International Journal of Computer Science and Security (IJCSS)

ISSN : 1985-1553

VOLUME 2, ISSUE 4

PUBLICATION FREQUENCY: 6 ISSUES PER YEAR

International Journal of Computer Science and Security (IJCSS)

Book: 2008 Volume 2, Issue 4
Publishing Date: 30-08-2008
Proceedings
ISSN (Online): 1985-1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Table of Contents

Volume 2, Issue 4, August 2008.

Pages

On Reliability Analysis of Fault-tolerant Multistage Interconnection Networks

Rinkle Aggarwal
Department of Computer Science & Engineering,
Thapar University,
Patiala –147004 (India)
raggarwal@thapar.edu

Dr. Lakhwinder Kaur
Department of Computer Engineering,
Punjabi University,
Patiala–147002 (India)
mahal2k8@yahoo.com

Abstract

The design of a suitable interconnection network for inter-processor communication is one of the key issues of the system performance. The reliability of these networks and their ability to continue operating despite failures are major concerns in determining the overall system performance. In this paper a new irregular network IABN (Irregular Augmented Baseline) has been proposed. IABN is designed by modifying existing ABN (Augmented Baseline) network. ABN is a regular multi-path network with limited fault tolerance. IABN provides three time more paths between any pair of source-destination in comparison to ABN. The reliabilities of the IABN and ABN multi-stage interconnection networks have been calculated and compared in terms of the Upper and Lower bounds of Mean time to failure (MTTF). The proposed network IABN provides much better fault-tolerance and reliability at the expanse of little more cost than ABN.

Keywords: Multistage Interconnection Networks, Reliability, Augmented Baseline Network, Irregular Augmented Baseline Network, Fault-tolerance.

1. INTRODUCTION

Advances in LSI and VLSI technology are encouraging greater use of multiple-processor systems with processing elements to provide computational parallelism and memory modules to store the data required by the processing elements. Interconnection Networks (INs) play a major role in the performance of modern parallel computers. Many aspects of INs, such as implementation complexity, routing algorithms, performance evaluation, fault-tolerance, and reliability have been the subjects of research over the years. There are many factors that may affect the choice of appropriate interconnection network for the underlying parallel computing environment [5,6]. Though crossbar is the ideal IN for shared memory multiprocessor, where N inputs can simultaneously get connected to N outputs, but the hardware cost grows astronomically. Multistage Interconnection Networks (MINs) are recognized as cost-effective means to provide programmable data paths between functional modules in multiprocessor systems [1]. These networks are usually implemented with simple modular switches, employing two-input two-output switching elements. Most of the MINs proposed in the literature have been constructed with 2x2 crossbar switches as basic elements, and have $n = \log_2 N$ switching stages with each stage consisting of N/2 elements, which makes the cost of this network as O(NlogN), as compared to $O(N^2)$ for a crossbar [4]. The pattern of interconnection may be uniform or non-uniform, which classifies the MINs to be regular or irregular respectively [7]. In the case of irregular networks, the path length varies from any input to any output, in contrast with regular networks, where it is the same [10]. Fault-tolerance in an interconnection network is very important for its continuous operation over a relatively long period of time [8]. Fault-tolerance is the ability of the network to operate even in the presence of faults, although at a degraded performance. Permutation capability and other issues related to MINs have also been widely covered, but little attention has been paid to the reliability of these networks. Reliability [8] of a system is the probability that it will perform its intended function satisfactorily for a given time under stated operating conditions. Reliability can be measured in terms of Mean Time to Failure (MTTF). The MTTF of a MIN is defined as the expected time elapsed before some source is disconnected from some destination [3]. The analysis is based on the lower and upper bounds of the network reliability. This paper is organized as follows : Section 2 describes the structure and design of ABN and proposed network IABN. Section 3 provides the reliability analysis of ABN. Section 4 discuss the reliability analysis of IABN. Finally conclusions are given in Section 5.

2. STRUCTURE AND DESIGN OF NETWORKS

2.1 ABN (Augmented Baseline Network)

An ABN of size N x N consists of, two identical groups of N/2 sources and N/2 destinations. The switches in the last stage are of size 2 x 2 and the remaining switches in stages 1 through n-3 ($n=\log_2 N$) are of size 3 x 3 [9]. In each stage, the switches can be grouped into conjugate subsets, where a conjugate subset is composed of all switches in a particular stage that lead to the same subset of destinations. The switches, which communicate through the auxiliary links, form a conjugate loop. The conjugate loops are formed in such a way that the two switches, which form a loop, have their respective conjugate switches in a different loop. This pair of loops are called conjugate loops [1]. Each source is linked to both the groups via multiplexers. An ABN of size 16 x 16 is illustrated in Fig. 1.

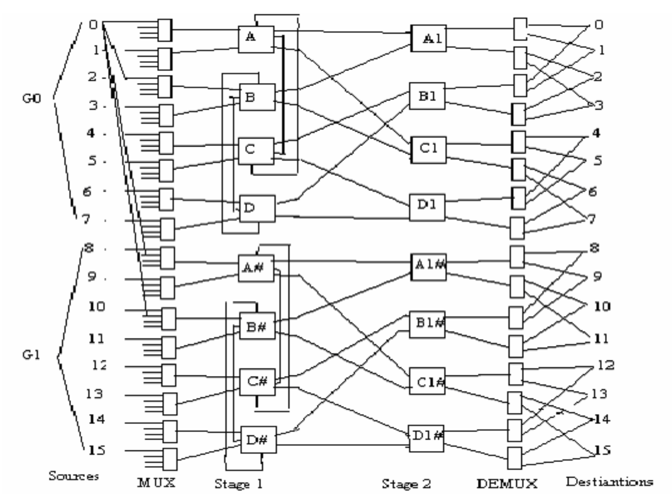


FIGURE 1: An ABN of size 16 X 16.

2.2 IABN (Irregular Augmented Baseline Network)

An Irregular Augmented Baseline Network is an augmented baseline network with one additional stage, additional auxiliary links and increased size of demultiplexers. An IABN of size N x N consists of two identical groups of N/2 sources and N/2 destinations. Each group consists of a multiple path modified baseline network of size N/2. The switches in the last stage are of size 2 x 2 and the remaining switches in stages 1 through n-2 ($n=log_2N$) are of size 3 x 3. In each stage, the switches can be grouped into conjugate subsets, where a conjugate subset is composed of all switches in a particular stage that lead to the same subset of destinations. The modified baseline network achieves the multiple path property by permitting two switches in the same conjugate subset that are not a conjugate pair to communicate through auxiliary links. Each source is linked to both the groups via multiplexers. There is one 4 x 1 MUX for each input link of a switch in stage 1 and one 1 x 4 DEMUX for each output link of a switch in stage n-1. Each group consisting of a modified baseline network of size N/2 plus its associated MUXs and DEMUXs is called a subnetwork. Thus an IABN consists of two identical sub-networks which are denoted by G^i. For example, in Figure 1, switches A, B, C, D belonging to stage 1 of a subnetwork (G^i) form a conjugate subset, switches A and B form a conjugate pair, and switches A and C form a conjugate loop.

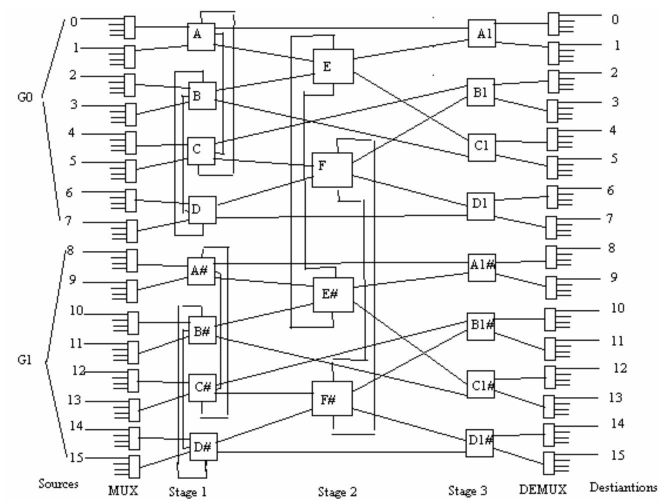


FIGURE 2 : An IABN of size 16 X 16.

2.3 Routing tag for ABN and IABN

A source selects a particular subnetwork (G^i) based upon the most significant bit of the destination. Each source is connected to two switches (primary and secondary) in a subnetwork. Let the source S and destination D be represented in binary code as:

$S=s_0, s_1,\ldots,s_{n-2},s_{n-1}$
$D=d_0, d_1,\ldots,d_{n-2},d_{n-1}$

(i) Source S is connected to the ($s_1,\ldots,s_{n-2}$) primary switch in both the sub-networks through the multiplexers.
(ii) Source S is also connected to the [{($s_1,\ldots,s_{n-2}$)+1}mod N/4] secondary switch in both the sub-networks through the multiplexers.

3. RELIABILITY ANALYSIS OF ABN

3.1 Upper bound (optimistic)

In ABN each source is connected to two multiplexers in each sub-network, and each switch has a conjugate. So if we assume that the ABN is operational as long as one of the two multiplexers attached to a source (in a particular sub-network) is operational and as long as a conjugate pair (loop or switch) is not faulty, then we will permit as many as one half of the components to fail and the ABN may still be operational. This permits a simple reliability block diagram of the optimistic (upper) bound as shown in Figure 3.

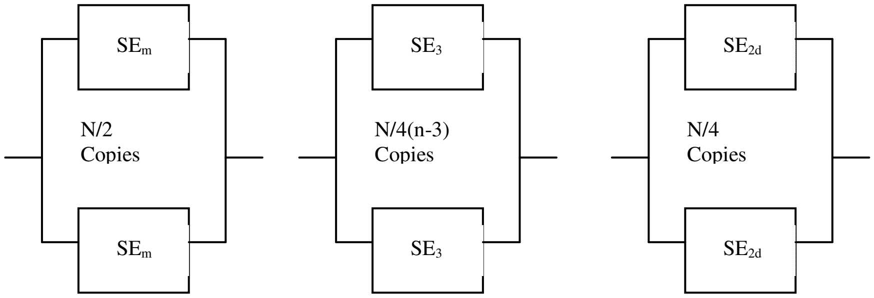


FIGURE 3: Reliability block diagram of ABN for MTTF upper bound.

The expression for the upper bound of the ABN reliability is:

$R_{ABN\text{-}ub}(t) = f1 * f2 * f3$

$$f1 = \left[1 - \left(1 - e^{-\lambda_m t}\right)^2\right]^{\left(N/2\right)}$$

$$f2 = \left[1 - \left(1 - e^{-\lambda_3 t}\right)^2\right]^{N/4(n-3)}$$

$$f3 = \left[1 - \left(1 - e^{-\lambda_{2d} t}\right)^2\right]^{\left(N/4\right)}$$

Where,

$\lambda_m = \lambda$, $\lambda_3 = 2.25\lambda$, $\lambda_{2d} = 2\lambda$

$$MTTF_{ABN\text{-}ub} = \int_0^\infty R_{ABN\text{-}ub}(t).dt$$

3.2 Lower bound (pessimistic)

At the input side of the ABN, the routing scheme does not consider the multiplexers to be an integral part of a 3 x 3 switch. For example, as long as at least one of the two multiplexers attached to a particular switch is operational, the switch can still be used for routing. Hence, if we group two multiplexers with each switch in the input side and consider them a series system (SE_{3m}), then we will have a conservative estimate of the reliability of these components. Their aggregate failure rate will be $\lambda_{3m} = 4.25\lambda$. Finally these aggregated components and the switches in the intermediate stages can be arranged in pairs of conjugate loops. To obtain the pessimistic (lower) bound on the reliability of ABN, we assume that the network is failed whenever more than one conjugate loop has a faulty element or more than one conjugate switch in the last stage fails. The reliability block diagram is shown in Figure 4.

$R_{ABN\text{-}lb}(t) = f1 * f2 * f3$

$$f1 = \left[1 - \left(1 - e^{-2\lambda_m t}\right)^2\right]^{\left(N/8\right)}$$

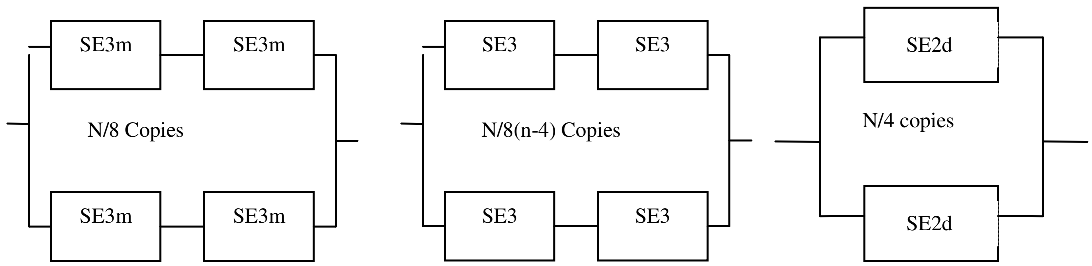


FIGURE 4: Reliability block diagram of ABN for MTTF lower bound.

$$f2 = \left[1-\left(1-e^{-2\lambda_3 t}\right)^2\right]^{N/8(n-4)}$$

$$f3 = \left[1-\left(1-e^{-\lambda_{2d} t}\right)^2\right]^{\left(N/4\right)}$$

Where,

$\lambda_{3m=}4.25\lambda$, $\lambda_{3=}2.25\lambda$, $\lambda_{2d=}2\lambda$

$MTTF_{ABN\text{-}lb} = \int_0^\infty R_{ABN\text{-}lb}(t).dt$

4. RELIABILITY ANALYSIS OF IABN

4.1 Upper bound (optimistic)

In IABN each source is connected to two multiplexers in each sub-network, and each switch has a conjugate. So if we assume that the IABN is operational as long as one of the two multiplexers attached to a source (in a particular sub-network) is operational and as long as a conjugate pair (loop or switch) is not faulty, then we will permit as many as one half of the components to fail and the IABN may still be operational. This permits a simple reliability block diagram of the optimistic (upper) bound as shown in Figure 5.

