIES

In this section, we briefly give some basic definitions and results for stochastic equations in infinite dimensions and cosine families of operators. We refer to Prato and Zabczyk [6] and Fattorini [8] for more details. Let X and E be two real separable Hilbert spaces and $L(E,X)$ be the space of bounded linear operators from E into X, equipped with the usual operator norm $\|\cdot\|$. Let (Ω,Γ,P) be a complete probability space furnished with a normal filtration $\{\Gamma_t\}_{t\geq 0}$ generated by the Q–Wiener process w

on (Ω,Γ,P) with the linear bounded covariance operator Q such that $trQ<\infty$. We assume that there exist a complete orthonormal system $\{e_i\}_{i\geq 1}$ in E, a bounded sequence of nonnegative real numbers $\{\lambda_i\}$ such that $Qe_i=\lambda_i e_i, i=1,2,3,...,$ and a sequence $\{\beta_i\}$ of independent Brownian motions such that

$$\langle w(t),e\rangle=\sum_{i=1}^{\infty}\sqrt{\lambda_i}\langle e_i,e\rangle\beta_i(t),\ \ e\in E$$

and $\Gamma_t=\Gamma_t^w$,where Γ_t^w is the sigma algebra generated by $\{w(s);t\geq 0\}$. Let $L_2^0=L_2(Q^{1/2}E;X)$ denote the space of all Hilbert –Schmidt operators from $Q^{1/2}E$ to X with the inner product $\langle\psi,\varphi\rangle_{L_2^0}=tr[\psi Q\varphi^*]$. Let $L^p(\Omega,\Gamma_t,X)$ is the Hilbert space of all Γ_t-measurable square integrable random variables with values in a Hilbert space X.

In this paper, we consider the following second-order neutral impulsive stochastic differential equations with delays of the form

$$d[x'(t)-f_0(t,x(t-\delta(t)))]=[Ax(t)+f_1(t,x(t-\rho(t)))]dt+f_2(t,x(t-\sigma(t)))d\omega(t),\ t\geq 0, \quad (1)$$

$$x_0(\cdot)=\varphi\in D^b_{\Gamma_0};\quad x'(0)=x_1, \quad (2)$$

$$\Delta x(t_k)=I_k(x(t_k))\ \Delta x'(t_k)=\tilde{I}_k(x(t_k)),\quad \text{where } k=1,2,...,m, \quad (3)$$

where $\varphi\in D^b_{\Gamma_0}$ and x_1 is also an Γ_0-measurable X-valued random variables independent of w. $A:D(A)\subset X\to X$ is the infinitesimal generator of a strongly continuous cosine family on X; $f_i:R_+\times X\to X\,(i=0,1);\ f_2:R_+\times X\to L_2^0$ are appropriate mappings and $I_k,\tilde{I}_k:X\to X$ are appropriate functions. Moreover, let

$0=t_0<t_1<...<t_m<t_{m+1}=\infty,$

$\Delta x(t_k)=x(t_k^+)-x(t_k^-),$

$\Delta x'(t_k)=x'(t_k^+)-x'(t_k^-),\ x(t_k^+)$ and $x(t_k^-)$ denote the right and left limits of x at t_k. Similarly $x'(t_k^+)$ and $x'(t_k^-)$ denote the right and left limits of x' at t_k. Moreover I_k, $\tilde{I}_k$ represents the size of the jump. Let $\delta,\rho,\sigma:R_+\to[0,\tau]\ (\tau>0)$ are continuous. The space D is assumed to be equipped with the norm $\|\varphi\|_D=\sup_{-\tau\leq t\leq 0}\|\varphi(t)\|_X$. Here $D^b_{\Gamma_0}([-\tau,0],X)$ denote the family of all almost surely bounded, Γ_0-measurable, continuous random variables from $[-\tau,0]$ to X. Let us introduce the spaces

$$H([0,T];X)=\{x:J\to X,x|_{(t_k,t_{k+1}]}\in C((t_k,t_{k+1}],X),\ k=1,2,3,...,m$$

and there exist $x(t_k^+)$ for $k=1,2,3,...,m\}$ and

$$H'([0,T];X)=\{x\in H([0,T];X),x|_{(t_k,t_{k+1}]}\in C'((t_k,t_{k+1}],X),\ k=1,2,3,...,m$$

and there exist $x'(t_k^+)$ for $k=1,2,3,...,m\}$.

It is obvious that $H([0,T];X)$ and $H'([0,T];X)$ are Banach spaces endowed with the norm $\|x\|_H=\sup_{t\in[0,T]}E\|x(t)\|_X^p$.It is easy to see that H' provided with the norm $\|x\|_{H'}=\|x\|_H+\|x'\|_H$.

In this section, we mention some basic concepts, notations, and properties about cosine families of operators [8, 27].

Let $L(E;X)$ is the space of bounded linear operators from E into X. The one parameter family $\{C(t);t\in R\}\subset L(X)$ satisfying

(i) $C(0)=I$,

(ii) $C(t)x$ is continuous in t on R for all $x\in X$,

(iii) $C(t+s)-C(t-s)=2C(t)C(s)$

for all $t,s\in R$ is called a strongly continuous cosine family.

The corresponding strongly continuous sine family $\{S(t);t\in R\}\subset L(X)$ is define

$$S(t)x=\int_0^t C(s)xds,\ t\in R,\ x\in X.$$

The generator $A:X\to X$ of $\{C(t);t\in R\}$ is given by $Ax=(d^2/dt^2)C(t)x\big|_{t=0}$ for all $x\in D(A)=\{x\in X:C(\cdot)x\in C^2(R;X)\}$

It is well known that the infinitesimal generator A is a closed, densely defined operator on X. Such cosine and sine families and their generators satisfy the following properties.

Lemma 2.1: [8]

Suppose that A is the infinitesimal generator of a cosine family of operators $\{C(t);t\in R\}$.Then the following terms hold.

(i) There exists $M^* \geq 1$ and $\alpha \geq 0$ such that $\|C(t)\| \leq M^* e^{\alpha|t|}$ and hence $\|S(t)\| \leq M^* e^{\alpha|t|}$.

(ii) $A\int_s^{\hat{r}} S(u)x\,du = [C(\hat{r}) - C(s)]x$ for all $0 \leq s \leq \hat{r} \leq \infty$.

(iii) There exists $N^* \geq 1$ such that $\|S(s) - S(\hat{r})\| \leq N^* \left|\int_s^{\hat{r}} e^{\alpha|s|} ds\right|$ for all $0 \leq s \leq \hat{r} \leq \infty$.

Lemma 2.2: [6]. For any $r \geq 1$ and for arbitrary L_2^0 - valued predictable process $\phi(\cdot)$ such that

$$\sup_{s\in[0,t]} E\left\|\int_0^s \phi(u)dw(u)\right\|_X^{2r} \leq (r(2r-1))^r \left(\int_0^t \left(E\|\phi(s)\|_{L_2^0}^{2r}\right)^{\frac{1}{r}} ds\right)^r.$$

Definition 2.3: A stochastic process $\{x(t), t \in [0,T]\}$ $0 \leq T < \infty$ is called a mild solution of equations (1), (2) and (3) if

(i) $x(t)$ is adapted to Γ_t, $t \geq 0$.

(ii) $x(t) \in X$ had $ca\grave{d}l\grave{a}g$ paths on $t \in [0,T]$ a.s and for each $t \in [0,T]$, $x(t)$ satisfies the integral equation

$$\begin{aligned} x(t) &= C(t)\varphi(0) + S(t)\big(x_1 - f_0(0, x(0,-\delta(0)))\big) \\ &+ \int_0^t C(t-s) f_0(s, x(s-\delta(s)))ds \\ &+ \int_0^t S(t-s) f_1(s, x(s-\rho(s)))ds \\ &+ \int_0^t S(t-s) f_2(s, x(s-\sigma(s)))dw(s) \\ &+ \sum_{0<t_k<t} C(t-t_k) I_k(x(t_k)) \\ &+ \sum_{0<t_k<t} S(t-t_k)\tilde{I}_k(x(t_k)) \qquad (4) \end{aligned}$$

Definition 2.4: Let $p \geq 2$ be an integer. Equation (3) is said to be asymptotically stable in pth moment if it is stable in pth moment and for any $\varphi \in D^b_{\Gamma_0}$, $x_1 \in X$, we have

$$\lim_{T\to\infty} E\{\sup\|x(t)\|_X^p\} = 0$$

3. ASYMPTOTIC STABILITY OF SECOND-ORDER NEUTRAL STOCHASTIC DIFFERENTIAL EQUATIONS

Now let us present the main result of this paper. We consider the asymptotic stability in the pth moment of mild solutions (1), (2), (3) by using the fixed point principle. Moreover, for the purpose of asymptotic stability, we shall assume that in this work $f_i(t,0) = 0$ $(i = 0,1)$ and $f_2(t,0) = 0$, $I_k(0) = 0$, $\tilde{I}_k(0) = 0$, $k = 1,2,...,m$. Then equations (1), (2) and (3) have a trivial solution when $\varphi = 0$ and $x_1 = 0$.

To prove the following result, we impose the following conditions.

(I) The cosine family of operators $\{C(t); t \geq 0\}$ on X and the corresponding sine family $\{S(t); t \geq 0\}$ satisfy the conditions $\|C(t)\|_X \leq Me^{-bt}$, $\|S(t)\|_X \leq Me^{-at}$, $t \geq 0$ for some constants $M \geq 1$ and $0 < a, b \in R_+$.

(II) The functions f_i $(i = 0,1,2)$ satisfy the Lipchitz condition and there exist positive constants K_1, K_2, K_3 for every $t \geq 0$ and $x, y \in X$, such that

$$\|f_i(t,x) - f_i(t,y)\|_X \leq K_i\|x - y\|_X;\ i = 0,1.$$

$$\|f_2(t,x) - f_2(t,y)\|_X \leq K_3\|x - y\|_X;\ i = 2$$

(III) The function $I_k, \tilde{I}_k$ and there are positive constants q_k, g_k such that

$$\|I_k(x) - I_k(y)\|^p \leq q_k\|x - y\|^p,$$

$$\|\tilde{I}_k(x) - \tilde{I}_k(y)\|^p \leq g_k\|x - y\|^p,$$

for each $x, y \in X$ $(k = 1,2,3,...,m)$.

(IV) $I_k(0) = 0$, $\tilde{I}_k(0) = 0$, $k = 1,2,3,...,m$.

Theorem 3.1:

Assume the conditions (I)-(IV) hold. Let $p \geq 2$ be an integer and $c_p = \left(\frac{p(p-1)}{2}\right)^{\frac{p}{2}}$. If the inequality

$$[5^{p-1}M^p(k_1^p b^{-p} + k_2^p a^{-p} + k_3^p (2a)^{\frac{-p}{2}} + \hat{L} + \hat{D})] < 1$$

is satisfied, then the second-order neutral stochastic differential equations with delays (1), (2) and (3) is asymptotically stable in pth moment.

Proof: Define an operator $\Psi : H \to H$ by

$$\Psi(x)(t) = C(t)\varphi(0) + S(t)\big(x_1 - f_0(0, x(0,-\delta(0)))\big) + \int_0^t C(t-s) f_0(s, x(s-\delta(s)))ds$$

$$+ \int_0^t S(t-s) f_1(s, x(s-\rho(s)))\, ds$$

$$+ \int_0^t S(t-s) f_2(s, x(s-\sigma(s)))\, dw(s)$$

$$+ \sum_{0<t_k<t} C(t-t_k) I_k(x(t_k)) + \sum_{0<t_k<t} S(t-t_k) \widetilde{I}_k(x(t_k))$$

$$= \sum_{i=1}^{7} F_i(t)\ ;\ t \geq 0. \qquad (5)$$

In order to prove the asymptotic stability, it is enough to prove that the operator Ψ has a fixed point H.To prove this result, we use the contraction mapping principle. To apply the contraction mapping principle, first we verify the mean square continuity of Ψ on $[0,\infty)$.

Let $x \in H$, $t_1 \geq 0$ and $|r|$ is sufficiently small then

$$E\|\Psi(x)(t_1+r) - \psi(x)(t_1)\|_X^p \leq 7^{p-1} \sum_{i=1}^{7} E\|F_i(t_1+r) - F_i(t_1)\|_X^p .$$

We can see that

$$E\|F_i(t_1+r) - F_i(t_1)\|_X^p \to 0, i = 1,2,3,4,6,7 \; as \; r \to 0.$$

Moreover by using Holder's inequality and lemma 2.2, we obtain

$$E\|F_5(t_1+r) - F_5(t_1)\|_X^p \leq 2^{p-1} c_p \left[\int_0^{t_1} \left(E \left\| \begin{matrix} (S(t_1+r-s) - S(t_1-s)) \\ \times f_2(s, x(s-\sigma(s))) \end{matrix} \right\|_X^p \right)^{(2/p)} ds \right]^{(p/2)}$$

$$+ 2^{p-1} c_p \left[\int_{t_1}^{t_1+r} (E\|S(t_1+r-s) f_2(s, x(s-\sigma(s)))\|_X^p)^{(2/p)} ds \right]^{(p/2)} \to 0 \; as \; r \to 0, \qquad (6)$$

Thus, Ψ is continuous in pth moment on $[0,\infty)$.

Next , we show that $\Psi(H) \subset H$. From (5), we obtain

$$E\|(\psi x)(t)\|_x^p \leq 8^{p-1} E\|C(t)\varphi(0)\|_X^p + 8^{p-1} E\|S(t)x_1\|_X^p + 8^{p-1} E\|S(t) f_0(0, x(0-\delta(0)))\|_X^p$$

$$+ 8^{p-1} E \left\| \int_0^t C(t-s) f_0(s, x(s-\delta(s)))ds \right\|_X^p + 8^{p-1} E \left\| \int_0^t S(t-s) f_1(s, x(s-\rho(s)))\, ds \right\|_X^p$$

$$+ 8^{p-1} E \left\| \int_0^t S(t-s) f_2(s, x(s-\sigma(s)))\, dw(s) \right\|_X^p + 8^{p-1} \sum_{0<t_k<t} E\|C(t-t_k) I_k(x(t_k))\|_X^p$$

$$+ 8^{p-1} \sum_{0<t_k<t} E\left\|S(t-t_k)\, \widetilde{I}_k(x(t_k))\right\|_X^p .$$

Now, we estimate the terms on the right hand side of (7) using (I), (II), (III) and (IV) we obtain

$$8^{p-1} E\|C(t)\varphi(0)\|_X^p \leq 8^{p-1} M^p e^{-bpt} \|\varphi\|_D^p \to 0 \quad \text{as } t \to \infty, \qquad (8)$$

$$8^{p-1} E\|S(t)x_1\|_X^p \leq 8^{p-1} M^p e^{-apt} \|x_1\|_X^p \to 0 \quad \text{as } t \to \infty, \qquad (9)$$

$$8^{p-1} E\|S(t) f_0(0, x(0,-\delta(0)))\|_X^p \leq 8^{p-1} M^p e^{-apt} K_1 \|x(-\delta(0))\|_X^p \to 0 \text{ as } t \to \infty, \qquad (10)$$

$$8^{p-1} \sum_{0<t_k<t} E\|C(t-t_k) I_k(x(t_k))\|_X^p \leq 8^{p-1} M^p e^{-pbt} \|I_k(x(t_k))\|_X^p \to 0 \text{ as } t \to \infty, \qquad (11)$$

$$8^{p-1} \sum_{0<t_k<t} E\left\|S(t-t_k)\, \widetilde{I}_k(x(t_k))\right\|_X^p \leq 8^{p-1} M^p e^{-pat} \left\|\widetilde{I}_k(x(t_k))\right\|_X^p \to 0 \text{ as } t \to \infty, \qquad (12)$$

From I, II, III, (IV) and Holder's inequality, we have

$$8^{p-1} E \left\| \int_0^t C(t-s) f_0(s, x(s-\delta(s)))ds \right\|_X^p \leq 8^{p-1} M^p K_1^p \left[\int_0^t e^{-b(t-s)} ds \right]^{p-1} \int_0^t e^{-b(t-s)} E\|x(s-\delta(s))\|_X^p ds$$

$$\leq 8^{p-1} M^p K_1^p b^{1-p} \int_0^t e^{-b(t-s)} E\|x(s-\delta(s))\|_X^p \, ds . \qquad (13)$$

For any $x(t) \in H$ and any $\varepsilon > 0$, there exist a $t_1 > 0$, such that $E\|x(s-\delta(s))\|_X^p < \varepsilon$ for $t \geq t_1$.

Thus from (13), we obtain

$$8^{p-1} E\left\| \int_0^t C(t-s) f_0(s, x(s-\delta(s)))\, ds \right\|_X^p$$

$$\leq 8^{p-1} M^p K_1^p b^{1-p} e^{-bt} \int_0^{t_1} e^{bs} E\|x(s-\delta(s))\|_X^p ds$$

$$+ 8^{p-1} M^p K_1^p b^{-p} \varepsilon . \quad (14)$$

As $e^{-bt} \to 0$ as $t \to \infty$ and by assumption on Theorem 3.1, there exists $t_2 > t_1$, such that for any $t \geq t_2$, we have

$$8^{p-1} M^p K_1^p b^{1-p} e^{-bt} \int_0^{t_1} e^{bs} E\|x(s-\delta(s))\|_X^p ds$$

$$\leq \varepsilon - 8^{p-1} M^p K_1^p b^{-p} \varepsilon \quad (15)$$

From (14) and (15), for any $t \geq t_2$, we obtain

$$8^{p-1} E\left\| \int_0^t C(t-s) f_0(s, x(s-\delta(s)))ds \right\|_X^p < \varepsilon .$$

That is to say,

$$8^{p-1} E\left\| \int_0^t C(t-s) f_0(s, x(s-\delta(s)))ds \right\|_X^p \to 0$$

as $t \to \infty$. (16)

Similarly we can obtain

$$8^{p-1} E\left\| \int_0^t S(t-s) f_1(s, x(s-\rho(s)))ds \right\|_X^p \to 0$$

as $t \to \infty$. (17)

Now for any $x(t) \in S$, $t \in [-\tau, \infty]$, we have

$$8^{p-1} E\left\| \int_0^t S(t-s) f_2(s, x(s-\sigma(s)))\, d\omega(s) \right\|_X^p$$

$$\leq 8^{p-1} c_p M^p \left[\int_0^t \left(e^{-ap(t-s)} E\|f_2(s, x(s-\sigma(s)))\|_X^p \right)^{(2/p)} ds \right]^{(p/2)}$$

$$\leq 8^{p-1} c_p M^p \left[\int_0^t e^{-2a(t-s)} (E\|x(s-\sigma(s)))\|_X^p)^{(2/p)} ds \right]$$

$$\leq 8^{p-1} c_p M^p k_3^p \left[\int_0^{t_1} e^{-2a(t-s)} (E\|x(s-\sigma(s)))\|_X^p)^{(2/p)} ds \right.$$

$$\left. + \int_{t_1}^t e^{-2a(t-s)} (E\|x(s-\sigma(s)))\|_X^p)^{2/p} ds \right]^{p/2}$$

$$\leq 8^{p-1} c_p M^p k_3^p \int_0^{t_1} \left(e^{-2a(t-s)} (E\|x(s-\sigma(s)))\|_X^p)^{(2/p)} \right)^{(p/2)} ds$$

$$+ 8^{p-1} c_p M^p k_3^p \varepsilon (2a)^{-p/2} \quad (18)$$

As $e^{-pat} \to 0$ as $t \to \infty$ and by assumption on Theorem 3.1, there exists a $t_2 > t_1$, such that for any $t \geq t_2$, we have

$$8^{p-1} c_p M^p k_3^p \int_0^{t_1} \left(e^{-2a(t-s)} (E\|x(s-\sigma(s)))\|_X^p)^{(2/p)} \right)^{(p/2)} ds$$

$$\leq \varepsilon - 8^{p-1} c_p M^p k_3^p \varepsilon (2a)^{-p/2} . \quad (19)$$

From (18) and (19), for any $t \geq t_2$, we obtain

$$8^{p-1} E\left\| \int_0^t S(t-s) f_2(s, x(s-\sigma(s)))dw(s) \right\|_X^p < \varepsilon. \quad (20)$$

That is to say

$$8^{p-1} E\left\| \int_0^t S(t-s) f_2(s, x(s-\sigma(s)))dw(s) \right\|_X^p \to 0 \; as \; t \to \infty$$

. (21)

Thus from (8)-(12) and (16), (17), (21), we can obtain $E\|(\Psi x)(t)\|_x^p \to 0 \;\; as \;\; t \to \infty$ .Thus we conclude that $\Psi(H) \subset H.$

Next we prove that Ψ is a contraction mapping .To see this, Let $x, y \in H$ and for $s \in [0, T]$, we obtain

$$\sup_{s \in [0,T]} E\|(\Psi x)(t) - (\Psi y)(t)\|_X^p$$

$$\leq 5^{p-1} \sup_{s \in [0,T]} E\left\| \int_0^t C(t-s) \begin{pmatrix} f_0(s, x(s-\delta(s))) \\ - f_0(s, y(s-\delta(s))) \end{pmatrix} ds \right\|_X^p$$

$$+ 5^{p-1} \sup_{s \in [0,T]} E\left\| \int_0^t S(t-s) \begin{pmatrix} f_1(s, x(s-\rho(s))) \\ - f_1(s, y(s-\rho(s))) \end{pmatrix} ds \right\|_X^p$$

$$+5^{p-1}\sup_{s\in[0,T]}E\left\|\int_0^t S(t-s)\begin{pmatrix} f_2(s,x(s-\sigma(s))) \\ -f_2(s,y(s-\sigma(s)))\end{pmatrix}d\omega(s)\right\|_X^p$$

$$+5^{p-1}\sup_{s\in[0,T]}E\left\|\sum_{0<t_k<t}C(t-t_k)\big(I_k(x(t_k))-I_k(y(t_k))\big)\right\|_X^p$$

$$+5^{p-1}\sup_{s\in[0,T]}E\left\|\sum_{0<t_k<t}S(t-t_k)\big(\widetilde{I}_k(x(t_k))-\widetilde{I}_k(y(t_k))\big)\right\|_X^p$$

$$\le 5^{p-1}M^p[k_1^p b^{-p}+k_2^p a^{-p}+k_3^p c_p(2a)^{-p/2}$$

$$+e^{-pbT}E(\sum_{k=1}^m\|q_k\|_X^p)+e^{-paT}E(\sum_{k=1}^m\|g_k\|_X^p)]$$

$$\times\sup_{s\in[0,T]}E\|x(t)-y(t)\|_X^p.$$

Therefore, Ψ is a contraction mapping and hence there exist an unique fixed point $x(\cdot)$ in H which is the solution of the equations (1)-(3) with $x_0(\cdot)=\varphi, x'(0)=x_1$ and $E\|x(t)\|_X^p\to 0$ as $t\to\infty$. This completes the proof.

Corollary 3.2:

If the conditions (I) to (IV) hold, then the second- order neutral impulsive stochastic differential system (1) to (3) is mean square asymptotically stable if

$$5M^2(k_1^2b^{-2}+k_2^2a^{-2}+k_3^2(2a)^{-1}+\hat{L}+\hat{D})<1$$

where $\hat{L}=e^{-2bT}E\left(\sum_{k=1}^m\|q_k\|_X^2\right)$,

$\hat{D}=e^{-2bT}E\left(\sum_{k=1}^m\|g_k\|_X^2\right)$.

4. REFERENCES

[1] Appleby, J. A. D., (2008), Fixed points, stability and harmless stochastic perturbations, preprint.

[2] Balasubramaniam, P., and Muthukumar, P., Approximate controllability of second-order stochastic distributed implicit functional differential systems with infinite delay, J. Optim. Theory Appl., 143 (2) (2009), 225-244.

[3] Caraballo, T., Asymptotic exponential stability of stochastic partial differential equations with delay, stochastics, 33 (1990), 27- 47.

[4] Caraballo, T., Real, J., Partial differential equations with delayed random perturbations: existence, uniqueness and stability of solutions, Stoch. Anal. Appl. 11 (1993), 497-511.

[5] Caraballo, T., Real, J., Taniguchi, T. The exponential stability of neutral stochastic delay partial differential equations, Discrete and continuous Dynamical systems, series A, 18 (2-3) (2007), 295-313.

[6] Da Prato, G., Zabczyk, J., 1992. Stochastic Equations in infinite Dimensions (Cambridge University Press, Cambridge).

[7] Dauer, J.P., Mahmudov, N. I., Integral inequalities and mild solutions of semilinear neutral evolution equations, J. Math. Anal. Appl. 300 (1) (2004), 189-202.

[8] Fattorini, H.O., 1985. Second order linear Differential equations in Banach Spaces, North Holland Mathematics Studies series No. 108 (Elsevier Science, North Holland).

[9] Hale, J. K., Lunel. S. M. V., 1991. Introduction to Functional differential equations (Springer-Verlag, Berlin).

[10] Hu, L., Ren, Y., Existence results for impulsive neutral stochastic functional integro-differential equations with infinite delays, Acta Appl. Math. 111 (3) (2010), 303-317.

[11] Ichikawa, A., Stability of semilinear stochastic evolution equations, J. Math. Anal. Appl. 90 (1982), 12-24.

[12] Khas'minskii, R., 1980. Stochastic stability of differential equations, Sijthoff and noordhoff, Netherlands.

[13] Kolmanovskii, V. B and., Myshkis, A., 1992. Applied Theory of Functional Differential Equations (Kluwer Academic, Norwell, MA).

[14] Lei Zhang, Yongsheng Ding, Tong Wang, Liangjian Hu, and Kuangrong Hao, Controllability of second-order semilinear impulsive stochastic neutral functional evolution equations, Mathematical Problems in Engineering 748091 (2012), 1-13.

[15] Liu, K., Truman, A., A note on almost exponential stability for stochastic partial differential equations, Statist. Probab. Lett. 50 (2000), 273-278.

[16] Luo, J., Fixed points and exponential stability of mild solutions of stochastic partial differential equations with delays, J. Math. Anal. Appl. 342 (2008), 753-760.

[17] Luo, J., Stability of stochastic partial differential equations with infinite delays, J. Comput. Appl. Math. 222 (2008), 364-371.

[18] Luo, J., Exponential stability for stochastic neutral partial functional differential equations, J. Math. Anal. Appl. 355 (1) (2009), 414–425.

[19] Luo, J., Taniguchi, T., Fixed points and stability of stochastic neutral partial differential equations with

infinite delays, Stochastic Analysis and Applications, 27 (2) (2009), 1163-1173.

[20] Mahmudov, N. I., and Mckibben, M. A., Abstract second-order damped Mckean-Vlasov stochastic evolution equations, Stoch. Anal. Appl. 24 (2006), 303-328.

[21] Nieto, J.J., Rodriguez-Lopez, R., Boundary value problems for a class of impulsive functional equations, Comput. Math. Appl. 55 (2008), 2715-2731.

[22] Nieto, J.J., Rodriguez-Lopez, R., New comparison results for impulsive integro-differential equations and applications, J. Math. Anal. Appl. 328 (2007), 1343-1368.

[23] Ren, Y., Dandan, S., Second order neutral impulsive stochastic evolution equations with delays, J. Math. Phys. 50 (2009), 102709.

[24] Sakthivel, R., Ren, Y., Kim, H., Asymptotic stability of second-order neutral stochastic differential equations, J. Math. Phys. 51 (2010), 052701.

[25] Samoilenko, A.M., Perestyuk, N.A., 1995. Impulsive Differential Equations, World Scientific, Singapore.

[26] Taniguchi, T., Liu, K., A., Truman, Existence and uniqueness and asymptotic behavior of mild solution to stochastic functional differential equations in Hilbert spaces, J. Differential Equations 18 (2002), 72-91.

[27] Travis, C.C., Web, G.F., Cosine families and abstract nonlinear second order differential equations, Acta Math. Acad. Sci. Hung. 32 (1978), 75-96.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 422 - 423, 2013

Noise processing methods for Media Processor SOC

Thomas Mohan

National Institute of Electronics
and Information Technology
(NIELIT), Calicut, Kerala,
India.

Abstract: Images taken with both digital cameras and conventional film cameras will pick up noise from a variety of sources. Many further uses of these images require that the noise will be (partially) removed - for aesthetic purposes as in artistic work or marketing, or for practical purposes such as computer vision. Various types of noises include improper black level, salt-and-pepper noise, speckle noise, etc. These noises can be removed with the help of a media processor SOC. The approach mentioned here explains the methods that can be used to remove the above mentioned noises. Each method is explained in detail with necessary diagrams.

Keywords: noise processing; black level; speckle noise; salt and pepper noise; median filter

1. INTRODUCTION

Some common types of noises found in images from digital camera are: Improper black level, fixed pattern noise, salt-and-pepper noise, and speckle noise. These noises can be partially or fully removed by properly processing the image data. No single method is available which will remove all these noises simultaneously. Each one has to be taken care of individually. The data coming out of the image sensor [1] will commonly be in Bayer format. In raw Bayer data [2], each image pixel will have only one color component (Red, Blue or Green). The noise processing algorithms [3] can be highly effective in this stage. Hence the algorithms discussed here modify the data in raw Bayer format itself, before it is converted to RGB format by the media processor SOC.

Improper values of Black level leads to the whitening of image dark region and perceived loss of overall contrast. Dark current from the sensor and lens flare from the lens are the main reasons. This type of noise shall be removed from the image before any other processing [4] has happened on the data. When there is a random variation in pixel values in an image with uniform brightness, it is said to contain speckle noise. These variations are caused by the sensor's unique physical properties. When white and black pixels occur randomly in an image, it is called salt and pepper noise. These normally occur when the pixel values goes out of allocated range. In the coming section, each noise is considered and the methods that can be used to remove them are explained. These methods can be incorporated [5] in a media processor SOC to get good quality images.

2. PROPOSED SCHEME

Here, noise removal method for each type of noise is explained separately.

2.1 Improper black level

Offset and multiplier values can be applied to the image data to successfully correct the black level [6]. First, a pre-offset can be applied to correct any improper black level is provided by the sensor. Then a multiplier can be used to make sure that the image data is in the optimum range. Then post-offset can be applied to remove any improper shift in black level still present in positive or negative direction. Each color in Bayer data will have separate offset and gain values. But all the pixels in a particular Bayer channel will be processed with a single value.

$$\text{Output data} = ((\text{Input data} + \text{Pre-offset}) * \text{Multiplier}) + \text{Post-offset} \quad (1)$$

To identify the offsets and multiplier values required, image is captured with lens cap on. Then a histogram is plotted with the received Bayer data. A sample histogram for Red component in Bayer data is shown. An unwanted offset can be seen in the left portion of the histogram (Unwanted because the image is captured with lens cap on).

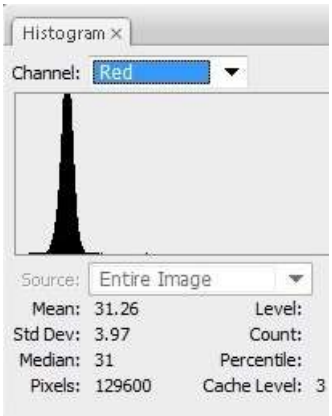


Figure 1. Histogram – Red channel without correction

This offset is configured as the pre-offset value (with negative sign). Multiplier value is also configured to make the data range optimal to take care of bright as well as dark images. Finally, a post-offset is used if required. The histogram of the result image, with the unwanted offset corrected is shown below.

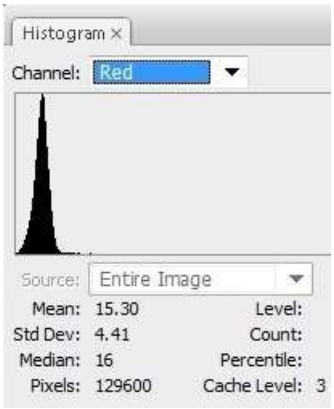


Figure 2. Histogram – Red channel after correction

2.2 Speckle and Salt and Pepper noise

A median filtering method can be used to remove both these noises [7]. Since these noises affect only certain individual pixels without changing the values of neighboring pixels, a median value from the selected neighborhood can be used to replace the affected pixel. Range of the neighborhood has to be properly selected to make sure that the application of this filter does not adversely affect the clarity of the image. The neighborhood can be selected as shown below:

00-G	01-R	02-G	03-R	04-G
10-B	11-G	12-B	13-G	14-B
20-G	21-R	22-G	23-R	24-G
30-B	31-G	32-B	33-G	34-B
40-G	41-R	42-G	43-R	44-G

Figure 3. Green Median Selection

Pixel 22 is the pixel of interest. Green median = median (02, 11, 20, 31, 42, 33, 24, 13, 22). This median will be compared with pixel 22.

00-R	01-G	02-R	03-G	04-R
10-G	11-B	12-G	13-B	14-G
20-R	21-G	22-R	23-G	24-R
30-G	31-B	32-G	33-B	34-G
40-R	41-G	42-R	43-G	44-R

Figure 3. Red Median Selection

Pixel 22 is the pixel of interest. Red median = median (00, 02, 04, 20, 22, 24, 40, 42, 44). This median will be compared with pixel 22. Similar median is selected from blue pixels also.

A threshold value has to be defined which decides whether a pixel has to be replaced with the median value or not. Each pixel will be taken and compared with the median from its neighborhood. If the difference between these two pixels exceeds the configured threshold value, then the pixel of interest can be replaced with the median value. If not, the pixel can be left as such. Such a median method is superior to the method of averaging the pixels in that the sharpness of the image will not be greatly affected [8] with median method.

3. CONCLUSION

In this paper we propose two methods for effectively removing some most common noises in digital video. These methods can be easily implemented in a media processor SOC to deliver good quality video. The advantage of these methods is that this will not be such an overhead to the computing tasks of the media processor. Hence the media processor SOC when run at high frequencies can encode this corrected image data for recording or streaming over network.

4. REFERENCES

[1] Abbas El Gamal, Helmy Eltoukhy, "CMOS imaging sensors," IEEE Circuits & Devices Magazine, May/June. 2005, pp. 6-20.

[2] Ramirez, C., Mora Mas F.J., Enseat J., "Property of Images in Bayer Formats in the Digital Processing of Images" IEEE Electronics, Robotics and Automotive Mechanics Conference, 2008. CERMA '08, pp. 267 - 271, 2008.

[3] Junichi Nakamura, "Image Sensors and Signal Processing for Digital Still Cameras," Taylor & Francis Group, 2006, pp. 87-88.

[4] G.R. Arce, "Nonlinear Signal Processing: A Statistical Approach", Wiley:New Jersey, USA, 2005.

[5] I. Pitas, A. N. Venetsanopoulos, "Nonlinear digital filters:principles and applications", Kluwer academic publishers, 1990.

[6] Zhaowen Li, Tingcun Wei and Ran Zheng, "Design of Black Level Calibration System for CMOS Image Sensor," ICCASM,vol.10, October 2010, pp. 643-647.

[7] Gallagher Jr N C Wise G L. "A theoretical analysis of properties of the median filters, " IEEE Trans. on Acoustics Speech, Signal Processing, vol 29, pp. 1136-1141, 1981.

[8] E. Arias-Castro and D.L. Donoho, "Does median filtering truly preserve edges better than linear filtering?", Annals of Statistics, vol. 37, no. 3, pp. 1172–2009.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 424 - 430, 2013, ISSN: 2319–8656

High Performance Computing for Satellite Image Processing and Analyzing – A Review

Mamta Bhojne
Advanced Computing Training School (ACTS),
Centre for Development of Advanced Computing
(C-DAC), Pune, India.

Abhishek Chakravarti
Advanced Computing Training School (ACTS),
Centre for Development of Advanced Computing
(C-DAC), Pune, India.

Anshu Pallav
Advanced Computing Training School (ACTS),
Centre for Development of Advanced Computing
(C-DAC), Pune, India.

Sivakumar V
Geomatics Solutions Development Group,
Centre for Development of Advanced Computing
(C-DAC), Pune, India.

Abstract: High Performance Computing (HPC) is the recently developed technology in the field of computer science, which evolved due to meet increasing demands for processing speed and analysing/processing huge size of data sets. HPC brings together several technologies such as computer architecture, algorithm, programs and system software under one canopy to solve/handle advanced complex problems quickly and effectively. It is a crucial element today to gather and process large amount of satellite (remote sensing) data which is the need of an hour. In this paper, we review recent development in HPC technology (Parallel, Distributed and Cluster Computing) for satellite data processing and analysing. We attempt to discuss the fundamentals of High Performance Computing (HPC) for satellite data processing and analysing, in a way which is easy to understand without much previous background. We sketch the various HPC approach such as Parallel, Distributed & Cluster Computing and subsequent satellite data processing & analysing methods like geo-referencing, image mosaicking, image classification, image fusion and Morphological/neural approach for hyper-spectral satellite data. Collective, these works deliver a snapshot, tables and algorithms of the recent developments in those sectors and offer a thoughtful perspective of the potential and promising challenges of satellite data processing and analysing using HPC paradigms.

Keywords: Satellite Image, Remote Sensing, High Performance Computing, Parallel Computing, Distributed Computing & Cluster Computing

1. INTRODUCTION

High Performance Computing (HPC) is the recently developed technology in the field of computer science, which evolved due to meet increasing demands for processing speed. HPC brings together several technologies such as computer architecture, algorithm, programs and system software under one canopy to solve advanced complex problems quickly and effectively. This technology focuses on developing and implementing methods like parallel processing, cluster processing and distributed processing for solving problems. Parallel processing is a computing approach to increase the rate at which the set of data is processed by processing different parts of the data at the same time [1]. Unlike other methods where data in inputted in memory system in a step by step manner, distributed processing uses parallel processing on multiple machines, where data is distributed to all parts of the memory system at once. Parallel computing may be seen as a particular tightly coupled form of distributed computing [2] and distributed computing may be seen as a loosely coupled form of parallel computing [3]. In cluster computing many CPUs hooked up via high speed internet connections to a central server which gives each of them several task [1]. With the advancement of satellite remote sensing technology we are getting high spatial, spectral and radiometric resolution images with a huge data available. But problems occur when Remote Sensing image processing speed falls far behind which means that abundant data cannot be translated into useful information in time. Recently, application of HPC technology is getting more importance in remote sensing research work. The utilization of HPC systems in remote sensing applications has become more and more widespread in recent years [4]. HPC is able to improve the computing speed to a great extent in massive data processing, which makes itself an effective way to solve the problem of processing efficiency in remote sensing data. In this paper we present various techniques and methods of High Performance Computing for remotely sensed satellite image processing and analyzing. The following sections briefly describe the High Performance Computing technology for remote sensing data processing and analyzing methods.

2. PARALLEL COMPUTING

Parallel processing is the simultaneous processing of the same task on two or more microprocessors in order to obtain faster results. The computer resources can include a single computer with multiple processors, or a number of computers connected by a network, or a combination of both. The processors access data through shared memory. With the help of parallel processing, a number of computations can be performed at once, bringing down the time required to complete a project. Parallel processing is particularly useful in projects that require complex computations [5]. Han S.H. *et al.* (2009) explained that parallel processing system denotes a multiple-processor computer system consisting of centralized multiprocessors or multi-computers [6]. Figure-1 shows task based parallel processing workflow of automatic geometric correction (step 0), image matching (step 1) and Digital Surface Model generation (step n) using various data / block.

In parallel computing more than one processor is required to perform any task. There are two basic types of parallel computer systems *i.e.*, shared memory multi-computers (SMMC) and message passing multi-computers (MPMC) [7].

The difference between these two types is based on their memory storage unit. In SMMC memories are shared among computers, which means multi-computers share a uniformly coded storage unit and data exchange is realized by addressing operations. Whereas, MPMC uses network to connect computers or processors and each computer has its own storage unit which cannot be accessed by other computers [8].

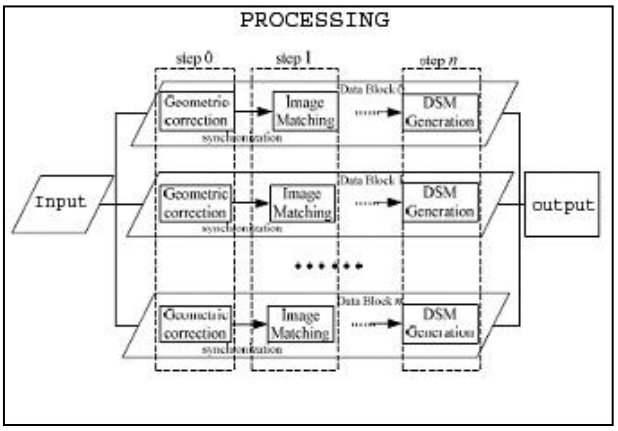


Figure 1. Task based parallel processing workflow (modified after, Hangye Liu *et al.*, 2009).

2.1 Image fusion

Image fusion is the process of merging multi-spectral image having high spectral resolution and pan-chromatic image having high spatial resolution (co-georeferenced). There are different algorithms and operations used for image fusion like Brovey, SFIM, HFM, Wavelet, HIS, Gram-Schmidt, PCA, etc. Yang J. H., *et al.*, (2010) explained that the parallel processing framework can be applied to most image fusion algorithms, which are divided into three categories such as component substitution (CS), modulation based fusion techniques and multi resolution analysis (MRA) based fusion techniques [9]. On satellite image fusion, algorithms can be examined in main four steps i.e., i) Co-register of MS and Pan image, ii) Upscale (interpolation) of MS image, iii) Gather spatial image in Pan image and iv) Merge spatial details with MS image [10]. They analyzed fourteen data fusion methods, execute both serial and parallel algorithms and compare execution times and quality performances. After experimenting serial and parallel algorithm they concluded that all parallel algorithms performed on average 4.4 times faster than serial algorithms with minimum 1.75 and 4.4 times faster. Yang Jinghui *et al.*, (2012) proposed that the parallel processing mechanism can divide an entire image into different blocks which are dispatched to different processing units [11]. Thus the processing efficiency is improved. Although, splitting the computation to more processing threads shortens the executing time but, it also increases the additional cost caused by inefficient memory usage when number of threads increases. In order to check the efficiency of different fusion methods, Alper *et al.*, (2013) applied indexes like Spectral Angle Mapper (SAM), Root Mean Square Error(RMSE), Relative Average Spectral (RASE) and Erreur Relative Globale Adimensionelle de Syntheses (ERGAS) [10]. SAM is used to measure the angle between the spectral vector of fused MS bands and original MS bands to analyze the spectral similarity [12]. Smaller results express high similarity between the images and higher express low similarity [13].

$$SAM(i) = arccos\left(\frac{\langle \hat{v}_i, v_i \rangle}{\|\hat{v}_i\|\|v_i\|}\right) \quad (1)$$

v^= spectral vector of fused image band

I = band

RMSE defines an error between the reference image and fused image for each band. The lower value or RMSE shows the higher spectral quality.

$$RMSE(i) = \frac{1}{tP}\sqrt{\sum_{k=1}^{tP}\left(M_i(k) - \hat{M}_i(k)\right)} \quad (2)$$

M = spectral vector of referenced image

tP =total pixels

RASE expressed the average implementation of RMSE of each spectral band,

$$RASE = 100\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(\frac{RMSE^2(i)}{\mu_i}\right)} \quad (3)$$

μi= mean radiance of n spectral bands of the reference image

Lower values for ERGAS represent higher spectral quality,

$$ERGAS = 100\frac{h}{l}\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(\frac{RMSE^2(i)}{\mu_i}\right)} \quad (4)$$

h= resolution of pan image

l= resolution of MS image

They further explained that the variation in performance of each test differs according to characteristics of methods and their algorithms, hardware limits, cache memory usage, hyper threading etc. They concluded that the best result is observed on Gram-Schmidt followed by IHS- Wavelet hybrid method.

2.2 Image classification

Image classification is the most important part of digital image processing. The intent of the classification process is to categorize all pixels in a digital image into one of several land cover classes or themes. This categorized data may then be used to produce thematic maps of the land cover present in an image [14]. There are two types of image classification- supervised and unsupervised. Supervised classification makes use of the training samples. While in unsupervised classification natural clustering or grouping of the pixel values i.e., gray levels of the pixels are observed. Smit M. *et al.*, (2000) described that technology to rapidly process imagery data into useful information products has not kept pace with the rapidly growing volume and complexity of imagery data increasing available from government and commercial sources. Significant processing speed improvements have been achieved by implementation of classification methods on

the highly parallel integrated virtual environment (HIVE) - a Beowulf class system using parallel virtual machine software [15].

Kato Z. *et al*., (1999) dealt with the problem of unsupervised classification of images modeled by Markov Random Fields (MRF). They worked on parameter estimation methods related to monogrid and hierarchical MRF models using some iterative unsupervised parallel segmentation algorithms. They described algorithms which have been tested on image segmentation problems [16]. Also comparative tests have been tested on noisy synthetic data and on real satellite images. The algorithms were implemented on a Connection Machine CM200 [17, 18]. They compared the obtained parameters and segmentation results to the supervised results presented by Kato Z. *et al*., (1996) in the given Table 1 [19].

Table 1. Comparison of supervised and unsupervised classification (Number of misclassifed pixels)

Model	Image	Supervised	Unsupervised
Monogrid	Checkerboard	260 (1.59%)	213 (1.41%)
	Triangle	112 (0.68%)	103 (0.63%)
Hierarchical	Checkerboard	115 (0.7%)	147 (0.9%)
	Triangle	104 (0.63%)	111 (0.68%)

The result shows that unsupervised algorithms provide results comparable to those obtained by supervised segmentations, but they require much more computing time due to hyper parameter estimation and they are slightly more sensitive to noise. The main advantage is that unsupervised methods are completely data-driven where only input parameter is the number of classes.

