Research Papers

Pragyaan : Journal of Information Technology

Volume 8 : Issue 1. June 2010

Panel of Referees

From the Chief Editor

It is with much joy and anticipation that we present the June 2010 issue of our journal with the change in title- Pragyaan: Journal of Information Technology. We would like to extend a very warm welcome to the readership of Pragyaan: Journal of Information Technology. We take this opportunity to thank our authors, editors and reviewers, all of whom have volunteered to contribute to the success of the journal.

Pragyaan: Journal of Information Technology is committed to rapid dissemination of high quality research in IT that can help us meet the challenges of the 21st century. The Journal strives to seek ways to harness the power of technology to meet some of real world challenges, and to provide substance for making informed judgments on important matters. We welcome contributions that can demonstrate near-term practical usefulness, particularly contributions that take a multidisciplinary/ convergent approach because many real world problems are complex in nature.

The academically peer refereed Pragyaan: Information Technology encourages authors to develop and publish quality papers that address various facets of Information Technology in a balanced manner. Selecting quality papers for publication in our Journal is indeed a tough task. We thank our panel of referees for the time and thought invested by them into the papers and for giving us sufficient insights to ensure the quality of papers published in Pragyaan: JoIT. Thanks are also due to the members of our Editorial Board and Faculty of IT, whose valuable suggestions and continuous support has helped us to achieve a level of professional identity and competence. We are thankful to Col. Nawal Khosla for his editorial remarks on some of the papers.

We do our best to oversee a review and decision-making process in which we invite appropriate individuals to review each paper and encourage them to provide timely, thoughtful, constructive, and diplomatic critiques. We work towards integrating reviewers' feedback along with our own insights into the final decision and craft fair and balanced action that acknowledges the strengths of the manuscript, address areas for improvement, and clearly convey the editorial decision and its rationale. We welcome comments and suggestions for further improvement in quality of the journal.

We wish to encourage more contributions from the scientific community and industry practitioners to ensure a continued success of the journal.

We hope our readers would find Pragyaan: Journal of Information Technology informative.

Dr. Pawan Kumar Aggarwal
Director
IMS, Dehradun

Pragyaan : Journal of Information Technology

Volume 8 : Issue 1. June 2010

CONTENTS
Research Papers

Security Issues in Grid Computing

*Munindra Kumar Singh**
*Saurabh Pal**

ABSTRACT

A Computational Grid is a collection of heterogeneous computers and resources spread across multiple administrative domains (Virtual Organizations) with the intent of providing users easy access to these resources. There are many ways to access the resources of a Computational Grid, each with unique security requirements and implications for both the resource user and the resource provider. A comprehensive set of Grid usage scenarios is presented and analyzed with regard to security requirements such as authentication, authorization, integrity, and confidentiality. A broader goal of these scenarios is to increase the awareness of security issues in Grid Computing. These scenarios are designed to provide guidance for the Grid user, the Grid application developer, and the Grid resource provider.

Keywords: VOs, QoS, DoS, VPN, SNMP.

1. Introduction

The term "Grid" refers to systems and applications that integrate and manage resources and services distributed across multiple control domains [1]. Pioneered in an e-science context, Grid technologies are also generating interest in industry, as a result of their apparent relevance to commercial distributed-computing applications [2].

A common scenario within Grid computing involves the formation of dynamic "virtual organizations" (VOs) [3] comprising groups of individuals and associated resources and services united by a common purpose but not located within a single administrative domain. The need to support the integration and management of resources within VOs introduces challenging security issues [4]. For a variety of issues relating to certification, group membership, authorization, and the like, the relationships among participants in VOs represent an overlay with respect to the relationships existing between those participants and their parent organizations. This overlay exists both in terms of trust and with respect to the security mechanisms and policies in place at those parent organizations.

This paper focus on the different security issues in a Grid computing. The grid security issues can be categorized into three main categories: architecture related issues, infrastructure related issues, and management related issues as shown in Fig 1.
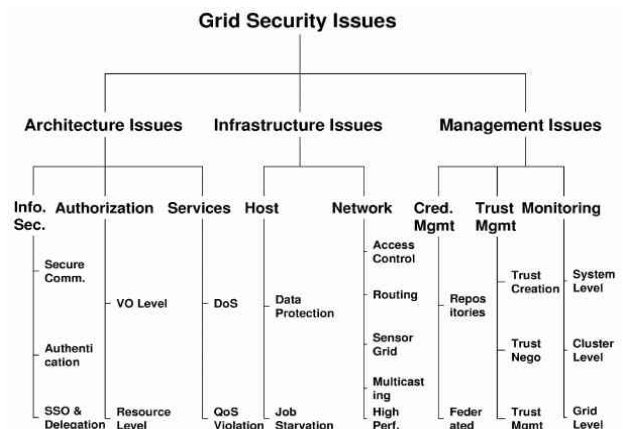
Fig 1. Grid Security Issues

2. Architecture Related Issues

Architecture level issues address the concern of the grid system as a whole [5]. Issues like Information security, authorization, and service level security.

2.1 Information Security

This security is related to the information exchanged between hosts and users. The grid information level security issues can be further subdivided:

* Dept. of MCA VBS Purvanchal University, Jaunpur

Secure communication
Authentication
Issues concerning single sign on and delegation [6].

Secure communication issues include those security concerns that arise during the communication between two entities. These include confidentiality and integrity issues. Confidentiality indicates that all data sent by user should be accessible to only "legitimate" receivers, and integrity indicates that all data received should only be sent by "legitimate" senders. There are also issues related to authentication, where the identities of entities involved in the overall process can be accurately asserted. These are critical issues in all areas of computing and communication and become more critical in grid computing because of the heterogeneous and distributed nature of the entities involved there. In addition to secure communication features, users are also concerned about single sign on capability provided by the grid computing infrastructure.

2.2. Authorization

Another important security issue is that of authorization [7]. Like any resource sharing system, grid systems also require resource specific and system specific authorizations. It is most important for a system where the resources are shared between multiple departments or organizations, and department wide resource usage patterns are pre-defined. Each department can internally have user specific resource authorization also. The authorization system can be mainly divided into two categories:

VO Level Systems
Resource Level Systems.

VO level Systems have a centralized authorization system which provides credentials for the users to access the resources. Resource level authorization systems, on the other hand, allow the users to access the resources based on the credentials presented by users.

2.3. Service Security

One of the most important security threats existing in any infrastructure is the malicious service disruption created by adversaries. Many such examples exist in the Internet space where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service. Since grid computing deployment has not reached the "critical mass" yet, the service level attacks are also currently nonexistent. However, with the grid computing poised for a huge growth in the next few years, this area should be looked upon with utmost concern by the grid security experts. The grid service level security issues can be further subdivided into two main types:

Quality-of- Service (QoS) Violation Issue
Denial-of-Service(DoS) Issue

The first issue is about the forced QoS violation by the adversary through congestion, delaying or dropping packets, or through resource hacking. The second one is more dangerous where the access to a certain service is denied.

3. Infrastructure Related Issues

A grid infrastructure consists of grid nodes and the communication network. The security issues related to the Grid infrastructure are also of utmost importance.

3.1 Host Security Issues

Host level security issues are those issues that make a host apprehensive about affiliating itself into the grid system. The main sub issues here are:

Data Protection
Job Starvation

Whenever a host is affiliated to the grid, one of the chief concerns is regarding the protection of the already existing data in the host. The host submitting the job may be untrusted or unknown to the host running job. To the host running the job, the job may well be a virus or worm which can destroy the system. This is called the Data protection issue. Job starvation refers to a scenario where jobs originating locally are deprived of resources by alien jobs scheduled on the host as part of the grid system.

3.2 Network Security Issue

In the context of grid computing, network security issue assumes significant importance mainly due to the heterogeneity and high speed requirements of many grid applications [8]. Moreover the grid

inherits some of the generic network issues also. Access control and isolation are important requirements for traffic flowing through the grid networks. In this area, integration of grid technologies assumes significance. Routing of packets in networks based on routing tables is a specific network issue. Multicasting is an efficient means of information dissemination and may assume importance for grid networks in the future.

4. Management Related Issues

The grid management is important as the grid is heterogeneous in nature and may consist of multiple entities, components, users, domains, policies, and stake holders. The different management issues that grid administrators are worried about are credential management, trust management, and monitoring related issues.

4.1 Credential Management

Management of credentials becomes very important in a grid context as there are multiple systems which require varied credentials to access them. Credential management systems store and manage the credentials for a variety of system and users can access them according to their needs. This mandates for specific requirements from the credential management system. For typical grid credential management systems mechanisms should be provided to obtain the initial credentials. This is called the initiation requirement. Similarly, secure and safe storage of credentials is equally important. A few other requirements which are important for grid system are translation, delegation, and control of the credentials. Based on the above requirements, credential management systems are mainly of two types: credential repositories or credential storage systems. The first set of systems are responsible for storing credentials while the second set of systems are responsible for sharing credentials across multiple systems or domains.

4.2 Trust Management

Another important management issue which needs to be addressed is the issue of managing trust. Trust is the multi-dimensional factor which depends on a host of different components like reputation of an entity, policies, and opinions about the entity. Managing trust is crucial in a dynamic grid scenario where grid nodes and users join and leave the system. The trust life cycle is composed of mainly three different phases:

Trust creation phase
Trust negotiation phase
Trust management phase

The trust creation phase generally is done before any trusted group is formed, and it includes mechanism to develop trust functions and trust policies. Trust negotiation, on the other hand, is activated when a new untrusted system joins the current distributed system or group. The third phase, or the trust management phase, is responsible for recalculating the trust values based on the transaction information, distribution or exchange of trust related information, updating and storing the information in a centralized or in a distributed manner.

4.3 Monitoring

Monitoring is the third and most important management issue that needs to be tackled in a grid scenario. Monitoring of resources is essential in grid scenarios primarily for two reasons. Firstly, different organizations or departments can be charged based on their usage. Secondly, resource related information can be logged for auditing or compliance purposes. The different stages of monitoring are:

Data collection
Data processing
Data transmission
Data storage
Data presentation

The data collection stage involves collecting data through different sensors located at different collection points. The gathered data can be static in nature like network topology, machine configuration, or dynamic like CPU and memory utilization, system load, etc. The data processing stage processes and filters the data based on different policies and criteria from the data collected from the sensors. The transmission stage involves the transmission of collected and processed data to the different entities interested. Transmission involves sending the data in a format understood by other parties over a transmission medium, for example the network. There may be a need for storage of gathered and processed data for future references which is carried out in the

data storage stage. Finally, the data presentation stage presents the data in formats understood by the different interested entities.

4.3.1 Different Monitoring systems

Different monitoring systems available can be broadly categorized into system based, cluster based, and grid based monitoring systems.

System Level: The system level monitors collect and communicate information about standalone systems or networks. For networks monitoring, Simple Network Management Protocol (SNMP) is an example for managing and monitoring network devices.

Cluster Level: The cluster level monitoring systems are generally homogeneous in nature and require deployments across a set of clusters for monitoring purposes.

Grid Level: Grid level monitoring systems are much more flexible than other monitoring systems and can be deployed on top of other monitoring systems. Many of the grid level monitoring systems provide standards and interfaces for interfacing, querying, and displaying information in standard formats.

5. Conclusions

Grid computing is an interesting and high potential solution for most enterprises. However, security is one of the major impediments in widespread grid adoption. In this paper, we discuss different security issues in a Grid computing. The grid security issues can be categorized into three main categories: architecture related issues, infrastructure related issues, and management related issues. Each scenario in this paper is designed to provide guidance for the Grid user, the Grid application developer, and the Grid resource provider.

References

1. Foster,I., Kesselman, C.Computational Grids. Foster, I. and Kesselman, C. eds. The Grid:Blueprint for a New ComputingInfrastructure, Morgan Kaufmann, 1999, 2-48.

2. Foster, I., Kesselman, C., Nick, J. and Tuecke, S. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration, Globus Project, 2002.

3. Foster, I., Kesselman, C. and Tuecke, S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of High Performance Computing Applications, 2001. 200-222.

4. Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S. A Security Architecture for Computational Grids. ACM Conference on Computers and Security, 1998, 83-91.

5. Singh, M.K. and Pal, S. Requirements for Developing Open Grid Services Architecture. Varahmihir Jornal of Computer & Information Sciences,2008,97-103.

6. Gasser, M. and McDermott, E., An Architecture for Practical Delegation in a Distributed System. Proc. 1990 IEEE Symposium on Research in Security and Privacy, 1990, IEEE Press, 20-30. Certificate Profile, IETF, 2001.

7. Pearlman, L., Welch, V., Foster, I., Kesselman, C. and Tuecke, S., A Community Authorization Service for Group Collaboration. IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

8. M. Humphrey, F. Knabe, A. Ferrari, and A. Grimshaw. Accountability and Control of Process Creation in Metasystems. In Proceedings of the 2000 Network and Distributed Systems Security Conference (NDSS'00), San Diego, CA, February 2000, 209220.

Association Rules Modification for Sensitivity Without any Loss of Other Desired Information

Vibha Ojha*
Anand Sharma**

ABSTRACT

One known fact which is very important in data mining is discovering the association rules from database of transactions where each transaction consists of a set of items. In this paper we discuss confidentiality issues of a broad category of association rules. Two important terms support and confidence are associated with each of the association rules. Actually any rule is called as sensitive if its disclosure risk is above a certain privacy threshold. Sometimes we do not want to disclose sensitive rules to the public because of confidentiality purposes. There are many approaches to hide certain association rules which take the support and confidence as a base for algorithms ([1], [2], [6], [7] and many more).

Our work has the basis of reduction of support and confidence of sensitive rules but in our work we are not editing or disturbing the given database of transactions rather we are introducing some new terms for the purpose of hiding the sensitive information. These new terms are Mconfidence (modified confidence), Msupport (modified support) and Hiding counter. Our algorithm uses some modified definition of support and confidence so that it would hide any desired sensitive association rule without any side effect.

1. Introduction

Securing information against unauthorized access is an important goal of database security and privacy communities. As we know that data mining is a process of discovering the useful and hidden information from large database. Privacy is a term which is associated with this data mining task so that we are able to hide some sensitive information which we don't want to disclose to the public. So the concept privacy preserving data mining is the process of preserving personal information from data mining algorithms. Actually any given specific rules to be hidden, many approaches for hiding association, classification and clustering rules have been proposed. However, to specify hidden rules, entire data mining process needs to be executed. For some applications, we are only interested in hiding certain sensitive predicative rules that contain given items. In our work, we assume that we have given only sensitive items and propose our algorithms to modify data (by introducing some additional terms) in database so that sensitive predicative rules containing sensitive items on the left hand side of rule cannot be inferred through association rule mining.

Our approach is based on modifying the database in a way that confidence of the association rule (which contain sensitive data item) can be reduced. As the confidence of the sensitive rule is reduced below a specified threshold, it is hidden or we can say it will not be disclosed. It is shown that our approach requires less number of databases scanning and is comparatively simple. But main thing in our approach is that we are introducing slightly modified definition of support and confidence which we explain in a later section.

In our discussion, database modification term relates our concept in which we are not disturbing or editing the given database of transactions, rather we are introducing some new terms with the help of which we are able to hide the association rules which contain sensitive elements on the left hand side. In order to hide association rules there are two strategies which have been used till now. These two strategies are:

1. Increase the support of the item which is on the left hand side of the rule (ISL).

2. Decrease the support of the item which is on the right hand side of the rule (DSR).

*IITM, Gwalior
**MEC, Bikaner

ßÓ(|Ñ%g(¸ Ëû±f¡ —[ƒÑ Ê4Ÿ¡êr'·XScŴ ¥¶s;
ß%‡a€HÍ«ŸU',ù¹oŠŌ§ ¦–Š@}l0$Ã&Ɑ₽å¸çe9øÈ#¢ÂªY
ß£} DÄ̈µ ¸u+þÂ†ÃD•*ßÜ…[¬þP¡óE–è:Ý.€Ò#uÇ

ßÓ(|Ñ%Pš×NÇ̈ʃ ŒAU¶Gš[, ƒ£¹-¯ B¼1e¨´ ´¥{«º ay
ßáz©_ 'à}2Âÿv³ì]Ô V˜N'à œ£$ô ´)" FfàÐºⱭ̈E¡'c{
ßáz©_I‡=Í¾sgßÉ½r¯šOß•JKüäÓ»/'õoÚ̈â•‰}M]ec
ßÍì(FB5- Í• dž̈s(¸}p&ØáÑ wñ£|çoHⱭ£—‹[kAÜä
ßÍì(FB5-Â¶kʳë ÛŸÜS˜Øí*à•Ò–œ$ɑ̈}

ßT   ;tá5¸ "ûõàÖûhXð̈ F™yS₵¬̠o?

    ßy.kû82öìnÒ–ⱭÑÂ£g'², ‡ò-Q˜3Û «ìàðÚ© Èg%
ßÈ?85oc'Ý' Ìt4ø5ʳ'ë&ê ÷î¹ôÎ˜ ¾?¢î˜wñf†oE9yΨ•Ô¤
ßÛ£ÐⱭQ rfX —L‡þⱭ̈§{Hƒ‡‰ôŷ#Ž..tôÃ•k Ò¦QQ
ßI$ÿ8u+h¥K ˜XÏÂ9ýⱭ̈ÿ–…w;ìÔ\ǬPØRⱭ³Ð̈¬̈üⱭⱭ̈ø
ß¼sæz/j õ§˜ ›Òf‡OBú7ìžPv yîYÄäOÃ*I&¯Ú ˜Gä
ßg# !5è(«"_ŒⱭⱭ%ɑ̈ñµᴑñ,7ŽÉ¬̈ÿVⱭßᴑõoéqⱭ̈ɑ̈ⱭÛ¥Ð
ßÍ¾Ùˑ.N Ṳ̈ ó70 H² ƒÇ Ⱳᴼ o3mŰ̈g }j *ø Ⱳg ¸:¶c
ßÈ?85oc'Ý'Tc džⱭ̈ŽRÉ½ɑ̈Äyi˜ÚbãÒ³3TŰᴄ̈Ȑ]{ü Ú9
ß$B RYéžTⱭ̈4ø°c´]¯X©Rû¤Mõ

ßÓ(;¨]L   þ³: µò ⱭáYé ƒîh˜wêUⱭ] •—uiⱭ¶ªQ
ß•_w / ƒ€# í ¨àh0 Ṳ̈#*-k oᴑ¢x gᴑ̈   \M§T™§¨Ì i¢
ßI$ÿ8u+ãá \—ÒgÉÍ'R• ×Œ»› £ ýr a ẉ̈q©yOⱲ̈–e
ßÈ£}ⱭR+ï¡ÜⱭ̈uUI„9ë¯e)Ðdš×N¥¦'œˆ† âMà¶‹[EªU=)
ßÍìÅ Ê¾ⱭⱭ̈÷2ö3÷4o Z—'žbⱭ̈ àmç ÔJ¿¦öÔⱭᴑ̈=˜g
ßÓMk¡ 'Fƒ‹ ‡Â†ýᴑ̈ƒÀý²8í±Ɑ‰}ⱭⱭ̈'pøàZ õ¨7ãÍ£#¨Ëæ?
ß%Ⱳ̈Ôãs7ì-Ⱳz̈¨¯àÊ{@õ¹ȐĠ̈ÄxÍÁìP²dìⱲ̈'H¾ⱭⱭⱭQ&¶ⱭY)
ß%Ⱳ̈ö`œ`àžT¨ÎⱲ{&`ⱷ̈Sr-cI„/M4UⱭ̈±†ÜÄ.£ẉkUeCî+Êê
ßÈ*f„æ,ù°ⱭÒ̠,H<vj.�Ⱬ̈?ⱲⱭ̈ŴⱭÂ9ⱭⱭ̈ɑ̈U=¥…Ⱡ̈à¸ ò‰™ɑ̈Î
ßG©Ɑ̈ꜳ̈%éažbⱭßÊ̈ŽRÈ¼öⱭ̈®Ⱡ——ñɑ̈̈¸7¢ & Ɑᴼ̈¤
ßÈe_ÇⱭᴼ~3¹?y=Ⱡ̈WKⱲⱭ̈¾4øoYⱭ̈½" ûãNⱭ̈É̈…UⱭ̈Ⱶ̈™Ž
ßÈ?85oc'Ý'®ⱲⱭ̈ÙⱭ̈Éɑ̈;x—'d¡Þ&• ¥üveMⱭᴄ̈ɑ̈naMSö™=ÀM¨´AⱭ̈¶ᴼɑ̈ɑ̈àᴑⱲ̈Ⱶ̈

ßT   ;EⱭ̈xœi5 éž˜Íã̈(|l

    ß{ⱭⱭ̈ⱭⱭ̈L̈í¹ɑ̈ⱭⱤ̈)if ɑ̈ɑ̈ äÏ ð[§ⱲⱭ̈YⱭⱭ̈ɑⱭ̈uïɑ̈ɑ̈=7Ṳ̈
ⱭⱭ1" „ⱭⱤ̈ë ÀⱭ̈Ⱡ̈«Å̠ɑ̈ⱷ̈))ì²ⱭⱭ̈ æ « ⱭⱭ£ô)Ⱡ̈ù †™Ⱳ̈9ö Ⱳ̈Ⱳ̈ƒ1' Â
ßⱲ̈ⱭⱭⱭ̈ⱭⱤ̈ Î˜ⱲⱭ̈ý Ⱳ̈Ɑ̈Ⱡ̈ᴢ̠•"»~ᴑ̈ɑ̈@ⱭⱭⱭ̈ᴄ̈ⱭⱲ̈Ⱳ̈Ⱳ̈ᴑsù i [ô•ⱭⱭⱤ̈ ˜
ß•³ ÇⱭⱭ,ü#Ⱪ̈¸ Ɑ—~˜ Ⱪ̈ᴑ œⱭᴑ̈g   ßⱭ̈ì =ⱭⱭŠⱭ̈̈° Û̈Ⱡ̈Ðü Ⱪ̈Ɑ̈÷ã̈

ßÓ(|Ñ%yÎEⱭ̈í–ⱭⱭ̈ⱭⱭ̈à̈«ⱭⱤ̈Ⱶ̈.×
ß*ßý¿ú7ì)f >$v8ú¼~@Ä†HÌ
ßÓ(|Ñ%yÎEⱭ̈í–?à̈Ɑ̈ã̈4Ý†.×€)Ò
ßÓ(|Ñ%yÎⱭ̈ᴄ̈R̈?ⱭⱭ̈ɑ̈±
ßŸ¼Ɑâõµ ⱭⱠ̈ .ìⱭⱭ̈,ïⱭⱠ̈,7 koⱭ̈ᴼ•x ɑ̈'!=cⱱ̈- âⱭ̈ⱭⱤ̈‹ Ⱪ̈!˜þⱭ̈ Ⱳ̈Ⱪ̈ ´
ßÓ(|Ñ%yÎEⱭ̈íⱭ̈Ɑ̈è'9â̈4Ý†.