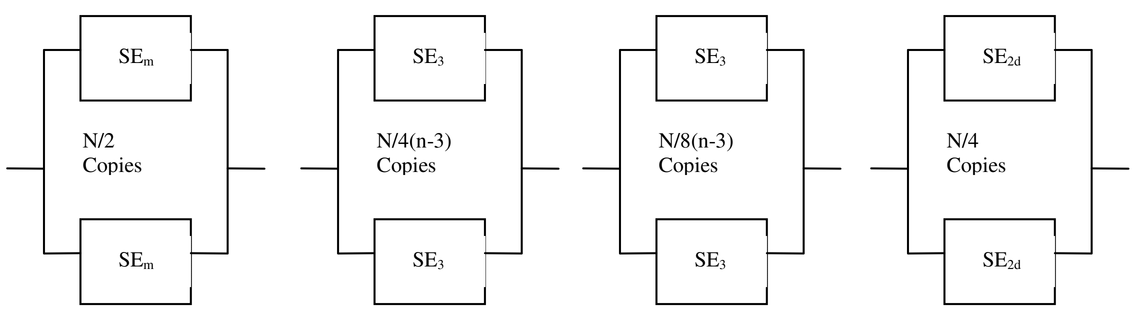


FIGURE 5: Reliability block diagram of MABN for MTTF upper bound.

$R_{IMABN\text{-}ub}(t) = f1 * f2 * f3 * f4$

$$f1 = \left[1-\left(1-e^{-\lambda_{m} t}\right)^2\right]^{\left(N/2\right)}$$

$$f2 = \left[1 - \left(1 - e^{-\lambda_3 t}\right)^2\right]^{N/4(n-3)}$$

$$f3 = \left[1 - \left(1 - e^{-\lambda_3 t}\right)^2\right]^{N/8(n-3)}$$

$$f4 = \left[1 - \left(1 - e^{-\lambda_{2d} t}\right)^2\right]^{\left(N/4\right)}$$

Where $\lambda_{m=}\lambda$, $\lambda_{3=}2.25\lambda$, $\lambda_{2d=}3\lambda$

$$MTTF_{IABN-ub} = \int_0^\infty R_{IABN-ub}(t).dt$$

4.2 Lower bound (pessimistic)

At the input side of the IABN, the routing scheme does not consider the multiplexers to be an integral part of a 3 x 3 switch. For example, as long as at least one of the two multiplexers attached to a particular switch is operational, the switch can still be used for routing. Hence, if we group two multiplexers with each switch in the input side and consider them a series system (SE_{3m}), then we will have a conservative estimate of the reliability of these components. Their aggregate failure rate will be $\lambda_{3m} = 4.25\lambda$. Finally these aggregated components and the switches in the intermediate stages can be arranged in pairs of conjugate loops. To obtain the pessimistic (lower) bound on the reliability of IABN, we assume that the network is failed whenever more than one conjugate loop has a faulty element or more than one conjugate switch in the last stage fails. The reliability block diagram is shown in Figure 6.

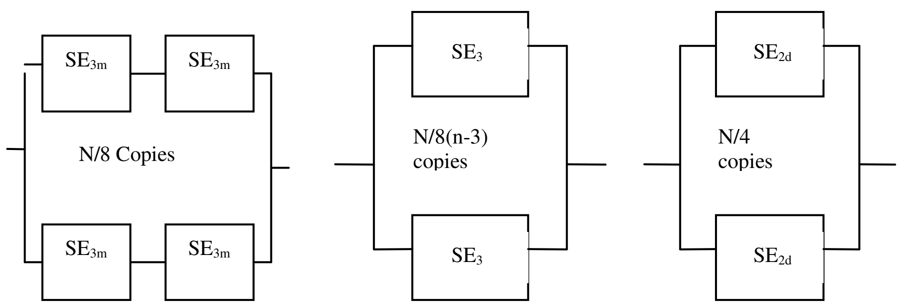


FIGURE 6: Reliability block diagram of MABN for MTTF lower bound.

$R_{IABN-lb}(t)$= f1 * f2 * f3

$$f1 = \left[1 - \left(1 - e^{-2\lambda_{3m} t}\right)^2\right]^{\left(N/8\right)}$$

$$f2 = \left[1 - \left(1 - e^{-\lambda_3 t}\right)^2\right]^{N/8(n-3)}$$

$$f3 = \left[1 - \left(1 - e^{-\lambda_{2d} t}\right)^2\right]^{\left(N/4\right)}$$

Where $\lambda_{3m=}4.25\lambda$, $\lambda_{3=}2.25\lambda$, $\lambda_{2d=}3\lambda$

$$MTTF_{IABN-lb} = \int_0^\infty R_{IABN-lb}(t).dt$$

The results of the MTTF Reliability equations have been shown in Table 1.

LogN	**ABN**		**IABN**	
	Lower Bound	*Upper Bound*	*Lower Bound*	*Upper Bound*
4	4.934369	5.141202	5.665934	5.847616
5	4.717386	4.923061	5.437529	5.556905
6	4.508375	4.71246	5.223375	5.302414
7	4.30494	4.507272	5.018943	5.068058
8	4.105551	4.306118	4.821243	4.846257
9	3.909194	4.108067	4.628248	4.632892
10	3.71518	3.912467	4.438573	4.425513

TABLE 1: MTTF of ABN and IABN for different network size

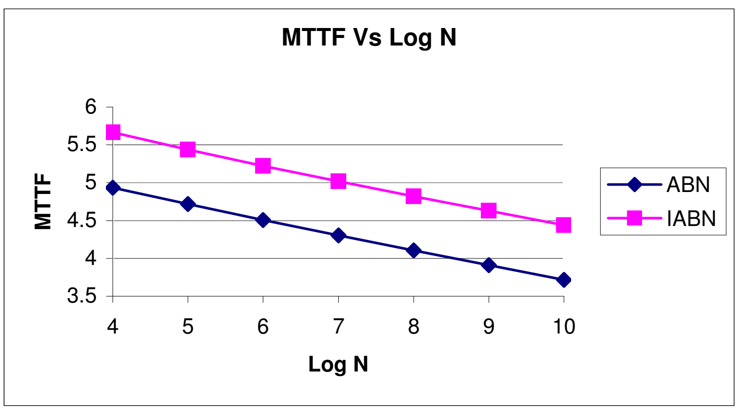


FIGURE 7: MTTF (Lower Bound) comparison of ABN and IABN

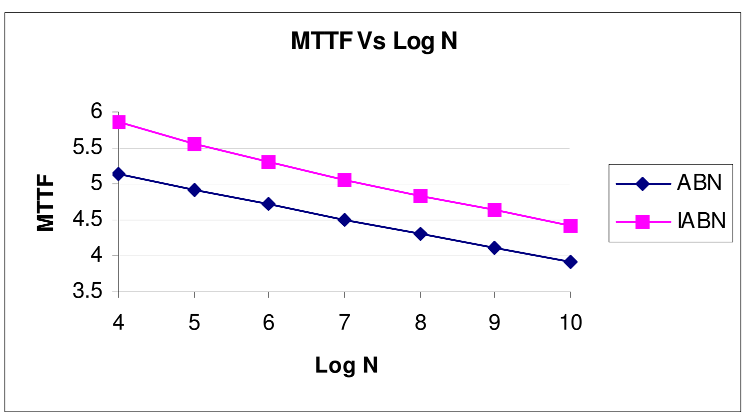


FIGURE 8: MTTF (Upper Bound) comparison of ABN and IABN

5. CONCLUSION

An Irregular Augmented Baseline Network (IABN) is designed from regular Augmented Baseline Network (ABN) have one extra stage. IABN is a dynamically re-routable and provides multiple paths of varying lengths between a source-destination pair. It has been found that in an IABN, there are six possible paths between any source-destination pair, whereas ABN has only two paths with same length. Thus proposed IABN is more fault-tolerant. The reliability analysis shows that IABN has better performance than ABN for both lower and upper bounds.

6. REFERENCES

1. Aggarwal R., Aggarwal H. and Kaur L., “On Bandwidth analysis of Irregular Fault-tolerant Multistage Interconnection networks”, International Review on Computers and Software, Vol. 3, No. 2, March 2008, pp. 199-202.

2. Aggarwal H., and Bansal P.K., Routing and Path Length Algorithm for cost effective Modified Four Tree Network, IEEE TENCON, 2002, pp. 293-294.

3. Bansal P.K., Joshi R.C. and Singh K., “On a fault-tolerant Multi-stage interconnection network”, International Journal of Electronics and Electrical Engineering, Vol 20, No.4, 1994,, pp. 335-345.

4. Bansal P.K.,Joshi R.C, Singh K. and Siroha G.P., “Fault-tolerant Augmented Baseline Multistage Interconnection Network”, International Conference IEEE TENCON 91, INDIA, Aug. 1991, pp. 200-204.

5. Bhuyan Laxmi N., Yang Qing and Agrawal Dharma P., “Performance of Multiprocessor Interconnection Networks”, IEEE Computer, Vol. 22, Feb. 1993, pp. 25-37.

6. Duato Jose, Yalamanchili Sudhakar and Ni Lionel, “Interconnection Networks: An Engineering Approach”, IEEE Computer Society, 1997.

7. Lubazewski M. and Coutois B., ”A Reliable Fail-safe System”, Parallel and Distributed Systems, IEEE Computer Society, Vol. 47, No. 2, Feb. 1998, pp. 236-241.

8. Nitin, “On analytic Bounds of Regular and Irregular Fault-tolerant Multistage Interconnection Networks”, International Conference on PDPTA, June 26-29, 2006.

9. Sadawarti Harsh and Bansal P.K., “Fault tolerant Irregular Augmented Shuffle Network” WSEAS International Conference on Computer Engineering and Applications, Gold Coast, Australia, 17-19, Jan, 2007.

10. Sengupta J. and Bansal P.K, “Reliabilty and performance measures of regular and irregular multi-stage interconnection networks”, International Conference IEEE TENCON, 2000, pp. 531-536.

11. Sengupta J. and Bansal P.K., “Performance Analysis of Regular and Irregular Dynamic MINs”, International Conference IEEE TENCON 99, Sept. 1999, Cheju Island, Korea, pp. 427-430.

12. Sharma Sandeep, Kalhon K.S., Bansal P.K. and Singh Kawaljeet, “Improved Irregular Augmented Shuffle Exchange Multistage Interconnection Network”, International Journal of Computer Science and Security, Vol. 2, No. 3, 2008, pp. 28-33.

A Context Transfer Approach to Enhance Mobile Multicast

AISHA-HASSAN A. HASHIM aisha@iiu.edu.my
Faculty of Engineering/ Electrical and Computer Department
International Islamic University Malaysia
Kuala Lumpur, 53100, Malaysia

ABDI NASIR AHMED abdinaser_10@hotmail.com
Faculty of Engineering/ Electrical and Computer Department
International Islamic University Malaysia
Kuala Lumpur, 53100, Malaysia

ABDULRHMAN BIN MAHFOUZ abdulrhman_bm@hotmail.com
Faculty of Engineering/ Electrical and Computer Department
International Islamic University Malaysia
Kuala Lumpur, 53100, Malaysia

Sheroz Khan sheroz@iiu.edu.my
Faculty of engineering/ Electrical and Computer Department
International Islamic University Malaysia
Kuala Lumpur, 53100, Malaysia

Abstract

With the advent of the handheld devices and multimedia applications, there has been an increasing interest for mobile multicast. IETF proposes two approaches. The first approach is Bi-directional Tunneling (BT), where the mobile node subscribes to a multicast group through its home network. The second approach is Remote Subscription (RS), where the mobile node joins the multicast group via a local multicast router on the foreign link being visited. However, in BT approach the home agent is typical far and this will lead to high signaling cost at the same time the home agent represents a single point of failure and introduces scalability issues. RS approach suffers mainly from frequent tree reconstruction. The main aim for this paper is to propose a new mobile multicast approach to reduce the signaling cost and reduce the packet loss especially in case of macromibiliy. The proposed solution integrates Hierarchical Mobile IPv6 with Mobile context transfer. This paper presents and evaluates the proposed solution. Our results shows that compared to BT approach, the proposed solution gives lower signaling cost.

Keywords: context transfer, Hierarchical Mobile IPv6, multicast, signaling cost.

1. INTRODUCTION

Nowadays, the trend of using wireless devices has increased, due to development of the wireless evolutionary systems [1] and the high demand for the Internet. Therefore**,** offering a large range of wireless mobile services to highly heterogeneous users for a highly effective handover becomes very crucial. However, it is a challenging issue to maintain the simplicity, the reachability of a MN and the continuity of the service offered to the MN when moving from one network to another, in another word during the handover. Basically, the handover is a change in MN's point of attachment to the Internet such that the MN is no longer connected to the same IP subnet as it was previously**.** In recent years**,** a great effort of research has been spent on the issue of mobility, and it proposed or resulted in development of the existing architecture and the operation of services based on context as well as specific mechanisms and protocols for support of mobility. This includes proposals on Mobile IPv6 (MIPv6) [5, 6, 9] developed by the IETF Mobile IP Working Group (WG). Also there are other solutions have been proposed for mobility support, Fast Handovers Mobile IPv6 (FMIPv6) [7, 8, 9] and Hierarchical Mobile IPv6 (HMIPv6) [9, 10, 11]. However, these solutions are not able to re-establish both IP connectivity and service context within the time constraints imposed by real-time applications such as Voice over IP. Therefore, Context Transfer Protocol (CXTP) [6, 12, and 13] has been suggested as an alternative way of restoring the service context at the new access network.

The CXTP is designed by the IETF to provide general mechanisms for exchange of context data for moving mobile nodes (MN) between access routers (AR). It gives support of the seamless handover based on service continuation using context and could be used to transfer different kind of control data and resources based services [14]. It aims to contribute to the enhancement in handover performance and proposed for MN for quickly re-establishment of their services when the nodes move and change their access routers.

2. RELATED WORK

Work in [6 and 13] specifies the multicast receiver mobility based on context transfer. Defining the multicast context transfer operations and data structures required for MLDv2. Multicast context transfer block and operational considerations for optimized multicast context transfer based on FHMIPv6 and Candidate Access Router Discovery (CARD) are described. The requirements for MLDv2 context extension and operation at access routers to support multicast context transfer for mobile IPv6 are specified. Interactions of MLDv2 with PIM-SM for multicast routing state update based on multicast listening context transfer are overviewed. CARD protocol is used in [7, 10] to choose "optimal" access networks based on the mobile node's requirements for Candidate Access Router (CAR)'s capabilities. However, more focus is given to multicast listeners.

Mobile multicast in the framework of HMIPv6 approach is discussed in [10]. The multicast packet forwarding is based on mobility anchor points defined for the HMIPv6 architectures. However this proposal suffers in case of inter domain mobility. In [13], different approaches are overviewed to achieve sender and receiver multicast mobility in internet environment. It describes the problems faced by the multicast senders and multicast receivers, as well as the available solutions to senders and receivers.