2.3 Image mosaicking

Hongyu Wang (2005) has explained that image mosaicking is the process of combining a set of small images into a larger composite image [20]. However, it is very complex to mosaic multiple small images because individual images must be projected into a common coordinate space, overlap between images has to be calculated, the images should be processed so that the backgrounds match, and images composed while using a variety of techniques to handle the presence of multiple pixels in the same output space. To accomplish these tasks, a suite of software tools called Montage has been developed. The modules in this suite can be run on a single processor computer using a simple shell script, and can additionally be run using a combination of parallel approaches. These include running MPI versions of some modules, and using standard grid tools. In the latter case, processing workflows are automatically generated, and appropriate data sources are located and transferred to a variety of parallel processing environments for execution. As a result, it is now possible to generate large-scale mosaics on-demand in timescales that support iterative, scientific exploration [21]. Yan Ying Wang *et al*., (2010) described that image mosaic for large scale RS images, the registration and blending of mosaic is I/O sensitive and time consuming. They proposed an Optimized Image Mosaic Algorithm with Parallel I/O and Dynamic Grouped Parallel Strategy Based on Minimal Spanning Tree to solve the problems associated with image mosaicking. An effective parallel strategy of data splitting is adopted in the time-consuming part, registration and blending. In addition, the multi-thread parallel I/O strategy which is overlapping I/O and computing time is adopted to speed up the algorithm efficiency. Its outstanding parallel efficiency and perfect linear speedup is shown through experimental and comparative analysis [22].

2.4 Morphological /neural approach for hyperspectral satellite image processing

Valencia D. *et al*., (2007) demonstrated new parallel processing methodologies for hyper spectral image processing based on neural architectures and morphological concepts [23]. The computational performance of the proposed methods is demonstrated using real analysis scenarios based on the exploitation of AVIRIS data using two parallel computer systems and SGI Origin 2000 multicomputer located at the Barcelona Supercomputing Center (BSC) and the Thunderhead Beowulf cluster at NASA's Goddard Space Flight Center (NASA/GSFC). They developed a new parallel morphological /neural approach for hyper spectral image classification and specifically discuss implementation aspects using several commodity cluster-based architectures. They proposed methods for hyper spectral analysis which can be included in the category of spectral un-mixing and classification approaches respectively [24]. Valencia D. *et al*., (2007) described classification problem of spectral mixing, and then introduce a morphological operations to solve the problem using SOM (Self Organizing Map) and end member extraction-based approach/ algorithms [23]. Based on the morphological concept they proposed Automated End member Extraction Algorithm (AMEE) method, and allows soft classification of hyper spectral images in fully automated fashion. In addition to this they discussed parallelization strategies for AMEE and SOM algorithms. The proposed parallel algorithm fully exploits the underlying parallelism inherent in image processing methods which, minimizes the communication between processors [25]. Execution time (in seconds) of the AMEE algorithm at the SGI Origin 2000 multi-computer for several combinations of number of iterations. I_{MAX}, and number of processors, N is given in the Table 2 & 3.

Table 2. AMEE algorithm (time in seconds) in SGI origin 2000 (From Valencia D. *et al*., 2007).

N	I_{MAX}=1	I_{MAX}=3	I_{MAX}=5	I_{MAX}=7
1	372	1066	1809	2476
2	182	522	864	1178
4	89	252	429	569
8	264	143	338	293

Execution time (in seconds) of the AMEE algorithm at the Thunderhead Beowulf cluster for several combinations of number of iterations. I_{MAX} and number of processors N. They concluded that parallel computing at the massively parallelism level, supported by message passing, provides a unique framework to accomplish the above goals. For this purpose, computing systems made up of arrays of commercial off-the-shelf computing hardware are a cost-effective way of exploiting this sort of parallelism in remote sensing applications. Specifically, the proposed MPI-based parallel implementation minimizes inter-processor communication overhead and can be ported to any type of distributed memory system.

Table 3. AMEE algorithm (time in seconds) in Thunderhead Beowulf cluster (From Valencia D. *et al*., 2007).

N	I_{MAX}=1	I_{MAX}=3	I_{MAX}=5	I_{MAX}=7
1	311	947	1528	1925
4	124	321	557	685
16	45	95	144	156
36	26	46	61	71
64	19	29	41	43
100	12	20	26	29
144	9	15	20	23
196	6	11	17	20
256	4	10	14	18

3. CLUSTER COMPUTING

A computer cluster is a group of interconnected CPU's which are employed to process large datasets. The interconnection can be of many different types including via LAN, ftp server, Bluetooth network, Wi-Fi, etc. Computer cluster emerged as a result of convergence of a number of computing trends including the availability of low cost microprocessors, high speed networks and software for high performance distributed computing [1]. Clusters are usually deployed to improve performance and availability over that of single computer, while typically being much more cost effective than single computers of comparable speed or availability [26]. A cluster computing system is a compromise between a massively parallel processing system and a distributed system [27]. The architecture of cluster computing is given in the Figure 2.

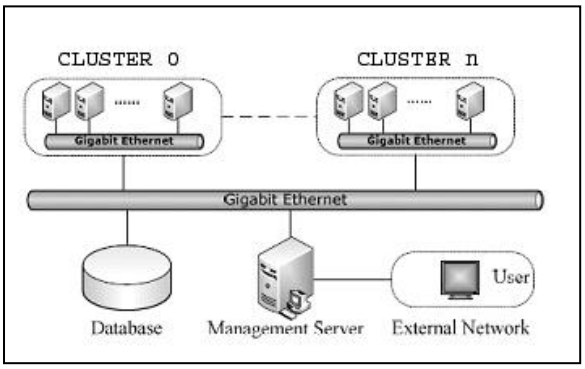


Figure 2. Architecture of remote sensing parallel processing system based on cluster computing (Modified after, Hangye Liu *et al*., 2009).

During recent years, cluster systems have played a more important role in the architecture design of high-performance computing area. Yuanli Shi *et al*., (2012) stated that Satellite Environment Center, Ministry of Environment Protection of China has built a powerful cluster system which is designed to process massive remote sensing data of HJ-1 satellites automatically every day [28]. To verify the performance of cluster system, image registration has been chose to experiment with one scene of HJ-1 CCD sensor. The experiments of imagery registration show that it is an effective system to improve the efficiency of data processing, which could provide a response rapidly in applications. Wang Xuezhi *et al*., (2010) have developed a web based data processing system based on Geospatial Data Abstraction Library (GDAL) which made the use of cluster computing and parallel computing [29]. The system achieved not only the online processing of 14 vegetation indices like NDVI and EVI, but also the online gap-fill algorithm for Landsat-7 SLC-off datasets.

Yang C.T. and Hung C.C. (2000) present the basic programming techniques by using PVM (Parallel Virtual Machine) to implement a message-passing program to utilize the parallelism of cluster of SMPs (Symmetric Multi Processor) [27]. The matrix multiplication of the parallel ray tracing problems is illustrated and the experiments are also demonstrated on Linux SMPs cluster. The program for matrix multiplication is given below:

```
for (i = 0; i < N; i ++ ) {                    /* can be parallelized */
    for (j = 0; j < M; j++ ){                  /* can be parallelized */
    c[i] [j] = 0;
      for (k = 0; k < P; k++)
         c[i] [j] = c[i] [j] + a[i] [k] * b [k] [j];
   }
}
```

The matrix multiplication algorithm is implemented in PVM (Parallel Virtual Machine) using the master-slave paradigm. The experimental results showed that the highest speedup were 10.89 and 13.67 respectively for matrix multiplication of the PVMPOV (an unofficial version of Pov-ray), when the number of processors is 16, by creating 16 tasks on SMPs cluster. The results of this study will make theoretical and technical contributions to the design of a PVM program of a Linux SMP clusters for remote sensing data processing. It also shows that Linux/PVM cluster can achieve high speedups for applications.

4. DISTRIBUTED COMPUTING

Distributed computing is the process of aggregating the power of several computing entities to collaboratively run a single computational task in a transparent and coherent way, so that they appear as a single centralized system. Connecting users and resources in a transparent, open and scalable way is the main goal of distributed operating system [30]. Godfrey B.(2002) has described that distributed computing works by splitting the larger into smaller chunks which can be performed at the same time independently of each other [31]. The two main entities in distributing computing are the server and the many clients. A central computer, the server will generate work packages which are passed onto worker clients. The clients will perform the task, detailed in a work package data and when it has finished the completed work package will be passed back to the server. The working process of semi distributed scheduling policy is given in the Figure 3.

Processing image data generated by new remote sensing systems can severely tax the computational limits of the classic single processor systems that are normally available to the remote sensing practitioner. Operating on these large data sets with a single computer system, sometimes simplifying approximations are used that can limit the precision of the final result. Recent work at Pacific Northwest National Laboratory strongly suggest that a distributed network of inexpensive PCs can be designed that is optimal to deal with intensive computationally problems. The new type of distributed computing will remove computational constraints; image processing algorithms for remote sensed images are now being considered [32].

Geo referencing is basic function of remote sensing data processing. It is a process of assigning geographic information

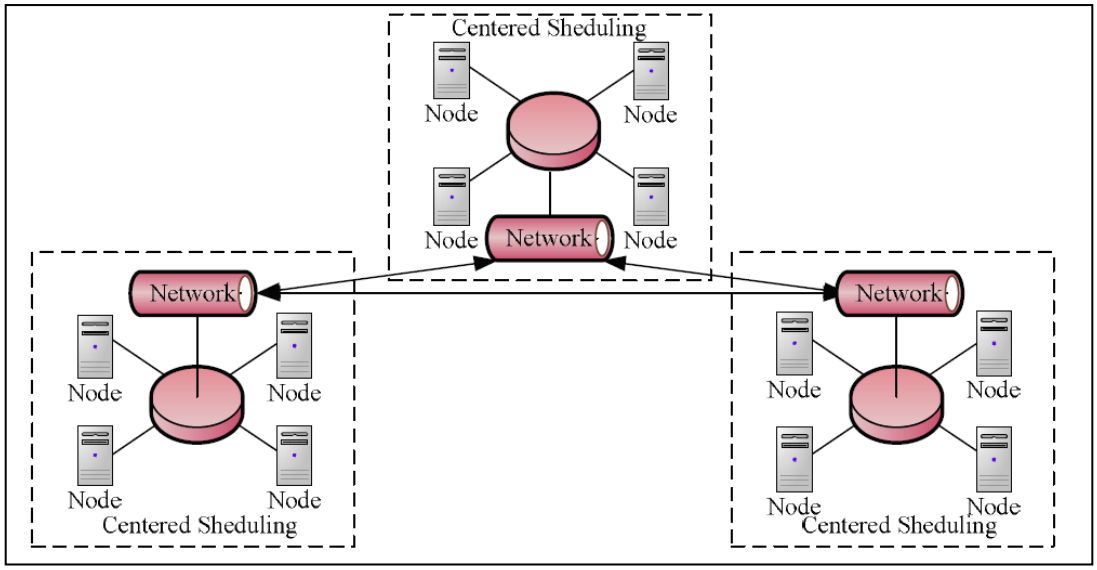


Figure 3. Semi distributed scheduling policy (modified after, Hangye Liu *et al*., 2009).

to an image. Knowing where an image is located in the world allows information about features contained in that image to be determined. This information includes location, size and distance. But it is very time consuming and computationally intensive process. To improve the efficiency of processing Yincui Hu *et al*., (2005) focuses on parallelization of remote sensing data on a grid platform [33]. As an important new field in the distributed computing arena, Grid computing focuses on intensive resource sharing, innovative applications, and, in some cases, high performance orientation. They performed their experiments on MODIS level 1B data. Two strategies were followed by them for geo referencing process viz. parallel rectification on grid and data partition strategy. They explained three components to rectify image, i.e. transformation model selection, coordinate transformation and resampling to correct every part of the large image. The partition strategy influences the process of efficiency and determines the merge strategy. According to feature of algorithm the applied backward decomposing techniques which comprises four steps i.e. partitioning the output array into equal sized block, computing geographical range of every block, finding GPCs triangulations contained with geographical range and extract block from original data in accordance with these triangulation. This extracted block is the data that will be distributed to producers. The experiment shows that data- parallel geo-reference is efficient especially for large-size data. The large data is decomposed into small parts and distributed to the Grid. The experiments indicate that Grid is efficient for data-parallel geo-reference.

Shamim Akhter *et al*., (2005) described a parallel approach in cluster computing and MPI (Message Passing Interface) parallel programming and provide results of experiments on studying the porting of remote sensing algorithm [34]. They used MPI as programming tool and all the codes were tested Beowulf cluster using GNU C compiler with the MPICH. implementation of MPI. They performed their experiment in compressed ASTER image and uncompressed MODIS image. The tasks are allocated to slave processor by a master processor. After getting data from input file, server put these data into 2D array which is distributed to different processors using either of two procedures, first, distributed each input pixel of a particular remote sensing image to corresponding processor and distributed row or column of that image at a time to the corresponding processor. Figure 4 shows flow of task allocation by master processor.

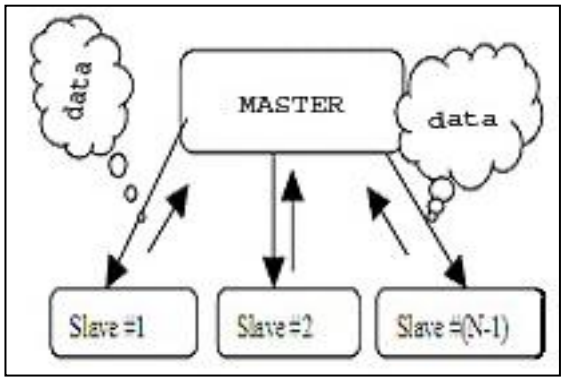


Figure 4. Client server paradigms (modified after, Shamim *et al*., 2005).

From these two experiments with a simple processing at two images size difference, it is observed that there is a point of convergence of all curves for a given image with an increasing number of operations applied.

5. CONCLUSIONS & FUTURE SCOPE

Methods discussed above are some of the techniques that are the subset of High Performance Computing (HPC) techniques that are being employed today to process large amounts of data. Thus different approaches can be employed for different projects. Parallel processing is particularly useful in projects that require complex computations. Parallel processing framework can be applied to most image fusion algorithms and hyper spectral image processing based on neural architectures and morphological model. Distributed computing is particularly useful when large amounts of data have to be processed within a given time period, keeping in mind the economic restrictions. A distributed network of inexpensive PCs can be designed that is optimal to deal with the type of computationally intensive problems encountered in processing remotely sensed images. Cluster computing is one of the most widely used HPC approach for processes such as geo-referencing, image transformation, image mosaicking, etc. Currently most of these approaches are limited to military

and government organizations but private enterprises are also employing this technology at a rapid pace. Although, more research work requires on satellite data processing and analyzing over HPC platform for getting an enhanced and fast output for various remote sensing applications.

6. ACKNOWLEDGMENTS

The authors are thankful to ACTS, C-DAC, Pune for providing facilities and support to carry out this study. Authors would like to extend their gratitude to Ms. Asima Mishra, Joint Director–GSDG and Dr. Sunil Londhe GSDG, C-DAC, Pune for their encouragement.

7. REFERENCES

[1] WIKI. (2013). http://wiki.answers.com/Q, Accessed. June, 2013.

[2] Peleg D. (2000). Distributed Computing: A Locality-Sensitive Approach, SIAM, ISBN 0-89871-464-8:pp. 10. https://en.wikipedia.org/wiki/Distributed_computing. Accessed, June, 2013.

[3] Ghosh and Sukumar (2007). Distributed Systems – An Algorithmic Approach. Chapman & Hall/CRC. https://en.wikipedia.org/wiki/Distributed_computing. Accessed, June, 2013.

[4] Lee, C. A., Gasster, S. D., Plaza, A., Chang, C. I., & Huang, B. (2011). Recent developments in high performance computing for remote sensing- A review. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing. 4.3: 508-527.

[5] WISEGEEK. (2013). http://www.wisegeek.com/what-is-parallel-processing.html. Accessed, June, 2013.

[6] Han S.H, Joon Heo, Hong Gyoo Sohn and Kiyun Yu. (2009). Parallel Processing Method For A Airborne Laser Scanning Data Using a PC Cluster and a Virtual Grid. Sensors, 2009, 9: pp.2555-2573; DOI: 10.3390/s90402555. www.mdpi.com/1424-8220/9/4/2555/pdf. Accessed, June, 2013.

[7] Barry Wilkinson B. and Michael Allen (2002). Parallel Programming. China Machine Press. www.cse.ucsc.edu/classes/cmpe113/Fall02/slides1.4.ps. Accessed, June, 2013.

[8] Hangye Liu, Yonghong Fan, Xueqing Deng, Song Ji. (2009). Parallel Processing Architecture of Remote Sensed Image Processing System Based on Cluster. IEEE Image and Signal Processing 09. CISP '09. 2nd International Congress. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5300938. Accessed June, 2013.

[9] Yang J.H., J.X. Zhang, Li Haitao, Sun Yushan, Pu Pengxian.(2010). Pixel Level Fusion Methods for Remote Sensing Images: a Current Review,Technical Commission VII Symposium, Vienna, Austria. pp.680. http://www.isprs.org/proceedings/XXXVIII/part7/b/pdf/680_XXXVIII-part7B.pdf. Accessed, June, 2013.

[10] Alper A G., Adnan O, Meric Y., Sedef K P., Serdar B., and Mesut K. (2013). Remote Sensing Data Fusion Algorithms With Parallel Computing. . http://academia.edu/3266480/Remote_Sensing_Data_Fusion_Algorithms_with_Parallel_Computing. Accessed June, 2013.

[11] Yang Jinghui, Zhang Jixian (2012). A Parallel Implementation Framework For Remotely Sensed Image Fusion. ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume I-7, 2012 XXII ISPRS Congress, 25 August – 01 September 2012, Melbourne, Australia. http://www.isprs-ann-photogramm-remote-sens-spatial-inf-sci.net/I-7/329/2012/isprsannals-I-7-329-2012.pdf. Accessed, June, 2013.

[12] Yuhas R.H., Goetz A.F. And Boardman J.W. (1992). Discrimination Among Semi Arid Landscape End Members Using Spectral Angle Mapper (SAM) Algorithm. Summeries Of The Third Annual JPL Airborne Geosciences Workshop ,Vol. 1,Pasadena, CA:JPL Publication.pp.147-149. http://academia.edu/3266480/Remote_Sensing_Data_Fusion_Algorithms_with_Parallel_Computing. Accessed, June, 2013.

[13] Chikr M E Mezouar, N.Taleb, K.Kpalma and J. Ronsin (2011). An HIS Based Fusion For Color Distortion And Vegetation Enhancement In Ikonos Imagery. Geosciences And Remote Sensing, IEEE Transactions on,Vol.49,No.5. pp. 1590-1602. http://academia.edu/3266480/Remote_Sensing_Data_Fusion_Algorithms_with_Parallel_Computing. Accessed, June, 2013.

[14] SC.(2013). Remote sensing University Lecture note. http://www.sc.chula.ac.th/courseware/2309507/Lecture/remote18.html, Accessed, June, 2013.

[15] Smit M.,Garegnani J,Bechdol M and Chettri S.(2000). Parallel Image classification on HIVE. Applied imagery pattern recognition workshop,IEEE, 2000:39-46. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=953601&tag=1. Accessed, June, 2013.

[16] Kato Z., Zerubia J., Berthod M. (1999). Unsupervised parallel image classification using Markovian models. Pattern Recognition 32 (1999) 591Ð604, p.591-602. http://www.inf.u-szeged.hu/~kato/papers/pattrec99.pdf. Accessed, June, 2013.

[17] Hillis W.D. (1985). The Connection Machine. MIT press New York. http://www.inf.u-szeged.hu/~kato/papers/pattrec99.pdf. Accessed, June, 2013.

[18] TMC, Thinking Machines Corporation, Cambridge, Massachusetts, Connection Machine Technical Summary (1989). Version 5.1 ed. http://www.inf.u-szeged.hu/~kato/papers/pattrec99.pdf. Accessed, June, 2013.

[19] Kato Z, Berthod M, Zerubia J., A. (1996). hierarchical Markov random Field model and multi-temperature annealing for parallel image classification, Compute. Vision Graphics Image Process. Graphical Models Image Process. 58:18-37. http://www.inf.u-szeged.hu/~kato/papers/pattrec99.pdf. Accessed, June, 2013.

[20] Hongyu Wang (2005). Parallel Algorithms For Image And Video Mosaic Based Applications.p.1. http://athenaeum.libs.uga.edu/bitstream/handle/10724/8351/wang_hongyu_200508_ms.pdf?sequence=1. Accessed, June, 2013.

[21] Katz D.S., Nathaniel Anagnostou, G. Bruce Berriman, Ewa Deelmans, John Good Joseph C.Jaco, Arl Kesselman, Anastasia Laity, Thomas A. Prince, Gurmeet Singh, Mei Hui Su, Roy Williams (2006). Astronomical Image Mosaicking On a Grid: Initial Experiences. Engeneering the Grid Status and Perspective. Book - American Scientific Publishers. ISBN:1-58883-038-1. http://montage.ipac.caltech.edu/publications/montage_ETG.pdf. Accessed June, 2013.

[22] Yan Ying Wang, Yan Ma, Peng Liu, Dingsheng Liu and Jibo Xie. (2010). An Optimized Image Mosaic Algorithm with Parallel IO and Dynamic Grouped Parallel Strategy Based on Minimal Spanning Tree.

Proceeding Gcc '10 proceeding of the 2010 ninth international conference on grid and cloud computing.pp. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05662698. Accessed, June, 2013.

[23] Valencia D., Plaza A., Martinez P., Plaza J. (2007). Parallel Processing of High Dimensional Images Using Cluster Computer Architectures. IJCA, vol.14, no. 1. pp 23-34. IJCA, Vol. 14, No. 1: pp.23-34. http://www.umbc.edu/rssipl/people/aplaza/Papers/Journals/2007.IJCA.Cluster.pdf. Accessed, June, 2013.

[24] Plaza A., Martínez P., Pérez R. and Plaza J. (2004). A New Approach for Mixed Pixel Classification in Hyperspectral Imagery Based on Extended Morphological Profiles. Pattern Recognition, 37:1097-1116. http://www.umbc.edu/rssipl/people/aplaza/Papers/Journals/2007.IJCA.Cluster.pdf

[25] Seinstra F.J., Koelma D., And Geusebroek J. M., (2002). A Software Architecture For Transparent Parallel Image Processing. Parallel Computing,28: pp.967-923. http://www.umbc.edu/rssipl/people/aplaza/Papers/Journals/2007.IJCA.Cluster.pdf. Accessed, June, 2013.

[26] Bader D., Pennington R. (2007). Cluster Computing Applications. The international journal of high performance computing. 15(2):181-185. http://en.wikipedia.org/wiki/Computer_cluster. Accessed, June, 2013.

[27] Yang C.T. and Hung C.C. (2000). Parallel Computing in Remote Sensing Data Processing. GIS DEVELOPMENT, AARS, ACRS, Image Processing. 1(1):1-6. http://www.a-a-r-s.org/acrs/proceeding/ACRS2000/Papers /OMP00-4.htm. Accessed June, 2013.

[28] Yuanli Shi, Wenming Shen, Wencheng Xiong, Zhuo Fu, Rulin Xiao (2012). High Performance Cluster System Design for Remote Sensing Data Processing. High-Performance Computing in Remote Sensing II. Proceedings of the SPIE, Volume 8539, article id. 85390N.

[29] Wang Xuezhi, Lin Qinghui, Zhou Yuanchun (2010). A Web-Based Data-Processing System For LandsatImagery. http://www.codata.org/10Conf/abstracts. Accessed, June, 2013.

[30] WORDIQ (2013). Distributed_computing. http://www.wordiq.com/definition/Distributed_computing, Accessed. June, 2013. Accessed, June, 2013.

[31] Godfrey B. (2002). Document, Primer on Distributed Computing. http://www.bacchae.co.uk/docs/dist.html. Accessed June, 2013.

[32] Petrie G. M., Dippold C., Fann G., Jones D., Jurrus E., Moon B. (2002). Distributed Computing Approach For Remote Sensing Data. (Conference) Symposium On Parallel And Distributed Computing, SPDP. http://academic.research.microsoft.com/Paper/2563627.aspx. Accessed, June, 2013.

[33] Yincui Hu, Yong Tang, Jiakui Tang, Shaobo Zhong and Guoyin Cai. (2005). Data Parallel Method for Georeferencing of MODIS Level 1B Data Using Grid Computing. 5th International Conference, Atlanta, GA, USA, May 22-25, 2005, Proceedings, Part III. http://rsgisforum.irsa.ac.cn/download/05_SCI/Data-parallel%20method%20for%20georeferencing%20of%20MODIS%20level%201B%20data%20using%20grid%20computing.pdf. Accessed, June, 2013.

[34] Shamim Akhter , Kiyoshi Honda , Yann Chemin , M. Ashraful Amin (2005). Experiments On Distributed Remote Sensing Data (Modis And Aster) Processing Using Optima Cluster. http://www.academia.edu/1760912/EXPERIMENTS_ON_DISTRIBUTED_REMOTE_SENSING_DATA_MODIS_AND_ASTER_PROCESSING_USING_OPTIMA_CLUSTER. Accessed, June, 2013.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 431 - 435, 2013, ISSN: 2319–8656

Accountability in Distributed Environment For Data Sharing in the Cloud

K .Neeraja
JNTU Hyderabad
Hyderabad, India

B.Savitha Reddy
JNTU Hyderabad
Hyderabad, India

D. Rajani
JNTU Hyderabad
Hyderabad, India

Abstract—Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. To address this problem, in this paper, we propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users 'data in the cloud. In particular, we propose an object-centred approach that enables enclosing our logging mechanism together with users' data and policies. We leverage the JAR programmable capabilities to both create a dynamic and travelling object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, we also provide distributed auditing mechanisms.

Keywords—Cloud computing, accountability, data sharing.

1. INTRODUCTION

CLOUD computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable and often virtualized resources as a service over the Internet. To date, there are a number of notable commercial and individual cloud computing services, including Amazon, Google, Microsoft, Yahoo, and Sales force. Details of the services provided are abstracted from the users who no longer need to be experts of technology infrastructure. Moreover, users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services

2. EXISTING SYSTEM

To allay users' concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments.

Problems on existing system:

First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on.

Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

3. PROPOSED SYSTEM

We propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and track able. Our proposed CIA framework provides end-to end accountability in a highly distributed fashion. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honoured, but also enforce access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while

the pull mode refers to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed.

Our main contributions are as follows:

- We propose a novel automatic and enforceable logging mechanism in the cloud.
- Our proposed architecture is platform independent and highly decentralized, in that it does not require any dedicated authentication or storage system in place.
- We go beyond traditional access control in that we provide a certain degree of usage control for the protected data after these are delivered to the receiver.

4. MODULES

4.1 Cloud Information Accountability (CIA) Framework:

CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honoured, but also enforce access and usage control rules as needed.

4.2 Distinct mode for auditing:

Push mode:

The push mode refers to logs being periodically sent to the data owner or stakeholder.

Pull mode:

Pull mode refers to an alternative approach whereby the user(Or another authorized party) can retrieve the logs as needed.

4.3 Logging and auditing Techniques:

1. The logging should be decentralized in order to adapt to the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled, and require minimal infrastructural support from any server.

2. Every access to the user's data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity that accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed.

3. Log files should be reliable and tamper proof to avoid illegal insertion, deletion, and modification by malicious parties. Recovery mechanisms are also desirable to restore damaged log files caused by technical problems.

4. Log files should be sent back to their data owners periodically to inform them of the current usage of their data. More importantly, log files should be retrievable anytime by their data owners when needed regardless the location where the files are stored.

5. The proposed technique should not intrusively monitor data recipients' systems, nor it should introduce heavy communication and computation overhead, which otherwise will hinder its feasibility and adoption in practice.

4.4 Major components of CIA:

There are two major components of the CIA, the first being the logger, and the second being the log harmonizer.

The logger is strongly coupled with user's data (either single or multiple data items). Its main tasks include automatically logging access to data items that it contains, encrypting the log record using the public key of the content owner, and periodically sending them to the log harmonizer. It may also be configured to ensure that access and usage control policies associated with the data are honoured. For example, a data owner can specify that user X is only allowed to view but not to modify the data. The logger will control the data access even after it is downloaded by user X. The log harmonizer forms the central component which allows the user access to the log files. The log harmonizer is responsible for auditing.

We conduct experiments on a real cloud test bed. The results demonstrate the efficiency, scalability, and granularity of our approach. We also provide a detailed security analysis and discuss the reliability and strength of our architecture.

4.4.1 Overview of CIA

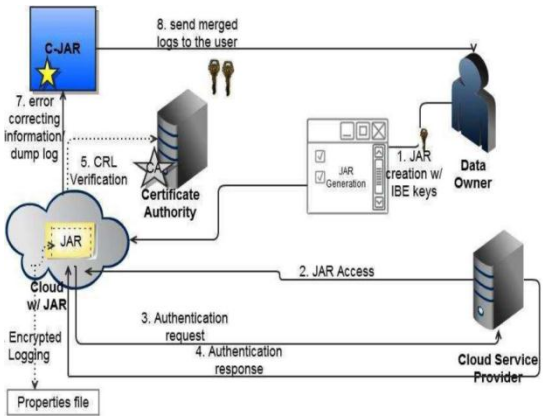


Fig 1. Architecture of CIA

The overall CIA framework, combining data, users, logger and harmonizer is sketched in Fig. 1. At the beginning, each user creates a pair of public and private keys based on Identity-Based Encryption (step 1 inFig.1). This IBE scheme is a Weil-pairing-based IBE scheme, which protects us against one of the most prevalent attacks to our architecture. Using the generated key, the user will create a logger component which is a JAR file, to store its data items. The JAR file includes a set of simple access control rules specifying whether and how the cloud servers, and possibly other data stakeholders (users, companies) are authorized to access the content itself. Then, he sends the JAR file to the cloud service provider that he subscribes to. To authenticate the CSP to the JAR (steps 3-5 in Fig. 1), we use Open SSL-based certificates, wherein a trusted certificate authority certifies the CSP. In the event that the access is requested by a user, we employ SAML-based authentication, where in a trusted identity provider issues certificates verifying the user's identity based on his username.

Once the authentication succeeds, the service provider (or the user) will be allowed to access the data enclosed in the JAR. Depending on the configuration settings defined at the time of creation, the JAR will provide usage control associated with logging, or will provide only logging functionality. As for the logging, each time there is an access to the data, the JAR will automatically generate a log record, encrypt it using the public key distributed by the data owner, and store it along with the data (step 6 in Fig. 1). The encryption of the log file prevents unauthorized changes to the file by attackers. The data owner could opt to reuse the same key pair for all JARs or create different key pairs for separate JARs. Using separate keys can enhance the security without introducing any overhead except in the initialization phase. In addition, some error correction information will be sent to the log harmonizer to handle possible log file corruption (step 7 in Fig. 1). To ensure trustworthiness of the logs, each record is signed by the entity accessing the content. Further, individual records are hashed together to create a chain structure, able to quickly detect possible errors or missing records. The encrypted log files can later be decrypted and their integrity verified. They can be accessed by the data owner or other authorized stakeholders at any time for auditing purposes with the aid of the log harmonizer (step 8 in Fig. 1).

5. EXPERIMENTAL RESULTS

In the experiments, we first examine the time taken to create a log file and then measure the overhead in the system. With respect to time, the overhead can occur at three points: during the authentication, during encryption of a log record, and during the merging of the logs. Also, with respect to storage overhead, we notice that our architecture is very lightweight, in that the only data to be stored are given by the actual files and the associated logs. Further, JAR act as a compressor of the files that it handles. Multiple files can be handled by the same logger component. To this extent, we investigate whether a single logger component, used to handle more than one file, results in storage overhead.

5.1 Log Creation Time

In the first round of experiments, we are interested in finding out the time taken to create a log file when there are entities continuously accessing the data, causing continuous logging. Results are shown in Fig. 2. It is not surprising to see that the time to create a log file increases linearly with the size of the log file. Specifically, the time to create a 100 Kb file is about 114.5 ms while the time to create a 1 MB file averages at 731 ms. With this experiment as the baseline, one can decide the amount of time to be specified between dumps, keeping other variables like space constraints or network traffic in mind.

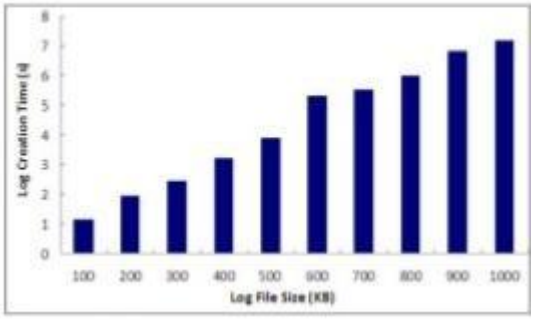


Fig 2. Time to create log files of different sizes

5.2 Authentication Time

The next point that the overhead can occur is during the authentication of a CSP. If the time taken for this authentication is too long, it may become a bottleneck for accessing the enclosed data. To evaluate this, the head node issued OpenSSL certificates for the computing nodes and we measured the total time for the OpenSSL authentication to be completed and the certificate revocation to be checked.

Considering one access at the time, we find that the authentication time averages around 920 ms which proves that not too much overhead is added during this phase. As of present, the authentication takes place each time the CSP needs to access the data. The performance can be further improved by caching the certificates. The time for authenticating an end user is about the same when we consider only the actions required by the JAR, viz. obtaining a SAML certificate and then evaluating it. This is because both the OpenSSL and the SAML certificates are handled in a similar fashion by the JAR. When we consider the user actions (i.e., submitting his username to the JAR), it averages at 1.2 minutes.

5.3 Time Taken to Perform Logging

This set of experiments studies the effect of log file size on the logging performance. We measure the average time taken to grant an access plus the time to write the corresponding log record. The time for granting any access to the data items in a JAR file includes the time to evaluate and enforce the applicable policies and to locate the requested data items.

In the experiment, we let multiple servers continuously access the same data JAR file for a minute and recorded the number of log records generated. Each access is just a view request and hence the time for executing the action is negligible. As a result, the average time to log an action is about 10 seconds, which includes the time taken by a user to double click the JAR or by a server to run the script to open the JAR. We also measured the log encryption time which is about 300 ms (per record) and is seemingly unrelated from the log size.

5.4 Log Merging Time

To check if the log harmonizer can be a bottleneck, we measure the amount of time required to merge log files. In this experiment, we ensured that each of the log files had 10 to 25 percent of the records in common with one other. The exact number of records in common was random for each repetition of the experiment. The time was averaged over 10 repetitions. We tested the time to merge up to 70 log files of 100 KB, 300 KB, 500 KB, 700 KB, 900 KB, and 1 MB each. The results are shown in Fig. 6. We can observe that the time increases almost linearly to the number of files and size of files, with the least time being taken for merging two 100 KB log files at 59 ms, while the time to merge 70 1 MB files was 2.35 minutes.

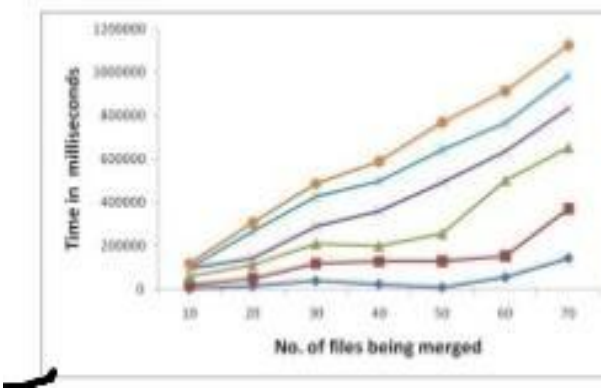


Fig 3. Time to merge log files

5.5 Size of the Data JAR Files

Finally, we investigate whether a single logger, used to handle more than one file, results in storage overhead. We measure the size of the loggers (JARs) by varying the number and size of data items held by them. We tested the increase in size of the logger containing 10 content files (i.e., images) of the same size as the file size increases. Intuitively, in case of larger size of data items held by a logger, the overall logger also increases in size. The size of logger grows from 3,500 to 4,035 KB when the size of content items changes from 200 KB to 1 MB. Overall, due to the compression provided by JAR files, the size of the logger is dictated by the size of the largest files it contains.

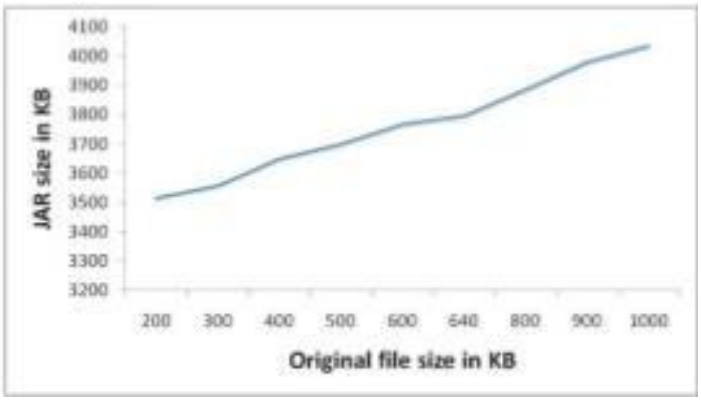


Fig 4. Size of the logger component

6. CONCLUSION AND RESEARCH

We proposed innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. Our approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge.

In the future, we plan to refine our approach to verify the integrity of the JRE and the authentication of JARs. For example, we will investigate whether it is possible to leverage the notion of a secure JVM being developed by IBM. This research is aimed at providing software tamper resistance to Java applications. In the long term, we plan to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of travelling content. We would like to support a variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance controls.

7. REFERENCES

[1] P. Ammann and S. Jajodia, “Distributed Timestamp Generation in Planar Lattice Networks,” ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. ACM Conf. Computer and Comm. Security, pp. 598- 609, 2007.

[3] E. Barka and A. Lakas, “Integrating Usage Control with SIP-Based Communications,” J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.

[4] D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.

[5] R. Bose and J. Frew, “Lineage Retrieval for Scientific Data Processing: A Survey,” ACM Computing Surveys,

vol. 37, pp. 1- 28, Mar. 2005.

[6] P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '06), pp. 539-550, 2006.

[7] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.

[8] OASIS Security Services Technical Committee, "Security Assertion Markup Language (saml) 2.0," http://www.oasis-open.org/ committees/tc home.php?wg abbrev=security, 2012.

[9] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust,pp. 187-201, 2005.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 436 - 442, 2013, ISSN: 2319–8656

Reduction of types of Noises in dental Images

P.Subbuthai
Department of Electronics and Instrumentation
Bharathiar University
Coimbatore
India

K.Kavithabharathi
Department of Electronics and Instrumentation
Bharathiar University
Coimbatore
India

S.Muruganand
Department of Electronics and Instrumentation
Bharathiar University
Coimbatore
India

Abstract---This paper presents a filter for restoration of Dental images that are highly corrupted by salt and pepper noise and speckle noise, Poisson noise. After detecting and correcting the noisy pixel, the proposed filter is able to suppress noise level. In this paper for each noise proposed different type of filter and compare these three types of filter with their PSNR value and MSE value and SNR value. After filtering stage maximum detected noise pixels will be filtered and simulation results show the filtered image.

Index Terms—Dental Image, FIR Filter, Gaussian Filter, Median Filter, Poisson Noise, Salt and Pepper Noise, Speckle Noise.

1. INTRODUCTION

The medical imaging devices particularly X-ray, CT/MRI and ultrasound are manufacturing overabundant pictures that are utilized by medical practitioners within the method of designation. The most downside visage by them is that the noise introduced attributable to the consequence of the coherent nature of the wave transmitted. These noises corrupt the image and sometimes cause incorrect designation. Every of those medical imaging devices are littered with differing types of noise. As an example, the x-ray pictures are typically corrupted by Poisson noise, salt and pepper noise, speckle noise.

The requirement to get rid of salt-and-pepper noise is very necessary before succeeding image process tasks are disbursed as a result of the contamination of image by salt-and-pepper noise is caused in great deal and therefore the occurrence of noise will severely harm the knowledge or data contained within the original image. The only and therefore the traditional thanks to take away salt-and-pepper noise is by windowing the noisy image with a standard median filter [1].

Spatial filtering is that the commonest technique for speckle noise reduction. The averaging technique is that the most well-liked linear filtering methodology among the varied spatial filters that with success removes noise from a distorted image however it's the impact of probably blurring the image.[2],[3],[4].

In [5] is conferred FIR filter based mostly Genetic mixed noise removal. A window of size 5 * 5 is taken into account. If the window is found in no abrupt changes in grey levels i.e. flat area, estimation of central pixel is that the average of all the constituents in window closes the central constituent. If it's not flat space, abrupt changes in intensity of the constituent, estimation of central constituent is that the averages of solely similar constituent close the central pixels. So as to avoid conversion between real valued and bit string, real valued chromosomes square measure used instead of bit strings.

In [6] bestowed spatially adjustive denoising algorithmic program for one image corrupted by Gaussian noise. During this work, local statistics like local weighted mean, local weighted activity and native maxima are accustomed observe the noise. So as to suppress the additive noise, a spatially additive Gaussian filter is employed. as a result of this filter is associate adequate thanks to handle the degree of local smoothness since it's pictured as perform of native statistics. During this planned methodology, the parameters like process price, over-smoothness, detection error, smoothing degree of re-constructed image ar taken in to associate account to effectively take away the noise elements.

2. TYPES OF NOISE

2.1. Salt and Pepper Noise

A typical variety of impulse noise in a very medical image is salt and pepper noise that represents itself as every which way occurring white (salt) and black (pepper) pixels. The noise density could be a term accustomed quantifies the number of salt and pepper noise in a picture. A complete noise density of nd in an $M \times N$ image means $nd \times M \times N$ pixels contain noise. In general, if the whole noise density of a salt and pepper noise is d, then it implies that every of the salt noise and therefore the pepper noise includes a noise density of $nd/2$. It's attainable that the salt noise and therefore the pepper noise have completely different noise densities as nd1 and nd2, and consequently the whole noise density is $nd = nd1 + nd2$

Fig.1. Salt and Pepper Noise

2.2. Speckle Noise

The speckle noise model may be approximated as multiplicative and is given by

$$n_{i,j=}nf_{i,j}m_{i,j} + a_{i,j} \quad (1)$$

Where $n_{i,j}$ represent the noisy pixel and $nf_{i,j}$ represent the noisy free pixel, $m_{i,j}$ signify the multiplicative noise and $a_{i,j}$ indicate the additive noise respectively i,j are indices of the spatial locations. Because the effect of additive noise is considerably smaller compared with that of multiplicative noise (1) may be written as

$$n_{i,j} = nf_{i,j}m_{i,j} \quad (2)$$

Logarithmic compression is applied to the envelope detected echo signal in order to fit within the display range [7]. Logarithmic compression affects the speckle noise statistics and it becomes very close to white Gaussian noise. The logarithmic compression transforms multiplicative form in (2) to additive noise form as

$$\log(n_{i,j}) = \log(nf_{i,j}) + \log(m_{i,j}) \quad (3)$$

$$x_{i,j} = y_{i,j} + n_{i,j} \quad (4)$$

The term $\log(n_{i,j})$ is the noisy image in the medical image after logarithmic compression is denoted as $x_{i,j}$ and the term $\log nf_{i,j}$, $\log m_{i,j}$ these are the noise free pixel and noisy component after logarithmic compression, as $y_{i,j}, n_{i,j}$ respectively

Fig.2. Speckle Noise

2.3. Poisson Noise

The noise in X-ray imaging and Nuclear Imaging (PET, SPECT) is sculptural with Poisson noise. X-ray photons incident on a receptor surface in an exceedingly random pattern. We have a tendency to can't force them to be evenly distributed over the receptor surface. One space of the receptor surface might receive a lot of photons than another space, even once each the area are exposed to identical average x-ray intensity. Altogether medical imaging procedures victimization gamma or x-ray photons most of the image noise is made by the random behavior of the photons that area unit distributed at intervals the image. This is usually selected quantum noise. Every individual photon could be a quantum (specific quantity) of energy. It's the quantum structure of associate x-ray beam that makes quantum noise [8].

A Poisson noise assume that each pixel x of an image f(x) is drawn from a Poisson distribution of parameter $\lambda = f_0(x)$ where f_0 is the original image to recover. The Poisson density is given as

$$p(f(x) = k) \text{ Is equal to } \lambda^k e^{-\lambda}/k! \quad (5)$$

Fig. 3. Poisson Noise

3. PROPOSED METHODOLOGY

The quality of image is corrupted by various noises in its acquisition and transmission as shown in fig 1, 2, 3. Image denoising becomes a major problem in the field of image processing [9]. Several noise reduction techniques are available for removing noise. Various algorithms are used to denoise the noisy image and individual filtering process is used to reduce the noise level. Due to the loss of edges the image is either blurred or over smoothed. Noise reduction is used to remove the noise without losing detail present in the images.

In existing algorithms such as SMF and AMF, median values are used to replace the corrupted pixels. But it fails in case of high noise density. To overcome this drawback, proposed method uses Iterative Decision Based Algorithm. At first, the proposed algorithm extracts the pixels corrupted by using three cases of windows such as minimum, maximum and median. By checking the pixel element value against the maximum and minimum values in the window selected, the corrupted and uncorrupted pixels in the image are detected.