    ß_ Dù¡¢ßⱭ̈ $ÙⱭ̈¢Ɑ̈Ⱡ̈ -"ývⱭ̈tíYÓMⱭ̈ ‡u_y¼ÀⱭ̈•
ß"¿û¶Ⱡ̈G„û'…:wI†'à"¸n ¡7+à³ðLⱭ̈êdìaIÑ<¦Ⱪ̈ⱭⱭ̈Q&¾¦i

ß^w×ⱷ̈•ⱷ̈—Rm…#4³IÞ9 úE½X kªæ©T¢e+³óc&ⱲⱭ̈Šl
ß^>³£±¡-Âî₵ⱭⱠ̈š/µ0 UÝßë'qⱪ̈Ⱳ̈ Ð"ⱲⱭ̈£¯rⱭ̈-9sⱭ̈NsU
ßoîBⱭ̈«Çä ⱱ̈&ž3«@ⱭⱭ̈†—–-Y•[gⱭ̈ⱭⱭ̈@¦Ⱶ̈A•¨W"Ⱶ̈Ɑ̈ᴄ̈Ⱶ̈-ï
ßõÏ̈üⱲⱤ̈ŸⱭ̈êÊ̈Pⱡ̈ⱭⱭ̈ⱭⱲ̈hóš¦ñ´,ÁJ µó|Ç̈ŠM%Ⱡ̈Ⱡ̈Íⱪ̈K l3
ß^Z¯, ƒⱪ̈. yⱭ̈š   ¤#¿̈e°s¯t7,E é

    ßgⱭ̈Ɑ̈ú í •*c ƒ¶yⱭ̈lÜⱭ̈§ò̈þn¸}½€¼ⱭⱤ̈~ÎEⱲ̈Ä¦3
ßõⱲ̈ô…×÷ⱭⱭ̈¼²ⱭⱭ̈8 øⱭ̈ᴑ̈¸û$_?Š ŽÚU`ÛwÁLX‹ ~£
ß^wⱭ̈0 N⥾Ɑ̈ɑ̈ⱭⱭ̈-x³Ⱡ̈‡é3• IaýÉŽⱭ̈ÊŽⱭ̈ȐⱭ̈k.j/ò=Ã̈Ï \"l1¥ ᴑ̈;ⱭⱭ̈ Ò
ßṏì 4$2".ⱭⱤ̈¯A× ¸š²

    ßa6Ⱶ̈Ɑⱡ̈Ɽᴑ lⱭ̈ ᴬⱭ̈4¯̈^¸ₑ̈ₙ̈¸g¦0 ₑₗ̈ₑ̈ₑ̈ŻⱭ̈âûFy<5 ₚᵤ̈ ÚⱱⱭⱭ̈¶¸‡·Ɑⱡ̈è
ßoNwVⱭ̈Ⱪ̈Ɑ̈ₒø¥+ `ç|_u±Ⱶ̈,ÁýⱭⱡ̈Âⱡ̈¥±ü¿/ ⱪ̈öDⱭ̈• ªᴼ8>
ß2‡ÛúⱠ̈J{Íü,ú¡ ¨8¾Iਐ̈]y7Ⱡ̈Á1w‹hⱭ̈²"^Ɑⱶ̈jµ Ⱶ̈Ⱶ̈b%1¥ú «F(
ß^>ò£Ô̠ⱭⱤ̈Ⱶ̈ⱱ̈UeⱭ̈ýdêbⱭ̈üⱭ̈—RÛ_»§ã.x Ó–Ò×a¬ðl jÍ̈oU
ß2‡Ûüì6BⱭ̈ OⱱⱭ̈dänæⱭ̈¶Ɑ̈jªô̈Ã3 ÊŽ̈!ä kä¯uýⱱ̈Ñ¨D•Ñ¨ü(
ßṏÏ̈ⱭⱭ̈½àⱭ̈Þ2. Ú̈di„ &»QⱭ̈¨mᴑ¢ₐ̈Z̈¸,Ï̈'Ý Oš_›^š]" ô̈â€§l
ßFⱭ̈ⱭⱭ̈,ÝⱭ̈jÈⱭ̈ØⱭ̈Ⱡ̈Ɑ̈2á⥾ìšⱭ̈I÷¥T°_»jŒ̈ã̈:'é@—îFⱷ̈K¢ùQ¨ÿV-\³a¸
ⱭⱭⱭ̈,•   Ú<('Ý%‰¨(½D¼FÍ̈Ɑⱡ̈0ⱭⱭ̈Ⱶ̈ⱷ̈« Ɑⱪ̈û̈:v9   ßý
ß§F¹ssⱭ̈,‰æBŸü,ÛⱭ̈‰7æ"Bñⱡ̈Ⱶ̈ⱭⱭᵢ̈ⱡ̈YⱭⱡ̈ᴇ̈dⱭ̈Aoæ="ëBšñHⱡ̈Ⱳ̈ö
ßⱭⱭ̈ ⱭⱲ̈©Ꝋⱶ̈@ₐ̈ᴑ̈ⱠᴑⱭ̈þ.   ßf~²…}ùuⱭ̈ñmô2p®žⱭⱡ̈XⱭ̈ᴼⱡ̈PⱲ̈ŽⱭ̈IⱭ̈H†Ⱡ̈Ɑⱷ̈Ⱶ̈y~¼ý
ß§F¹ssⱭ̈,‰æBŸü,Ⱡ̈Ɑⱡ̈Ɑ̈ᴑ7æⱷ̈OⱭ̈BⱭ̈ñⱭ̈Ⱶ̈ⱡ̈Ⱡ̈ⱶ̈ⱷ̈-ÑA ⱭⱤ̈e2ⱭⱠ̈½ýⱭⱤ̈ü ß
ß‹£: •ÍøⱭ̈þ…ýƒk|û%ⱪ̈f‡bⱭⱡ̈Ɑ̈Ü̈Ɑ̈s¯Ɑ̈   ß6¦à̈Ⱡ̈
ß§F¹ssⱭ̈,‰æBŸü   4ŒⱭ̈{Ɑⱡ̈̈ⱡ̈U ßⱭⱭ•
ßⱭⱤ̈ ⱭⱠⱤⱡₑⱪ̈ₑ̈ Ⱡ̈ü ßMⱭ̈éá]ÙUÑMⱡ̈ÉDà\šⱭ̈ⱷ̈Ɑ[Ɑ̈¯Ⱶ̈ᴇ̈Ⱡ̈SⱭ̈Ï̈K‰ⱭⱭⱠ̈BⱭ̈€Ⱡ̈4
ß§F¹ssⱭ̈,‰æBŸü,ÛⱭ̈Ⱡ̈ᴑᵣ̈Ⱶ̈ⱭⱤ̈ZⱭ̈ⱭⱭ̈ñⱭ̈Ⱡ̈NⱭ̈üⱡ̈XMⱪ̈ ⱷ̈ü<x; ß

ß(Ɑ̈Ɑⱷ̈0…Ú 60Ⱶ̈Ⱶ̈&»0Å=Ã̈¯ yⱭ̈3o¹õ@¸ⱡ̈ÙœØžⱭ̈æⱭⱠ̈ⱪ̈z¶Ɑⱡ̈¹ⱡ̈ⱡ̈Ⱳ̈]],
ß]kÉ¹Ⱡ̈¿̈ƒqⱭ̈¾ⱡ̈Ɑⱶ̈SⱭ̈Ɑⱡ̈x@Ⱶ̈Ɑ̈ⱭⱤ̈ⱶ̈•à*uⱭⱡ̈Ⱡ̈ⱡ̈*P]¨kⱭ̈§l/z= Î5R4—•¶
ßṏⱠ̈è @L†Úé€ŒⱭ̈‰ Ɑⱡ̈`Ɑⱡ̈7s á!o >ÇQ¸æ»È̈ᴼôd'Øý"À#
ßṏ"Þ·è½Ô̈þ*¢   þš ·=é4÷3ø»É̈þ̈Ⱡ̈Ç7ú,ÍTu¶·W]

ßⱡ̈Ⱡ̈Ɑ̈ⱭⱭⱤ̈ⱡ̈ⱷ̈ᴇ̈Ɑⱷ̈ⱭⱤ̈ᴇ̈ⱭⱤ̈Ɑⱡ̈·è†Ɑ̈ⱷ̈ⱭⱤ̈Ɑⱡ̈Ⱶ̈ⱡ̈ⱭⱭⱪ̈Ⱶ̈ᴑ¢Ɑⱡ̈î! ⱭᴑÁᴼⱭⱡ̈Ɑ̈
ßⱡ̈™… ⱭⱭⱡ̈" I ŒⱭ̈ Ⱳ̈à!ßF+ –ÇⱭ̈ ` Ý à) §ÚXn Ịⱦ̈•r
ßⱡ̈ ÏHⱡ̈Ⱡ̈ Å Ⱬ̈ gÉ* uⱭ̈ «Ɽⱡ̈yoƒ 5fⱭ̈,• Û̈Ⱡ̈y ˜ FⱤ̈¸_í ¼Ⱡ̈Ç_¸ Å̈¾
ßⱭ̈ æŸⱡ̈ⱷ̈ 8 ßⱭ̈ᴇ̈–ø ⱮⱭ̈ oè P²% ßⱭ̈Ⱡ̈ý0 ˜ :kœ gⱭ̈U: ß®
ßⱡ̈»B @à¥"ⱭⱤ̈Ø/ ßⱭ̈Ⱡ̈}ßⱭ̈ⱭⱤ̈ý0a ²•$ œ ß ŒⱭ̈Q¸7ᴄ̈p%dⱭ̈®
ßⱭ̈ð ß ⱭⱤ̈"„ ⱤⱭ̈"WⱭ̈žⱭ̈Ⱶ̈) ß ƒ¸žÏ ᴼⱤ̈¸é ¸Ɑⱡ̈ ßⱭ̈¹
ß TÛ̈2¿̈ƒF Å̈ⱡ̈ ßJ ⱠⱭ̈të ⥾ⱭⱤ̈ RⱭ̈

    ßaßⱭ̈ⱷ̈ «@¸¶›

	ßⱭⱡ̈Ãr	î¦_"p
ß§F¹ss §c»jⱭ̈Eu#		î=4
ß§F¹ssⱭ̈,§Ç̈v$Ó̈ⱭⱠ̈Þ̈Œ:ⱭⱠ̈=4Eô̈		
ß§F¹ssⱭ̈ §c»jⱭ̈Eu#		Ò€.ⱡ̈÷4
ß§F¹ssⱭ̈,§Ç̈v$Ó̈ⱭⱠ̈ÞⱭ̈Œ:ⱭⱠ̈=		
ß§F¹ssⱭ̈ §c»jⱭ̈Eu#Ò€.Ý̈·9è–		
ß§F¹ssⱭ̈,§Ç̈v$Ó̈ⱭⱠ̈Þ̈Œ:ⱭⱠ̈ⱷ̈«-E		

ßUªp   » ù®ë(Þ"W"Ñ´Åì ¼Ü'¢‰þxÉB¼**9**‡—m௺é9ØW
ßÚ<x¦%ýîmø#q¬ËV̊ỏ0ô̂@W"JÁ;¾4̓-Šn/"ðð/Æ}̈3 Yø¤î-
ß<[6qŨ¾¯s(e û-çÛ̂ŸU®ë%̂ÛTtẗe7-5$ž»|œ, è.̂îGKwE
ßž;5ÕMÇ<@•̋Ẑ6ảĨe&æ#B̂Ỏᵗ Àýž=$EºŜ^êrÝ·kWAúY̌g•
ßD¹ P:v] h Þ̈ ¬¬€jžô Þ4 /´^̂ ̌Õ̓' ü Ü Ǎ̈Ũ Êq
ßúÕóÚä"×Q̧EÕŠ?ô̧ỚÍ LeÝ3ᵢȀC]F4®xí D{̄—g[W̄¬
ßûȖ̂ȰXe)f£SPk·XҊo!ÖÕÖö1l`4Ý} • Šyû̂ ̧ø4̂ %¾Yø¤î-
ßÛ¶nl©¨àȖ7¶ñhà•Ò-ÑÅ¾ÿẢ4bNÃKµ>"³•øÎ̞ᵢ3M̧Ö¾C,
ßÛySñ¾45ù4Ž̧RÚ̂ô1ð÷ïf₤Õ¢ß4·pJ´ 2›Q̧ÂJ»E úäsèCU
ß©,¹~ à¦Ï"Ð̧¿th ~·1õ̇e^›PÈ̃Œ¶Ǎ̈ᵒ ̌ Ìïpøä̂A̧_... ßW–
ßû%Nᵢ̋3‡ÿò´¾ø©῟q   ßYᵇᵒL .± Æmë ZI³?O;øÎG@̇+
ßž<Z̧Þç$´ņ̃ÃK\—ÑÅ̂Î̈Â†;Á̂^\m"eíÕ@£

ßß   ßÅU©™B A0ÍÖáÒ"…"

        ß̄ÓÐpIºLpI¹%Ã̧Æ̧ ̓Ǎ̇R ̓Ò̂ᵗ̓Ñ̈l ð%̧̃ᵈ7–Ž̧ÒÚ ¥mõ=e
ßi²̧.̧.̧̧çŽÈ T̈ö \5ᵢᵈI ᵢ2₄̧.žᴺ$7›p"`̀ | u¼ẍ᷑ ¹ ‡kÂ̇• SỄe̋D
ß { ¨Š®ᵉ±ᵈ̋Ħé €̧¤₄ -„¾̧ốÍ$Ệ •;x ¡ | | £Q̧•, ̄â̧̇-K̇æ
ßŠ÷ •̇X̊K+X̣§ š\̄–᷈ ᵍ ´´̇ïKž >/Ô̇4 Kᴮᵈ3N¹₄ᵢ̧ŜÝ Íᶜmü̧Æᴱ5Ẻᶜ{
ᶜÇ̧ÙᶠȞ̊fy;e•Ê̄=â̇̄ ₤̄-̧i Æ Fj é̄ ̄êï a¨Z̄-ß ̄Ī–Ý $ÀḚ̂ =[Ą̇
ß¤Å̧Ī-[Q M̧ᶜíí –o"kDt Š ₍ᵀ̧T„*Nᴹ᷒Ḉ̧Hᵃaẫ 0 ¾9 9̣Ě̊ᵢ °̍ {
ß̇Ì5Ḑᵈᵃ —xŠ̃üW̧Ī@ ̓UzN Í(S®É §Ìž zÊᵢ̇ÀC¡ø u¤Ž̧
ß {èú. "S P ê ý£) Ṁ̊ «Ï̈» Í Êᵃ ø J 4 á £᷈᷈(ᵈ̧ᵢ ì̧ • ;
ß̇Š̈ ̄ u̧Ỡ̌³s ᵀ̇E̋X̧k•Ê̇@̇ í I£±q3m̧/]Ė̇ÙQ̧+ S̋-⅛ȩ́̇•-5-̂Ǫ̧3̧¾Ö̧)
ß ᶠȨ̂ẓ̃~j̊5̧Y̧2ᵢ ¤yø ò ÷·Ü̧ʄ¦é R̥̩ ¼ᵃ̇Ẏ̋øᵍ̧ ¡¼0 ´§̊ž ̄÷{ þ Þ

ß+¼ »^̌«HQ[Mÿ

ßaYQIUx

ß+   »ô…ü±r?̧Ƈ,¼°ê ÚRᵃ8
ß+   »†óý OCÒ^ĻƒÇõ̃j*à•• ᵞ ᵣMÉ3TÎ½" ð
ß+   »†…ŽÊ¾‰M̧§Ya`Ë-†ñká ̄ ” {›Þ´Ǟ•
ß+   »ô…ᵢl᷀9-ᵞ̈\™Ņᴀᴛᴇ̃̃-̧Søᵢ pÍ
ß+   »(eᵞ̇Ð W̧ᵢ̇ó·m̊ᵒRÈ¼ù%̊Đ½Ḛ̇Ḩ̂ᵢÉᵢP, Öm̧ⅭᴬᵢŞ/ƒÖ
      ßÓ—‹ÇṦᴹᵒḈ̇P• Œ
ß+   »mᵃ• ,3é$è$è%Ņ̃ÅÅwî̂-Â<¦Š̃mçÂ È—Q̧₅ḣ̇S̄
      ß‰œ]È̋} Å̊ᵒ̇®Ü©•

ß̃q̧ÓÄ†ßV [Oß̈ÏF̧ƒ8̇¤á ᵇ'b̄Ëveß Æ)&tüä•q9úø°
ßúÕóÚä"×Q̧ᵢ̧õ†Ã̇•NÓ‡SFûî)iFÎ̇9DÜ9Ñ<¦?ᵢ?oMᵣ̧ᵐ¤
ßÛ=Ûx.ã

ß†.³Üýí L̤ᵋ̇ô̧.¬p«o̧ᵃ̧pᵍ̧d p%̧ᵇ̧Äü„̧ï̧₄̧õ`áL3-Î̧̇ÿ/Æ̋u̧_@̧ᵇ̇Y,
ßÜµ6̧Ǫ̧ä¤ȩŸ̇ᵒ̇Ẫ

ß–q̧̊L EÛ™̧ĮꝐ0ä"²ï çÁ ß
ß
ßž< ìÒᵇ^>zᵢ̧§ủÎ̇'Ꝑ̧Ò̧ᵢ̤̈̕Ņ̇ᵤ6q®d,u€
ßž<w–á̧Ỹ̇y:KLþ;ðä '

For each rule R like containing x on LHS
{
//Check whether Mconfidence of the rule
//goes below MCT or not.
While (Mconfidence (R)>=MCT)
// increase the hiding counter of
// rule R by 1
{
Hiding_counter(R)=Hiding_counter(R)+1
}
}
}

End of procedure: Output the rules which do not contain sensitive elements on the left hand side.

4.2   Example

        Suppose we have given a database of transactions [7] as below

TID	Items
T1	ABD
T2	B
T3	ACD
T4	AB
T5	ABD

        We have also given a MST of 60% and a MCT of 70%. We can see four association rules can be found as below

AB   (60%, 75%)
BA   (60%, 75%)
AD   (60%, 75%)
DA   (60%, 100%)

Now we have to hide D and B.

4.2.1   By previous methods:
We can see that by simple ISL algorithm if we want to hide D and B, we check it by modifying the transaction T2 from B to BD (i.e. from 0100 to 0101) we can not hide the rule D   A.

T1	ABD	1101
T2	B	0100
T3	ACD	1011
T4	AB	1100
T5	ABD	1101

↓

        So by above explanation we can see that rule D   A can not be hidden by ISL approach because by modifying T2 from B to BD (i.e. from 0100 to 0101) rule

D   A will have support and confidence 60% and 75% respectively. Now we will check it by DSR approach.

T1	ABD	1101
T2	B	0101 ←
T3	ACD	1011
T4	AB	1100
T5	ABD	1101
↓		
T1	ABD	→ 0101
T2	B	0100
T3	ACD	1011
T4	AB	1100
T5	ABD	1101

We see bye DSR approach rule DA is hidden as its support and confidence 40% and 66% respectively, but as a side effect the rule A   D is also hidden. Similar is the condition for BA.

4.2.2   Our Approach

T1	ABD
T2	B
T3	ACD
T4	AB
T5	ABD

(Msupport, Mconfidence, Hiding, Counter)
AB →(60%, 75%, 0)
AD→(60%, 75%, 0)
DA→(60%, 100%, 0)

↓   First we hide B

T1	ABD
T2	B
T3	ACD
T4	AB
T5	ABD

(Msupport, Mconfidence, Hiding Counter)
AB → (60%, 75%, 0)
BA → (50%, 60%, 1)← rule is hidden
AD→ (60%, 75%, 0)
DA→ (60%,100%, 0)
↓   Now we hide D

T1	ABD
T2	B
T3	ACD
T4	AB
T5	ABD

Msupport, Mconfidence, Hiding Counter
AB →(60% , 75% , 0)
BA →(50% , 60% , 1)
AD→(60% , 75%, 0)
DA→ (43% , 60% , 2)← rule is hidden

6.   Conclusion

As from our example, we see that our approach is better in the way that it hides rules which can not be hidden by some of the previous works. We see in the example that proposed method is hiding the given association rules (with sensitive items on the left hand side of the rule) without any side effect.

Our algorithm is also simpler in the sense that we have to do only one step of modification as we are only incrementing the hiding counter each time(to decrease the confidence of sensitive rule) rather than checking all transactions again and again and ordering them in increasing or decreasing order as required by some of the previous works(which work on the basis of reducing the support and confidence of the sensitive association rules).

References

1.   Shyue-Liang Wang, Yu-Huei Lee, Steven Billis, Ayat Jafari "Hiding Sensitive Items in Privacy Preserving Association Rule Mining" 2004 IEEE International Conference on Systems, Man and Cybernetics.

2.   Vassilios S. Verykios, Ahmed K. Elmagarmid, Elisa Bertino, Yucel Saygin and Elena Dasseni "Association Rule Hiding", IEEE Transactions on Knowledge and Data Engineering, Vol. 16 No. 4, April 2004.

3.   Yucel Saygin, Vassilios S. Verykios, Chris Clifton "Using Unknowns to Prevent Discovery of Association Rule" SIGMOD Record, Vol. 30, No. 4, December 2001.

4.   Chris Clifton, Don Marks "Security and Privacy Implications of Data Mining", In Proceedings of the 1996 ACM SIGMOD Workshop on Data Mining and Knowledge Discovery.

5. R. Agrawal and R. Srikant, "Privacy preserving data mining", In ACM SIGMOD Conference on Management of Data, pages 439450, Dallas, Texas, May 2000.

6. Yi-Hung Wu, Chia-Ming Chiang, and Arbee L.P. Chen, Senior Member, IEEE Computer Society Hiding Sensitive Association Rules with Limited Side Effects IEEE Transactions on Knowledge and Data Engineering, Vol. 19, No. 1, January 2007

7. Shyue-Liang Wang, Ayat Jafari "Hiding Sensitive Predictive Association Rules", Department of Computer Science, New York Institute of Technology, New York USA.

8. Shyue-Liang Wang, Rajeev Maskey, Ayat Jafari One Scan Sanitization of Informative Association Rules.

9. R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases", In Proceedings of ACM SIGMOD International Conference on Management of Data Washington DC, May 1993.

10. S. Oliveira, 0. Zaiane, "Algorithms for Balancing Privacy and Knowledge Discovery in Association Rule Mining", Proceedings of 71h International Database Engineering and Applications Symposium (IDEAS03), Hong Kong, July 2003.

11. Wu, Y.H., Chiang, C.M., and Chen, A.L.P. Hiding sensitive association rules with limited side effects. IEEE Transactions on Knowledge and Data Engineering, 2007, 19(1):29-42.

12. Fienberg, S. and Slavkovic, A. Preserving the confidentiality of categorical statistical data bases when releasing information for association rules. Data Mining and Knowledge Discovery, 11(2):155180, 2005.

Comparative Performance Analysis of Load- Balanced Clustering in Wireless Sensor Networks (WSNs)

Dr. Raj Kumar*
Sharad Goyal

ABSTRACT

The advancement of the technology has increased the potential use of wireless sensor networks (WSNs) in a number of ways, such as in environmental control in office buildings, robot control, guidance in automatic manufacturing environments, interacting toys, and the smart home etc. In this paper, an evaluation on the basis of effectiveness as well as their deficiencies has been done on the most important areas of wireless sensor networks such as load balancing techniques based on clustering. A new clustering scheme named Net Clustering is proposed that may reduce the power consumption as well as network lifetime problem.

Keywords: Wireless Sensor Networks, Clustering, Load Balancing, Inter-Clustering

1. Introduction

Wireless sensor networks (WSN) have emerged as one of the most exciting fields in Computer Science research over the past several years. Sensor is a small, lightweight device which measures the environment of physical parameters such as temperature, pressure, relative humidity. Sensor Networks are cheap, smart devices with multiple onboard sensors which are networked through wireless links and the Internet. These are highly distributed networks of wireless sensor nodes, deployed in large numbers to monitor the environment or system. The quality of a sensor network is given by the coverage area it covers and the exposure. Coverage depends on the range area it covers, sensitivity and density of the sensing nodes. Exposure defines the ability of observing a target in the vicinity of the sensor node. The broad application areas of WSNs can be described in the fields of tracking contaminations in hazardous environments, habitat monitoring in the nature preserves, military sensing, enemy tracking in battlefield environments, building surveillance & monitoring, physical security, industrial & manufacturing automation and distributed robotics etc.

2. Clustering

Since grouping of nodes into clusters has been the most general technique for supporting the scalability and the increasing the lifetime of the WSNs. Clustering is an important mechanism in large multi-hop wireless sensor networks for obtaining scalability, reducing energy consumption and achieving better network performance. It is an effective mean for managing such high population of nodes. Most of the research in this area has been focused on energy-efficient solutions, but has not been thoroughly analyzed the network performance in terms of data collection with respect to time. Out of number of approaches one of the successful approaches for tackling the maintenance of these networks is by decomposing the network into clusters. Since clusters are manageable, intra-cluster maintenance is done tightly, while inter-cluster connectivity is reduced by orders of magnitude this way. Clustering is commonly used in order to limit the amount of routing information stored and maintained at individual hosts. Cluster-based network is divided into subsets. Each group of nodes contains a single leader (cluster head) and several ordinary nodes. The main objective of clustering is to minimize the total transmission power

*Asst. Professor Gurukula Kangri Vishwavidyalaya Haridwar

aggregated over all nodes in the selected path and balance the load of the nodes among the cluster heads to prolong the lifetime of the network. The main advantages of clustering such as increasing the network scalability, supporting the data aggregation, reducing the energy consumption etc., enhances the performance of Wireless Sensor Networks (WSNs).
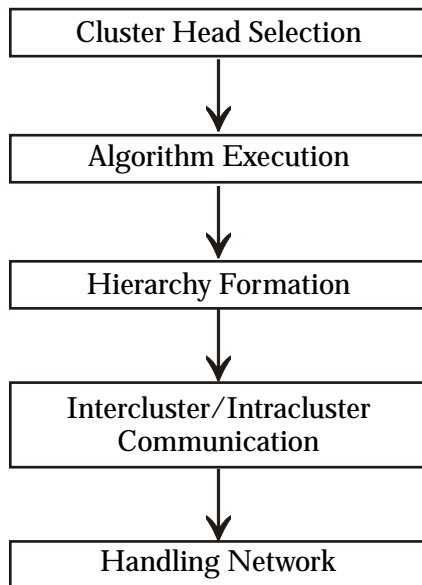
```
┌─────────────────────────────┐
│   Cluster Head Selection    │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│    Algorithm Execution      │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│    Hierarchy Formation      │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│  Intercluster/Intracluster  │
│       Communication         │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│     Handling Network        │
└─────────────────────────────┘
```

Fig 1. Clustering Process

2.1   Objectives of Clustering

Clustering algorithms in the literature differ in terms of their objectives. Often the clustering objective is set in order to facilitate meeting the applications requirements. For example, if the application is sensitive to data latency, intra and inter-cluster connectivity and the length of the data routing paths are usually considered as criteria for cluster head selection and node grouping. The main objectives for network clustering are:

- Load balancing
- Fault Tolerance
- Enhancing network connectivity
- Reduction in communication delay
- Maximizing the network lifetime

2.2   Advantages of Clustering

Increasing the network lifetime by changing the role using load balancing technique.
Reduce channel contentions and collisions.
It is more suitable for larger areas.

2.3   Disadvantages of Clustering

Overhead of cluster formation and maintenance Nodes which are near to cluster heads sometimes get overloaded and sometimes may get dead.

2.3.1   Load-Balanced Clustering

Since each cluster performs various data processing tasks so to take the optimal use of each cluster the load of network should be distributed equally among the all clusters. Given the duties of cluster heads, it is intuitive to balance the load among them so that they can meet the expected performance goals [1]. Load balancing is a more pressing issue in WSNs where cluster heads are picked from the available sensors [2]. In such cases, setting equal-sized clusters becomes crucial for extending the network lifetime since it prevents the exhaustion of the energy of a subset of CHs at a high rate and prematurely making them dysfunctional. Even distribution of sensors can also leverage data delay [3]. When CHs perform data aggregation, it is imperative to have similar number of nodes in the clusters so that the combined data report becomes ready almost at the same time for further processing at the base-station or at the next tier in the network.

Load balanced clustering [4] increases the system stability and improves the communication between different nodes in the system. The main objective of this approach is to cluster sensor network efficiently around few high-energy gateway nodes. Clustering enables network scalability to a large number of sensors and extends the life of the network by allowing the sensors to conserve energy through communication with closer nodes and by balancing the load among the gateway nodes. Gateways associate the cost, to communicate with each sensor in the network. Clusters are formed based on the cost of communication and the load on the gateways.

The setup of network is performed in basically two phases these are: Bootstrapping and Clustering.

In the bootstrapping phase, gateways discover the nodes that are located within their communication range. Gateways broadcast a message indicating the start of clustering. It is to be assumed that receivers of sensors are open throughout the clustering process. Each gateway starts the clustering at a different instance of time in order to avoid collisions. In reply, the sensors also broadcast a message with their maximum transmission power indicating their location and energy reserve in this message. Each node discovered in this phase is included in a per-gateway range set.

In the clustering phase, gateways calculate the cost of communication with each node in the range set. This information is then exchanged between all the gateways. After receiving the data from all other gateways each gateway starts clustering the nodes based on the communication cost and the current load on its cluster. When the clustering is over, all the sensors are informed about the ID of the cluster they belong to. Since gateways share the common information during clustering, each sensor is picked by only one gateway. For inter-cluster communication all the traffic is routed through the gateways.

To evaluate the efficiency of various approaches we have studied the performance of sensor networks applying various different routing protocols. After analysis, it is found that, among the various routing protocols, the clustering approach improves the scalability as well as lifetime of the networks. Clustering having the number of advantages and disadvantages too.

3.   Net-Clustering

While in active state, the sensor node consumes much energy from the battery. As sensors are battery operated; keeping the sensor active all the time will limit the duration of the battery. When the network is in setup state there are number of occasions when a particular sensor may not requires its operations. Therefore, optimal organization and management of the sensor network is very crucial

in order to perform the desired function with an acceptable level of quality and to maintain sufficient sensors' energy to last for the duration of the required objective. To achieve required objective organization of the sensor network should be such type that enables the appropriate selection of only a required subset of the sensors to be turned on and thus avoids excess drainage of the sensor's energy. Energy-aware network management [5] will ensure a desired level of performance for the data transfer while extending the life of the network.

We have used a novel approach called Net-Clustering in that we prepare a network with more groups of clusters of sensor nodes in a network. It is obvious that the cost of particular network will rise but quality of network will enhance several times as compared to installing the node only for required network. As one node will die due to any mishandling or power overloading/underloading, the remaining nodes will be active till the usage of network. Moreover, another advantage of this approach is that we can have this network setup for long time. If we compare the network setup cost with respect to time and quality of network, it will be more economical as well as more sound quality wise.

For example: Now a days traffic lights on the signals are installed with LED (Light Emitting Diodes). Each signal lights having bunch of LEDs and the input power of these LEDs is controlled by battery. As one light consists of no. of LEDs, if one or more LEDs are fused then the traffic light still goes on working for long time. The remaining LEDs which are in the ON state are sufficient enough to guide the person on the road. It is only due to the increased number of cluster of LEDs as compared to the single bulb system in a light.
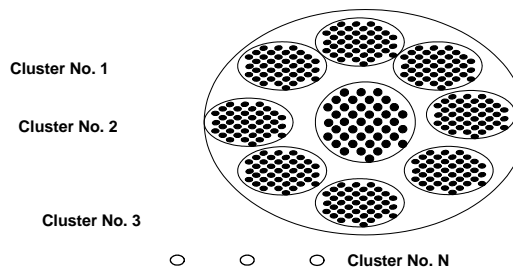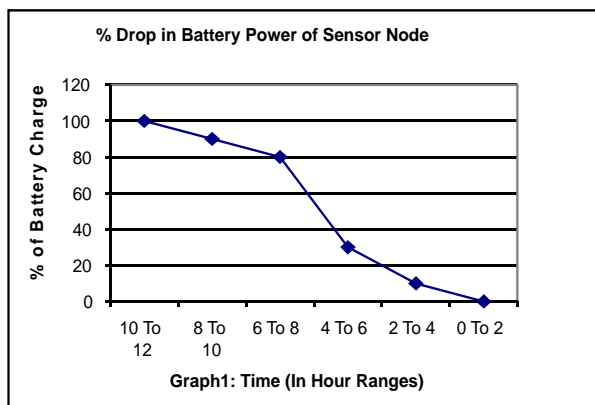

Fig 2. Inter-Clustering of Nodes

Table 1

Hours Range%	Drop in Battery Power	Remaining Battery Power
10 To 12	100	0
8 To 10	90	10
6 To 8	80	20
4 To 6	30	70
2 To 4	10	90
0 To 2	0	100

Explanation of Graph

In Table 1 and Graph 1, percentage drop in battery power has been shown. For making the graph, we have taken four mobiles of same made. Battery of all is fully charged and not a single call has been attended during the testing phase. Observations show that on an average each battery has a lifetime of 10-12 hours (in ideal conditions). The main outcome of this observation is that after about 7 hours the percentage drop of battery power suddenly increases to 80% which is non linear.

4.   Parameters of Performance

Since any network is composed of various associated devices, their attributes and characteristics vary according to the size of the area as well as network, location in which it is deployed, etc. So the performance of the network depends on various parameters which discussed below :

4.1   Network Partitioning and Lifetime of sensors

When the first node runs out of energy, the network within a cluster is said to be partitioned [5], reflecting the fact that some routes become invalid. However, it is difficult to precisely define the performance parameter. To study the impact of energy awareness on network lifetime the partitioning can broadly be described in two phases.

4.1.1   Pre-partition of Network

It is defined as the number of data packets sent and successfully delivered before network partition. Network is considered partitioned if all the given sources are partitioned from their respective target regions. In some sense, this performance parameter indicates the network lifetime.

4.1.2   Post-partition of Network

It is defined as some pairs of nodes in the network getting still connected after partition. From this parameter we can evaluate how much performance of the network is affected due to these joined pairs of nodes.

In [6] an approach for energy aware and context aware routing of sensor data has been defined. The approach calls for network clustering and assigns a less-energy-constrained gateway node that acts as a centralized network manager. Based on energy usage at every sensor node and changes in the mission and the environment, the gateway sets routes for sensor data, monitors latency

throughout the cluster, and arbitrates medium access among sensors. From the simulation, it has been observed that this approach can achieve substantial energy saving. Table 2 along with the time to network partition, gives an indication of network lifetime under various routing schemes.

4.2 Average Delay Per Packet

It is defined as the average time a packet takes from a sensor node to the gateway. Although energy is an important factor in sensor networks, in some critical applications it requires sensed data to be reported with minimum delay. As per a, study delay in the network may be of two types. It may be due to the broadcast nature of wireless medium or due to total delay.

4.3 Network Throughput

It is defined as total number of packets received at the gateway divided by the simulation time. This parameter gives a good idea of the efficiency of network traffic supported by each cluster in the network. A high throughput indicates that the system supports better routing for data and control messages.

4.4 Average Energy Consumed Per Packet

Minimizing the energy per packet will, in general, yield better energy savings. The energy constrained hand-held devices should be able to estimate the energy requirement of an application that has to be executed and make subsequent decisions about its processing ability based on user-input and sustainable battery life. Therefore, the concept of 'energy aware' software is integral to such systems. In [7] a simple energy model for software based on frequency and supply voltage as parameters has been proposed. The model incorporates explicit characterization of leakage energy as opposed to switching energy. A technique to isolate the two components has been demonstrated. The relative significance of these energy components under different duty cycle tasks has also been explored. The concept of energy aware software is introduced. A simple energy model for software is presented that separates the switching and leakage components and

predicts its total energy consumption with less than 5% error for a set of benchmark programs. The experiments have been performed on the StrongARM SA-1100 microprocessor. A mathematical model for the total leakage current has also been proposed and it has been shown that they can account for about 10% of the energy dissipation for low threshold voltage microprocessors and, assuming continuous operation, the leakage energy fraction gets significantly higher for lower duty cycle

4.5 Power Consumption in the Network

Since transmission of data in the network consumes energy, the more the transmissions in the network, the more energy will be consumed. This situation will be significant when the scale of the network is large, say thousands or more of nodes. This parameter is an average of power consumed taken at different instances of time during the network.

4.6 Standard Deviation of Load per Cluster

For testing the reliability of the system, standard deviations for different sensors densities is calculated of load by using 5 gateways and increasing the number of sensors in the system from 100 to 500 with uniform increments.

5. Comparative Performance Evaluation of Studied Routing Approaches

5.1 Energy-Aware Routing

Sensors messages are routed through multiple hops based on the current energy level of the sensors, distance, delay, in-out traffic, etc. [6]. LEACH [8] proposes a clustering based protocol that utilizes randomized rotation of local cluster heads to evenly distribute the energy load among the sensors in the network. It is similar in spirit with other energy aware routing protocols in terms of load balancing. However, their underlying assumption is different from ours. They assume adjustable transmitting power and assume that the cluster head talks directly to the gateway node. We assume each node has fixed transmission power optimizing transmission power in a multi-hop network is outside the scope of this paper.

5.2   Minimum-Hop Routing

A packet is forwarded to the gateway using the minimum number of hops in the cluster.

5.3   Direct Routing

Messages are directly transmitted to the gateways. No intermediate hops or routes are created in the system.

5.4   Minimum-Distance Routing

This approach favors the use of a closer node as a hop, leading to a longer end-to-end delay.

5.5   Minimum-Distance Square Routing

Routes are set favoring closer hops, with the objective of minimizing the sum of the square of inter-hop distance.

5.6   Linear-Battery Routing

Minimize energy consumption assuming linear battery discharge model [5].

Table 2. Relative Performance Summary of Routing Techniques Studied

S. No.	Performance Parameters	Routing Techniques						
		Energy Aware	Minimum Hop	Direct	Minimum Distance	Minimum Distance Square	Linear Battery	Load Balanced Clustering
1	Network Partitioning And Lifetime of Sensors [4]	Improved by factor 2	Improved by factor 2	No Change	No Change	Improved by by factor 7	No Change	Improved by by factor 4
2	Throughput of the System [4]	No Change	No Change	No Change	No Change	No Change	No Change	No Change
3	Average Delay per Packet [4]	Produce 1/2 delay as Shortest Distance	Produce 1/2 delay as Shortest Distance	No Change	No Change	Performs better than Load Balanced Clustering	No Change	Produce 1/2 delay as Shortest Distance
4	Average Energy per Packet [4]	Load-Balanced Clustering is 1.24 times better	Load-Balanced Clustering is 1.24 times better	Load-Balanced Clustering is 1.17 times better	Load-Balanced Clustering is 1.17 times better	Load-Balanced Clustering is 1.17 times better	No Change	No
5	Power Consumption in network [4]	No Change	No Change	No Change	No Change	No Change	No Change	Conserve more than 1.5 times

6.   Conclusions

Survivability is a very important criterion for deciding the efficacy of network. It includes a measure of the network lifetime as well as the kind of service it provides during its life. Both these factors are important in evaluating networks and neither can be considered in isolation. For example a network that does not forward packets at all satisfies the first condition and one that just burns itself out fast trying to ensure full reliability would satisfy the second one. This paper defines the various novel distributed inference schemes, for efficient clustering in multi-hop WSNs. The objective of each scheme is to select

the cluster heads that minimize the overall transmission cost and at the same time balance the load among the nodes, for a longer network lifetime. Evaluation of all available information, is better and leads to a significant improvement in the network performance.

References

1. M. Younis, K. Akkaya, A. Kunjithapatham, Optimization of task allocation in a clusterbased sensor network, in: Proceedings of the 8th IEEE Symposium on Computers and Communications (ISCC'2003), Antalya, Turkey, June 2003. Workshop on Sensor Networks (EWSN), Berlin, Germany, January2004.

2. O. Younis, S. Fahmy, HEED: A Hybrid, Energy-E.cient, Distributed clustering approach for Ad Hoc sensor networks, IEEE Transactions on Mobile Computing 3 (4) (2004) 366379.

3. S. Banerjee, S. Khuller, A clustering scheme for hierarchical control in multi-hop wireless networks, in: Proceedings of 20th Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'01), Anchorage, AK, April 2001.

4. Gupta G. and Younis M., "Performance Evaluation of Load-Balanced Clustering of Wireless Sensor Networks", Department of Computer Science and Elec. Eng., University of Maryland Baltimore County, Baltimore, MD 21250, 2003.

5. S. Singh, M. Woo and C. S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks", Proc. of ACM MOBICOM'98, Dallas, Texas, October 1998.

6. M. Younis, M. Youssef, K. Arisha, .Energy-Aware Routing in Cluster-Based Sensor Networks., in the Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS2002), Fort Worth, Texas, October 2002.

7. A. Sinha and A. Chandrakasan, .Energy Aware Software., Proceedings of the 13th International Conference on VLSI Design, pp. 50-55, Calcutta, India. January 2000.

8. W.Rabiner Heinzelman, A. Chandrakasan, and Hari Balakrishnan. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In Proceedings of the 33rd International Conference on System Sciences (HICSS '00), 2000.

9. Rahul C. Shah and Jan M. Rabaey, Energy Aware Routing for Low Energy Ad Hoc Sensor Networks, Berkeley Wireless Research Center, University of California, Berkeley

10. F. Zhan, C. Noon, .Shortest Path Algorithms: An Evaluation Using Real Road Networks,. Transportation Science, 1996.

11. J. Rabaey, J. Ammer, J.L. da Silva, D. Patel, "PicoRadio: Ad- hoc wireless networking of ubiquitous low-energy sensor/monitor nodes," IEEE Computer Society Workshop on VLSI 2000, Orlando, FL, pp. 9--12, April 2000.

12. W. Rabiner Heinzelman, A. Chandrakasan, and H. Balakrishnan, .Energy-Efficient Communication Protocols for Wireless Microsensor Networks,. Hawaii International Conference on System Sciences (HICSS '00), January 2000.

13. D. Estrin, R. Govindan, J. Heidemann, and S. Kumar. Scalable coordination in sensor network;ks. Proc. of ACM/IEEE MobiCom 1999, Seattle, Washington, August 1999

Emerging Trends in Software Engineering: Software as a Service

*Ashwini Kumar**
*Vishu Tyagi**

ABSTRACT

Software is everywhere - in devices in our pockets, in the vehicles we travel in, in our banks, hospitals and homes - and its correct operation is essential for our health and well-being. Over the past decade, software applications have grown significantly in terms of their size and capabilities.

Between now and 2025, the ability of organizations and their products, systems, and services to compete, adapt, and survive will depend increasingly on quality of software. As is being seen in current products (automobiles, aircraft, radios) and services (financial, communications, defense), software provides both competitive differentiation and rapid adaptability to competitive change. It facilitates rapid tailoring of products and services to different market sectors, and rapid and flexible supply chain management. The resulting software-intensive systems face ever-increasing demands to provide safe, secure, and reliable systems; to provide competitive discriminators in the marketplace; to support the coordination of multicultural global enterprises; to enable rapid adaptation to change; and to help people cope with complex masses of data and information. These demands will cause major differences in the processes currently used to define, design, develop, deploy, and evolve a diverse variety of software-intensive systems

Software engineering (SE) is about developing, maintaining and managing high-quality software systems in a cost-effective and predictable way. This paper is an attempt to educate the reader that in some cases traditional software applications remain the right choice, but in other cases deploying SaaS applications provide a better business case..

1. Introduction

SaaS is a software delivery model where instead of purchasing the software, users can rent the software on a monthly cost-per-user or usage basis and can scale up or down as needed.

Software as a service (SaaS, typically pronounced 'Sass') is a model of software deployment where an application is hosted as a service for the customers across the Internet. By eliminating the need to install and run the application on the customer's own computer, SaaS alleviates the customer's burden of software maintenance, ongoing operation, and support. Using SaaS can reduce the up-front expense on software purchases, through less costly, on-demand pricing.

From the software vendor's standpoint, SaaS has the attraction of providing stronger protection of its intellectual property and establishing an ongoing revenue stream. The SaaS software vendor may host the application on its own web server, or this function may be handled by a third-party application service provider (ASP).

The Software-as-a-Service (SaaS) revolution allows companies to subscribe to software applications and outsource operating the back-end infrastructure to the SaaS vendor. In most cases, the SaaS vendor can do this much more cost effectively; providing overall cost savings for the company. As a result, companies can spread their IT budget for many more applications to support and grow their business operations which will in turn contribute to the bottom line.

2. Features of SaaS

2.1 Rent Instead of Buy [6]

One of the downside of traditional software is the risk of buying an application that doesn't fit immediate and changing requirements. Either way, people are stuck with what they bought, and the only

*ABES Institute of Technology, Ghaziabad

solution is to buy new software. SaaS takes away this risk. If the application no more fits the requirements, the subscription just needs to be stopped. Another problem with traditional software is the difficulty of version control. Updates can be costly, and re-installation can be problematic. With a SaaS application, one always have the latest version every time they sign on.

2.2 Working of Software as a Service

Software as a Service or "on demand" applications refer to web-based software applications where the underlying hardware and software components are shared by all users of the application. The hardware that is used to run the software is not located at the customer's premises but in high-tech data centers and is managed by the provider of the service. Users gain access to the software interface through an internet browser. No software has to be installed on the user's computer and they don't need to worry about upgrades of the software or backups of the data that is saved.

SaaS is based on the principle of sharing: the sharing of resources, computer hardware, knowledge, and most importantly the sharing of cost. Typically, one pays for the software based upon usage, which usually translates into a monthly subscription. Basically, the software is rented instead of buying.

2.3 Safety and Security [4]

One of the greatest advantages of a Saas application is the safety and security of remote storage. Saas providers like Planet DDS have their servers in high security facilities, which are designed to house the servers of companies like Merrill Lynch and Bank of America. They are impenetrable without appropriate security clearance, and they can withstand the greatest of natural disasters. Additionally, a real time back-up of all data is co-located in a second facility. This type of security far exceeds that of a typical dental office.

2.4 SaaS is Ideal for Multi-Locations

Besides lower costs and greater sophistication, the greatest value of Saas in dentistry is undoubtedly the anytime, anywhere access to data.

Dentists who own or work in multiple locations are already taking advantage of this tremendous feature. Appointments can be made at anytime for any location. Central business functions, like billing and insurance management, can be done from anywhere or easily outsourced. Reports can evaluate practice performance by any and all locations.

Also, since only a browser and an internet connection to access the application is needed, it can be deployed very rapidly and can be scaled upward to any number of offices. And, if all that isn't enough, the ultimate reason for multi-locations to use SaaS is that it is a fraction of the cost of other solutions. The internet is the network, and the servers are owned and operated by the SaaS provider. There is no need for expensive hardware, costly networking, and outrageous communications costs.

2.5 Connectivity

Since SaaS applications are online, they can be easily accessed by anyone with security clearance. For instance, a bookkeeper or accountant need not come to client's office to gather production and collection information.

More importantly, SaaS allows direct patient communications. Patients can register online; they can view statements online; they can pay online. Appointment reminders can be automatically sent from information on the appointment scheduler. And, these ideas are only the tip of the iceberg.

The key characteristics of SaaS software can be summarized as [8]:

- Network-based access to, and management of, commercially available software activities that are managed from central locations rather than at each customer's site.

- Enabling customers to access applications remotely via the Web which obviates the need for downloadable patches and upgrades.

- Generally priced on a per-user basis, sometimes with a relatively small minimum number of users, and often with additional fees for extra bandwidth and storage.

3. Potential Applications of SaaS [2], [7]

With the features mentioned above, SaaS can assume different roles of software in an organization, such as:

3.1 Enterprise Software Application Business Functions

- Organize internal and external information.
- Share data among internal and external users.
- The most standard type of software applicable to SaaS model.
- Example: Saleforce.com CRM application, Siebel On-demand application.

3.2 Single-User Software Application

- Organize personal information.
- Run on users' own local computer.
- Serve only one user at a time.
- Inapplicable to SaaS model.
- Data security issue.
- Network performance issue.
- Example: Microsoft office suite.

3.3 Infrastructure Software

- Serve as the foundation for most other enterprise software application inapplicable to SaaS model.
- Example: Window XP, Oracle database.

4. Delivery Models for SaaS

Fig.1 shows various infrastructural delivery models for SaaS. SaaS sytems can be configured and delivered using any of these models to cover all deployment bases. SaaS software can be hosted as isolated tenancy, Hybrid tenancy or Multi tenancy.
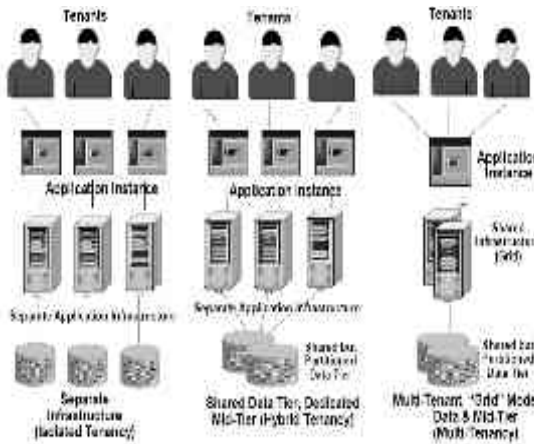
Fig 1. Delivery Models for SaaS

5. Ecosystem of SaaS

Fig.2 depicts various participants which make SaaS a reality for the users and all of which facilitate extending the services to a broader range of market and delivering a larger variety of customer solutions.
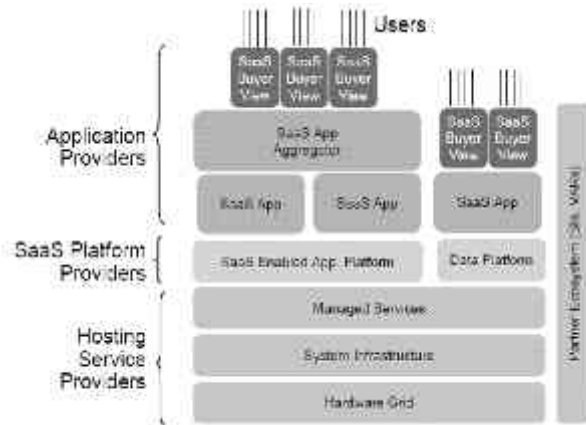
Fig 2. Ecosystem

6. Advantages [8], [11]

The advantages of SaaS over traditional software are substantial:

1. No upfront costs or risk if the application isn't right.

2. Lower hardware and networking costs. The internet is the network and one only needs a browser for access.

3. Safer and more secure data storage. Data is typically stored in highly secure locations and backup is instantaneous.

4. Anytime, anywhere access. One doesn't have to be in the office to see or work with their data.

5. No need to compromise on the software specifications. One is able to rent high-end software, instead of settling for a lesser product because of price.

6. Online collaboration with colleagues. Each one of them can look at the same data, at the same time from anywhere with internet access.

7.   Conclusion

This paper has presented, SaaS as a mature technology in a number of industries, and it has started to make inroads in dentistry. Since the Web is now woven into the lives of over one hundred million people in this country, it is inevitable that SaaS applications will become an important part of the dental and medical industry. One of the most compelling reasons for developing SaaS applications is the opportunity to implement alternative pricing models that focus on establishing and maintaining recurring revenue streams. Most SaaS vendors charge some kind of monthly "hosting" or "subscription" fee.

References

1.   Iod, Sotware as a Service, Kogan Page Ltd, 2002.

2.   E. TenWolde. Worldwide Software on Demand 2007-2011 Forecast: A Preliminary Look at Delivery Model Performance, IDC No. 206240, 2007. IDC Report.

3.   Frederick Chong, Gianpaolo Carraro and Roger Wolter, Multi-Tenant Data Architecture, MSDN Library, Microsoft Corporation, June 2006,

4.   Frederick Chong and Gianpaolo Carraro, Architecture Strategies for Catching the Long Tail, MSDN Library, Microsoft Corporation, April 2006,

5.   Robert Mahowald, Do Service Providers Deliver Value and Reduce Enterprise Costs?, IDC, 2003

6.   Robert Mahowald, Conferencing through Service Providers for Low Cost and Reliability, IDC Executive Brief, November 2003

7.   Geoffrey A. Moore, Living on the Fault Line, Revised Edition, HarperCollins, 2002

8.   Timothy Chou, The End of Software: Finding Security, Flexibility and Profit in the On Demand Future, SAMS Publishing, 2005

9.   Microsoft Wages Campaign Against Using Free Software, The Wall Street Journal, December 9, 2002

10.   MultiMedia Communications, A Detailed Analysis of "On-Premise vs. Service Provider" Costs and Risks, WebEx Communications, 2005

11.   Messaging Total Cost of Ownership: Microsoft Exchange 2003 and Lotus Domino in Small and Medium Organizations, META Group, July 2004

12.   Software as a Service, Wikipedia.org, July 2006

Rural Mobile Telemedicine Unit with Medical Image Processing System : A proposed model for Uttarakhand

*Dr. Durgesh Pant **
*Dr.M.K. Sharma ***
*Anand Singh ****

ABSTRACT

We have proposed a model for mobile telemedicine system, and discuss its applications and feasibility of implementing it in Uttarakhand. This paper presents technical considerations required to realize a practical mobile telemedicine system, techniques for multiple medical data transmission, and process to compress the multiple medical data using image processing software applications before transmission. The latter is necessary as we have limited bandwidth of network in the proposed model . The telemedicine system could be used in moving vehicles for remote / hilly states of India and other developing countries .

Keywords : Uttarakhand, Telemedicine, ICT ,Medical Image Processing, RTU , MTU , DICOM , MVE

1. Introduction

The condition of primary healthcare centers in Uttarakhand is not very good. Most of these exist for name sake only, with hardly any medical or para-medical staff. Because of difficult terrains it is not possible to set up hospitals in the area. In such a scenario, telemedicine can be a better solution to provide emergent aid to the 2.5 million   citizen of Uttarakhand. Telemedicine can be helpful to change the whole meaning of healthcare in hilly or remote regions .[1]

An effective telemedicine system with the help of computer and communication technologies can be designed for the hilly state of Uttarakhand, that should facilitate delivery of some health related services to remote / hilly areas. In this paper, we present a mobile health system, having medical image processing system and telemedicine applications for hilly / remote areas of Uttarakhand . First, we will identify functional requirements for a mobile telemedicine system.   Second, we describe the structure and functions of medical image processing system. Lastly, we discuss medical image processing methods that can be used to solve basic problems related with transmission of medical images in a telemedicine system .

2. Why Telemedicine for Uttarakhand

Telemedicine has been defined as the use of telecommunications to provide medical information and services. It may be as simple as two health professionals discussing a case over the telephone or as sophisticated as using satellite technology to broadcast a consultation between providers at different facilities in two countries, using videoconferencing equipment. Telemedicine is the practice of medicine over distance through the use of computers and telecommunications. Following can be the benefits of this model for Uttarakhand :

- Telemedicine can bring a geographically remote specialist into the actual examination room or operating room via a live inter-active system which is very useful for states like Uttarakhand .

- Telemedicine can electronically transport a vast range of medical care into remote areas from urban areas of state.

- Patients and physicians who live hours or days away from advanced medical care, or even basic services, can directly gain access to high quality medical expertise without leaving their native place, using telemedicine system .

*Professor & Head , Department of Computer Science Kumoun University , Nainitaal
**Asst. Professor, Department of Computer Science Amrapali Institute , Haldwani-(Uttarakhand) sharmamkhld@gmail.com
***Senior Lecturer , Department of Computer Science IMS   ,Dehradun -(Uttarakhand)

Video consultations from a rural clinic of Uttarakhand village to a specialist in Urban city like Delhi can alleviate prohibitive travel and associated costs for patients.

3. Design of Proposed Model

Telemedicine is defined as technologically facilitated remote consultation and diagnosis. Telemedicine systems are characterized by the type of information sent (such as clinical information, medical images, or on-line consultation) and by the means used to transmit this information using modem, local or wide area networks, Ethernet or by other form of network data transmission.
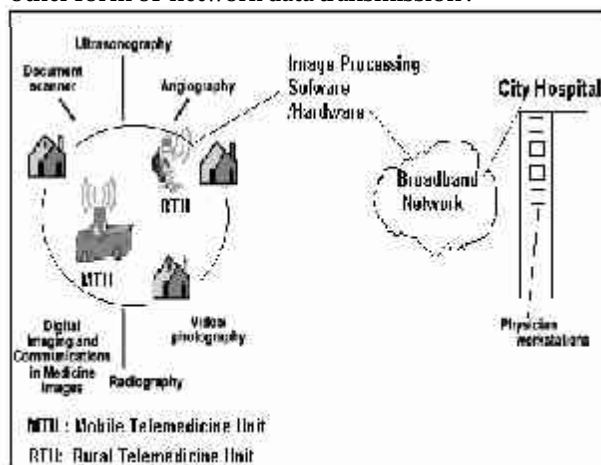

Fig 1 . Proposed Telemedicine Model for Uttarakhand with Image Processing Unit

The proposed model shown in Fig 1, will be an ICT based mobile telemedicine system, which will work as an emergency health care unit for urban and rural areas of Uttarakhand state. The system consists of two major parts. First is a Rural Telemedicine Unit (RTU) or Mobile Telemedicine Unit (MTU), that may be portable (easily movable) and located at the patient's site, and second is a base unit or doctor's unit located in a medical monitoring hospital. Communication between the two units can be established using wireless digital cellular, radio packet or ordinary fixed telephone lines.

3.1 Telemedicine Workstation

In order to provide medical care, especially in remote areas, we need to use a flexible, cost-effective telemedicine workstation. The purpose of telemedicine is to link district hospitals, city clinics, and remote locations to enable health care providers to exercise their expertise at the location of the patient or other doctors, using a combination of video, audio, and externally acquired images. The telemedicine system should give remote telemedicine unit a better access with urban health units and help to manage limited health care resources more effectively. Possible applications of this unit include ultrasound examinations, radiology, pathology, endoscopy, dermatology etc .

3.2 Telemedicine Data Transmission Network

The telemedicine workstation should be a single board multimedia system capable of digitizing audio and video, displaying up to 1280 x 1024 pixels, on high processing operations per second using a multimedia video processor. Workstation will use a network card such as an asynchronous transfer mode (ATM) interface adapter, so that the system is able to transmit and receive video, audio, and medical images at a fast speed. For high-bandwidth applications, the workstation should encode video using the Motion Picture Experts Group (MPEG) standard and for low-bandwidth links, the International Telecommunication Union (ITU) H.320 standard for video conferencing can be used.

3.3 Medical Image Processing Unit

Basic image manipulation functions such as 90 degree rotations, horizontal and vertical flip are essential to correct the errors in image acquisition and assure that images can be presented to the clinicians in a way that they are accustomed to viewing them. Zooming and panning are necessitated by the limited spatial resolution of CRTs when compared to X-ray films. Real-time window/level (brightness and contrast adjustment) is required because of the need to interactively examine medical images with more than 8 bits/pixel by adjusting the range (window) and the center position (level) in the wide input dynamic range. In the case of diagnostic video, manipulation functions such as play, record, pause and rewind are

important for simulating the VCR environment often used in ultrasound consultation.

4. Study of Earlier Work

Two telemedicine workstations were connected between the University of Washington and Madigan Army Medical Center (50 miles from the university) in January 1995 and demonstrated to a group of physicians from the University of Washington, Madigan Army Medical Center, and Seattle Veteran's Administration Hospital. A workstation, a Fore Systems (Warrendale, Pennsylvania) ASX-200 ATM switch and a DS-3 connection to a US West regional fiber ring supporting ATM over synchronous optical network (SONET) were installed at each site. X-ray, CT, and MR images were exchanged, manipulated, and discussed interactively between the two sites. Ultrasound video was acquired, compressed at one site, transmitted, decompressed, and displayed at the other site in real time using MPEG-1 at 30 frames per second (FPS). The general response from the physicians was positive, particularly with regard to the image quality, real-time MPEG video, and responsiveness of the system. Also, several areas for improvement were identified. Most significantly, the host central processing unit (CPU) (i486) and host buses (VL and EISA) of each workstation proved to be a bottleneck, limiting image transfer throughput to 13-15 Mb/s out of the 45 Mb/s DS-3 services .

5. Medical Imaging and Communications Standards/Software

5.1 DICOM

The Digital Imaging and Communications in Medicine (DICOM) standard was created by the National Electrical Manufacturers Association (NEMA). Its aim is to support the distribution and viewing of medical images from CT, MRI and other medical modalities. The DICOM format is an extension of the older NEMA standard. A DICOM file contains a header and the image data. The header stores information about the patient's name, the type of scan, position and dimension of image and lots of other data. The image data part contains all the image information. The ANALYZE format stores the header (*.hdr) and the image data (*.img) in separate files. The DICOM image data can be compressed in contrast to ANALYZE data either lossless or lossy in order to reduce disk space. DICOM is the common standar for scans in hospitals [13].

5.2 Medical Volume Explorer (MVE)

MVE is a visualization program for medical data. It is based on OpenGL, GLScene and on Cg shaders from NVIDIA.The program supports different 2D views (axial, coronal and sagittal), Direct Volume Rendering, Maximum Intensity Projection (MIP) gradient lighting and a stereoscopic anaglyph visualization. MVE has a multi format file interface for CT, MRI, PET and SPECT data and can read DICOM, ANALYZE, BMP, GIF, JP2000, JPG, PNG, PCX, PNG, TGA and TIF files.

The Volume Viewer as the main module displays 3D data directly without further conversion of the geometry like surface construction algorithms (marching cubes). The result is a natural and clear representation of the volume data. The volume object can be rotated and scaled in real-time and viewed as a stereoscopic image. MVE is divided into 4 modules :-

1. File Viewer for selecting and opening files.

2. Image Viewer for 2D visualization of axial, coronal and sagittal images.

3. Volume Viewer for 3D visualization with "Direct Volume Rendering" of the whole volume including very high resolution (512 x 512 x 512 voxels), clipping volumes with any angles, maximum intensity projection (MIP), stereoscopic anaglyph visualization.

4. Information Viewer for information about DICOM and ANALYZE files.

The program is freely available for medial, academic, research and educational use [14].

5.3 Sample Image Processing in DICOM Standards

People familiar with the medical imaging typically talk about the 'window center' and the 'window width' of an image. This is simply a way of describing the 'brightness' and 'contrast' of the image. These values are particularly important for Xray/CT/PET scanners, which tend to generate consistently calibrated intensities so a specific C:W pair for every image can be used (e.g. 400:2000 might be good for visualizing bone, while 50:350 might be a better choice for soft tissue). Note that contrast in MRI scanners is relative, and so a C:W pair that works well for one protocol will probably be useless with a different protocol or on a different scanner. Fig 2 illustrates the concept of changes to 'window center' and 'window width'. Along the top row three views of the same image with different C:W settings can be seen. The bottom row illustrates the color mapping for each image (with the vertical axis of the graph showing rendered brightness and the horizontal axis showing the image intensity). Consider this image with intensities ranging from 0 to 170, a good starting estimate for this image might be a center of 85 (mean intensity) and width of 171 (range of values), as shown in the middle panel. Reducing the width to 71 would increase the contrast (left panel). On the other hand, keeping a width of 171 but reducing the center to 40 would make the whole image appear brighter.
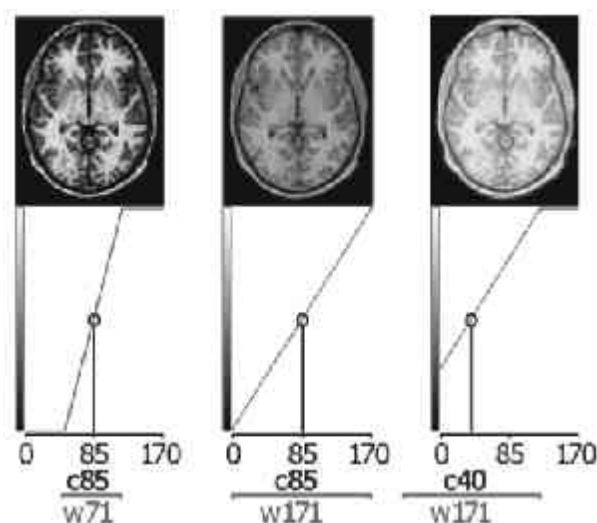

Fig 2. Concept of changes to 'window center' and 'window width' in DICOM

5.4 Some Free DICOM Viewers

My free ezDICOM software runs on Windows computers. Available as a standalone Windows program or as an ActiveX component (allowing plug-and-play use with Delphi, Visual Basic, C#, Visual C, Internet Explorer and other ActiveX aware programs). It is able to display most types of DICOM image (many other viewers are limited to showing uncompressed grayscale DICOM images) and can automatically detect and open Analyze, DICOM, Genesis, Interfile, Magnetom, Somatom and NEMA images. ezDICOM is part of the Sourceforge community.

MRIcro is my freeware for Windows and Linux. MRIcro can view Analyze, DICOM, ECAT, Genesis, Interfile, Magnetom, Somatom and NEMA images and convert them to the popular Analyze format. This program uses the same dicom.pas Pascal unit as ezDICOM, but includes a number of additional features. It is more difficult to use than ezDICOM, but also more powerful.

MRIcron is my open source successor to MRIcro. It runs on Windows, Linux and Macintosh. The included dcm2nii can convert DICOM images to the popular Analyze and NIfTI standards.

Julius is a free DICOM viewer/browser and volume renderer for Windows and Linux computers. Julius is not only a DICOM viewer but also a software framework for medical applications.

FP Image is a free DICOM viewer/browser for Windows that can also anonymize images.

Rubo Medical Imaging has a free demo of their Windows DICOM software, with some functions disabled.

Inviweb has a free version of their Windows DICOM viewer.

Able Software has a free version of their "3D-Doctor" Windows software, with some functions disabled.

5.5 DICOM Servers and Clients

PacsOne is a free Picture Archive and Communication System (PACS) for Windows. It contains a DICOM server, a PACS server (using MySQL) and a web server (Apache).

K-PACS aims to deliver a DICOM viewer and storage system, modelled after the previously free E-Film.

PACSview and ACRNview are free Windows programs with command line Unix programs available.

The Mallinckrodt Institute of Radiology distributes their Central Test Node (CTN) software. They also include documentation.

Tiani distributes JDicom: a set of free Java tools that include some useful DICOM file sharing utilities.

SimpleDICOM is a free DICOM client and viewer.

MIND is a free DICOM query/move tool for Windows NT and most UNIX platforms.

6. Conclusion

It goes without saying that the delivery of health care will change over the next few decades and, in all probability, even over the next five years. It seems that advances in IT and telecommunication services will be a foundation on which these changes will be transported and delivered. IT and Telecommunications will play an especially important role in rural health care delivery that will be unparalleled. This is in a large measure due to the sparse population density coupled with the fact that there will be only a few major centers of advanced care in these rural areas. It is not easy to setup high cost telemedicine units on many locations in Uttarakhand, particularly in many hilly and remote areas where the communication and transportation infrastructure has not been available yet. Deployment of the system could be very problematic especially in case of emergency or natural disaster such as land sidings, earth quake and heavy rain . Most of the population

of Uttarakhand is spread out in hilly areas. Because of the demography condition of state, a mobile and/or movable system will be demanding because a fixed system is difficult to be reached by patient living in remote urban or rural area, as the band width available for communication network is low, we need good medical image processing and compressing software applications as a part of that telemedicine mobile units. To cut cost of this model, we have suggested some free available software to start with a demo project .

References

1. Pant & Sharma, "Doctors are getting 'wired' in novel ways to benefit Uttaranchal Citizen using Telemedicine services" , CSI Communication , Vol. 30, ISSN 0970-647X, pp. 40-42 , Feb 2007

2. Vaisla & Sharma "Connecting urban doctors and rural patients," Communications News, Vol. 31, No. 2, pp. 26, 29, 1994.

3. Guttag, R. J. Gove, and J. R. Van Arken, "A single-chip multiprocessor for multimedia: The MVP," IEEE Computer Graphics & Applications, Vol. 12, No. 6, pp. 53-64, 1992.

4. "MPEG-1 CD, Committee Draft ISO/IEC 11172, Working Group 11," International Standards Organization, IPSJ, Tokyo, Dec. 6, 1991

5. R. Handel, M. N. Huber, and S. Schroder, ATM Networks: Concepts, Protocols, Applications, Addison-Wesley, Reading, MA, 1993.

6. M. L. Hilton, "Wavelet and wavelet packet compression of electro cardiograms ,"IEEE Trans. Biomed. Eng., vol. 44, pp. 394402, 1997.

7. S. M. S. Jalaleddine, C. G. Hutchens, R. D. Strattan, andW. A. Coberly, "ECG data compression techniques-a unified approach," IEEE Trans.Biomed. Eng., vol. 37, pp. 329343, 1990.

8. J. C. Lin, "Applying telecommunication

technology to health-care delivery, "IEEE Eng. Med. Biol. Mag., vol. 18, pp. 2831, 1999.

9. Z. Lu, D. Y. Kim, and W. A. Pearlman, "Wavelet compression of ECG signals by set partitioning in hierarchical trees algorithm," IEEE Trans.Biomed. Eng., vol. 47, pp. 849856, 2000.

10. A. Said andW. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," IEEE Trans. Circuits Syst.Video Technol., pp. 243250, June 1996.

11. D. S. Taubman and M. W. Marcellin, JPEG2000 Image Compression Fundamentals, Standards and Practice. Boston, MA: Kluwer, 2002.

12. M. Vetterli and J. Kovacevic, Wavelets and Subband Coding. Englewood Cliffs, NJ: Prentice-Hall, 1995.

13. [http://www.medical-image-processing.info /DICOM/index.htm]

14. [http://www.medical-image-processing.info/MVE/index.htm]

Binary Image Mapping for Digital Rights Management with Computer Graphics: Theory, Practice and Approaches

Simab Hasan Rizvi *
Aditya Kumar Gupta **

ABSTRACT

Open literary archive evolution is a modern global phenomenon encapsulating within the concern for plagiarist acts. Filthy attempts raise the necessity to cache fingerprints of literature, accessible to global community, a mandatory practice. Finger printing demands the generation of digital pattern analogous to DNA-print for a creation. A document is a commixing of only two sections namely print area and spaces.

Spaces are residual portion between the prints, it may be a inter-character, inter-word, inter-line, inter-column, margins etc. Dissimilar documents may have same dimensions of margins and columnar settings which are immune to changes in content but it will be rare to have same inter-word space maps for dissimilar text.

A space map will change categorically whenever there is any modification of the content hence proves to be an effective tool for tracing the document dissemination life cycle and warehousing. Scope of this work has dual purpose - for securing the sanctity of literary works along with fingerprinting so that the exchange of documents over internet can effectively be traced. This stage of our work is centered towards the affirmation of our belief that a space map is unique for a document.

The proliferation of digital network has drastically changed the data dissemination process and it now has become the greatest pool of information. Of all sort searches and downloads, literary content constitute the prominent proportion. These works of individuals are their respective creations and the sanctity of such existences needs to be maintained. Although the creations are fully secured through global and regional laws but those required to be invoked against filthy acts demand the evidence for both migration and tampering.

Keywords : Fingerprinting, Digital Right Management, Binary Image,

1. Introduction

The proliferation of digital network has drastically changed the data dissemination process and it now has become the greatest pool of information. Of all sort searches and downloads, literary content constitute the prominent proportion. These works of individuals are their respective creations and the sanctity of such existences needs to be maintained. Although the creations are fully secured through global and regional laws required to be invoked against filthy acts but those demand the evidence for both migration and tampering. Online archives are making their existence with more and more journals and magazines providing access interface for profit / non-profit making. Resource objects in digital form enjoy several advantages from quality to ease of dissemination. On the contrary it poses major challenge to distinguish the pirated from the original copy. To be in command of right over literary content, there exist two approaches first is the pessimistic i.e. restricted right transfer and other is optimistic i.e. total right transfer with strict monitoring. Objective of digital rights management is not only to restrict to management and elicitation of rights but also encompass monitoring and fingerprinting of the work. Vigilance over the distribution system requires minimum of three issues viz. the source, destination and asset DNA print.

Content and structural analysis and tagging can play crucial role in management of digital rights.

* Lecturer, Department of Computer Application Sevdie Institute of Management Technology, Lucknow
**Assistant Professor , Department of Computer Application, School of Management sciences, Varanasi

The preceding analysis type is a finer in comparisons to the later; a coarse analysis might be done as primitive tool for locating the probable asset while micro analysis could be followed up over suitable subset. A canvas utilization pattern of a binary image poses to be potential for harnessing a fingerprint. Remaining of the paper concentrates over the analysis of document image. Section 2 dissect resource components, Section 3 performs the semantic investigation of characteristics through profiling, Section 4 discusses the experiment for our view avowal and Section 5 exposits the findings.

2. Document Image

A document is essentially a binary image with regular horizontal patterns, homogenous through out the stretches. It might be containing two foreign components namely the diagram and images. Diagram shares the same canvas of the host whereas image has it own. Further, a diagram is difficult to segregate and require complex computation contrary to image that can be easily traced by change in the colour depth. The uniform structure of a document, excluding figure and image, do also have certain irregularities such as indentations, heading, font formatting, font variation and font colouring. All these features do have their own impact on the appearance of documents, like change in spacing and the assumption of being binary. On coarser side, document content is surrounded by band of under-utilized width of canvas and it is divided into vertical sections, minimum one, which may be of different dimensions and dominantly are being separated by another band of underutilized canvas strip.

2.1 Visual Perception

A document image is predominantly of two colours unlike that of regular images. A regular image has a larger set of colours and that too in multiple layers and has a lot of features to fingerprint and those features can be easily traced through the colour gradient. These images also have good capacity to hold foreign components imperceptibly. As documents are essentially binary images, hence we have only bi-level colour depth, further the features are not demarcated by colour gradients unlike that in images. Features are distinguished through discreet quantization of patterns and subsequently finger printing can be done, either by generating pattern maps or pattern distribution interrelation statistical computations. Pattern interrelation statistical computation does not guarantee a unique finger print; hence in our work we focus over the pattern maps.

Pattern maps require structural re-clustering after the removal of undesired structures. Re-clustering provides a compact formation of required patterns we may call this "Pre-map Filtering". The filtered residue projects the desired concise map of scattered patterns.

3. Profiles

Pre-map filtering requires a low level analysis of the document to extract the required set. Profiles are the tools being used to locate pattern sets for Pre-map filtering. The sample data are shown at the end of the paper. The profile is generated for both horizontal as well as vertical sample print pattern. Through these profiles we can identify the distribution of underutilized portion of the canvas.

Vertical Profile reveals longitudinal layout, the unused canvas which is commonly the demarcation for segments within the image. Each column segment has to be individually finger printed and cumulative print will be generated then after. (Fig 1)

Horizontal Profile reveals the details regarding header, footer, top margins, bottom margins, annotations, title etc. Header and footer are proprietary hence, are insignificant for our cause. Similarly top margins and bottom margins represent an unused canvas. These too are irrelevant towards finger printing constitution hence, are filtered out to locate for actual content. Annotations are the special text elements violating general layout hence, could be identified by the terminations of formats and resumption after the block. A horizontal profile hence helps in identification of underutilized canvas, irrelevant segments and special segments. (Fig 2)

Paragraph Profile is primarily used to identify the weight of segments. Higher the weight - richer will
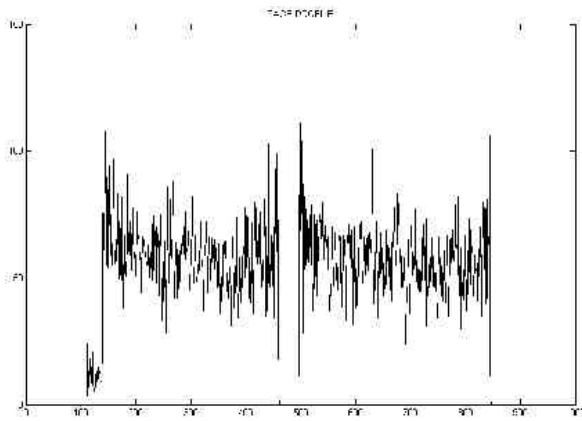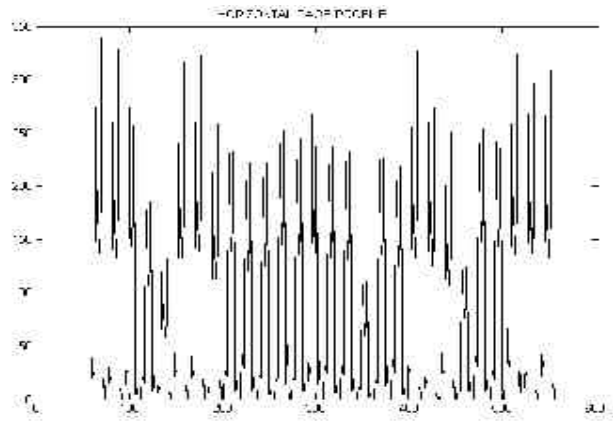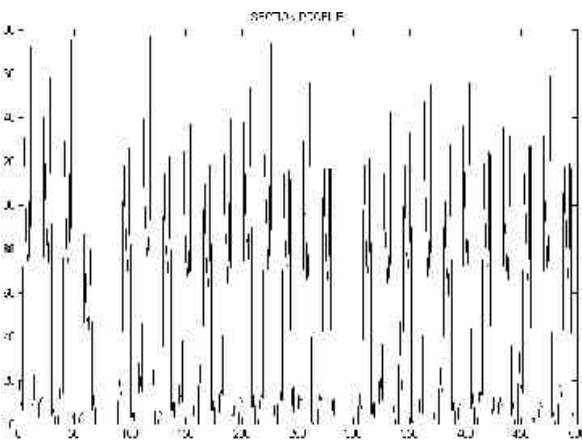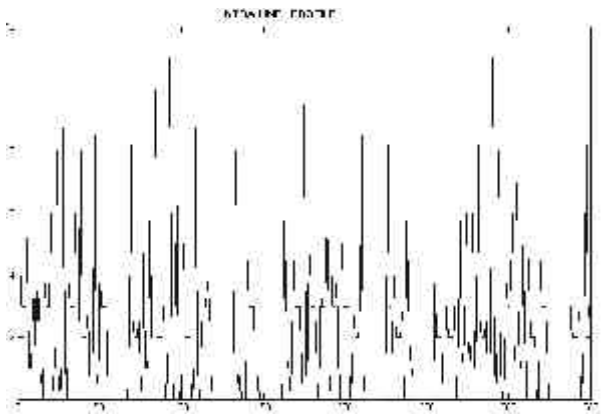
Fig 1

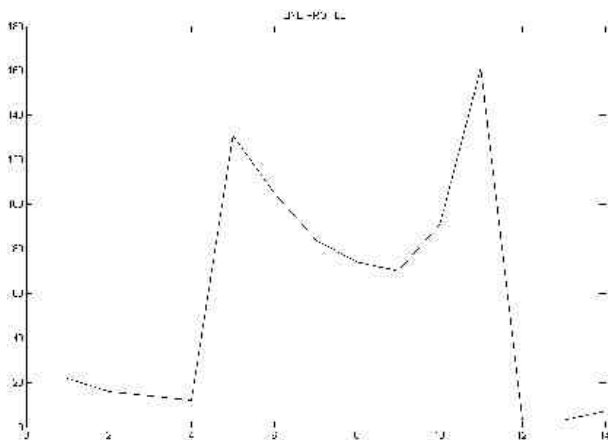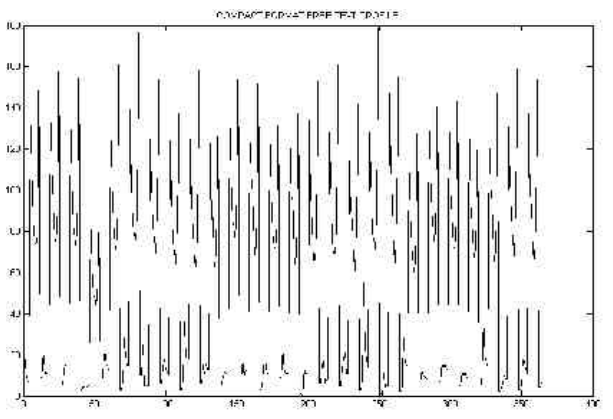Fig 2

Fig 3

Fig 5

Fig 4

Fig 6

Sample Under Study

Sample-1

them effective the management uses Multimedia Presentation for communication of strategies, targets and decisions besides the conventional text dispatches. This help in better communication besides helping in quicker reviews and better participation among the Decision Makers and decision implementers for evolution, evaluation and implementation of strategy.

Modern day corporate institutions prominently use the digital electronic devices and media for communication due to their various inherent advantages, yet at the very same time there exist a grave lacuna in this system of communication, which is that the system is capable of producing indistinguishable number of copies of the digital data. The major issue of contention here is what if someone within the closer circuit infringes the system and propagates wrong and/or altered information; by the time it will be noticed and taken care of, the damage to reputation, prestige and trade would already have been done to a magnitude beyond imagination. [8,9]

The above two implementation of Multimedia System very much qualifies for their incorporation under laws in relaion to data. The Copyright laws are well in force to protect the hard work of individuals / corporate, to develop an Intellectual asset, through the Right of

The range of tampering may vary from being a minor alteration of information to complete change in content, or modification of the actual content and marketing it, as the plagiarists own property.

Since Multimedia now a day's prominently exists in Digital form due to its quality of signals being higher in comparisons to analog, low space requirement and adaptability towards error correction. The major concern is for Digital Intellectual Property Rights because the digital content, copied as well as the original, produce same quality signal thus it caannot be challenged on mere comparison. At the same time the ever growing span and reliability of the digital public network, the Internet — is also an area of the concern with respect to locating the point of infringement.

Our intriguing concern is protection of information available publicly i.e. released for compliance of Freedom of Information. Towards such Information, IT can be a very constructive partner. Ever since concerns for IPR and profitability, has acquired greater proportion owing to it being declare as one's assets, and the entire global intellectual community is working towards evolving a system for development and maintenance of IPR. The System does not necessarily mean only the human resource, but also incorporates the Technology; wherein the human resources with

Sample-2

them effective the management uses Multimedia Presentation for communication of strategies, targets and decisions besides the conventional text dispatches. This help in better communication besides helping in quicker reviews and better participation among the Decision Makers and decision implementers for evolution, evaluation and implementation of strategy.

Modern day corporate institutions prominently use the digital electronic devices and media for communication due to their various inherent advantages, yet at the very same time there exist a grave lacuna in this system of communication, which is that the system is capable of producing indistinguishable number of copies of the digital data. The major issue of contention here is what if someone within the closer circuit infringes the system and propagates wrong and/or altered information; by the time it will be noticed and taken care of, the damage to reputation, prestige and trade would already have been done to a magnitude beyond imagination. [8,9]

The above two implementation of Multimedia System very much qualifies for their incorporation under laws in relaion to data. The Copyright laws are well in force to protect the hard work of individuals / corporate, to develop an Intellectual asset, through the Right of

The range of meddling may vary from being a minor alteration of information to complete change in content, or modification of the actual content and marketing it, as the plagiarists own property.

Since Multimedia now a day's prominently exists in Digital form due to its quality of signals being higher in comparisons to analog, low space requirement and flexibility towards error correction. The major concern is for Digital Intellectual Property Rights because the digital content, copied as well as the original, produce same quality signal thus it caannot be challenged on mere comparison. At the same time the ever growing span and reliability of the digital public network, the Internet — is also an area of the concern with respect to locating the point of infringement.

Our intriguing concern is protection of information available publicly i.e. released for compliance of Freedom of Information. Towards such Information, IT can be a very constructive partner. Ever since concerns for IPR and profitability, has acquired greater flexibility owing to it being declare as one's assets, and the entire global intellectual community is working towards budding a system for development and maintenance of IPR. The System does not necessarily mean only the human resource, but also incorporates the Technology; wherein the human resources with

be the map, smaller the weight - rare will be the map. Density of map does have their obvious advantages and disadvantages; major advantage with low density maps is their compactness against the richer one. A paragraph profile comprises of series of line profiles after the decomposition of interline-formatting. (Fig. 3)

Line Profile is generated with the paragraph profiling process. Each line profile divulges the demarcations among the coloured segments. It also discloses canvas occupancy factor for the line. Boundary demarcations unfold the word and space profiles. (Fig 4)

Word Profile defines the quantization factor for the inter-word space profiling since any change to the word directly modifies the inter-word space profiling. In our experiment, we identified the quantization of factor 4. As the study sample become rich the quantization may vary, hence we will be experimenting with the dynamic quantization in advance stages. (Fig 5)

4. Experiment

Our experiment hovers around the structural fragmentation of sample. The samples taken for the purpose are identical to each other except for four instances in Sample 2 where the actual words are replaced with suitable synonym.

Each sample is individually processed through pre-map filtering process wherein, we segregate the document components. A format free version of the sample section is generated and relative

inter-word space distribution is computed. The output of the process is crude image comprising of map of print vs space (Fig 6). Both the samples are subsequently overlapped to generate a variation map corresponding to differences in the two document images.

5.0 Conclusion

The experiment was done to identify the worthiness of the space distribution for text document, finger printing and monitoring process. During the experiment the clone of sample contain certain synonym for the text segments. The figure has very correctly mapped the region of dissimilarity to the region where text synonyms were substituted in document image.

References

1. Charles Ducken et. al. (2004, June) "JISC Digital Management Study, Interim Report"

2. Norishige Morimote, (1999) "Digital Watermarking Technology with Practical Application", Information Science spl. issue on Multimedia Information Technology-Part 1, vol -2 , No. 4,.

3. Chun-Shien Lu, (2004) Multimedia Security Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, IDEA Group Publishing, , ISBN: 1-59140-192-5.

4. http://www.digimarc.com/tech/papers.asp

Checkpointing Algorithm in Alchemi.NET

*Neeraj Kumar Rathore**
*Dr. Inderveer Channa***

ABSTRACT

The Grid is rapidly emerging as the means for coordinated resource sharing and problem solving in multi-institutional virtual organizations while providing dependable, consistent, pervasive access to global resources. The emergence of computational Grids and the potential for seamless aggregation and interactions between distributed services and resources, has led to the start of new era of computing. Tremendously large number and the heterogeneous nature of grid computing resource make the resource management a significantly challenging job. Resource management scenarios often include resource discovery, resource monitoring, resource inventories, resource provisioning, fault isolation, variety of autonomic capabilities and service level management activities.

Fault tolerance has become the main topic of research as till date there is no single system that can be called as the complete system that will handle all the faults in grids. Checkpointing is one of the fault-tolerant techniques to restore faults and to restart job fast. The algorithms for checkpointing on distributed systems have been under study for years. These algorithms can be classified into three classes: coordinated, uncoordinated and communication-induced algorithms. In this paper, a checkpointing algorithm that has minimum checkpointing counts equivalent to periodic checkpointing algorithm has been proposed which has relatively short rollback distance at faulty situations and produces better performance than other algorithms in terms of task completion time in both fault-free and faulty situations. This algorithm has been implemented in Alchemi. NET because it does not currently support any fault tolerance mechanism.

Keywords: Fault tolerance, checkpointing, Distributed, Alchemi, and Middleware etc.

1. Introduction

Rajkumar Buyya defined the Grid as:

"Grid is type of parallel and distributed system that enables the sharing, selection and aggregation of geographically distributed resources dynamically at runtime depending on their availability, capability, performance, cost, user quality-of-self-service requirement" [2].

Advances in networking technology and computational infrastructure make it possible to construct large-scale high performance distributed computing environments that provide dependable, consistent and pervasive access to high end computational and heterogeneous resources despite geographical distribution of both resources and users.

In a heterogeneous computing environment like Grid, a suite of different machines ranging from PC to supercomputer is loosely inter-connected to provide a variety of computational capabilities to execute collections of application tasks that have diverse requirements.

These kinds of large scale high performance distributed services have recently received substantial interest from both research as well as industrial point of view. However, an important research problem for such systems is the lack of fault tolerance system. The heterogeneous and dynamic nature of grids makes them more prone to failures than traditional computational platforms. So, the system managing such infrastructures needs to be smart and efficient to overcome the challenge of fault detection and recovery.

*Department of Computer Engineering
**Thapar University, Patiala (Punjab).INDIA

The paper introduces grid computing, discusses about the motivation of research work, different ways to handle these failures architecture, concept of virtual organization and faults in grid. After studying fault tolerance in different grid middleware Alchemi.NET has been chosen. After analyzing the detailed performance of Alchemi.NET, different areas related to fault tolerance in which the discussed middleware still lacks have been identified. It has been realized that, in order to support fault tolerance in computational grid (Alchemi.NET Framework based), it is useful to provide a checkpointing support for avoiding the grid to be down during failures. A checkpoint algorithm for fault tolerance system, which is used in the Alchemi.NET, and the basic requirements for implementation of the proposed algorithms are discussed.

2. Faults in Grid

As VO involve a large number of complex heterogeneous networks, in which faults are a major concern. As grid is a distributed and unreliable system involving heterogeneous resources located in different geographical domain, for this case, fault tolerant resource allocation services [1] have to be provided. In particular, when crashes occur, tasks have to be reallocated quickly and automatically, in a completely transparent way from the user's point of view.

Thus, one of the main challenges for grid computing is the ability to tolerate failure and recover from them (ideally in a transparent way). Current grid middleware still lacks mature fault tolerant features and next generation grids needs to solve this problem providing a more dependable infrastructure to execute large-scale computations by using remote clusters and high performance computing system. A resource management system for the grid should address the issues of fault tolerance.

2.1 Fault Tolerance Definitions

Fault tolerance is the survival attribute of computer systems. The function of fault tolerance is "…to preserve the delivery of expected services despite the presence of fault-caused errors within the system itself. Errors are detected and corrected, and permanent faults are located and removed while the system continues to deliver acceptable service [3]".

Fault tolerance is the property of a system that continues operating consistently with its specifications even in the event of failure of some of its parts [4]. From a user's point of view, a distributed application should continue despite failures. The fault tolerance has become the main topic of research. Till now there is no single system that can be called as the complete system that will handle all the faults in grids. Grid is a dynamic system and the nodes can join and leave voluntarily. For making fault tolerance system a success, following point must be considered:

How new nodes join the system,
How computing resources are shared,
How the resources are managed and distributed

2.2 Research Findings

As described earlier that Grid environments are featured by an increasingly growing virtualization and distribution of resources, such situations impose greater demands on fault-tolerance capabilities. In the fault tolerance mechanisms, different types of schemes and techniques are used, which are beneficial to make grid fault tolerant. Checkpointing is one of the techniques of fault tolerance. Till now many middleware in the grid environment are not fully fault tolerant. Different middleware have different levels of fault tolerance. Some of the middleware like Alchemi.NET do not have a robust fault tolerance mechanism. Therefore, in this research work Alchemi.NET has been chosen and a checkpointing algorithm has been designed for it.

3. Why Alchemi.NET?

Alchemi.NET is an open source software framework that allows painless aggregation of the computing power of networked machines into a virtual supercomputer and develop applications to run on the grid. Alchemi.NET includes:

The runtime machinery (Windows executables) to construct grids.

A .NET API and tools to develop .NET grid applications and grid-enabled legacy applications.

It has been designed with the primary goal of ease in use without sacrificing power and flexibility. As Alchemi.NET is the emerging technology, so a lot of work has to be done to make it a standard .NET based middleware. We have used Alchemi.NET as the framework to setup the grid [7].

There can be many reasons for choosing Alchemi.NET as the framework for building the computational grid and then further choosing to build a fault tolerant system for it. Some of these reasons are:

Alchemi.NET is the first .NET based stable grid. Most importantly Alchemi.NET is open source. So one can do any number of changes in it.
Another important reason is that most of the systems in our labs are running Windows Operating Systems.
Fault tolerance research area is still under development in Alchemi.NET.
Checkpointing is also not available in Alchemi.NET.

3.1 Fault Tolerance in Alchemi.NET

Fault tolerance is the property of a system that helps it to continue operating consistently with its specifications even in the event of failure of some of its parts. From a user's point of View, a distributed application should continue despite failures. Alchemi.NET based distributed syste is characterized by a collection of autonomous processing elements, called nodes. Each of these nodes has some computing resources as well as the possibility to exchange information with some of the other nodes. These are referred to as its neighbors and the communication between these nodes take place through a central authority called Manager. The Manager controls the working of all the executors. Users interact with the Manager for submitting and enquiring the status of their jobs.

A 'grid application' consists of a number of related grid threads. Grid applications and grid threads are exposed to the application developer as .NET classes / objects via the Alchemi.NET API. When an application written using this API is executed, grid thread objects are submitted to the Alchemi.NET Manager for execution by the grid. Alternatively, file-based jobs (with related jobs comprising a task) can be created using an XML representation to grid-enabled legacy applications for which precompiled executables exist. Jobs can be submitted via Alchemi.NET Console Interface or Cross-Platform Manager web service interface, which in turn convert them into the grid threads before submitting them to the Manager for execution by the grid.

3.2 Present Fault Tolerance Scenarios in Alchemi.NET

1. Heartbeat mechanism used by Alchemi.NET: Executors send the heartbeat messages at some interval to the Manager to whom they are connected. This will help the Manager to maintain the status of the Executors. In case the Manager doesn't receive the heartbeat messages from the executor between the pre-decided times, the Manager consider that executor to be dead and update its information. Here the reason for not receiving of the message is considered to be hardware failure; OS reboot or process being killed. These are termed as hard failure of executor.

2. Executor fails "hard" due to a hardware failure, an OS reboot or the process being killed. In this case Alchemi. NET is using the heartbeat technique to re- schedule the thread to another Executor.

3. Executor fails "soft" due to the user logging off or stopping down the Executor. In this case the Manager is informed that the

Executor is going offline and the thread is re-scheduled (this scenario fails many times). This is an acceptable solution.

4. Restart the incomplete job: In case if the job remains unfinished due to any reason like- hardware failure, failure of the Manager, etc the Alchemi.NET Manager stores the status of the job by using "a p p l i c a t i o n _ i d", "internal_thread_id" and "executor_id" fields it maintain in the SQL database.

5. Dynamically determine new nodes added or deleted: As the new node is added or removed, the Manager is being provided with the information dynamically and it updates the console information to make a correct record of the information so as to avoid any faults.

4. Problem Formulation

As seen from literature survey Alchemi.NET does not support fault tolerance, therefore in this paper a checkpointing algorithm has been implemented for Alchemi.NET.

4.1 Proposed Checkpointing Algorithm

A checkpointing algorithm has been designed for better fault tolerance in Alchemi. NET. Checkpointing is one of the fault- tolerant techniques to restore faults and to restart the job in a shorter time. In this paper, a new checkpointing algorithm has been proposed which has minimum checkpointing counts equivalent to the periodic checkpointing algorithm, and relatively short rollback distance at faulty situations. The proposed algorithm is better than previously proposed checkpointing algorithms in terms of task completion time in both of fault-free and faulty situations.

4.2. Proposed Solution

Checkpointing schemes associate each local checkpoint with a checkpoint sequence number and try to enforce consistency among local checkpoints with the same sequence number. These checkpointing schemes have the easiness, recovery time advantages and low overhead over other checkpointing schemes. Proposed checkpointing algorithm reduces the checkpoint overhead compared to previously suggested checkpointing algorithms and which have a relatively short rollback distance in faulty situation. In the proposed scheme, we use checkpoint sequence number to take a message checkpoint. However, unlike the other algorithms, only one message checkpoint can exist between two consecutive periodic checkpoints. Therefore, our checkpointing algorithm has smaller number of checkpoints than other checkpointing algorithms. Moreover, like the other algorithms, the dependency among checkpoints is removed by message checkpoints. In result, our checkpointing algorithm has a relatively short rollback distance in faulty situation. The algorithm has a better performance than the others in terms of task completion time in both of fault free and faulty situations. New checkpointing algorithm is discussed here under:

5. Checkpointing Algorithm

Step 1: The algorithm runs for n processes where the process value P(i) is varies from 0 to n-1.

Step 2: The flag value is initialized. If new checkpoint flag value is (NCF) =0 (False) that means there is no checkpoint flag in the current interval and if the value is NCF =1 (True) that means there is a checkpoint flag in the current interval.

Step 3: After assigning the value of the process, start with while loop when process P (i) till the end.

Step 4: In the checkpoint, if the current time value of the process equals to the checkpoint time than check

If (NCF==0)
Take a stable checkpoint with current process state; Increase checkpoint number by 1;
Checkpoint increase by current time plus checkpoint
And Set new checkpoint flag = false;

Otherwise, if condition does not match take a stable checkpoint with new checkpoin

Step 5: After new checkpoint flag is checked, process P (i) send and receive the message and check

If senders checkpoint number is greater than current checkpoint number than again check

If (NCF==1)
Set current checkpoint number to senders;
Else
Take a new checkpoint with current process state;

Set current checkpoint number to senders;
And Set new checkpoint flag = True;

Step 6: At last, process received a message.

Step 7: If any failure occurs in between the execution, after resuming value pick from the memory and go to step 3.

With the new checkpointing algorithm, each process takes a periodic checkpoint at each checkpoint (CP) time. At this point, before taking a checkpoint, each process investigates if there is a new checkpoint in current interval. If one exists, then the content of new checkpoint, which is stored in memory, is written to a stable storage. Otherwise, the current state information of the process is written to a stable storage. After checkpointing, a checkpoint sequence number is increased by 1 and CP time is updated. During normal execution, each process takes a message checkpoint before processing a received message. Each process, before processing message, compares its current checkpoint number with the checkpoint number of message sender that is tagged on each message. If the checkpoint number of message sender is bigger than the current checkpoint number, then each process investigate if there is a new checkpoint in current checkpoint interval. If a new checkpoint exists, then set the current checkpoint number to the message sender's checkpoint number and process the received message. Otherwise, the current state information of process is written to memory (new checkpoint) and current Checkpoint number is set to the message sender's checkpoint number. After taking new checkpoint, each process executes the received message

5.1 Complexity Analysis of the Proposed Algorithm

The Complexity of the above algorithm is O (n). Because n processes run n time within while loop, for each process P(i), the if-else statements with in the while loop gets executed. Assuming that first if-else loop runs j times, where j is a constant when the current time equals to the checkpoint time. Then, the process P (i) has to process the received message if sender checkpoint number is greater than the current checkpoint. The if-else construct runs k times, where k is a constant and since the algorithm is running for then processes so the total complexity of the algorithm is O (j+k)*n. This is approximately equal to the O (n). The O(n) complexity of the algorithm is better to implement any type of checkpointing algorithm in real time environment. For the requirement for the implementation of the new framework is given below.

6. Experimental Results

In Checkpointing algorithm, data can be stored in permanent log file on the basis of checkpointing, which has been proposed in the previous section. An application developed in VB.Net, C# (front end) and SQL SERVER (back end database). The results are shown in the form of screen shots. Alchemi.NET grid can be viewed as a virtual machine with multiple processors. A grid Application can take advantage of this by creating independent units of work to be executed in parallel on the grid (each unit of work is executed by a particular Executor).

6.1 Experimental Evaluation

After successfully building the checkpointing algorithm, it has been tested in two stages. First the test strategy has been formed and then the test case has been defined.

6.1.1 Test Strategy

In the implementation, we have taken a part of different departments of the Thapar University in as computational grids. For building the application

for our system, we have used MS SQL Server as the database. The checkpoint Manager for managing the proper working of Manager is implemented using the steps described above and tested our system by running the sample application.

6.1.2 Test Cases

Following are the test cases that we are going to use to check our system.

Test Case #1 Executor On/Off

We dynamically switch on and off the executors. While doing this, we kept on checking the status of the executing jobs through the Alchemi.NET Console Manager.

TestCase#2 Checkpointing between Manager and executor

We have been checking the working of the Manager. This module is just like a checkpoint monitoring system, in which the Manager invokes checkpoint signal at a regular interval of time

Test Case #3 Automatic Checkpointing

We check this case with the help of automatic checkpoint monitor facility provided in the MS SQL server. It uses the snapshot agents to update the database and present information.

Test Case #4 Manager Stopped

This case is tested in two parts. First, by manually disconnecting the Manager and noting down the results and secondly, by switching off the system without disconnecting the Manager.

6.2 Experimental Results

We found that our proposed system helps to increase the performance of grid by providing the checkpointing concept. When the system fails, the checkpoint saved data successfully comes into foreplay. The test case three was tested using the Microsoft SQL Server built in facility to monitor. Test case 4 is the main test case that was to be tested. Executors have to be reconnected to this checkpoint.

7. Conclusion

The sharing of computational resources is a main motivation for constructing Computational Grids in which multiple computers are connected by a communication network. Due to the instability of grids, the fault detection and fault recovery is a very critical task that must be addressed. The need for fault tolerance increases as the number of processors and the duration of computation increases.

In this paper, we have investigated the issues and challenges involved in dealing with faults in Alchemi. NET middleware and the checkpoint algorithm in Alchemi. NET for dealing with various kinds of faults has been implemented. Further the efficiency of our proposed system under various conditions has been evaluated.

8. Future Work

The future extension of the project can be done in two ways:

8.1 Extension of the implementation

The current implementation is done within LAN with limited number of PCs, this can be extended for systems outside the city network.

If the failure occurs, then the backup is stored in log file. But this is to be done manually. There must be some provision so that on failure of Manager Executors will automatically store data in log file.

This implementation is kind of third party software that will improve the grid fault tolerance. But this can be integrated into the Alchemi.NET middleware code to help the user to easily use it.

8.2 Extension of proposed method

Our approach of checkpoint can be extended to work on support for multiclustering with peer-to-peer communication between Managers.

References

1. Kamana Sigdel, "Resource Allocation in Heterogeneous and Dynamic Networks" MS Thesis, Delft University of Technology, 2005.

2. Francois Grey, Matti Heikkurinen, Rosy Mondardini, Robindra prabhu, "Brief History of Grid", http://Gridcafe.web.cern.ch/Gridcafe/Gridhistory/history.html

3. Paul Townend and Jie Xu-"FaultTolerance within a Grid Environment", University of Durham,DH1 3LE, United Kingdom

4. Varun Sekhri,"CompuP2P: A light-weight Architecture for Internet computing "Iowa State Univ., Iowa, 2005.

5. Rajkumar Buyya, "The Nimrod-G Resource Broker: an economic Based Grid Scheduler" http://www.buyya.com/thesis/Gridbroker.pdf

6. Foster, I., Kesselman, C And Tuecke, S., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International Journal of High Performance Computing Applications, 15 (3). 200-222. 2001.

7. Liang Pangolin Kian NG,"N1GE6 Checkpointing and Berkeley lab Checkpoint/Restart" Dec 28, 2004

8. Paul Townend and Jie Xu, "Fault Tolerance within a Grid Environment".

9. Y. M.Wang and W. K. Fuchs. Optimistic message log-ging for independent checkpointing in message-passing systems. In Proceedings of the 11th Symposium on Reliable Distributed Systems, pages 147{154, October 1992.

10. M. Chandy and L. Lamport. Distributed snapshots: determining global states of distributed systems. ACM Transactions on ComputerSytems, 3(1):63{75, February 1985.

11. J.H. Abawajy,"Fault-Tolerant Scheduling Policy for Grid Computing Systems", IPDPS'04.

12. Ian Foster "What is the Grid? A Three Point Checklist" Argonne National Laboratory & University of Chicago, ttp://www.gridbus.org/papers/TheGrid.pdf.

13. David De Roure and others, "The Semantic Grid: Past, Present and Future", Proceedings of the 2nd Annual European Semantic Web Conference (ESWC2005), Volume 93, Issue 3, 2005.

14. Foster and C. Kesselman, "The Globus Project: a Status Report", In Proc. of Seventh Heterogeneous Computing Workshop(HCW98), IEEE Computer Society Press, March, 1998.

Software Fault Tolerant Computing: An Introduction

Dr.K.C.Joshi*

ABSTRACT

Though Software Fault Tolerant Computing has a tremendous role in the ever-expanding world of Software systems, not much research work has been carried out in the said field. In order to arrive at clear understanding of Software Fault Tolerant Computing, an extensive theoretical analysis is presented. A framework of Software Fault Tolerant Computing is designed and discussed. The research work primarily deals with a comprehensive study of Software Fault Tolerant Computing, hence it takes into account various terms associated with Software Fault Tolerant Computing such as origin of fault tolerance, fault tolerant systems, fault tolerance computing, components of fault, and software fault tolerance methods. A detailed discussion of these terms has been done in this paper.

Keywords: Software Fault Tolerance, Redundancy, Exception Handling, Byzantine Fault.

1. Introduction

The term Software fault tolerance has two interpretations: one that deals with the tolerance of software faults (namely, design faults), while the other discusses the control and operation of fault tolerant mechanism (usually hardware -oriented) through software- implemented functions. We will emphasize on the former interpretation. In other words, software fault tolerant computing is concerned with all the techniques necessary to enable a system to tolerate software faults remaining in the system after its developments. These software faults may or may not manifest themselves during systems operations, but when they do, software fault tolerant techniques should provide the necessary mechanisms of the software system to prevent system failure occurrences. There is less work in the area of software fault tolerance. Current fault tolerance research areas are varied and there is no obvious central direction for future research activities. There is growing feeling in the research community, as evidenced at conferences and workshops, of a need to develop a focused, or at least a more clearly defined state of fault tolerance research.

2. Origin of Fault Tolerance

Algirdas Avizienis originally formulated the concept of fault tolerance in 1967, and said that "A system is fault-tolerant if its programs can be properly executed despite the occurrence of logic faults." The fault tolerance concept resulted from three converging developments.

First, the earliest use of computers made it apparent that even with careful design and good components, physical defects and design errors were unavoidable. Thus, designers of early computers used practical techniques to increase reliability. They used:

- Redundant structures to mask failed components;

- Error control codes and duplication or triplication with voting to detect or correct information errors;

- Diagnostic techniques to locate failed components;

- Automatic switch overs to replace failed subsystems.

Second, in parallel with these evolving engineering techniques, computing pioneers such as John Von Neumann and Edward F. Moore and Claude E. Shannon addressed the general problem of building reliable systems from unreliable components. William H. Pierce unified their theories of masking redundancy and incorporated some others.

Computer Center, IASE, M.J.P. Rohilkhand University, Bareilly

Third, in 1958 NASA challenged Caltech's Jet Propulsion Laboratory to build unmanned spacecraft for interplanetary exploration. These missions would last 10 years or more and require onboard computing. The task of designing computers that could survive a journey of several years and then deliver peak performance deep in space was unprecedented. Existing studies indicated that providing a large number of spare subsystems promised longevity, if the spares could be employed in sequence. JPL's problem was to translate this idealized "spare replacement" system model into a flight worthy implementation of spacecraft guidance and control computer. The proposal to do this, "A Self-Testing-and-Repairing System for Spacecraft Guidance and Control" (STAR), was presented in October 1961.

3.   Fault Tolerant Systems

With the support of JPL and NASA, eight years later the effort (led by Algirdas Avizienis and five researchers: George C. Gilley, Francis P. Mathur, David A. Rennels, John A. Rohr, and David K. Rubin) culminated in a laboratory model of the JPL-STAR computer. US Patent No. 3,517,671 granted to Algirdas Avizienis in 1970 and assigned to NASA, validated the concept's originality. A flight model of the JPL-STAR was designed for a 10 to 15 year space mission, but construction stopped when NASA discontinued the Grand Tour mission.

Nevertheless, the project did afford the study of all accessible engineering solutions and theory concerning reliability. From a confusing variety of theories and techniques emerged the unifying concept of fault tolerance. And in 1971 JPL and the IEEE Computer Society co-sponsored the first International Symposium on Fault-Tolerant Computing. During the succeeding 25 years the set of faults that fault-tolerant systems had to tolerate grew extensively. The original concept dealt with transient and permanent logic faults of physical origin. The increasing complexity of software and VLSI chip logic emphasized the impossibility of removing all design faults prior to operation. Thus, faults due to human design errors were added to the demands of fault tolerance. The possible causes of faults, then, include

natural phenomena of internal or external origin and accidental or intentional human actions. In either case, faults will cause errors. If error detection and recovery do not take place in a timely manner, a failure will occur that will be manifested by the denial or an undesirable change of service.

There are two ways to build a fault-tolerant system. The *bottom-up* approach entails designing an infrastructure of autonomously fault-tolerant subsystems (microprocessors, memories, sensors, displays, and so on) and integrating this infrastructure with global fault tolerance functions such as reconfiguration and externally supported recovery. The *top-down* approach allows a system to be built using existing (off-the-shelf) subsystems that may have little or no fault tolerance at all. A global monitoring function is then implemented to provide fault tolerance. Top-down design is the prevailing practice.

An examination of both approaches clearly makes a case for the long-range merits of the bottom-up technique. Moreover, similarities between fault tolerance and the human immune system suggest an analogy that offers developers and users of high-confidence systems a greater understanding and acceptance of bottom-up fault tolerance.

4.   Fault Tolerant Computing:

In designing a fault-tolerant system, we realize that 100% fault-tolerance cannot be achieved. Moreover, the closer we wish to get to 100%, the more costly our system will be, either in hardware and/or software redundancy.

To design a practical system, one must consider the degree of replication needed.

This will be obtained from a statistical analysis for probable acceptable behavior. Factors that enter into this analysis are the average worst-case performance in a system without faults and the average worst-case performance in a system with faults.

How much fault tolerance does a system need?

A system is said to be *k fault tolerant* if it

can withstand *k* faults. If the components fail silently, then it is sufficient to have *k+1* components to achieve *k fault tolerance* (*k* components can fail and one will still be working). If the components exhibit Byzantine faults, then a minimum of *2k+1* components are needed to achieve *k fault tolerance*. In the worst case, *k* components generate false replies but the remaining *k+1* will provide a majority vote and cause the correct outcome to win.

5.   Components of Faults

1.   Transient Faults: These faults occur once and then disappear. For example, a transmission times out but works fine when attempted a second time.

2.   Intermittent Faults: These faults are the most annoying of component faults. This fault is characterized by a fault occurring, then vanishing, then occurring again, then vanishing again… An example of this kind of fault is a loose connection.

3.   Permanent Fault: This fault is persistent; it continues to exist until the faulty component is repaired or replaced. Examples of this fault are disk head crashes, buggy software, and burnt-out hardware.

4.   System Faults: System faults may be either *fail-silent failures* or *Byzantine faults*. A fail-silent, or fail-stop, fault is one where the faulty unit stops functioning and produces no ill output (it produces no output or produces output to indicate failure). A Byzantine fault is one where the faulty unit continues to run but produces incorrect results. Byzantine faults are obviously more troublesome to deal with.

6.   Software Fault Tolerance Methods:

Software fault tolerance includes:

(a)   Data Diversity: Ammann and Knight [1] proposed data diversity as a software fault tolerance strategy to complement design diversity. The employment of data diversity involves obtaining a related set of points in the program data space, executing the same software on those points, and then using a decision algorithm to determine the resulting output. Data diversity is based on a generalization of the works of Gray, Martin and Morris [2], which utilize data diverse approaches relying on circumstantial changes in executing conditions. These execution conditions can be changed deliberately to effect data diversity. This is done using data expressions to obtain logically equivalent variants of the input data. Data diversity use data re-expression algorithms (DRA) to obtain their input data.

The fault tolerance of a system employing data diversity depends upon the ability of the DRA to produce data points that lie outside of a failure region, given an initial data point within a failure region. The program executes correctly on re-expressed data points if they lie outside a failure region. Many real time control systems and other applications can use DRAs.

(b)   Design Diversity: It has been observed that redundancy alone is not sufficient for tolerance of software design faults, so some forms of diversity must accompany the redundancy. Diversity can be applied to several layers of the system- hardware, application software, system software, operators and the interfaces between these components. Since the exact copies of software component redundancy cannot increase reliability in the face of software design faults, we need to provide diversity in the design and implementation of the software. The design diversity consists: recovery blocks, N-version programming, distributed recovery blocks, N-self Checking Programming, consensus recovery block and retry voting.

(c)   Reasonableness Checks: Assertions can be used as part of a reasonableness checking acceptance test (AT) such as range or bounds AT. The range or bounds AT is reasonableness test type of AT. It simply determines whether a result is within preset minimum and/or maximum limits. If the result is within the bounds, it is accepted. This test is very simple, thus minimizing the potential for adding design faults to the system implementing the AT.

(d)   Acceptability Checks: These are the most basic approach to self-checking software. They are used with the recovery blocks, CRB, distributed RB, Retry Blocks, and acceptance voting (AV) techniques. The AT is used to verify that the system's behaviour is

acceptable based on an assertion on the anticipated system state. It returns the value true or false . An AT needs to be simple, effective, and highly reliable to reduce the chance of introducing additional design faults, to keep run-time overhead reasonable, to ensure that antipated faults are detected, and to ensure that nonfaulty behaviour is not incorrectly 'detected'.

(e)   Assertions: These are a fairly common means of program validation and error detection. As early as 1975. Randell[3] presented executable assertions as central to the design of fault tolerant programs. An executable assertion is a statement that checks whether a certain conditions holds among various program variables, and, if that condition does not hold, takes some action. Assertions may be set up to only produce a warning upon detection of a corrupt state or they may take or initiate corrective action. For example, upon the detection of a corrupt state, the assertion may halt program execution or attempt to recover from the corrupt state.

(f)   Watchdog timers: The hardware fault tolerance architecture related to the retry blocks (RtB) technique is stand by sparing or passive dynamic redundancy. It is the data diverse complement of the recovery block (RB) scheme. The RtB technique uses acceptance tests (AT) and backward recovery to accomplish fault tolerance. A watchdog timer(WDT) is also used and triggers execution of a s backup algorithm if the original algorithm does not produce an acceptability result within a specified period of time . The algorithm's results are examined by an AT. If the algorithm results pass the AT, then the RtB is complete.

(g)   Exception handling:

        Exception handling is the interruption of normal operation to handle abnormal responses. The purpose of exception handling is to ensure that system transaction execution executions will preserve the invariant properties inherent to the component system modules in spite of possible exception occurrences (anticipated as well as unanticipated). The design of exception handlers requires that consideration be given to the possible events triggering the exceptions, the effects of those events

on the system, and the selection of appropriate mitigating actions [Pradhan 96]. [Randell 95] lists three classes of exception triggering events for a software component: interface exceptions, internal local exceptions, and failure exceptions.

Interface exceptions are signaled by a component when it detects an invalid service request. This type of exception is triggered by the self-protection mechanisms of a module and is meant to be handled by the module that requested the service.

Local exceptions are signaled by a module when its error detection mechanisms find an error in its own internal operations. These exceptions should be handled by the module's fault tolerant capabilities.

Failure exceptions are signaled by a module after it has detected an error which its fault processing mechanisms have been unable to handle successfully. In effect, failure exceptions tell the module requesting the service that some other means must be found to accomplish its function.

7.   Recommendations

1.   Because of the size and duration of any serious research effort needed for Software Fault Tolerance, the size of the research community dealing with this area has been in a steady decline in the past 10 years.

2.   Yet the problems of software faults are real. No prudent manager responsible for constructing a large-scale safety-critical system wants to assume that software faults will not exhibit symptoms during the system's operational life.

3.   Hopefully, government agencies will begin to pay more attention to the growing neglect of software fault-tolerance research.

8.   Conclusion:

        Software fault tolerant computing is concerned with all the techniques necessary to enable a system to tolerate software faults remaining in the system after its developments. These software faults

may or may not manifest themselves during systems operations, but when they do, software fault tolerant techniques should provide the necessary mechanisms of the software system to prevent system failure occurrences.

References

1. Ammann P.E. and J.C. Knight. 'Data Diversity: an approach to software fault tolerance', IEEE Trans. On Computers, Vol 37, No 4, 1988, pp 418-426.

2. Gray, J., 'why do computers stop and what can be done about it?', Proc Fifth Symp. Reliability in distributed Software and database system Jan. 1986, pp 3-12.

3. Randell, B. 'System structure for software fault tolerance', IEEE Trans. On Software Engineering, Vol. SE-1 No. 2, 1975, pp. 220-232.

4. Pradhan ,D. K., Fault-Tolerant Computer System Design, Prentice-Hall, Inc., 1996.

5. Randell B. and Jie Xu, The Evolution of the Recovery Block Concept, in Software Fault Tolerance, Michael R. Lyu, editor, Wiley, 1995, pp. 1 21.

6. Randell B., et al, editors, Predictably Dependable Computing Systems, Springer, 1995.

7.] Lyu, M.R. (ed) , Handbook of Software Reliability Engineering , New York , McGraw Hill, 1996.

8. Shooman, M.L., 'Probabilistics models for software reliability prediction' , In Statistical Computer Performance Evaluation, Ed. W. Freiberger, Academic Press, New York, 1972, pp. 485-502.

9. L. Pullum, 'Software Fault Tolerance Techniques and Implementation', Artech House, 2001.

10. Anderson, T. and P.A. Lee, Fault Tolerance Principles and Practice, Prentice Hall, 1981.

11. Avizienis, A., The Methodology of N-Version Programming, in Lyu, Michael R. ed., Software Fault Tolerance, John Wiley & Sons, 1995, pp. 23-46.

12. K.C. Joshi & Durgesh Pant, 'Software Fault Tolerant Computing: Needs and Prospects', ACM Ubiquity, Vol 8 issues 16 , April 24- April 30 , 2007.

13. Avizienis, A., 'The N-version approach to fault-tolerant software'. In IEEE Transactions on Software Engineering SE-11(12):14911501, December 1985.

14. A. Avizienis and J. Kelly, 'Fault tolerance by design diversity: concepts and experiments' , In IEEE Computer, 17(8):6780, August 1984.

Client Technology Web Based Service Oriented Mobile Augmented Reality System

*Jatin Shah**
*DR. Bijendra Agrawal***

ABSTRACT

Various types of technology available in market for developing mobile Client - Web based Service Oriented, like Open Source PHP , ROR, .NET, JAVA are few popular web development technology. Mobile has its own limitation mobile OS, it's network standards, memory, processing capacity etc. Developing client for mobile augmented reality system focus mainly two technology for its advance features - 1) Microsoft technology and 2) Java based technology. Both technologies have its own constraints for mobile but which are very comfortable for scalability, portability, and language independent.

1. Introduction

Client side web Based Service is responsible for easy access on client browser, so client can register themselves to authorized to access other required services. Main responsibility of the client is to send data to the middle level services to reach the destination (linked with other web based services n level) and receive the augmented data directly from server side client or middle level services.

Web Services have an open standard hence any device as well as server side client can access it without any problem of OS and with minimum Installation or Processes. Authorized user have been given different rights to send video, audio or 3D image data to middle level services.

Here we define the terms Augmented Reality and Mobile Augmented Reality System. The Computer System that combined the real and the virtual in order to assist users in interacting with their physical environments are called Augmented Reality System.

Mobile Augmented Reality System is one in which augmentation occurs through available knowledge of where the user is e.g. user's location and therefore his surrounding environments.

2. Web Technologies for Client

Various types of tools are available in market for developing web based application/software.

.NET Microsoft Technology provides very powerful framework and very rich library to user for any kind of web/window based development for mobile or normal web based application. Java is another platform for developing this kind of application. Java provides very large library and different packages for this. PHP and ROR are very popular open source web development technology recently used in the market. They also provide the framework and rich library for the advance development.

Due to Mobile OS, it's processing capacity and limited memory and storage space, we focus mainly on two technologies, .NET and Java. Development should be easy, provide very powerful languages like ASP.NET, J2ME and provide dynamic controls that can help user fast development and interaction with Real Time Audio, Video, or Image Processing that requires Augmentation.

2.1 Microsoft .NET

Microsoft .NET is product suite that enables organizations to build smart, enterprise-class web services. Note the important difference- .NET is a product strategy, whereas J2EE is a standard to which products are written. Microsoft .NET is largely a rewrite of windows DNA, which was Microsoft's previous platform for developing enterprise applications. Windows DNA includes many proven technologies that are in production today, including Microsoft Transaction Server (MTS) and COM+,

*MCA, Research Scholar , KSV University, Gandhinagar,
**Principal, VKMS College, Vadu, Gujarat

Microsoft Message Queue technologies, and includes a web services layer as well as improved language support.
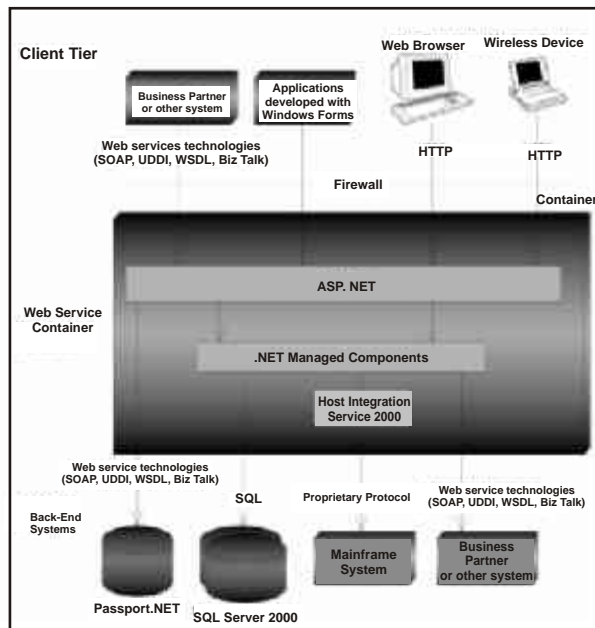
The .NET application is hosted within a container, which provides qualities of service necessary for enterprise applications, such as transactions, security , and messaging services.

The Business layer of the .NET application is built using .NET managed components. This layer performs business processing and data logic. It connects to databases using Active Data Objects (ADO.NET) and existing systems using services provided by Microsoft Host Integration Server 2000, such as the COM Transaction Integrator (COM TI). It can also connect to business partners using Web Services Technologies (SOAP, UDDI, WSDL).

Business Partners can connect with the .NET application through web services technologies.

Traditional 'thick' clients, web browsers, wireless devices connect to Active Server Pages (ASP.NET) which render user interfaces in HTML, XHTML, or WML.

Microsoft .NET offers language-independence and language-interoperability. This is one of the most intriguing and fundamental aspects of the .NET platform. A single .NET component can be written, for example, partially in VB.NET, the .NET version of Visual Basic, and C#, Microsoft's new object oriented programming language. First, source code is translated into Microsoft Intermediate Language, sometimes abbreviated MSIL, sometimes IL. This IL code is language-neutral, and is analogous to Java bytecode. The IL code then needs to be interpreted and translated into a native executable. The .NET Framework includes the Common Language Runtime (CLR), analogous to the Java Runtime Environment (JRE), which achieves this goal.

The CLR is Microsoft's intermediary between .NET developer's source code and the underlying hardware, and all .NET code ultimately runs within the CLR. This CLR provides many exciting features not available in earlier versions of Windows DNA, such as automatic garbage collection, exception handling, cross-language inheritance, debugging, and "side-by-side" execution of different versions of the same .NET component.

2.2   JAVA : The Foundation for J2EE

The J2EE architecture is based on the Java programming language. What's exciting about Java is that it enables organizations to write their code once , and deploy that code onto any platform. The process is as follows :

1.   Developers write source code in Java.

2.   The Java code is compiled into bytecode, which is a cross-platform intermediary, halfway between source code and machine language.

3.   When the code is ready to run, the Java runtime Environment (JRE) interprets this bytecode and executes it at run-time.

J2EE in an application of Java. J2EE components are transformed into bytecode and executed by a JRE at runtime. Even the containers are typically written in Java.

2.3   J2EE and Web Services

J2EE has historically been an architecture for building server-side deployments in the Java

programming language. It can be used to build traditional web sites, software components, or packaged applications. J2EE has recently been extended to include support for building XML-based web services as well. These web services can interoperate with other web services that may or may not have been written to the J2EE standard. J2EE application is hosted within a container, which provides qualities of service necessary for enterprise applications, such as transactions, security, and persistence services.
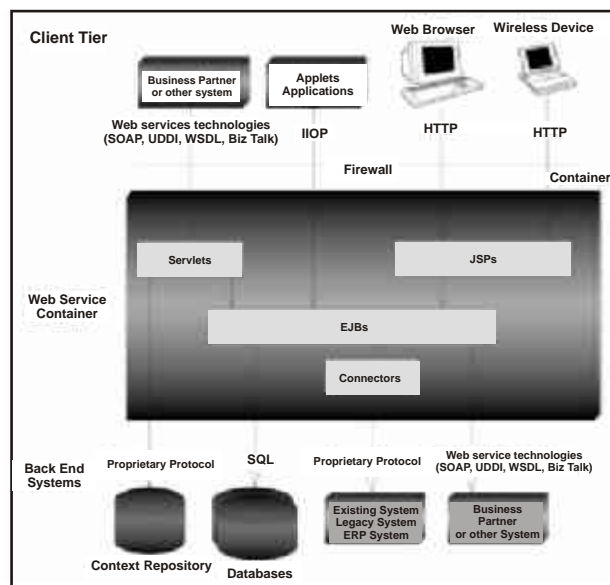
The business Layer performs business processing and data logic. In large-scale J2EE applications, business logic is built using Enterprise JavaBeans (EJB) components. This layer performs business processing and data logic. It connects to databases using Java Database Connectivity (JDBC) or SQL/J, or existing systems using the Java Connector Architecture (JCA). It can also connect to business partners using web services technologies (SOAP, UDDI, WSDL, ebXML) through the Java APIs for XML (the JAX APIs).

The business partners can connect with J2EE applications through web services technologies (SOAP, UDDI, WSDL, ebXML). A servlet, which is a request/response oriented Java Object, can accept web service requests from business partners. The servlet uses the JAX APIs to perform web services

operations. Shared context services will be standardized in the future through shared context standards that will be included with J2EE.

Traditional 'thick' clients such as applets or applications connect directly to the EJB layer through the Internet Inter-ORB Protocol (IIOP) rather than web services, since generally the thick clients are written by the same organization that authored J2EE application, and therefore there is no need for XML-based web service collaboration.

Web browsers and Wireless devices connect to JavaServer Pages (JSPs) which render user interfaces in HTML, XHTML, or WML.

3.   Comparative Analysis

Both Sun J2EE and Microsoft .NET provide runtime mechanisms that insulate software developers from particular dependencies. In addition to a web service-oriented XML layer of Indirection between platforms, languages, and enterprise architectures, Sun J2EE and .NET offer language-level intermediation via the Java Runtime Environment (JRE) and the Common Language Runtime (CLR) respectively.

Table 1. Analogy Java and .NET

Feature	J2EE	.NET
Type of technology	Standard	Product
Middleware Vendors	30+	Microsoft
Interpreter	JRE	CLR
Dynamic Web Pages	JSP	ASP.NET
Middle-Tier Components	EJB	.NET Managed Components
Database Access	JDBC, SQL/J	ADO.NET
SOAP,WSDL,UDDI	Yes	Yes
Implicit middleware (load-balancing, etc)	Yes	Yes

Microsoft .NET offers a variety of time-to-market features not found in J2EE as well. Most

notably, ASP.NET is independent of client device, and allows for user interfaces to be rendered to alternative user interfaces without rewriting code. Microsoft also offers Queued Components which are superior to Message Driven Beans. It should be noted here that Microsoft has tried to simplify server-side programming greatly by removing support for features found in traditional enterprise applications, such as stateful servers and simple transactions. If developers need to go outside this box, their code must be made to be non-managed and reside outside the .NET framework rather than take advantage of it. Microsoft also provides business process management and E-Commerce capabilities, which are available in some J2EE implementations but not all.

In conclusion, we feel the ability to achieve rapid application development offered by both J2EE and .NET is definitely not equal. It is, however, comparable. The feature differences are minor and it is very difficult to make a compelling argument either way.

When building web services, in general one should always prefer to have a single-vendor solution. A single vendor is usually more reliable, interoperable and less error-prone than a two-vendor bridged solution.

One of J2EE's strengths is that it has spawned a wide variety of tools, products and applications in the marketplace, which provide more functionality in total than one vendor could ever provide. However , this strength is also a weakness. With lower-end J2EE implementations, one need to mix and match tools to get a complete solution, which could result in low-level hacking due to imperfections in portability. Larger vendors, such as IBM, ORACLE, BEA and iPlanet, each offer a complete solution, and thus their products are fully interoperable. Thus it is important to choose a larger vendor to avoid interoperability headaches.

NET provides a fairly complete solution from a single vendor-Microsoft. This solution may lack some of the higher end features that J2EE solutions offer, but in general, the complete web services vision that Microsoft will be providing is equal in scope to that of a larger J2EE vendor.

Developers of Java GUI applications will find that .NET provides a rich set of features in Windows Forms. These features offer an easy migration path for Swing and Java/AWT developers to move graphical applications to the native Windows interface. JSP programmers will find much to like when migrating code to ASP.NET (also known as Web Forms). This improved version of ASP now supports development in C# in addition to existing Visual Basic and Jscript. ASP.NET server controls give developers the flexibility to extend tag funct ionality-perfect for migration of JSP tag libraries.

A key differentiator of the .NET platform is integrated support for Web services. As much of .NET is built using XML technologies, the platform offers full support for SOAP, WSDL, and UDDI. With tools such as Microsoft Visual Studio.NET, it is a trivial matter to expose application functionality as a Web service. Although Java does offer all the technologies necessary to build Web services, it is not at the crux of the J2EE platform these shows in the level of development effort required.

One approach for migrating applications to .NET is to rewrite existing functionality in C#. A total rewrite may be viable if the existing Java application has architectural deficiencies that require a major overhaul to rectify. Development managers should allocate sufficient time for team members to learn the extensive array of .NET API calls, switch development environments, and implement new deployment procedures. "Although the learning process takes time", states O'Brien, "experience has shown development using the .NET environment is more productive than J2EE".

A safer strategy would be to migrate parts of the application to .NET and leave the remaining components running in Java. There are multiple ways to accomplish this goal, and the desired approach depends on the level of integration desired. A simple approach is expose key application interfaces using Web services. The .NET components can make SOAP calls to the Web services and incorporate the results. This solution may be viable if, initially, the business logic stayed on the Java server while presentation layer functions are moved over to

ASP.NET. Over time the business logic components could be rewritten in C# and deployed on the .NET server.

Interoperability between C# and Java code can also be achieved by using wrapper solutions. Wrappers, otherwise known as software bridges, allow for transitions between incompatible software environments. This approach has been used for many years to solve compatibility problems from *thinking* between Windows and DOS* to connecting mainframes with Web applications. A third party wrapper product, such as JNBridge*, allows .NET classes to call Java classes if as they were native .NET code.

Java applications already deployed on Visual J#, Microsoft's version of Java based on JDK1.1.4, will experience seamless interoperability as both the Java and C# components execute in the same .NET Common Language Runtime. Visual J# is provided by Microsoft primarily as a convenient way for Visual J++ 6.0 developers to adopt the .NET platform. Developers of J2EE applications will not find Visual J# suitable due to the many incompatible changes that have occurred between JDK1.1.4 and the most recent JDK, version 1.3.

Microsoft is working to smooth the migration path with the introduction of its Java Language Conversion Assistant* (JCLA) tool. This tool is central to its JUMP to .NET strategy (Java User Migration Path to Microsoft .NET) and is designed to convert Visual J++ 6.0 projects directly into C# with minimal developer intervention. The tool also remaps Java API calls into functionally equivalent .NET versions. Although useful for Visual J++ 6.0 users, JCLA is not suitable for J2EE app locations as it is limited to JDK1.1.4 compliant applications.

ArtinSoft, developers of the Microsoft JCLA tool, is building a conversion tool tailored to the requirements of enterprise Java applications. This tool supports the latest JDK and an ever-increasing swath of the J2EE API. "Users of the Microsoft JCLA tool are experiencing conversion rates of 90%", says Federico Zoufaly, Executive VP of ArtinSoft. "The J2EE focused migration tool which is in the final development stages aims to achieve a conversion rate of at least 80%," he added.

4.   Conclusion

Choosing right technology for Mobile is the key element for Mobile Augmented Reality System. We have described all the factors mainly two technologies Microsoft and Java.

To develop Web Based Service Oriented Client for Mobile, we choose the Microsoft Technology because of many advantages likes portability, scalability, simple Interface etc. For Augmentation, we need the client to communicate with the middle level services or directly with the server to send/receive data. For all this we need a powerful server that can process and augment the data and get back to the client. So we need a powerful server that can manage all the task and Microsoft has the best option for giving any kind of server support. If the client is based on Microsoft and can easily interact with the server or mid level component.

References

1.   http://www.middleware-company.com

2.   Easton, M., King, J., Cross Platform .NET Development Using Mono, portable.NET, and Microsoft .NET, Apress,2004

3.   Chappel, D., Understanding .NET: A Tutorial and Analysis, Addison-Wesley, 2002

4.   Sierra, K., Bates, B., Sun Certified Programmer & Developer for Java 2, McGraw Hill, 2003

5.   Meijer, E., Gough, J., Technical Overview of the Common Language Runtime,2001

6.   www.technial-insight.com, Allan McNaughton-Principal Analyst

Design of Wireless Sensor Network Node on Zigbee for Motion Detection

*Sanjay Singh **
*Rajesh Singh***
*Dr. Sukumar Ray Chaudhuri****

ABSTRACT

To interface a motion sensor and a camera with ZigBee and microcontroller 128, so that we can use the nodes for having an eye on employee or in nuclear reactor for surveillance. The motion sensor will detect any movement and camera will detect the person. Till any movement the camera will be in dead position and as it gets any motion detection it becomes active facing in the direction of the movement and send signals through wireless interface to the master position. Therefore saving power and increasing its durability.

Keywords: Atmega 128, Zigbee, WSN, PIR

1. Introduction

A sensor node, also known as a 'mote' (chiefly in North America), is a node in a wireless sensor network (WSN) that is capable of processing, gathering sensory information and communicating with other connected nodes in the network. WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to co-operatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Wireless sensor networks have been an active research topic for around a decade. The recent release of standards in the field, such as IEEE802.15.4 and ZigBee (5), brought the technology out of research labs and stimulated the development of numerous commercial products. Moving from early research in military applications, sensor networks now are widely deployed in diverse applications including home automation, building automation, and utility metering.

The aim of this paper is to design a wireless motion data logging system with 8 bit embedded micro controller and low power Zig Bee RF transceiver the primary goal of the proposed system are :

- Continous motion detection,
- To transmit data to remote personal computer,
- To implement peer to peer net work.

The paper is organized as follows.

Section 2 discuss the proposed system, Section 3 describes the hardware development, Section 4 gives the description of software used in the sensor node. Finally the paper is concluded with result, conclusion and future work.

2. Proposed Work

Fig 1 shows a signal block diagram of the Wireless sensor network node using ZigBee Transceiver module. A micro controller receives position information of the human from three PIR (Passive Infra Red) sensor modules. This position information of the human is transmitted to the motor controller and the Transceiver. The motor controller controls the motor of the display unit by using the obtained position information. Next, the slave node Transceiver sends a signal to the master node Transceiver to share the position information in the wireless network.
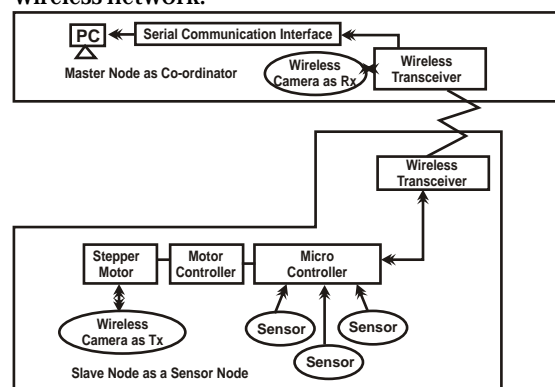
Fig 1. Block Diagram WSN Node

*Research Scholar, Singhania University, Rajasthan
**Assistant Professor, Department of Electronics & Communication Engineering, DBIT, Dehradun
*** Prof. Department of Electronics & Communication Engineering, UDML College of Engineering , Jaipur

3.   Hardware Development

3.1   Master Node (Sink)

The basic components of master node are: CC2500(Transceiver Unit), MAX232, DB9 and PC.
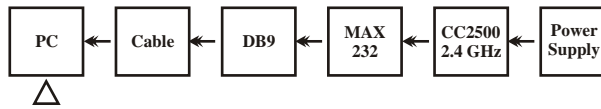
Fig 2. Block Diagram of Master Node
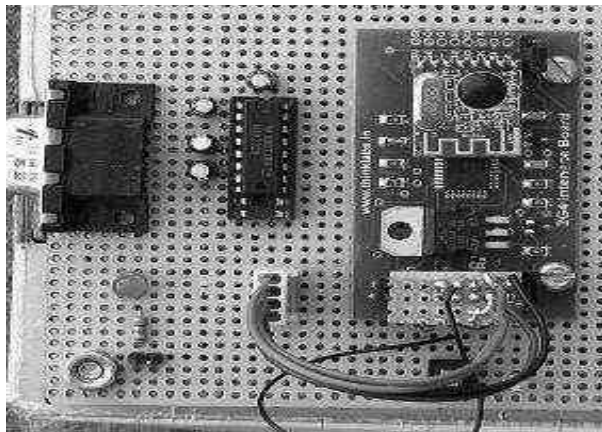
Fig 3. View of Master Node

3.1.1   CC2500 (Transceiver Unit)

The selection of commercially available transceiver can be done on the basis of their key features like, type of modulation, carrier frequency, operating voltage, througput, transmitted power, current in receiving, transmitting mode, etc. it consumes fraction of power needed by other wireless protocols such as - Blurtooth and 802.11 variants.

3.1.2   MAX232

The MAX232 family of line drivers/ receivers is intended for all EIA/TIA - 232E and V.28/ V.24 communication Interfaces, particularly, where +-12V is not available.

3.2   Slave Node

The basic component of slave node are: AVRmicrocontroller Atmega 128, CC2500, PIR sensor, Stepper motor and wireless camera.
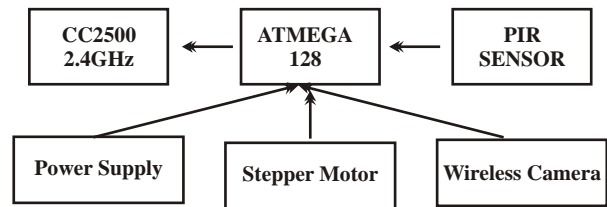
Fig 4. Block Diagram of Slave Node
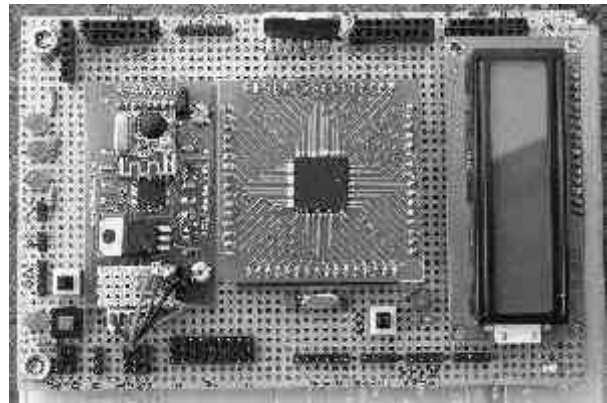
Fig 5. View of Slave Node

3.2.1   Microcontroller Module

The AVR Atmega 128 is a 8 bit micro controllerhaving 128K flash memory, 4K of RAM, 16 bit of inbuilt ADC, Timer 2/8 bit, 2/16 bit, operating voltage of 4.5 - 5.5 V and low power consumption. it has embedded debugging, in-system flash programming through a standard JTAG interface supported by a wide range of development tools.

3.2.2   PIR Sensor Unit

The passive Infra Red Sensor module is used for motion detection. it works from 3.5V to 5V and gives TTL output which can be directly fed to the micro controller. It consists of Pyroelectric sensor and Fresnel lens that detect motion by measuring change in the infra red levels emitted by the object. it can detect motion up to 20 feet. Our system uses three PIR sensor and a camera mounting device.

3.2.3   Wireless Camera

The camera is mounted on a slave node with the help of stepper motor. The motion of camera is controlled by the stepper motor while motion of human being is detected by the PIR sensor.

4.   Software Development

Microcontroller has been programmed to test the hardware as well to achieve the goal of WSN application, which involved the following steps [Fig 6].
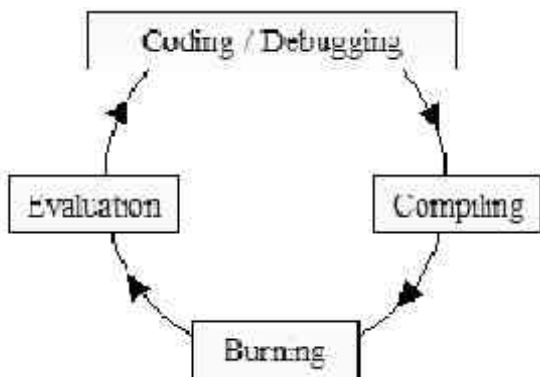
Fig 6. Software Development Cycle

Coding/debugging of WSN node Program is done by using AVR Studio 4.0 software (Fig 7).
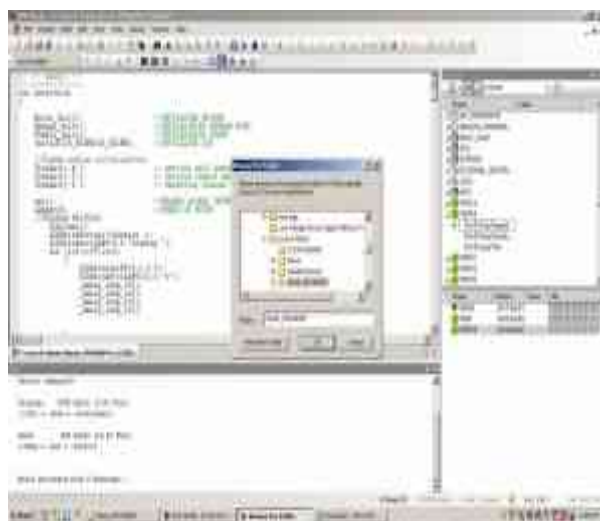
Fig 7 Coding / Debugging

Compiling of the code is done by using software PonyProg 2000v2.06f.

5.   Conclusion and future work

The system has been integrated and tested to function properly. The goal of real time motion data transmission between the Master Node and the Slave Node is achieved. The wireless transmission results

have been obtained through Terminal v1.9b. It shows the recorded motion.

The results obtained for code size are shown in Table 1.

Table1. Code Size

Application	Code Size
Program	3942 B
Data	690B
Total	4632B

The results obtained for power dissipation are shown in Table 2. The three components that dominate power dissipation for slave sensor node are the microcontroller, the radio and the buffers.

Table 2. Power dissipation

Node Design	Current Consumption
Master Node	
Transceiver 2.4 GHz	60mA
Miscellaneous (Driver, Connector, cable)	12mA
Total	72mA
Slave Node	
Microcontroller Atmega128 (Active)	19mA
Transceiver 2.4 GHz	60mA
Motion sensor	3mA
Stepper motor	1000mA
Camera unit	15mA
Total	1097mA

The Mica2 sensor mote and Mica Z, which uses the TinyOS over the AVR platform, has been compared in terms of code size and power with the present work .The current consumption of Mica Mote is found around 67mA while with that of present work is around 82mA(without camera unit). The code size of the Mica Mote for radio application

has been found 9.5 KB while for the present work it has been found 4.632KB. It can be seen from the above data that power consumption of the motes is comparable while code size of the implemented sensor node is much less than when compared to Mica Mote. The increase in code size in Mica Mote is due to TinyOS (13). The design WSN node system can be used as :

    Wireless Home Security

    Home Automation System

    Area monitoring

    Industrial monitoring

Future scope of work

    Implementation of multi node network.

    Implement network for real time applications.

References

1.   IEEE Communications Magazine April 2007

2.   Halit Eren, "Wireless sensors and instruments networks, design, and applications," Transl. Ji Xiaodong, Zhao Beiyan, and Peng Mugen, China Machine Press, pp 129-132, January 2008.

3.   Wang Shu, Yan Yujie, Hu Fuping, and Qu Xiaoxu, "The theory and application of wireless sensor network," Beijing University of Aeronautics & Astronautics Press, pp 11-124, July 2007.

4.   Jin Chun, Luo Zuqiu, Luo Feng, and Chen Qianbin, "The foundation of ZigBee technology and the analysis of cases," National Defense Industry Press, January 2008.

5.   ZigBee Alliance, http://www.zigbee.org/

6.   TI Products, http://www.ti.com/

7.   IEEE Std. 802.15.4-2006, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks[S]", 2006.

8.   Rogelio Reyna Garcia, "Understanding the ZigBee stack," manuscript Shizhuang Lin, Jingyu Liu, and Yanjun Fang, "ZigBee Based Wireless Sensor Networks and Its Applications in Industrial," Proceedings of the IEEE International Conference on Automation and Logistics, August 18-21, 2007, Jinan, China.

9.   J.Y. Chen, X.P. Zhou, "ZigBee Wireless Communication Technology in Industrial Controls," Radio Engineering of China, Vol. 36, No. 6, pp. 61-64, 2006.

10.   Feng Xiao, Liu Qiuli, "ZigBee application in Remote monitor system of oil field," Petroleum Instruments, vol. 20, no. 6, pp. 68-67, 2006.

11.   Liu Jiangsha, Lei Wei, Yin You, "Designing of a wireless RF unit basingon CC2430," International Electronic Elements, 2007, 4.

12.   Yin Ming, Wang Liwei, "Design of General Wireless Communications Module Based on Zigbee," Computer and Communications, vol. 5, no.24, pp. 110-112, 2006.

13.   http://www.tinyos.net/: TinyOS Operating system designed for wireless embedded sensor networks

Semantic network in a free-software computer operating system

Rajiv Nair_ and G. Nagarjuna*
Arnab K. Ray**

ABSTRACT

A nonlinear model has been posited for the global analysis of data pertaining to the semantic network of a complex operating system (free and open-source software). While the distribution of links in the dependency network of this system is scale-free for the intermediate nodes, the richest nodes deviate from this trend, and exhibit a nonlinearity-induced saturation effect. This also distinguishes the two directed networks of incoming and outgoing links from each other. The initial condition for a dynamic model, evolving towards the steady dependency distribution, determines the saturation properties of the mature scale-free network.

Keywords: Networks; Nonlinear dynamics; Structures and organization in complex systems; Computer science

1. Introduction

Scale-free distributions in complex networks have been very well studied by now [14]. The ubiquity of scale-free properties is quite noteworthy, and spans across vastly diverse domains like (to name a few) theWorldWideWeb [5] and the Internet, the social, ecological, biological and linguistic networks [3], income and wealth distributions [6, 7], trade and business networks [8], and semantic networks [9].

It should occasion no surprise, therefore, that further developments have led to the discovery of scale-free features in the architecture of computer software as well. A recent work [10] has shown that the structure of object-oriented software is a heterogeneous network characterised by a power-law distribution. More in keeping with the purpose of this present paper, an earlier work on complex networks in software engineering [11] had found evidence of power-law behaviour in the inter-package dependency networks in free and opensource software (*FOSS*). It is a matter of common knowledge that when it comes to installing a software package from the open-source *Debian GNU/Linux* repository, many other packages — the "dependencies" — are also called for as prerequisites. This leads to a network of these dependencies, and every such package may be treated as a node in a network of dependency relationships. Each dependency relationship connecting any two

packages (nodes) is treated as a link (an edge), and every link establishes a relation between a prior package and a posterior package, whereby the functions defined in the prior package are called in the posterior package. This enables reuse (economy) of functions and eliminates duplicate development. As a result the whole operating system emerges as a coherant and stable semantic network [9]. However, unlike other semantic networks, the network of nodes in the *Debian* repository is founded on a single relation spanning across all its nodes: Y depends on X; its inverse, X is required for Y.

So, given any particular node, its links (the relations with other nodes) can be of two types—incoming links and outgoing links—as a result of which, there will arise two distinct kinds of directed network [3]. For the network of incoming links, a newly-reported work [12] has empirically established the relevance of Zipf's law and the conditions attendant on it [13] in open-source *GNU/Linux* distribution. Carrying further along these very lines, the present paper purports to study and model the finite-size effects in a *FOSS* network. There is a general appreciation that for any system with a finite size, the power-law trend is not manifested indefinitely [14, 15], and in the context of the *FOSS* network, this is a matter that is recognised as one worthy of a more thorough investigation [12]. Deviations from the power-law trend appear for both the heavily-linked

*Homi Bhabha Centre for Science Education, Tata Institute of Fundamental Research, V. N. Purav Marg, Mankhurd, Mumbai 400088, India
**Department of Physics, Jaypee Institute of Engineering and Technology, A-B Road, Raghogarh, Guna 473226, Madhya Pradesh, India

ßÎ©ꞐÌ¾ ˜M^ꞏꞒꞏSÍ   ÉA þ³iHÂ¤' ˆómç`ꞐIE {c7ä´
ߢ Ä ¦%½ F‹ U· ·g–ñ¡ æÉ ꞏꞐ þ ¦@÷–%¦ o ƒ•¨ ¤
ßÎ0lGÓ^>XLÅzµ©Ꞑ²ꞏ̈ .Í4ã   Ö̈ÉÍUÅꞐꞐXÆꞏ ƒSꞏ YøG
ßÎ̧|›mH…ꞏꞐ̈§õ2¿3oꞏ²é&¡ꞏꞏ^éa,°*¨Ÿ¯¨)Ꞑ4‡ò ¬.ðä°Îm13
ßùꞏꞐ̈y:)ÞVÎÂ ƒÍ Áþ Ñ ƒ8î sg¡W"¡ G+~øçaðÆ²¥ â„œ
ß+$ìQ—ſꞑui)í*ì)}A{̧nꞐwꞏ°íá£

ßZ   1 YIÒ! zyj[®&–$-<ã)6;üÖZ=O_

    ß o$ꞏꞑU;¾Âw´ñ,i¾r wkBꞏ¼G½6¿Cꞏꞏ%ꞏꞐ©ꞏyGò
ßï   úÅ œ;Ú· dÅ¢Æe8 @d5 ẞØ$ꞐÕ ß=ú" ẞò #A¬"3ꞏ
*ẞr^GFš+f   €Óẞ²s(fY Xè%Ꞑꞏ•6<Å/©ꞑÙùAꞏw"äꞏ´
ß+$5—ã Ö^Ļã™iꞐ8î)Ç   &Üœ÷bꞑiWẞJꞐꞏꞏkA©ø•ÈÊ
ßæ̧"¢» A5¬bꞏꞐi©9ꞏØ?"Í è%•ꞐꞑõꞐ±.ꞏꞏyyóáꞐꞐFøIMìyˆ
ßO*ŠeÅꞏ Yá¡SFÖ ÙꞐ̈!×   'bò´wì s• ˜ §ꞐB8©(Ø=#ò
ßO*ẞû8,i¤€ñ.•ÐÕ ¥™]šꞐꞐꞐÄif† ~ Œ-Š1¡Ꞑꞏ?OꞐI²QüÈÊ
ßZ¼45—5JUG;ÀuYH†;w› î VÎÇ~÷"´xòl Y•[«ꞏꞐÆq9
ßmꞐ?ꞐBꞏ ~ ̃ ẞéÂꞐ¶ 0¨hꞏꞑhꞏBꞏó©ꞏꞑ꞉U'V̧ƒù À*9ꞏæ\È¥u¶Æ̧Úú¦ç
ßÎ̂'4[ë%é ŸT¿ ƒGý9ꞏ¦ @õ{?¶Ꞑn«maꞏ̈§!¯)ª+ ÍꞏꞐꞏꞏiOC,1̧ˆ
ßæ"̧„~8š•

ß¤Ú ß¯e¢f¡ v° 4ê ê u²Ö´Ý;´gÒ=§!ŒtꞏÐs(þò°Ü ²
ß ýꞏVꞐBàg ¬Cꞏ ¡?Õꞏè8 J Ñƒ ß š¨Õꞏi Hꞏ.«u Ì.•–ö
ß©qꞐꞏꞑÿ;Ì   ÒÄꞐꞏ,9ýÁv³î~BꞏꞏꞐꞐ àD®¬rçꞐꞏIW ƒꞐ¥̧Ø ƒ¶
ß+g£õœÖÈ€½nꞏWꞏꞏꞏꞐꞏꞏꞑꞐꞐꞑZâ˜ŒEPu½Ꞑ4®öpꞏꞏꞐꞏꞐꞑꞑꞑ꞉oW]
ßuꞏ<ò×ꞏQꞐꞑ꞉ß O5ê' ßꞐ½ꞏꞏ—MꞐ¢*²üv7¬‰|ÎꞐꞏꞐ꞉u C+
ß ƒõèÐG;ꞐÈù½réꞑꞏ…Ð' a   ¡½0ª)¬vþ†u(cꞐØ-ƒ"ꞏꞏ mâ²
ß¬wä`· K5•ꞏð†Éy Ꞑꞏ̈äx yJß%ꞐꞐ t c   N ß à7 1K g
ßÎ0lf.Õ–ŠŅ}ðꞐ"I ꞏª l½)êꞐ ï*gvꞏꞏþs[ãN¹ꞏ§«Ì65 è¾êà
ß   ÑÅ‰Æ{̧nꞏꞏz?ô¨EꞐꞏꞏT¨xµ-â¨ µ>Æ@¬fîYÓ{Kꞏꞏ&QMm™Š
ßÆꞏdÆ̧ÐꞐ̈ ƒPNBꞏ•èÜ²¦[˜HØꞏꞏꞐꞏ~ôn]EꞐÈ̀´y }eŸðÀ´úꞏYK
ßld,'†Jµ   ,7t* ã6ú°p }Aµꞏò̧¢€€úeMꞐꞑꞐꞏꞑꞏꞏꞐꞑꞑ꞉Ó™©ꞏPꞏꞏꞏꞑꞏ²
ßæÁ#…¿ꞏꞏꞏ̈Ꞑ6̧Ꞑꞏæ^RꞐꞏꞏꞏæ¦g¡•YÅꞏoFš!ꞏÊèSÍ OÉ3že5Ø-ꞏ‡'¤s
ßÓò.LNꞏẞ×BCõ¶ꞐꞐh£àꞐꞐñꞏ£gá– 2…ꞏyaÖáLÔ¼‡ꞏꞐꞏ°Oô
ßÎ¯L'%ꞏꞏgꞏꞏcꞐꞏz?Ꞑꞏq>ÿꞐ̧©ꞏꞐꞏꞏWÍ'Ì ¸9vÝ%Ꞑꞏ%FÀ44¨Ü ðÀ©•æꞐꞏ ¤ž
ß'l(ẞWK…:u9ïꞏ{o%ꞐꞏE8ù‰Äꞏ꞉êꞏꞏꞑꞑꞐꞏꞏꞑꞑ.™ꞏ}ꞏꞏ꞉¢*ꞏÞꞏ´§ kꞐyMmª
ßO5¶§kâÖ ƒ*à ¨XꞐꞏꞏꞏꞏÃ

    ßUþ;RâÕꞐꞏꞐꞏꞑ꞉@ꞏꞑnꞏõ¦r3ꞏꞏ̂.ën TŠ ‰ꞏꞐꞏꞐꞐꞏꞏꞑ꞉ꞏꞐꞐꞏ꞉Ꞑ§ꞏꞐyO$5E5àà
ßÎ0Nmꞏ¦ã™©ꞐꞏꞐꞏꞏꞐꞏꞐꞏꞐꞑ§ꞏg¢–ZÅ¥à®dꞏ+hꞐo÷iꞏꞑꞑꞐꞏ̈è¯™èøꞏꞏꞐ̈
ßlÍ§ãÝ~r2&̂ꞐꞐꞏꞏꞑ꞉ꞏqU   ß¼qð*à•Y–ZꞐꞏꞏꞐꞑꞐꞑꞐáLꞏꞏ§ꞐꞐꞐꞏꞏꞏꞏꞐꞏꞏꞑ.mØꞐꞑ꞉ꞐqlÊŸ¼[{žꞐꞏ
ßO´ÓÍ/ꞏꞏꞐꞏꞏꞏꞐꞐ Â†þꞏꞏꞐꞐꞏꞐꞏä"l0*î+ï*vj\ 0¨•"ª   _çR:³–]ꞏꞏꞐꞏꞏꞐꞏꞑ꞉ꞏꞐꞏꞏꞐÆÖ°OoŒ
ß+I$ìß ßꞐꞑꞐꞏE‡Á8

ß"ꞏꞏꞏ̈60 ëꞏꞐ¦Ûh,ꞏ̈ꞏ €DùꞏꞏꞐꞑꞑXè"ÚꞏꞐꞏꞏꞐꞏꞐꞏꞐꞏꞏꞑꞐꞑꞐꞑ꞉ꞏꞐꞏꞑꞑ꞉ÐꞐꞏÃxßÇ<̧ꞐꞏꞑꞐꞑꞑ꞉P̧.‡îâ   Ꞑꞏ.Q–

---

that when $\quad = 0$, which implies the absence of nonlinearity, there will be a global power-law distribution for the data, going as $\quad (x) = (x/c)$, regardless of any non-zero value of . The situation becomes quite different, however, when $\quad 0$. In this case, there will a saturation state for on extreme scales of x, and this can be seen easily from Eq. (1) itself, from which the limiting value of is obtained as $= {}^{-1/}$.