3. DESIGN OF THE PROPOSED SOLUTION (HMMCT)

- Problem Statement

The main goal of the mobile IPv6 is to re-establish the service for the mobile device as long as it moves to a new network. In another words, the Mobile IPv6 maintain the reachability while moving in the IPv6 network. At the same time, the group communication has also become a need for the people, because of its use in variety of application including video conferencing, voice over IP, and massive multiplayer gaming. As a result, the integration of both the multicast IP and mobile IP (multicast mobility/mobile multicast) become a crucial in our daily life. Mobile multicast becomes the backbone for numerous applications ranging from the multimedia conference scenarios where the host can be the sender or the receiver, to the real-time communication such as voice over IP which require seamless handover to limit the disruptions or delay. Unfortunately, the existing mobility support specification does not support the multicast. As a result, the possibilities of using multicast in mobile environment suffers so many problems such as packet loss, packet latency, join latency, tree reconstruction, and higher signaling cost and so on. As a consequence the IETF proposed two solutions based on the MIPv6 which are bidirectional tunneling and remote subscription. However, these two solutions are not efficient and effective especially, during the hand off period.

- Current Challenges

The difficulties or the challenges of mobile multicast can be summarized as follows:

- The existing IP multicast protocols does not satisfy the needs of nods for mobility.
- The handoff time of MN and the delay in rejoining multicast group is too long, so it cannot meet the QoS yet.[4]
- The reconstruction of multicast tree caused by MN handoff increase the signaling cost
- The existing IP multicast protocols have the problem of triangular route and tunnel convergence. [15, 16].
- The reconstruction of the multicast tree as the MN transfer to a new network. The MN will be receiving the multicast data in the old network, although it moves to the new network and the cost associated with tree construction is high.
- As the mobile nodes handoff to another network, the MN suffers from packet loss and joins delay.
- In case the foreign network does not support the multicast, all the multicast traffic will be rejected.
- As long as tunnel used, the process of encapsulation and decapsulation must take place, which in turn it increase the size of the header and therefore increases the cost.
- Packets out of order, and also, Packets Duplication, when receive different multicast data from different multicast router.

- The Architecture of the Proposed Solution (HMMCT)

The proposed solution, Hierarchal Mobile Multicast Context Transfer uses the multicast HMIPv6 to maintain the intra-domain mobility and uses the multicast context transfer to provide the inter-domain mobility. This HMMCT has been proposed to provide a seamless handover and to reduce the disruption for the mobile nodes whether they move within the same MAP domain or different domains and to allow the mobile nodes to receive the packets during the handover efficiently especially for real-time services and applications. As it has been said earlier the M-HMIPv6 protocol used to provide a seamless handover for the MH when moving within the same MAP domain, since the MAP works as a local home agent. However there are some limitations come with the HMIPv6 mobile multicast when a mobile host moves to a new MAP domain as stated in the design issues. So the proposed architecture HMMCT concerns to solve these problems, by utilizing the multicast context transfer between two different MAPs. The context transfer can reduce the time needed to re-establish the service since the multicast context transfer block will be transferred between the two MAPs before the handover is completed, so all the information needed for the MH to join the multicast group is already transferred and the MH can join the multicast group as soon as the mobile node moves to the new MAP domain. Also the signaling cost will be reduced since the communication is localized between the two MAPs and the mobile node doesn’t need to send the group membership message again to the new MAP since the new MAP already received the information needed for that in the multicast context transfer block. Fig (1) shows the proposed architecture.

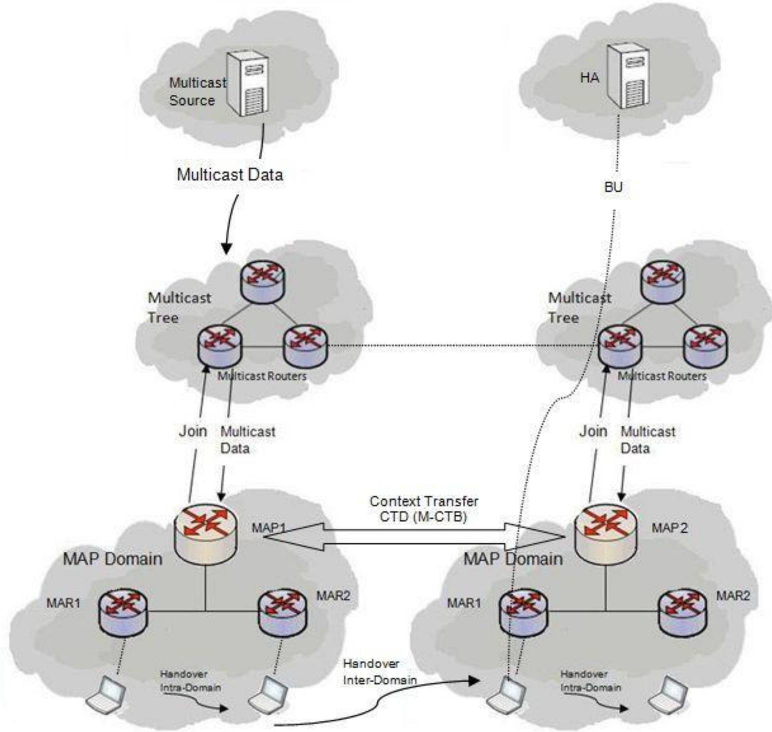


FIGURE 1: HMMCT architecture.

- How HMMCT Works

The Hierarchical Mobile IPv6 scheme introduces a new function, the MAP. A MN entering a Multicast enabled MAP's domain will learn about the regional Care-of-address, RCoA of the M-MAPs through MLD membership query. After receiving the MLD membership query, the MN sends an MLD membership report message to subscribe to a multicast group by using its on link care-of-address, LCoA. Upon reception of a tunneled MLD listener report, the M-MAP will record multicast group membership in its Binding Cache, observe and maintain multicast group membership on its specific tunnel interface, checks the MNs current group membership, and forward multicast group traffic to the MN. So the M-MAP is acting as a local HA, and will send the join message to the multicast senders and the M-MAP will receive all the multicast packets on behalf of the mobile node it is serving and then will encapsulate and forward them directly to the mobile node's current address. If the mobile node changes its current address within a local MAP domain LCoA, it only needs to register the new LCoA address with the M-MAP by sending a binding update to binds its LCoA with the RCoA of the M-MAP. Hence, the mobile node can receive the multicast packets without the need to send MLD membership report, because only the RCoA needs to be registered with correspondent nodes and the HA, and the RCoA does not change as long as the MN moves within a MAP domain. This way of handling the mobility makes the mobile node's mobility transparent to the correspondent nodes it is communicating with. But if the MN detects an inter-domain mobility, the MN will send a message to the previous M-MAP to activate the context transfer or the context transfer can be triggered by link layer 2. Specifically, a predictive multicast context transfer is used. After the context activation, the multicast context transfer block (M-CTB) is built at the previous M-MAP in interaction with multicast information in the previous M-MAP. The M-CTB includes the multicast addresses required for the multicast services of the moving mobile node. M-CTB is sent from the previous to the next M-MAP in the Context Data message. When the next M-MAP receives the context data with the M-CTB, the next M-MAP will provide the context data to the MLD for updating the multicast context and establishment of an individual node MLD context. Therefore, once the MH moves to the next M-

MAP, the MH will be able to receive the multicast packets immediately through tunneling form the next M-MAP, because the next M-MAP already sent the join message to the multicast source. Then the MLDv2 supplies the information from the M-CTB to the multicast routing protocol to build the routing context for the multicast addresses. Fig (2) shows the signal flow of HMMCT.

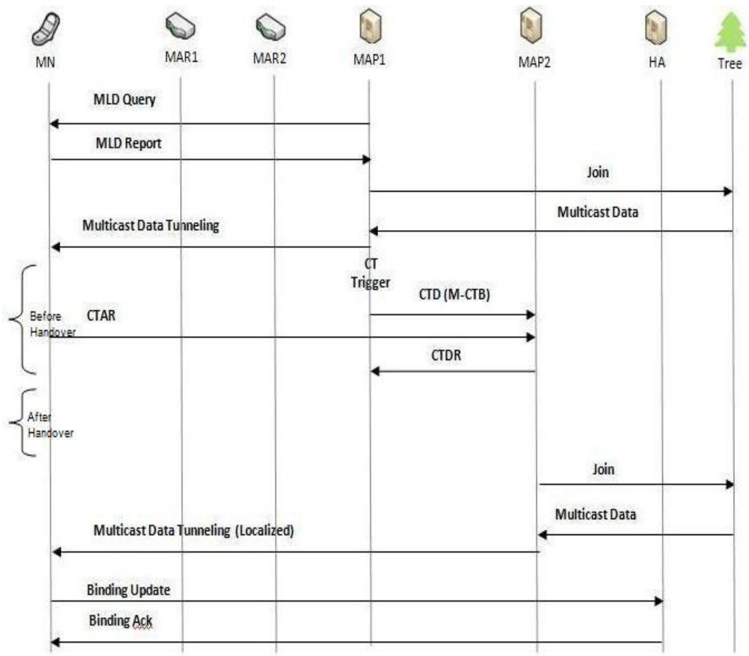


FIGURE 2: The signal flow of HMMCT

4. PERFORMANCE EVALUATION OF THE PROPOSED ARCHITECTURE

In this paper the analytical approaches will be used. The parameters used to be evaluated are the service recovery time, and signaling cost. These two different approaches will be explained next.

- Service recovery time

Referring to the signal flow diagram of HMMCT and BT, the total service recovery time is calculated and compared to each other. In the case of bi-directional tunneling, after the handover of the MN from one network to another, the total service recovery time is calculated by:

Trec. BT = T1+T2+T3

Where
T1: is the time taken to send BU message from MN to HA
T2: is the time taken for the HA to send ACK to the MN
T3: is the time taken to receive the multicast data.

The handover in HMMCT is divided in to two parts, the inter-domain mobility and intra-domain mobility. In inter domain mobility, the MN only sends BU message to the MAP and MAP reply by sending ACK to the MN, and hence the total service recovery time in this case can be calculated by:

Trec. HMMCT, inter = T4+T5+T6

Where
T4: is the time taken to send BU from the MN to the MAP
T5: is the time taken to send ACK from the MAP to MN
T6: is the time taken to receive the multicast data

The second case of the HMMCT is the intra-domain mobility, where the MN handoff from one MAP to another MAP. In this situation the context transfer protocol is used to reduce the service recovery time, and the total service recovery time for HMMCT, intra is calculated by:

Trec. HMMCT, intra = T7+T8

Where
T7: is the time taken to send the join message from the MAP to the multicast tree
T8: is the time taken to receive the multicast data.

The first case that is the BT take the highest time in order to recover the service, and this is due to the large distance between the MN and the HA, and this has been proved mathematically from the above equations. The inter domain mobility is the best and this is due to the short distance between the MN and the MAP, and even the intra-domain mobility recovery time is reduced by using the context transfer which implements the predictive signaling.

- Total Signaling Cost

It is assumed that the signaling cost is the summation of the binding update cost and the packet delivery cost. In this analysis of the signaling cost, the HMMCT is compared with the bi-directional tunneling which is the proposal of the IETF.

Firstly, the binding update cost is discussed. Each time the mobile node moves from one subnet to another subnet, the mobile node needs to send a binding update to the home agent in order to update its location. The cost of binding update is affected by different factors that are, the number of the mobile nodes, residence time of the mobile node in the subnet or the frequency of changing the subnet, the length of the path that the binding update follow in term of numbers of hops, and the encapsulation and dencapsulation processing time. The HMIPv6 divides the mobility into two parts which are micro-mobility (intra-domain) and macro-mobility (inter-domain), and this reduce the frequency of changing the sub-network because the movement is localized. So the round trip delay is minimized by localizing the movement of the MN because the MAP acts as the HA, and this leads to reduction in the total signaling cost. The binding update cost is calculated from the following equation:

C, BU =L*e*N*f

Where
L= distance the BU message travel.
N=number of mobile nodes
e= processing time for encapsulation and dencapsulation
f=frequency of changing the network ant it is equivalent to 1/T where T is the residence time

It is clear that the binding update messages cost for BT is higher than the HMMCT, this is because each time the MN handover a binding update message is needed to be sent to the HA in BT, however, binding update message is needed only when there is an intra domain-mobility and this would involve processing cost. So as the number of the MNs increase the cost would increase as well. The residence time in HMMCT is higher because the movement is localized.

Secondly, the packet delivery cost is discussed. The packet delivery cost is assumed to depend mainly on the length of the path taken by the packets to be delivered mobile node. Bi-directional tunneling (BT) suffers from high signaling cost, and this is due to the large distance between the mobile node and the home agent, and the encapsulation and dencapsulation process which is taking place every time there is a movement. This high signaling cost is because of the triangular routing problem which experience by the BT. HMMCT suffers from less signaling cost due to localization of the movement. The packet delivery cost can be calculated by:

Cost = distance* encapsulation processing cost.

For the BT, the packet delivery cost can be calculated by:

C, PD, BT= D1*e1+D2*e1

The packet delivery cost for HMMCT calculated by:

C, PD, HMMCT=D3*e2+D4*e2

Where
D*1*: distance from MN to HA.
D2: distance from HA to the multicast data source.
D3: distance from MN to MAP.
D4: distance from MAP to the multicast source.
CPD, BT: packet delivery cost for BT
CPD, HMMCT: packet delivery cost for HMMCT

The D1,D2 distances is larger than D3,D4, and in the BT there will be a lot of encapsulation and dencapsulation process which leads to the increase of the packet delivery cost and the signaling cost.

Fig (3) shows the total signaling cost verses the number of the MN, and the graph shows the higher signaling cost for the BT and especially as the number of MNs increase.

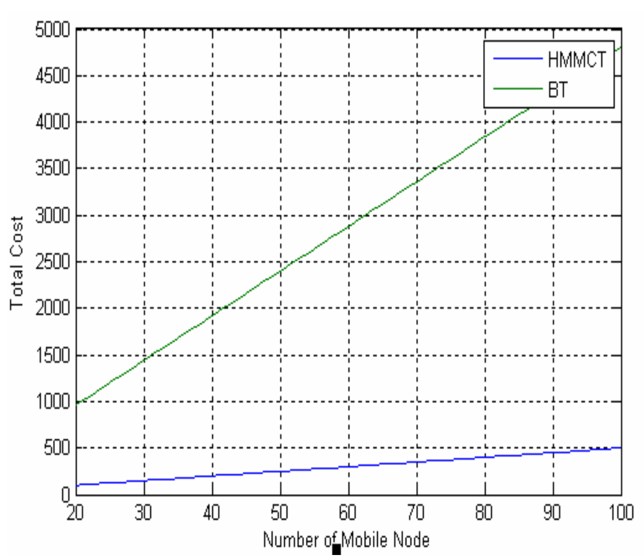


FIGURE 3: The signal cost vs. number of mobile node (for BT and HMMCT).