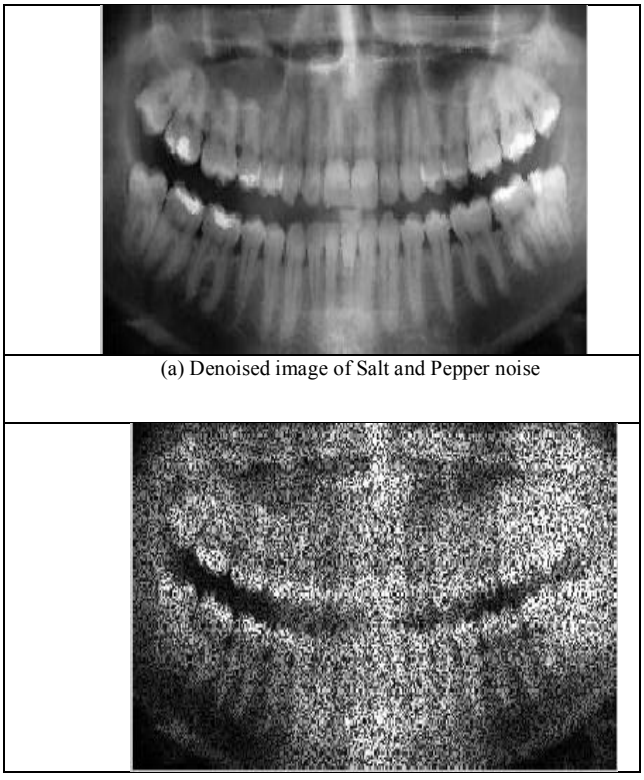
The maximum and minimum values of the impulse noise will be in the dynamic range of (0, 255). If the currently processed pixel has a value within the minimum and maximum values in the processing window, it is an uncorrupted pixel and it does not requires any modification. If the value is not within the range, the pixel becomes corrupted pixel and it will be replaced by either the median pixel value or by the mean of the neighborhood processed pixels (if the median itself is noisy).It results in smooth transition among the pixels. In the case of high noise density, the median value should be noisy. Therefore, the pixel value is replaced by the mean of the neighborhood processed pixels.

$$\begin{bmatrix} P_1 & P_2 & P_3 \\ P_4 & C & Q_1 \\ Q_2 & Q_3 & Q_4 \end{bmatrix}$$

In the 3×3 window, P1, P2, P3 and P4 indicates the pixel values which are processed already, C indicates the current pixel to be processed, and Q1, Q2, Q3 and Q4 indicates the pixels which are yet to be processed. If the median value of the window becomes noisy, then the current pixel value C will be replaced by the mean of the neighborhood processed pixels P1, P2, P3 and P4. The values of the pixels Q1, Q2, Q3 and Q4 should not be considered since they indicate the unprocessed pixels.

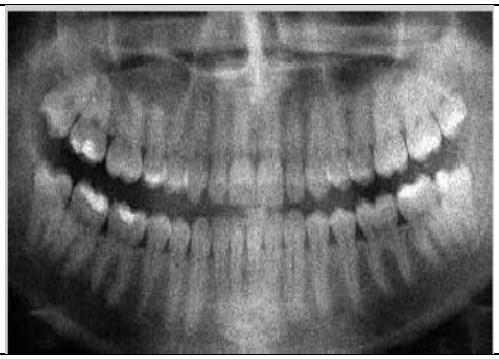
The steps of the algorithm are elucidated as follows:

- Select a two dimensional window W of size 3×3. Assume that the pixel being processed is C x, y.
- Compute – W min, W med and W max - the minimum, median and maximum of the pixel values in the window W respectively.
- Case a: If W min < Cx, y < Wmax, then Cx, y is an uncorrupted pixel and its value is left unchanged. Otherwise Cx, y is a noisy pixel.
- Case b: If Cx, y is a noisy pixel, it will be replaced by Wmed, the median value, only if Wmin < Wmed < Wmax.
- Case c: If Wmin < Wmed < Wmax is not satisfied, Wmed itself is a noisy pixel value. In this case, Cx, y will be replaced by the mean of the neighborhood processed pixels.
- Repeat Steps 1 to 3 until all the pixels in the entire image are processed.



(a) Denoised image of Salt and Pepper noise

(b) Denoised image of Speckle Noise



(c) Denoised image of Poisson Noise

Fig. 4. Denoised image

In these proposed output images also have some noise. So different type of filters are used to remove the noises in these image

4. TYPES OF FILTERS

4.1. Median Filter

Filtering is a part of image enhancement it is used to enhance certain details such as edges in the image that are relevant to the application. Additionally thereto, filtering can even be used to eliminate unwanted components of noise. Medical images typically contain salt and pepper noise and Poisson noise. This noise appears owing to the presence of minute grey scale variations within the image. Median filtering could be a widespread technique of the image improvement for removing noise without effectively reducing the image sharpness [10].

Median filter is kind of common as a result of it provides excellent noise-reduction talents, with primarily less blurring than similar size linear smoothing filters. Here, the median method was performed by simply a 3×3 windowing operator over the image. It considers each pixel and its neighbors in pictures to search out whether or not it's an illustration of the environment. It replaces the value of component with the median of the neighboring pixel components. Tend to calculate the median by sorting the whole component values from the neighborhood into numeral sort then replaced the component being studied with the middle component worth. If the neighborhood below condition constitutes a good pixel worth, the common of the 2 middle component values is that the median.

4.2. FIR Filter

As we know, linear system parameterization is Associate in an important category of system modeling with a large space of applications. The foremost standard among the category of linear model is that the finite impulse response (FIR). It's obligatory in order to modify the estimation task and to scale back the computational load in time period application. Let $u(i,j)$ be the input of a linear 2DFIR model, defined over a regularly spaced lattice $(i,j) \in [I_1, I_2]$, where I_1, I_2 specify the order of the input data. The output of the 2D finite impulse response (FIR) digital filter, $y(i,j)$ is given by 2D finite impulse response (FIR) digital filter, $y(i,j)$, is given by

$$y * i,j) = \text{summation}\,(w(t,I)u(i-t,j-1))$$

Where the value of $t = 0$ to $N_1 - 1$, $I = 0$ to $N_2 - 1$ and $u(i,j)$ is the input signal $w(t,I)$ is the model coefficients and N_1, N_2 specify the order of the FIR filter. Usually, the 2D signal is presented as a matrix. Therefore, the weight matrix $w(i,j)$ and then input matrix (i,j) .

4.3. Gaussian Filter

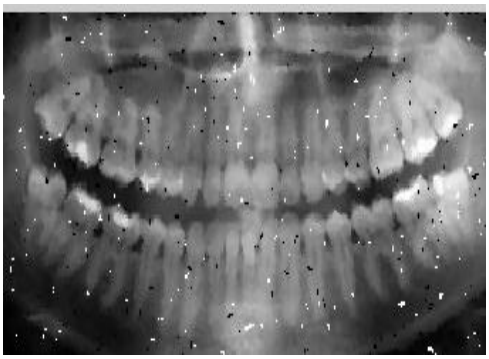
Among all linear filters, Gaussian filter perhaps plays the most important role in both theory and applications. Gaussian filtering is a commonly used image filtering technique which is a WAP with weights defined as $w_{ij} \propto \exp\left(-\left\|x_i - x_j\right\|\right), i \neq j$

$$w_{ij} = 0$$

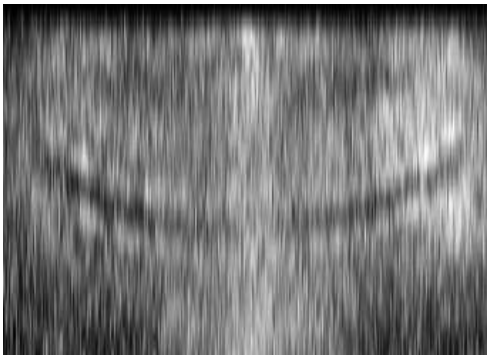
Where $\|.\|_2$ is the L2 norm. Because of the rapid decay of w_{ij} as a function of distance. Gaussian smoothing is effectively a local filtering method. As an image denoising algorithm Gaussian filter is well known to over smooth images, resulting in the loss of significant detail, especially edge sharpness.

5. EXPERIMENT RESULTS

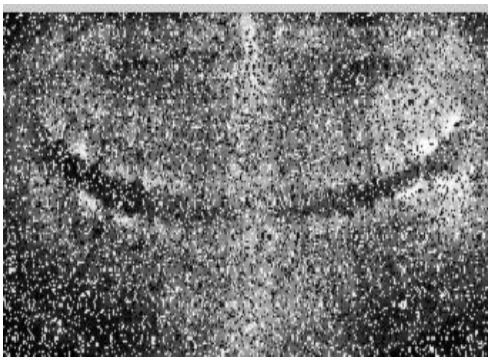
This section discusses the experimental results that obtained by applying the previously described median filter, fir filter, Gaussian filter to the salt and pepper noise, speckle noise, Poisson noise .



(a)Removal of salt and pepper noise using Median filter

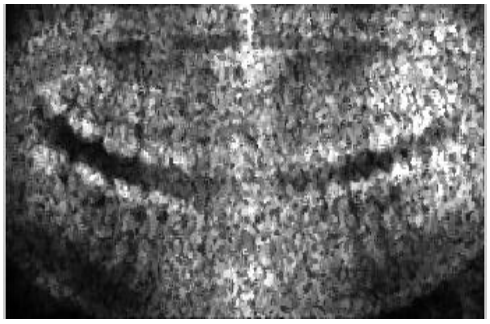


(b) Removal of salt and pepper noise using Fir filter

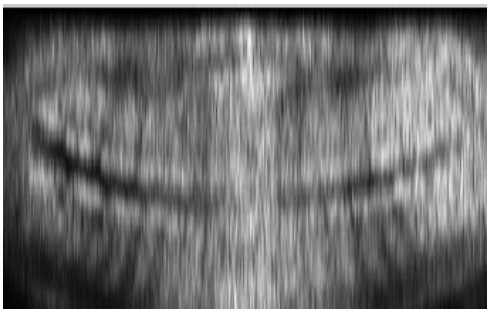


(c) Removal of salt and pepper noise using Gaussian filter

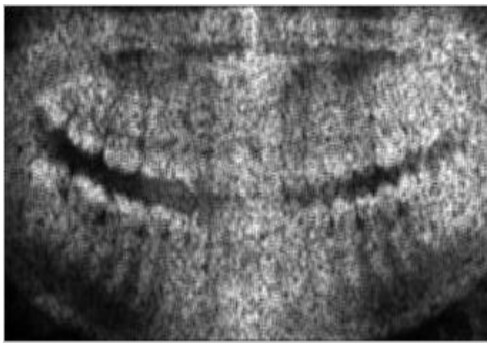
Fig. 5 removal of salt and pepper noise using different filters



(a) Removal of speckle noise using median filter

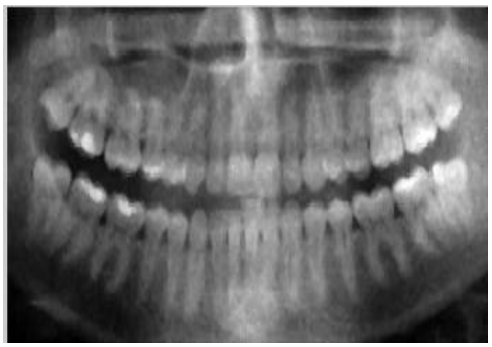


(b) Removal of speckle noise using Fir filter



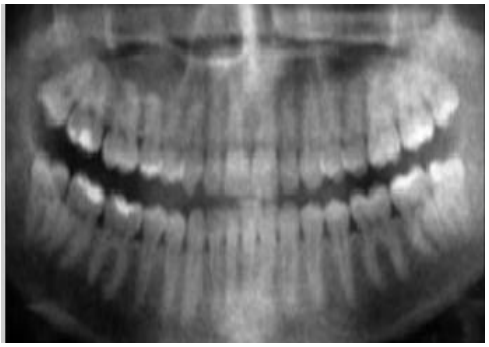
(c) Removal of speckle noise using Gaussian filter

Fig. 6 Removal of speckle noise using different filters



(a) Removal of Poisson noise using median filter

(b) Removal of Poisson noise using Fir filter



(c) Removal of Poisson noise using Gaussian filter

Fig. 7 Removal of Poisson noise using different filters

We show experimental evidence of the arguments proposed in Fig 5, 6, 7. First, our interest is in determining if the quality metrics based on the Mean Square Error (MSE) are sufficient tools in determining the quality of denoised images. For this, we measure the MSE and PSNR and SNR of denoised images.

5.1. PSNR

PSNR is the Peak Signal-to-Noise ratio in decibels (dB). The PSNR is only meaningful for data encoded in terms of bits per sample, or bits per pixel.

$$\mathrm{PSNR} = 20\log10\left(255/\sqrt{\mathrm{MSE}}\right) \quad (1)$$

5.2. MSE

MSE is defined as mean square error

$$\mathrm{Error} = \mathrm{abs}(A - B) \quad (2)$$

$$\mathrm{MSE} = \left(\sqrt{\left(\mathrm{mean}\left(\mathrm{mean}(\mathrm{Error}.\hat{}2)\right)\right)}\right) \quad (3)$$

Where Error is difference between the absolute value of A and B Where A is the filtered image and B is the Denoised image

5.3. SNR

SNR is defined as Signal to Noise Ratio, it is calculated as

$$dv = \mathrm{var}(B(:), 1) \quad (4)$$

$$\mathrm{SNR} = 10 * \log10(dv/\mathrm{MSE}) \quad (5)$$

Where dv is used to calculate the variance of the denoised image of B

TABEL 1 Salt and Pepper Noise

Filter	MSE	SNR	PSNR
Median Filter	16.1102	21.5710	23.9888
FIR Filter	39.5464	17.6709	16.1887
Gaussian Filter	29.4191	18.9557	18.7582

TABEL 2 Speckle Noise

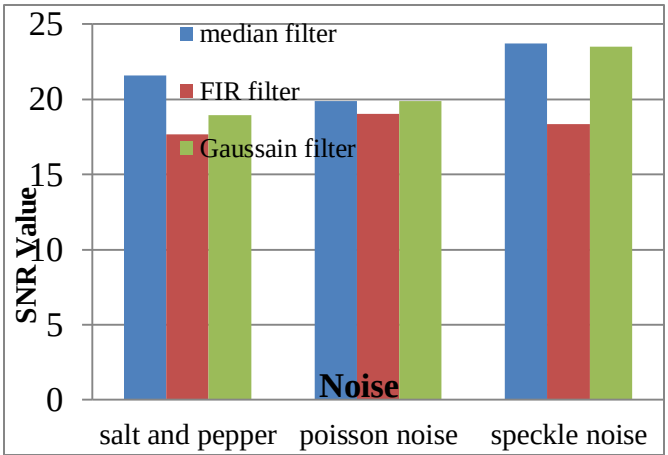
Filter	MSE	SNR	PSNR
Median Filter	55.0061	19.8825	12.8950
FIR Filter	66.5863	19.0528	11.6631
Gaussian Filter	57.7815	19.6688	11.7826

TABLE 3 Poisson Noise

Filter	MSE	SNR	PSNR
Median Filter	10.3225	23.7178	27.8551
FIR Filter	35.5534	18.3468	17.1132
Gaussian filter	10.8411	23.5049	27.4293

To evaluate the filter effectively, three main statistical measures are used. They are PSNR, MSE, and SNR. To compare these output values and find out the better filtering result of denoised X-ray images.

In table 1 the performance of various filter for salt and pepper noise. Each filter in table 1 is tested and compared with other type of filter by using of output value of PSNR, MSE, and SNR. In this median filter technique is comparatively good for high density noise. It is observed



that the filter have PSNR and SNR is high compared to other filters and also it have low MSE value.

The second categories of the filtering method for the speckle noise has taken for the discussion and performed with three types of filters are shown in table 2. Median filter gives best result compared with other type of filters. In overview of all the filters in table2, median filter gives much improved results and providing a high degree of performance.

The third categories of this filtering method for the Poisson noise are shown in table 3. Here also median filter gives a high performance other than other type of filters.

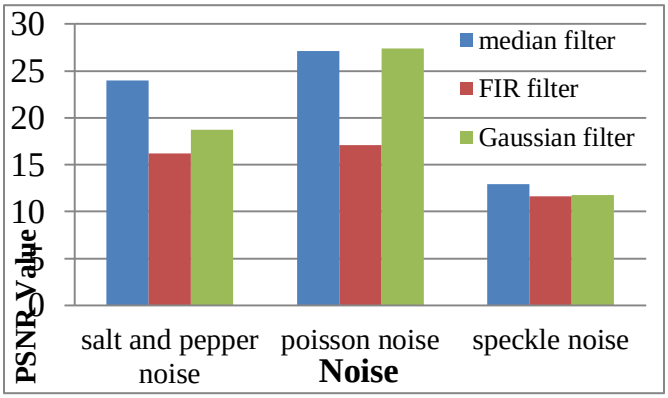


Fig. 8 Comparison of PSNR value for three type of Noise using different filters

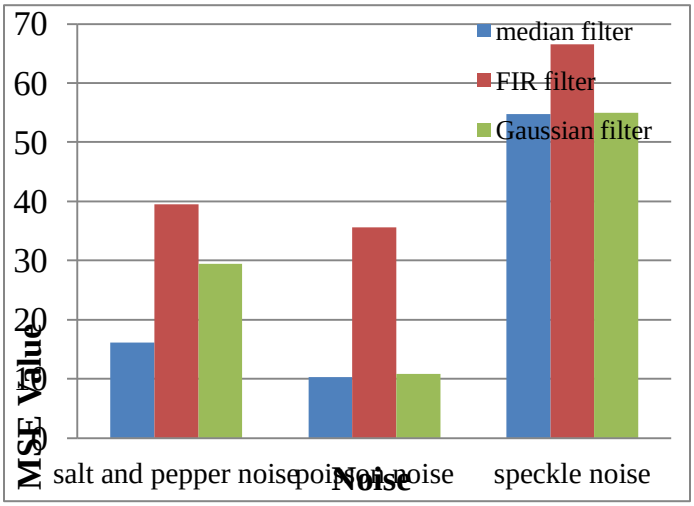


Fig. 9 Comparison of MSE value for three type of noise using different filter

Figure 8 shows the Peak Signal-to-Noise-Ratio improvement as function of the noise level for the proposed filters and, for comparison, of median filter, Fir filter, Gaussian filter. In this three type of noises are salt and pepper noise, Speckle noise, Poisson noise. In this Poisson noise have high PSNR value used by median filter.

Figure 9 shows Mean Squar Error for three type of noise used filtering of median filter, Fir filter, Gaussian filter. Comparsion of MSE value in figure 9 , Poisson noise have low MSE value done by median filter.

Fig. 10 Comparison of SNR Value for three type of noise using different filter

Figure 10 shows the Signal to Noise Ratio. Here also poisson noise have hign SNR value are done by median filter.

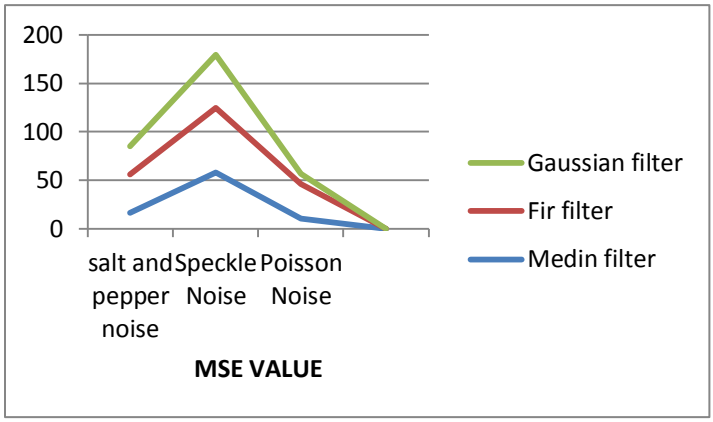


Fig. 11 comparison of MSE value for three filters

From figure 11 clearly noticed that the median filter provide better performance

6. DISCUSSION AND CONCLUSION

As per discussed in x-ray dental. After finding the salt and pepper noise in X-ray image various filtering techniques have been applied and it is found that the median filter works better for the noisy image. PSNR value is 23.9888 and MSE value is 16.1102

After finding the speckle noise in X-ray image various filtering techniques have been applied and it is found that the median filter works better for the noisy image. PSNR value for this 12.8950 and MSE value 55.0061 and SNR value 19.6688

After finding the Poisson Noise in X-ray image various filtering techniques have been applied and it is found that the median filter works better for the noisy image. PSNR value 27.8551 and MSE value 10.3225 and SNR value 23.7178.

In this work we have taken medical images X-ray dental image for detecting noises. We have detected Salt & Pepper noises and speckle noise and Poisson noise also removed these noises from the above medical images by applying the various filtering techniques like Median Filtering, FIR filtering, Gaussian filtering. The results are analyzed and compared with standard pattern of noises and also evaluated through the quality metrics like MSE, SNR, and PSNR. Through this work we have observed that the choice of filters for de-noising the medical images depends on the type of noise and type of filtering technique, which are used. It is remarkable that this saves the processing time. And also compare three types of filter and observe median filter gave the best accuracy. This experimental analysis will improve the accuracy of X-ray dental image. The results, which we have achieved, are more useful and they prove to be helpful for general medical practitioners to analyze the symptoms of the patients.

7. REFERENCES

[1]. Kh. Manglem Singh, —Fuzzy Rule based Median Filter for Gray-scale Images, Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, April 2011.

[2]. 2. Faten A.A.Dawood, Rahmita W.Rahmat, and Suhaini B. Kadiman et al. "Automatic boundary detection of wall motion in two dimensional echocardiography images". Journal of computer science. J. computer sci., 2011, 7(8), pp: 1261-1266.

[3]. 3. Md. Robiul Hoque, and Md. Rashed-al-Mahfuz. "A new approach in spatial filtering to reduce speckle noise". International journal of soft computing and Engineering. IJSCE, 2011, volume-1, Issue-3, pp: 29-30.

[4]. 4. Juan Zapata and Ramon Ruiz. "On Speckle noise reduction in Medical Ultrasound Images",Recent advances in signals and systems, 2009, pp:126-131.

[5]. M.S. Safari, A. Aghagolzadeh," FIR filter based Fuzzy-Genetic Mixed noise removal", IEEE 2007.

[6]. Tuan-Anh Nguyen, Won-Seon Song, Min-Cheol Hong," Spatially Adaptive Denoising algorithm for a single image corrupted by Gaussian noise", IEEE Transaction on Consumer Electronics, Vol. 56, No. 3, Aug 2010, pp 1610-1615

[7]. V.Dutt, "Statistical analysis of ultrasound echo envelope,"Ph.D. dissertation, Mayo Graduate School, Rochester, 1995.

[8]. D.T. Kuan and A.A. Sawchuk, "Adaptive noise smoothing filter for images with signal dependent noise," IEEE Trans. Pattern Anal. Mach. Intell., vol. PAMI-7, no. 2, pp. 165–177, 1985.

[9]. Rafeal C. Gonzalez and Richard E. Woods, "Digital image processing," 2"'t, ed. Addison Wesley Longman, 1999.

[10]. Chan, R.H., C.W. Ho and M. Nikolova, Salt-and pepper noise removal by median-type noise detectors and detail-preserving regularization. IEEETrans. Image Proc., 14: 1479-1485. 2005

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 443 - 448, 2013, ISSN: 2319–8656

Priority Based Hybrid Automation Testing Tool

Priyanka
Thapar University
Patiala, India

Sunita Garhwal
Thapar University
Patiala, India

Abstract: Software testing is an important means to ensure software quality and to improve software reliability. As the size and complexity of software applications is continually growing, manual testing becomes infeasible in such arena. Automation of the software testing process saves time and provides better utilization of resources and thus, plays a significant role in the testing activity.

This paper presents a hybrid testing tool which extends the support to automatic testing by providing functionality of both GUI and Code based testing. Moreover, it also prioritizes modules under test to achieve a certain degrees of confidence in the testing of web applications that are under tight project deadlines. The proposed hybrid approach allows to combine the benefits of both approaches while keeping a simple interface and treating the two types of tests in a unified fashion.

Keywords: Testing, Automation, Priority, Hybrid Testing, Code Parser

1. INTRODUCTION

Software organizations are competitive in all the aspects, especially in terms of the quality of the products to be delivered and the context of the time line. With the increasing demands for faster time-to-market and the continuous growth of higher software quality, the software market is becoming more challenging. These challenges are embedded in all areas of software engineering, including verification and validation. Also, increase in the software complexity raises the probability of more defects.

Software tests have to be repeated often during development cycles to ensure quality. Every release of the software may be tested on all supported operating systems and hardware configurations. Manual testing is costly and time consuming whereas, automating the testing process provides the solution for improving the effectiveness of software testing [1]. Thus, automation testing plays an important role in ensuring testing software quality and reliability.

Automation testing is an important aspect in software industry. In order to develop an effective automation tool, a priority based hybrid automation tool has been designed. The existing GUI automation tool is enhanced by adding the functionality of code based testing which is further improved by adding a layer of priority to the automation testing [2]. The tool is used to create completely automated tests for the validation of the functionality and behaviour of the application.

1.1 GUI Testing

GUI testing is a process to test application's user interface to detect whether application is functionally correct or not. GUI tests are performed from the view of the end users of the application and thus, GUI testing is vital for quality assurance[3]. It involves carrying set of tasks and comparing the respective outcomes with the expected output and ability to repeat same set of tasks multiple times with different data inputs and same level of accuracy. GUI testing is used to determine whether the various GUI components

react in the desired manner or not. Implementing GUI testing improves quality, speeds up development process and reduces risks towards the end of the software development life cycle[4]. It can be performed manually with the help of human tester as well as automatically with the help of a software program.

1.2 Manual vs. Automatic Testing

Manual and automation are two different approaches of testing with same goal. Manual testing is conducted by writing test cases and then manually executing them[1]. Automation Testing makes use of software to control the execution of tests and the comparison of actual outcomes with predicted outcomes. Manual testing has advantage of human intuition and common sense which can't be replaced by automation tools but on the other end, it is time consuming, cumbersome and repetitive process and thus, often fails to provide required coverage for the testing process which requires multiple execution cycles. In contrast to manual testing, automated testing requires very less effort on developer's side. It not only automates test case execution, but also test case generation and test result verification. When using automated testing systems, users have to specify what to test and not how. In particular this means that the users have to automatically select relevant manual test cases with regards to the current testing goal [4]. A fully automated testing system is able to test the entire software without any user intervention. Manual testing of software is tedious task and thus, there is a great need for reducing the high costs by means of automated testing [5].

2. PROPOSED TOOL

The proposed tool is a combination of following:

i) Manual testing

ii) Automation testing

iii) Code driven testing

iv) Priority based testing

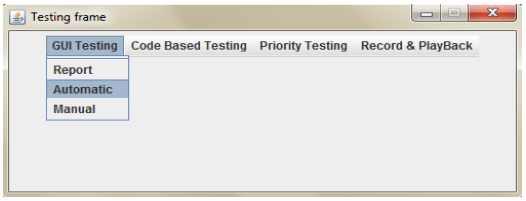


Figure 1. Testing Tool Window

2.1 Manual Testing

It is the process of manually testing the software for defects/bug. Manual testing requires a tester to perform the manual test operations without the help of any automation software.

A manual tester performs the following steps:

i) Select the module to be tested

ii) Enter a test case manually

iii) Execute the test.

iv) Verify the actual result with expected result.

v) Record the results as pass or fail.

vi) Make a summary report of pass and fail test cases.

vii) Publish the report.

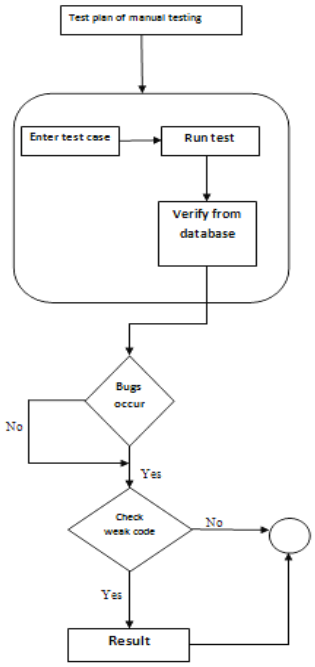


Figure 2. Flow Chart of Manual Testing

2.2 Automation Testing

Automation testing means using automation tool to execute the test case suites. It involves the use of software to control the execution of the test.

The tester would perform the following steps for automation testing.

i) Select the module to be tested.

ii) Browse the test case suite file.

iii) Start the testing process.

The automation tool performs the following:

i) Enter the test data into the system under test.

ii) Compare the actual outcomes with predicted outcomes

iii) Record the test case results as pass or fail

iv) Generate the detailed test report

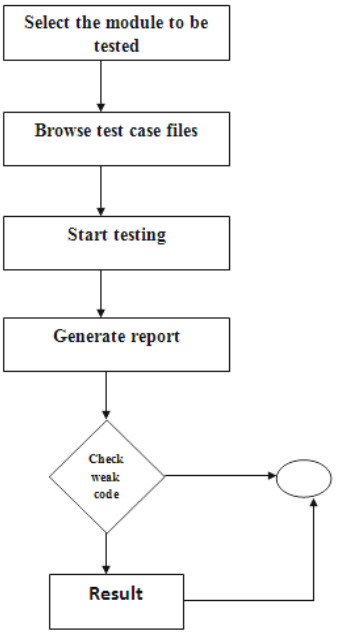


Figure 3. Flow Chart of Automation Testing

2.3 Code Based Testing

The principal of code based testing is to have each and every event/action in the program executed at least once during the test. On the basis of the code based testing, a tester attempts to determine all the reachable elements in the software under the test. The testing process begins by first creating a xmi file for the software under test followed by parsing the xmi to examine the weak code i.e. the code which is not being used during the current execution of the software.

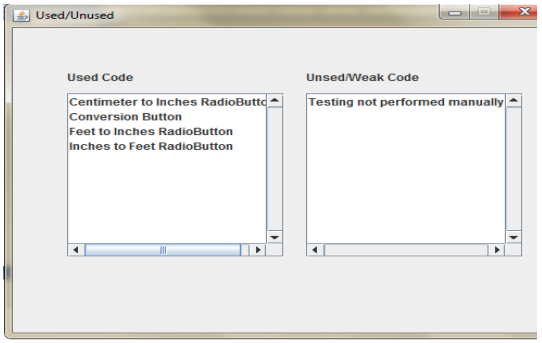


Figure 4. Weak Code Window for Priority Testing

2.4 Priority Based Testing

In this phase of testing, tester defines priority for various modules of application under test. The priorities will be used to execute tests over the specified modules in a specific order. High priority modules will be tested prior to the low priority modules.

Once the testing process for a particular module is over, the test report is generated and the tester is notified accordingly. The testing process continues till the test report for each module under test is generated successfully.

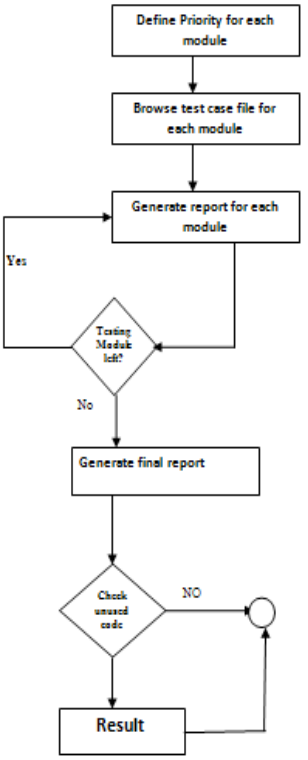


Figure 5. Flow Chart of Priority based Testing

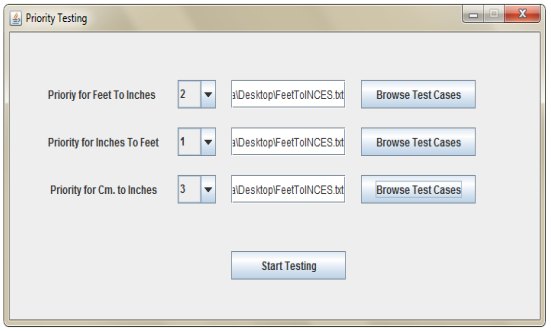


Figure 6. Input Frame for Priority based Testing

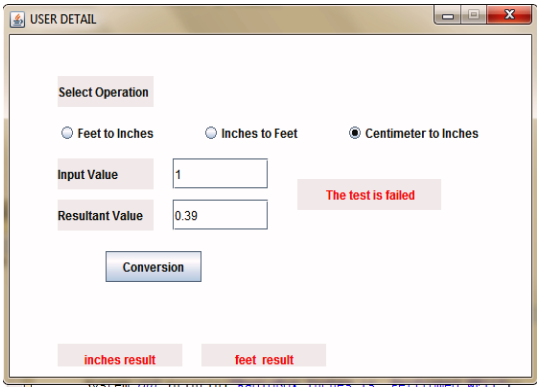


Figure 7. Notifications on Testing Window

2.5 Responsibilities of Proposed Tool

The proposed tool has the following capabilities:

i) *Efficiency in recording*: It can capture all the events and actions that were performed on the application during the automation and manual testing which ever being performed at that particular instant of time.

ii) *Reporting of test results*: The test results can be reported passed/failed statement at the time of manual, automation and priority testing.

iii) *Parsing the code*: It can parse i.e. analyze the source code of any program written in java to examine the various fields, methods, constructors and the interfaces of the java program being examined.

iv) *On camera testing*: The user has a privilege to have the snapshots of the various events involved during the whole testing process.

v) *Prioritizing the testing of modules*: The user can prioritize various modules under test to define the flow of testing in the required manner.

vi) Finding the weak code: The tool can help the user to determine the weak code i.e. code not being used during the testing of the software under observation.

2.6 Comparative Analysis of Testing Types

The following graph shows the efficiency of various types of testing in terms of time. From the results, it can be concluded that priority based testing is more efficient in terms of time in comparison to automatic and manual testing.

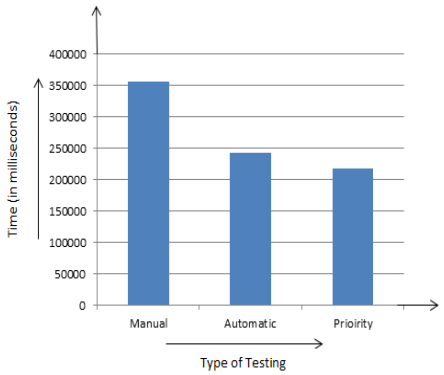


Figure 8: Testing Vs. Time

3. CONCLUSION

GUI testing is vital for quality assurance because the GUI tests are performed from the view of the end users of the application. Many times all the functionality of the application can be invoked through the GUI and therefore GUI tests can cover the entire application.

As the size and complexity of software is continually growing, manual testing becomes very difficult and tedious task. But on the contrary, automated testing can help to improve efficiency of the testing process in order to identify areas of a program that are prone to failure.

The proposed model allows the user to define priority for each of the modules under test. After each of the modules is tested effectively, the corresponding testing report is generated automatically and is available for the review while other modules are being tested. The priority based automation tool helps to minimize the user intervention to a large extent, which makes it highly efficient and less time consuming.

The code based testing helps the user to identify the structural components which are not being used in that particular phase of the testing process, hence enables user to debug the entire application efficiently. The capability of record and playback and on-camera testing further improves the efficiency of tool.

Hence, priority based hybrid automation tool proves to be highly efficient in terms of quality and time.

4. FUTURE SCOPE

Various future opportunities that can be explored are as follows:

i) The code parsing feature of the proposed tool is able to parse only the java source code files which can be extended by making the it language independent.
ii) The design of tool can be generalized to test any GUI java application.
iii) More features of the code based testing can be explored so that the tool can serve as a total solution for testing.

5. REFRENCES

[1] A. Leitner, I. Ciupa and B. Meyer, "Reconciling Manual and Automated Testing: the AutoTest Experience", Proc. 40th Hawaii International Conference on System Sciences, pp: 261-271, January 2007.

[2] M. Ali, S. Mushtaq and N. Arshad., "Priority-Based Automated Testing of Web Application", Proc. IEEE Conference on Communication and Information Technology, 2012.

[3] P .Nagarani and R. VenkataRamanaChary "A Tool Based Approach for Automation of GUI Applications", Proc. 3rd IEEE International Conference of Computing Communication &Networking Technologies, pp: 1-6, July26-28, 2012.

[4] P. Aho, N. Menz and T. Räty "Enhancing Generated Java GUI Models with Valid Test Data", Proc. IEEE Conference on Open System, September 2011.

[5] J.Prabhu and N.Malmurugan "A Model for GUI Automated Testing Framework in Software System", *International Journal of Computer Applications*, vol. 64, no.15, February 2013.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 449 - 454, 2013, ISSN: 2319–8656

Shape Oriented Feature Selection for Tomato Plant Identification

A. Hazra
Department of Computer Science & Engineering, Jadavpur University, Kolkata, India

K. Deb
Department of Computer Science & Engineering, Jadavpur University, Kolkata, India

S. Kundu
Department of Computer Science & Engineering, Jadavpur University, Kolkata, India

P. Hazra
Faculty of Horticulture, Bidhan Chandra Krishi Viswavidyalaya, Kalyani, Nadia, India

Abstract: Selection of relevant features for classification from a high dimensional data set by keeping their class discriminatory information intact is a classical problem in Machine Learning. The classification power of the features can be measured from the point of view of redundant information and correlations among them. Choosing minimal set of features optimizes time, space complexity related cost and simplifies the classifier design, resulting in better classification accuracy. In this paper, tomato (Solanum Lycopersicum L) leaves and fruiting habits were chosen with a futuristic goal to build a prototype model of leaf & fruit classification. By applying digital image processing techniques, tomato leaf and fruit images were pre-processed and morphological shape based features were computed. Next, supervised filter and wrapper based feature selection techniques were adopted to choose the optimal feature set leading to small within-class variance and large among-class distance which may be of utter importance in building the model for recognition system of the tomato leaf and fruiting habit genre.

Keywords: Tomato Leaf, Tomato Fruit, Morphology, Feature Selection, Filter based Feature Selection, Wrapper based Feature Selection

1. INTRODUCTION

Being one of the most consumed vegetables worldwide and cultivating in almost every corner of the world, Tomato (Solanum Lycopersicum L) gained economic importance by the beginning of twentieth century. Wild Tomatoes are native of western South America, distributed from Ecuador to northern Chile, and with two endemic species in the Galápagos Islands (Peralta and Spooner, 2005). It is one of the most investigated species, both in genetic and genomic studies (Foolad 2007). So it becomes a necessity to classify and recognize the large number of cultivars present in Tomato for farmers, seed producing agencies, botanists, Agricultural R&D labs and others. Plant Identification is important in GIS based remote sensing and in national parks, where a botanist manually identifies the species through time-consuming, tedious experiments. Thus digital image processing techniques can be applied to the verification process to increase speed up, accuracy and fully automation. The following table (Table 1) shows the Species for tomatoes and their wild relatives along with their fruit colour.

Leaf/fruit classification is a tough task as inter-class similarities or intra-class variations are quite natural in mathematical modelling of biological samples (colours and textures are quite similar in different tomato species). Also colour depth, variation along with textures of the leaves and fruits usually change with plant age so colour based recognition of the samples is not realistic. The variations in the gray scale histogram images (Figure 1) belonging to same cultivar/species were shown which gives enough evidence about the limitations of the colour image processing techniques in this case. Here we have chosen shape oriented feature extraction strategies, after which best features were selected based upon filter and wrapper based techniques. A detailed flow diagram is given (Figure 2).

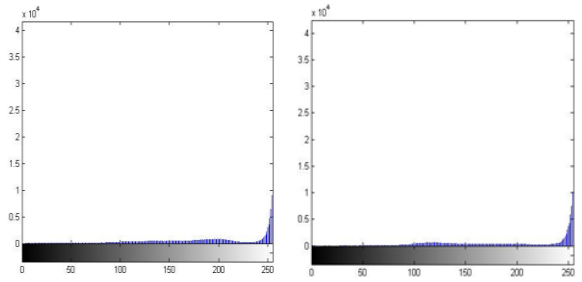


Figure 1 – Histogram showing Intra class variations in same tomato leaf/fruit species

2. DATA COLLECTION, PRE-PROCESSING

Images were collected at dawn in Bidhan Chandra Krishi Viswavidyalaya to avoid the sunlight noises and each image (2816 X 2112 pixels) was captured from an equidistant point to avoid the overhead related to image normalization. The image samples were categorized based on their genetic characters i) Top Leaflet and ii) Fruit Bearing Habit (Figure 3). Then the noisy backgrounds were replaced by a white uniform background (Figure 4). After that, the pre-processing steps were carried out in which the images were complemented, converted to HSV Colour space, grey scale and finally to binarized images. Next the morphological operations (thinning, small component removal, morphological dilation, noise prone zone removal) were performed to get the enhanced binarized images (Figure 5). Once we get the enhanced binarized images, morphological shape features were calculated by approximating the leaf boundary with an ellipse and fruiting habit as an irregular shape. The longest length (Major Axis/Branch Length) and breadth (Minor Axis/Branch Width) of leaves and fruits

(Figure 5) were calculated from the developed user interface. All shape based features are described in the next section.

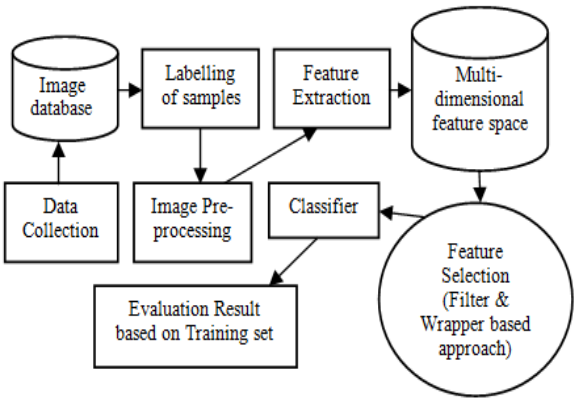


Figure 2 – Proposed feature selection and evaluation approach

Figure 3 - Top Leaflet and Fruiting Habit

Figure 4 - Processed Images of Top Leaflet and Fruiting Habit

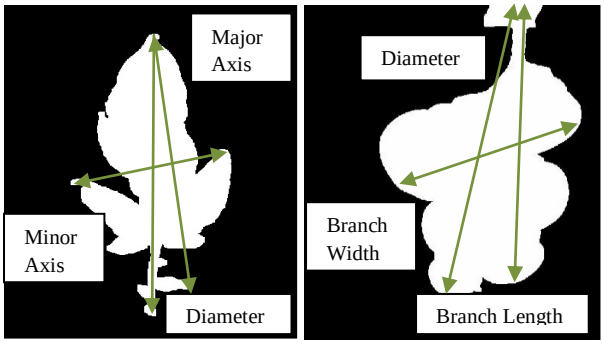


Figure 5 – Choosing Main features from the GUI end

Table 1 – Different tomato cultivars all around the world

New nomenclature	Fruit color
Solanum lycopersicoides	Green-yellow when maturing, black when ripe
Solanum sitiens	Green-yellow when maturing, black when ripe
Solanum juglandifolium	Green to Yellow green
Solanum ochranthum	Green to Yellow green
Solanum pennellii	Green
Solanum habrochaites	Green with darker green stripes
Solanum chilense	Green to whitish green with purple stripes
Solanum huaylasense	Typically green with dark green stripes
Solanum peruvianum L.	Typically green to greenish-white, sometimes flushed with purple
Solanum corneliomuelleri	Typically green with dark green or purple stripes, sometimes flushed with purple
Solanum arcanum	Typically green with dark green stripes
Solanum chmeilewskii	Typically green with dark green stripes
Solanum neorickii	Typically green with dark green stripes
Solanum pimpinellifolium L.	Red
Solanum lycopersicum L.	Red
Solanum cheesmaniae	Yellow, orange
Solanum galapagense	Yellow, orange

3. FEATURE SELECTION

3.1 List of Morphological Features

- **Major Axis/Branch Length (L):** The length between the top and bottom end of the leaf/ fruit branch.(Averaged) (Figure 5)
- **Minor Axis/Branch Width (W):** The breadth between the two distant ends of the leaf/ fruit branch.(averaged) (Figure 5)
- **Aspect Ratio/Length Width Ratio (A_R):** Ratio between the Major Axis (Branch Length) and Minor Axis (Branch Width). [$A_R = L / W$]
- **Orientation/Branch Angle (α):** Angle between the Major Axis (Branch Length) with X axis; representing leaf/fruiting branch bending nature).
- **Eccentricity (€):** Ratio of the distances between two foci of an ellipse. (Applicable for leaf feature only). [€ = $\sqrt{1 - b^2/a^2}$, 2a,2b being the lengths of Major and Minor Axis respectively,$0 < € < 1$ in case of ellipse]
- **Area (A):** Total amount of space inside the two dimensional leaf/fruiting branch surface.
- **Perimeter (P):** Two dimensional 8 connectivity based neighborhood boundary of the closed geometric leaf/fruit surface.
- **Equivalent Diameter(E_D):** The diameter of the circle with the same area with the two dimensional leaf/fruit surface.
- **Number of On Pixels (O_P):** The total count of white pixels inside the leaf/fruit surface.
- **Form Factor(F_F):** The "roundness" of the leaf/fruiting branch.[$F_F = 4\pi A / P^2$]
- **Rectangularity(R):** Measures how rectangular the leaf/fruiting branch is. [R = L.W/A]
- **Solidity(S):** Ratio between the Area (A) of the binarized image and the Area of its Convex Hull ($A_{convex\ hull}$). [$S = A / A_{convex\ hull}$]

- **Concavity (C_a):** Difference between the Convex Hull Area ($A_{convex\ hull}$) and Area (A) of the binarized image. [$C_a = A_{convex\ hull} - A$]
- **Perimeter Ratio/Major-Minor Axis(P_R):** The ratio between the Perimeter(P) and the summation of its Major Axis(Branch Length) and Minor Axis(Branch Width). [$P_R = P/ L+W$]
- **Convexity(C):** Ratio between the Perimeter of the Convex Hull ($P_{convex\ hull}$) and the actual Perimeter (P) of the binarized image. [$C= P_{convex\ hull} / P$]
- **Smooth Factor(S_F):** Ratio of the image area smoothened by a 5×5 median filter to that smoothened by a 2×2 median filter.
- **Diameter (D):** The longest distance between any two points on the closed geometric surface of the leaf/fruiting branch.(Fig. 5)
- **Narrow Factor (N_F):** The "narrowness" of the leaf/fruiting branch. [$N_F = D/L$]
- **Perimeter Ratio of Diameter (P_{RD}):** Ratio of the Perimeter (P) and Diameter (D) of the Leaf/fruiting branch. [$P_{RD} = P/D$]
- **Compactness (C_A):** Associating the Area (A) of the image sample over its Diameter (D).[$C_A = \sqrt{4A/\pi}/D$]
- **R-Factor (R_F):** Ratio of the Perimeter of the Convex Hull ($P_{convex\ hull}$) and Diameter (D). [$R_F = P_{convex\ hull} / D$]
- **Euler Number (E_N):** The topology of a binarized image measured as the total number of objects in the image minus the total number of holes in the image.