3. Fitting the Model

The parameters , and in the integral solution given by Eq. (2) can now be calibrated using the distribution of links and nodes obtained from the *Debian* repository. The distribution network for incoming links has been plotted in Fig 1. The continuous straight line in this log-log plot indicates the purely power-law behaviour. While this gives a satisfactory description for the network distribution on intermediate scales of x, there is a clear departure from the power law as x ? 8 . The solution given by Eq. (2) fits both the power law and the departure from it, for the values $= -1$, $= -2$ and $= -6$. It would be very interesting to note here that the values of and remain unchanged when it comes to giving a model fit to the dependency distribution for outgoing links, as it has been plotted in Fig. 2. The only distinguishing factor here is the value of , set at $= 1$.

It should instructive here to make a theoretical examination of the value of _ obtained from the data, and its accompanying consequences. Some algebraic manipulations on Eq. (2), followed by a power-series expansion will lead to the series

from which it is not difficult to see that a self-contained and natural truncation for this series can only be achieved when $= -1$. It is remarkable that the *Debian* data conform to this fact, and in consequence of this value of , Eq. (1) is reduced to being a linear, first-order, nonhomogeneous equation, with actually playing the role of a nonhomogeneity parameter.

ßaT Ê{¸ S ¦ ßÊ¯CsŽ…ügÉ?¹§!! ðäÂ¶Ÿ£/Oúk;
ßGA;Y4\ÜÖ·M©-c Ý'⁊KÑˆÎ YÊî„ù• [ÇÏÉ‡ₔW3Ð⅟₄öŸæ%
ß¢ct dÉ,⁺¶• ŸŽdèk ƒ Umv•.¤ẅçîØ æí0 À & ¼Wo„
ßG¿Áü9î+ï,¤ C€5ü̃⅟₄XÇ>óomi�ₗⱠⱮ̃²̈—nÙ̧çyî•k k —5Eĉâ
ßæÀ"ƒ|Ô̧Ë̈"XⅢÀ̇"³đ 'ž̃ĺ,½4~'€oÚﬁ̧Â,ÇòÉÜ̃æä
ß.Hﬂ̃í,7+f*ßW-bŸ/Ⅰ⅃Ø̃̇@ä!z ¤ﬁ̧p ô|ø̧/š~é Ú¡²ₘ ‡=]üO
ß¤ₘu"ë&êₐₑR Ụ̈ꞌĺꞌUS~ḁ̧p5n̈ₗ²†ÚₗⱮ̧̧SÉG̃¼ª\Ç• oU̧3…²]ø
ß¤ápàà' ²d(®cⱲ̧ₕh2⁹⁄₂̈ù*g@4q&Ã=²aⱧﬄ̧ⅱƒS(Ⅰ̃äô"?%e
ßG©áß§È̂꞉̌|ƒ̧3̃ᵳ̃dXȨ̂€øÙR¦‰

ßßqí ã̧¤ ÿⱦX†y/l?ô1%̃ÏÙ,èžJ =Å/©xkv öE .5Ễi)ø
ßçáÿ¾û6ú4(εð̧¥à• —Iņ̃×ú4 Kká aÚbJµ• -càⱮ̧¶¶ â̇Ȩ̂Ü̃̈h
ßÈμ̧jꞋ̈ŠÇ}p2 ßₗ¶œ&mᵥₗk¦LÆÅ<`Úﬁ̧õo̧ò]× Ú§}S"ᵇₒ³¾„ú
ßæà̈E§ⱼ⁴̃₂Ḑ.≺Á̈¶ₘ̇ₐ Økꞅ̌ÆꞇJ„ ~ aÖ̂ßÑ̃Ⱨ̧{•ᵽ̧ÔÈ̇ₒₒø
ßæƒ}Ý¥..Ɠ̧ü8ₒ̧§ₗ̧ú̧¿t4Å̧ J Õ ÛŖ—Œtügr ud¼̇Ɏ̃Ⱨₐ̇•ᵽⱣ̧ₗ
ßƒ]û3÷»ø̧3̧ h¥i—}Aⱦ̇40̃ₘₑD†J†u•• ₗ yîƒⅠ̂Â'… " ßCâ
ß Â̧ï̃⅃̧ä~¸ₗ̧B5ÜI§₋̧ₗȨ̂¡á—L?ôè© ß, 2áçŽú!Œ̧ₙ₋•‚ ḇ̧«+KOmä
ß.Ⱨ̧₋‰Ô̧Ó̂Å̧l©ýÁûï̃³hS̃Õ̧‡ THý̧ý̧ä ä út"O⊣Äîâ‚ºȨ̂k i)ø
ßƒ]û3÷»ø̧ß_ₒ̧ₚ̧⁴⁋>õ†8r(ÝŸ̈"Ð†Ã×MÕÄ«ÌT¿@'¯…

ßßqí «ÿⱦ6J• Â̧¶k̈—L%̃ₒ̧ₚ̧}…\ 1\ÇH⫫q| Ꞌ¡²‡Ö̧À̈Ⱨ̧i)ø
ßçáÿ¾û6ú4(ε¼q¬éa·ò,¿ &\—ﬁ̧R½2¬4½̧6̧̂êÞî̧ᵽ "{%Ⅰ̧
ß,…..?]Þ æ̧ ¡Þ·l"×Ê¾• ßP5 ð̧o™žûã nè ᵥₗyc35u¾]})¨
ß…ﬂ̧Ⅰ̧,BÒÑ̈ₗ§̧û ÝÑ̃†¥̧Z•Ò̧ⱼ̈Ⱳⱥ̧ÖⱧ̧mₐ̧kä]×÷q̧Ü̃¼̈ₗ"[_e¤
ß.Ⱨ̧₋x¦ﬁ̧Þ }2Ã Eú̧î²g¤ZÐ…Ø̧`èⱿ̧ⱳ̧¢=§!BⱲ̧Ɛ̧ⱺ̧Ƥ̧Ḁ̈ksŽ•

---

convergence of _ towards a limit given by = 1 (with remaining unchanged at? 1). Thus, all other parameters (and) remaining the same, nonlinearity (quantified by) becomes a deciding factor in determining the character of a dependency network.

With the measured values of = ? 1 and = ? 2, as derived from the data for both types of network, the saturation properties in the network (for any value of) can, therefore, be expressed in a simplified form from Eq. (2) by the solution

$$\tilde{\varsigma}(c) = \varpi - \left(\frac{\supset}{\varpi_c}\right)^{\curlyvee} \tag{4}$$

The implications of the foregoing result are striking. One of these is that nonlinearity (or nonhomogeneity) sets a firm lower bound to the number of the rich nodes in the saturation

FIG. 3: For the distribution of all the links, irrespective of their directional properties, the power-law fit of = ? 2 is effective only on the intermediate scales. For larger values of x, the departure from the fit is misleading. This region is better modelled in the way it has been shown in Figs. 1 & 2. A solitary top node is to be seen for x ?9000.

regime (corresponding to high values of x), regardless of any arbitrarily high value of x, i.e. ? ̈ _ as x ? ̈ ⱦ. This obvious deviation from the power-law regime enables a few top nodes in the network of outgoing links to get disproportionately rich, as shown in Fig. 2, in a process that is somewhat reminiscent of Bose-Einstein condensation in complex networks [17, 18]. The situation is quite the opposite for the network of

incoming nodes, as Fig. 1 shows, where the top nodes ought to have accreted more links if a pure power law were to have been followed. The crucial qualitative result of all this is that nonlinearity also serves to distinguish the directional characteristics of a network, depending on the value and especially the sign of . And this affords an unambiguous quantitative means to differentiate between networks of incoming and outgoing links. Otherwise a simplistic distribution of *all* nodes and links taken as a whole, without accounting for the directedness of the links, can lead to a misleading picture, as it has been shown in Fig. 3. A scale for the onset of the nonlinearity-driven saturation effects can also be ascertained by requiring the two terms on the right hand side of Eq. (4) to be in rough equipartition with each other. This will yield the saturation scale in the distribution network as xsat c\ \$^{-1/2}$. The *Debian* data indicate that roughly the top 1% of the nodes fall within this scale, with the package *libc6* seeming to be the most profusely connected node (having 9026 links) in the entire network.

Some very weakly-linked nodes (for small values of x) may also be noticed in Figs. 1 & 3. These nodes deviate from the power-law solution as well. The present literature in the domain of econophysics, where all relevant data distributions are nearly the same as what has been shown here, indicates that the distribution of such feeble nodes might very well be theoretically modelled by a Boltzmann-Gibbs or a log-normal distribution [6, 1922], below a certain lower cut-off value of x (the lower limit of the range of the power-law regime).

4.   Dynamic Evolution

The *FOSS* network is not a static entity. Rather it is a dynamically evolving network, undergoing continuous additions (even deletions) and modifications across several generations of *Debian* releases, contributed by the community of free-software developers. So any realistic model should account for this evolutionary aspect of the network distribution. And indeed, by now many theoretical models [2325] have afforded varied insight into the general question of dynamic evolution of networks. It has also been demonstrated conclusively that scale-

$$\frac{\partial \phi}{\partial t} = -x \frac{\partial \phi}{\partial x} - \lambda \left(\frac{x}{c}\right)^{\lambda}, \qquad (5)$$

$$\frac{dt}{\tau} = \frac{dx}{x} = \frac{d\phi}{\lambda (x/c)^{\lambda}}, \qquad (6)$$

$$f\left(\ln x + \frac{t}{\tau}\right) = \phi - \left(\frac{x}{c}\right)^{\lambda}, \qquad (7)$$

$$\phi(x,\tau) = \eta + \left(\frac{x}{c}\right)^{\lambda} \left[1 - \exp\left(\frac{\lambda t}{\tau}\right)\right], \qquad (8)$$

converge to the distribution given by Eq. (4), for t ? 8 . In this regard the initial condition and its consequences are worth stressing. The evolution of started with a homogeneous distribution, , but during the evolution the entire network got dynamically self-organised in such a manner, that the eventual static scalefree distribution had its saturation properties determined by what the homogeneous initial field was like (at t = 0). And of course, this also serves to characterise the directional properties among the links in the steady network.

While the solution given by Eq. (8) approaches the static scale-free distribution exponentially through time, another simple linear model described by (without altering the static condition implied by Eq. (5) in anyway) = (/ x) c⁻ x⁻¹, gives, on applying the method of characteristics, a power-law type of convergence towards the static distribution, as (x, t) = + (x/c) - c⁻ [x + (t/)] , for = - 2 and t ? 8 . This diversity of modelling, as it frequently happens while studying the development of complex structures [28], can suggest a precise direction for analysing data, and allow for a better understanding of the governing mechanisms behind the dynamics.

5. Conclusion

The significance of nonlinearity and saturation, as regards a quantitative characterisation of the incoming and outgoing distribution in the *Debian GNU/Linux* network, has been cogently argued for. One might rightly expect to encounter similar features in other networks. And indeed, given the possibility that the entire network of software packages in an operating system can be construed to be a cognitive (albeit nonautonomous) system, its characteristics can furnish a model that can shed light on much more complex but realistic autonomous cognitive systems, such as the human society, or even the human mind.

Reference

1. M. Newman, A.-L. Barab´asi, and D. J.Watts, *The Structure and Dynamics of Networks* (Princeton University Press, Princeton and Oxford, 2006). [2] S. N. Dorogovtsev and J. F. F. Mendes, cond-mat/0106144.

2. R. Albert and A.-L. Barab´asi, Rev. Mod. Phys. 74, 47 (2002).

3. M. E. J. Newman, SIAM Review 45, 167 (2003).

4. R. Albert, H. Jeong, and A.-L. Barab´asi, Nature 401, 130 (1999).

5. P. Richmond, S. Hutzler, R. Coelho, and P. Repetowicz, *Econophysicsand Sociophysics,* Pg.131 (Eds. B. K. Chakrabarti, A. Chakraborti & A. Chatterjee) (WILEY-VCH Verlag GmBH & Co. KGaA, Weinheim, 2006).

6. A. K. Gupta, *Econophysics and Sociophysics,* Pg.161 (Eds. B. K. Chakrabarti, A. Chakraborti & A. Chatterjee) (WILEY-VCH Verlag GmBH & Co. KGaA, Weinheim, 2006).

7. A. Chatterjee and B. K. Chakrabarti(Eds.), *Econophysics of Markets and Business Networks* (Springer-Verlag Italia, Milano, 2007).

8. M. Steyvers and J. B. Tenenbaum, Cognitive Science: A Multidisciplinary Journal 29(1), 41 (2005).

9. S. Valverde and R. V. Sol´e, cond-mat/0307278.

10. N. LaBelle and E. Wallingford, cs/0411096.

11. T. Maillart, D. Sornette, S. Spaeth, and G. von Krogh, Phys. Rev. Lett. 101, 218701 (2008).

12. X. Gabaix, The Quarterly Journal of Economics 114, 739 (1999).

13. A.-L. Barab´asi and H. E. Stanley, *Fractal Concepts in Surface Growth* (Cambridge University Press, Cambridge, 1995).

14. R. N. Mantegna and H. E. Stanley, *An Introduction to Econophysics* (Cambridge University Press, Cambridge, 2000).

15. S. H. Strogatz, *Nonlinear Dynamics and Chaos* (Addison-Wesley Publishing Company, Reading, MA, 1994).

16. G. Bianconi and A.-L. Barab´asi, Europhys. Lett. 54(4), 436 (2001).

17. G. Bianconi and A.-L. Barab´asi, Phys. Rev. Lett. 86, 5632 (2001).

18. A. Dr˘agulescu and V. Yakovenko, Eur. Phys. J. B 17, 723 (2000).

19. A. Dr˘agulescu and V. Yakovenko, Eur. Phys. J. B 20, 585 (2001).

20. A. C. Silva and V. Yakovenko, Europhys. Lett. 69(2), 304 (2005).

21. A. Chatterjee and B. K. Chakrabarti, Eur. Phys. J. B 60, 135 (2007).

22. A.-L. Barab´asi and R. Albert, Science 286, 509 (1999).

23. P. L. Krapivsky, S. Redner, and F. Levyraz, Phys. Rev. Lett. 85, 4629 (2000).

24. S. N. Dorogovtsev, J. F. F. Mendes, and A. N. Samukhin, Phys.Rev. Lett. 85, 4633 (2000).

25. A.-L. Barab´asi, R. Albert, and H. Jeong, Physica A 272, 173 (1999).

26. L. Debnath, *Nonlinear Partial Differential Equations for Scientists and Engineers* (Birkh¨auser, Boston, 1997).

27. A. J. Koch and H.Meinhardt, Rev.Mod. Phys. 66, 1481 (1994).

Invitation and Guidelines for Contributers

PRAGYAAN : Journal of Information Technology, is a biannual publication of IMS, Dehradun. Its objective is to create a platform, where ideas, concepts and applications related to Management can be shared. Its focus is on pure research, applied and emerging issues in management.

The articles are invited from academicians, practicing managers and research scholars.

Guidelines for Contributors

1. The whole document should be in **Times New Roman**, single column, 1.5 line spacing. A soft copy of the document formatted in MS Word 97 or higher should be sent as submission for acceptance.

2. Title of the paper should be use font Times New Roman 16", Bold.

3. Author names should be in 12", Bold, followed by affiliations in normal 12" font size. Names of all the authors must be in the same row. First author will be considered for all communication purposes.

4. First Page of the document should contain Title and Author names followed by 4-5 lines about each author. Nothing else should be written on this page.

5. The following pages should contain the text of the paper including: Title, Abstract, Keywords, Introduction, Subject Matter, Conclusion & References. Author names should not appear on this page to enable blind review.

6. All paragraph headings should be Bold, 12".

7. Place tables/figures/images in text as close to the reference as possible. Table caption should be above the table. Figure caption should be below the figure. These captions should follow Times New Roman 11".

8. Provide a numbered list of references used in the text, at the end of the document. The list should be ordered alphabetically by first author, and referenced by numbers in brackets [1]. Citations to be given at the end of document should follow the following format.

   [1] Panther, J. G., Digital Communications, 3rd ed., Addison-Wesley, San Francisco, CA (1999).

9. Use non-proportional font (san serif, 11") for contents (such as source code) to be separated from main text.

10. Do not include headers, footers or page numbers in your submission. These will be added when the publications are compiled.

11. Section headings should be bold. Subsection headings should be bold + italics. Font size in both cases should remain as 12".

12. Page size should be 18x23.5 cm (7"x9.25"), justified on the page, beginning 1.9 cm (.75") from the top of the page and ending with 2.54 cm (1") from the bottom. The right and left margins should be 1.9 cm (0.75"). Number of pages should not exceed 10.

13. Articles which are published should not be reproduced or reprinted in any other form either in full or in part without the prior permission of the editor.

14. Wherever copyrighted material is used, the author should be accurate in reproduction and obtain permission from the copyright holders, if necessary.

15. Papers presented or submitted in a seminar must be clearly indicated at the bottom of the first page.

16. All manuscripts should be addressed to:

Monika Chauhan
Editor
PRAGYAAN :Journal of Information Technology
Institute of Management Studies
Makkawala Greens
Mussoorie Diversion Road
Dehradun - 248009 Uttarakhand (India)
Phones: 0135-2738000, 2738001
E-mail : editor.pragyanit@gmail.com
        editorpragyaanit@ims.edu.in

To

The Editor

Pragyaan : Journal of Information Technology,
Institute of Management Studies,
Makkawala Greens,
Mussoorie- Diversion Road,
Dehradun
Pin- 248001, Uttarakhand
Fax: +91-0135-2738005
E-mail : editor.pragyanit@gmail.com
         editorpragyaanit@ims.edu.in

Sir,

Sub: Assignment of Copyright

I/We, _____, author(s) of
the article entitled

_____

do hereby authorize you to publish the above said article in **PRAGYAAN: JOURNAL OF INFORMATION TECHNOLOGY**

I/We further state that:

1)   The Article is my/our original contribution. It does not infringe on the rights of others and does not contain any libelous or unlawful statements.

2)   Wherever required I/We have taken permission and acknowledged the source.

3)   The work has been submitted only to this journal **PRAGYAAN: JOURNAL OF INFORMATION TECHNOLOGY** and that it has not been previously published or submitted elsewhere for publication.

I/We hereby authorize you to edit, alter, modify and make changes in the Article in the process of preparing the manuscript to make it suitable for publication.

I/We hereby assign all the copyrights relating to the said Article to the **Institute of Management Studies, Dehradun.**

I/We have not assigned any kind of rights of the above said Article to any other person/Publications.

I/We agree to indemnify the **Institute of Management Studies, Dehradun.** against any claim or action alleging facts which, if true, constitute a breach of any of the foregoing warranties.

First author   **Second author**   **Third author**

1. Name: 2. Name: 3. Name:

Signature: Signature: Signature:

SUBSCRIPTION/ADVERTISEMENT RATES

The Subscription rates for each of our three journals, viz., Pragyaan: Journal of Information Technology, Pragyaan: Journal of Management and Pragyaan: Journal of Mass Communication are as follows:

Category	1 Year		3 Years		5 Years	
	Domestic Rates (Rs.)	Foreign Rates (US $)	Domestic Rates (Rs.)	Foreign Rates (US $)	Domestic Rates (Rs.)	Foreign Rates (US $)
Academic Institutions	500	30	1200	75	2000	120
Corporate	1000	60	2500	150	4000	240
Individual Members	400	25	1000	60	1600	100
Students	300	20	700	40	1200	75

Advertisement Rates (Rs.)

Location/Period	1 Year	2 Years	3 Years
B/W (Inside Page)	10,000/- (2 Issues)	18,000/- (4 Issues)	25,000/- (6 Issues)
Colour (Inside Back Cover)	17,000/- (2 Issues)	30,000/- (4 Issues)	45,000/- (6 Issues)
Single Insertion (1 Issue) (Inside B/W Page) - Rs.5000/-			

------------✂--✂------------

SUBSCRIPTION FORM

I wish to subscribe to the following journal(s) of IMS, Dehradun:

Name of Journal	No. of Years	Amount
Pragyaan: Journal of Information Technology	☐	☐
Pragyaan: Journal of Management	☐	☐
Pragyaan: Journal of Mass Communication	☐	☐
Total		☐

A bank draft/cheque bearing no _____ dated_____ for Rs. _____ Drawn in favour of Institute of Management Studies, Dehradun towards the subscription is enclosed. Please register me/us for the subscription with the following particulars:

Name _____ (Indiviual/Organisation)

Address_____

_____

Phone_____ Fax _____ E- mail_____

Date: _____   Signature (individual/authorized signatory)

Please send the amount by DD/Local Cheque favouring Institute of Management Studies Dehradun, for timely receipt of the journal. Outstation cheques shall not be accepted.

Please cut out and mail along with your cheque/DD to: The Registrar, Institute of Management Studies, Makkawala Greens, Mussorrie Diversion Road, Dehradun 248009, Uttarakhand, India
Phone No. 0135-2738000, 2738001

IMS at a glance

The recent call for knowledge capital has increased the demand for a quality education specifically in professional courses like IT, Management, and Mass Communication.

With a focus on catering to the demands of modern industry, Institute of Management Studies, Dehradun started its venture in the year 1996, under the aegis of IMS Society, which is registered body under The Societies Registration Act 1860.

The potential employers of professional students today are looking for visionaries with skills to create future. IMS Dehradun has accordingly taken a stride to produce world class professionals. It is totally committed to provide high quality education, enhance the intrinsic abilities, and promote managerial and technological skills of the students.

IMS has been constantly pouring its efforts to upgrade effectiveness of educational process, and is committed to:
- Provide sound academic environment to students for complete learning.
- Provide state of-art-technical infrastructure.
- Facilitate students and staff to realize their potential.
- Promote skills of the students for their all round development.

Since its inception, it has been conducting professional courses in business administration, information technology and mass communication in a best professional manner. These courses are affiliated to Uttarakhand Technical University or HNB Garhwal University, Uttarakhand. Today more than 2000 students are admitted at the Institute in courses like PGDM, MBA, MCA, MIB, MA (Mass Comm.), BBA, BCA, B.Sc. (IT) and BA (Mass Comm.). Our courses, namely, PGDM, MBA and MCA are duly approved by AICTE and Ministry of HRD, Government in India.

The Institute has also taken up activities to facilitate respectable placement for our students. Our Corporate Resource Center (CRC) has been working with the industry to cater to its current needs effectively and the final placement scenario has been phenomenal. Many organizations are showing strong desires to have our students on board as their employees. For all round development of our students, many extra curricular activities are arranged. This is proving to be useful in translating efforts of our students into positive results.

The Institute brings out three Journals, one each in the three disciplines of IT, Management, and Mass Communication, in an effort to fulfill our objective of facilitating and promoting quality research work in India.