5. CONCLUSION & FUTURE WORK

This paper presents and suggests a new solution to the mobile multicast issues which suffers from high signaling cost, packets drop and packets latency. The new protocol is compared with the bi-directional approach. The paper integrates the Hierarchical Mobile IPv6 with Mobile context transfer. It has shown in this paper that the HMMCT suffers less signaling cost. In the future, this new protocol would be simulated and evaluated using network simulator 2 (ns-2).

6. ACKNOWLEDGEMENT

We would like to acknowledge the research centre management at the International Islamic University Malaysia for their support for this research.

7. REFERENCES

1 R. Berezdivin, R. Breining, and R. Topp. *"Next-Generation Wireless Communications Concepts and Technologies". IEEE Commun. Mag.*, vol. 40, Mar. 2002, pp. 108–16.

2 Karan Singh, R. S. Yadav, Ranvijay. *"A Review Paper on AD HOC Network Security".* International Journal of Computer Science and Security, Vol.1, Issue 1, 2007.

3 A.K. Othman. *"GPS-less Localization Protocol for Underwater Acoustic Networks".* International Journal of Computer Science and Security, Vol. 1, Issue 1, 2007.

4 R.Asokan, A.M.Natarajan, C.Venkatesh. *"Ant Based Dynamic Source Routing Protocol to Support Multiple Quality of Service (QoS) Metrics in Mobile Ad Hoc Networks".* International Journal of Computer Science and Security, vol. 2, issue 3, 2008.

5 C. Perkins, *"IP Mobility Support",* RFC2002, Oct. 1996.

6 I. Miloucheva, K.Jonas. *"Multicast Context Transfer in mobile IPv6"*. SATCOM, 2005.

7 R. Koodli, E. Perkins, *"Fast Handovers and Context Transfer in Mobile Networks"*, Nokia Research Center, 2004.

8 Xia, F. and Sarikaya, B. *"FMIPv6 extensions for Multicast Handover",* draft-xia-mipshop-fmip-multicast-00.txt, (work in progress), September 2006.

9 X. P. Costa, R. Schmitz, H. Hartenstein, M. Liebsch, *"A MIPV6, FMIPV6 and HMIPV6 Handover Latency Study: Analytical Approach"*, NEC EUROPE Ltd, Heidelberg, 2005.

10 T. C. Schmidt, M. Waehlisch. *"Seamless Multicast Handover in a Hierarchical Mobile IPv6 Environment"*. IETF, December 2005.

11 Soliman, H., Castelluccia, C., El-Malki, K., Bellier, L. *"Hierarchical Mobile IPv6 mobility management"*. RFC 4140, August 2005.

12 J. Loughney, M. Nakhjiri, C. Perkins, R. Koodli. *"Context Transfer Protocol*". RFC4067, 2005.

13 H. Santos, A. Mantos*. "Context Transfer of Mobile IPv6 Multicast Listeners"*. Internet Draft (work in progress expired), February 2006.

14 I. Miloucheva. "*Context Management for Efficient Mobile Multicast Service"*. FOCUS, 2004.

15 Schmidt, T. *"Multicast Mobility in MIPv6: Problem Statement and Brief Survey"*. Draft irtf-mobopts-mmcastv6-ps-01.txt (work in progress), July 2007.

16 J. Kempf. *"Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network".* IETF, September 2002.

17 J. Xie and I. F. Akyildiz. *"An optimal location management scheme for minimizing signaling cost in Mobile IP". IEEE International Conference on Communications (ICC)*, New York, pp. 3313–3317, April 2002.

18 S. Fu, M. Atiquzzaman, L. Ma, and Y. Lee*. "Signaling cost and performance of SIGMA, A seamless handover scheme for data networks". Accepted by Journal of Wireless Communication Mobile Computing*, 2005.

A Vertical Search Engine – Based On Domain Classifier

Rajashree Shettar rajshri.shettar@gmail.com
Department of Computer Science,
R.V. College of Engineering,
Bangalore, 560059, Karnataka, India

Rahul Bhuptani rahul.bhuptani@gmail.com
Department of Computer Science,
R.V. College of Engineering,
Bangalore, 560059, Karnataka, India

Abstract

The World Wide Web is growing exponentially and the dynamic, unstructured nature of the web makes it difficult to locate useful resources. Web Search engines such as Google and Alta Vista provide huge amount of information many of which might not be relevant to the users query. In this paper, we build a vertical search engine which takes a seed URL and classifies the URLs crawled based on the page's content as belonging to Medical or Finance domains. The filter component of the vertical search engine classifies the web pages downloaded by the crawler into appropriate domains. The web pages crawled is checked for relevance based on the domain chosen and indexed. External users query the database with keywords to *search;* The Domain classifiers classify the URLs into relevant domain and are presented in descending order according to the rank number. This paper focuses on two issues – page relevance to a particular domain and page contents for the search keywords to improve the quality of URLs to be listed thereby avoiding irrelevant or low-quality ones.

Keywords: — domain classifier**,** inverted index, page rank, relevance, vertical search.

1. INTRODUCTION

The term "search engine" refers to a software program that searches the Web and returns a list of documents in which the keywords are found. Vertical search engines, or domain-specific search engines also called "Vortals", facilitate more accurate, relevant and faster search by indexing in specific domains. Some of the examples of vertical search engines are Financial Search Engines, Law Search Engines, etc. The number of index able web pages is of the order of billions and because of the enormous size of the Web, general-purpose search engines such as Google and Yahoo can no longer satisfy the needs of most users searching for specific information on a given topic. The Broad-Based search engines have gotten broader, so have their search results. This has become increasingly frustrating to users who have turned to search engines to find information on a specialized topic, be it local information, travel sites or specific business channels. The search engine technology had to scale up dramatically in order to keep up with the growing amount of information available on the web [1]. The number of index able web pages is in the order of billions. In contrast with large-scale engines such as Google [2], a search engine with a specialized index is more appropriate to services catering for specific topic and target groups because it has more structure content and offers more precision. A user visiting a vertical search engine may have a prior knowledge of the domain, so extra input to disambiguate the query might not be needed [3]. Many vertical search engines, or domain-specific search engines, have been built to facilitate more efficient search in various domains. **LookSmart**, an online media and technology company that has launched more than 180 vertical search sites, contends that Web users will increasingly use the Internet the way they do cable television, opting for specialized channels that speak directly to their concerns. In [9] on-line solutions to medical information discovery are presented which tackles medical information research with specialized cooperative retrieval agents. In [10] the document index keeps information about each URL page. It is a fixed width (ISAM), Index Sequential Access Mode index, ordered by document ID. In [11] the Vertical search engines solve part of the problem by keeping indexes only in specific domains. They also offer more opportunity to apply domain knowledge in the spider applications that collect content for their databases. Here the authors use three approaches to investigate algorithms for improving the performance of vertical search engine spiders: a breadth-first graph-traversal algorithm with no heuristics to refine the search process, a best-first traversal algorithm that uses a hyperlink-analysis heuristic, and a spreading-activation algorithm based on modeling the Web. Topic focused crawler [12] is used to collect data. A novel score function is used to evaluate the URL's correlation about the specific topic. Only URLs those whose score is greater than a given threshold is fetched. Factors that contribute to the score are content of the web pages, including the keywords, text and description; the anchor text of the URL; link structure of the URL and pages. In [13] authors use page ranking as a fundamental step towards the construction of effective search engines for both generic (horizontal) and focused (vertical) search. Ranking schemes for horizontal search like the PageRank algorithm used by Google operate on the topology of the graph, regardless of the page content. On the other hand, the recent development of vertical portals (*vortals*) makes it useful to adopt scoring systems focused on the topic and taking the page content into account.

In this paper we propose and present an efficient search engine which takes a seed URL as input. The web pages are crawled based on the domain the URL belongs to i.e either medical or financial domain. The crawler applies indexing techniques for web page analysis and keyword extraction to help determine whether the page content is relevant to a target domain (medical or financial) thereby finding the number of good URLs. Further, domain knowledge is incorporated into the analysis to improve the results, precision rate. The words on the web page are checked against a list of domain-specific terminology and a higher weight is assigned to pages that contain words from the list. Finally, the experimental results are given to assess the features of the relevance score along with the ranked URL for the search keywords provided by the users.

2. WORKING OF VERTICAL SEARCH ENGINE

A vertical search engine searches for specific medical or finance related terms from the crawled web pages. The vertical search engine maintains two lexicons based one for medical and the other for finance domain. The lexicons are built with the knowledge of the domain experts. It evaluates relevance of web pages in context of the domain using content analysis technique. Filter out pages which are not relevant to domain by using TFIDF scores (Term Frequency – Inverse Document Frequency). It is a weighting method used to describe documents in Information Retrieval (IR) problems. The word frequency of the document is calculated. The more a word appears in a document, its term frequency (TF) is high and is estimated to be significant in the document. Inverse document frequency (IDF) measures how infrequent the word is in the document. There are many variants of TFIDF [5] when a user enters a web search query into a search engine (typically by using keyword), the engine examines its inverted index and provides a listing of best matching web pages according to the criteria. The usefulness of the vertical search engine depends on the relevance (information retrieval) of the "result set" it gives back.

3. SYSTEM ARCHITECTURE

The vertical search engine based on domain classifier is built on seven modules; a crawler (spider), HTML parser, filter, domain classifier, page ranker, URLdb, search - supported by a user interface. These modules are described from section 3.1 to section 3.7. Figure 1 depicts the modules involved in building the vertical search engine.

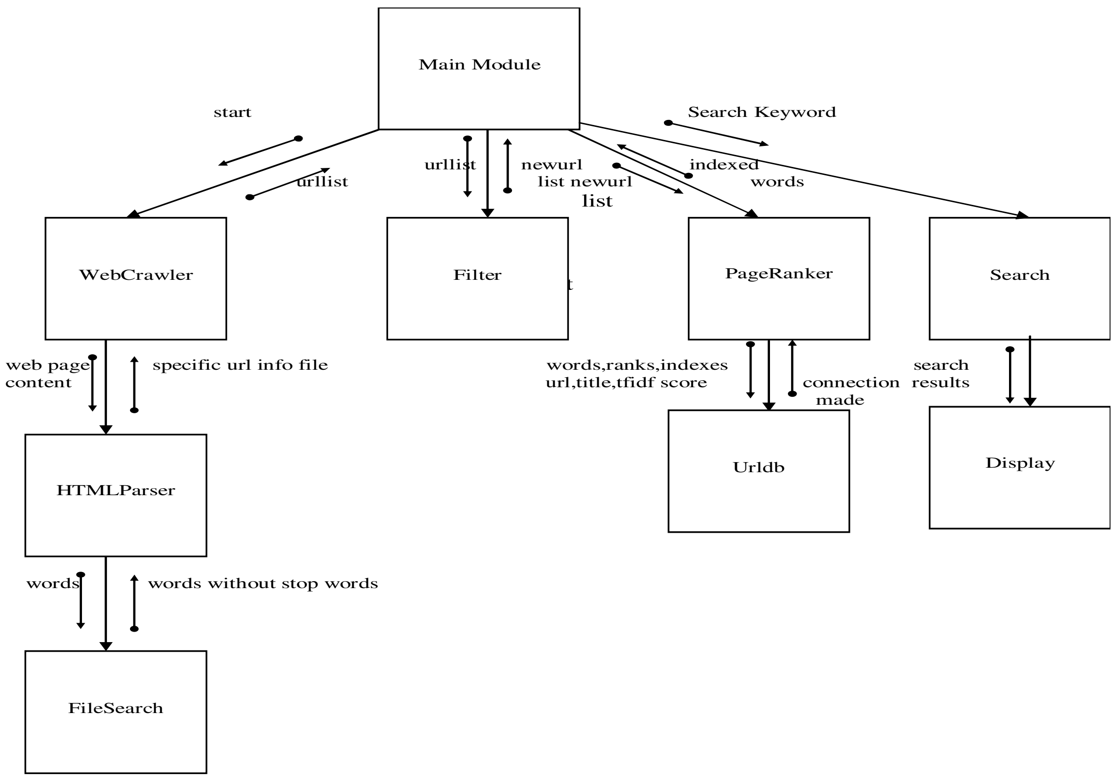


Figure 1: Vertical Search Engine Architecture.

3.1 Web Crawler

The web crawler crawls in a breadth first manner from a given seed URL downloads its contents and retrieves the embedded “Links” and puts them into a queue. The Crawler then recursively takes the URL from the head of the queue and repeats the above procedure till a depth of five or till the queue is empty and the crawling process does not cover the whole web. Crawler handles malformed URLs and robots.txt file. Only HTML pages are crawled and it can handle only HTTP protocol. The crawler calls the HTML parser module to retrieve relevant information from the web page. It also retrieves the last modified time of the page. The working of the web crawler is as shown in figure 2.

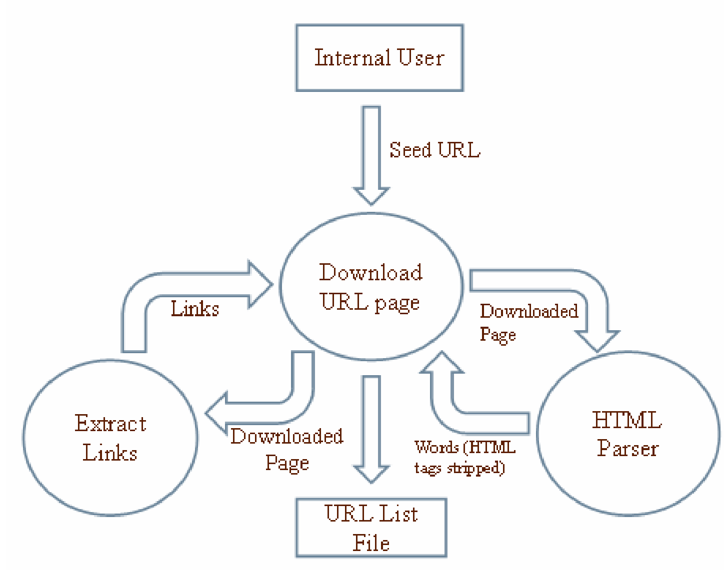


Figure 2: Working of a Web Crawler.

3.2 HTML Parser

HTML parser is the module which tokenizes contents of the file and recognizes the html tags and words. The html tags, style sheets, the stop words (words like to, in and etc which occur frequently and are not content dependant) are stripped off. HTML parser returns the title of the web page along with the words extracted (multiple occurrence taken care) with respective indexes in the page. The HTML parser calls the URL Filter module. An example of the HTML parser output is as given below.