3.2 Feature Selection

There are several approaches available for feature subset selection in machine learning. Selection of most effective features for classification from a large data set can be obtained by three basic selection strategies i) filter method ii) wrapper method and iii) embedded method. In filter based method, an attribute evaluator is used to evaluate the attributes/features and a ranker to rank all the features present in the feature data set. Next, the lower ranked features are omitted one by one and predictive accuracy is checked each time through a classifier (by measuring Mean Absolute Error, RMS Error, Relative Absolute Error, Root relative Squared Error etc.). One problem is that there is a possibility of being over fit of the model in filter based methods because the weights put by the ranker algorithm in order to rank the features can be very different than the weights put by the classification algorithm. The wrapper based approach uses a subset evaluator which creates all possible subsets from the multidimensional feature data set by using a search technique (Best First Search, Linear Floating forward Selection). Then a classifier is used to evaluate each feature subset to consider the subset with which the classifier performs the best recognition result. In embedded method, classifier dependent feature selection is done. In this work, filter and wrapper based techniques were adopted to observe the outcomes.

Feature selection and classification tasks were performed with the open-source WEKA Machine Learning workbench. In case of filter based technique, both univariate (Information Gain, Ben-Bassat, 1982) and multivariate (Correlation based feature selection, Hall, 1999) approaches were used. In case of wrapper based approach, classifier subset evaluation using Naive Bayes classifier was utilized to test the instances along with different search strategies. Knowledge of the dependencies among the features can be gained by finding out the internal relationships among the features and the quantification of their descriptive powers.

4. EXPERIMENTAL RESULTS

4.1 Filter based Approaches (Information-Gain and Correlation measurement)

Information gain, being a goodness measurement criterion in machine learning and associating with entropy calculation, measures the purity of randomly drawn examples. Through Information Gain technique, all the features can be ranked using ranker search method from the feature set. The entropy of a random variable X is defined as

$$H(X) = -\sum_{i=0}^{m} p(x) log_2((p(x)) \quad \textbf{(1)}$$

Where m is the number of observed outcomes of the random variable X, p(x) being the probability density function for X. Now, if the observed value of random feature variable X is evenly distributed according to Y, then the entropy of X after observing Y is

$$H(X/Y) = -\sum_{i=0}^{m} p(y) \sum_{i=0}^{m} p\left(\frac{x}{y}\right) log_2((p(x/y)) \quad \textbf{(2)}$$

Hence the information gain depicts the extra information of X with respect to Y, saying the amount of entropy decreased for X, formulated as Information gain = H(X)−H(X/Y). According to the Info-gain phenomenon, the feature ranking of the 10 and 14 best features of tomato leaf and fruit feature data set from the 22 morphological features were shown (Figure 6). The classification result on the data set was given (Figure 7) which depicts that the percentage of the correctly classified leaf and fruit instances using Naive Bayes classifier are 82.2% and 97.62% respectively. The Cohen's kappa coefficient of tomato leaf and fruit classes is 0.8095 and 0.9744, describing the statistical measure of inter-rater agreement for tomato leaf and fruit feature variables along with mean absolute error, R.M.S. error, relative absolute error and root relative squared error measurements(Figure 7). The total numbers of instances used in training of tomato leaf and fruit classes are 45 and 42 respectively. The performance of the Naive Bayes classifier was measured by observing some crucial parameters e.g. True positive rate (TP rate), False positive rate (FP rate), Precision, Recall, F-score/F-measure, Receiver operating characteristics (ROC) area. It is observed that the average true class prediction (TP rate) rate being 82.22% and 97.6% for the tomato leaf and fruiting habit respectively. The class prediction rates (average) being positive in case of false samples (FP rate) are 0.013 and 0.002. The precision for the tomato leaf and fruiting habit indicates the ratio between the true positive over the total retrieved samples are 86.1% and 98.2% respectively and a recall indicates the fraction of relevant instances that are retrieved are 81.4% and 100%. F-score/F-measure is an accuracy measurement criterion of a classifier which is the harmonic mean of the precision and recall.

$$\text{F-Score/F-Measure} = \frac{2\times(precision\times recall)}{(precision\times recall)} \quad \textbf{(3)}$$

81.4% and 97.6% F-Measure are found in leaf and fruit feature data sets. The Receiver operating characteristics (ROC) curve is the plot between FP rate and TP rate showing

the behaviour of a classifier. The AUC (area under the curve) measure is noted as 0.981 and 1 which is almost ideal for a classifier (Figure 8). So, the result depicts that Naive Bayes classifier acts ideally on tomato leaf and fruiting habit data.

Ranking Value	Attribute Name
1.347	Minor Axis
1.209	Diameter
1.209	R-Factor
1.195	Perimeter Ratio of Diameter
1.155	Rectangularity
0.961	Compactness
0.909	Perimeter Ratio
0.787	Eccentricity
0.787	Aspect Ratio
0.562	Major Axis
0	Area
0	Orientation
0	Euler number
0	Convexity
0	Concavity
0	Narrow Factor
0	Smooth Factor
0	On Pixel
0	Equivalent Diameter
0	Solidity
0	Form Factor
Search Method	Attribute Ranking
Attribute Evaluator	Information Gain Ranking Filter
	(Supervised)

Ranking Value	Attribute Name
2.335	Narrow Factor
1.933	Aspect Ratio
1.474	Perimeter Ratio
1.23	Branch Width
1.227	Rectangularity
0.827	Branch Length
0.738	Diameter
0.738	Perimeter Ratio of Diameter
0.736	On Pixel
0.736	Area
0.736	Equivalent Diameter
0.736	solidity
0.732	Perimeter
0.732	Convexity
0	R-Factor
0	Euler Number
0	Smooth Factor
0	Form Factor
0	Compactness
0	Orientation
Search Method	Attribute Ranking
Attribute Evaluator	Information Gain Ranking Filter
	(Supervised)

(Figure 6 - Ranking of the leaf and fruit attributes through Information Gain Ranking Filter)

Correctly Classified Instances	37	82.22%
Incorrectly Classified Instances	8	17.77%
kappa Statistic	0.8095	
Mean Absolute Error	0.0265	
Root mean Squared Error	0.1387	
Relative Absolute Error	21.31%	(Approx.)
Root relative Squared Error	55.61%	(Approx.)
Total Number of Instances	45	(Training)

Correctly Classified Instances	41	97.62%
Incorrectly Classified Instances	1	2.38%
kappa Statistic	0.9744	
Mean Absolute Error	0.0025	
Root mean Squared Error	0.0427	
Relative Absolute Error	1.88%	(Approx.)
Root relative Squared Error	16.57%	(Approx.)
Total Number of Instances	42	(Training)

Figure 7 - Evaluation result and accuracy measurement on Tomato Leaf/Fruiting habit data set using CFS and Info-gain techniques

TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Tomato Leaf Class
1	0	1	1	1	1	Class 1
0.667	0	1	0.667	0.8	0.992	Class 2
1	0	1	1	1	1	Class 3
1	0	1	1	1	1	Class 4
1	0	1	1	1	1	Class 5
0.667	0	1	0.667	0.8	0.992	Class 6
1	0.024	0.75	1	0.857	0.976	Class 7
0.667	0.024	0.667	0.667	0.667	0.992	Class 8
0.333	0	1	0.333	0.5	0.968	Class 9
1	0.071	0.5	1	0.067	1	Class 10
1	0	1	1	1	1	Class 11
1	0.024	0.75	1	0.857	0.992	Class 12
0.333	0.024	0.5	0.333	0.4	0.865	Class 13
1	0.024	0.75	1	0.857	0.976	Class 14
0.667	0	1	0.667	0.8	0.968	Class 15
0.822	**0.013**	**0.861**	**0.822**	**0.814**	**0.981**	**(Weighted Avg.)**

TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Tomato Fruit Class
1	0	1	1	1	1	Class 1
1	0	1	1	1	1	Class 2
1	0	1	1	1	1	Class 3
1	0	1	1	1	1	Class 4
1	0	1	1	1	1	Class 5
1	0	1	1	1	1	Class 6
1	0	1	1	1	1	Class 7
0.667	0	1	0.667	0.8	1	Class 8
1	0.026	0.75	1	0.857	1	Class 9
1	0	1	1	1	1	Class 10
1	0	1	1	1	1	Class 11
1	0	1	1	1	1	Class 12
1	0	1	1	1	1	Class 13
1	0	1	1	1	1	Class 14
0.976	**0.002**	**0.982**	**0.976**	**0.976**	**1**	**(Weighted Avg.)**

Figure 8 - Performance evaluation of Naive Bayes classifier for each class; feature selection based on Information gain technique

This section discusses on correlation based feature selection techniques. Correlation based Feature Selection (CFS) is a multivariate method used in feature selection with some popular search strategies like best first search (BFS) and linear floating forward selection (LFFS) etc. Naive Bayes classifier was used to validate the results. The correlations among attributes and category variable can be classified into weak correlation, strong correlation and without any correlation. An ideal feature vector is strongly correlated with category attribute and not correlated with any other feature vectors (otherwise they are redundant). In this work, linear correlation coefficient measurement with Pearson product moment criterion was computed to find the correlations among the features and category attribute. Generally, the correlation measurement is defined as

$$\text{Correlation } x, y = \frac{\sum_{i=1}^{n}(x_i - x')(y_i - y')}{(n-1)STD_x \; STD_y} \quad \textbf{(4)}$$

$$x' = \sum_{i=1}^{n} x_i \quad , \quad y' = \sum_{i=0}^{n} y_i \quad \textbf{(5)}$$

$$\mathbf{STD_x} = \frac{\sqrt{\sum_{i=1}^{n}(x_i - x')^2}}{n-1}, \; STD_y = \frac{\sqrt{\sum_{i=1}^{n}(y_i - y')^2}}{n-1} \quad \textbf{(6)}$$

Where x, y are feature vectors x', y' are their means, STD_x and STD_y are the standard deviations of feature vectors x and y. The range of Correlation varies between -1 to 1. The more the $|\text{Correlation}_{x, y}|$ approaches towards 1, correlation between x , y increases. If $\text{Correlation}_{x, y}$ is zero, the features are independent of each other, and if $\text{Correlation}_{x, y}$ approaches towards -1, the features are more negatively correlated. CFS technique evaluates the worth of a subset of features by considering their individual predictive ability along with the degree of redundancy among them with a searching strategy (Best First search, Exhaustive search, Linear Forward Selection etc.). The most relevant features found in CFS method are listed below. (Table 2) The performance of Naive Bayes classifier applied on the most relevant feature set found using CFS technique was given in the following figure. (Figure 9)

Table 2 - Top Leaflet and Fruiting Habit

Problem Set	Best Features
Tomato leaf feature data set	Minor Axis, Aspect Ratio, Rectangularity, Perimeter Ratio, Diameter, Perimeter Ratio of Diameter, R-Factor
Tomato fruiting habit feature data set	Branch Width, Aspect Ratio, Perimeter, Rectangularity, Concavity, Perimeter Ratio, Diameter, Narrow Factor, Perimeter Ratio of Diameter

TP Rate	FP rate	Precision	Recall	F-Measur	ROC Area	Class
1	0	1	1	1	1	a
0.667	0.024	0.667	0.667	0.667	0.992	b
1	0	1	1	1	1	c
1	0	1	1	1	1	d
1	0	1	1	1	1	e
0.667	0	1	0.667	0.8	1	f
1	0.024	0.75	1	0.857	1	g
0.667	0	1	0.667	0.8	1	h
0.667	0.024	0.667	0.667	0.667	0.992	i
1	0.048	0.6	1	0.75	1	k
1	0	1	1	1	1	l
0.667	0	1	0.667	0.8	1	m
0.333	0	1	0.333	0.5	0.992	n
1	0.048	0.6	1	0.75	1	o
0.822	0.013	0.863	0.822	0.817	0.998	Weighted Average

TP Rate	FP rate	Precision	Recall	F-Measur	ROC Area	Class
1	0	1	1	1	1	a
1	0	1	1	1	1	b
1	0	1	1	1	1	c
1	0	1	1	1	1	d
1	0	1	1	1	1	e
1	0	1	1	1	1	f
1	0	1	1	1	1	g
1	0	1	1	1	1	h
1	0	1	1	1	1	i
1	0	1	1	1	1	k
1	0	1	1	1	1	l
1	0	1	1	1	1	m
1	0	1	1	1	1	n
1	0	1	1	1	1	o
1	0	1	1	1	1	Weighted Average

Figure 9 - Performance evaluation of Naive Bayes classifier; features selected using CFS based technique

4.2 Wrapper based Approach

As a part of wrapper based feature selection, some search methods (best first search and linear floating forward selection) were used in combination with Naive Bayes classifier to find out the best subset of features with which the Naive Bayes classifier performs the best recognition result. A basic flow diagram was given. (Figure 10)

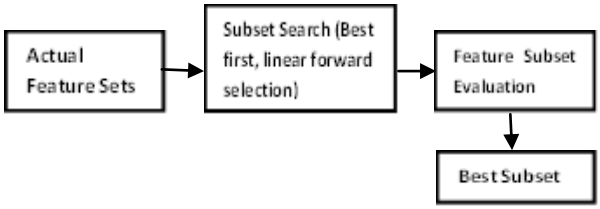


Figure 10 – Wrapper based classifier sub-set evaluation via Naive Bayes classifier

Best first (Greedy Hill climbing augmented with backtracking facility) search and Linear floating forward selection search strategies were taken individually to find out the best discriminating feature sub set for tomato leaf and fruiting habit recognition model. As a classifier, Naive Bayes algorithm was used as an inductive algorithm to estimate the merits of the feature sets. A stopping criterion for the selection of feature subset was specified as the number of subsets can be huge. So, a predefined number of iterations were specified for this purpose. After the selection of the best subset of features for tomato leaf and fruiting habit data set, a validation procedure was also adopted to check the predictive accuracy of the subset based on the Naive Bayes classifier.

Search Method for Leaf Data Set	Selected Attributes
	Minor Axis
Best First Search	Area
	Perimeter Ratio of Diameter
Linear Forward Floating Selection	Minor Axis
	Concavity
	Perimeter Ratio of Diameter

Search Method for Fruiting Habit Data Set	Selected Attributes
Best First Search	Aspect Ratio
	Perimeter Ratio
	Narrow Factor
Linear Forward Floating Selection	Aspect Ratio
	Perimeter Ratio
	Narrow Factor

Figure 11 – Most relevant features selected for Tomato Leaf/Fruiting Habit Data Set

Correctly Classified Instances	37	82.22%
Incorrectly Classified Instances	8	17.77%
Kappa Statistic	0.8095	
Mean Absolute Error	0.0191	
Root Mean Squared Error	0.1255	
Relative Absolute Error	15.3125	
Root Relative Squared Error	50.3026	
Total Number of Instances	45	

Correctly Classified Instances	42	100.00%
Incorrectly Classified Instances	0	0.00%
Kappa Statistic	1	
Mean Absolute Error	0	
Root Mean Squared Error	0	
Relative Absolute Error	0	
Root Relative Squared Error	0.00%	
Total Number of Instances	42	

Figure 12 – Evaluation through Naive Bayes classifier and accuracy measurement on Tomato Leaf/Fruiting Habit Data Set

TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
1	0	1	1	1	1	a
0.667	0.024	0.667	0.667	0.667	0.992	b
1	0	1	1	1	1	c
1	0	1	1	1	1	d
1	0	1	1	1	1	e
0.667	0	1	0.667	0.8	1	f
1	0.024	0.75	1	0.857	1	g
0.667	0	1	0.667	0.8	1	h
0.667	0.024	0.667	0.667	0.667	0.992	i
1	0.048	0.6	1	0.75	1	j
1	0	1	1	1	1	k
0.667	0	1	0.333	0.5	0.992	l
0.333	0	1	0.333	0.5	0.992	m
0.667	0.024	0.667	0.667	0.667	0.992	n
1	0.048	0.6	1	0.75	1	0
0.822	0.013	0.863	0.822	0.817	0.998	Weighted Average

TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
1	0	1	1	1	1	a
1	0	1	1	1	1	b
1	0	1	1	1	1	c
1	0	1	1	1	1	d
1	0	1	1	1	1	e
1	0	1	1	1	1	f
1	0	1	1	1	1	g
1	0	1	1	1	1	h
1	0	1	1	1	1	i
1	0	1	1	1	1	j
1	0	1	1	1	1	k
1	0	1	1	1	1	l
1	0	1	1	1	1	m
1	0	1	1	1	1	n
1	0	1	1	1	1	Weighted Average

Figure 13 – Performance evaluation of Naive Bayes classifier; features selected using Wrapper based technique

It is observed that the best discriminatory features recorded using best first search technique are minor axis, area, perimeter ratio of diameter, aspect ratio and perimeter ratio, narrow factor in case of tomato leaf and fruiting habit feature data set respectively. Similarly in case of linear floating forward selection strategy, the best relevant features are minor axis, concavity, perimeter ratio of diameter and aspect ratio, perimeter ratio, narrow factor for tomato leaf and fruiting habit feature data set. (Figure 11)

An overall 82.22% and 100% recognition accuracy using Naive Bayes algorithm with kappa statistic 0.8095 and 1 were noted with optimally chosen tomato leaf and fruiting habit features using wrapper based approach (Figure 12) and the predictive accuracies are almost ideal for each of the leaf and fruiting habit classes (Figure 13). An important observation was noted that in both filter and wrapper based approaches the recognition accuracy of tomato leaf data set was 82.22 % but in case of fruiting habit data set it became 97.6%(Info-gain), 100%(CFS) and 100%(wrapper based). So, better predictive accuracy for fruiting habit data set was observed in case of CFS and wrapper based techniques. These observation results may be of utter importance when building a leaf/fruiting habit recognition model.

5. CONCLUSION

An elaborative description and observation results are produced in this work where the concentration was given to supervised learning based feature subset selection problems using both filter and wrapper based approaches. Here, we have investigated both univariate (Information gain) and multivariate (Correlation based) feature selection strategies with horticultural feature data set. But embedded feature selection strategies like Simulated Annealing, Decision Tree or Random Multinomial Logit (RMNL) also demand a lot of attention which need to be explored. The relevant attributes found in separate feature selection approaches were evaluated and compared using Naive Bayes algorithm. In Info-gain method, reduced number of features were 10, 14 and in CFS technique it is 7, 9 whereas in wrapper based approach it is 3, 3 respectively from 22 number of features. When these different techniques can be combined a better classification result may be obtained for tomato leaf and fruiting habit. Also scope for automating the whole process and investigating other methods for feature selection requires further studies.

6. REFERENCES

[1] S. Kundu, A. Hazra, K.Deb, P. Hazra, “Dimensionality Reduction of Morphological features of Tomato Leaves and Fruiting Habits”, IEEE International Conference on Communications, Devices and Intelligent Systems, CODIS-2012, pp. 608-611.

[2] Pavan Kumar Mishra, Sanjay Kumar Maurya, Ravindra Kumar Singh, Arun Kumar Misra, “A semi-automatic plant identification based on digital leaf and flower Images”, IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM - 2012).

[3] M. Dash, H. Liu, “Feature Selection for Classification”, Intelligent Data Analysis 1 (1997) 131-156, Elsevier.

[4] Hossain. J. and M. A. Amin, “Leaf Shape Identification Based Plant Biometrics”, Proceedings of 13th International Conference on Computer and Information Technology (ICCIT 2010).

[5] J. Huang, N. Huang, L. Zhang, H. Xu, “A method for feature selection based on the correlation analysis”, IEEE International Conference on Measurement, Information and Control (MIC 2012).

[6] George H. John, Ron kohavi, Karl Pfleger, “Irrelevant Features and the Subset Selection Problem”, Machine Learning: Proceedings of the Eleventh International Conference, 1994Morgan Kauffmann Publishers, San Francisco, CA.

[7] Pat Langley, “Selection of Relevant Features in Machine Learning”, Proceedings of the AAAI Fall Symposium on Relevance (1994), New Orleans, LA.

[8] Yvan Saeys, Inaki Inza, Pedro Larranaga, “A review of feature selection techniques in bioinformatics”, BIOINFORMATICS, vol. 23 no. 19 2007, pages 2507-2517.

[9] Dionysios Lefkaditis, Georgios Tsirigotis, “Morphological feature selection and neural classification for electronic components”,Journal of Engineering Science and Technology Review 2(1), 2009, 151-156.

[10] Jinsong Leng, Craig valli, Leisa Armstrong,“A wrapper-based Feature Selection for Analysis of Large Data Sets”, 3rd International Conference on Computer and Electrical Engineering,(ICCEE 2010),pp. 166-170.

[11] Yvan Saeys, Inaki Inza, Pedro larranaga, “ A review of feature selection techniques in bioinformatics”,BIOINFORMATICS,vol. 23 no. 19 2007. Pages 2507-2517.

[12] Ron Kohavi, George H. John, “ Wrappers for feature subset selection”, Artificial Intelligence 97(1997) 273-324, ELSEVIER.

[13] Hai Nguyen, Katrin Franke, Slobodan Petrovic, “Improving Effectiveness of Intrusion Detection by Correlation Feature Selection”, IEEE International Conference on Availability, Reliability And Security, pp. 17-24.

[14] M.Hall,“Correlation Based Feature Selection for Machine Learning”, Doctoral Dissertation, University of Waikato, Department of Computer Sceince ,1999.

[15] Ben-Bassat, M., “Pattern Recognition and Reduction of Dimensionality”, In P.R. krishnaiah and L.N. Kanal,editors, Handbook of statistics-II, North Holland,1982, 773-791.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 455 - 458, 2013, ISSN: 2319–8656

Dynamically Adapting Software Components for the Grid

B. Dhanalakshmi
Aryabahata Institute Of Technology and Science
Jawaharlal Nehru Technological University
Hyderabad, India

Abstract: The surfacing of dynamic execution environments such as 'grids' forces scientific applications to take dynamicity. Dynamic adaptation of Grid Components in Grid Computing is a critical issue for the design of framework for dynamic adaptation towards self-adaptable software development components for the grid. This paper carries the systematic design of dynamic adaptation framework with the effective implementation of the structure of adaptable component. i.e. incorporating the layered architecture environment with the concept of dynamicity.

Keywords: grid; adaptation; resources; entities; component specific level; component independent level.

1. INTRODUCTION

A grid [4] is a type of parallel and distributed system, which aims at exploiting the ability to share and aggregate distributed computational capabilities. Number of resources may differ from processor to processor or processor to grid [4] while performing scientific applications. Therefore, adopting the software components for the programming model enables security and portability on different resource infrastructures.

This adaptability framework project model can be used to adapt the software components at run time to varying conditions. This framework report gives the transparency of adaptability in scientific and distributed applications by giving the framework impact and its requirement. This gives the ability of software to autonomously react and repair non convenient events observed during program execution without any intervention by the programmers.

Adaptability ensures that the application continuously executes the best configuration depending on the actual execution environment.

2. PROPOSED SCHEME

In this scheme, the applications involve several services like information services, resources reservation/allocation, file transfer and job launching and monitoring, which are executed on different environments. Grid components may change in processor availability, network availability, resource sharing between applications, administration tasks, failures etc...These environments constitute a disseminated, heterogeneous, highly dynamic communication structure that makes the applications as adaptive software includes different mechanisms to modify the behavior of application or components dynamically. This scheme suggests a layered approach model to put together self-adaptive entities:

The central stage level defines the mandatory functionalities for adaptive entities, while upper stage levels define the structure to bring together primitive or composite components adaptation [11].

With the allocated resources, we may define the best way that is used by scientific applications modify themselves depending on their actual execution environment. This framework gives the ability of software to *autonomously react to* and *repair non convenient events observed* during program execution without any intervention by the programmers /users. In the autonomous computing, adaptation is further characterized as activity performed by code, acts to events, performs suitable actions, identifies wrong behavior etc..

This paper presents a framework intended to help developers in the task of designing dynamically adaptable components, which puts the emphasis on an experimental evaluation of the cost of using such a framework.

3. DYNAMIC ADAPTATION

In order to achieve an adaptation, a component needs to be able to get information about the system (the component itself and its environment), to make a decision according to some optimization rules and to modify or replace some parts of its code. Any scientific system amalgamates its modifications in a crystal clear way for its end users. These modifications include adapting to variable run-time conditions, masking failures, performance measures and the evolution of scientific application components. 'Dynamic adaptation' [1] coats different techniques for managing all these modifications in the execution environment.

Dynamic adaptation [5] is classified into three dimensions named kinds, characteristics and techniques. These dimensions are introduced because they answer the frequent questions of administrators and developers of the application. This classification is the result of our investigation of existing adaptable platforms.

For the sake of reusability, it is highly desirable to separate the adaptation engine from the content of the component. I capture adaptability within a framework as Dynamic Adaptation for Components (Dynaco [1]). Associated to a component's content, it forms a dynamically adaptable component.

This paper presents a framework intended to help developers in the task of designing dynamically adaptable components,

which puts the emphasis on an experimental evaluation of the cost of using such a framework.

4. DYNAMIC ADAPTATION

Applications are of 2 types as, Resource-Aware: describe resources options, select resources and then run and Dynamic Adaptive: collect runtime information, consider/decide to change resources, select resources and run.

A generic adaptability framework for decomposition of adaptability in 4 steps: Observe the execution environment as it evolves, Decide that the component should adapt, Plan how to achieve the adaptation, Schedule and execute planned actions.

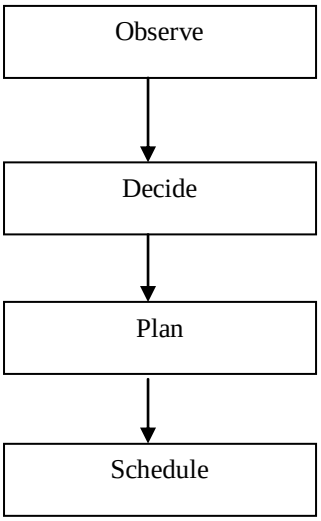


Figure 1. Proposed Design Architecture

4.1 Architectural Design

This divides adaptability into some number of sub-functionalities as Able to observe characteristics of the environment in order to trigger adaptability; When a change is detected, the framework has to decide an adaptation strategy according to observed measures; Once a strategy has been decided, the framework has to plan actions to implement it;

At last; planned actions have to be executed synchronously with the execution of applicative code.

This model exhibits the functional description for the adaptation process with the entities Decider, Planner and Executor. The environmental changes received as events will affect the decider and produces as a strategic plan for dynamic adaptation.

The *Planner* derives list of actions from the strategy in order to achieve the different steps of the process of adaptation. The *executor* implements the different steps of adaptation to modify the component.

Software components that are used in the adaptability framework are separated into some number of functional "boxes" disseminated into 3 levels as shown in figure 1. At the functional level, the service provides an expected implementation of the component is expected to do. If the component was not dynamically adaptable, then it would have the service.

The *component-independent level* [1] contains all mechanisms that can be defined independently of the content of the service functional box. The decider box is the start point of any adaptation. It decides whether the component should be adapted or not.

The *component-specific level* [1] holds the specializations of the adaptation framework for the developers. The specified framework consent the developer to focus the decider for the needs of its component. It describes how decisions can be made. The plan templates describe how the planner can build plans depending on the requested reaction and on the current execution environment.

4.2 Structural Design

This splits adaptability into four sub-functionalities as Able to observe characteristics of the environment in order to trigger adaptability; When a change is detected, the framework has to decide an *adaptation strategy* [5] according to observed measures; Once a strategy has been decided, the framework has to plan actions to implement it;

At last; planned actions have to be executed synchronously with the execution of applicative code.

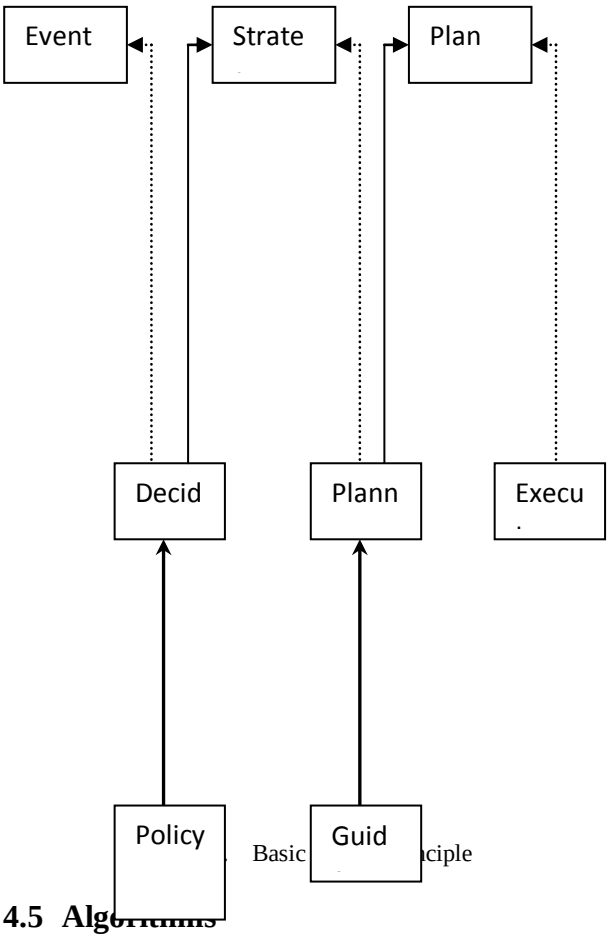
4.3 Events Generation

The Decision making process[2] of dynamic adaptation given by the policy procedure which will give the information about the decisions and strategies that are used to change the component's behavior depending on the execution environment.

Monitors [13] are the entities that are used to create the events and these events are helpful in the monitoring of components execution. All these events are observed by decider or monitor.

4.4 Adapting the Components

Subsequent to adaptation plan, next is the executor's turn, which is regarded as a virtual machine [13] that will monitor the control flow instructions with in the adaptation plan depending on the execution schedule. To do so executor depends on the adaptation points [2] this will have the information about component states. The component states are constrained by integrity and consistency requirements.



Basic nciple

4.5 Algorithms

Following are the two algorithms that are used in this framework.

4.5.1 Converter

The first algorithm, the *converter* converts a given component to particular interface by deterministically matching the given component/interface pair to an adapter on demand. The algorithm will rely on the executable notations for interfaces, adapters and components, e.g., it will have to find out at runtime which edges a given component supports and which borders a given adapter maps to.

4.5.2 Binder

The second algorithm, the *binder* combines the given interface with an implementation instance, which is considered as a component or a component enclosed by adaptors.

4.6 Autonomic Implementation of the Schema

The schema notation of this framework is as below.

do

{

decide:

what has to adapt

what has to discard

how to adapt

on trigger:

decide possible implementations for the policy

commit:

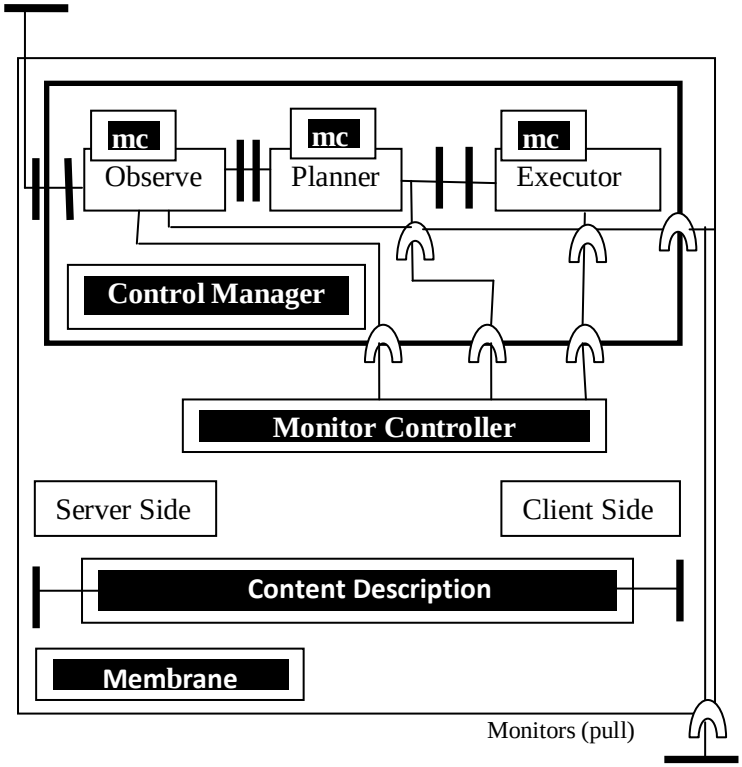
plan for predefined implementation

plan adaptive code mechanisms

schedule all the executable operations

} while(!end)

Monitors (push)



Monitors (pull)

Figure 3. Structure of an adaptable component using this Framework [13]

4.7 Realization as a Framework Model

In the Framework model realization, the two contents are defined as: The *content description* realizes the component state functionalities; the *membrane* [2] is a possessor consisting of non-functional services that manage the component's behavior. In an adaptation plan, dynamic execution environments depend on the behavior of dynamically adaptable components. The *Control Manager* is responsible for the existed components. A modification controller (mc) realizes the adaptable component's actions.

The *executor* [13] execute actions depending on the plans given by the planner. Server sides (push model) and client

sides (pull model) are applicable to the adaptable component while executing them.

Modifications are possible by pushing and pulling the adaptation methods by which the model implements the adaptability concept on components.

5. CONCLUSION

This framework analyses how to design dynamic adaptability support for scientific applications. It is independent of formalisms and technologies. Also evaluate the proposed model as well as the possibilities to write generic adaptation policies at the collection and application levels.

This framework for adaptability is independent of the applications like numerical algorithms, transaction systems etc…

Still lot of problems to be investigated / solved (adaptation policies, performance models ...). For the future work, the activity of generalizing the approach is considered. i.e., generic definition of global adaptation points should be implemented.

6. ACKNOWLEDGMENTS

My sincere thanks to the experts, who have contributed towards development of this framework.

7. REFERENCES

[1] Jérémy Buisson, Françoise André, and Jean-Louis Pazat. Dynamic adaptation for grid computing. In P.M.A. Sloot, A.G. Hoekstra, T. Priol, A. Reinefeld, and M. Bubak, editors, Advances in Grid Computing- EGC 2005 (European Grid Conference, Amsterdam, The Netherlands, February 14-16**, 2005**, Revised Selected Papers), volume 3470 of LNCS, pages 538–547, Amsterdam, February **2005.** Springer-Verlag.

[2] Je´re´my Buisson, Franc¸oise Andre´, and Jean-Louis Pazat. Performance and practicability of dynamic adaptation of parallel computing : an experience feedback from Dynaco. Publication interne 2006 Projeeects Paris.

[3] Jérémy Buisson, Françoise André, and Jean-Louis Pazat. Enforcing consistency during the adaptation of a parallel component. In The 4th International Symposium on Parallel and Distributed Computing, July **2005**.Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[4] Greg Burns, Raja Daoud, and James Vaigl. LAM: An Open Cluster Environment for MPI. In *Proceed- ings of Supercomputing Symposium*, pages 379–386, **1994**.

[5] Introduction to Grid Computing – A IBM’s red book for details about Grid Computing is also useful for installation of Globus Tool Kit 4.

[6] Jérémy Buisson, Françoise André and Jean-Louis Pazat. A framework for dynamic adaptation of parallel components**.** In *ParCo 2005*, Málaga, Spain, 13-16 September **2005**.

[7] Pierre-Charles David and Thomas Ledoux. Towards a framework for self-adaptive component-based applications. In *DAIS’03*, volume 2893 of *LNCS*. Springer-Verlag, November **2003.**

[8] Brian Ensink and Vikram Adve. Coordinating adaptations in distributed systems. In *24th International Conference on Distributed Computing Systems*, pages 446–455, March **2004**.

[9] Brian Ensink, Joel Stanley, and Vikram Adve. Program control language: a programming language for adaptive distributed applications. *Journal of Parallel and Distributed Computing*, 63(11):1082–1104, November **2003**.

[10] Introduction to Grid Computing – A IBM’s red book for details about Grid Computing is also useful for installation of Globus Tool Kit 4.

[11] Research group on “Performance models and adaptivity”: http://www.di.unipi.it/~marcod/WP3homepage/RG_adaptivity/index.html

[12] Segarra, M.T. ; Dept. of Comput. Sci., IT/TELECOM-Bretagne, Brest ; Andre, F.Autonomic and Autonomous Systems, 2009. ICAS '09. Fifth International Conference on « Building a context-aware ambient assisted living application using a self adaptive distributed model

[13] http://hal.archives-ouvertes.fr/docs/00/05/76/49/PDF/PI-1782.pdf

.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 459 - 464, 2013, ISSN: 2319–8656

Interweaving Knowledge Acquisition and Product Functionality

C.Janani
Department of Computer Applications,
Bharathiar University,
Coimbatore, India

T.Devi
Department of Computer Applications,
Bharathiar University,
Coimbatore, India

Abstract: This research is concerned with the detailed study on Product Functionality and to select a Knowledge Acquisition Method for Acquiring Knowledge on Product Functionality efficiently. The purpose of this research is to ensure that important aspects of product data are taken into account in knowledge management projects. The most important venture of this research is to design a questionnaire for acquiring knowledge on product functionality, and then test the designed questionnaire with certain industrial product data collection.

Keywords: Knowledge, Product Functionality (PF), Product Knowledge, Knowledge Acquisition (KA), Bill of Materials (BOM)

1. INTRODUCTION

This research is concerned with the process of Acquiring Knowledge on Product Functionality efficiently. A product must perform to meet customer needs and the functional requirements to capture the intended behavior of the product - what the product will do. This behavior may be expressed as functions, tasks, or services the product is required to perform. In order to be successful in a global market, a product developed must provide better functionality to its users in comparison to the current products. This research paper analyses the product introduction process in order to identify basic element, relationship of a product in an organization. It also presents a fundamental structure for understanding product functionality and the prerequisite for their integration. The main objective of this paper is to acquire knowledge on product functionality using industrial product data collection.

A product is an object developed by human or mechanical effort or by natural process. It can be anything produced as a result of generation or growth or labor or thought or by operation of unintentional causes. A product is viewed upon as a technical system, which is as a set of interrelated subsystems or machine elements comprising a whole article that intends to achieve a particular function [Maryam A and Dorothy E, 2001]. A product not only depends upon one single function, but also on a sequence of key functions, which together describes its worth. In order to have control over the diverse goal of a new product development process, functional and physical integration of the product is very vital. Experts define a product's functionality as a set of rules/goals to identify product features, benefits, purpose and use. It represents the progress of a product that can be recognized and experienced by consumers.

2. PRODUCT FUNCTIONALITY

A product can be described from many different points of view, each potentially defining a different product structure. A product is designed and developed according to a specific product structure. A product structure called Bill-of-Materials (BOM) is a collection of component descriptions organized as a part of functional hierarchy. Each component description contains the necessary information for making a piece of the product [Tomi M., et al.]. Functionality is an abstract product characteristic that a customer or sales person uses to describe what the product can be used to do and what requirements the product can satisfy [Alexander et al. 2001].

There is an emerging need for enhanced support of development processes in computer-aided theoretical design of various kinds of products, ranging from day-to-day appliances to industrialized systems. Possibly, the most vital stage in a product life-cycle is the phase in which the product is utilized by users, and intended to perform its implicit functions. But the issue is to recognize why products often fail to offer the intended function to users' satisfaction. This issue must be regarded in the perspective of the budding use of knowledge based systems in support for better designing of products.

Rapid changes in market requirements compel businesses to develop customized product with cost and time efficiency of mass production. Due to lack of standardized product functionality knowledge acquisition methods, in-depth product knowledge such as BOM, functional dependencies, assembly constraints and configuration rules cannot be managed effectively. A product developed long time ago under the assumptions of its functional effectiveness at that time can be reused in business years later for better advancement. Functionality is the most important property of a product, i.e. if the product does not possess right functions then other properties are uninteresting [Mortensen and Hansen, 1999].

2.1 Product Structure and Bill of Materials

The product structure provides a hierarchical classification of the items which form a product. With the product structure, the understanding of the components which compose a product as well as their attributes can be represented. The product structure shows the material, component parts sub-assemblies and other items in a hierarchical structure that represents the grouping of items on an assembly drawing or the grouping of items that come together at a stage in the manufacturing process [Adapted by DRM Associates from the CONFLOW Project, Nov 2012]. Product structure management provides the mechanism to capture and manage as-designed product structures with ease. It allows for the creation and re-use of unlimited numbers of parts and assemblies, to provide for many different variations of a basic structure or the creation of complex, one-of-a-kind structures.

In Fig.1, a product named 'Product 1' is shown graphically with the summarized products structure and the number of all items that are needed to make the parent products are enclosed in brackets. The product structure diagram which is used to create a version of the product to sustain development and the BOM capture the relationship between the components of a product [Adapted by DRM Associates from the CONFLOW Project, Nov 2012].

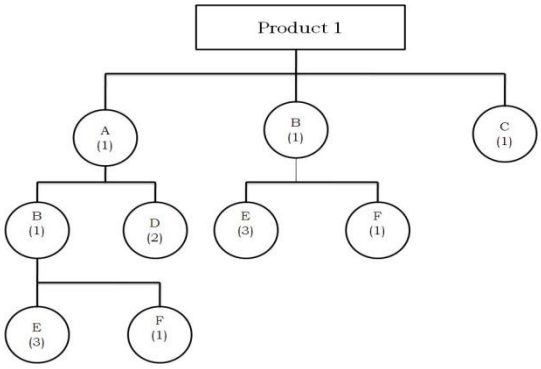


Figure. 1 Product Structure [Adapted by DRM Associates from the CONFLOW Project, Nov 2012]

A Bill of Material is a formally structured list for a product which lists all the component parts of the object with the name, reference number, quantity and unit of measure of each component. A BOM can only refer to a quantity greater than or equal to one of an object. It is a product data structure, which captures the end products, its assemblies, their quantities and relationships. It is a product data structure which captures the end-products, its assemblies, their quantities and relationships [Adapted by DRM Associates from the CONFLOW Project, Nov 2012]. There are usually two kinds of bills of materials needed for a product: engineering and manufacturing BOM. The engineering BOM normally lists items according to their relationships with parent product as represented on assembly drawings. But this may not be sufficient to show the grouping of parts at each stage of the production process nor include all of the data needed to support manufacturing or procurement. These requirements may force the arrangement of the product structure to be different in order to assure manufacturability [Adapted by DRM Associates from the CONFLOW Project, Nov 2012].

2.2 Function Structure and Sub-Functions

Function is a relationship between input and output of energy, material and information [Tomiyama 1993, Qian and Gero, 1996]. Product function is an effect on the environment of the product. The functions are themselves described as structures that are defined at the instance level [Shaw, 1989]. Function is a higher level of abstraction than structure, and helps to capture the designer's intent [Tor et al., 2003]. A function is primary if you can associate it with the purpose of the product and it is essential to that purpose. Primary functions define the product. Groups of functions, taken together, may constitute a primary function, too. Any function that contributes to the utility of the product but that is not a primary function is a secondary or sub function.

Functionality is the ability of the product of function. The Actual Product Function is in concert with force flow analysis. In a conceptual design the functional structure of a design object is determined and the basic physical mechanisms that realize the function structures are also determined [Tomiyama, 1993]. Functionality is the most important property of a product, i.e. if the product does not possess right functions then other properties are uninteresting [Mortensen and Hansen, 1999].

2.3 Functional Requirements

An abstracted description of work is that a product must perform to meet customer needs. Functional requirements capture the intended behavior of the product- what the product will do. This behavior may be expressed as functions, tasks, or services the product is required to perform. Therefore, functional requirements do not include performance characteristics, operating conditions, use cases, and specifications. The information that is supported is in the form-features cannot be obtained easily. The functional requirements of a system will be capable of overcoming these deficiencies [Shah, 1988].

2.4 Functionality Dependencies

The product's functionality depends on the product features relevant to the target market. Critical topics include prioritization of functionalities and capabilities based upon market demands. The functionality of the product plays an important role in the technical process. At any stage of the process it is necessary to see whether the product's functionalities have been achieved. Based on this the decision about the direction of the project, the resources required to achieve the product functionalities would be planned. The functionality of the product is treated as the separate element from the product itself. Thus, functions during technical process are achieved through specifying and identifying changes in the attributes of the product elements and relationship between the product elements [Thirupathi, 1998].