Example: <html><title>hello world</title><body>Hello World! This is our demo for words extracting. </body></html>. The output will be: title: "hello world" |words:Hello(1,3);World(2,4);demo(5);words(6);extracting(7);

3.3 Filter

The search engine being vertical and not generic, all web pages crawled by the spider module from the internet will not be necessary for further processing. Only those web pages which are relevant to the medical domain or finance domain, which contains about 20,000 words relevant to medical field or financial field are selected. Thus it filters the URLs which are queued up by the crawler module into appropriate domains. Hence we need to check how important the page is, and how well it adheres to the topic concerned and discard the URLs which divert from the topic; by analyzing the TDIDF scores. We check each word in a URL page if it exists in the domain lexicon (Medterms.txt/Financeterms.txt). If it does then we calculate its term frequency (TF) and inverse document frequency (IDF) score. The rank of each URL page is the sum of TFIDF scores of all the words in the web page which are also in the domain lexicon. If the sum exceeds a threshold value then we consider those URLs as relevant and index the page. The threshold value is chosen to be the average of the TFIDF scores of the filtered web pages.

$$TFIDF = TF\ (\text{term frequency}) * IDF\ (\text{inverse document frequency}). \quad (1)$$

$$TF = \frac{(\text{no. of times each lexicon word in the page occurs})}{(\text{total no. of words found in that page}).} \quad (2)$$

$$IDF = \frac{(\text{total no. of web pages})}{(\text{no. of web pages in which the lexicon word occur})} \quad (3)$$

The tokenized words are placed in an inverted index corresponding to medical and finance domains which are created for searching. Inverted index consist of word, URL in which the word is found, rank of the word in this URL.

3.4 Domain Classifier

The filter classifies the URLs crawled based on the two domain lexicons medical and finance. The domain classifier displays the table containing URLs with the TFIDF scores calculated for each domain.

3.5 Page ranker

The success of search engines tends to be attributed to their ability to rank the results. This is non-trivial as the average number of words in a user query is around two; hence the corresponding matching pages tend to be large. The relevant URLs are taken up by the page ranker which ranks them according to their prominence and frequency. Prominence is based on the location where the word occurs (URL itself, title, first paragraph, rest of the body and domain lexicon), thus respective ranks or weights are assigned to the words depending on where they occur in the document. This weight decreases as the location of the word in the document loses its importance. The strategy used for ranking [4] is as shown in the table 1. Example: “intranet” occurs once in URL, once in title (position 2), twice in rest of the body. Rank of “intranet” = (0.50 + 0.60 + 2*0.03) = 1.16.

Word in “URL”:	0.50
Word in “title”	1st word : 0.65 2nd word : 0.60 3rd word : 0.55 default : 0.50
Word in “paragraph”:	0.25
Word in rest of the page :	0.03 * frequency of the word

Table 1: Page Rank calculation.

If this rank number is *large*, content of the page will be regarded as *fit* to the keyword. The second factor frequency of the word is calculated and added to the prominence weight. This rank calculated for each word is stored along with the URL it occurs in and where it occurs is stored into the database.

3.6 URLdb

This module establishes MySQL database connection and stores the given data into the database. This module stores the URL information –name of the URL, title, first 25 words in the web page. Connection to the database server is established through JDBC interface using MySQL / J Connector com.mySQL.jdbc.Driver. We also specify the location of the database using its URL address: jdbc:mySQL://localhost:3306/mySQL. After successful connection, we create the table "URLinfo" and insert URL details using SQL queries.

3.7 Search

The main purpose of this project is to provide efficient search for the user queries. An intelligent search module has been designed which analyzes the user query and fetches the required results from the database. Figure 3 shows the working of keyword search module. It eliminates stop words in the search query (of, the, and etc). It displays the results in a browser with the title of the web pages along with their links and relevance scores. This module establishes database connection to MySQL and generates a query for retrieval of the web pages according to the keywords supplied by the user through the GUI. It also calculates the new ranks of the web pages (if required) dynamically according to the search.

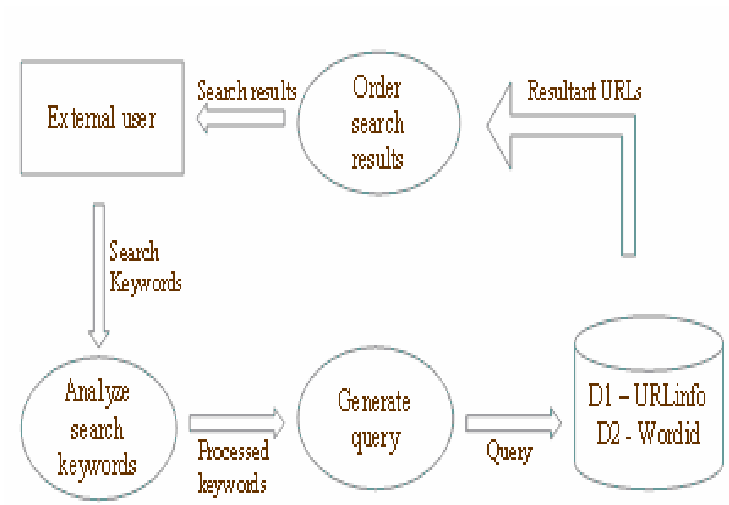
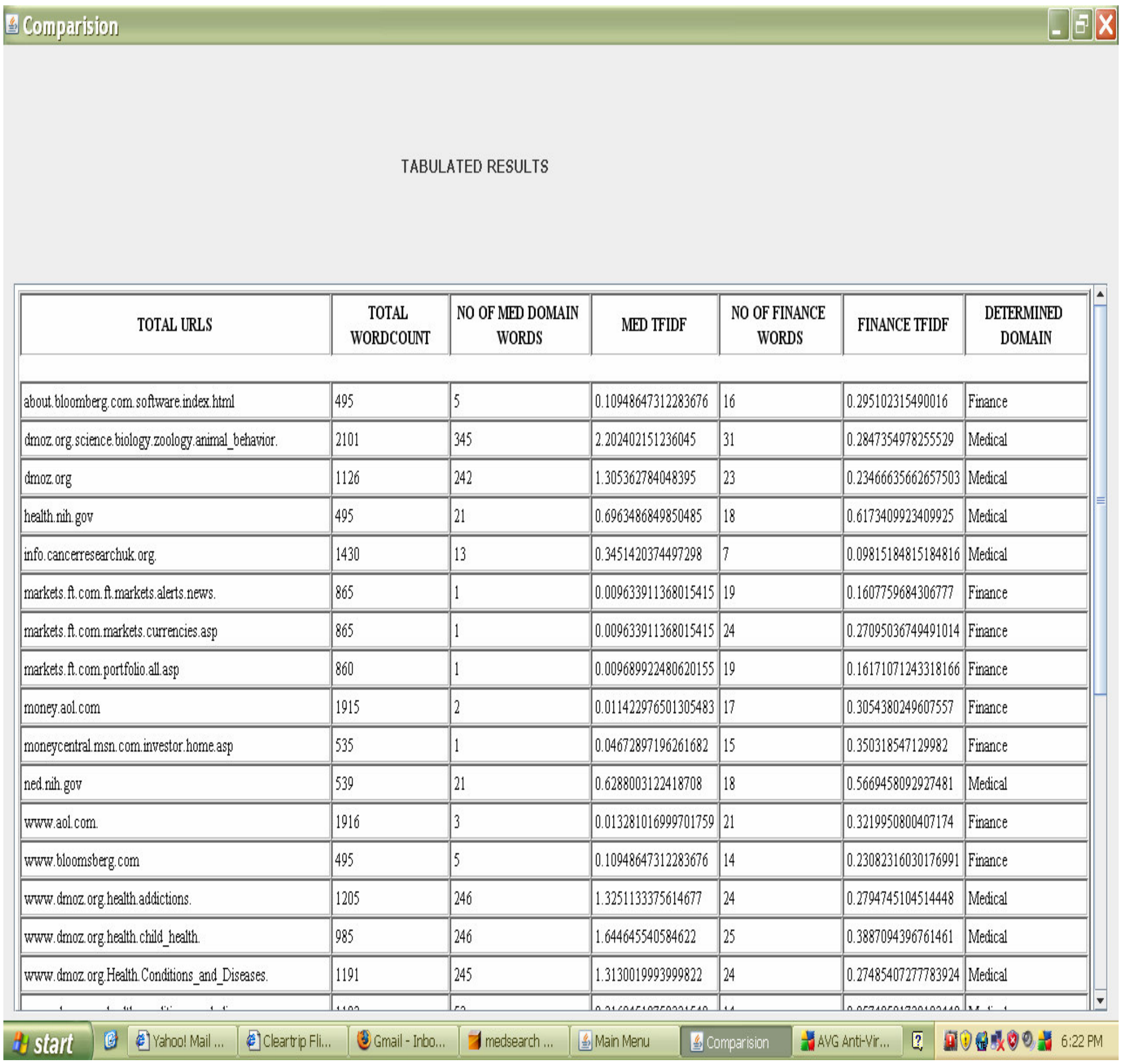


Figure 3: Module for keyword search.

4. EXPERIMENTAL RESULTS

The Vertical search engine is designed to run on limited physical resources. This is developed on Windows XP operating system, using JDK 1.6 and MySQL server 5.0; JDBC APIs for interfacing with the database using mysql-connector-java-5.0.7.; browser used is Internet Explorer. The relevance of each web page to the medical domain and finance domain is evaluated using a measure called TFIDF and a domain lexicon containing about 20,000 words relevant to medical and finance field are used. We calculate the TFIDF value of all words in the web page present in the lexicon. If the sum exceeds the threshold value then we consider it for indexing. The threshold value considered for experiment is the average of the TFIDF scores. The best seed URL (most relevant to the domain) is given to the crawler as input initially and we limit the crawl to of depth 5 from the seed and web pages considered are static. Only keyword search is provided and natural language processing is not provided. Figure 4 shows the list of URLs crawled with total word count and number of medical words and finance words found in the URL webpage along with the TFIDF score. Figure 5 displays the search results on a browser. The URLs listed contain the

search keywords along with their relevance score. The results are listed in a browser so as to enable downloading of the corresponding web pages.
The graph 1 shows total number of URLs crawled and the good URL found after filtering process. Graph 2 is plotted for total URLs crawled and their precision rate. The Graph 3 is plotted for total URLs against the average TFIDF score.



TOTAL URLS	TOTAL WORDCOUNT	NO OF MED DOMAIN WORDS	MED TFIDF	NO OF FINANCE WORDS	FINANCE TFIDF	DETERMINED DOMAIN
about.bloomberg.com.software.index.html	495	5	0.10948647312283676	16	0.295102315490016	Finance
dmoz.org.science.biology.zoology.animal_behavior.	2101	345	2.202402151236045	31	0.2847354978255529	Medical
dmoz.org	1126	242	1.305362784048395	23	0.23466635662657503	Medical
health.nih.gov	495	21	0.6963486849850485	18	0.6173409923409925	Medical
info.cancerresearchuk.org.	1430	13	0.3451420374497298	7	0.09815184815184816	Medical
markets.ft.com.ft.markets.alerts.news.	865	1	0.009633911368015415	19	0.1607759684306777	Finance
markets.ft.com.markets.currencies.asp	865	1	0.009633911368015415	24	0.27095036749491014	Finance
markets.ft.com.portfolio.all.asp	860	1	0.009689922480620155	19	0.16171071243318166	Finance
money.aol.com	1915	2	0.011422976501305483	17	0.3054380249607557	Finance
moneycentral.msn.com.investor.home.asp	535	1	0.04672897196261682	15	0.350318547129982	Finance
ned.nih.gov	539	21	0.6288003122418708	18	0.5669458092927481	Medical
www.aol.com.	1916	3	0.013281016999701759	21	0.3219950800407174	Finance
www.bloomsberg.com	495	5	0.10948647312283676	14	0.23082316030176991	Finance
www.dmoz.org.health.addictions.	1205	246	1.3251133375614677	24	0.2794745104514448	Medical
www.dmoz.org.health.child_health.	985	246	1.644645540584622	25	0.3887094396761461	Medical
www.dmoz.org.Health.Conditions_and_Diseases.	1191	245	1.3130019993999822	24	0.27485407277783924	Medical

Figure 4: User Interface showing the domain classification based on medical and finance lexicons for the list of URLs crawled with total word count and number of medical words and finance words found in the URL webpage along with the TFIDF score.