3. INTERWEAVING KA AND PF

Knowledge management of new product development provides an approach to represent and manage product domain entities and relations. KA is depicted as the major problem in illustrating the functionality of any product. But the complexity of the product descriptions in certain businesses causes difficulty. The product engineers/developers can no longer understand a product the way it is portrayed. The problem is due to brief addressing of the configuration product structure models in the object oriented methods look more comprehensible than its detailed functional components.

Knowledge management in product development covers a broad spectrum of activities and operations at many levels, from the individuals to the whole enterprise and between enterprises. Effective KM can only be achieved through a holistic approach, addressing not only technological solutions, but also people, processes and links of core business activities. The purpose is to reuse knowledge, create worth in enterprise, create new knowledge by any possibility, and thus provides economical knowledge mobility for the circle of knowledge management. Knowledge management is a gradual and circular process in knowledge-based product development system as shown in Fig.2 [Li and Xie, 2004].

In practice, there may not always be intent, or even an ability, to use archived product knowledge to automatically generate new design solutions. Nevertheless, whether the goal is automated synthesis or computer-supported designer synthesis, the basic need to retrieve and reuse knowledge in subsequent design activities remains the same. From this

perspective, the common requirements are to take as input some articulation of a target design or specification, to retrieve previously generated knowledge according to some measure of similarity, and to evaluate multiple potential matches to determine which most closely meets the specification [Li and Xie, 2004].

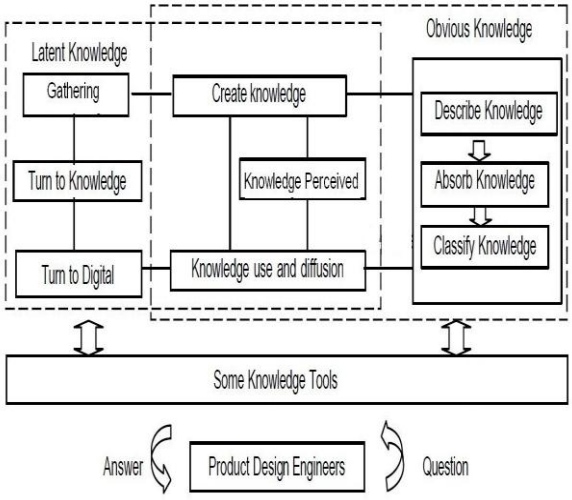


Figure. 2 Process of Knowledge Acquisition in Product Development [Li and Xie, 2004]

3.1 Industrial Knowledge Acquisition

Knowledge is also embedded in the technologies, methods, and rules of thumb used by individuals in a product development processes. KA is invested in the methods, ways of doing things, and successes that demonstrate the value of the knowledge developed. The knowledge in new product development is localized around particular problems faced in a given platform. The effective development of knowledge in organizations demands that individuals specialize or localize around different problems in a specific domain [Paul R. C., 2002]. It is important that KA techniques are extended to cover not only the static knowledge about a product, but also the dynamic knowledge about the design processes of the product. Due to their high complexity, product development processes should be expected to be a highly rewarding field for the application of knowledge management [Christian W, et al., 2004]. The lack of a proper product representation which includes its function, behavior, and structure is a foremost limitation of the existing systems.

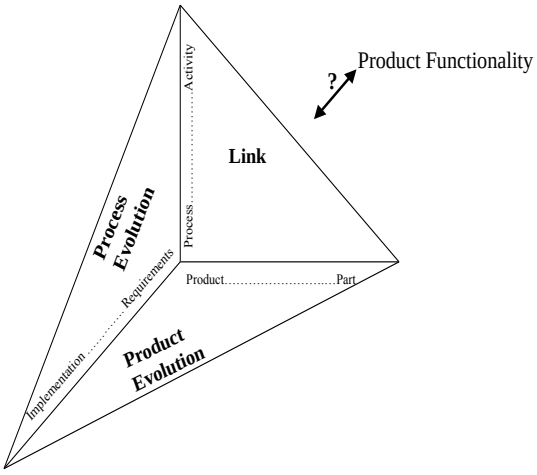


Figure. 3 Dimensions of Product Development Process [Thirupathi, 1998]

Table 1. Product Functionality Sample Data Acquired

Sl. No.	Product name	Components	Functions	Primary / Secondary
1.	Mobile charger	Insulation wire	For power supply connection	Primary
		Regulator	To stabilize the voltage supply	
		Rectifier	To convert from AC to DC	
2.	Microwave Oven	Induction coil	To produce heat	Primary
		Ventilator	For cooling the system and processing air supply	
3.	Air Cooler	Gas Container	×Not Specified	Primary
		Filter Paper		Secondary
		Cooling Fan		Primary
4.	Pen	Refill	Used to contain ink	×Not Specified
		Ink	To write	Primary
		Plastic	Acts as outer body	Secondary
5.	Sin-treed Component	Gear & Gerotors	×Not Specified	×Not Specified
		Hubs		
		Piston		
		Bearing		

An optimal use of the resources such as people, computers and machines requires that they are part of a system which able to master the action flow and the information flow. Mastering action and information flow improves the quality of the products, due to avoidance of errors and increased production flexibility. The quality of a product depends on the functionalities that it provides. Even though achieving product functionality is an essential goal and is the key to the success of a new product, there is no model in the related areas that considers product functionality and its relationship with the process that introduces the product; the semantic link (goals, control) between the product functionality and process have been vastly ignored. Modeling methodologies should tackle this problem of modeling product functionality in order to control the Product development process effectively. In large enterprises, new products that have high market value are produced by embedding product development processes and knowledge acquisition techniques to make sense of the system. The effectiveness of a product developed depends on the privileged circumstances of the knowledge that design experts bear in solving problems and the probability of trying innovative methods and generate new interpretations. None of the candidate architectures and associated methodologies is, as yet, completely developed, described and documented to address ← the goal (product functionalities) view of the process, ↑ the link between the process and its goal, → evolution of information and ↓ the link between the process and its output (Fig. 3) [Thirupathi, 1998].

The product knowledge of an enterprise can operate as a bond for integrating processes that are carried out in various domains. Mastering product functionality data allows a better integration of the product development process. For acquiring product data and its functionality, manufacturing companies involved in new product development process have been considered. In order to acquire this product knowledge, a questionnaire has been designed. The sample size of the data acquired is thirty corresponding to different products. The questionnaire gathers creditable information about the product data such as:

- Name and segments of the product
- Specifications and purpose of the segments
- Assembly/Component functions
- Functionality of the product
- Parameter used for rating the product and
- Electronic storage details of the product data and product functionality

The gained product knowledge corresponds to thirty products from thirty different design engineers. Each product has its own purpose, specification, assembly/components and functions. The designers have produced few details about each of the components in the product and their functions. This product data collection gives a concise breakdown of the product functionality details obtained via the sample data which explains briefly the various functionalities of the given product. It enlightens the various products, its assembly and function data acquired through questionnaire.

3.2 Analysis of Product Functionality Data

This analysis is useful in study the data based on segments, components, functions and parameters of a product and its functionality. The collected product knowledge corresponds to thirty products and they can be categorized into three branches of product data storage. The product data storage can be sorted out into data which are digitally stored, which are not stored digitally and which details about storage are not specified.

In Table 1, the column “product name” lists the different products whose production data has been acquired. The column “components” lists the different segments of the product. The column “functions” and “primary/secondary” illustrate the various product functions and its rate accordingly. The × mark in the table shows that many designers are unable to explain or the knowledge on the functionalities of a product is less among the designers.

Table 2. Product Functionality Data Storage Analysis

DATA STORAGE	DATA SIZE (30)	PERCENTAGE (%)
Data Not Specified	19	63%
Stored Data	3	10%
Data Not Stored	8	27%

From the table 2, it concludes that only 10% of product functionality data is stored digitally and approximately 90% (No knowledge of storing product functionality data=63%, and product functionality data not stored=27%) of designers do not store functionality information digitally. The fig 4 is a pie-chart that represents the facts about functionality of a product’s data storage.

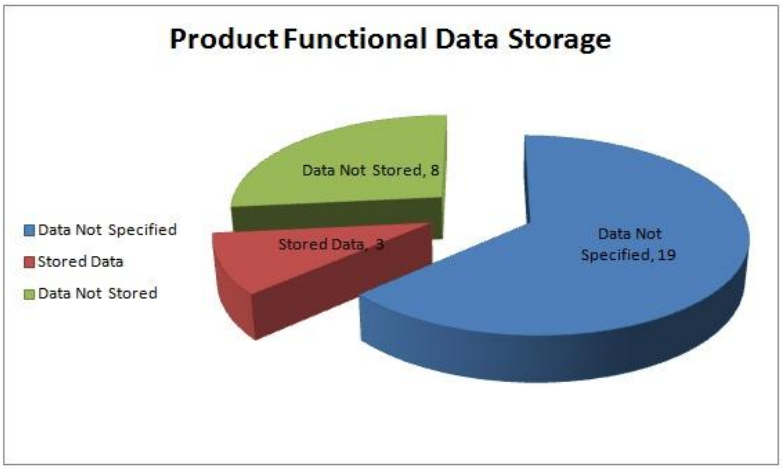


Figure. 4 Product Functionality Data Storage Analysis with Samples Data of Size 30

4. RESULTS AND DISCUSSIONS

Knowledge is one way by which individuals exhibit their proficiency in solving problems i.e., being a good design engineer to meet all the customer requirements. Product functionality designing is essential to describe the generality in product structures. When a design engineer sees the significance the current design has on creating an effective product, it will be necessary to transform that knowledge into a working prototype. Hence, experts have need of a general technique or tool that ensures consistency and offers appropriate mechanisms for mass data processing for integrating knowledge management and product development.

A conventional type of product knowledge comprises of product design skills, process scheduling experiences, management artifice, and market necessity information. The purpose of product functionality is to represent product family through a general design structure. Actually it is a process that acquires and represents product knowledge briefly with its functional structure. This depicts the components that are needed for a product, the quantity of components and their dependencies. This assists the design team to identify and rank areas of focus for product improvement.

Engineers engaged in product development bring to their work the formal and articulated expertise that has been socially constructed through time by particular professional or academic communities. This knowledge initially frames attention when approached with a problem; however, by making sense of particular problems and of the information encountered in particular situations, and by taking action and revising their interpretations, new knowledge both tacit and explicit is developed. This form of collective sense-making, entailing personal links between people with different knowledge can yield new knowledge [Susan et al., 2003].

5. CONCLUSION

This research is an outcome of selecting a knowledge acquisition method for acquiring knowledge on product functionality efficiently. It highlights about a product, its functions and sub-functions, its overall functionality while developing a new product. The product functionality data is not stored digitally. Most of the design engineers are unaware of the importance of product functionality and relevant associated data; they concentrate only on the physical design of a product in the development process. In due course of time, if the product is not manufactured in bulk quantity, then the knowledge about product functionality and hence the product may disappear.

It concludes that most of the design engineers are unaware of product functionality. Those who have knowledge about the functionalities of a product do not store them digitally. Those who store product data do not store product functionality data. It affirms that only one in a tenth digitally store the functionality data. In order to overcome this issue, it is necessary to cultivate knowledge in the minds of designers to store every minute functions and parameters of a product during the development process.

REFERENCES

[1]. Adapted by DRM associates from the CONFLOW project, (nov 2012). Http://www.npd-solutions.com/bom.html. “product structure and bills of material”. (online). Visited: nov, 2012.

[2]. Alexander felfernig, gerhard friedrich, et al (2001). “conceptual modeling for configuration of mass-customizable products”. Artificial intelligence in engineering, 15, pp.165-176.

[3]. Christian weber, martin pohl, michael steinbach. (2004). “new ideas for knowledge management in product development projects”. International design conference, dubrovnik, may 18 - 21.

[4]. Li shaobo and xie qingsheng. (2004). “knowledge management in product development integration system”. Cad/cims institute, guizhou university of technology, guiyang guizhou china, 550003. Proceedings of the 6th international conference on frontiers of design and manufacturing.

[5]. Maryam alavi, dorothy e. (2001). “leidner. Knowledge management and knowledge management systems: conceptual foundations and research”. Mis quarterly, vol. 25, no. 1 (mar., 2001), pp. 107-136.

[6]. Mortensen n. H., hansen c.t. (1999). “structuring as a basis for product modelling”. Critical enthusiasm – contributions to design science, pp. 111-128, isbn 82-91917-08-6.

[7]. Paul r. Carlile. (2002). “a pragmatic view of knowledge and boundaries: boundary objects in new product development”. Organization science, © informs vol. 13, no. 4, jul–aug ‘02, pp. 442–455.

[8]. Qian l. Gero j.s. (1996). “function-behavior-structure paths and their role in analogy-based design”. Artificial intelligence for engineering design, analysis and manufacturing, 10:289-312.

[9]. Shah j.j., rogers m.t. (1988). “functional requirements and conceptual design of the feature-based modelling system”. Computer-aided engineering journal, 5(1). Pp.9-15.

[10]. Shaw n.k., bloor m.s., pennington a.de. (1989). “product data models”. Research in engineering design, 1, pp.43-50.

[11]. Susan albers mohrmana, david finegold, allan m. Mohrman jr. (2003). “an empirical model of the organization knowledge system in new product development firms”. Journal of engineering technology and management, pp.7-38.

[12]. Thirupathi d. (1998). “integrated information model for managing the product introduction process”. Ph.d. Thesis, coventry, u.k. university of warwick.

[13]. Tomi männistö, hannu peltonen and reijo sulonen. (1996). “view to product configuration knowledge modelling and evolution”. Helsinki university of technology, iia research centre and laboratory of information processing science.

[14]. Tomiyana tetsuo, yasushi umeda, hiroyuki yoshikama. (1993). “a cad for functional design”. Annals of the cirp, vol. 42/1/1993, pp. 143-146.

[15]. Tor s.b., britton g.a., zhang w.y. (2003). “a graph and matrix representation scheme for functional modelling in conceptual die design”. Proceedings of the international conference on production research, 13-16 aug, blacksburg, virginnia, usa.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 465 - 473, 2013, ISSN: 2319–8656

Effective Implementation of Green Computing

Navdeep Kaur
Guru Kashi University,
Talwandi Sabo,
Punjab, India.

Pardeep Mittal
Guru Kashi University,
Talwandi Sabo,
Punjab, India.

Abstract: A safe and non-polluted environment is the basic need of a living being. But today the situation is getting changed. Our environment is getting polluted day by day at a very high rate. The use of computing devices plays a vital role in harmfulness of environment. To reduce these harmful impacts the concept of Green Computing must be implemented. In this research paper we count some factors and find some issues and challenges which are barrier towards implementation of green computing. The main reason the awareness of a common user. If a common user is getting aware about the harmful impacts of use of computing devices over environment and takes some steps at own level to reduce electricity, the concept of green computing will be implemented.

Keywords: Energy Star, Blackle, TCO, ICT, CO_2 Emission.

1. INTRODUCTION

Green computing is the study and practice of designing, manufacturing, using and disposing of computers, servers, associated, subsystems such as monitors, printers, storage devices, and networking and communication systems efficiently and effectively with minimal or no impact on environment. The concept Green computing is come into existence in 1992 when the U.S environmental protection agency launched energy star, energy star is voluntary labeling and recognize energy efficiency in monitors, climate control equipment and other technologies. The goal of green computing are power management and energy efficiency choice of eco-friendly hardware and efficient software and material recycling and increasing the product's life. With the help of ICT (Information and Communication Technology), Green computing become an effective approach to grow segments that affects carbon emission. It also implements Energy Star management strategies and technologies that reduced energy consumption waste. Today computing devices are the basic need of human. These devices make our life easy as they save a lot of time and human efforts. The benefits of computing device are known to everyone but no one is aware about the harmful impacts of computing devices on environment. The main reason behind it is the less awareness about the harmful impacts of the use of computing devices. I take a little initiative to aware the common man about the term Green Computing, its benefits and how the Green Computing is implemented.

2. OBJECTIVES OF STUDY

The main objectives of the study are:

1. To aware the common man about term green computing.
2. To reduce energy consumption & protect the environment.
3. To find the difficulties occur in implementation of green computing.
4. To aware the common man about the efforts need to done by them for green computing.
5. To aware the common man about the organizations who take initiatives to promote green computing.
6. To make the people aware about the role of government to promote green computing.

3. RESEARCH METHODOLOGY

For implementation of green computing we have to go through various issues and challenges occur in implementation of green computing. After a thorough study of these issues and challenges we choose various factor variables. These factor variables are further categorized into various categories and a questionnaire is prepared from these factor variables. Questionnaire is distributed among 220 people and collected their responses. We prepare results from these responses using statistical tools and represent these results with the help of graph. After preparing graph conclusions are draw using data mining tools.

4. CATEGORY FACTOR VARIABLES:

V1. Do you ever use any computing device?

V2. Which type of computing device are you using?

- 2.1. Laptop
- 2.2. Desktop
- 2.3. Mobile
- 2.4. Net book
- 2.5. Any other please mention

V3. Are you familiar with term operating system?

(If yes, check the following, if no skip this question)

- 3.1. Which operating system have you ever used?
  - 3.1.1. Linux
  - 3.1.2. Unix
  - 3.1.3. Windows
  - 3.1.4. DOS
  - 3.1.5. Mac
  - 3.1.6. Any other please mention

V4. Which type of processor do you use?

1.1. Intel
1.2. AMD
1.3. VIA
1.4. Don't know

V5. Which search engine do you use?

5.1. Google
5.2. Yahoo
5.3. Blackle
5.4. Bing
5.5. Any other please mention

V6. Do you ever use printer?

(If yes than please check the following)

6.1. Which type of printer do you usually used?
6.1.1. Inkjet
6.1.2. DeskJet
6.1.3. Laser Jet
6.1.4. Any other please mention

V7. Awareness about environment.

7.1. Do you really care about environment?
7.2. Do you know that the use of computing devices put harmful impacts on our environment?
7.3. Do you know about term CO_2 emission?
7.4. Do you know most of the CO_2 emission is generated through computers and its devices?
7.5. Do you know the high consumption of electricity also plays a big role towards harmful environment?
7.6. Do you know most of the parts of computers are not biodegradable?
7.7. Do you know there are many toxic chemicals are used while manufacturing of computer?
7.8. Do you know about world environment day?
7.9. Do you know world environment day is celebrated on 5th June of every year?
7.10. Do you know world environment day is celebrated to raise global awareness to take positive environmental action?
7.11. Do you know world environment day is going to complete his 41 year on 5th June (1973-2013)?
7.12. Do you know every year a new theme related to environment is taken for world environment day to save our environment?
7.13. Do you know in last 41 years (1973-2013) term green computing is not become the theme of world environment day?

V8. Awareness about Green Computing, (please attempt if already known)

8.1. Familiar with term Green Computing.
8.2. Green Computing is also refer to environmentally sustainable computing.
8.3. The goal of green computing is to reduce the hazardous material and save our environment.

V9. Energy star program – please check if already familiar

9.1. Energy Star is an international standard for energy efficient consumer products.
9.2. Energy star launched in 1992 by Environmental Protection Agency and the Department of Energy.

V10. Are you know about TCO Development, (Please check if already known)

10.1. TCO development is the sustainably certification for IT products.
10.2. It works to ensure that the manufacturing and recycling of IT products are carried out with regards to environment.
10.3. TCO development is headquartered in Stockholm, Sweden, with regional presence in USA and Asia.
10.4. TCO development introduced TCO certificate for sustainability certification of IT products.
10.5. TCO certificate was associated with computer monitors but later TCO revision also defines standards for computers, keyboards, printers, mobile phones and office furniture.

V11. How much you aware about recycling and disposing, (please check if already familiar)

11.1. Familiar with disposing of computing devices
11.2. Familiar with recycling of computing devices
11.3. Familiar with formal and informal disposing
11.4. Informal disposing is harmful to our environment
11.5. Formal disposing is costly but sustainable to our environment.

V12. How much you aware about manufacturer's initiatives towards green computing - are you ever know?

12.1. Dell purchasing 129% of its conventional usages in green power
12.2. Dell's latitude E-Series laptops and the OptiPlex desktops are designed for energy efficiency
12.3. HP's eco solution program provides inventive, High quality products and services that are environmentally sound
12.4. Intel's core i3, i5, and i7 processors minimize the amount of unnecessary power that get used
12.5. These CPU's are small in size and made of high+k+transistor technology that doesn't over leak electricity.
12.6. Wipro's green testing lab at Sarjapur campus that test products to conforms that they are "green" complies

12.7. Wipro's e-waste disposal service, Eco friendly product engineering design and green data centres are steps towards green computing.

V13 How much effort you are taking towards green computing?

13.1. Do you have more than one computer?
13.2. Are you using computer from a long time?
13.3. Are you using computer more than 5 hour per day?
13.4. Do you turn off your computer when it is not in use?
13.5. When you purchase new electronic device do you consider energy star logo?
13.6. Have you any product with energy star logo?
13.7. Are you doing efforts to saving energy at home?
13.8. Do you always consider about cost while purchasing product?
13.9. Have you seen or heard about any campaign about green computing?
13.10. Have you ever disposed any computing device?
13.11. Do you use screensavers on your computer?
13.12. Does screen saver save energy when computer is idle?
13.13. Do you know Google's Blackle search engine is less energy consuming search engine?
13.14. Do you ever use Google's blackle search engine?
13.15. Are you printing more than 20 pages daily?
13.16. Is cartridge refilling greener than replacing it?
13.17. Can you save a lot of money by Green Computing?

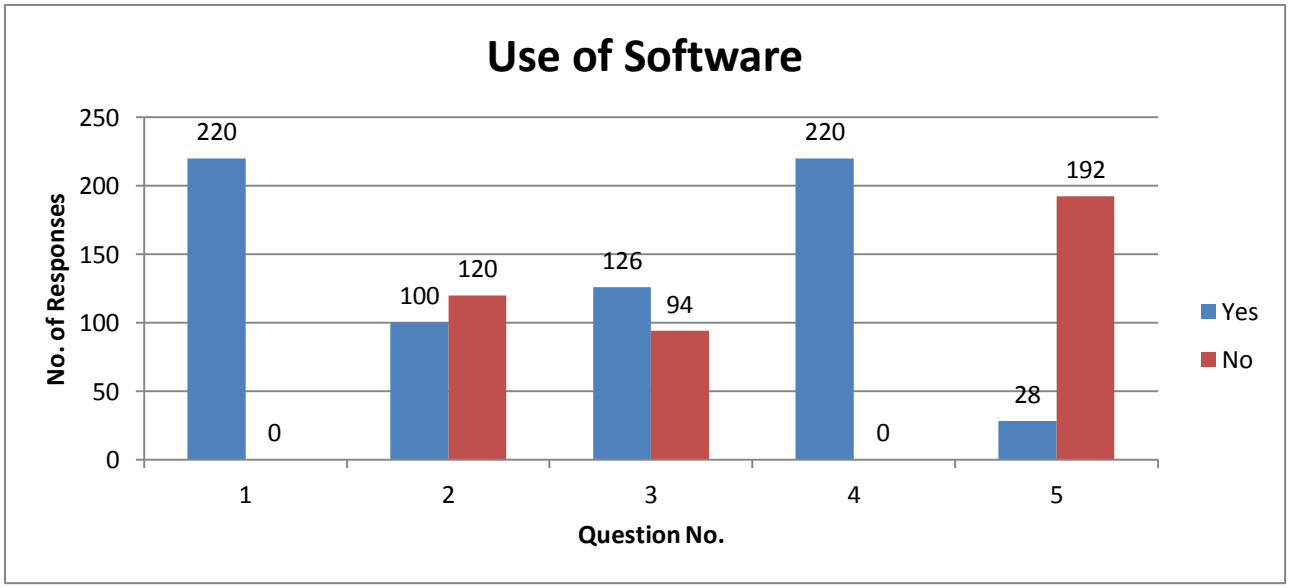
V14. Role of government towards green computing

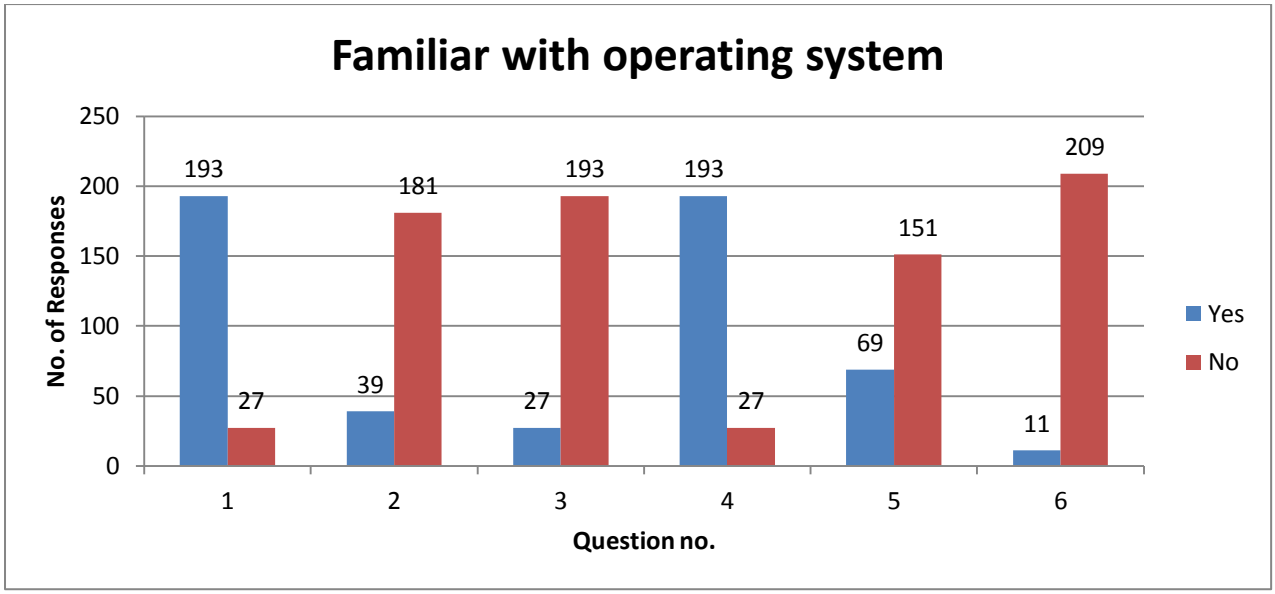
14.1. Should government reserve some money for green computing in budget?
14.2. Should government have to promote green computing?
14.3. Should government have to promote formal disposing?
14.4. Should government have to give subsidy for formal disposing?
14.5. Should government take steps to aware people about green computing?

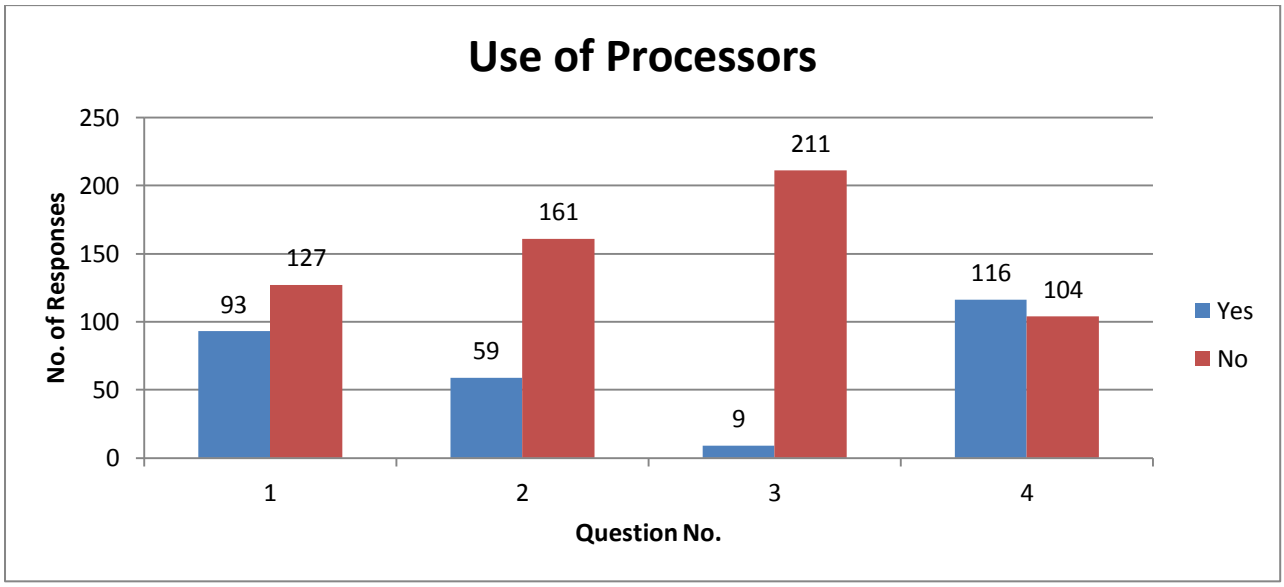
V15. The objectives of my research – are you agree or not?

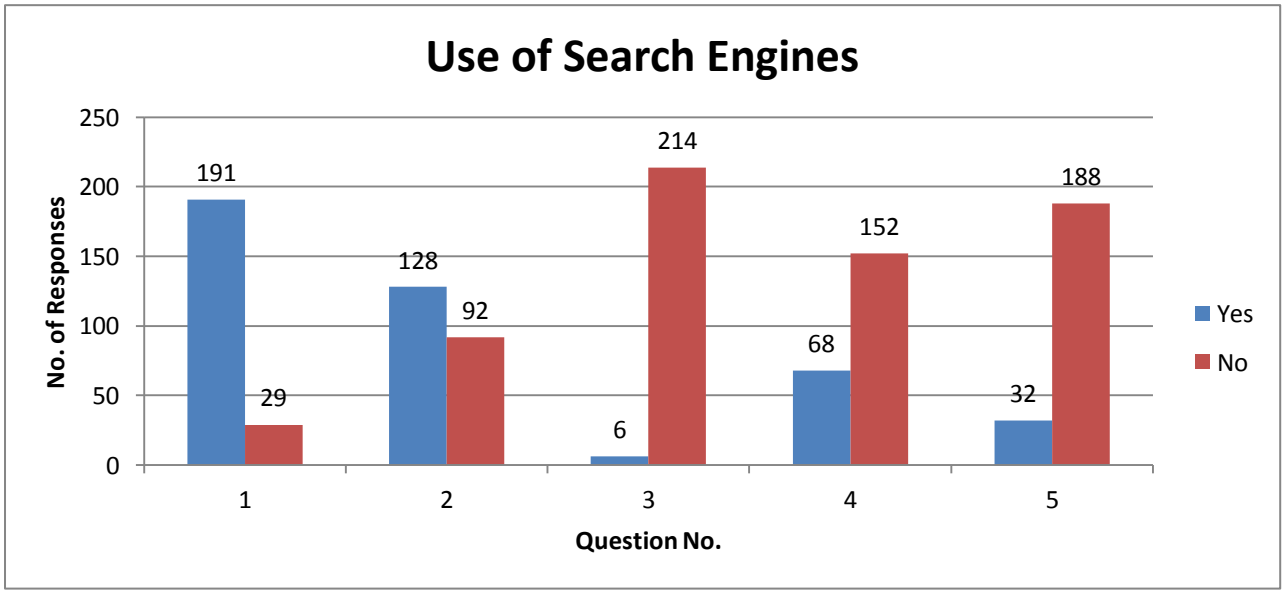
15.1. Every common man should have to aware about green computing and its benefits
15.2. Government should have to take strict actions to implement green computing
15.3. Computer manufacturers should has to manufacture less energy consuming and less heat generating devices
15.4. Every computer user must turn off their computer if it is not in use for more than 3 minutes
15.5. Various NGO's should also have to take serious actions to save our environment not only from other pollutions but also from the pollutions that is generated through the use of computer and its devices
15.6. Time to time campaign should have been conducted to aware a common man with green computing
15.7. Universities and colleges should have to aware their students about green computing
15.8. Green Computing should also have to be teaching as a regular subject in every university and college.

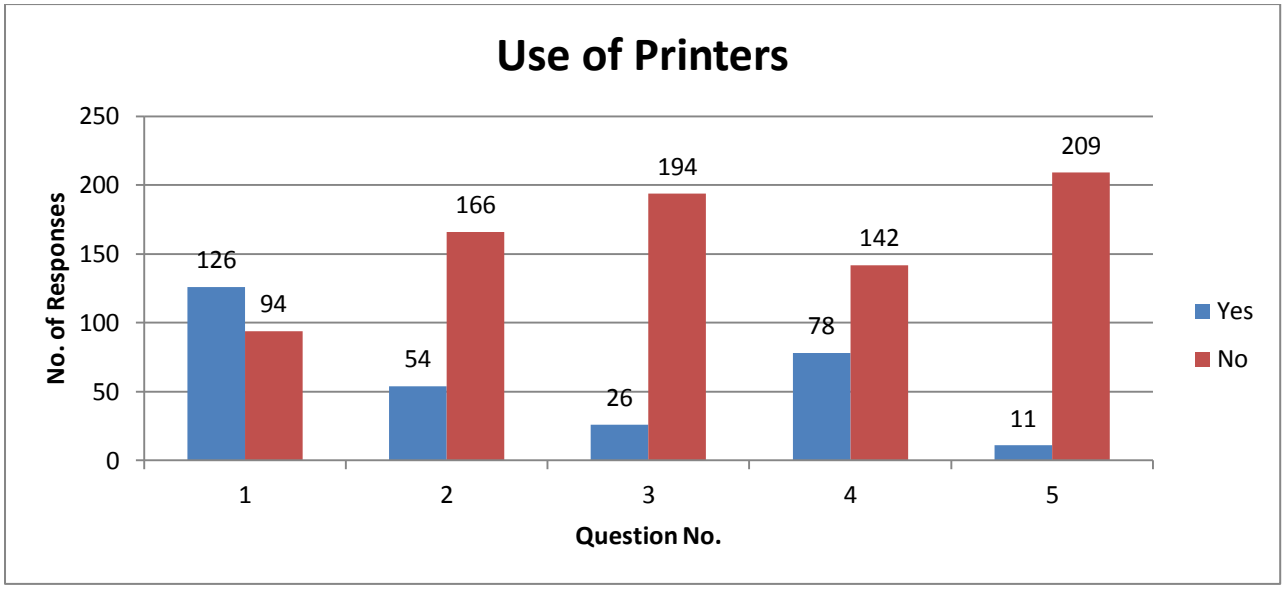
5. ANALYSIS AND INTERPRETATION (USING DATA GRAPHS)

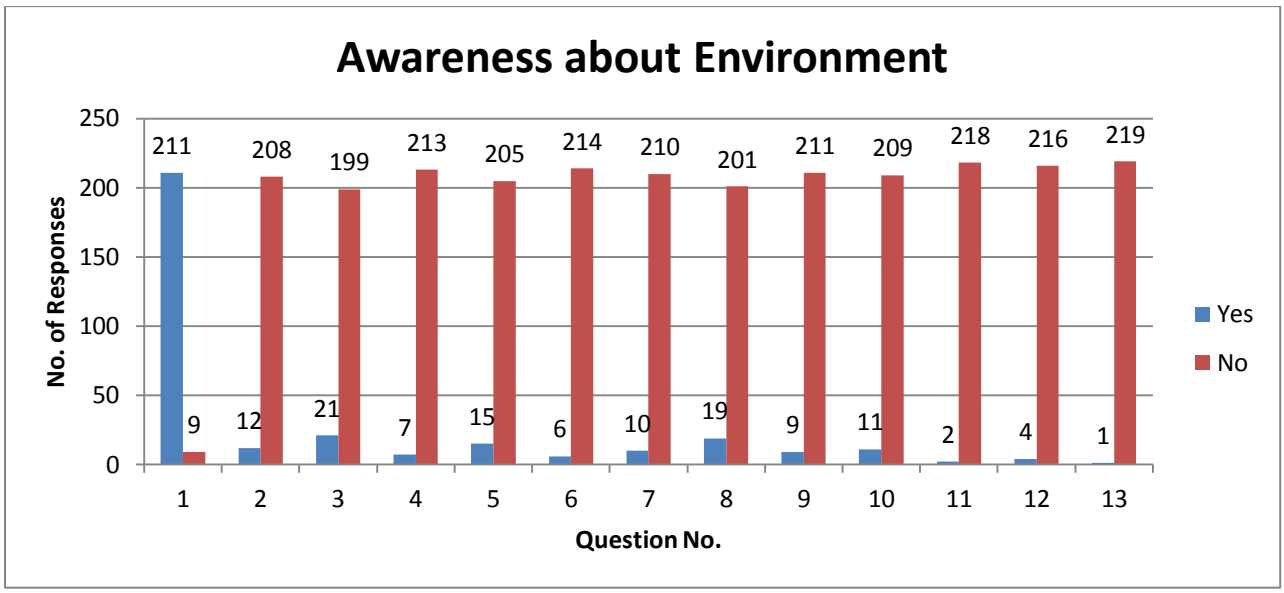


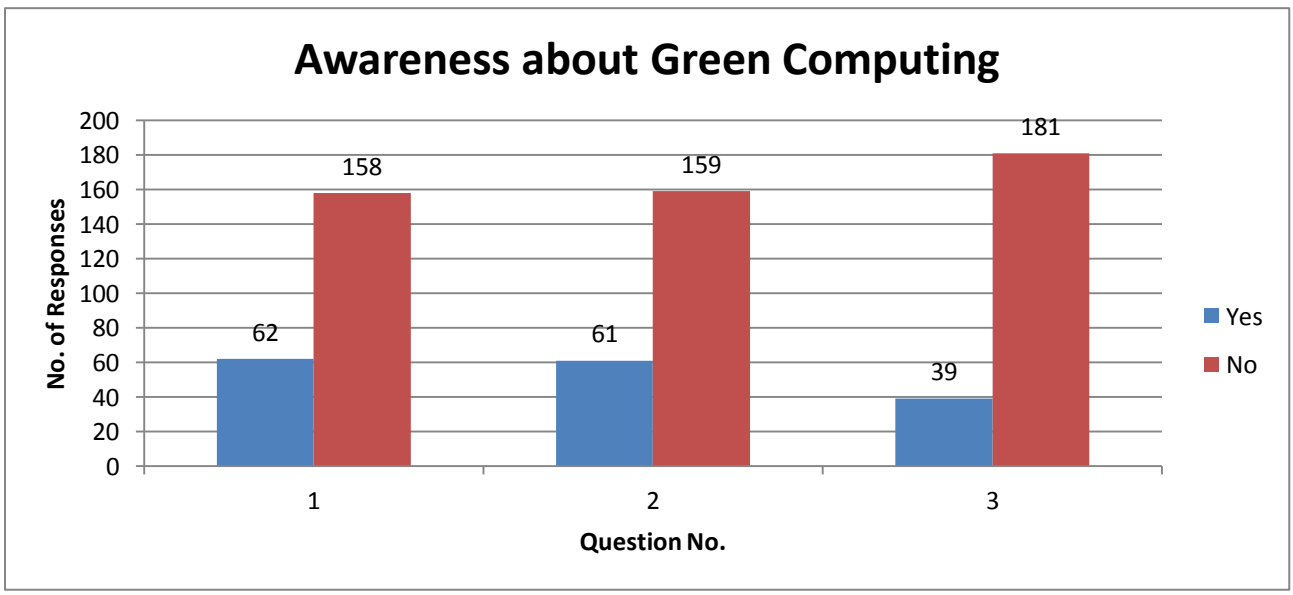

Familiar with operating system
No. of Responses
250
200
150
100
50
0
193
27
39
181
27
193
193
27
69
151
11
209
1
2
3
4
5
6
Question no.
Yes
No

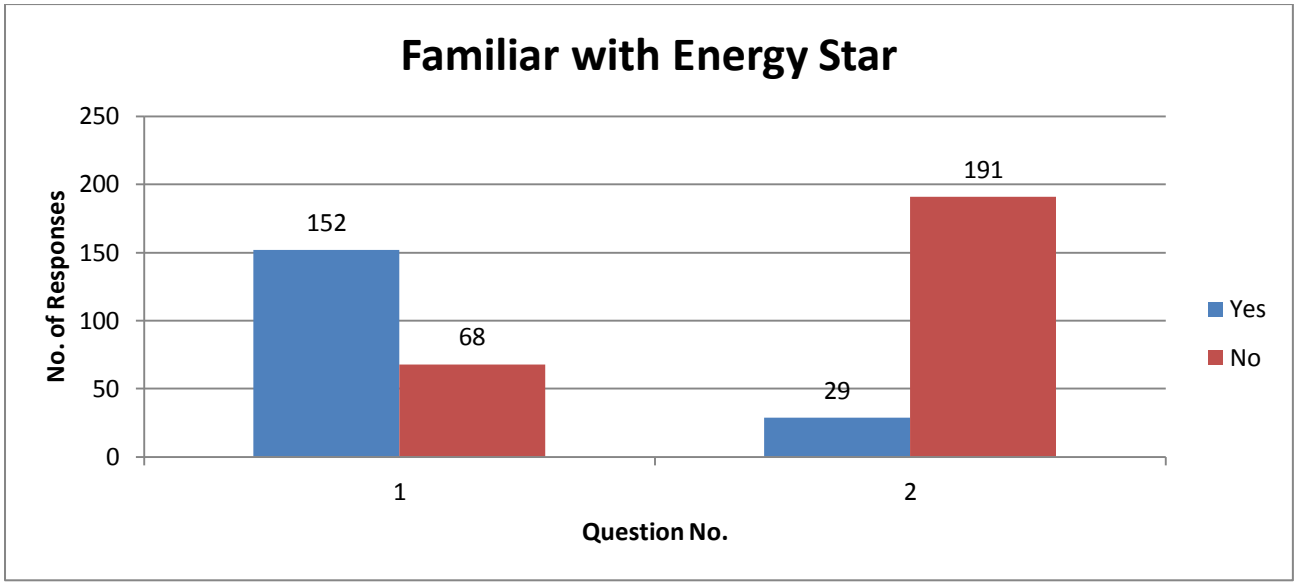

Use of Processors
No. of Responses
250
200
150
100
50
0
93
127
59
161
9
211
116
104
1
2
3
4
Question No.
Yes
No

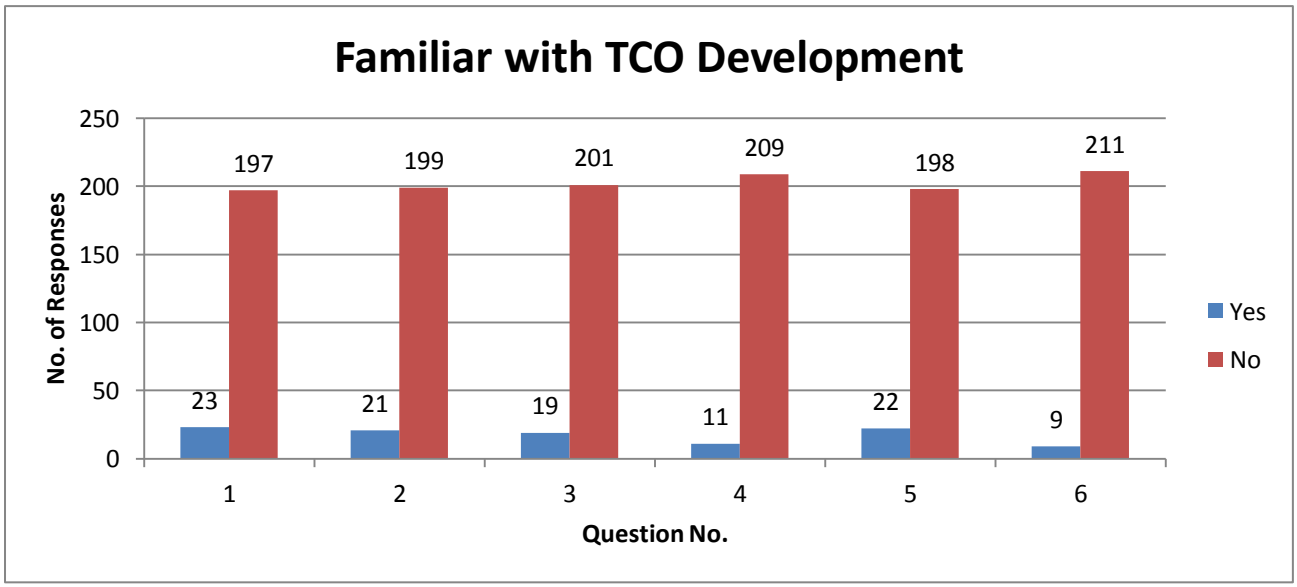

Use of Search Engines
No. of Responses
250
200
150
100
50
0
191
29
128
92
6
214
68
152
32
188
1
2
3
4
5
Question No.
Yes
No