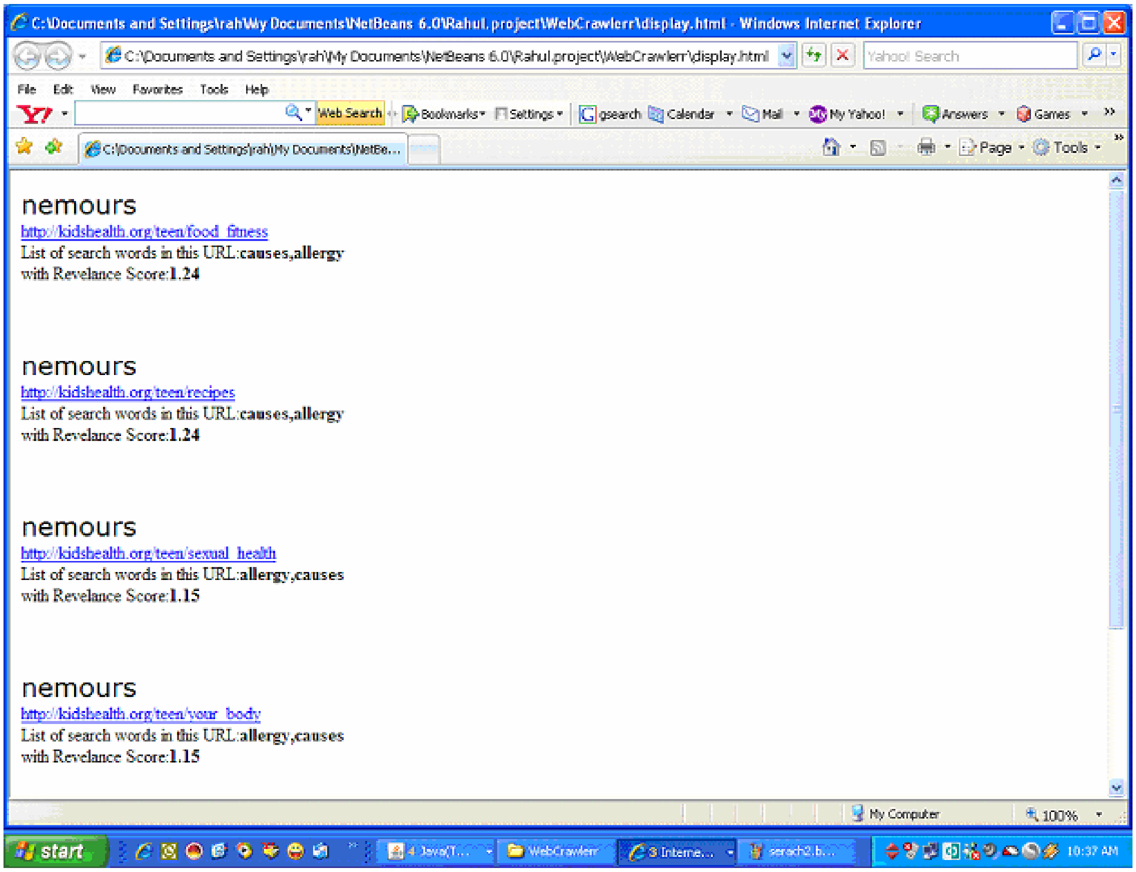
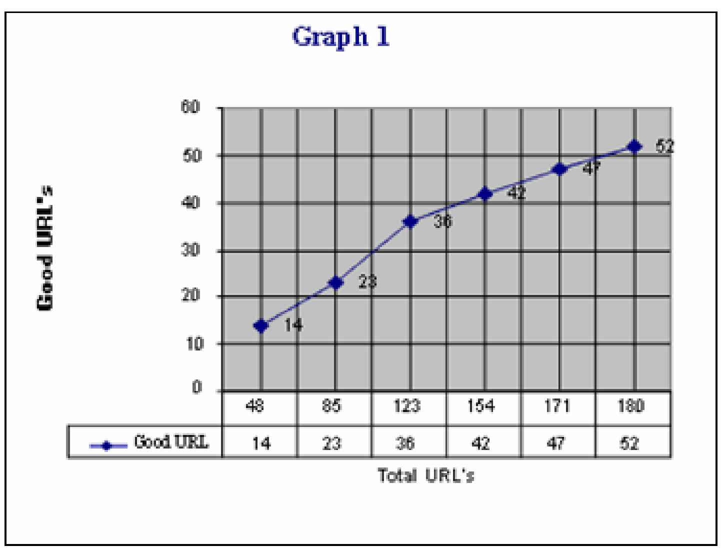


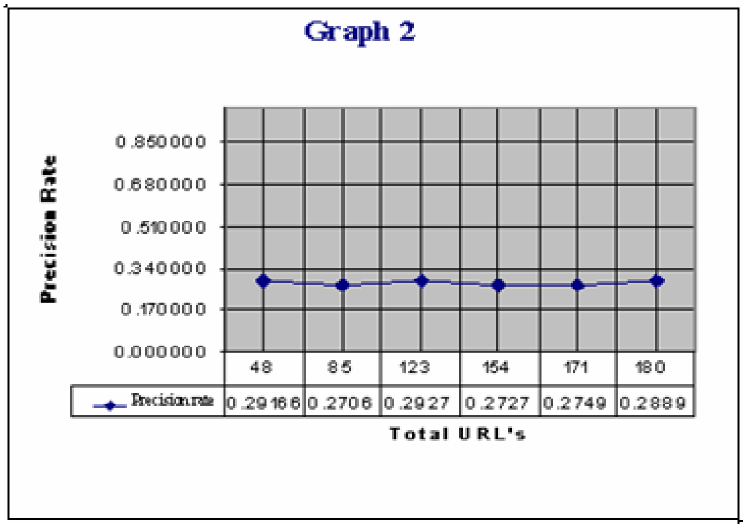
Figure 5: User Interface showing the result of the search operation with the search keywords contained in the web pages of the URLs listed along with their relevance score.



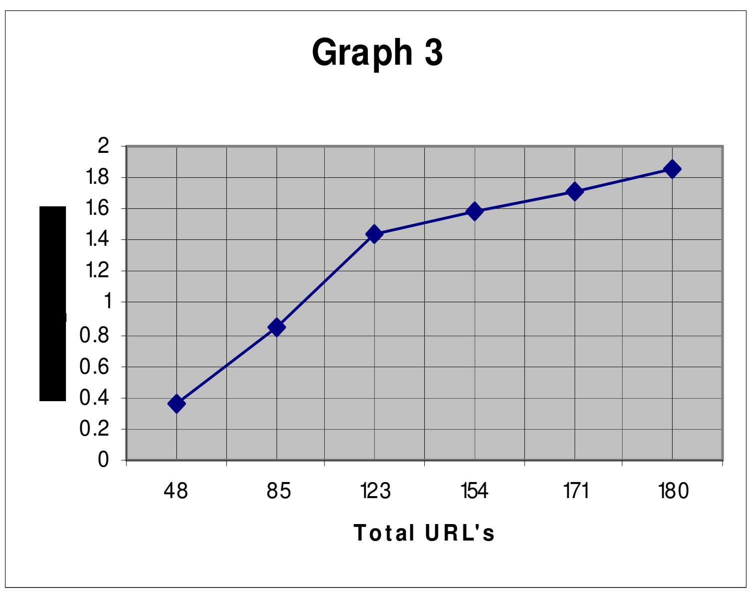
Graph 1: Total number of URL's crawled against the total number of Good URLs extracted by the Vertical Search Engine.

The precision rate is calculated as follows:

$$\text{Precision rate} = \frac{\text{Number of good URLs}}{\text{Total number of crawled URLs}} \qquad (4)$$



Graph 2: Total URLs crawled and their precision rate.



Graph 3: Total URLs against the average TFIDF score.

5. CONCLUSION

Vertical search engine is a fast emerging technology, giving serious competitions to generic search engines. The main aim of this paper is to provide users with highly relevant results for medical and finance domain, thus saving user the precious time of avoiding wading through irrelevant search results, hence providing better choice than a generic engine. In this paper we have presented the architecture and implementation details of a vertical search engine. We have indexed about 1, 00,000 words from about 180 URLs. The URLs which are irrelevant i.e. not pertaining to the medical and finance domain are filtered out based on the TFIDF threshold value. Only URL links which contain the search keywords specific to the medical and finance lexicon are listed. The vertical search engine model presented gives efficient results pertaining to the domain chosen. Thereby reducing the users search time for specific topic and giving the user a more relevant and specific URL list for search operation.

6. FUTURE ENHANCEMENTS

The vertical search engine can be enhanced by including phrase search and algorithms like link analysis can be added to provide better results. The domain classifier can be extended for more domains by training the network to automatically classify the domains each web page belongs to using neural network strategy.

7. REFERENCES

[1] George Almpanidis, Constantine Kotropoulos, and Ioannis Pitas. Aristotle University of Thessaloniki, Department of Informatics. “Focused Crawling Using Latent Semantic Indexing” – *An Application for Vertical Search Engines.*

[2]Google Search Technology. Online at http://www.google.com/technology/index.html.

[3] R. Steele, “Techniques for Specialized Search Engines”, *in Proc. Internet Computing, Las Vegas, 2001.*

[4] Ng Zhug Whai, “A new city university search engine”, Department of information technology.

[5] Pascal Soucy, Guy W. Mineau, Beyond TFIDF weigting for Text Categorization in the Vector Space model, 2005.

[6] Manber, U., Smith, M., and Gopal, B. “WebGlimpse: Combining Browsing and searching”, in *Proceedings of the USENIX 1997 Annual Technical Conference.*

[7] Monica Peshave, “How search engine works and a Web Crawler Application”, Dept of Computer science,University of Illinios at Springfield, Spingfield,IL 62703.

[8] Castillo, C. (2004). “Effective Web Crawling”, *PhD thesis, University of Chile*.

[9] Baujard, O., Baujard, V., Aurel, S., Boyer, C., and Appel, R.D. “Trends in Medical Information Retrieval on the Internet”, *Computers in Biology and Medicine, 28,1998.*

[11] Michael Chau and Hsinchun Chen, “Comparison of Three Vertical Search Spiders”, *Journal of Computer* ,Vol. 36, No. 5, 2003, ISSN 0018-9162, pp. 56-62, publisher IEEE Computer Society.
[12] Ye Wang, Zhihua Geng, Sheng Huang, Xiaoling Wang, Aoying Zhou, “Academic Web Search Engine – generating a Survey Automatically”, Department of ComputerScience, Fudan university, China.

[13] “Web Page Scoring Systems for Horizontal and Vertical Search”, Michelangelo Diligenti , Marco Gori,Marco Maggini , Siena, Italy.

Hierarchies in Contextual Role- Based Access Control Model (C-RBAC)

Muhammad Nabeel Tahir m_nabeeltahir@hotmail.com
Faculty of Information Science and Technology
Multimedia University, Melaka, Malaysia

Abstract

Hierarchical representation is a natural way of organizing roles in role-based access control systems. Besides its advantages of providing a way of establishing parent-child relationships among different roles, it also provides a facility to design and organize context dependant application roles that users may activate depending on their current context (spatial, temporal) conditions. In this paper, we show that if spatial roles are organized in hierarchical relationships, it can cause the problem of disambiguation in making access control decisions especially when the user moves from one location to another location frequently in a single transaction and a single session. We extend our work of Contextual Role-Based Access Control (C-RBAC) by introducing hierarchical relationship among subject, location and purpose roles and solve the disambiguation problem in hierarchy by considering user motion direction and his/her context roles (spatial and spatial purpose) in order to make more fine grained and better access control decisions.

Keywords: Access Control, RBAC, Purpose Role, Spatial Role, Location Modeling.

1. INTRODUCTION

Patients have important roles to play in addressing privacy and security concerns. The greatest concerns regarding the privacy of health information derive from widespread sharing of patient information throughout the health care industry and the inadequate federal and state regulatory framework for systematic protection of health information. At the level of individual organizations, electronic health information is vulnerable to both authorized users who misuse their privileges to perform unauthorized actions (such as browsing through patient records) and outsiders who are not authorized to use the information systems, but break in with the intent of malicious and damaging action. Adequate protection of health care information depends on both technology and organizational practices for privacy and security.

Health care organizations have to deal with a number of processes, procedures that are controlled through different applications. They also have to make sure that all the implemented applications must follow the rules and policies that have been addressed by Health Insurance Portability and Accountability Act (HIPAA) [1] to make sure the confidentiality, integrity and secrecy of patient record. Many privacy and authorization based access control models have been proposed in past to protect organizational resources. Examples are location-based [2], [3], [4], [5], time-based [6], [7], [8]. However they have limited flexibility as none of them consider the purpose for which access is given to the user to perform various activities. Also these models lacks in partitioning organization into a domain environment as these models rely on the spatial extent defined within the total responsibility space. Thus, making difficult for the security officer to manage the authorization permissions for the whole space defined within an organization. Few purpose-based access control model [9], [10], [11] have been proposed for various applications that relies on role-based access control (RBAC). But these models do not provide the proper semantics and constraints for purposes with spatial extents. These models address only spatial and temporal characteristics of roles and some others, only purpose characteristics.

In this paper, we extend our work of recently proposed C-RBAC model [12] that relies on spatial roles with the presence of spatial purposes and spatial domains. We provide few examples to show how our model incorporates location hierarchy schema and location hierarchy instance, user motion direction and spatial purposes in order to solve the hierarchical disambiguation.

The remainder of this paper is organized as follows. Next section briefly presents C-RBAC model and some relevant definitions. We then present hierarchies in C-RBAC and define location hierarchy (schema and instance level), spatial domain hierarchy, spatial purpose hierarchy. Lastly we conclude the paper along with future research direction.

2. PRELIMINARIES

In this section, we provide some definitions for location, spatial domain, spatial role and spatial purposes that are the building blocks of our model.

Definition 1 (Location): We define the location as a set of attributes that defines the scope of some area/region and give some name to it.

Location (loc) = {attr1, attr2, attr3…attrn }, where n > 0

Definition 2 (Physical Location): Physical location ploc is a set of points that represents a polygon, line or a single point.

ploc = {<pos1, pos2…posn >, <DVAL>, dunit }

where n > 0, DVAL is a set of directional distances {m1, m2, m3, m4} representing distances of east, west, north and south; and dunit represents distance measurement unit.

PLOC is set containing all physical locations identified by the system such that

PLOC = {ploc1, ploc2…plocn}
where n > 0

Definition 3 (Logical Location): Logical location lloc is an abstract meaning of a set of physical locations. A logical location can be characterized by many physical locations such that:

lloc = {ploc1, ploc2… plocn}, where n > 0

LLOC is a set containing all the logical locations identified by the system such that

LLOC = {lloc1, lloc2…llocn}
where n > 0

Definition 4 (Relative Location): Relative location rloc is a range/perimeter defined with respect to a physical or logical location such that:

rloc = <l, dunit, dir>, such that

where l $\in$ PLOC/LLOC, dunit is a distance measurement unit, dir is a geometric or logical direction value

RLOC is a set of all relative locations identified by the systems such that

RLOC = {rloc1, rloc2…rlocn}
where n > 0

We also define the functions occurrenceploc (rloc); occurrencelloc (rloc) that generates a set of physical or logical locations with respect to the relative location rloc given.

C-RBAC HIERARCHIES

The central components on which C-RBAC model relies are location, domain and purpose roles. Like subject roles in RBAC, hierarchical relationship exists among locations, domains and purposes roles. Sandhu et al. proposed [13] that hierarchical relationship can be defined by introducing the partial order $\preceq$ between roles such that ri $\preceq$ rj means that: (a) rj inherits all permissions assigned to ri; (b) users which have been assigned rj have also been assigned ri. We use this concept as a base of defining hierarchical relationship among different locations in C-RBAC model.

Location Hierarchies

In our model, the traditional hierarchical relationship is not sufficient to deal with the location in the presence of domains. Therefore, we extend the traditional hierarchical relationship by defining Location Hierarchy Schema (LHS) and Location Hierarchy Instances (LHI).

Location Hierarchy Schema (LHS)

LHS allows the security administrator to define a common name for a set of hierarchically organized logical locations within a spatial domain. Hierarchical relationship defined among logical locations within the schema represent the internal organization structure within a spatial domain. As logical locations are organized in a hierarchical manner, all the relationships defined in [14] exist among locations.

Definition 5 (Location Hierarchy Schema): A location hierarchy schema is a tuple <LHS, ls>, where LHS is the location hierarchy schema name and ls is logical locations set organized in a hierarchical relationship within the schema such that; ls → 2lloc.

Let lhsi be the location hierarchy schema name, ls is defined as, ls → occurencesls (lhsi) → 2lloc, where lloc $\in$ LLOC. Because of hierarchical relationship among logical locations, relationships contains (lloc1, lloc2), disjoint (lloc1, lloc2) holds [14].

Consider a scenario of a hospital in which X-Ray, Laboratory are the departments and General Ward, Surgery and ICU are wards. We further assume that each department and ward has its own architecture, for example departments may have reception area, doctor offices and waiting room and wards may have patient rooms, doctor offices, nursing room, waiting hall and main general hall in which patients are admitted as shown in figure 1.

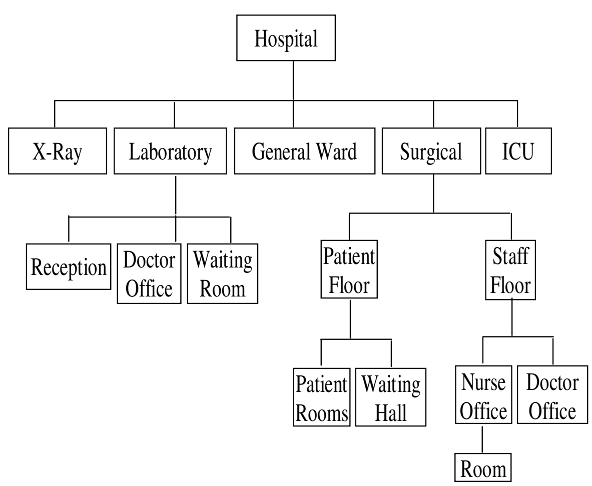


Figure 1: Hospital wards and departments.

Assume that:
- General Ward has patient and staff floor
- Patient floor has Patient Rooms, Waiting Hall
- Staff Floor has Nurse Office, Doctor Office room.

By using logical locations, we can define location hierarchy schema for a ward figure 2(a) and for a department figure (b).

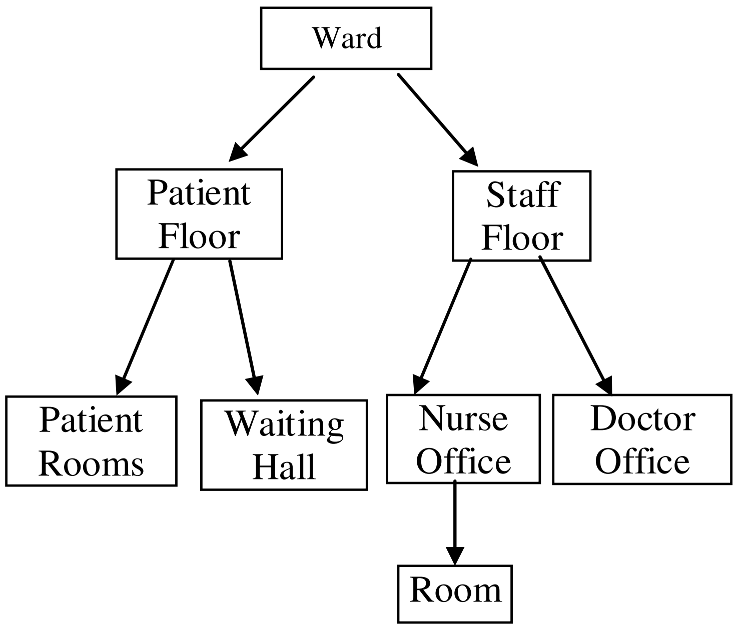


Figure 2(a): Location hierarchy schema for ward.

LHS <Ward, ls> and ls → occurencesls (Ward) → 2lloc, that is ls = {PatientFloor, StaffFloor, PatientRooms, WaitingHall, NurseOffice, DoctorOffice, Room}.

Similarly, LHS for department can be defines as LHS <Department, ls> and ls → occurencesls (Department) → 2lloc, that is ls = {Reception, DoctorOffices, WaitingRoom} as shown in figure 2(b).

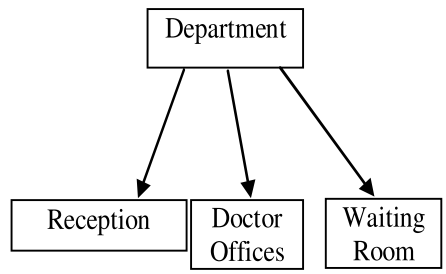


Figure 2(b): Location Hierarchy Schema for department.

Location Hierarchy Instance (LHI)

Location Hierarchy Instance is defined as an instance fulfilling the location relationship pattern defined within LHS.

Definition 6 (Location Hierarchy Instance): Given a location hierarchy schema lhs, lhi can be defined as <LHI, ps> where LHI is the location hierarchy instance name and ps is the physical locations set organized according to the hierarchical relationship among logical locations defined within the schema such that given lhi, ps → occurencesps (lhij) → 2ploc, where ploc ∈ PLOC.

By definition 2, each physical location defined in LHI is defined along with the directional distances to its east, west, north and south. For example <NurseOffice, {30, 10, 25, 46}, meter> and <DoctorOffice, {23, 30, 15, 75}, meter> shows that the distance between NurseOffice and DoctorOffice is 30 meters. By constant monitoring the current values of user position, user speed and motion direction can easily be obtained for access control decisions. We define the function DirectionalDistance (ploc, dir) that returns the distance between the physical location ploci to plocj defined in the direction dir.

Location hierarchy instance for the ward and department is shown in figure 4(a) and 4(b) respectively.

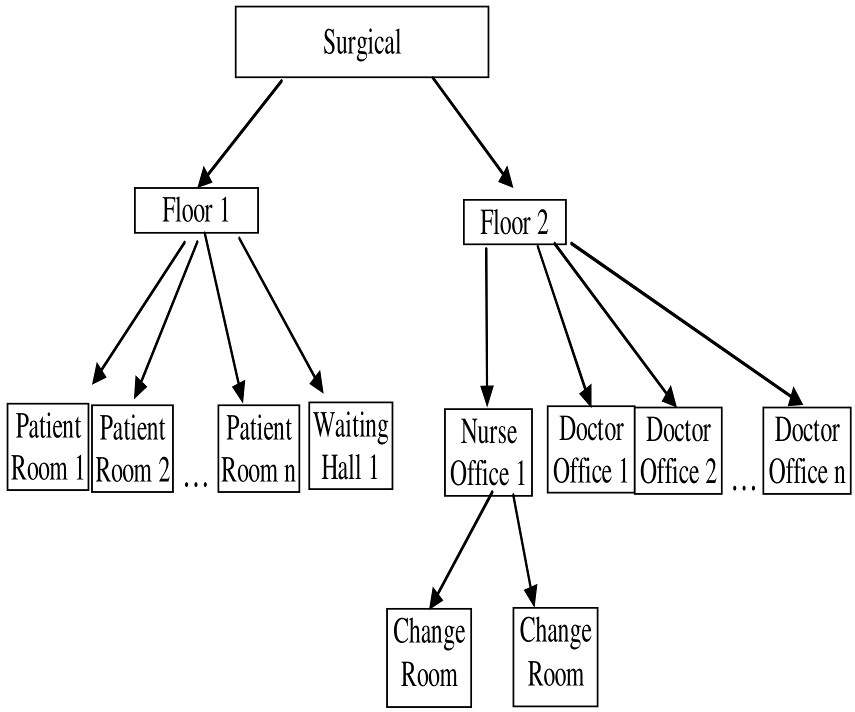


Figure 3(a): Location Hierarchy Instance for ward.

LHI <Surgical, ps> and ps → occurencesps (Surgical) → 2ploc, that is ps = { Floor1, Floor2, PatientRoom1,..PatientRoomn,WaitingHall1,NurseOffice1,ChangeRoom1,ChangeRoom2,Doctor Offices1,DoctorOffices2,DoctorOfficesn,}.

Similarly, for department as shown in figure 3(b), LHI can be defined as LHI <Laboratory, ps> and ps → occurencesps (Laboratory) → 2ploc, such that; ps = {Reception1, DoctorOffice1, DoctorOffices2,…DoctorOfficen,,WaitingHall1}.

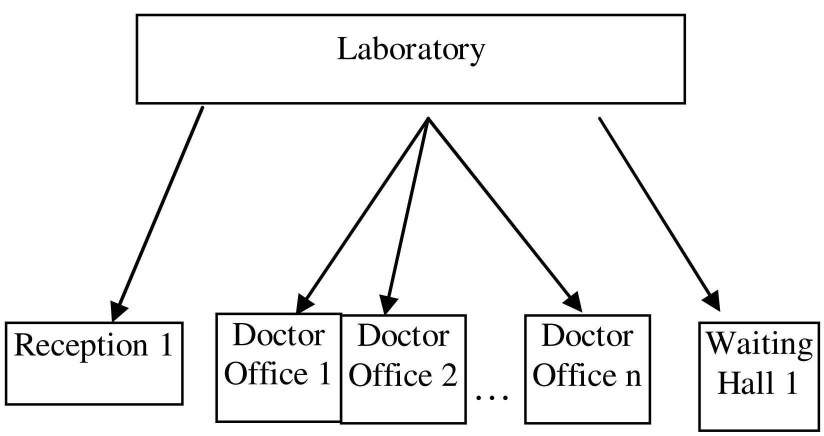


Figure 3(b): Location Hierarchy Instance for department.

Location Hierarchy Schema and Instance Functions

Let LHSS = {lhs1, lhs2,…, lhsn} be the set of location hierarchy schema and LHIS = {lhi1, lhi2 ,…, lhin} be the set location hierarchy instances. We define:
-SchemaOf (lhin) → lhsn, such that; occurencesls (lhsn) → 2lloc (definition 5.1)
-InstanceOf (lhsn) → 2lhi, such that occurencesps (lhin) → 2ploc (definition 5.2)

Location Hierarchy Schema and Instance Hierarchies (LHSH & LHIH)

Given two location hierarchy schemas, it may be possible that relationships like contains, disjoint and overlaps exist. Like location hierarchy schema, relationships also exists among physical locations e.g. contains (ploc1, ploc2), disjoint (ploc1, ploc2). We borrow the logical and physical location relationships from [14] and define the following relationships for LHS and LHI given in table 1.

Relations	***Semantics (physical locations)***	***Semantics (logical locations)***
	For all lhi, such that $lhi_n \rightarrow InstanceOf\ (lhs_n)$	
lhs_1 *contains* lhs_2	$contains(lhi_1, lhi_2) \rightarrow (\forall ploc_2, ploc_2 \in occurrence_{ps}(lhi_2) \rightarrow (\exists ploc_1, ploc_1 \in occurrence_{ps}(lhi_1) \wedge contains(ploc_1, ploc_2)))$	$contains(lhs_1, lhs_2) \rightarrow (\forall lloc_2, lloc_2 \in occurrence_{ls}(lhs_2) \rightarrow (\exists lloc_1, lloc_1 \in occurrence_{ls}(lhs_1) \wedge contains(lloc_1, lloc_2)))$
lhs_1 *disjoint* lhs_2	$disjoint(lhi_1, lhi_2) \rightarrow (\forall ploc_1, ploc_1 \in occurrence_{ps}(lhi_1) \rightarrow (\exists ploc_2, ploc_2 \in occurrence_{ps}(lhi_2) \wedge disjoint(ploc_1, ploc_2)))$	$disjoint(lhs_1, lhs_2) \rightarrow (\forall lloc_1, lloc_1 \in occurrence_{ls}(lhs_1) \rightarrow (\exists lloc_2, lloc_2 \in occurrence_{ls}(lhs_2) \wedge disjoint(lloc_1, lloc_2)))$
lhs_1 *overlap* lhs_2	$overlap(lhi_1, lhi_2) \rightarrow (\forall ploc_2, ploc_2 \in occurrence_{ps}(lhi_2) \rightarrow (\exists ploc_1, ploc_2 \in occurrence_{ps}(lhi_1) \wedge overlaps(ploc_1, ploc_2))) \wedge (\forall ploc_1, ploc_1 \in occurrence_{ps}(lhi_1) \rightarrow (\exists ploc_2, ploc_2 \in occurrence_{ps}(lhi_2) \wedge overlaps(ploc_1, ploc_2)))$	$overlap(lhs_1, lhs_2) \rightarrow (\forall lloc_2, lloc_2 \in occurrence_{ls}(lhs_2) \rightarrow (\exists lloc_1, lloc_2 \in occurrence_{ls}(lhs_1) \wedge overlaps(lloc_1, lloc_2))) \wedge (\forall lloc_1, lloc_1 \in occurrence_{ls}(lhs_1) \rightarrow (\exists lloc_2, lloc_2 \in occurrence_{ls}(lhs_2) \wedge overlaps(lloc_1, lloc_2)))$

Table1: Relationships among LHS and LHI

Domain Hierarchy

The main goal of a distributed system is to connect users and resources in a transparent, open, and scalable way. Besides its many advantages, distributed systems allow organizations to divide large problems into many small problems which are distributed to many computers. Later, the small results are reassembled into a larger solution. Similarly distributed processing require that a program be parallelized—divided into sections that can run simultaneously, distributed computing also requires that the division of the program take into account the different environments on which the different sections of the program will be running.

Because of its strewn nature, it may be possible that a single request may be divided into many small requests for parallel or distributed processing that may

require services of different resources from different locations. This result organizations not only to know the requestor identity and the spatial context of the user but also the purpose for which a request to access a resource has been made.

A lot of work have been done by many researchers on domains by answering different problems like how to define a domain [15], domain hierarchies, communication among multi-domain and multi-level domains [16], [17] and [18]. Hansen et al. proposed an extension of RBAC model that relies on the notion of spatial roles [2]. In their work, they proposed logical location domains that reflect organizational location infrastructure and security policy. However their work is very simple and does not address issues like how spatial roles can be organized within logical location domains. Furthermore their work assumes the fixed spatial granularity of the position; primary location cells; on which roles can be acquired by the user. A good effort has been made in defining spatial roles by Bertino et. al [3]. In their model, spatial feature of role relies on role extend and logical position. However, their work does not address the organization of spatial roles within the domain scope. Furthermore, their model is not compliant with privacy requirements defined by HIPAA in which user purposes/intentions also take part in access control decision process. Few other notable approaches are the work by Corradi et. al [4] and Fu et. al [5]. We extend our work of C-RBAC model [12] and show how spatial domain can make use of LHS and LHI to organize spatial roles along with spatial purposes within spatial domain boundary.

Definition 7 (Spatial Domain): Spatial domain is a logical boundary surrounding at least one or a list of object(s) that are (a) associated with the location and purpose context and (b) identifiable by the system. Spatial domains are defined through spatial domain expression such that;

Spatial Domain <SDOM, LHSS>

where, SDOM is spatial domain name and LHSS is location hierarchy schema set specifying locations covered by SDOM through LHS, such that; LHSS → SchemaDomain (SDOM) → 2lhs.