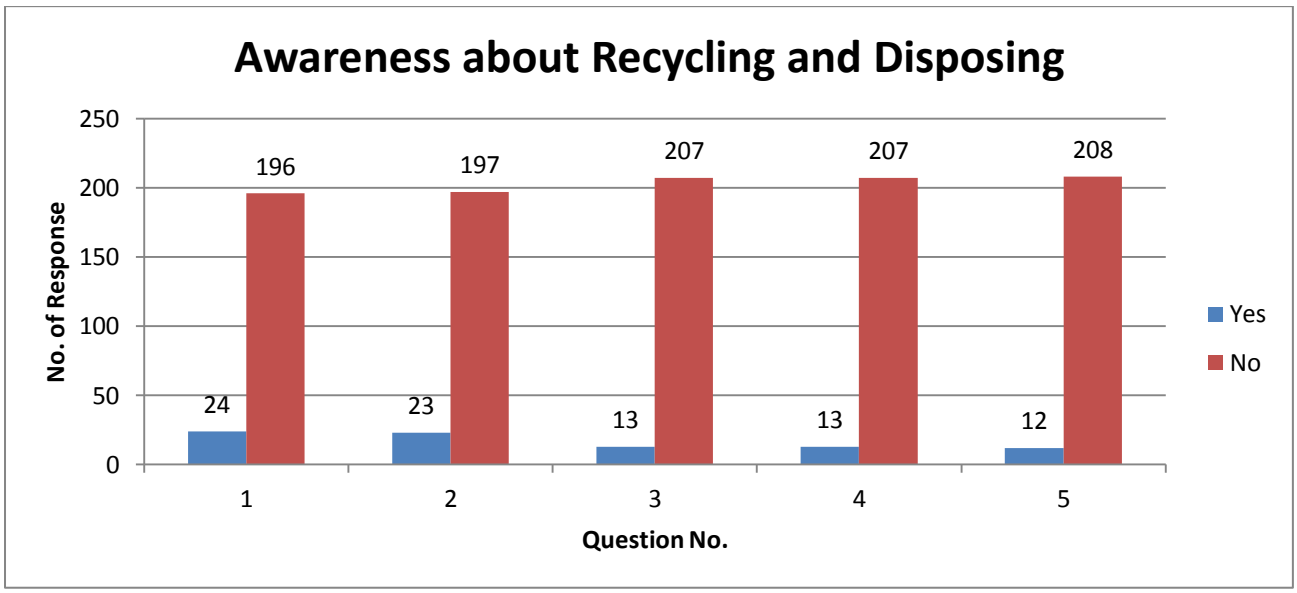

Use of Printers
No. of Responses
250
200
150
100
50
0
126
94
54
166
26
194
78
142
11
209
1
2
3
4
5
Question No.
Yes
No

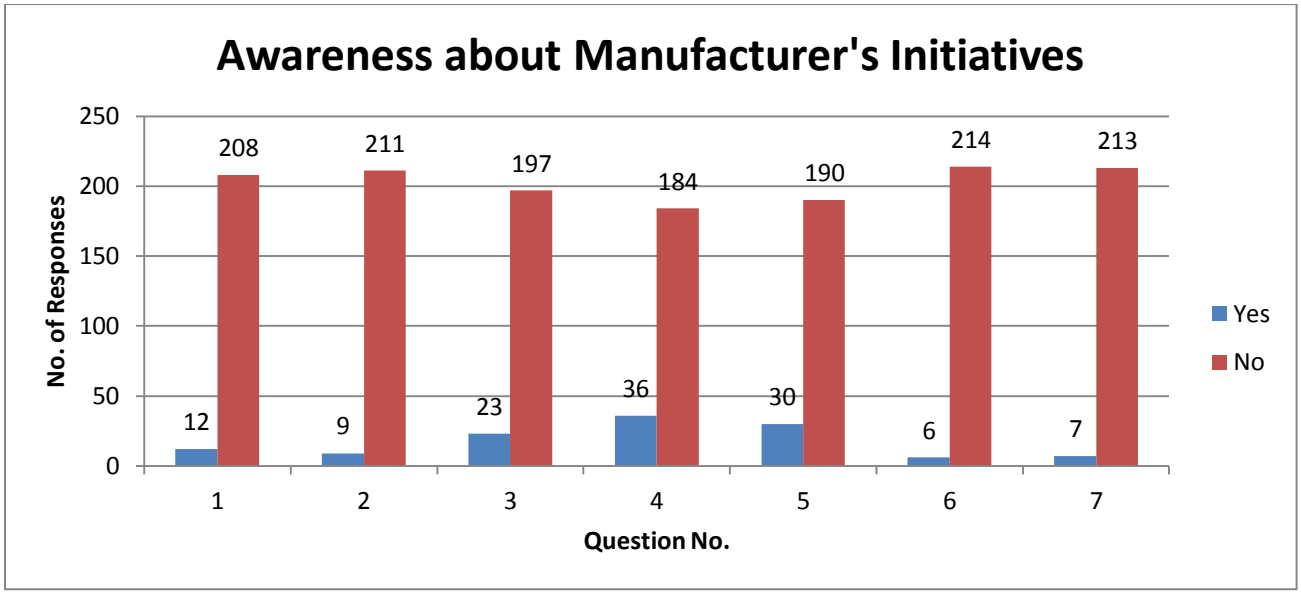

Awareness about Environment
No. of Responses
250
200
150
100
50
0
211
9
208
12
199
21
213
7
205
15
214
6
210
10
201
19
211
9
209
11
218
2
216
4
219
1
1
2
3
4
5
6
7
8
9
10
11
12
13
Question No.
Yes
No

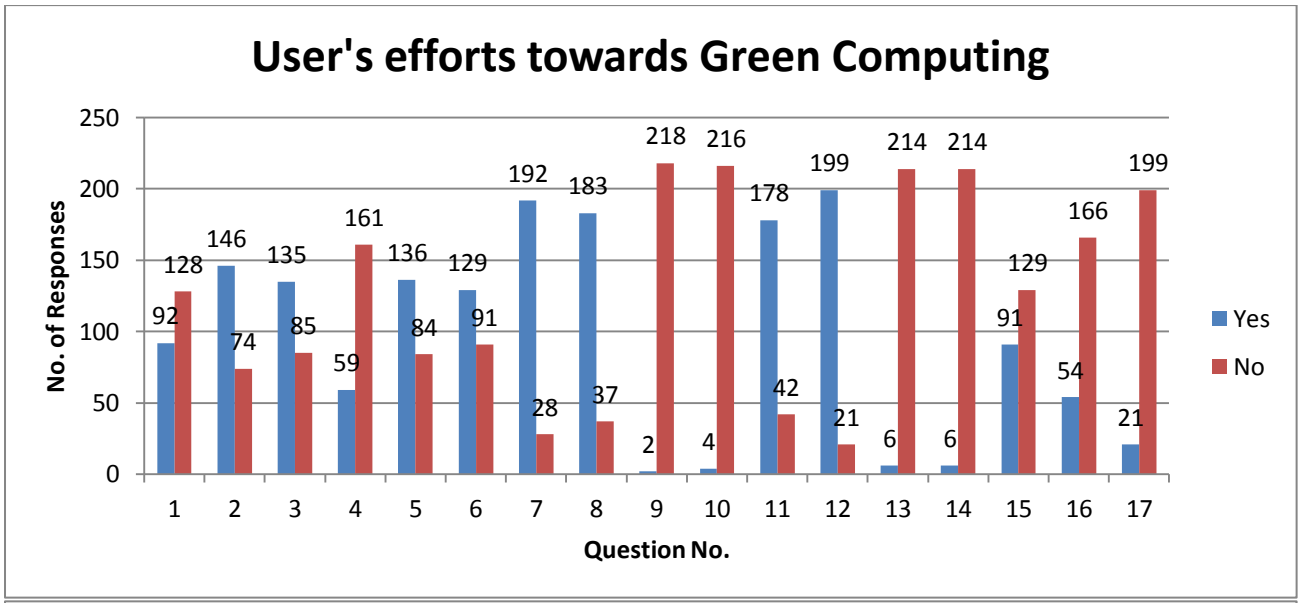

Awareness about Green Computing
No. of Responses
200
180
160
140
120
100
80
60
40
20
0
62
158
61
159
39
181
1
2
3
Question No.
Yes
No

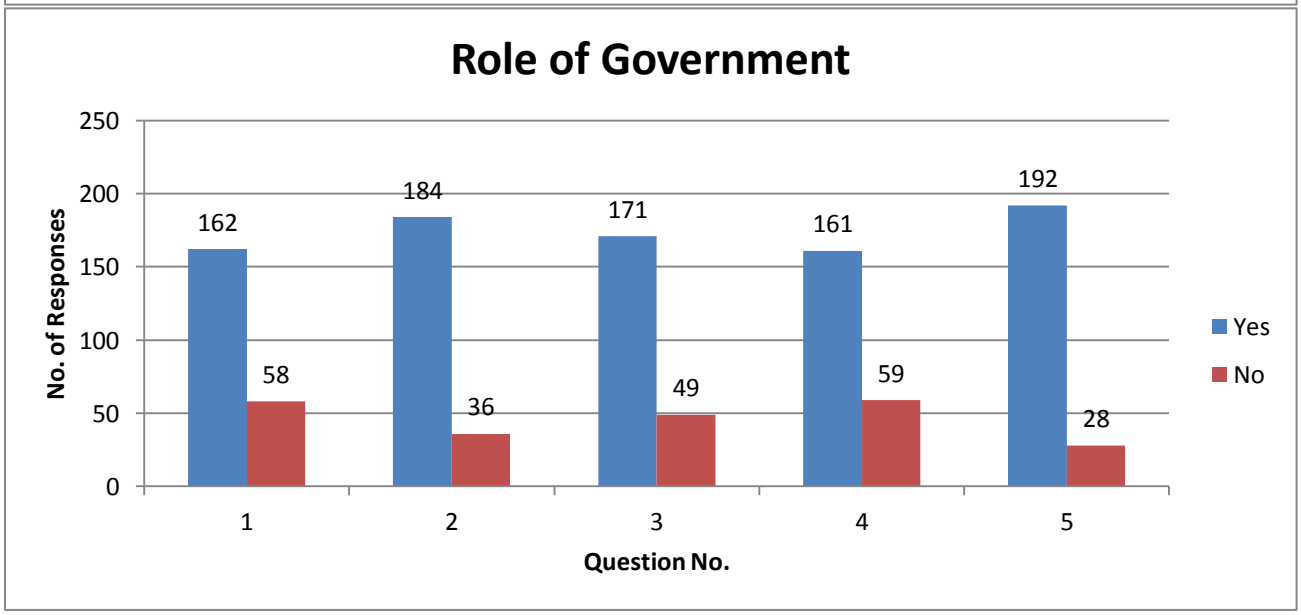

Familiar with Energy Star
No. of Responses
250
200
150
100
50
0
152
68
29
191
1
2
Question No.
Yes
No

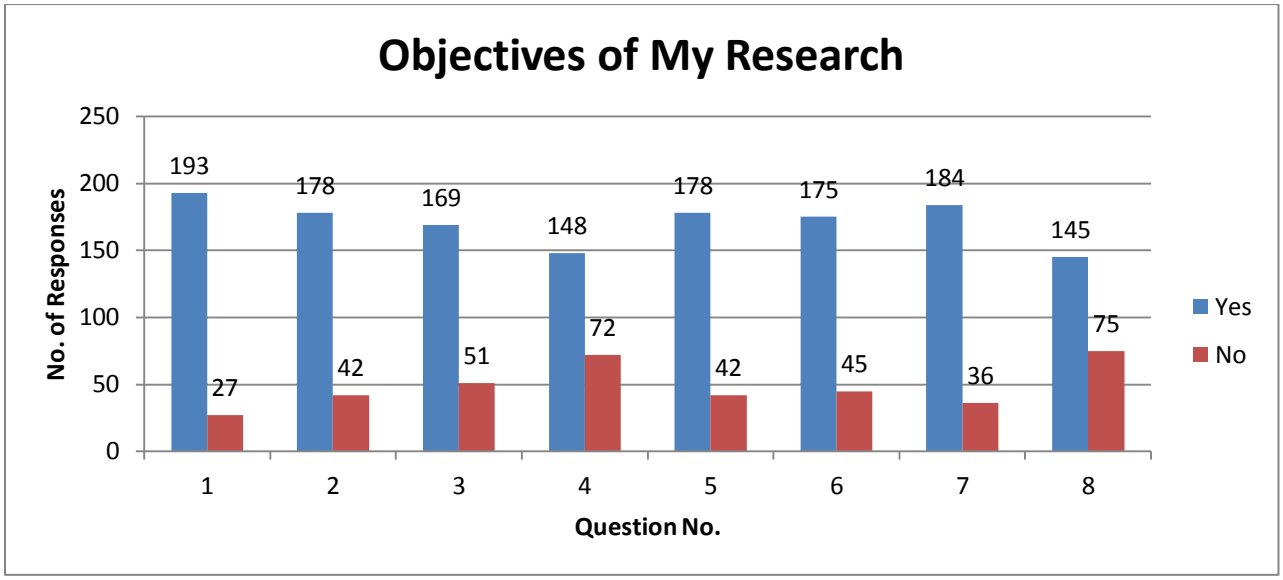

Familiar with TCO Development
No. of Responses
250
200
150
100
50
0
197
199
201
209
198
211
23
21
19
11
22
9
1
2
3
4
5
6
Question No.
Yes
No


Awareness about Recycling and Disposing
No. of Response
250
200
150
100
50
0
196
197
207
207
208
24
23
13
13
12
1
2
3
4
5
Question No.
Yes
No


Awareness about Manufacturer's Initiatives
No. of Responses
250
200
150
100
50
0
208
211
197
184
190
214
213
12
9
23
36
30
6
7
1
2
3
4
5
6
7
Question No.
Yes
No


User's efforts towards Green Computing
No. of Responses
250
200
150
100
50
0
92
128
146
74
135
85
59
161
136
84
129
91
192
28
183
37
2
218
4
216
178
42
199
21
6
214
6
214
91
129
54
166
21
199
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
Question No.
Yes
No


Role of Government
No. of Responses
250
200
150
100
50
0
162
58
184
36
171
49
161
59
192
28
1
2
3
4
5
Question No.
Yes
No



6. CONCLUSION

1. According to my survey report 100% people are using computing devices in which almost everyone using mobile phones, 45 % use laptop and 57% use desktops.
2. 87% people are familiar with term operating system, all these 87% people are familiar with windows operating system but only 17% are familiar with Linux and only 5% are familiar with Mac which are consuming less power than windows operating system.
3. AMD and VIA are less energy consuming microprocessors but only 26% use AMD and 4% use VIA processor but 42% are using Intel's microprocessor. More than 50% people are even not know about their microprocessor then how they can be know the features of these.
4. Google's Blackle search engine is the lowest energy consumption search engine but only 2% people are familiar with it and use it.
5. According to my survey 57% people are using printers and from these 57%, 35% are using lesser printer but they do not know that lesser printer is the highest energy consumption printer. Inkjet printer consumes very low energy as compare to lesser printer but only 24% people are using inkjet printers.
6. Todays everyone says that he/she really cares about our environment but they are even not familiar with the terms that are produces harmful impacts on our environment. According to survey only 1 to 9.5% people are known about these terms like CO_2 emission and role of high consumption in polluted environment. There is one interesting fact comes that people are not know about the world environment day and the purpose to celebrate that day. Here a big fact arises that in last 41 years from 1973 to 2013 green computing is not taken as a theme of world environment day. Why?
7. Only 17 to 28% people are familiar with green computing and its goals.
8. Energy Star program is an international standard for energy efficient products but 69% people are familiar with it.
9. Only 4 to 10% people are aware about TCO development its certificate.
10. A computer can be recycle and disposed of safely to save our environment but only 6% people are familiar with formal disposing and it benefits over environment.
11. Todays various computer manufacturers are taking some initiatives for green computing but only 2 to 16% people are aware about it.
12. Near about 66% people are using computer from a long time and more than 5 hours in a day and 41% have more than one computer but only 26% users are turn off their computer when they are not in use. Even 90% people are agree with the term that screen saver saves electricity when computer is idle and 80% people are using screen saver on their screen but in actual screen saver consumes more electricity when computer is idle.
13. When I told about the green computing and its benefits to these 220 peoples 73 to 87% people are agree with that government have to take steps towards the awareness of green computing.
14. 65 to 87% people are agree with the objectives of research.

7. REFERENCES

[1] Christian ReimsbachKounatze, "TOWARDS GREEN ICT TRATEGIES: ASSESSING POLICIES AND PROGRAMMES ON ICT AND THE ENVIRONMENT", June 2009.

[2] Fatima Zahra Hanne, "GREEN IT - Why Developing Countries Should Care?", July 2011.

[3] Marguerite Reardon, "Energy – aware Internet Routing Coming soon", August 18, 2009.

[4] AppaGovindasami, Suresh Joseph, "Optimization of Operating Systems towards Green Computing", Sep-Dec 2012.
[5] RiyazA.Sheikh, Dr. U.A. Lanjewar, "Green Computing - Embrace a Secure Future", 2010.
[6] Mydhili K Nair, Dr. V. Gopalakrishna, "Generic Web Services - A step towards Green Computing", 2009.
[7] UsamaAwan, ShakeelSarwar, Muhammad Amir Raza, "Green Consumer Behaviour and Environmental Sustainability", September 2011.
[8] Rajguru P.V., Nayak S. K., More D.S., "Solution for Green Computing", June 2010.
[9] JyotiTayade, "Green Computing-Need of Today", April 2012.
[10] RichaSinha, NidhiPurohit, HiteishiDiwanji, "Energy Efficient Dynamic Integration of Thresholds for Migration at Cloud Data Centers", 2012.
[11] K. Mukherjee, G. Sahoo "Green Cloud: An Algorithmic Approach", November 2010. Tom Worthington, "ICT Sustainability: Assessment and Strategies for a Low Carbon Future", 2011.
[12] http://searchdatacenter.techtarget.com/ definition/ green-computing
[13] http://timesofindia.indiatimes.com/topic/Green-computing
[14] http://www.greencomputing.co.in/
[15] http://www.wikipedia.org/

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 474 - 480, 2013, ISSN: 2319–8656

Successive approximation of neutral stochastic functional differential equations with infinite delay and Poisson jumps

Diem Dang Huan

School of Mathematical
Science, Nanjing Normal
University, Nanjing 210023,
China
Faculty of Basic Sciences,
Bacgiang Agriculture and
Forestry University, Bacgiang,
Vietnam.

Abstract: We establish results concerning the existence and uniqueness of solutions to neutral stochastic functional differential equations with infinite delay and Poisson jumps in the phase space $C((-\infty,0];R^d)$ under non-Lipschitz condition with Lipschitz condition being considered as a special case and a weakened linear growth condition on the coefficients by means of the successive approximation. Compared with the previous results, the results obtained in this paper is based on a other proof and our results can complement the earlier publications in the existing literatures.

Keywords: neutral stochastic functional differential equations; Poisson jumps; infinite delay; successive approximation; Bihari's inequality

1. INTRODUCTION

Stochastic differential equations are well known to model problems from many areas of science and engineering, wherein, quite often the future state of such systems depends not only on the present state but also on its past history (delay) leading to stochastic functional differential equations (SFDEs) and it has played an important role in many ways such as the model of the systems in physics, chemistry, biology, economics and finance from various points of the view (see, e.g. [1,2] and the references therein).

Recently, SFDEs with infinite delay on the space $BC((-\infty,0];R^d)$, which denotes the family of bounded continuous R^d-value functions φ defined on $(-\infty,0]$ with norm $\|\varphi\| = sup_{\theta\in(-\infty,0]}|\varphi(\theta)|$ have been extensively studied by many authors, for instance, in [3], Wei and Wang studied the existence and uniqueness of the solution for SFDEs with infinite delay under uniform Lipschitz condition and a weakened linear growth condition, Zhou et al. [4] investigated the stability of the solutions for SFDEs with infinite delay, and in 2010, Xu and Hu [5] have proved the existence and uniqueness of the solution for neutral SFDEs with infinite delay in abstract space. Note that, the results on the existence and uniqueness of the solution for the above equations is obtained if the coefficient of the equation is assumed to satisfy the Lipschitz condition and the linear growth condition. Furthermore, on the neutral SFDEs with delay, once can see monograph [1] and the references therein for details.

On the other hand, the study of neutral SFDEs with Poisson jumps processes also have begun to gain attention and strong growth in recent years. To be more precise, in 2009, Luo and Taniguchi [6] considered the existence and uniqueness of mild solutions to stochastic evolution equations with finite delay and Poisson jumps by the Banach fixed point theorem, in 2010, Boufoussi and Hajji [7] proved the existence and uniqueness result for a class of neutral SFDEs driven both by the cylindrical Brownian motion and by the Poisson processes in a Hilbert space with non-Lipschitzian coefficients by using successive approximation, in 2012, Cui and Yan [8] studied the existence and uniqueness of mild solutions to stochastic evolution equations with infinite delay and Poisson jumps in the phase space $BC((-\infty,0];H)$, and also in 2012, Tan et al. [9] established the existence and uniqueness of solutions to neutral SFDEs with Poisson Jumps. However, until now, there is no work on the existence and uniqueness of the solution to neutral SFDEs with infinite delay and Poisson jumps in the phase space $C((-\infty,0];R^d)$ under non-Lipschitz condition and a weakened linear growth condition. Therefore, motivated by [5,8,9] in this paper, we will closes the gap and further perfects the theorem system of existence and uniqueness of the solution to the following d-dimensional neutral SFDEs with infinite delay and Poisson jumps:

$$d[x(t) - g(x_t)] = f(t, x_t)dt + \sigma(t, x_t)dB(t)$$

$$+h(t,x_t)dN(t), \qquad t \in [t_0,T], \qquad (1.1)$$

with an initial data

$$x_{t_0} = \varphi = \{\varphi(t): -\infty < t \le 0\} \qquad (1.2)$$

is an F_{t_0}-measurable $C((-\infty,0];R^d)$ -value random variable such that $\varphi \in M^2((-\infty,0];R^d)$, where $x_t = x(t+\theta),\ \theta \in (-\infty,0]$ can be considered as a $C((-\infty,0];R^d)$ - value stochastic process. Moreover, let the functions $g: C((-\infty,0];R^d) \to R^d$;

$$f,h: [t_0,T] \times C((-\infty,0];R^d) \to R^d;$$

$$\sigma: [t_0,T] \times C((-\infty,0];R^d) \to R^{d\times m}$$

all be Borel measurable.

The aim of our paper is to establish an existence and uniqueness results for solution of Eq.(1.1) with initial data (1.2) in the phase $C((-\infty,0];R^d)$ under non-Lipschitz condition and a weakened linear growth condition based on successive approximation method. Our main results rely essentially on techniques using a iterative scheme (see, [10]) which is partially different from the Picard iterative and Bihari's inequality. We will see that the proof of claim in the theorem of this paper is partially different and even simpler than the work has been previously published.

The rest of this paper is organized as follows: In Section 2, we will give some necessary notations, concepts and assumptions. Section 3 is devoted to prove the existence and uniqueness of Eq.(1.1) with initial data (1.2) under non-Lipschitz condition and a weakened linear growth condition. In the last section, concluding remarks are given.

2. PRELIMINARIES RESULTS

This section is concerned with some basic concepts, notations, definitions, lemmas and preliminary facts which are used through this article.

Let (Ω,F,P) be a complete probability space equipped with some filtration $\{F_t,t\ge 0\}$ satisfying the usual conditions (i.e., it is right continuous and $\{F_t,t\ge 0\}$ contains all P-null sets). Let $|\cdot|$ be the Euclidean norm in R^d i.e., $|x| = \sqrt{x^T x}$, $x \in R^d$. If A is a vector or a matrix, its transpose is denoted by A^T. If A is a matrix, its trace norm is represented by $|A| = \sqrt{A^T A}$, while its operator norm is denoted $|A| = sup\{Ax: |x| = 1\}$, (without any confusion with $\|\rho\|$). Without loss of generality, let t be a positive constant. Assume that B(t) is a m-dimensional Brownian motion defined on complete probability space, that is $B(t) = (B_1(t), B_2(t),\ldots, B_m(t))^T$, and N(t) is a scalar Poisson process with intensity λ. Assume that B(t) and N(t) are independent of $\{F_t,t\ge 0\}$. Let $C((-\infty,0];R^d)$ denotes the family of all right-continuous functions with left-hand limits (cadlag) $(-\infty,0]$ to R^d. The space $C((-\infty,0];R^d)$ is assumed to be equipped with the norm $\|\rho\| = sup_{\theta\in(-\infty,0]}|\rho(\theta)|$. We denote by $\varphi \in M^2((-\infty,0];R^d)$ the family of all $\{F_t,t\ge 0\}$ -measurable, R^d -valued process $\varphi(t)= \varphi(t,\omega)$, $t\in(-\infty,0]$ such that $E\int_{-\infty}^{0}|\varphi(t)|^2dt < \infty$. And let $L^p([a,b];R^d)$, $p\ge 2$ be the family of R^d -valued F_t-adapted processess $\{\gamma(t): a \le t \le b\}$ such that $\int_a^b|\gamma(t)|^p dt < \infty$. Further, we consider the Banach space B_T of all R^d -valued F_t -adapted cadlag process x(t) defined on $(-\infty,T]$, $T>0$ such that

$$\|x\|_{B_T}^2 := E\left(\sup_{t\in(-\infty,T]}|x(t)|^2\right) < \infty.$$

For simplicity, we also have to denote by $a\wedge b := \min\{a,b\}$ and $a\vee b := \max\{a,b\}$.
Let us give the definition of solution for Eq.(1.1) with initial data (1.2).

Definition 2.1 An R^d -valued stochastic process x(t) defined on $-\infty<t\le T$ is called the solution of Eq.(1.1) with initial data (1.2), if it has the following properties:

(i) x(t) is continuous and $\{x(t): t_0 \le t \le T\}$ is F_t -adapted;

(ii) $\{f(t,x_t)\} \in L^1([t_0,T];R^d)$, $\{\sigma(t,x_t)\} \in L^2([t_0,T];R^{d\times m})$, and $\{h(t,x_t)\} \in L^2([t_0,T];R^{d\times m})$;

(iii) $x_{t_0} = \varphi$ and for $t_0 \le t \le T$,

$$x(t) = \varphi(0) - g(\varphi) + g(x_t) + \int_{t_0}^{t} f(s,x_s)ds$$

$$+ \int_{t_0}^{t} \sigma(s,x_s)dB(s) + \int_{t_0}^{t} h(s,x_s)dN(s), \qquad (2.1)$$

A solution x(t) is said to be unique if any other solution x*(t) is indistinguishable with x(t), that is

$$P\{x(t) = x^*(t), \text{ for any } -\infty<t\le T\} = 1.$$

In order to guarantee the existence and uniqueness of the solutions to Eq.(1.1) with initial data (1.2), we propose the following assumptions:

(**H1**) For all $\xi, \eta \in C((-\infty,0];R^d)$ and $t_0 \le t \le T$, it follows that

$$|f(t,\xi)-f(t,\eta)|^2 \vee |\sigma(t,\xi)-\sigma(t,\eta)|^2$$
$$\vee |h(t,\xi)-h(t,\eta)|^2 \le \tau(\|\xi-\eta\|^2),$$

where $\tau(\bullet)$ is a concave, nondecreasing, and continuous function from R^+ to R^+ such that $\tau(0)=0, \tau(u)>0$ for $u>0$ and $\int_{0^+} \frac{du}{\tau(u)} = \infty$.

(**H2**) For all $t_0 \le t \le T$, it follows that f(t,0), σ(t,0), h(t,0)∈L^2 such that

$$|f(t,0)|^2 \vee |\sigma(t,0)|^2 \vee |h(t,0)|^2 \le C_0,$$

where C_0>0 is a constant.

(**H3**) There exists a positive number K∈(0,1) such that, for all $\xi, \eta \in C((-\infty,0];R^d)$ and $t_0 \le t \le T$,

$$|g(\xi)-g(\eta)| \le K\|\xi-\eta\|.$$

Remark 2.1 To demonstrate the generality of our results, let us illustrate it using concrete function τ(•).
Let ε∈(0,1). Set

$$\tau_1(u)=u, \ \forall u \ge 0.$$

$$\tau_2(u)=\begin{cases} u\log(\frac{1}{u}), & 0\le u\le\varepsilon, \\ \varepsilon\log(\frac{1}{\varepsilon})+\tau_2'(\varepsilon-)(u-\varepsilon), & u>\varepsilon, \end{cases}$$

$$\tau_3(u)=\begin{cases} u\log(\frac{1}{u})\log\log(\frac{1}{u}), & 0\le u\le\varepsilon, \\ \varepsilon\log(\frac{1}{\varepsilon})\log\log(\frac{1}{\varepsilon})+\tau_3'(\varepsilon-)(u-\varepsilon), & u>\varepsilon, \end{cases}$$

where ε is sufficiently small and τ_i', $i=2,3$ is the left derivative of τ_i, $i=2,3$ at the point ε. Then τ_i, $i=1,2,3$ are concave nondecreasing functions definition on R^+ satisfying $\int_{0^+} \frac{du}{\tau_i(u)} = \infty$.

Remark 2.2 If there exist a positive constant δ, such that τ(u)= δu, u∈C((-∞,0];R^d) then assumption (**H1**) implies the Lipschitz condition.

3. EXISTENCE AND UNIQUENESS OF SOLUTION

In this section, we shall investigate the existence and uniqueness of the solution to Eq.(1.1) with initial data (1.2).

The main result of the paper is the following theorem.

Theorem 3.1 Assume the assumptions of (**H1**)-(**H3**) hold. Then, there exist a unique solution to Eq.(1.1) with initial data (1.2). Moreover, the solution belongs to B_T.

To prove the uniqueness of the solution for Eq.(1.1) with initial data (1.2), we shall establish the following lemma.

Lemma 3.1 Let the assumptions of Theorem 3.1 hold. If x(t) is a solution of Eq.(1.1) with initial data (1.2), then there exists a positive constant C* such that

$$\|x(t)\|_{B_T}^2 \le C^*.$$

Proof For every integer n ≥ 1, define the stopping time

$$\tau_n = T\wedge\inf\{t\in[t_0,T]: \|x_t\| \ge n\}.$$

Obviously, as n → ∞, $\tau_n \uparrow$ T a.s. Let $x^n(t) = x(t\wedge\tau_n)$, for $-\infty<t\le T$. Then, for t∈[t_0,T], $x^n(t)$ satisfy the following equation:

$$x^n(t)=\varphi(0)-g(\varphi)+g^n(x_t)$$
$$+\int_{t_0}^{t} f(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}ds+\int_{t_0}^{t}\sigma(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}dB(s)$$
$$+\int_{t_0}^{t} h(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}dN(s),$$

where $\mathbf{1}_A$ is the indicator function of a set A. Set

$$I^n(t):=\varphi(0)+\int_{t_0}^{t} f(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}ds$$
$$+\int_{t_0}^{t}\sigma(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}dB(s)$$
$$+\int_{t_0}^{t} h(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}dN(s).$$

By Lemma 2.3 (p. 204) in [1] and assumption (**H3**), we have

$$|x^n(t)|^2 \le \tfrac{1}{K}|g(x_t^n)-g(\varphi)|^2+\tfrac{1}{1-K}|I^n(t)|^2$$
$$\le \sqrt{K}\|x_t^n\|^2+\tfrac{K}{1-\sqrt{K}}\|\varphi\|^2+\tfrac{1}{1-K}|I^n(t)|^2.$$

Hence

$$E\sup_{t_0\le s\le t}(|x^n(t)|^2) \le \sqrt{K}E\sup_{-\infty\le s\le t}(|x^n(t)|^2)$$
$$+\frac{K}{1-\sqrt{K}}E\|\varphi\|^2+\frac{1}{1-K}E\sup_{t_0\le s\le t}|I^n(t)|^2 .$$

Noting the fact that

$$\sup_{-\infty<s\le t}|x^n(s)|^2 \le \|\varphi\|^2 + \sup_{t_0\le s\le t}|x^n(s)|^2,$$

we can get

$$\mathrm{E}\sup_{-\infty\le s\le t}(|\mathrm{x^n(t)}|^2) \le \frac{1+\mathrm{K}-\sqrt{\mathrm{K}}}{(1-\sqrt{\mathrm{K}})^2}\mathrm{E}\|\varphi\|^2 + \frac{1}{(1-\sqrt{\mathrm{K}})(1-\mathrm{K})}\mathrm{E}\sup_{t_0\le s\le t}|I^n(t)|^2.$$

Using the basic inequality $|a+b+c+d|^2 \le 4|a|^2+4|b|^2+4|c|^2+4|d|^2$, Hölder's inequality, and for the jump integral, we convert to the compensated Poisson process $\tilde{N}(t) := N(t) - \lambda t$, which is a martingale, we have

$$|I^n(t)|^2 \le 4|\varphi(0)|^2 + 4\left|\int_{t_0}^t f(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}ds\right|^2 + 4\left|\int_{t_0}^t \sigma(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}dB(s)\right|^2 + 4\left|\int_{t_0}^t h(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}dN(s)\right|^2$$

$$\le 4|\varphi(0)|^2 + 4(t-t_0)\int_{t_0}^t |f(s,x_s^n)|^2 ds + 4\left|\int_{t_0}^t \sigma(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}dB(s)\right|^2 + 8\left|\int_{t_0}^t h(s,x_s^n)\mathbf{1}_{[t_0,\tau_n]}d\tilde{N}(s)\right|^2 + 8\lambda^2(t-t_0)\int_{t_0}^t |h(s,x_s^n)|^2 ds.$$

By Theorem 7.2 (p. 40) in [1], the Doob martingale inequality (apply for the jump integral, see, for example [1]), assumptions (**H1**) and (**H2**), one can show that

$$\mathrm{E}\sup_{t_0\le s\le t}|I^n(t)|^2 \le 4E|\varphi(0)|^2 + 4(t-t_0) \times E\int_{t_0}^t |f(s,x_s^n)|^2 ds + 16E\int_{t_0}^t |\sigma(s,x_s^n)|^2 ds + 8[4\lambda+\lambda^2(t-t_0)]E\int_{t_0}^t |h(s,x_s^n)|^2 ds$$

$$\le 4E\|\varphi\|^2 + 8C_0(T-t_0)[4+(T-t_0) +2(4\lambda+\lambda^2(T-t_0))] + 8[4+(T-t_0) +2(4\lambda+\lambda^2(T-t_0))]E\int_{t_0}^t \tau(\|x_s^n\|^2)ds.$$

Given that $\tau(\bullet)$ is concave and $\tau(0)=0$, we can find a pair of positive constants a and b such that $\tau(u)\le a+bu$, for all $u \ge 0$. So, we obtain that

$$\mathrm{E}\sup_{t_0\le s\le t}|I^n(t)|^2 \le 4E\|\varphi\|^2 + 8(C_0+a)(T-t_0)\times [4+(T-t_0)+2(4\lambda+\lambda^2(T-t_0))] + 8b[4+(T-t_0)+2(4\lambda+\lambda^2(T-t_0))]\times \int_{t_0}^t E(\|x_s^n\|^2)ds \le C_1 + C_2\int_{t_0}^t \mathrm{E}\sup_{-\infty\le r\le s}(|\mathrm{x^n(r)}|^2)\mathrm{ds},$$

where

$$C_1 := 4E\|\varphi\|^2 + 8(C_0+a)(T-t_0)\times [4+(T-t_0)+2(4\lambda+\lambda^2(T-t_0))]$$

and

$$C_2 := 8b[4+(T-t_0)+2(4\lambda+\lambda^2(T-t_0))].$$

Thus, we can get

$$\mathrm{E}\sup_{-\infty\le s\le t}(|\mathrm{x^n(t)}|^2) \le \frac{\mathrm{C_1}}{(1-\sqrt{\mathrm{K}})(1-\mathrm{K})} + \frac{1+\mathrm{K}-\sqrt{\mathrm{K}}}{(1-\sqrt{\mathrm{K}})^2}\mathrm{E}\|\varphi\|^2 + \frac{\mathrm{C_2}}{(1-\sqrt{\mathrm{K}})(1-\mathrm{K})}\int_{t_0}^t \mathrm{E}\sup_{-\infty\le r\le s}(|\mathrm{x^n(r)}|^2)\mathrm{ds}.$$

By the Gronwall inequality yields that

$$\mathrm{E}\sup_{-\infty\le s\le t}(|\mathrm{x^n(t)}|^2) \le C_3 e^{C_4},$$

where

$$C_3 := \frac{\mathrm{C_1}}{(1-\sqrt{\mathrm{K}})(1-\mathrm{K})} + \frac{1+\mathrm{K}-\sqrt{\mathrm{K}}}{(1-\sqrt{\mathrm{K}})^2}\mathrm{E}\|\varphi\|^2$$

and

$$C_4 := \frac{\mathrm{C_2}}{(1-\sqrt{\mathrm{K}})(1-\mathrm{K})}.$$

Letting t = T, it then follows that

$$\mathrm{E}\sup_{-\infty\le s\le T}(|\mathrm{x}\ \ (s\wedge\tau_n)|^2) \le C_3 e^{C_4}.$$

Consequently,

$$E\sup_{-\infty\le s\le\tau_n}(|x(s)|^2)\le C_3e^{C_4}.$$

Letting $n\to\infty$, it then implies the following inequality

$$E\sup_{-\infty\le s\le T}(|x(s)|^2)\le C_3e^{C_4}.$$

Thus, the desired result holds with $C^*:= C_3e^{C_4}$. This completes the proof of Lemma 3.1.

Now, motivated by [10], we shall introduce the sequence of successive approximations to Eq.(2.1) as follows:

Define $x^0(t)=\varphi(0)$ for all $t_0\le t\le T$. Let $x_{t_0}^n=\varphi$, $-\infty<t\le 0$, n=0,1,2, … and for all $t_0\le t\le T$, n=1,2, …, we define the following iterative scheme:

$$x^n(t)=\varphi(0)-g(\varphi)+g(x_t^n)+\int_{t_0}^t f(s,x_s^{n-1})ds$$
$$+\int_{t_0}^t\sigma(s,x_s^{n-1})dB(s)+\int_{t_0}^t h(s,x_s^{n-1})dN(s).\ (3.1)$$

Next, we prove the main result of our paper.

Proof of Theorem 3.1. The proof is split into the following three steps.

Step 1. We claim that the sequence $\{x_t^n\}_{n\ge0}$ is bounded. Obviously, $x^0(t)\in B_T$. Moreover, by the same way as in the proof of Lemma 3.1 and note that

$$\max_{1\le n\le k}E\sup_{-\infty<s\le t}|x^{n-1}(s)|^2\le E\|\varphi\|^2+$$
$$\max_{1\le n\le k}E\sup_{-\infty<s\le t}|x^n(s)|^2,$$

we can easily show that $x^n(t)\in B_T$, for , $-\infty<t\le T$ and n=1,2,.... This proves the boundedness of $\{x_t^n\}_{n\ge0}$.

Step 2. We claim that the sequence $\{x_t^n\}_{n\ge0}$ is a Cauchy sequence in B_T. For m, n ≥ 0 and t∈ [t_0,T], from (3.1) and by Lemma 2.3 in [1], we can get

$$|x^n(t)-x^m(t)|^2\le\frac{1}{K}|g(x_t^n)-g(x_t^m)|^2$$
$$+\frac{3}{1-K}\left|\int_{t_0}^t[f(s,x_s^{n-1})-f(s,x_s^{m-1})]ds\right|^2$$
$$+\frac{3}{1-K}\left|\int_{t_0}^t[\sigma(s,x_s^{n-1})-\sigma(s,x_s^{m-1})]dB(s)\right|^2$$
$$+\frac{3}{1-K}\left|\int_{t_0}^t[h(s,x_s^{n-1})-h(s,x_s^{m-1})]dN(s)\right|^2.$$

By Hölder's inequality, Theorem 7.2 in [1], the Doob martingale inequality for the jump integral, and assumptions (**H1**), (**H3**), we obtain that

$$E\sup_{t_0\le s\le t}(|x^n(t)-x^m(t)|^2)$$
$$\le K\,E\sup_{t_0\le s\le t}(|x^n(t)-x^m(t)|^2)$$
$$+\frac{C_5}{(1-K)}\int_{t_0}^t\tau(E\sup_{t_0\le r\le s}(|x^{n-1}(r)-x^{m-1}(r)|^2))ds,$$

where $C_5:=3[4+8\lambda+(2\lambda^2+1)(T-t_0)]$, which further implies that

$$E\sup_{t_0\le s\le t}(|x^n(t)-x^m(t)|^2)\ \le\frac{C_5}{(1-K)^2}$$
$$\times\int_{t_0}^t\tau(E\sup_{t_0\le r\le s}(|x^{n-1}(r)-x^{m-1}(r)|^2))ds.\ (3.2)$$

Let

$$y(t):=\lim_{n,m\to+\infty}sup\ E\sup_{t_0\le s\le t}(|x^n(t)-x^m(t)|^2).$$

From (3.2), for any ε > 0, we have

$$y(t)\le\varepsilon+\frac{C_5}{(1-K)^2}\int_{t_0}^t\tau(y(s))\,ds.$$

By the Bihari inequality [11], which implies that, for all sufficiently small ε > 0,

$$y(t)\le G^{-1}\left[G(\varepsilon)+\frac{C_5}{(1-K)^2}(T-t_0)\right],\qquad(3.3)$$

where $G(r)=\int_1^r\frac{du}{\tau(u)}$ on r > 0 and $G^{-1}(\bullet)$ is the inverse function of G(•). By assumption, $\int_{0+}\frac{du}{\tau(u)}=\infty$ and the definition of τ(•), one sees that $\lim_{\varepsilon\to0}G(\varepsilon)=-\infty$ and then

$$\lim_{\varepsilon\to0}G^{-1}\left[G(\varepsilon)+\frac{C_5}{(1-K)^2}(T-t_0)\right]=0.$$

Therefore, letting ε→0 in (3.3), we infer that for all s∈[t_0,T], y(t)=0.

This shows that sequence $\{x_t^n\}_{n\ge0}$ is a Cauchy sequence in L^2. Hence, $x^n(t)\xrightarrow{L^2}x(t),n\to\infty$, that is $E|x^n(t)-x(t)|^2\xrightarrow{n\to\infty}0$. Furthermore, by the boundedness of $\{x_t^n\}_{n\ge0}$ in Step 1, letting n→∞ we can easily derive that $\|x(t)\|_{B_T}^2\le C^*$, where C* is a positive constant. This shows that x(t)∈B_T.

Step 3. We claim the existence and uniqueness of the solution to Eq.(1.1).

Existence: By the same way as in Step 2, and the sequence $x^n(t)$ is uniformly converge on $(-\infty,T]$, letting $n\to\infty$ in (3.1), we can derive the solution of Eq.(1.1) with the initial data (1.2). Thus the existence of the Theorem 3.1 is complete.

Uniqueness: Let both x(t) and z(t) be two solutions of Eq.(1.1). By Lemma 3.1, $x(t), z(t)\in B_T$. On the other hand, by the same way as in Step 2, we can show that there exist a positive constant C_6 such that

$$\mathrm{E}\sup_{t_0\le s\le t}(|x(s)-z(s)|^2)$$
$$\le C_6\int_{t_0}^{t}\tau(\mathrm{E}\sup_{t_0\le r\le s}(|x(r)-z(r)|^2))ds.$$

Consequently, for any $\varepsilon > 0$

$$\mathrm{E}\sup_{t_0\le s\le t}(|x(s)-z(s)|^2)$$
$$\le \varepsilon + C_6\int_{t_0}^{t}\tau(\mathrm{E}\sup_{t_0\le r\le s}(|x(r)-z(r)|^2))ds.$$

By Bihari's inequality, for all sufficiently small $\varepsilon > 0$, we can show that

$$\mathrm{E}\sup_{t_0\le s\le t}(|x(s)-z(s)|^2)\le G^{-1}[G(\varepsilon)+C_6(T-t_0)],$$

where $G(r)=\int_1^r\frac{du}{\tau(u)}$ on $r > 0$ and $G^{-1}(\bullet)$ is the inverse function of $G(\bullet)$. By assumption, we get

$$\mathrm{E}\sup_{t_0\le s\le t}(|x(s)-z(s)|^2)=0,$$

which further implies $x(s)\equiv z(s)$ almost surely for any $s\in[t_0,T]$. Therefore, for all $-\infty<s\le T$, $x(s)\equiv z(s)$ almost surely. The proof for Theorem 3.1 is thus complete.

Remark 3.1. By using methods similar to many articles about the theorems of the existence and uniqueness of the solution for SFDEs (see [1] or [9], Theorem 3.6), if non-Lipschitz condition is replaced by the local non-Lipschitz condition, then the existence and uniqueness theorem for neutral SFDEs with infinite delay and Poisson jumps in the phase space $C((-\infty,0];R^d)$ under local non-Lipschitz condition and the conditions (**H2**), (**H3**) is also derived.

Remark 3.2. If the phase space $C((-\infty,0];R^d)$ is replaced by the phase space $B((-\infty,0];R^d)$ (see [5]) which has origin was introduced by Hale and Kato [12] then by using method in our paper, conclusions of Theorem 3.1 also easily obtained.

Remark 3.3. If Eq.(1.1) with initial data (1.2) in the phase space $C((-\infty,0];R^d)$ under the non-Lipschitz condition and the weakened linear growth condition is replaced by the phase $C((-r,0];R^d)$ (i.e. with finite delay) under the uniform Lipschitz condition and the linear growth condition then Theorem 3.2 in Tan el at. [9] can be obtained by Theorem 3.1.

Remark 3.4. We have known that in paper [8], the proofs of the assertions are based on some function inequalities. If using our proof then the conclusions in paper [8] can be also obtained and we have saw that the procedures in our paper have become simpler than the procedures used in [8].

Remark 3.5. In real world problems, impulsive effects also exist in addition to stochastic effects. The theory of impulsive differential equations is much richer than the corresponding theory of differential equations without impulse effects. Differential equation with impulsive conditions constitute an important field of research due to their numerous applications in ecology, medicine biology, electrical engineering, and other areas of science. There has been a significant development in impulsive theory especially in the area of impulsive differential equation with fixed moments, see for instance the monograph by Lakshmikantham et al. [13]. Recently, the existence and uniqueness of the solution for impulsive SFDEs without infinite delay and Poisson jumps have been discussed in [14]. Therefore, it is necessary and important to consider the existence and uniqueness of the solution for SFDEs with infinite delay, Poisson jumps and impulsive effects. The results in this paper can be extended to study the existence and uniqueness of the solution for SFDEs with infinite delay, Poisson jumps and impulsive effects by employing the idea and technique as in Theorem 3.1.

4. CONCLUSION

In this paper, we have discussed for a class of neutral SFDEs with infinite delay and Poisson jumps in the phase space $C((-\infty,0];R^d)$ under non-Lipschitz condition with Lipschitz condition being considered as a special case and a weakened linear growth condition on the coefficients by means of the successive approximation. By using a iterative scheme, Bihari's inequality combined with theories of stochastic analytic, then the existence and uniqueness theorem for neutral SFDEs with infinite delay and Poisson jumps is obtained. The results in our paper extend and improve the corresponding ones announced by Xu and Hu [5], Cui and Yan [8], Tan el al. [9], Chen [10], and some other results.

5. ACKNOWLEDGMENTS

The author would like to thank the referees for comments and suggestions.

6. REFERENCES

[1] Mao, X. 2007. Stochastic Differential Equations and Applications. 2nd ed., Chichester, UK: Horwood Publishing Limited.

[2] Oksendal, B. 2005. Stochastic Differential Equations. 6th ed., New York: Springer.

[3] Wei, F. Y. and Wang, K. 2007. The existence and uniqueness of the solution for stochastic functional differential equations with infinite delay. J. Math. Anal. Appl., 333: 516-531.

[4] Zhou, S. B., Wang, Z. Y., and Feng, D. 2009. Stochastic functional differential equations with infinite delay. J. Math. Anal. Appl., 357: 416-426.

[5] Xu, Y. and Hu, S. G. 2010. The existence and uniqueness of the solution for neutral stochastic functional differential equations with infinite delay in abstract space. Acta Appl. Math., 110(2): 364-372.

[6] Luo, J. and Taniguchi, T. 2009. The existence and uniqueness for non-Lipschitz stochastic neutral delay evolution equations driven by Poisson jumps. Stoch. Dyn., 9(1): 627-638.

[7] Boufoussi, B. and Hajji, S. 2010. Successive approximations of neutral functional stochastic differential equations with jumps. Stat. Prob. Lett., 80: 324-332.

[8] Cui, J. and Yan, L. T. 2012. Successive approximations of neutral stochastic evolution equations with infinite delay and Poisson jumps. Appl. Math. Comput., 128: 6776-6784.

[9] Tan, J. Q., Wang, H. L., and Guo, Y. F. 2012. Existence and uniqueness of solutions to neutral stochastic functional differential equations with Poisson Jumps. Abstr. Appl. Anal., 2012, Art. ID 371239, 20 pp.

[10] Chen, H. B. 2010. The existence and uniqueness for the solution of neutral stochastic functional differential equations with infinite delay. J. Math. Research and Exposition, 30(4): 589-598.

[11] Bihari, I. 1956. A generalization of a lemma of Bellman and its application to uniqueness problem of differential equations. Acta Math. Acad. Sci. Hungar., 7：71-94.

[12] Hale, J. K. and Kato, J. 1978. Phase spaces for retarded equations with infinite delay. Funkcial. Ekvac., 21: 11-41.

[13] Lakshmikantham, V., Bainov, D., and Simeonov, P. S. 1989. Theory of impulsive differential equations. Series in Modern Applied Mathematics, 6. World Scientific Publishing Co., Inc., Teaneck, NJ.

[14] Shen, L. J. and Sun, J. T. 2010. Existence and uniqueness of solution for stochastic impulsive differential equations. Stoch. Dyn., 10(3): 375-383.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 481 - 486, 2013, ISSN: 2319–8656

WRTS: Wireless Sensor Based Real Time Traffic Information System

G.Bhaskar
Department of Computer Science and Engineering
Siddaganga Institute of Technology,
Tumkur, Karnataka, India.

Raghu BA,
Department of Computer Science and Engineering
Siddaganga Institute of Technology,
Tumkur, Karnataka, India.

Abstract: Due to increasing traffic density, driving takes longer time within cities than in highways. The situation is worse in peak hours, when people travel from home to offices and vice versa. Emergency services, like ambulance services, fire brigade, police service etc., are directly affected due to increased traffic density. The existing traffic monitoring techniques will fail to provide real time traffic information to the user. India is known for billion populations and like in majority of developing countries like Indian roads are non-lane based and it has chaotic traffic. The existing traffic monitoring techniques are mainly infrastructure based system. Which is expensive and it requires constant maintenance. This paper focuses on fetching real time traffic information which is infrastructure less based system which is inexpensive in nature and it is also reachable to a normal person, like fetching real time traffic information from user who carry smart phones which play a role of sensor during their travel. This leads to building of wireless sensor network of mobiles.

Keywords: Sensing; BTS, GPS, Traffic Light control, Chaotic Traffic, WRTS;

1. INTRODUCTION

Road traffic congestion is a recurring problem worldwide. In developing countries like India, a fast growing economy, the problem is acutely felt in almost all major cities. This is primarily because infrastructure growth is slow compared to growth in number of vehicles, due to space and cost constraints. Secondly, like in majority of developing countries like India traffic being non-lane based and chaotic is largely different from the western traffic. Like India, the second most populous country in the world, and a fast growing economy, is seeing terrible road congestion problems in its cities. Building infrastructure, levying proper taxes to curb private vehicle growth and improving public transport facilities are long-term solutions to this problem. These permanent solution approaches need government intervention. The Government of India has committed Rs.234,000 corers in the urban infrastructure sector Bus Rapid Transit (BRT), metro rails and mono rails are being built in different cities to encourage the use of public transport[10]. But still there is a steep growth of private vehicles Some cities like Bangalore, Pune, Hyderabad Delhi-NCR, with their sudden growths in the IT sector, also have a steep growth in population, further increasing transportation needs. Meeting such growth with infrastructure growth is seemingly infeasible, primarily because of space and cost constraints. Intelligent management of traffic flows and making commuters more informed about traffic and road status, can reduce the negative impact of congestion, though cannot solve it altogether. Traffic monitoring systems deployed until now, utilize data collected mainly through fixed sensors, which provide information about the number and speed of vehicles that cross them. Nevertheless, this type of system is not deployed at wide scales mostly because of its high cost. Mobile devices used as traffic sensors present major advantages compared to other solutions[11]. So far, all the existing solutions require the design, implementation and maintenance of special infrastructure, which can be both expensive and difficult to deploy. On the other hand, cellular networks are already widely deployed and provide large population coverage. Modern mobile devices come equipped with Global Position System (GPS) receivers which can calculate the device's location and speed with sufficient accuracy. On the communication side, many wireless standards (3G/4G/WLAN) are already included and most of the upcoming standards are expected to be integrated in the near future. This connectivity capacity and the array of sensors that mobile devices are equipped with, make them suitable for gathering a great amount of traffic data. Finally, modern mobile devices feature high resolution screens or touch screens that can be used for interacting with the driver and display detailed information. This paper presents Wireless Sensor Network Based Real Time Traffic Information System (WRTS) this focuses on fetching real time traffic information from user who carry smart phones which play a role of sensor during their travel. This leads to building of wireless sensor network of mobiles. This paper is organised as follows. In Section II of the paper, we present the Related Work, Section III gives the Scenario and Proposed system, and in section IV Implementation and results are presented, and section V deals with Conclusion, VI is Acknowledgement and finally Section VII have References for the paper.

2. RELEATED WORK

2.1 Impact of Traffic Jam in India

As the economic gloom intensifies, a report by the Ministry of Road, Transport and Highways only makes the picture worse. Traffic snarls on highways, delays at toll plazas,

accidents and political blockades annually cost the economy nearly ***Rs.40 billion*** in lost truck-operating hours, says the Second Report on Operational Efficiency of Freight Transportation by Road in India, released by minister of road, transport and highways C.P. Joshi here on July 1st 2012[1].

Traffic jam is a condition on road networks that occurs as use increases, and is characterized by slower speeds, longer trip times, and increased vehicular queuing. As demand approaches the capacity of a road (or of the intersections along the road), extreme traffic jam sets in. When vehicles are fully stopped for periods of time, this is colloquially known as a traffic jam.

Fig 2.1: CCTV View of Traffic jams in Bangalore.

Fig 2.2: Bangalore Traffic control Room.

Traffic jam has a number of negative effects:

- Wasting time of motorists and passengers. As a non-productive activity for most people, traffic jam reduces regional economic health.
- Delays, which may result in late arrival for employment, meetings, and education, resulting in lost business, disciplinary action or other personal losses.
- Inability to forecast travel time accurately, leading to drivers allocating more time to travel "just in case", and less time on productive activities.
- Emergencies: blocked traffic may interfere with the passage of emergency vehicles traveling to their destinations where they are urgently needed.
- Higher chance of jam due to tight spacing and constant stopping-and-going.

Fig 2.3: Bangalore City wide sensing Architecture [4].

There are two main kinds of roads, the yellow lines denote the major roads and the white lines denote minor roads. The junctions where the major roads intersect one another are shown by red squares and those where the minor roads intersect the major roads are shown by blue dots. *Traffic light control* is a vital necessity for both these type of intersections that will govern the traffic flow pattern over the entire city. Currently, in absence of automated signal control techniques, the traffic lights are either statically calibrated, or controlled by on-road policemen, or remotely controlled by manually seeing video feeds at the traffic control room.

As for like Indian commuters, the traffic applications currently available are rudimentary, with periodic updates gathered from traffic police broadcast on FM radios. There are a few route planners that give bus and train plans, but the plans are static, without considering the current congestion levels on different roads.

Choice of sensing method

Participatory sensing data inherently noisy [3]. Also probe vehicles might not be present at a given intersection at all times. Such sensing methods can thus be used for applications like travel time estimates and congestion maps to be disseminated to commuters, which can tolerate aperiodicity and noisiness. Applications like traffic light control on the other hand, need dedicated static sensors on the road that give highly accurate and strictly periodic updates about traffic conditions. Static sensors are costly but accurate, mobile and hybrid sensors are cheap but

noisy. Based on applications, we need to make a careful choice of which mode to use when and how to mix them appropriately [3]. The red squares and blue dots in Fig. 2.3 would thus be probable candidates for static sensing, while the mobile and hybrid sensors would span the city, in varying densities over time, as the green triangles in the figure.

2.3 Sample Case: Bangalore Traffic Monitoring System (BTS)

Explaining the existing system in the context of (BTS) At present, out of 160 cameras in Bangalore, connected to central traffic control room by BSNL leased lines, at most 90 cameras send data at any given time, because of problems in the wired connections. Instead of this star topology, will a tiered architecture help, where video feeds from a subset of roads are processed at local control rooms, before the information is passed to central control? Should there be a mix of wired and wireless communication to reduce cost and overhead of laying copper, or will wireless be too unreliable? Can communication costs be reduced through in-field computation and data compression? As for mobile sensing models, quantitative analysis of 3G and GPRS performance on Indian roads, using mobile for traffic data upload and download would be a feasible solution.

3. SCENARIO AND PROPOSED SYSTEM

This paper deals with scenario of tracking and fetching real time traffic information from the user's mobile during their travel. Application will update this traffic information to all the users in the same path. In this proposed system we have two algorithms Traffic_ServerRun and Traffic_ClientRun which usually runs on server and client which is user's mobile.

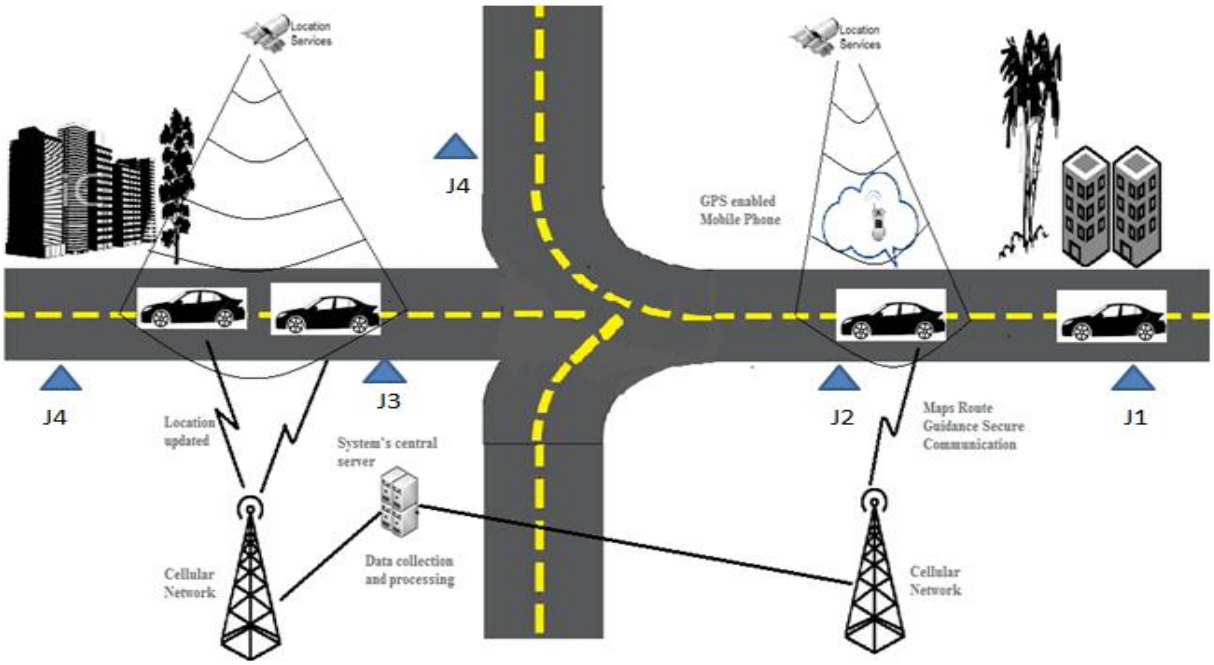


Figure 1: Illustrating complete Scenario of WRTS

Algorithm: Traffic Server_Run

V: Vertices where each vertex represent a junction
E: The Edge represents the path
Asj: Average Speed at Junction
Atj: Average Time at Junction
MC: Map co-ordinates

Begin
01: Initialize G with set of (V, E)
02: Receive_ Request (source, destination)
03: Load MC (C_1……C_n) € G (V', E') from database
04: **while**
05: Fetch junction points € G' (V', E') **do**
06: **for** each junction point in G' (V', E') **do**
07: ∀ **initial** users Call
08: Fetch_PrecalculatedAvgtime_Avgspeed ()
09: **end for**
10: **for** each junction point in G' (V', E')
11: Receive_enduser (*UID, Jdistance, Jspeed, J* time)
12: $JAs = \frac{\sum_{i=1}^{n} \text{spead of each user}}{\text{Number of users at the junction}}$
13: $JAt = \frac{\sum_{i=1}^{n} \text{time of each user to reach junction}}{\text{Number of users at the junction}}$
14: Update_Client (UID, *JAs* , *JAt*)
15: **end for**
16: **end while** (Till user reaches destination)
End

Algorithm: Traffic Client_Run
Input: Sensor Network G (V, E), Source, Destination
Output: Real time traffic information for user to reach destination

T [Lt, Ln]: Object Trajectory Data
Junction List[i]: Vector of Junction
P_{jt}: Previous Junction Time
C_{jt}: Current Junction Time

Begin
01: User inputs destination
02: **do**
Fetch latitude and longitude from GPS
03: **for** each junction in Junction List[i] **do**
04: dis=distance (T_{cur} (lat, long), T (J_i (Lt)), T (J_i (Ln)))
05: **if** (distance<100 meter)
06: P_{jt}=fetch time of junction i-1
07: C_{jt}=fetch time of junction i
08: *J* time= P_{jt}-C_{jt}
09: **end if**
10: Jdistance=distance(Prev(J_i(Lt) , J_i(Ln), Current (J_k(Lt) , J_k(Ln))
11: $JSpeed = \frac{Jdistance}{JdiferenceTime}$
12: Upload_ To_Server (*J*distance, *J*speed, *J* time)
13: **end for**
14: **end while** (Destination Reached)
End

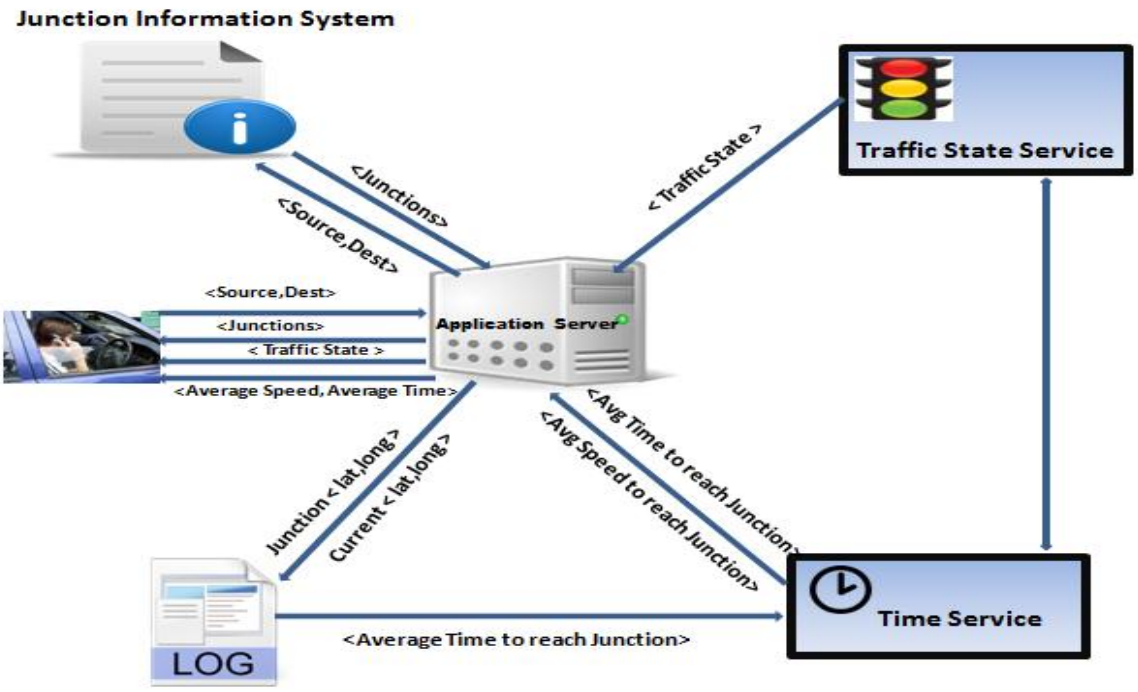


Figure 2: Framework/Architecture of Real Time Information System

Application is initiated once users starts journey by entering source and destination when there is a connection with the GPS service and the coordinates of the device are calculated, it notifies the communication thread to send updates to the server. This thread is running continuously on the background and calculates the location coordinates, Junction speed, Junction time of a user and constantly updates the server. In the meanwhile, the control thread is notified and a new map thread is initiated with focus on the mobile device's position. The map thread, using the Google Map API, is connected to a map server and presents the map of the area on the screen. The server application is listening on a specified port and is responsible for starting a serving thread for each connected client. Location updates and traffic updates are collected from all the clients, and the server sends back with Average speed, Average time to reach a junction to all the user on the same path. The log files with the client's tracks are stored on the server for further processing regarding the development of a traffic reconstruction algorithm As illustrated in Fig 1 and Fig 2 which explains the overall working of Wireless Sensor based Real Time Traffic Information System architecture. user gets traffic updates periodically before user reaches next junction in the path. For testing purposes, an application, which can emulate multiple clients by reading tracks location coordinates, calculating average speed, average time constantly and updating the same to all the users in the path this scenario is explained with snap shots in Implementation and Results section. The current implementation of secure communications between client and server is based on an already well tested protocol as SSL, ensuring the confidentiality of the communication and the proper authentication of the involved parties. For an application deployed at large scale, it has the drawback of having to issue a separate digital certificate for each user.

4. IMPLEMENTATION AND RESULTS

The core of the system is the mobile application running on the mobile devices. Application had been developed and implemented on android platform it uses Google Api for displaying maps. Application has two software threads

User Interface Functionality: Responsible for user interface the interaction with the user and control of the application.

Map and Traffic Functionality: Responsible for displaying map with traffic information based on the information sent from the server.

4.1 RESULTS

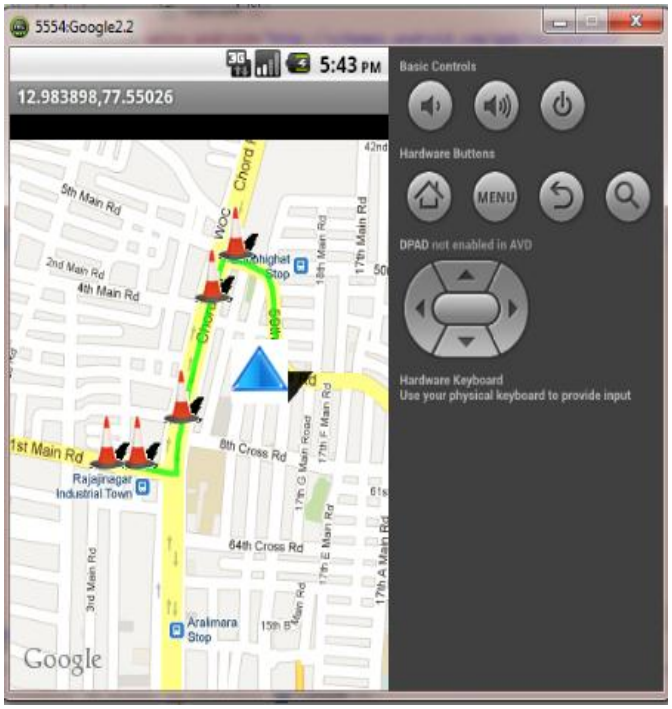


Figure 3:Illustrating junctions between source(Kormangala) and destination(Rajajinagar).

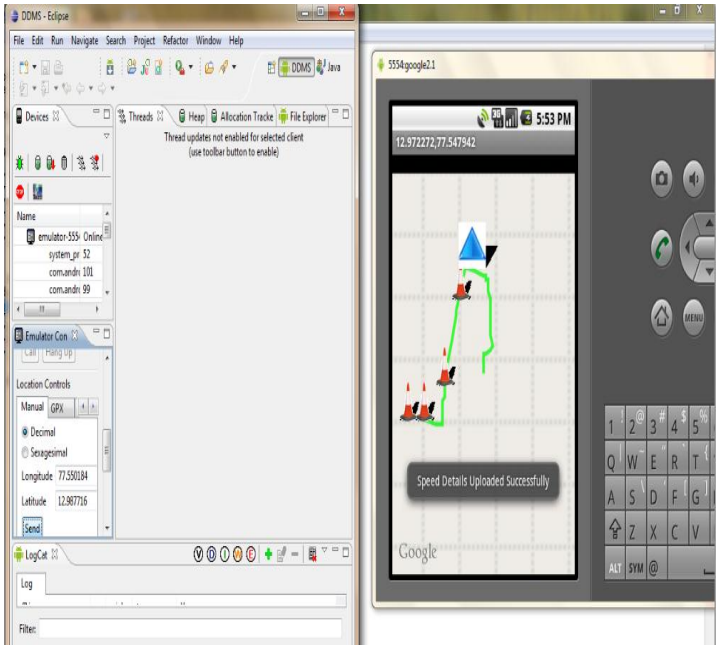


Figure 4: As user A moves to next junction his speed, time, location information is updated to server.

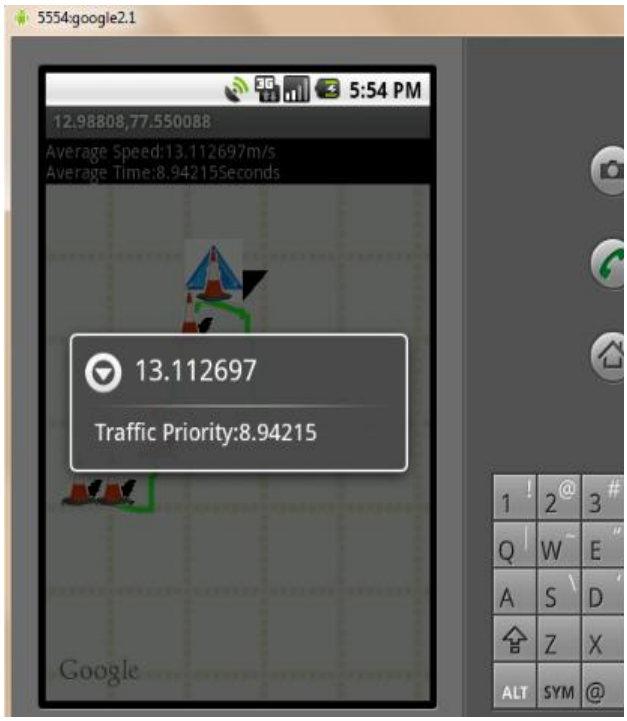


Figure 5: Illustrating Average speed and Average time (traffic priority).

Figure 6:Illustrating another user B as he moves to another junction he gets calculated Average speed and Average time from server based on the other user(A) who had travelled in that path.

5. CONCLUSION

This paper Presents Wireless sensor based Real time traffic Information System where mobile is used as sensor to capture traffic information which will overcome the existing Traffic Monitoring Techniques. This system will reduce Infrastructure cost and Monitoring cost of static deployed sensors in roads, because system WRTS uses mobile as sensors which will lead to building of Mobile wireless sensor network .This system is user friendly and easy to use. This system would be useful in reducing traffic jams.

6. ACKNOWLEDGMENT

I would like to acknowledge our college Siddaganga Institute of Technology, parents, I thank my advisor Asst Prof.G. Bhaskar for not only providing ideas and guidance but also for working along with me and being moral support for me.

7. REFERENCES

[1] Traffic Safety and City Public Transport System:

Case Study of Bengaluru, India P. S. Kharola, Geetam Tiwari, and Dinesh Mohan

[2] 3GPP TS 25.305, Stage 2 Functional Specification of UE Positioning, Dec. 2009.

[3] Intelligent Transport Systems for Indian Cities

Rijurekha Sen, Bhaskaran Raman

[4] http://www.mapofbangalore.com/maps/bangalore-road-map.html.

[5] M. El Najjar and P. Bonnifait, "A road-matching method for precise vehicle localization using belief theory and Kalman filtering", Autonomous Robots, vol. 19, 2005, pp. 173–191.

[6] Y. Wang and M. Papageorgiou, "Real-time freeway traffic state estimation based on extended Kalman filter: a general approach", Transportation Research Part B: Methodological, vol. 39, 2005, pp. 141-167.

[7] L. Mihaylova and R. Boel, "A particle filter for freeway traffic estimation", 43rd IEEE Conference on Decision and Control, 2004, pp. 2106-2111.

[8] S. Pramanik, "An efficient path computation model for hierarchically structured topographical road maps", IEEE Transactions on Knowledge and Data Engineering, vol. 14, 2002, pp. 1029–1046.

[09] GPS tracking unit Wikipedia The free encyclopedia available http://en.wikipedia.org/wiki/GPS_tracking_unit.

[10] Traffic congestion in Indian cities: Challenges of arising power Azeem Uddin Draft, 50th IEEE Conference on Decision and Control, 2004, pp. 2106-2111.

[11]TheMobileMillenniumProject.http://traffic.berkeley.edu/

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 487 - 491, 2013, ISSN: 2319–8656

Ensuring Security in Emergency through SMS Alert System

A.Sankari
Prist University
Thanjavur, India

K.Umasankar
Prist University
Thanjavur, India

Abstract: Short Message Services are increasingly being relied upon to disseminate critical information during emergencies. In recent days accident happens very common due to heavy traffic and increase in vehicle level and bad drivers, hence it requires a software to inform the service centre for instant help to save life of the people. Sending the nearest emergency service and/or police officers needed for reporting the accident can be quite tedious. The idea of this work is to reduce the time required by the emergency personnel to reach the accident area. This can be done if the information about an accident reaches the emergency services in time and accurately. The project eliminates any communication between the victim and the personnel which leads to confusion. This is done by finding the accurate position of the location by making use of the GPS services available in cell phones when the victim sends a message to the emergency number(such as 108). The project aims at reducing the severe loss due to injury and fatality rate in accidents to a great extent**.**

Keywords: GPS services, Short Message Services

1. INTRODUCTION

SMS allows individuals to transmit short, alphanumeric communications for a wide variety of applications. Whether to coordinate meetings, giving alert notification, offer reminders of an event or even vote for a contestant on a television game show, this discreet form of communication is now the dominant service offered by cellular networks. In fact, in the United States alone, over five billion text messages are delivered each month. While many of the applications of this service can be considered noncritical, the use of text messaging during emergency events has proven to be far more utilitarian. Premium-rated messages are also used in Donors Message Service to collect money for charities and foundations. DMS was first launched at April 1, 2004, and is very popular in the Czech Republic. For example, the Czech people sent over 1.5 million messages to help South Asia recover from the 2004 Indian Ocean Earthquake.

With millions of people attempting to contact friends and family on September 11th 2001, telecommunications providers witnessed tremendous spikes in cellular voice service usage. Verizon Wireless, for example, reported voice traffic rate increases of up to 100 percent above typical levels; Cingular Wireless recorded an increase of up to 1,000 percent on calls destined for the Washington D.C. area. While these networks are engineered to handle elevated amounts of traffic, the sheer number of calls was far greater than capacity for voice communications in the affected areas. However, with voice based phone services being almost entirely unavailable, SMS messages were still successfully received in even the most congested regions because the control channels responsible for their delivery remained available. Similar are the stories from the Gulf Coast during Hurricanes Katrina and Rita. With a large number of cellular towers damaged or disabled by the storms, text messaging allowed the lines of communication to remain open for many individuals in need, in spite of their inability to complete voice calls in areas where the equipment was not damaged and power was available.

2. PROPOSED SYSTEM

The proposed system requires the affected person to just send a message to the service center from their mobile. The message is sent through a software installed in mobile which doesn't require the user to type any text. Then the message will be received by the service center using GSM modem. The proposed system configuration is shown in Fig. 1. The latitude and longitude value of the place from which the message is sent is received in the server. The geo coding used in the server side now converts these values to precise location. The service center can now view the accident location on a map with the details about the nearest emergency services. Then they inform the type of the accident and appropriate location to the nearby service (police & fire). This will reduce the time required for the police and the emergency personnel to reach the accident location. The idea makes the location identification automatic. This helps in identifying the accident spot precisely and quickly. Hence it reduces the time required for the emergency services to reach the spot.

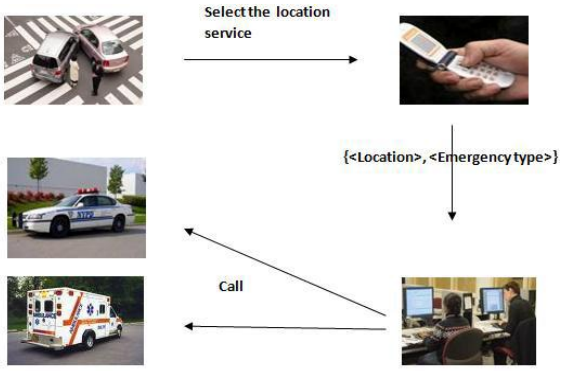


Fig 1 : Block diagram of proposed system

The technology used can be developed with the current equipment like GSM modem and Geo Code technique, and has the technical capacity to hold the data required by the new system.

1. This technology supports the modern trends of technology.
2. Easily accessible, more secure technologies.

Technical feasibility on the existing system and to what extend it can support the proposed addition. MVC and geo code is latest technique used by many smart phones now a days. We can add new modules easily without affecting the

Core Program. Most of parts are running in the server using the concept of stored procedures**.** Ensuring Security Intimations in emergency through SMS Alert
System implements and satisfied the technical feasibility level.

2.1 Operational Feasibility

This proposed system can easily implemented, as this is based on JSP coding (JAVA) & HTML .The database created is with MySql server which is more secure and easy to handle. The resources that are required to implement/install these are available. The personal of the organization already has enough exposure to computers. So the project is operationally feasible. It uses Mysql server for easy handling and GSM for better SMS receiving rates. It is easy to operate by non-technical users also.

2.2 Economical Feasibility

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system. More commonly known cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. If benefits outweigh costs, then the decision is made to design and implement the system. An entrepreneur must accurately weigh the cost versus benefits before taking an action. This system is more economically feasible which assess the brain capacity with quick & online test. So it is economically a good project. This emergency alert project used open source software for development so it is freely available and free of cost. And today most users have android mobile phones. There is no extra hardware cost for all. The advantages of the proposed system are

1. It eliminates any conversation between the victim and the service center. Hence it reduces any confusion and possibility of wrong information.
2. Software requirement is very less, hence it can be implemented easily. It does not require any specialized hardware to be installed.
3. There is no need of regular update. Even if there is any update it can be downloaded easily and does not require any cost.
4. Even the affected person can inform about the accident using the proposed system. Since it does not require typing any text or making a call it becomes simple for the victim.
5. Since messages can be sent even with low signals, it reduces any technical problem. Messages can be sent from places where making calls is not possible. Hence possibility of message reaching the service center is higher when compared to calls.
6. It is cheaper to use.

3. CELLULAR NETWORK ARCHITECTURE

In this section, we provide a technical overview of message delivery to understand how such cellular networks deliver text messages and a high-level description of how third-party vendors try to use these systems to deliver alert messages during emergency. We specifically examine GSM networks [3] in these discussions as they represent the most widely deployed cellular technology in the world; however, it should be noted that message delivery for other technologies such as CDMA, IDEN, and TDMA are very similar and are therefore subject to similar problems.

3.1 Sending a Message

There are a number of ways in which text messages can be injected into a GSM or CDMA network. While most users are only familiar with sending a text message from their phone, known as Mobile Originated SMS (MO-SMS), service providers offer an expanding set of interfaces through which messages can be sent. From the Internet, for instance, it is possible to send text messages to mobile devices through a number of webpages, e-mail, and even instant messaging software. Third parties can also access the network using so-called SMS Aggregators. These servers, which can be connected directly to the phone network or communicate via the Internet, are typically used to send "bulk" or large quantities of text messages. Aggregators typically inject messages on behalf of other companies and charge their clients for the service. Finally, most providers have established relationships between each other to allow for messages sent from one network to be delivered in the other. Fig. 2 shows these three high-level strategies. After entering a provider's network, messages are sent to the Short Messaging Service Center (SMSC). SMSCs perform operations similar to e-mail handling servers in the Internet, and store and forward messages to their appropriate destinations. Because messages can be injected into the network from so many external sources, SMSCs typically perform aggressive spam filtering on all incoming messages. All messages passing this filtering are then converted and copied into the necessary SMS message format and encoding and then placed into a queue to be forwarded to their final destination.

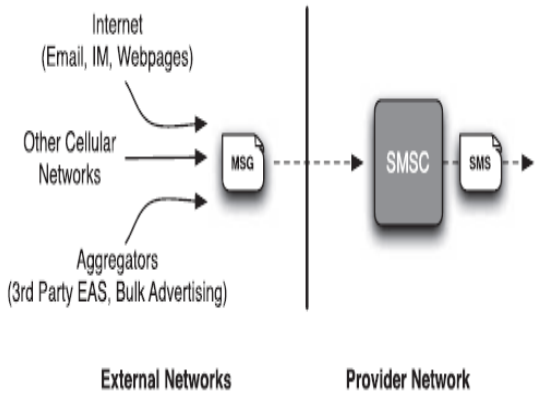


Fig. 2 : Processing of Text message

3.2 Finding a Device

Delivering messages in a cellular network is a much greater challenge than in the traditional Internet. Chief in this difficulty is that users in a cellular network tend to be mobile,

so it is not possible to assume that users will be located where we last found them. Moreover, the information about a user's specific location is typically limited. For instance, if a mobile device is not currently exchanging messages with a base station, the network may only know a client's location at a very coarse level (i.e., the mobile device may be known to be in a specific city, but no finer grained location information would be known). Accordingly, the SMSC needs to first find the general location for a message's intended client before anything else can be done.

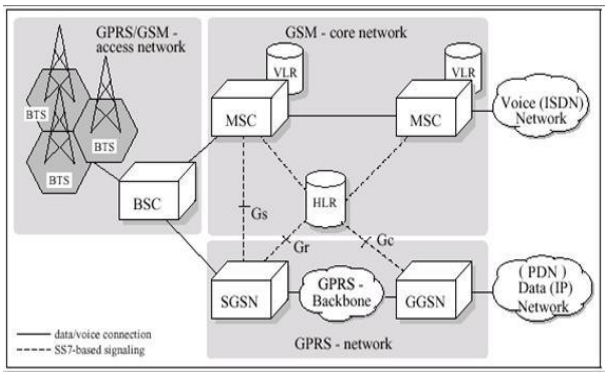


Fig. 3 : Network Architecture

A server known as the Home Location Register (HLR) assists in this task. This database acts as the permanent repository for a user's account information (i.e., subscribed services, call forwarding information, etc.). When a request to locate a user is received, the HLR determines whether or not that device is currently turned on. If a mobile device is currently powered off, the HLR instructs the SMSC to store the text message and attempt to deliver it at another time. Otherwise, the HLR tells the SMSC the address of the Mobile Switching Center (MSC) currently serving the desired device. Having received this location information, the SMSC then forwards the text message on to the appropriate MSC.

3.3 Wireless Delivery

As mentioned earlier, even the MSC may not know more information about a targeted device's location. In order to determine whether or not the current base station serving this device is known, the MSC queries the Visitor Location Register (VLR), which temporarily stores information about clients while they are being served by the MSC. In most cases, this information is not known, and so the MSC must begin the extensive and expensive process of locating the mobile device. The MSC completes this task by generating and forwarding paging requests to all of its associated base stations, which may number in the hundreds. This process is identical to locate a mobile device for delivery of a voice call. Upon receiving a paging request from the MSC, a base station attempts to determine whether or not the targeted device is nearby. To achieve this, the base station attempts to use a series of Control Channels to establish a connection with the user. First, the base station broadcasts a paging request over the Paging Channel (PCH) and then waits for a response. If the device is nearby and hears this request, it responds to the base station via the Random Access Channel (RACH) to alert the network of its readiness to receive information. When this response is received, the network uses the Access Grant Channel (AGCH) to tell the device to listen to a specific Standalone Dedicated Control Channel (SDCCH) for further exchanges. Using this SDCCH, the network is able to authenticate the client, perform a number of maintenance routines and deliver the text message. By limiting the operations necessary to deliver a text message to the control channels used for call setup, such messages can be delivered when all call circuits, known as Traffic Channels (TCHs) are busy. When the attempt to deliver the message between the targeted device and the base station is complete, the device either confirms the success or failure of delivery. This status information is carried back through the network to the SMSC. If the message was successfully delivered, the SMSC deletes it. Otherwise, the SMSC stores the message until a later period, at which time the network reattempts delivery. Fig. 2 offers an overview of this entire process.

3.4 Third-Party Provider Solutions

In the past few years, a significant number of third-parties offering to deliver alert messages (and other information services) via text messaging services. The architecture of these systems is relatively simple. Whether activated through a web interface, directly from a phone, or as software running on a campus administrator's computer, these services act as SMS aggregators and inject text messages into the network. In the event of an emergency message is sent to the service center from the victim or passerby mobile

3.5 Short Message Service

Short Message Service (SMS) is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. SMS text messaging is the most widely used data application in the world, with 3.6 billion active users, or 78% of all mobile phone subscribers. The term SMS is used as a synonym for all types of short text messaging as well as the user activity itself in many parts of the world. SMS is also being used as a form of direct marketing known as SMS marketing. Simple user generated text message services - include news, sport, financial, language and location based services, as well as many early examples of mobile commerce such as stocks and share prices, mobile banking facilities and leisure booking services. SMS as used on modern handsets originated from radio telegraphy in radio memo pagers using standardized phone protocols and later defined as part of the Global System for Mobile Communications (GSM) series of standards in 1985[] as a means of sending messages of up to 160 characters, to and from GSM mobile handsets. Since then, support for the service has expanded to include other mobile technologies such as ANSI CDMA networks and Digital AMPS, as well as satellite and Landline networks. Most SMS messages are mobile-to-mobile text messages though the standard supports other types of broadcast messaging as well.

3.6 GSM Technology

GSM is a cellular network, which means that cellphones connect to it by searching for cells in the immediate vicinity. There are 5 different cell sizes in a GSM network. The coverage area of each cell varies according to the implementation environment. Indoor coverage is also supported by GSM. GSM uses several cryptographic algorithms for security. A convenient facility of the GSM network is the short message service.

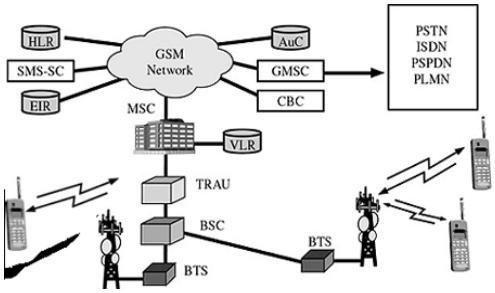


Fig. 4 : GSM Network along with SMSC

The Short Message Service – Point to Point (SMS-PP) was originally defined in GSM recommendation 03.40, which is now maintained in 3GPP as TS 23.040. GSM 03.41 (now 3GPP TS 23.041) defines the Short Message Service – Cell Broadcast (SMS-CB), which allows messages (advertising, public information, etc.) to be broadcast to all mobile users in a specified geographical area. Messages are sent to a Short message service center (SMSC) which provides a "store and forward" mechanism. It attempts to send messages to the SMSC's recipients. If the subscriber's mobile unit is powered off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile is powered on or has reentered the coverage area of the network. This function ensures that the message will be received.
Both mobile terminated (MT, for messages sent to a mobile handset) and mobile originating (MO, for those sent from the mobile handset) operations are supported. In Message delivery, delay or complete loss of a message is uncommon, typically affecting less than 5% of messages.

3.7 Data Base System

Database is required to store the information received through the message using GSM modem. The information can be then taken for further processing. The data stored in the database are the mobile number, the type of accident, the latitude value, the longitude value, the date and the time when the message was sent. First a connection between the server and the database is established using JDBC. Then the transfer of data takes place.

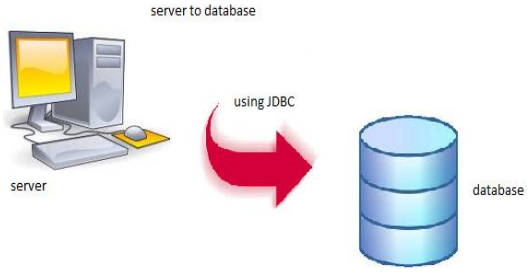


Fig. 5. Database Transfer system

JDBC allows multiple implementations to exist and be used by the same application. The API provides a mechanism for dynamically loading the correct Java packages and registering them with the JDBC Driver Manager. The Driver Manager is used as a connection factory for creating JDBC connections.

JDBC connections support creating and executing statements. Additionally, stored procedures may be invoked through a JDBC connection. It finds the exact location of the accident. The server then retrieves the contact details of the nearest emergency services from the databases and then inform them about the accident and its location.

4. TESTING RESULTS

This proposed system is tested from various mobile and different places by sending SMS to a designated emergency number. The screenshots of the results are furnished below.

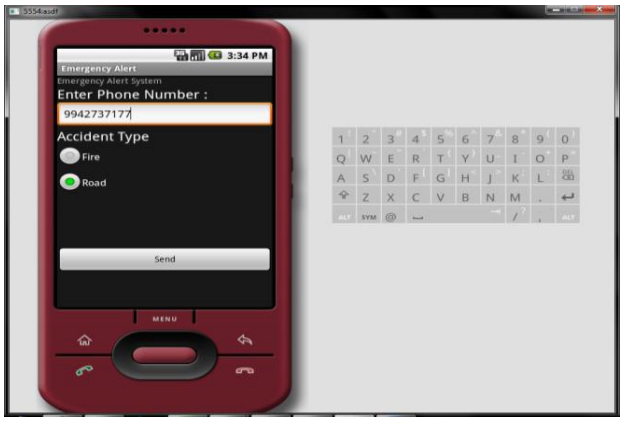


Fig. 6 : Software installed in Mobile phone for sending message

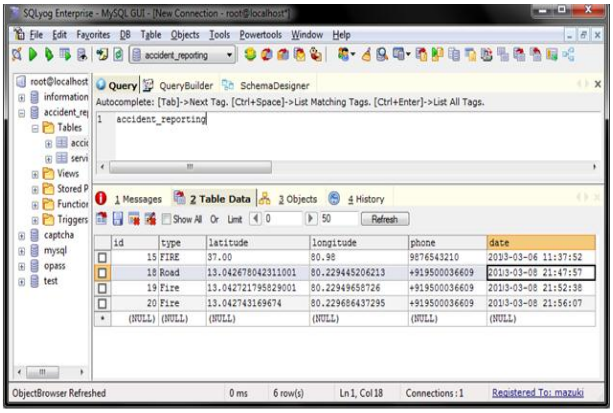


Fig. 7 : Details Stored in Database

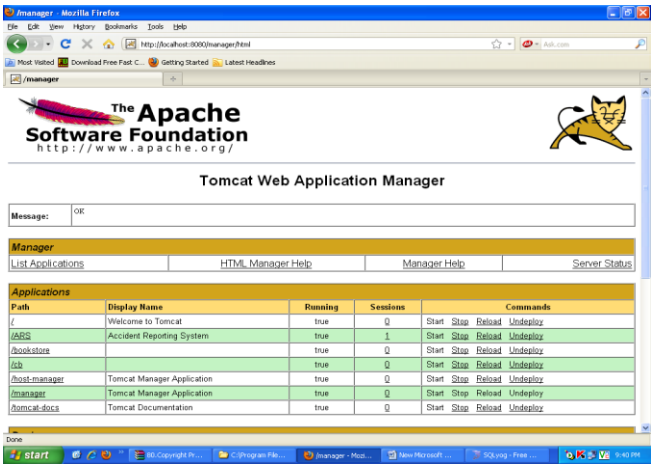


Fig. 8 : Running Apache server

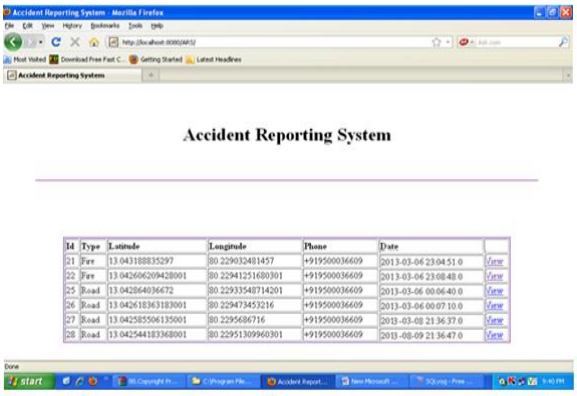


Fig. 9 : Precise location using geocoding technique

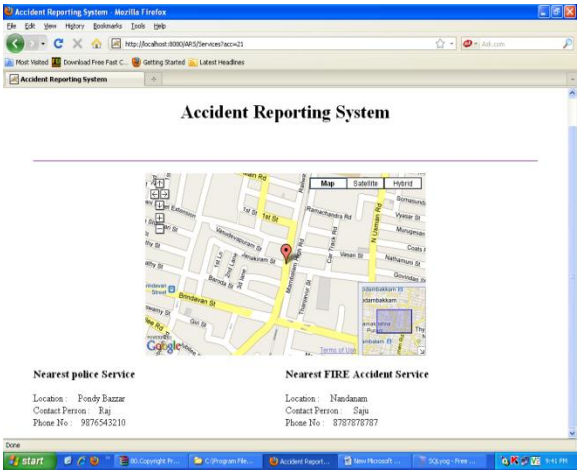


Fig. 10 : Viewing location in the map

5. CONCLUSION

The proposed SMS alert system is aimed to reduce the time required by the rescue team to reach the accident area. The message is sent through a software installed in mobile. Even the affected person can inform about the accident using the proposed system. It uses GPS to send the latitude and longtitude value of a place from which the messages is sent. The server receives the message using GSM Modem and uses reverse geocoding to convert latitude and longtitude value to exact location where the accident took place. The acknowledgement is sent from the service centre to the victim which reduces the panic in the person. There is neither any maintenance nor any service required for this system. Since messages can be sent even with low signals, it reduces any technical problem.

6. REFERECES

[1] Daniel Adkins, Karthik Lakshminarayanan, Adrian Perrig, and Ion Stoica. Taming IP packet flooding attacks. In Proceedings of Workshop on Hot Topics in Networks (HotNets-II), November 2003

[2] Patrick Traynor, "Characterizing the Security implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services" , IEEE / Trans. on Mobile Computing, vol. 11, no. 6, June 2012

[3] "Technical Realization of the Short Message Service (SMS),"Technical Report 3GPP TS 03.40 v7.5.0. 3rd Generation Partner-ship Project, 2002.

[4] "Analysis of the Short Message Service (SMS) and Cell Broadcast Service (CBS) for Emergency Messaging Applications; Emergency Messaging; SMS and CBS," Technical Report ETSI TR 102 444 V1.1.1. European Telecomm. Standards Inst., 2006.

[5] P. Bosch, L. Samuel, S. Mullender, P. Polakos, G. Rittenhouse, G., "Flat Cellular (UMTS) Networks," Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE

[6] R. Doverspike and A. Gerber, "Traffic Types and Growth in Backbone Networks," in Proc. of OFC/NFOEC, Invited Paper, 2011

[7] Jochen Schiller, Mobile Communications, II Edition, Addison Wesley

[8] Lu, W., Giordano, S. (2001) 'Challenges in Mobile Ad Hoc Networking,' collection of articles, IEEE Communications Magazine, 39(6).

[9] Campbell, A., Gomez, J., Kim, S., Valko, A., Wan, C.-Y., Turanyi, Z. (2000) 'Design, implementation and evaluation of Cellular IP,' IEEE Personal Communications, 7(4).

[10] Location management in cellular networks. In I. Stojmenovic (Ed.), Handbook of wireless networks and mobile computing (pp. 24–49). New York: John Wiley & Sons.

[11] Lin, Y.-D., & Hsu, Y.-C. (2000). Multihop cellular: A new architecture for wireless communications. Proceedings of IEEE INFOCOM.

[12] T.S.Ueng, Z.D.Tsai, J.C.Chang (2007) "SMS alert system AT NSRRC",Taiwan. Proceedings of PAC07, New Mexico, USA.

[13] Nilesh Agarwal, Leena Chandran-Wadia, Varsha Apte "Capacity Analysis of the GSM Short Message Service" Indian Institute of Technology Bombay.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 492 - 494, 2013, ISSN: 2319–8656

Effective Implementation of Green Computing Using RTI Data

Navdeep Kaur
Guru Kashi University,
Talwandi Sabo, Punjab, India

Pardeep Mittal
Guru Kashi University,
Talwandi Sabo, Punjab, India

Abstract: Today in the era of computerization the use of computers has various pros and cons. Computer saves our time and efforts to do a work but it also harmful to our health and environment. Today most of the CO_2 emission is caused because of use of computer and its devices. To reduce the harmful impacts of use of computer the concept of green computing must be implemented. Green computing is an approach to use, manufacture and disposed of a computing device with no or minimal impacts on our environment. The concept of green computing would be implemented if both the user and the manufacturer of the computer are taking initiatives. In this research paper we represent the data collected under RTI Act 2005 from various organizations about their efforts for the implementation of green computing. This data will be useful to represent the awareness of these organizations about green computing and what efforts they are taking for the implementation of green computing. This data is also a part of my research work.

Keywords: Energy Star, TCO certification, ICT, eco-friendly, Recyclability.

1. INTRODUCTION

Green computing is refers to initiatives to use technology in more environmentally friendly way. The growing green computing movement includes initiative within companies to use power more efficiently, reduce waste, and create more eco-friendly computing products. Many IT manufacturers and vendors are continuously investing in designing every efficient computing device, reducing the use of dangerous materials and encouraging the recyclability of digital devices. The concept Green computing is come into existence in 1992 when the U.S environmental protection agency launched energy star, energy star is voluntary labeling and recognize energy efficiency in monitors, climate control equipment and other technologies. The goal of green computing are power management and energy efficiency choice of eco-friendly hardware and efficient software and material recycling and increasing the product's life. With the help of ICT (Information and Communication Technology), Green computing become an effective approach to grow segments that affects carbon emission. To successful implementation of green computing various organizations and manufacturers have to take initiatives. In this research paper we take a little effort to represent the efforts of some organizations for the implementation of green computing.

2. OBJECTIVES OF MY STUDY

The main objectives of my research are:

1. To aware the common man about term green computing.
2. To reduce energy consumption & protect the environment.
3. To find the difficulties occur in implementation of green computing.
4. To aware the common man about the efforts need to done by them for green computing.
5. To aware the common man about the organizations who take initiatives to promote green computing.
6. To make the people aware about the role of government to promote green computing.

3. RESEARCH METHODOLOGY

For implementation of green computing we have to go through various issues and challenges occur in implementation of green computing. After a thorough study of these issues and challenges we choose various factor variables. We found that higher authorities also play a vital role for the implementation of green computing. We use RTI Act 2005 to collect the data from various government institutions about the efforts done for implementation of green computing. We prepare results from their responses.

4. RTI QUESTIONS

Q1. Please tell me the total no. of computing devices in your organization?

Q2. Please tell me the count of devices processor category wise (like Intel PIV, i3, i5, i7, celeron, AMD based) in your organization? Please use tabular form if possible.

Q3. Please tell me no. of computing device in your organization with energy star logo?

Q4. Please tell me no. of computing devices in your organization based on operating systems (like Linux, windows, DOS, UNIX etc.)

Q5. Please tell me the no.of conferences/Seminars/workshops conducted by your organization related to green computing for staff or students? Please mention their topics, dates also.

Q6. Please tell me the no. of CRT, LCD, LED monitors currently used by your organization?

Q7. Please tell me how many computing devices are disposed by you in last 5 years (from 1 April, 2009 to 31 March, 2013)? Please use tabular form if possible.

Q8. Please tell me which method of disposing of computing devices was adopted by your organization?

Q9. Please tell me about your organization's initiatives for green computing in last 5 years (from 1 April, 2009 to 31 March, 2013)?

Q10. Please tell me no. of computing device in your organization with TCO certification?

Q11. Please tell me that is there any campaign done by your organization in last three years to aware about green computing.

5. RTI DATA

Q. no.	DICT/CIET NCERT	IIT Ropar	CIET/P&RD/ NCERT	Punjab InfoTech	CIET/P&C
1	Monitors-97	522	Monitors-29	Desktop-95	Monitors-89
	Keyboards-97		Keyboards- 29	Laptop-46	Keyboards-89
	Mouse- 97		Mouse- 29		Mouse-89
	Machine- 97		Machine-29		Machine-89
	UPS – 97		UPS-27		UPS-92
	Printers-73		Printers-6		Printers-67
2	9 Computers Intel i5	All systems of i3,i5,i7	N/a	52 Desktop AMD	N/a
	5 Computers Intel Core			Rest varies from P3 to i5	
	4 Computers Intel Pentium D Inside				
	7 Computers Intel Core 2				
3	Nil	Nil	Nil	52 Desktop AMD Energy Star 5 rest are old	N/a
4	10 Linux	Linux 90, Windows 432	N/a	Apple 01, Rest Windows	N/a
	87 Windows 7				
	All 97 computer have DOS, UNIX				
5	Nil	Nil	N/a	NIL	n/a
6	20 LCD, 28 CRT, 15 LED	All LCD and LED	N/a	ALL LCD's	n/a
7	Nil	Nil	N/a	39 auctioned	n/a
8	Nil	Nil	N/a	open Auction	n/a
9	Nil	Nil	N/a	NA	n/a
10	Nil	Nil	N/a	52 Desktop of certified as DMI 2.0, FCC, UL, RoHS Compliance	n/a
11	Nil	Nil	N/a	Nil	n/a

6. RTI REPORT

1. DICT/CIET NCERT is using 558 computing devices from which 97 has CPU. Only 9 computers are Intel i5 whereas others are based on Intel Core, Pentium D etc. No computing device has energy star logo. Only 10 computers are based on Linux operating system others are based on Windows. No conferences or seminar is conducted based on Green computing. It use 20 LCDs, 15 LEDs and others are CRT Monitors. In last 5 years no computer is disposed of. It does not take any initiative towards Green Computing in last 5 years. No computer is certified with TCO certification and No campaign is organized in last three years for Green Computing.
2. IIT Ropar is using 522 computers and all the computers are based Intel family 2 processors i.e. i3, i5 and i7. No computing device has energy star logo. 90 computers are based on Linux OS and 432 are based on windows OS. No conferences or seminar is conducted based on Green computing. It use all LCD and LEDs monitors. In last 5 years no computer is disposed of. It does not take any initiative towards Green Computing in last 5 years. No computer is certified with TCO certification and No campaign is organized in last three years for Green Computing.

3. CIET/P&RD/NCERT 149 computing devices in which 29 CPUs. No other information is provided by P&RD department.
4. Punjab InfoTech use 95 Desktops and 46 Laptops. 52 Desktops are based on AMD and others are varies from p3 to i5. It has 52 desktops with Energy Star. No conferences or seminar is conducted based on Green computing. It use all LCD monitors. In last 5 years 39 computers are disposed of. The method used for disposing is open auction. It does not take any initiative towards Green Computing in last 5 years. 52 computers are certified with TCO certification and No campaign is organized in last three years for Green Computing.
5. CIET/P&C use 515 computing devices in which 89 are CPUs. No other information is provided by the universities.

7. CONCLUSION

The data collected from various organizations it is stated that every organization know about the differences of LCD/LED and CRT monitors but still they are using CRT monitors. Most of the respondent organizations have not using computers with energy star logo. No organization takes any initiative to implement green computing. No seminar and campaign is organized by any organization to promote green computing. No organization is using TCO certified products. The above data states that these organizations have not taking much useful efforts for green computing. They have to take serious efforts for implementation of green computing and to save our environment from the harmful impacts of use of computer and its devices.

8. REFERENCES:

[1] Active Energy Manager (AEM): +http://www-03.ibm.com/systems/software/director/aem/

[2]Power and Performance trade-off: http://spscicomp.org/wordpress/wpcontent/uploads/2011/05/brochard-Luigi_Perf-and PowerTrade-off.pdf

[3] Energy aware scheduling: http://domino.research.ibm.com/library/cyberdig.nsf/papers/C1C7497C25DBD116852573D400531DFD/$File/rc24463.pdf

[4]S Ruth. Green IT More Than a Three Percent Solution? IEEE Internet Computing, 2009.

[5]Alexander Szalay, Gordon Bell, H Huang, Andreas Terzis, and Alainna White. Low-power amdahl-balanced blades for data intensive Computing

[6] http://www.wikipedia.org/

[7]http://www.educause.edu/southwest-regional-conference/2010/implementing-green-computing-can-save-you-some-green

[8] http://www.greencomputing.co.in/

[9] Google green computing report

[10] http://energystar.gov/

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 495 - 498, 2013, ISSN: 2319–8656

Blur Detection Methods for Digital Images-A Survey

Rupali Yashwant Landge
Department of Computer Science and Engineering
Rajasthan college of Engineering for women, Jaipur

Rakesh Sharma
Department of Computer Science and Engineering
Rajasthan college of Engineering for women, Jaipur

Abstract: This paper described various blur detection methods along with proposed method. Digital photos are massively produced while digital cameras are becoming popular; however, not every photo has good quality. Blur is one of the conventional image quality degradation which is caused by various factors like limited contrast; inappropriate exposure time and improper device handling indeed, blurry images make up a significant percentage of anyone's picture collections. Consequently, an efficient tool to detect blurry images and label or separate them for automatic deletion in order to preserve storage capacity and the quality of image collections is needed. There are various methods to detect the blur from the blurry images some of which requires transforms like DCT or Wavelet and some doesn't require transform.

Keywords: Blur, DCT, DWT, SIFT, Wavelet.

1. INTRODUCTION

Advances in computational photography over the last decade have laid the foundations for the mass production of powerful low-cost digital cameras. This technology is indeed helping conventional users to generate high-quality content with inexpensive and bulky professional cameras. The Latest generation offers cameras with, auto-focusing and motion compensation functions. The aim of such functions is to improve picture quality by automatically post-processing and enhancing the quality of images captured with low-quality, low-price sensors and lenses. High-quality lenses and sensors are not only expensive but bulky and thus inappropriate for integration in small cameras and other devices such as mobile handsets. Computational photography offers highly efficient tools that can greatly improve the quality of pictures captured with low-quality lenses and sensors at very low cost.This approach offers a very appealing alternative to image capturing with high-quality lenses. Unfortunately, not all the shortcomings of low-cost digital cameras can be yet compensated by software post-processing. Indeed, simple factors such as limited light conditions, inappropriate exposure time and improper device handling can lead to unsatisfactory image quality. As a consequence, the search for better image enhancement and selection tools in the field of computational photography goes on.

Nowadays, high-quality digital cameras gain increasing attention as digital technology advances. Users can take hundreds of pictures a day. However, it is not easy for them to look through all their pictures to decide which of them can be deleted (for example, if the storage is full), or which of them should be taken for an enhancement process. Thus, they need some techniques of image quality estimation for telling the blurry images from the sharp ones. Imperfect focusing and/or motion is the main source of blurriness in digital photographs. Clearly, blurry images make up a significant percentage of anyone's picture collections captured with conventional digital cameras in usual conditions. As a consequence, a tool to automatically detect blurry images is urgently needed. The reason is twofold. On the one hand, blurry images can be labeled automatically and separated from good-quality images in conventional collections for browsing, viewing and later re-use. On the other hand, the same functionality can be used for automatic deletion in order to preserve storage capacity in the flash memory of a digital camera. The latter feature will enable users to virtually increase the storage capacity of their cameras by retaining only those pictures with perceptively good quality [1]. There are already some existing methods for blur detection or image quality estimation for digital images. However, most of them are time-consuming, computation intensive, need different kinds of transformations (e.g. DCT or DWT) or the detection ratio is not very high .Also there is one proposed algorithm for automatic real time detection of blurry images The algorithm is based on computing variance values of the local key points that are extracted from the given images through implementing Scale Invariant Feature Transform (SIFT) algorithm in a scale space. No transforms (DCT or DWT) are required to be applied to the images, and no edge locations need to be identified in the proposed method, which are the main techniques used in most of the existing methods. Only pixel values of the given images are directly employed in the algorithm [2]. The main objective is to automatically detect blurry images for automatic labeling and potential removal. The targeted application is low-cost digital cameras for conventional users. The presented approach is generic in the sense that it does not make assumptions on the cause of blurriness.

2. EXISTING BLUR DETECTION TECHNIQUES

Following are the existing blur detection techniques.

2.1 Blur Detection for Digital Images Using Wavelet Transform:

Blur detection scheme using Harr wavelet transform is a direct methods. It can not only judge whether or not a given image is blurred, which is based on edge type analysis, but also determine to what extent the given image is blurred, which is based on edge sharpness analysis[3]. The scheme takes advantage of the ability of Harr wavelet transform in both discriminating different types of edges and recovering sharpness from the blurred version. It is effective for both Out-of-focus blur and Linear-motion blur. Its effectiveness will not be affected by the uniform background in images.

Different edges are generally classified into three types: namely, Dirac-Structure, Step-Structure and Roof-Structure .Step-Structure is further classify into Astep-Structure and Gstep- Structure according to whether the change of intensity is gradual or not. for Gstep- Structure and Roof-Structure edge, there is a parameter a $(0 < a < n/2)$ indicating the sharpness of the edge: the larger a is, the sharper the edge is. The basic idea of the scheme is : In general, most natural images contain all types of edges more or less, and most Gstep-Structure and Roof- Structure are sharp enough. When blur occurs, no matter whether it is caused by Out-of-focus or Linear motion, both Dirac-Structure and Astep-Structure will disappear. What is more, both Gstep Structure and Roof-Structure tend to lose their sharpness.

The scheme judges whether a given image is blurred according to whether it has Dirac-Structure or Astep-Structure, and uses the percentage of Gstep-Structure and Roof-Structure which are more likely to be in a blurred image to determine the blur extent. The whole structure of the scheme is shown in Fig. 1.

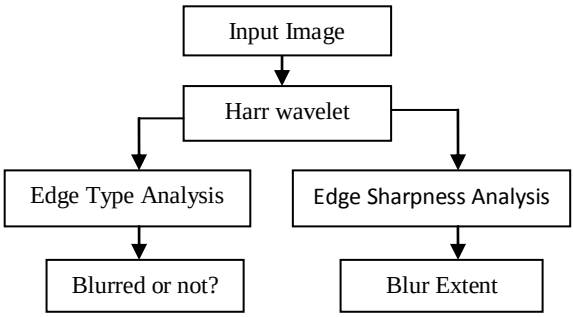


Fig.1 Structure of the HWT blur detection scheme

2.2 Blur Detection for Digital Images Using DCT:

Blur detection for DCT uses a new solution to aim at exploiting the available DCT information in MPEG or JPEG compressed video or images while involving a minimal computational load , the technique is based on histograms of non-zero DCT occurrences, computed directly from MPEG or JPEG compressed images. For MPEG compressed video, the scheme is suitable for all types of pictures: I-frames, P-frames or B-frames.

The objective of blur detection in this application is to provide a percentage indicating the global image quality in terms of blur: 0% would mean that the frame is totally blurred while 100% would mean that no blur at all is present in that particular frame. This blur indicator characterizes the global image blur caused by camera motion or out of focus. Since we focus analyzing MPEG compressed video data, it is desirable that the blur indicator can be directly derived from the DCT layer of an MPEG video bit stream. To achieve this objective, one should be aware that:

a) The DCT coefficients used within MPEG are intended for compression and are deeply related to the image content. Basically, they reflect the frequency distribution of an image block.

b) In a MPEG stream, DCT coefficients are directly applied on the pixels of I-frames. On the contrary, coefficients of P- and B-frames describe the residual image that remains after motion compensation [4].

It is therefore important to select a blur indicator which is as independent as possible from the particular content of an image as well as from the type of MPEG frames (I, P or B).

Blur is the opposite of edge sharpness. DCT coefficients render this sharpness via the high values of some AC coefficients. In this method blur measure therefore looks for the absence of such edges into the image, which is considered to prove a blurred image. Following three steps lead to the final measure:

Step 1. In order to characterize the global blur, it is proposed to establish a measure that takes into account the DCT information of the entire image as a whole. It is likely that any type of edge will cross some 8 x 8 blocks at least once in the image. Globalization among all DCT blocks would therefore enable to have an idea about the general edge sharpness, i.e. the global (camera or motion) blur.

Step 2. In order to be as independent as possible of the content of the image, coefficients should not be considered directly since their values are closely related to the type of image they depict. One rather proposes to look at the distribution of null coefficients instead of the values themselves: blurred images are likely to have all of their high frequency coefficients set to zero, whatever their content is.

Step 3. In order to remove the dependency to the image size, the number of blocks in the image should divide the number of times a coefficient is not zero. This would limit histogram values to 1. However, coefficients are often zeros in P- and B-frames. In order to homogenize the look of the histogram for all types of pictures, the number of non-zero occurrences of a coefficient is divided by the number of non-zero occurrences of the DC coefficient.

With these three steps, a measure (histogram) is obtained which is independent of both the image content and the type of MPEG frames.

2.3 Simple method for blur detection without using transform:

As a pre-processing, only converting the input images from RGB colours to grey-level luminance values is needed for the tool described below.

Following are the steps for above method

1) Input image array as IMn
2) Check if array is two dimensional or not, if not convert it
3) Calculate global invariance value S2p for different sample values
4) S2 p1 is sample variance value of the pre-image and S2 p2 is sample variance value of the taken image,
5) if image is first one only i.e. if n=1 and S2 p1 = S2p, Go for the next image
6) If not then calculate ratio R of sample variance values of pre-image and taken image.
7) If R=1 or R< 1 then image is blur, if want to delete then delete it
8) If not then image is not blur.

3. PROPOSED METHOD

In order to evaluate images, first calculate variance values of the local key points in consecutive images and then to evaluate the differences of these variances. For this reason SIFT operator had been chosen to detect the objects and find their special features. Moreover, after obtaining the locations of image local key points, select only fixed amount of samples for further calculations. This helps to speed up the process of image evaluation.

In order to estimate images, first apply only one part of the SIFT algorithm, that is, detecting local key points of the images objects. Then, generate additional images from the given one through the linear diffusion process. And finally, analyse the variance values calculated for the local key points of the original and its filtered images generated in the scale space. The variance value is calculate using formula given below:

$$W = \sum_{i=1}^{n-1} \frac{|(var(i) - var(i+1)|}{max\,|(var(i) - var(i+1)|)} \qquad i \in [1, n-1]$$

The algorithm for proposed method is described as follows:

1) input image;
2) apply SIFT to obtain key points of the image;
3) randomly select a certain amount of the key points from the given image and fixed location;
4) apply scale-space low-pass Gaussian filtering to the original image;
5) take the key points in the filtered images from the same locations fixed previously in the original image;
6) calculate variances for the taken key points in the original and filtered images and build the plot of it;
7) Analyze the curvature given in the plot.

The SIFT operator provides the number of key points found in the image and their position information. The number of key points varies from several hundreds to even hundreds of thousands per one image depending on the quality and structure of the image.

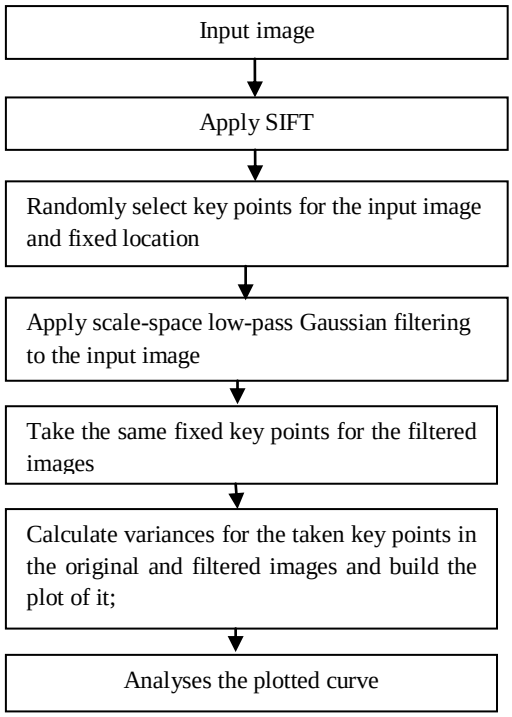


Fig 2.flowchart of proposed algorithm

4. CONCLUSION

The Harr wavelet scheme judges whether or not an image is blurred according to whether or not it contains any Dirac-Structure or Astep-Structure. Blur extent is characterized by blur confident coefficient based on the percentage of Gstep-Structure and Roof-Structure which are more likely to be in a blurred image. The scheme is effective and efficient. The DCT technique is directly applicable in the JPEG or MPEG compressed image without decompression. The method is effective for any type of images (I-, P- or B-

frames). The blur detection approach without using transform is simple, highly efficient and very accurate and fast than the other two i.e. using DCT and Harr wavelet transform. It is suitable for fully automated and real-time applications. The algorithm proposed in this paper is applicable for real digital cameras. No additional 'pre-images' are required in the method. Only taken pictures should be processed in the camera.

5. REFERENCES

[1] E. Tsomko H.J. Kim, E. Izquierdo "Linear Gaussian blur evolution for detection of blurry images" IET image process.,2010 Vol. 4,ISS.4pp.302-312

[2] Prasad D.Pulekar "Blur Detection in Digital Images-A Survey.

[3] Tong H., Mingjing L., Hongjiang Z., Changshui Z.:'Blur detection for digital images using wavelet transform'. IEEE Int. Conf. on Multimedia and Expo (ICME), 2004, pp. 17–20.

[4] X. Marichal, W. Y Ma, and H. J. Zhang, "Blur determination in the compressed domain using DCT information,"Proceedings of the IEEE International Conference on Image Processing, pp 386-390, 1999.

[5] LOWE D.G.: 'Distinctive image features from scale invariant keypoints', Int. J. Comput. Vis., 2004, 60, pp. 91–110

[6] VEDALDI A. 'An open implementation of SIFT detector and descriptor'. UCLA CSD Technical Report, 070012, 2006

[7] ZHANG Q., CHEN Y., ZHANG Y., XU Y.: 'SIFT implementation and optimization for multi-core systems'. IEEE Int. Symp. on Parallel and Distributed Processing, 2008, pp. 1–8

[8] LIU R., LI Z., JIA J.: 'Image partial blur detection and classification'. Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2008, pp. 1–8.

[9] BOULT B.E., CHIANG M.C.: 'Local blur estimation and super- resolution'. Proc. IEEE Conf. Computer Vision and Pattern Recognition, 1997, pp. 821–826

[10] TICO M., TRIMECHE M., VEHVILAINEN M.: 'Motion blur identification based on differently exposed images'. IEEE Int. Conf. Image Processing, 2006, pp. 2021–2024

[11] TSOMKO E., KIM H.J.: 'Efficient method of detecting globally blurry or sharp images'. Proc. Ninth Int. Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS), Klagenfurt, Austria, May 2008, pp. 171–174

[12] MARZILIANO P., DUFAUX F., WINKLER S., EBRAHIMI T.: 'Perceptual blur and ringing metrics: application to JPEG 2000', Signal Process.: Image Commun., 2004, 19, pp. 163–172

International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 499 - 503, 2013, ISSN: 2319–8656

An Improved Post-Quantum Cryptographic Scheme Based on NTRU

Sachin Kumar
Delhi University
Delhi, India

Shobha
Delhi University
Delhi, India

Saibal K. Pal
DRDO, Metcalfe House, Delhi, India

Abstract: In this paper we report a more secure and efficient encryption algorithm based on the NTRU cryptographic scheme. NTRU is lattice based scheme resistant to quantum computing, hence it falls under the class of post quantum cryptosystems. It is based on shortest vector problem (svp)[9].The main characteristics of the system are low memory and low computational requirements but it provides high level of security. We present modifications in the NTRU scheme for making it more secure and efficient particularly for applications in wireless and constrained devices. In the original scheme, repetitions in the plaintext message lead to repetitions in the cipher text, which is a source of weakness in the system. To overcome this problem each byte of the input has been digested with different operations that produce different encrypted text even for repeated content of the Plain text message. The second modification is enhancing the public key scheme that makes this system more robust. These two modifications in the NTRU scheme makes it secure even for use in the Quantum Computing environment.

Keywords: Public-key cryptosystem, NTRU, polynomial inverse, convolution product, post-quantum cryptography

1. INTRODUCTION

Post quantum cryptography is a fascinating area of research challenge. In existence of Quantum computer post quantum cryptography will be critical for the future interest as it is well known that quantum computer may destroy RSA, DSA, and ECDSA. Quantum computers can potentially break most of conventional cryptosystems based on the integer factorization problem and discrete log problem which are actually deployed in practice at present. Certain classical cryptosystems inspired by computational problems of nature that entirely different from the integer factorization and discrete log are potentially much harder to solve, will remain unaffected by the threat of Quantum Computing. So those are called QUANTUM-RESISTANT or more clearly 'POSTQUANTUM' cryptosystems [1].We has some question to answer like-

- Is there any need to worry about the threat of quantum computers?
- Why should focus not continue on RSA or other resistant cryptosystem for classical computers?

Now suppose a situation when someone announces that quantum computer is no more a mystery means it is constructed then computers using crypto systems will be unsecure. In such case we need to have some crypto systems resistant to quantum attacks. The reasons to work on Post Quantum Cryptography are [2]-

- Time is required to improve the efficiency of post-quantum cryptography.
- Time is required to build confidence in post-quantum cryptography.
- Time is required to time to improve the usability of post-quantum cryptography [1]

These reasons are suggesting that cryptographic community should work on the crypto systems that can provide the security in quantum computer environment. Following are some recommended areas of crypto systems resistant on quantum computing-

1) Hash-based cryptography- Most of the application requires the unbroken digital signature in quantum environment. Some hashed based schemes are found to be practical to post quantum cryptography. There are many example but classic one is **Merkle's tree hash-public-key signature system (1979)**, building upon a one-message-signature idea of Lamport and Diffie. [3]

2) Code-based cryptography-This category include classic example of **McEliece's hidden-Goppa-code** public-key encryption system proposed by McEliece in 1978. Reason to be resistant in quantum computer is that it is based on Goppa code which has been unbroken till recent research done. No attack of significant affects has been detected on the code based cryptography that's why it is most suitable candidate for post quantum cryptography[3].

3) Lattice-based cryptography- Lattice based cryptography has promises to the post quantum cryptography because they enjoy the very strong proof based on implementation as well provide very high level of security with simplicity. We will be discussing the one of such encryption scheme in this paper and improved version. [3]

4) Multivariate – quadratic - equations cryptography- In recent years these crypto systems have been considered resistant to attacks and based on the quadratic equation over finite field. All of them use facts that MQ problem is N-P complete. One of many interesting examples is Patarin's "HFEv–" public-key-signature system (1996), generalizing a proposal by Matsumoto and Imai.2 Daniel J. Bernstein. [3]

5) Secret-key cryptography- In this category of cryptography the leading example is the Daemen–Rijmen "Rijndael" cipher (1998), which was renamed "AES," the Advanced Encryption Standard. [3]

In our document we are working on the lattice based cryptography. We are proposing NTRU encryption more secure, resistant and efficient.

2. DESCRIPTION OF MODEL

The NTRU, a lattice based cryptosystem, the encryption basically depends on the mixing of polynomial having small coefficients with reduction modulo p and q, where p and q are some constants. The encryption and decryption of NTRU is O (N^2) when the block of massage is O(N), as compared to RSA having O(N^3) .The key generation is very easy and fast of O(N) as compared to RSA having O(N^2). System validity depends on the probability theory because it uses the random polynomial that is why each element has many possible encryptions [8].

Some defined notations, parameter [7] and definitions that are followed in entire system are-

Definition of a lattice: Let v1, v2…. vk be a set of vectors in Rm. The set of all linear combinations a1v1 + a2v2…+...+ akvk , such that each ai ∈ Z, is a lattice. We call it more formally as the lattice generated by v1, v2, . . . ,vk.

Bases and the dimension of a lattice• Let L = { a1v1 + a2v2 + . . . + anvn| ai ∈ Z, I = 1 , . . . n } and v1, v2 . . . ,vn are n independent vectors, then we call that v1, v2,. . . ,vn is a basis for Lattice and that L has dimension n which is equal to cardinality of a vector[4].

N: (Degree constant). A positive integer which defines the dimension of the vector.

q: (Large Modulus).A positive integer. The associated NTRU lattice is a convolution modular lattice of modulus q.

p: (Small Modulus). An integer or a polynomial.

Df, Dg :(Private Key Spaces). Sets of small polynomials from which the private keys are taken.

Dm (Plain text Space**)**: Set of polynomials that represent encrypts able messages.

Dr (Blinding Value Space).Set of polynomials from which the temporary blinding value used during encryption is selected.

Center (centering method). It is way of performing mod q reduction on cipher text.

Convolution product: The Ring of Convolution Polynomials is R =Z[X] / (XN −1). Multiplication of Polynomials (* between polynomials) in this ring corresponds to the convolution product of their associated vectors, defined by

$$(f * g)(X) = \sum_{k=0}^{N-1} \Big(\sum_{i+j=k \pmod N} f_i g_j \Big) X^k.$$

Operation between two polynomials refers to the convolution product while for the constant and the polynomial it is simple multiplication. There is one more notation Rq = (Z/*q*Z)[*X*] /(*XN*−1) convolution operation in Rq can also be called as modular convolutions[3].

Definition1.A binary polynomial is one whose coefficients are all in the set {0,1}. A trinary polynomial is one whose coefficients are all in the set {0,±1}.

Definition2. Following are definition of the polynomial spaces $B_N(d)$,$T_N(d)$,$T_N(d1,d2)$-
Polynomials in space $B_N(d)$ have d number of coefficients equal to 1 and the other coefficients are 0. Polynomials in space $T_N(d)$ have d +1 number of coefficients equal to 1, have d number of coefficients equal to −1, and the other coefficients are 0. Polynomials in space $T_N(d1,d2)$ have d1 number of coefficients equal to 1, have d2 number of coefficients equal to −1, and the other coefficients are 0.

NTRU Encryption Algorithm:

NTRU Encrypt consists of three basic functions-

- Key Generation
- Encryption of plain text
- Decryption of cipher text

NTRU Encrypt key generation consists of the following operations:

1) Randomly generate polynomials f and g in df, dg respectively.

2) Invert f in Rq to obtain fq, invert f in Rp to obtain fp, and check that g is invertible in Rq [5].

3) The public key h = p *g * fq (mod q). The private key is the pair (f, fp).

NTRUEncrypt Encryption:-

NTRUEncrypt Encryption consists of the following operations-

1) Randomly select a “small” polynomial r from dr.

2) Calculate the cipher text e as e ≡ r * h + m (mod q).

NTRUEncrypt Decryption:-

NTRUEncrypt decryption consists of the following operations:

1) Calculate a ≡ center (f * e), where the center operation reduces its input into the interval [A, A+q−1] where A is an integer which decide the domain of the interval.

2. Recover m by calculating m ≡ fp * a (mod p).

3. CONTRIBUTION

In this paper we have proposed a new way of doing encryption in the NTRU system. We have extended the key and have done some complexion on input massage and even on the public key. In out implementation we are applying operation of the each byte and order of the byte. On first byte we are exchanging the first four bit with last four bit and in the second byte we are exchanging the first two bit to the next two bit. This sequence is also followed in reverse order in decryption. For illustration take a byte sequence 11110110.When occurred at the first number it is converted to

11111001in Fig-1.When this comes on the second or even places it is converted to 11111001in Fig-2. On the second improvement in the encryption scheme we have some complex operation on the key itself due to which public key has changed. In previous implementation we have the public key.

$$h = p * g * fq \pmod q.$$

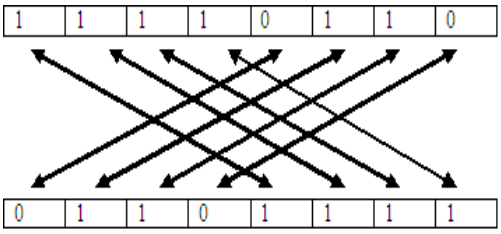


Fig 1: for odd placed byte

Where fq is the inverse of 'f' under modulo 'q' and * is convolution product of the two polynomial

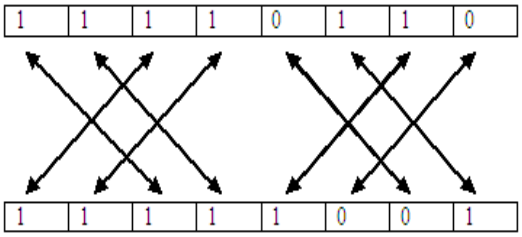


Fig 2: for even placed byte

Public Key Generation - Generate two polynomials randomly of degree N separately. Let these are r1 and r2 and do **Xoring** for each polynomial with other randomly generated polynomial. Convolution product is implemented for r1 and r2 with modulo q (say s) and find the convolution product of 's' and polynomial g. Now obtained product is multiplied by constant p modulo q(say t).We obtain convolution of g and fq and add 's' and 't' in it in modulo q .Result is h polynomial which is public key. Mathematically:-

r1 = r1 ^ random polynomial;

r2 = r2 ^ random polynomial;

s = r1 * r2 (modulo q);

t = ((s * g) * q) * p) % p;

h = p * g * fq (mod q)

h = (p * g * fq + s + t)(mod q)

Encryption:

1) Randomly select a "small" polynomial r belongs to Dr

2) Calculate the cipher text e as $e \equiv r * h + m \pmod q$ where m is message text.

Decryption:

In the decryption side we have private key (f, fp) (mod p). Now compute

a = f * e

Where e is an encrypted polynomial. Now obtain center of the polynomial from –q/2 to +q/2. This centering process is only for the maintaining the coefficient in the range between these –q/2 to +q/2. Now obtain the massage plain text by

m = fp * a (mod p)

Mathematical proof:

a = f * e

a = f * (p * r * h + f * m) (mod q)

m = fp * a (mod p)

m = fp * (f * p*r * h + f * m) (mod q) (mod p)

m = fp * (f * p * r *(p * g * fq + s + t + f * m) (mod q) + m) (mod q)(mod p)

m = fp * (f * p * p * r * g * fq + f * p * r * t + f * p * r * s + f * m)(mod q)(mod p)

m= (p *p * r * g * fq + p * r * r * s + fp * f * m)(mod q)(mod p)

m=m

Because these terms are multiple of p and when we take mod under p they get reduce to zero hence we get the original message.

4. IMPLEMENTATION

Public key generation:

Input: f and g polynomial.

Output: public key polynomial

1. Set: r1

2. Set: r2

3. Set r1 = r1 ^ random polynomial

4. Set r2= r1 ^ random polynomial

5. Set s = r1*r2;

6. Set t = p * g * s (mod q)

7. Set h = (g * fq + t + s)(mod q)

Here h is public key that provides more security when text is repeated more times

Digesting Input:

Input: g (polynomial of degree N with coefficient 0 or 1 only), m (plain text massage polynomial)

Output: Plain text massages polynomial.

0. Start:

1. Set: x=0,y=0

2.0 If (x mod 2 equals 0)

2.1 Set m + = g;

2.2 Set d = deg (N);

2.3.0 While (y < deg (N) / 2)

2.3.1 Set t = m [y];

2.3.2 Set m [y] = m [d + y]

2.3.3 Set m [d + y] = m [y];

3.0 Else then

3.1 Set y to zero

3.2 Set m - = g;

3.2.0 While (y < deg (N))

3.2.1 Set t = m [y];

3.2.2 Set m [y] = m [deg (N) – y];

3.2.3 Set m [deg (N) – y] = t;

4. End:

Undigesting Input:

Input: g (polynomial of degree N with coefficient 0 or 1 only), d (decrypted massage polynomial) [8].

Output: Plain text massages polynomial.

0. Start

1. Set: x = 0, y = 0;

2.0 If (x mod 2 equals 0)

2.1 Set d = deg (N);

2.2.0 While (y < deg (N) / 2)

2.2.1 Set t = m [y];

2.2.2 Set m [y] = m [d + y];

2.2.3 Set m [d + y] = m [y];

2.2.4 Set m + = g;

3.0Else then

3.1Set y to zero

3.1.0 While (y < deg (N))

3.1.1 Set t = m [y];

3.1.2 Set m[y] = m [deg (N) – y];

3.1.3Set m [deg (N) – y] = t;

3.1.4Set m - = g;

4. End;

5. OBSERVATION

Each public key cryptosystem has its own weakness and provide security based on some type of hard problem. Here in this NTRU encryption has some of its characteristics such as very less memory and computational cost. Security is based on the hard problem and the selection of the parameter set. in this scheme we have integer parameter N , P , Q and four set choosing the number of one and two in the polynomial like df ,dg ,dr etc.

TABLE 1
Comparison between NTRU and improved NTRU

Operation/entity	**NTRU**	**Improved Model**
Plain text block	$Nlog_2P$	$Nlog_2P$
Encrypted text block	$Nlog_2Q$	$Nlog_2Q$
Encryption speed	$O(N^2)$	$O(N^2)$
Decryption speed	$O(N^2)$	$O(N^2)$
Massage expansion	Log_pQ to 1	Log_pQ to 1
Private key length	$2Nlog_2P$ bits	$2Nlog_2P$ bits
Public key length	$Nlog_2Q$ bits	$Nlog_2Q$ bits

Now we are comparing the previous NTRU and the our model of on same set of parameter on each component like encryption and decryption and key size and other operation

We observe that both of the NTRU previous and our model have the same level of key length, and cost of operation encryption and decryption. While the change in the public key makes it more secure and digesting on the input makes it more complex to break

In the literature we have much public key crypto system with different type of hard problem including RSA based on difficulties of factoring problem, mackliece public key system on error detecting code and many others. When the modified scheme was compared with the other cryptosystem on key size and the operations we have concluded following TABLE II. This table concludes that NTRU message encryption varies even for long massage .Principle of expansion of the massage is exchange of the public key in massage block this is not significant problem. We have this solution for problem and this solution can also be implemented even for long massage with expansion of only after the first massage block. With this approach, from the sending side massage is with the polynomial with 0,1,-1 under modulo p=3,and interpreted as P1 for next massage block. The next massage block is p1*e1+m where m is first block of massage and m1 mod q

can be reduced exactly next block e2=p2*e2+m2 where p2 is calculated by squaring the m1 and reducing it by p=3. This process continues for massage of arbitrary length, hence this continues for massage of arbitrary length.

TABLE 2
Comparisons with other public key crypto system

Operation	NTRU (improved)	R S A	Mackliece
Encryption	N^2	N^2	N^2
Decryption	N^2	N^3	N^2
Public key	N	N	N^2
Private key	N	N	N^2
Massage expansion	varies	1-1	2-1

6. CONCLUSION AND FUTURE GUIDELINE

This document aims to meet the requirement of more secure and efficient NTRU. Security is achieved by introducing some more complex problem into the existing implementation and efficiency can be achieved by having some reduced implementation of polynomial multiplication of inverse computation. The most time consuming operation in NTRU are product of the polynomials because that is used for even for all operation like key generation, encryption and decryption.

In order to achieve the security we have achieved our goal to certain extent by modified algorithms with digesting function introduction. Comparison shown in this paper with other public key cryptosystem is much satisfying as cost remains the same and security increases highly. This is more important to build the confidence in post quantum cryptography. As this crypto system include very low computational requirement because polynomial coefficient are very small integer hence it is applicable for devices like mobile and embedded system with less computational power and which require sufficient amount of security[10].

For suggestion there can be two main areas one is reducing the cost of multiplication of polynomial which eventually will make the scheme more efficient. And the second one is using other scheme for security for case of repeated text. For this scheme digesting function-

F(x1+x1.x2+x2.x3…xn-1.xn) can be computed and undigesting correspondingly at decryption side where x1, x2, x3…xn are the byte of the text.

7. REFERENCES

[1] Introduction to post-quantum cryptography by Daniel.J. Bernstein Department of Computer Science, University of Illinois at Chicago.

[2] Post quantum cryptography by Daniel J. Bernstein, Johannes Buchmann Erik Dahmen Editors.

[3] Practical lattice-based cryptography: NTRUEncrypt and NTRUSign Jeff Hoffstein, Nick Howgrave-Graham, Jill Pipher,William Whyte.

[4] Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.

[5] The NTRU Public Key Cryptosystem – A Tutorial, http: //www.ntru.com.

[6] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Cli_ord Stein.Introduction to Algorithms. MIT Press and the McGraw-Hill Book Company, second edition, 2001.

[7] N. Howgrave-Graham, J. H. Silverman, W. Whyte, Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3, CT-RSA 2005.

[8] P. Shor, Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer, Preliminary version appeared in Proc. of 35th Annual Symp. on Foundations of Computer Science, Santa Fe, NM, Nov 20-22, 1994. Final version published in SIAM J. Computing 26 (1997) 1484.Published in SIAMJ .Sci.Statist.Comput.26:1484, 1997 e-Print Archive: quant-ph/9508027.

[9] M. Ajtai The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract) in Proc. thirtieth ACM symp on Th. of Comp.,1998, pp.10–19

[10] D. Bailey, D. Co±n, A. Elbrit, J. Silverman, and A. Woodbury, \NTRU in Constrained Devices," in Workshop on Cryptographic Hardware and Embedded Systems | CHES 2001 (C» . Ko»c, D. Naccache, and C. Paar, eds.)