Spatial Domain <SDOM, LHIS>

where, SDOM is spatial domain name and LHIS is location hierarchy instance set specifying locations covered by SDOM at instance level, such that; LHIS → InstanceDomain (SDOM) → 2lhi. It must be noted that one LHS can be defined more than one time within the same spatial domain but LHI name must be unique within the same spatial domain. However multiple instances of same LHS can be defined in two different spatial domains.

Furthermore, we define the LHS and LHI mapping functions for spatial domains such that, SchemaDomain (SDOM) → 2lhs, and InstanceDomain (SDOM) → 2lhi. Given a spatial domain; these functions return LHS and its instances LHI used by SDOM. Once a list of LHS or LHI used by SDOM is computed, logical and physical locations used by LHS and LHI can be easily computed through occurencesLSDOM (SDOM): $\bigcup_{x \in SchemaDomain(SDOM)} occurences_{ls}(x)$

and $occurences_{LSDOM}(SDOM): \bigcup_{x \in InstanceDomain(SDOM)} occurences_{ps}(x)$

We notice that location hierarchy schema and the derived instances used by spatial domains leads us to define hierarchical relationships among spatial domains because of LHS and LHI hierarchical relationships through contains and overlaps. Similarly it may be possible that a physical location ploc defined in one schema used by SDOMi may also be defined in another schema of SDOMj. We address these issues by defining multi-level spatial domain relationships and multi-spatial domain relationships. By using relationships among LHS and LHI as defined in table 1, we define

Definition 8 (Multi-Level Spatial Domain Relationship): Without loosing generality in location relationships defined in [14], we say that two domain SDOMi and SDOMj may have a multi-level relationship such that:

multiLvlDom(SDOMi, SDOMj) → (∀lhsj, lhsj ∈ SchemaDomain(SDOMj) → (∃ lhsi, lhsi ∈ SchemaDomain(SDOMi) Λ contains(lhsi, lhsj))).

Definition 9 (Multi-Spatial Domain Relationship): Let lhsi and lhsj be the LHS such that lhsi ∈ SDOMi and lhsj ∈ SDOMj. We define:

(i) multiDomovrlp (SDOMi,SDOMj) → (∀lhsj, lhsj ∈ SchemaDomain (SDOMj) → (∃lhsi, lhsi ∈ SchemaDomain (SDOMi) Λ overlaps (lhsi, lhsj))) Λ (∀lhsi, lhsi ∈ SchemaDomain (SDOMi) → (∃ lhsj, lhsj ∈ SchemaDomain (SDOMj) Λ overlaps (lhsi, lhsj)))

(ii) multiDomdisj (SDOMi, SDOMj) → (∀lhsi, lhsi ∈ SchemaDomain (SDOMi) → (∃lhsj, lhsj ∈ SchemaDomain (SDOMj) Λ disjoint(lhsi, lhsj)))

Purpose Hierarchy

Purpose; in many literatures is defined as “an anticipated outcome that is intended or that guides your planned actions” [22]. Many countries have ratified legislation to protect privacy for individuals [12]. For example, Gramm-Leach-Bliley Act (GLB Act) [19] for financial sector, Health Insurance Portability and Accountability Act (HIPAA) [1] for medical sector in United States, Personal Information Protection and Electronic Documents Act (PIPEDA) [20] in Canada have made organizations keen in knowing the user intentions in order to grant permissions. These legislations protect and enhance the rights of consumer, clients and patients etc. while restricting access usage of the information based on the user’s intentions [21].

Purpose-oriented model that control the illegal flow of information between objects in object-based systems is presented by [9]. They have discussed how to validate the purpose-oriented access rules through invocation graph and flow graphs that show the information flow relation among operations and objects. Covington et al. proposed the notion of environmental roles to capture environmental contexts to secure context-aware applications [10]. They also presented a security architecture that made use of environment roles through security policies to allow access to resources especially in home environments. However, no semantics have been given to show how environmental contexts can be attached with the roles. Furthermore, their work lacks in explaining how their proposed architecture restricts a user from acquiring two conflicting roles at a same time and how a relationship can be established between environmental roles. Their work also does not explain the explicit prohibition of environment roles and context aware security policies.

Ji Won et. al proposed purpose based access control for privacy protection in relational database systems in which multiple purposes can be associated with the data element at different granularity (attribute, column, tuple and entire table level) [11]. They also proposed the notion of intended purposes (that specify the intended usage of the data) and access purposes (that

specifies the purposes for which access can be given to use data element). Their purposed model relies on conditional roles that are based on role attributes and system attributes that can hold purpose values and context values of the role respectively. This means that every time when security administrator adds a new purpose in the purpose tree, he/she needs to define a new role attributes for each of the subject roles that can use it as an access purpose to access the data objects. However in our model we define purpose roles with respect to location called spatial purpose (SP) that can be attached with the subject roles. Similarly purpose roles can also be defined for spatial domains that reflect the reasons of communication between two domains. For example spatial purpose can be attached between a hospital and a research center with the purpose of research. By adopting this approach, we can also define constraints and obligation policies for domain based on its spatial nature that can be enforced at the time of making access control decisions about resource sharing. For example, we can define constraints on domain level that no user from research domain is allowed to access HIV results from laboratory domain for the purpose of research.
Furthermore in their work, users have to state their purposes when they try to access resources. Although this approach is quite simple and easy to implement, however the main drawback is that; the overall privacy that the system provides mainly relies on the user's trustworthiness.

In our approach we infer the access purpose runtime based on the current context of the user such that;

$$\text{Purpose } P \rightarrow U \times R \times T \times LoC\_AtR$$

where U ∈ Users, R ∈ Roles, T is time interval and Loc_AtR is a set of attributes e.g. user motion direction, motion speed, such that;

$$LOC\_ATR: \bigcup_{s \in SESSION} SLOC\_ATR(s)$$

Given the user session s, SLOC_ATR (s:sessIon) represents the current values of motion speed and motion direction of the session s activated by the user u with respect to its spatial context such that DirectionalDistance (ploc, dir) that returns the distance between the physical location ploci to plocj defined in the direction dir.

Definition 10 (Spatial Purpose): Spatial purpose is a purpose defined over some location context with respect to LHS such that;

Spatial Purpose SP <sp, lhs, spl>

where sp is spatial purpose name, lhs is location hierarchy schema and spl is spatial purpose location, a set of logical locations defining the boundaries for sp with respect to lhs such that; spl = {lloc1, lloc2…llocn}, where llocn ∈ occurencesls (lhsn).

Similarly, for LHI level, spatial purpose is defined as;

Spatial Purpose SP <sp, lhi, spl>

where sp is spatial purpose name, lhi is location hierarchy instance and spl is spatial purpose location, a set of physical locations defining the boundaries for sp with respect to lhi such that;

spl = {ploc1, ploc2…plocn}, where plocn ∈ occurencesps (lhin).

Like subject roles, spatial purposes also have a hierarchical relationship among them i.e. parent/child relationships. For instance, the purposes minor operations and major operations can be grouped together by a more general purpose, operation. The hierarchical relationship among different purposes is shown in figure 4 where each node represents the purpose and each edge represents the parent/child relationship.

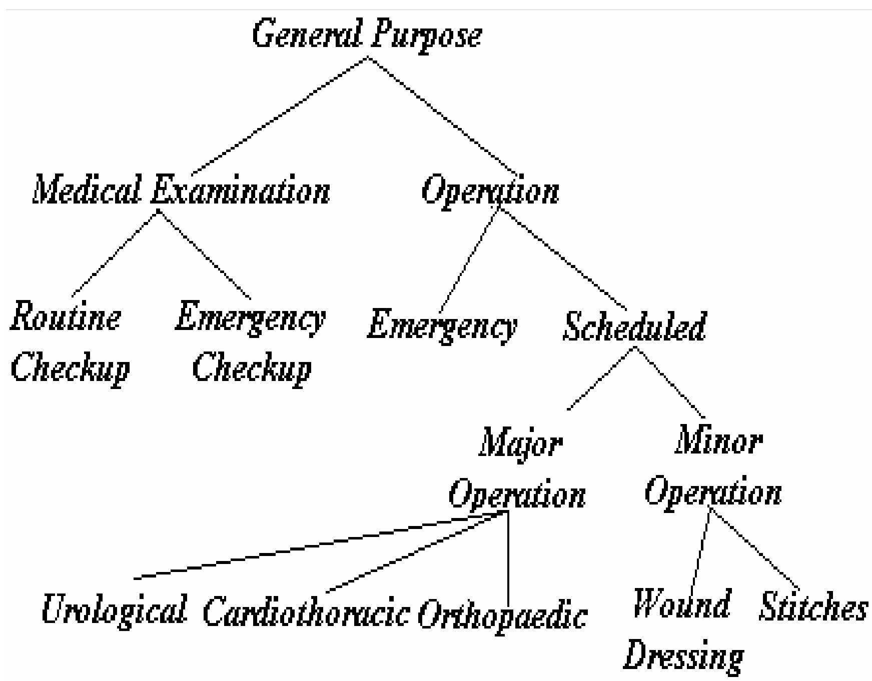


Figure 4: Purpose hierarchy

We define some functions for SP such that;

ParentPurposes (SP) → 2SP

ChildPurposes (SP) → 2SP

GetPurposeslloc (lloc) → 2SP; the function returns a set of spatial purposes defined with respect to logical location.

GetPurposesploc (ploc) → 2SP; the function returns a set of spatial purposes defined with respect to physical location.

GetPurposeslhs (lhs) → 2SP; the function returns a set of spatial purposes defined at location hierarchy schema level.

GetPurposeslhi (lhi) → 2SP; the function returns a set of spatial purposes defined at location hierarchy instance level.

IsParentPurposes (SP) → boolean, and
IsChild (SP) → boolean.

3. CONCLUSION AND FUTURE WORK

In this paper, we have extended our previous work on contextual role-based access control by introducing hierarchical relationships between locations, domains and purposes. We also introduce the notion of location hierarchy schema and location hierarchy instances. We emphasize that access control models cannot comply with HIPAA regulations without considering purposes/intentions of the users. We introduced the notion of spatial purposes that can be used by access control system to grant/deny permissions to the users depending on their current context values like time and location. However, separation of duty and conflicts may arise because of hierarchical relationship introduced between location schemas and instances with respect to purposes. We leave these issues for our future work.

4. REFERENCES

[1] . Health Insurance Portability & Accountability Act http://www.hipaa.org

[2] . Hansen F, Oleshchuk V. Spatial role-based access control model for wireless networks. In Proceedings of 58th IEEE Vehicular Technology Conference (VTC’03), 2093-2097, Orlando, Florida, 2003.

[3] . Bertino E, Catania B, Damiani ML, Persasca P. GEO-RBAC: A Spatially Aware RBAC. In Proceedings of 10th Symposium on Access Control Models and Technologies (SACMAT'05), 29-37, 2005

[4] . Corradi A, Montanari R, Tibaldi D. Context-based Access Control in Ubiquitous Environments. In Proceedings of 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004), 253-260, 2004

[5] . Fu S, Xu C. A Coordinated Spatio-Temporal Access Control Model for Mobile Computing in Coalition Environments. In Proceedings of 19th IEEE International Conference on Parallel and Distributed Processing, 289b-289b, Denver, CA, USA, 2005.

[6] . Joshi JBD, Bertino E, Shafiq B, Ghafoor A. Dependencies and Separation of Duty Constraints in GTRBAC. In Proceedings of 8th ACM Symposium on Access Control Models and Technologies, 51-64, Como, Italy, 2003.

[7] . Joshi JBD, Bertino E, Latif U, Ghafoor A. A generalized temporal role-based access control model. IEEE Transactions on Knowledge and Data Engineering, 17(1): 4-23, 2005.

[8] . Joshi JBD, Bertino E, Ghafoor A. Analysis of Expressiveness and Design Issues for a Generalized Temporal Role Based Access Control Model. IEEE Transactions on Dependable and Secure Computing, 2(2):157-175, 2005

[9] . Yasuda M, Tachikawa T, Takizawa M. A purpose-oriented access control model. In Proceedings of 13th International Conference on Information Networking, 168-173, Cheju, Korea, 1998.

[10] . Covington MJ, Moyer MJ, Ahmad M. Generalized role-based access control for securing future applications. In Proceedings of the 23rd National Information Systems Security Conference. Baltimore, MD, USA, 2000.

[11] . Byun J, Bertino E, Ninghui L. Purpose Based Access Control for Privacy Protection in Relational Database Systems. Technical Report 2004-52, Purdue University, USA, 2004.

[12] . Tahir N. Contextual Role-Based Access Control, Ubiquitous Computing and Communication Journal, 2(3), 2007

[13] . Sandhu R, Ferraiolo D, Kuhn R. The NIST Model for Role-Based Access Control: Towards A Unified Standard. In Proceedings of 5th ACM Workshop on Role-Based Access Control, 47-63, Berlin, Germany, 2000

[14] . S. Chandaran and J. Joshi. LoT-RBAC: A location and time-based RBAC model. In Proceedings of the 6th International Conference on Web Information Systems Engineering (WISE'05). Page(s): 361-375, NewYork, USA, 2005.

[15] . Yialelis N, Sloman M. A Security Framework Supporting Domain-Based Access Control in Distributed Systems. In Proceedings of IEEE ISOC Symposium on Network and Distributed Systems Security'96 1996; 26-34, San Diego.

[16] . Lee KH. A Distributed Network Management System with Multi-level Domain Approach. In Proceedings of International Conference on Communication Systems ICCS 1994; 789-793, Singapore.

[17] . Sloman M. Policy Driven Management for Distributed Systems. Journal of Network and Systems Management; 2(4): 333-361, 1994.

[18] . Constantine E. A role-based framework for distributed systems management. PhD Thesis, University of London, July 1998.

[19] . Gramm-Leach-Bliley Act (GLB Act): U.S. Senate Committee on Banking, Housing, and Urban Affairs http://banking.senate.gov/conf

[20] . Personal Information Protection and Electronic Documents Act http://www.nymity.com/pipeda/

[21] . A. Hameed, M. N. Tahir, S. Rehman. Impact of Role-Based Access Control in e-Governance. In Proceedings of 3rd International Conference on E-Governance, Lahore, Pakistan, 2005.

[22] . http://www.google.com/search?hl=en&rlz=1T4GFRC_en___MY202&defl=en&q=define: purpose&sa=X&oi= glossary_definition&ct=title

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA