RISCE Revista Internacional de Sistemas Computacionales y Electrónicos

ENERO 2012
Año 4, Volumen 4,Número 1

ESCOM

75 Años
INSTITUTO POLITÉCNICO NACIONAL
1936-2011

IPN

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos, Año 4, Vol. 4, No. 1, enero 2012, es una publicación bimestral editada por el Instituto Politécnico Nacional, Av. Luis Enrique Erro S/N, "Unidad Profesional Adolfo López Mateos", Del. Gustavo A. Madero, C.P. 07738, México D.F; a través de la Escuela Superior de Cómputo, Av. Juan de Dios Bátiz S/N esquina Miguel Othón de Mendizábal "Unidad Profesional Adolfo López Mateos", Col. Lindavista, C.P.07738, México, D. F., Tel. 57296000 ext. 52000,www.escom.ipn.mx. Editor responsable: Dr. Eduardo Bustos Farías, Reservas de Derechos al uso Exclusivo del Título No. 04-2008-062613190500-203, ISSN en trámite, ambos otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la última actualización de este número, Unidad de Informática IPN, M. en C. David Araujo Díaz, Av. Juan de Dios Bátiz S/N esquina Miguel Othón de Mendizábal "Unidad Profesional Adolfo López Mateos", Col. Lindavista, C.P.07738, fecha de la última modificación, 05 de julio de 2012.
Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación.
Queda estrictamente prohibida la reproducción total o parcial de los contenidos e imágenes de la publicación sin previa autorización del Instituto Politécnico Nacional.

La revista se especializa en el área de los sistemas computacionales y electrónicos; tanto en el desarrollo, como en la investigación en:

Ciencias de la Computación
Cómputo educativo
Cómputo Móvil
Comunicaciones
Disciplinas Emergentes
Electrónica
Física Electrónica
Ingeniería de Cómputo
Ingeniería de Software
Innovación Tecnológica
Inteligencia artificial
Matemática computacional
Procesamiento de señales
Robótica y cibernética
Sistemas de Información
Tecnologías de la Información

Distribución
La revista cuenta con 300 ejemplares que se distribuyen en:
Europa, Asía y América Hispana; mediante CD ROM y correo electrónico

Directorio

INSTITUTO POLITÉCNICO NACIONAL

DRA. YOLOXÓCHITL BUSTAMANTE DÍEZ
DIRECTORA GENERAL

MTRO. JUAN MANUEL CANTÚ ALVAREZ
SECRETARIO GENERAL

M. EN C. DAFFNY ROSADO MORENO.
SECRETARIA ACADÉMICA

DR. JAIME ALVAREZ GALLEGOS
SECRETARIO DE INVESTIGACIÓN Y POSGRADO

ING. ERNESTO MERCADO ESCUTIA
SECRETARIO DE SERVICIOS EDUCATIVOS

ING. OSCAR JORGE SÚCHIL VILLEGAS
SECRETARIO DE EXTENSIÓN E INTEGRACIÓN SOCIAL

M. EN C. FERNANDO ARELLANO CALDERON
SECRETARIO DE GESTIÓN ESTRATEGICA

M. EN C. EMMA FRIDA GALICIA HARO
SECRETARIA DE ADMINISTRACIÓN

LIC. JUDITH CLAUDIA RODRIGUEZ ZUÑIGA
DEFENSORA DE DERECHOS POLITÉCNICOS

ESCUELA SUPERIOR DE CÓMPUTO

ING. APOLINAR FRANCISCO CRUZ LÁZARO
DIRECTOR

DR. FLAVIO ARTURO SÁNCHEZ GARFIAS
SUBDIRECTOR ACADÉMICO

DR. JESÚS YALJÁ MONTIEL PÉREZ
JEFE DE LA SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

LIC. ARACELI LOYOLA ESPINOSA
SUBDIRECTORA DE SERVICIOS EDUCATIVOS E INTEGRACIÓN SOCIAL

M. EN C. JUAN VERA ROMERO
SUBDIRECTOR ADMINISTRATIVO

DR. EDUARDO BUSTOS FARÍAS
EDITOR DE RISCE

Miembros del comité Revisor

(Todo el comité técnico está formado por doctores en ciencias o su equivalente)

Francisca Losavio de Ordaz (Venezuela) (Universidad Central de Venezuela)
Alfredo Matteo (Venezuela) (Universidad Central de Venezuela)
Emmanuel F. Moya Anica (México)
Edgardo Manuel Felipe Riverón (Cuba) (México) (CIC)
Luis Enrique Palafox Maestre (México)
Eduardo F. Caicedo Bravo (Colombia)
Hilda Ángela Larrondo (Argentina)
Guillermo Leopoldo Kemper Vásquez (Perú)
Elizabeth León Guzmán (Colombia)
María Cecilia Rivera (Chile)
Satu Elisa Schaeffer (Finlandia) (UANL)
Rafael Canetti (Uruguay)
Javier Echaiz (Argentina)
Pablo Belzarena (Uruguay)
Carlos Beltrán González (Italia) (Universitá di Genova)
Elena Fabiola Ruiz Ledesma (México)
Jonatan Gómez (Colombia)
Armando De Giusti (Argentina)
Juan José Torres Manríquez (México)
Jesús Yaljá Montiel Pérez (México)
Luis Alfonso Villa Vargas (México)
Marco Antonio Ramírez Salinas (México)
Félix Moreno González (España) (UPM)
Salvador Godoy Calderón (México) (CIC)
José Luis López-Bonilla (México) (IPN ESIME ZAC)
Lorena Chavarría Báez (México)
Miguel Santiago Suárez Castañón (México)

ÍNDICE

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 4, Año 4. Enero 2012
Artículos con arbitraje

Performance Analysis of Uplink Channel for Mobile Location Networks

Gutiérrez-Begovich, L., Rivero-Ángeles, M. and Menchaca-Méndez, R.

***Abstract*— In this paper, we propose an integral teletraffic analysis on uplink channel for mobile location networks considering two scenarios: cellular coverage, and cellular no-coverage. For cellular coverage scenario, as a study case we introduce GSM/GPRS throughput analysis (by simulations) and access delay (mathematical analysis) for S-ALOHA. On the other hand, for cellular no-coverage scenario, an implementation and simulations of a cross-layer approach MANET Framework is proposed.**

***Index Terms*—S-ALOHA, throughput, backoff, access delay, MANET, cross-layer.**

INTRODUCTION

IN recent years, integration of new and better technologies on mobile computing devices, have led to apparition of new services. Some of these services are oriented to share location information through different data wireless networks. On particular scenarios, the successful transmission of information about user location could be crucial, above all at security and health services.

It's a well-known fact that the successful transmission of users' location depends at first, of the access to uplink channel on wireless networks through medium-access-control protocol (MAC) [1]. When a user is out of wireless coverage, the occurred events on this zone will be queued on the mobile, and subsequently will be transmitted when the user returns to a zone of wireless coverage. This is not a desired behavior, since important events could be delayed until user take wireless coverage again.

In this way, its important analyzes the main teletraffic metrics (delay, packet-loss probability, blocking probability, etc) for this kind of services, in order to improve throughput and the general performance on mobile location networks, for the wireless coverage scenario. On the other hand, for no-coverage scenario, is necessary introduce elements of mobile ad hoc networks (MANET), in order to combat excessive delay packet queuing.

In this work, we propose an integral teletraffic analysis that provides both scenarios for mobile location networks. As a study case, we choose GSM/GPRS as wireless system and STORM Framework [2] for MANET management

The organization of this paper is as follows: Section 2 provides prior work related with analysis performance on uplink channel for internet traffic considering several kind of services and related work on cross-layering approaches for MANET. Section 3 presents our conclusions and future work.

Manuscript received June 8, 2012. This work was supported in part by the Mexican National Polytechnic Institute.
L. Mauricio Gutierrez-Begovich is with the Section of Research and Graduate Studies of School of Computing at Mexican National Polytechnic Institute, Unidad Profesional ALM 07738, Mexico City, Mexico.
Mario. E. Rivero-Angeles is with the Section of Research and Graduate Studies of School of Computing at Mexican National Polytechnic Institute, Unidad Profesional ALM 07738, Mexico City, Mexico.
Rolando Menchaca-Mendez is with the Computer Research Center of the Mexican National Polytechnic Institute, Unidad Profesional ALM 07738, Mexico City, Mexico.

Related work

GPRS Uplink Channel

General Packet Radio Service (GPRS) is a packet mode wireless system that has been standardized to operate on GSM infrastructure, by introducing new packet support nodes and associated protocol stacks [2]. The RLC/MAC layers in the GPRS protocol stack essentially are responsible for the way in which the GSM/GPRS radio resources (frequency-time slot pairs) are shared by various mobile users. The uplink (mobile-to-base station link) channel resources are shared based on a *request-reservation* mechanism.

In particular, the GPRS MAC protocol is responsible for the way in which the GSM/GPRS radio frequency-time slot pairs are shared by the mobile users. The uplink channel resources are shared on a request-reservation basis. Two types of uplink channels are defined in GPRS. They are Packet Random Access Channel (PRACH) and Packet Data Traffic Channel (PDTCH). PRACH is used by all the mobiles, on a contention basis, for the purpose of sending resource request packets. Typically, TS0 slot in a GSM frame of 8 slots is used as PRACH. All mobiles are allowed to transmit on PRACH slots, following slotted-ALOHA protocol [3].

Most of the proposed analyzes for the upstream channel, consider saturation channel conditions or steady state, as they facilitate the analytical solution of the backoff delay [4, 5, 6, 11, and 12].

Major teletraffic studies on MAC layer are mainly concentrated on optimizing throughput for uplink channel of S-ALOHA and CSMA/CD protocols [7, 8, 9, and 10].

Cross-Layer MANET Frameworks

Cross-layer protocols, means a more complete approach of the concept of OSI communications model. The cross layer, includes two layers for work together in order to enable the compensation overload, latency or another mismatch of requirements, directly affected by layer deficiency.

A mobile ad-hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

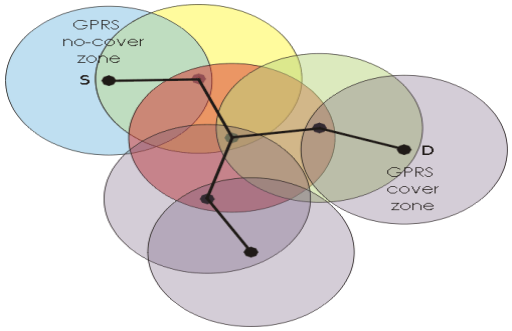


Fig. 2. A MANET diagram. Each node represents a mobile, and each color circle represents its own coverage zone (e.g. 802.11). A source (S) node transmit a data location packet to a destination (D) node, through a "on the fly" route.

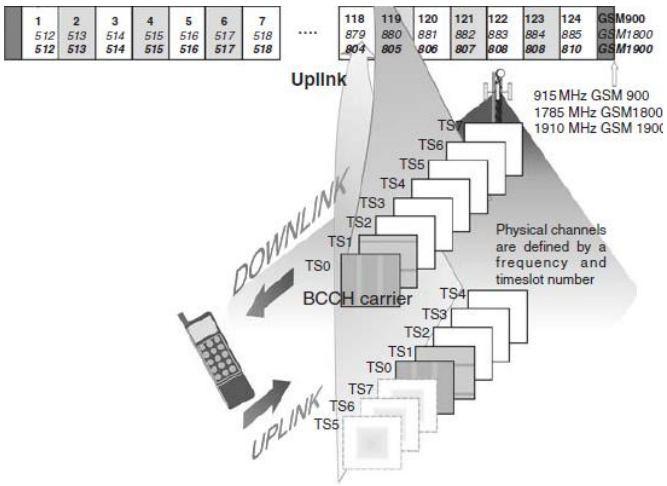


Fig. 1. GPRS frequency and time division frame for down/uplink channel.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

Another challenge, comes in the fact that the protocol arquitectures used particularly in MANETs, are derivatives of the protocol-stack architectures developed for wired networks and the Internet. In this sense, a manner of improve performance in MANETs is considering a cross-layer approach.

The growth of mobile devices and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid 1990s. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

The traditional protocol stack for MANETs, consider the 802.11 DCF for medium access control, regardless of the routing protocols for unicast (AODV) [13], OLSR [14]) and multicast (ODMRP [15]).

Furthermore, the aforementioned need for a MAC-Routing joint analysis has given rise to cross-layer approaches such as those proposed by CR Lin, et al. [16] and J.J. Garcia-Luna-Aceves, et. al. [17]. We choose the last one (STORM Framework), as it offers better performance (end-to-end delay, throughput, scalability and robustness for both, unicast and multicast traffic) than those mentioned above.

Conclusions

A brief review of the thesis topic "Performance Analysis of Uplink Channel for Mobile Location Networks" was presented, its main characteristics and performance measures. The current stage of research on the subject, make the study of techniques for analyzing the performance, analytical understanding of patterns of media access control (MAC) in mobile wireless networks, the writing of Chapter 1 and the simulation of S-ALOHA.

References

[1] Yu-Ching HSU, Ying-Dar LIN, "Two-Stage Dynamic Uplink Channel and Slot Assignment for GPRS", IEICE Trans, Vol.E5-A, No.1, January 2002.
[2] C. Bettstetter, H. J. Vogel, and J. Eberspacher, "GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface," IEEE Commun. Surveys, pp. 2-14, vol. 2, no. 3, 3rd Quarter, 1999.
[3] Peter McGuiggan, "GPRS IN PRACTICE, a companion to the specifications" John Wiley & Sons, Ltd. 2004.
[4] I. N. Vukovic and N. Smavatkul, "Delay analysis of different backoff algorithms in IEEE 802.11" in Proc. IEEE VTC—Fall, Sep. 2004, vol. 6, pp. 4553–4557.
[5] Y. Yang and T.-S. P. Yum, "Delay distributions of slotted ALOHA and CSMA" IEEE Trans. Commun., vol. 51, pp. 1846–1857, Nov. 2003.
[6] D. Raychaudhuri and K. Joseph, "Performance evaluation of slotted ALOHA with generalized retransmission backoff" IEEE Trans. Commun., vol. 38, no. 1, pp. 117–122, Jan. 1990.
[7] G. Bianchi, "Performance analysis of the IEEE 802.11 DCF" IEEE J. Sel. Areas Commun., vol. 18, pp. 535–547, Mar. 2000.
[8] L. Kleinrock, "Packet switching in a multiaccess broadcast channel: Performance evaluation" IEEE Trans. Commun., vol. COM-23, pp. 410–423, Apr. 1975.
[9] S. S. Lam, "Packet switching in a multiaccess broadcast channel: Dynamic control procedures". IEEE Trans. Commun., vol. COM-23, pp. 891–904, Sep. 1975.
[10] D. Altman, D. Barman, A. Benslimane, and R. El Azouzi, "Slotted ALOHA with priorities and random power" in Proc. Netw. Technol., Serv., Protocols; Performance Comput. Commun. Netw. Mobile Wireless Commun. Syst., 4th Int. IFIP-TC6 Netw. Conf., Waterloo, ON, Canada, May 2–6, 2005, vol. 3462, pp. 610–622.
[11] Mario E. Rivero-Angeles, et al. "Access Priority for Throughput Sensitive and Delay Sensitive Users in S-ALOHA Using Different Backoff Policies". Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd, pp. 201 - 205.
[12] Mario E. Rivero-Angeles, et al. "Differentiated Backoff Strategies for Prioritized Random Access Delay in Multiservice Cellular Networks". Transactions on Vehicular Technology, Vol. 58, No. 1, pp. 381-397, January 2009.
[13] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing". In Proc. of the Second IEEE Workshop on Mob. Comp. Syst and App.", 1999. WMCSA '99., pages 90–100, Feb 1999.
[14] P. Jacquet, A. Laouiti, P. Minet, and L. Viennot, "Performance analysis of OLSR multipoint relay flooding in two ad hoc wireless network models". In The second IFIP-TC6 NETWORKING Conference, may 2002.
[15] S.-J. Lee, M. Gerla, and C.-C. Chiang, "On-demand multicast routing protocol". In Proc. of the IEEE Wireless Comm. and Net. Conf., 1999. WCNC, pages 1298–1302 vol.3, 1999.
[16] C. R. Lin and M. Gerla, "Asynchronous multimedia multihop wireless networks". In Proc. of INFOCOM '97, volume 1, pages 118–125 vol.1, Apr 1997.
[17] J.J. García-Luna-Aceves, Rolando Menchaca-Mendez, "STORM: A Framework for Integrated Routing, Scheduling and Traffic Management in Ad Hoc Networks". IEEE Transactions on Mobile Computing, Issue: 99, August 2011.

L.M. Gutierrez-Begovich received the B.S. degree in Computer Systems by the School of Computing, National Polytechnic Institute, Mexico City, 2006; Worked in financial software development, Mexico City, 2007. Studied degree in the Communications Section of the Department of Electrical Engineering at Center Research and Advanced Studies (Cinvestav), Mexico City, 2008-2010 (without getting the degree). From 2010 has worked in the satellite tracking industry as CTO. Actually is a student of first semester of Master of Science program in the Mobile Computing, School of Computing, National Polytechnic Institute (IPN).

Mario E. Rivero-Angeles was born in México City, México, in 1976. He received the B.Sc. degree from the Metropolitan Autonomous University, México City, in 1998 and the M.Sc. and Ph.D. degrees in electrical engineering from the Centro de Investigacion y de Estudios Avanzados del Instituto Politecnico Nacional (CINVESTAV-IPN), México City, in 2000 and 2006, respectively. Since 2002, he has been an Assistant Professor with the Telematic Section, Advanced Technologies and Interdisciplinary Engineering Professional Unit (UPIITA-IPN), México City. He is also currently a Postdoctoral Researcher with the National Institute for Research in Computer Science and Control (INRIA), Rennes, France. His research interests include random access protocols and data transmission in cellular networks and wireless sensor networks.

R. Menchaca-Mendez received the B.S. degree in Electronic Engineering from the Universidad Autonoma Metropolitana, Mexico City, Mexico in 1997; the M.S. degree from the Mexican National Polytechnic Institute, Mexico City, Mexico in 1999; and his Ph.D. degree in Computer Engineering from the University of California at Santa Cruz in 2009. He is a professor and head of the Communications and Networking Laboratory at the Computer Research Center (CIC) of the Mexican National Polytechnic Institute (IPN).

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 4, Año 4. Enero 2012
Artículos con arbitraje

Core para control de una pantalla LCD-*touch* utilizando un FPGA

Gerardo Muñoz Estrada

***Resumen*— Recientemente los sistemas embebidos han ido cambiando e incorporándose a diversos productos, como por ejemplo aplicaciones de domótica, cómputo móvil, electrodomésticos, aplicaciones médicas, entre otras. El uso actual de interfaces táctiles para diversos sistemas ha motivado el desarrollo de este trabajo; en él se propone el diseño de un core para el control de una pantalla LCD-*touch*, el sistema se implementa en un FPGA, este tipo de implementación es conocido como SoPC (Sistema en un chip progrmable) y tiene la ventaja de que se puede programar de acuerdo a los requerimientos de la aplicación, lo cual permite que el sistema pueda ser reconfigurable y reprogramable.**

***Palabras Clave*—Core LCD-touch, interfaz táctil, SoPC**

INTRODUCCIÓN

EN la última década el avance tecnológico, sobre todo en sistemas móviles, ha tenido un desarrollo exponencial. Los sistemas móviles día a día son diseñados para ser más eficientes, tanto por el ahorro de energía como por el tamaño del mismo. De esta manera un mismo elemento, como es la pantalla sirve tanto de interfaz de salida, como para proporcionar datos de entrada al sistema. Ese es el caso de las pantallas *LCD-Touch*, que cumplen ambos tipos de interfaces. Pues la pantalla de los dispositivos servía sólo como un dispositivo de salida.

El diseño de sistemas embebidos, sobre todo en el área de las aplicaciones de cómputo móviles, se caracteriza por integrar en ellos una interfaz gráfica para la interacción con el usuario. Esto es gracias a la alta integración de componentes que la tecnología ha permitido hacer. Por ejemplo, un controlador de pantalla *LCD-touch* integra un sistema en un mismo chip (SoC, por sus siglas en ingles *System on a Chip*) diferentes módulos de hardware [1], [2], [3], [4], como son: microprocesador, módulos de memoria, periféricos de entradas/salidas y aceleradores de hardware, todos ellos dentro de un solo circuito integrado.

Los SoC pueden ser implementados utilizando la misma metodología en un FPGA [4], [5], esto debido al crecimiento en capacidad de dicha tecnología. De esta manera se tiene así un sistema en un chip programable, también llamados SoPC, de *Systems on a Programmable Chip* [6], [7].

Tradicionalmente en un sistema embebido el hardware se limitaba a ciertas características ya definidas e imposibles de modificar. Con el surgimiento de los SoPC se tiene una nueva alternativa debido a la versatilidad que presentan los dispositivos lógicos problamables (PLD's), en particular los del tipo FPGA [7]. La razón es que es posible incorporar hardware personalizado al sistema embebido desarrollado, por ejemplo: adaptar el procesador de acuerdo a la aplicación, incorporar únicamente el número de entradas/salidas necesarias, crear alguna interfaz para un periférico

Junio 8, 2012.
G. Muñoz. Alumno inscrito en la Maestría en Ciencias en Sistemas Computacionales Móviles en la Escuela Superior de Cómputo del Instituto Politécnico Nacional.; (e-mail: me.gerardo@gmail.com)

específico y/o desarrollar hardware acelerador especializado para tareas que requieren un carga especial de procesamiento.

Existen algunos productos comerciales que ofrecen el control de una pantalla *LCD-touch* pero todos ellos tienen un controlador integrado. En la mayoría de los casos es un microcontrolador específico, de algún fabricante, que posteriormente se integra a algún otro dispositivo programable, imposibilitando hacer modificaciones a la medida, por mínimas que sean. Además existen trabajos en los cuales se ha utilizado una pantalla LCD-*touch* en combinación con un FPGA[8], [9], [10] pero en ninguno de esos casos el *core* puede reutilizarse en otro sistema de similares características de hardware.

Lo que se plantea realizar en este trabajo es desarrollar un core, con el lenguaje de descripción de hardware VHDL, en un FPGA capaz de controlar una pantalla *LCD-touch*. Se propone que el *core* pueda ser utilizado en proyectos que requieran el uso de una interfaz de estás características, pudiendo incorporar el *core* genérico a un sistema de mayor tamaño. Para ello se contempla emplear sólo el lenguaje nativo y no las herramientas de *Mega-Core o Mega-Funtions* proporcionados por el software Quartus II, de Altera.

De esta manera se puede indicar que el objetivo principal de este trabajo es diseñar e implementar un *core* para el control de una pantalla LCD-*touch* que sirva como un *core* genérico para aplicaciones que requieran de una interfaz de este tipo. El *core* desarrollado es posible registrarlo como propiedad intelectual o como un *core* gratuito (open core).

Arquitectura propuesta

La arquitectura propuesta se puede dividir en 3 bloques principales, como se muestra en la Figura 1. En la misma figura se muestran las líneas de comunicación entre los bloques, mediante una interfaz serial se envían los comandos de configuración de registros del convertidor analógico digital y del LCD, además de recibir lectura de coordenadas de la pantalla *touch* a través del mismo medio

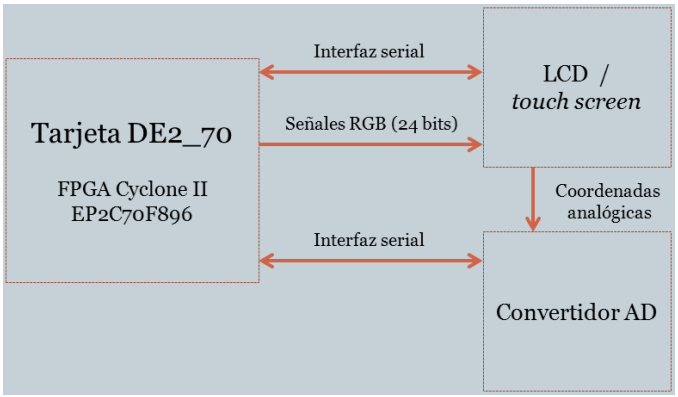


Fig. 1. Elementos de hardware del SoPC y líneas de comunicación entre los mismos

Para el diseño de este sistema se utilizará una metodología de diseño por bloques en donde no es necesario haber concluido uno para iniciar con el diseño de otro ya que al final la integración de los mismos podrá hacerse sin ningún problema.

Desarrollo

Para el desarrollo del sistema se procede inicialmente a plantear las líneas de comunicación necesarias, posteriormente las señales de reset y reloj y finalmente el diseño de cada uno de los componentes de control.

Comunicación

El protocolo serial utilizado para comunicar el Cyclone II con la pantalla LCD y el convertidor de coordenadas correspondiente a un punto tocado de la pantalla *touch*, se muestra en la Figura 2.

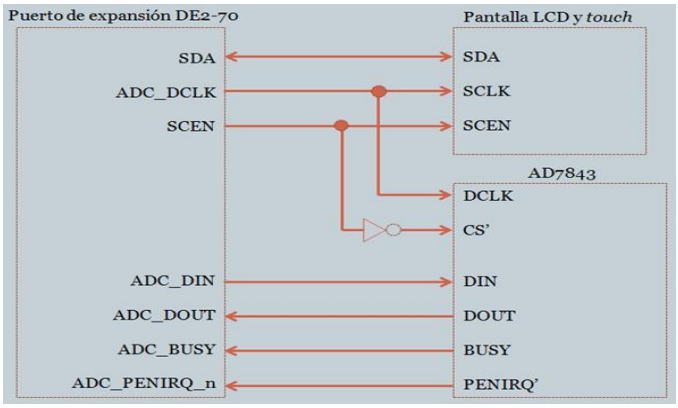


Fig. 2. Esquema de comunicación serial FPGA, LCD y convertidor analógico digital de la pantalla *touch*.

Tanto para el control del LCD como para el del convertidor se usa el mismo protocolo, es por eso que en la Figura 2 se observan dos líneas comunes para ambos elementos; la señal de reloj (ADC_DCLK – SCLK y DCLK) y la señal de habilitación (SCEN – SCEN y CS'). Las líneas restantes en ambos casos son para el envío y recepción de datos, registros y coordenadas.

En la Figura 3 y Figura 4 se muestra el formato que se debe seguir para este protocolo, en la 3 para el caso de configuración del LCD y en la 4 para la configuración de registros X y Y del convertidor.

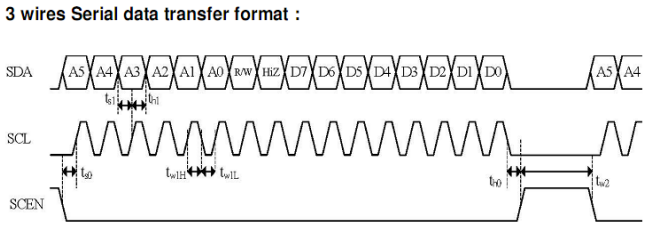


Fig. 3. Diagrama de tiempos de la interfaz de puerto serial

- SDA, señal para el envío de 16 bits para lo configuración de los registros del LCD.
- A5~A6, dirección del registro
- R/W, 1 read
- Z , señal que indica cambio a dato
- D7~D0, valor del registro
- SCL, señal de reloj con mínimo un T = 320 ns.
- SCEN, señal que indica inicio de transferencia de datos.

Para este caso se generó un componente dentro del proyecto escrito en VHDL con el cual se generaran dichas señales. Lo mismo se realizó para generar las señales que se observan en la Figura 3 y que sirven para la configuración y lectura de señales del convertidor.

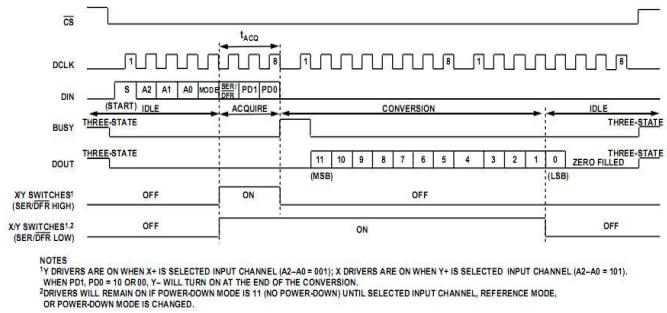


Fig. 4. Diagrama de tiempos y conversion de la interfaz de puerto serial

Componente para señales de reset

El archivo ***Reset_Delay***, usa un reloj de 50MHz y el iRST_n que es el botón de reset, teniendo esas señales como entradas su función es generar 2 retardos (oRST_0 y oRST_2), que funcionan como reset hacia los otros componentes, el primero después 41.94ms y el segundo de 83.88 ms; lo anterior para evitar problemas en la configuración de el LCD y convertidor analógico digital. Es decir, con esto se impide el envío de dato a imprimir en LCD o la solicitud de lectura de coordenadas antes de la configuración de los elementos necesarios para realizar dichas tareas.

Componente para detección de toque en la touch

Esta entidad determina la acción siguiente que se debe realizar en la pantalla LCD, genera un retardo para la exposición de cada imagen, dicho retardo es de 0.3355443 ms esto para evitar que se distorsione una imagen al querer presentar la siguiente, tiene como señales de entrada una señal de reloj de 50MH, una de reset, una más que cambia de estado cuando se ha tocado la pantalla *touch* y las últimas dos que indican las coordenadas correspondientes al punto tocado, a su salida tiene un bus por donde se envían las señales correspondientes a cada acción de acuerdo al punto tocado, por ejemplo avanzar o regresar alguna imagen.

Componente controlador del LCD

El archivo controlador del LCD, tiene dos señales de entrada: un reloj de 50MHz y una señal de reset con un retardo de 41.94 ms segundos después del botón de reset general; las señales de salida son SDAT, SCEN, SCLK y BUSY las cuales ya han sido descritas en el apartado de comunicación.

Componente controlador AD

Este componente consta de 5 señales de entrada y 6 de salida. Una señal de reloj de 50MHz, una de reset con retardo de 41.94 ms después de presionar el botón de reset general, recibe señales del convertidor AD una señal de ocupado, la lectura entregada por el ADC y la interrupción cuando se presenta un toque en la pantalla; las señales de salida son las de comunicación DCLK, DIN y las de el valor de las coordenadas X/Y correspondientes la zona tocada en la *touch*.

Componente para impresión en pantalla LCD

Encargado de generar las combinaciones de colores (RGB) para ser mostrados en la pantalla, por ejemplo, en el caso de mostrar blanco los valores son: 0,0,0; para el rojo: 255,0,0; para el verde son: 0,255,0 y para azul son: 0,0,255, Figura 5, como la combinación de colores, y los valores de las coordenadas de alguna imagen o figura. Como ejemplo este componente podría recibir las coordenadas X1, X2 y Y1, Y2 para dibujar un rectángulo en el LCD en dicha ubicación en el plano.

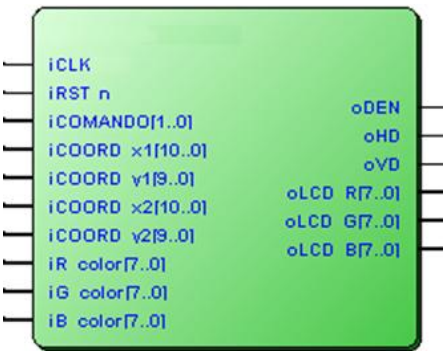


Fig. 5. Vista del bloque correspondiente al componente de impresión en pantalla LCD

Vista RTL del proyecto

El diagrama a bloques del SoPC se muestra de manera muy general en la Figura 6, en ella se muestran las señales de entrada al sistema, reloj y reset, el resto de las líneas son buses con una cantidad mayor de señales que interconctan a cada componente del sistema.

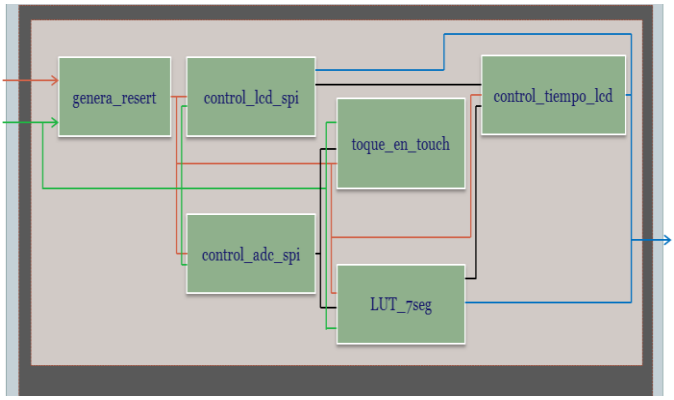


Fig. 6. Vista RTL del core diseñado

Resultados

A continuación se muestran dos imágenes de los resultados obtenidos en las simulaciones de los componentes, Figura 7 controlador LCD y Figura 8 controlador ADC.

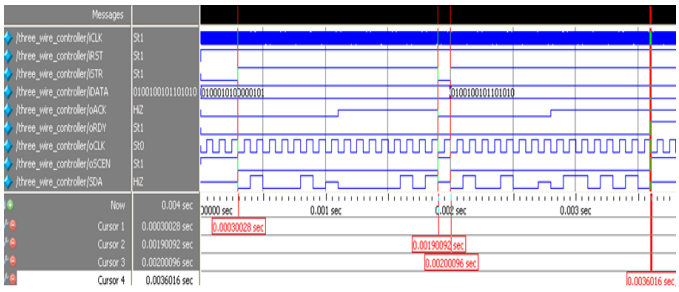


Fig. 7. Señales vistas en simulador del componente controlador LCD

Tanto en la Figura 7 como en la 8 se observa la generación de señales correspondientes al formato que se presentó con anterioridad, para el caso de la simulación del componente del controlador del LCD se muestra el valor de la señal de 16 bits para la configuración de 2 registros de los 20 posibles, mientras que en la simulación del componente del controlador ADC se configuran tan solo 2 registros uno para la configuración de la lectura de la coordenada X y el otro para la coordenada Y.

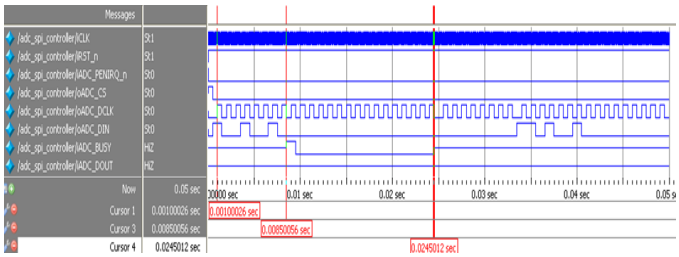


Fig. 8. Señales vistas en simulador del componente controlador ADC

Al final se puede observar en la pantalla algunas imágenes definidas en la entidad *control_tiempo_lcd*, en la Figura 9 se muestra la impresión de un rectángulo y en la Figura 10 la de una línea, en ambos casos las coordenadas y la combinación RGB se genera en la entidad previamente mencionada.

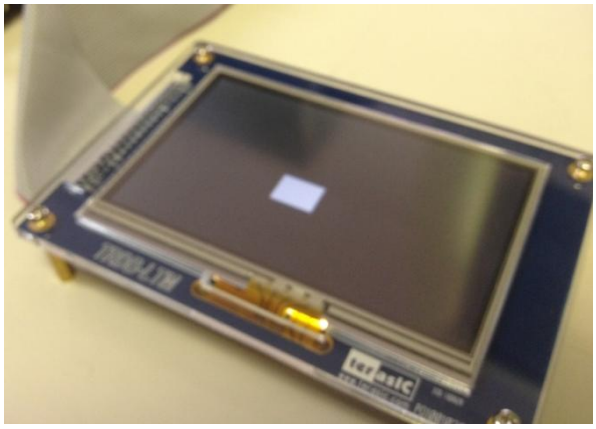


Fig. 9. Impresión de un rectángulo en el LCD especificando sus coordenadas y color.

El sistema fue realizado en la tarjeta DE2-70., que posee una FPGA CycloneII. El sistema ocupó sólo el 1% del total de elementos lógicos del dispositivo y puede tener una frecuencia máxima de operación de hasta 260MHz.

Conclusiones y trabajo futuro

El diseño de este *core*, para el control de una pantalla LCD-*touch*, fue implementado satisfactoriamente en la FGPA Cyclone II EP2C70F896. El área de ocupación fue de tan sólo el 1%. Esto indica que es posible realizar un sistema más complejo en el mismo dispositivo garantizando un desarrollo más ambicioso.

Es importante resaltar que la primer idea es la integración de este *core* a una arquitectura básica de dispositivos móviles implementada en un FPGA. De esta manera se permitiría la integración de más módulos relacionados con la misma arquitectura incorporando además de eso un procesador *soft-core*.

El uso de la programación modular y de un lenguaje de descripción de hardware ha facilitado el diseño y la modificación del mismo permitiendo con esto la integración de nuevas etapas conforme se avanza en el proyecto.

Finalmente resulta útil para ser integrado en algún tipo de proyecto donde se requiera una interfaz gráfica, que actualmente pueden ser en paneles de control industrial, de electrodomésticos, de casa habitación, etc.

Como trabajo futuro, se propone utilizar el core aquí diseñado en alguna interfaz de las que ya se ha mencionado.

Agradecimientos

Este trabajo ha sido soportado por el proyecto de investigación SIP:20121113 y el primer autor es estudiante becario PIFI.

Referencias

[18] D. Mihhailov, M. Kruss and A. Sudnitson, “FPGA Platform Based Digital Design Education”, International Conference on Computer Systems and Technologies – CompSysTech’08, 2008, pp. IV.4-1- IV.4-6.
[19] M. Esponda, “Trends in hardware Architecture for Mobile Devices”, Institut für Informatik Freie Universität Berlin, Noviembre 2004.
[20] S. Mosley and G.A. Jacoby, “A Reconfiguration of Mobile Clustering Architecture for Enhanced and Reliable Small Unit Computing”, CCECE/CCGEI May 5-7, 2008.
[21] P. Rickert and W. Krenik, “Cell Phone Integration: SiP, SoC, and PoP”, IEEE Design & Test of Computers, 2006, pp. 188-195.
[22] F. Lin, X.Jiao, Y.GUO, J. Zhang, W.Qiao, L.Jing, Y.Wang and Y. Ma, “System On Programmable Chip Development System”, Second International Workshop on Education Technology and Computer Science, 2010, pp. 471-474.
[23] L.E.M. Brackenbury, L.A. Palma and J.Pepper, “System on Chip Design and Implementation”, IEEE Transactions on Education, vol. 53, no.2, Mayo 2010.
[24] T. S. Hall and J. O. Hamblen, “System-on-a-Programmable-Chip Development Platforms in the Classroom”, IEEE Transactions on Education, vol. 47, no. 4, Noviembre 2004.
[25] M. Petouris, A. Kalantzopoulos and E. Zigouris, “An FPGA-based Digital Camera System Controlled from an LCD Touch Panel”, IEEE, 2009.
[26] L. Ludwiczak, J. Rozek and J. Pochmara, “HMI solution for controlling dynamic process with FPGA”, 15th. International conference on mixed design of integrated circuits and Systems, Junio 2008.
[27] S. J. Lee, S. H. Jin and J. W. Jeon, “FPGA based Auto Focus System using Touch Screen”, Proceedings of IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, August 2008.

G. Muñoz
Ingeniero Electrónico con especialidad en automatización y control.
Egresado del Tecnológico de Estudios Superiores de Ecatepec.
Actualmente cursando la Maestría en Ciencias en Sistemas Computacionales Móviles en la Escuela Superior de Cómputo del Instituto Politécnico Nacional
Línea de investigación: sistemas digitales para el cómputo móvil

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 4, Año 4. Enero 2012
Artículos con arbitraje

Modelo de Seguridad para Redes Aplicado a Dispositivos Móviles

Luis Enrique Hernández, Chadwick Carreto, Rolando Menchaca
Escuela Superior de Cómputo
Escuela Superior de ingeniería Mecánica y Eléctrica
Sección de Estudios de Posgrado e Investigación
México, D.F.
luisenriho@hotmail.com, ccarretoa@ipn.mx, fmenchac@ipn.mx

Resumen— El desarrollo de la tecnología de comunicación basada en redes inalámbricas móviles ha proporcionado nuevas expectativas para el desarrollo de sistemas de comunicación, así como nuevos riesgos, por lo que es necesario implementar modelos de seguridad adecuados para esta tecnología, es por esa causa precisamente que se propone en el presente trabajo el desarrollo de una aplicación basada en un Modelo de Seguridad para Redes la cual permitirá localizar la ubicación del usuario en cuanto este acceda a una aplicación utilizando su identificación personal, la cual estará asociada al dispositivo de comunicación con el cual se conecte a un servicio o red.

Palabras Claves: Seguridad, Redes Inalámbricas Móviles, Modelo de Seguridad.

Abstract- The development of communication technology based on mobile wireless networks has brought new expectations for the development of communication systems and new risks, making it necessary to implement appropriate security models for this technology, it is precisely for that reason that proposed in this paper the development of an application based on a Network Security Model which can locate the user's location as the access to an application using your personal identification, which is associated with the communication device which connect to a service or network.

Keywords: Security, Mobile Wireless Networks, Security Model.

I. INTRODUCCIÓN

La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas redes se haya disparado en el año 2002 siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

Pero como todas las nuevas tecnologías en evolución, presentan riesgos ya que usa uno de los canales más inseguros para transmitir “el aire”.

Por lo tanto en el presente trabajo se propone el desarrollo de un “Modelo de Seguridad en Redes Aplicado a Dispositivos Móviles” el cual implementa 4 niveles de seguridad garantizándole al usuario una mayor integridad de su información.

A continuación en la Sección II se brindara un marco conceptual donde se abordaran algunos de los conceptos mas importantes para el presente trabajo, en la Sección III de Antecedentes se mencionaran los modelos existentes de seguridad mas comunes para en la Sección IV definir el Planteamiento del Problema y en la Sección V la Propuesta de un Modelo de Seguridad que de solución a la problemática planteada. En la sección VI se da una visión del Caso de estudio desarrollado para probar las bondades del Modelo y en la Sección VII se da una serie de conclusiones y se define el trabajo a futuro.

II. MARCO CONCEPTUAL

Algunos de los conceptos que se manejan en el presente proyecto de investigación son los siguientes:

A. Computación Móvil

"Se define como la serie de artefactos y equipos portátiles, que hacen uso de la computación para lograr su funcionamiento."[1]

B. Computación Ubicua

"es la posibilidad de conectar todo lo que hay en el mundo a Internet, para proporcionar información acerca de cualquier cosa, en cualquier momento, en cualquier sitio, de forma transparente para el usuario." [2]

C. Seguridad

Seguridad es una característica de cualquier sistema (informático o no) que nos indica que este está libre de todo peligro, daño o riesgo, estos son algunos conceptos que la conforman:

- Autenticación.- "El sistema debe poseer los mecanismos necesarios para asegurarse que un usuario es realmente quién dice ser." [3],[4]

- Control de acceso.- "El administrador del sistema, así como cada usuario, deben poder controlar gradualmente los permisos de acceso a su información." [3],[4]

- Consistencia.- "Ante las mismas circunstancias, el sistema debe presentar el mismo comportamiento." [3], [4]

- Protección y separación.- "Los datos y las acciones de un usuario no deben ser visibles o modificables por otros, y no deben tener efecto para otros." [3], [4]

D. Problemática de la Seguridad

En las actuales redes inalámbricas es complejo garantizar que se cumplan todos los conceptos anteriormente citados.

Existen soluciones que cubren algunos aspectos, pero no existen soluciones 100% fiables y que cubran todos los aspectos de seguridad necesarios.

E. Sistema de Posicionamiento Global (GPS).

Los receptores GPS reciben la información precisa de la hora y la posición del satélite.

Estrictamente recibe una serie de parámetros generales sobre la ubicación y la operatividad de cada satélite con relación al resto de satélites de la red. Cuando el receptor ha captado la señal de, al menos, tres satélites calcula su propia posición en la Tierra mediante la triangulación de la posición de los satélites captados.

III. ANTECEDENTES

En las actuales redes inalámbricas es complejo garantizar que se cumplan todos los conceptos de seguridad.

Existen soluciones que cubren algunos aspectos, pero no existen soluciones 100% fiables y que cubran todos los aspectos de seguridad necesarios, los principales modelos existentes para resolver el problema de la seguridad en redes inalámbricas y alámbricas y lograr confidencialidad, integridad y disponibilidad:

A. WEP (Wired Equivalent Privacy) (Privacidad Equivalente al Cable)

"Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN." [5]

El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. No es compatible con IPSec.

El estándar IEEE 802.11 proporciona mecanismos de seguridad mediante procesos de autenticación y cifrado. En el modo de red Ad Hoc o conjunto de servicios avanzados, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, sólo aquellas estaciones que posean una llave cifrada serán autenticadas.

En WEP la intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire.

El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo WEP.

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación. Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional.

B. WPA \ WPA2 (Wi-Fi Protected Access) (Acceso protegido Wi-Fi)

"Es seguridad que demandan los usuarios y que WEP no puede proporcionar.

Las principales características de WPA \ WPA2 son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación." [5]

WPA es la abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (Transition Security Network).

WPA utiliza TKIP TKIP (Temporal Key Integrity Protocol) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo

sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

IV. PLANTEAMIENTO DEL PROBLEMA

En la actualidad existen modelos de seguridad en redes como los anteriormente citados, pero son poco aplicados o no se utilizan en redes móviles, por lo que no se garantiza que los usuarios de una red sean totalmente identificados y sobre todo autentificados lo cual genera un problema de inseguridad en las aplicaciones que utilizan estos modelos.

Los modelos anteriormente descritos utilizan 2 niveles de seguridad en el caso de WEB (Identificación y Autentificación) y 3 en el caso de WPA y WPA2 (Identificación, Autentificación y Confidencialidad), sin embargo eso ha sido probado que no es suficiente.

Se requiere el poder establecer modelos de seguridad más fuertes, con más características y sobre todo de varias faces, los anteriormente citados son solamente de dos faces y es necesario realizar una verificación externa para poder garantizar la identidad de una persona pero sobre todo autentificar a esa persona. Adicionalmente los mecanismos de no repudio son necesarios para dar certidumbre a una comunicación segura en redes inalámbricas.

V. MODELO DE SEGURIDAD PROPUESTO

A continuación (Figura 1) se presenta el Modelo de Seguridad Propuesto como solución a la problemática definida, es importante hacer mención que el modelo es de tres faces basado en tres capas principales mas una de apoyo para la no repudiación:

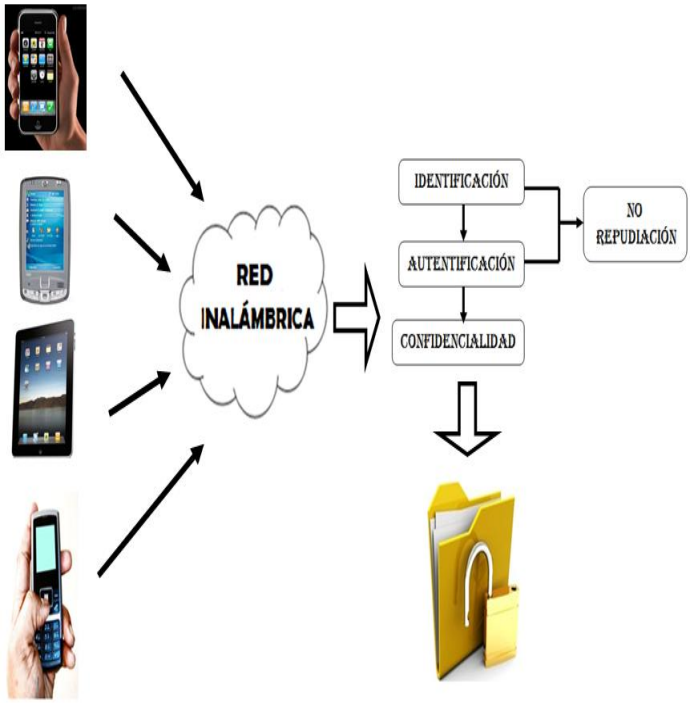


Fig. 1.1 Metodología de Seguridad por Capas

El modelo se puede describir de la siguiente forma:

Cuando un usuario desde cualquier dispositivo móvil ingresa a una red inalámbrica existirá un servicio de seguridad que esta definido por sus capas las cuales son:

- Identificación: la cual será brindada por medio de un usuario y su contraseña
- Autenticación: será asignada cuando el usuario garantice que él es quien dice ser por medias firmas electrónicas o sellos digitales.
- Confidencialidad: será avalada por medio de protocolos de encriptación de datos para proteger la información manejada por el usuario.

Como se había comentado anteriormente, adicionalmente y como una de las características de este modelo se integra una capa de No repudiación:

- No Repudio: será garantizado por medio de cellos de tiempo y con la vinculación del usuario y el dispositivo cuando el usuario se haya identificado y autentificado, de esta manera el usuario no podrá repudiar los cambios o el manejo que él haga en su información.

Estas cuatro capas de seguridad se integran con diversos sistema con el objetivo de lograr un nivel de seguridad lo mas óptimo posible para el manejo de datos.

A continuación se describirá un caso de estudio en el cual se implementa el modelo para probar sus características.

VI. CASO DE ESTUDIO

El sistema propuesto para probar el modelo se basa en un registro del lugar y hora en el que se encuentra un usuario, garantizando que el usuario es el identificado y esta asociado solamente a su dispositivo, para guardar una traza de sus actividades y su estado de localización.

El usuario se registrara y asociara al dispositivo que emitirá la señal de localización, el usuario se registrara y autenticara por medio de sus credenciales: certificado y firma electrónica. Cada dispositivo estará asociado por medio de su dirección MAC a solamente un usuario. Por lo cual se define un vinculo entre dispositivo y usuario autenticado.

Se diseñó un caso de estudio el cual permite registrarse en algún servicio por medio de un usuario y su contraseña y al tener acceso automáticamente se activara el GPS del dispositivo móvil y comenzara a guardar la posición del usuario en una base de datos diseñada en SQLite el cual es un sistema de gestión de bases de datos relacional que se encuentra contenida en una pequeña biblioteca escrita en C y es un proyecto de dominio público, de forma que cada determinado tiempo se guardaran las coordenadas del usuario.

Al finalizar el usuario su operación y salga de está el sistema guardara la base y la mandara al servidor principal, el cual llevara un registro de todas las posiciones geográficas del usuario así como de su identificación personal digital y la autenticación establecida con el Usuario.

Esto nos genera una traza del estado donde se encuentra el usuario así como de su interacción en un mapa de lugares basado en GoogleMaps. .

A continuación se puede apreciar algunas capturas de este caso de estudio:

La vista de acceso a la aplicación es un App estañar el cual se desarrollo para Android peor puede generase para cualquier otro sistema, el acceso es mediante un nombre de usuario y su contraseña Fig. 2.1:

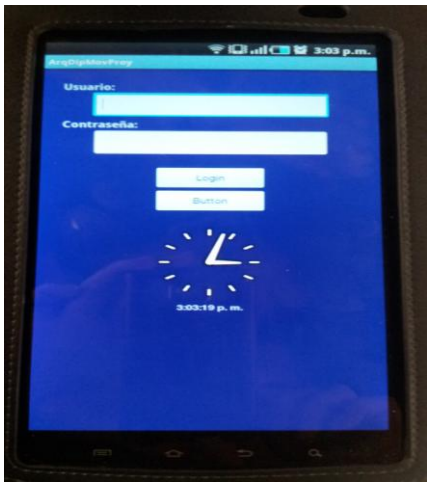


Fig. 2.1 Login.

Las coordenadas geográficas obtenidas por medio del GPS del dispositivo se clasifican encriptan y guardan en una base de datos, ordenándolas por fecha y hora en que se van obteniendo. Fig. 2.2:

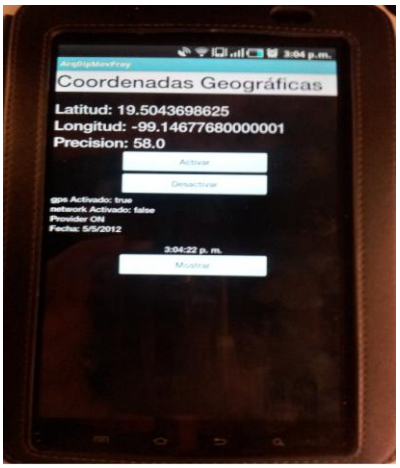


Fig. 2.2 Coordenadas Geográficas.

Por medio de una base de datos creada en SQLite se guardan todas las coordenadas geográficas recibidas durante el tiempo que el usuario se encuentre activo Fig. 2.3.

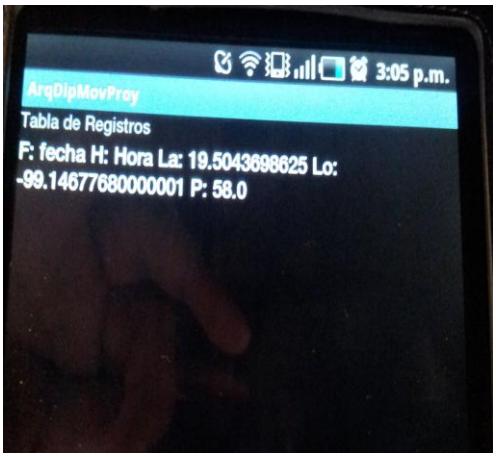


Fig. 2.3 Base de Datos.

Una vez el servidor reciba la base de datos podrá hacer un mapeo de la ubicación del usuario mostrando los desplazamientos que hizo durante el tiempo que accedió al servicio Fig. 2.4.

Fig. 2.4 Aplicación para Localización Satelital

CONCLUSIONES Y TRABAJO A FUTURO

En el presente trabajo se describió la propuesta de un Modelo de Seguridad para Redes aplicado principalmente a las redes Inalámbricas y sistemas Móviles. Como se pudo observar el Modelo se basa en un modelo de tres frases y cuatro capas. Pretende como aportación el poder garantizar no solamente la identificación y Autenticación, también pretende lograr un control de no repudiación, este modelo y sobre todo el control de no repudio se aplicó a un caso de estudio en el cual se implemento el modelo de tres fases y se logro localizar a usuarios para definir e identificar a los mimos asociándolos a su dispositivo móvil con la garantía de no poder negar que no se encontraba en el lugar detectado.

Como trabajo a futuro se realizaran pruebas con múltiples usuarios para poder obtener el grado de fiabilidad de la presente propuesta.

AGRADECIMIENTOS

Los autores del presente trabajo agradecen a ESCOM, ESIME, CIC, COFFA, SIP por las facilidades proporcionadas para el desarrollo del presente trabajo.

Referencias

[1] Computación Móvil y Computación Ubicua . [En Línea] <http://es.scribd.com/doc/21924686/computacion-movil> [Consulta : Septiembre 2011]

[2] *Josep Molas i Bertrán, "Computación Ubicua", Una nueva Junta Directiva de ATI para un nuevo periodo, Octubre 2001, pp.*

[3] *Coordinacion de Emergencias en Redes Teleinformáticas, Manual de Seguridad en Redes [En línea] <http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf> [Consulta : Octubre 2011]*

[4] *Gunnar Wolf. Seguridad en redes: >Que es? >Como lograrla? [En Línea] <http://gwolf.org/files/seg_en_redes.pdf> [Consulta : Septiembre 2011]*

[5] *Saulo Barajas. Protocolos de seguridad en redes inalámbricas [En Línea] <http://www.saulo.net/pub/inv/SegWiFi-art.htm >[consulta : octubre 2011]*

[6] *Pedro Navarro Pérez. WIRELESS APPLICATION PROTOCOL [En Línea] <www.uv.es/montanan/redes/trabajos/WAP_Pedro.doc >[consulta : octubre 2011]*

[7] *Rodolfo Quispe-Otazu. ¿Que es la Ingeniería de Software?. Blog de Rodolfo Quispe-Otazu [Internet]. Mayo 2007. Disponible en: <http://www.rodolfoquispe.org/blog/que-es-la-ingenieria-de-software.php> [consulta: 21 Septiembre 2011]*

[8] *Universidad de Valencia. Seguridad en Redes Inalámbricas. [En Línea] <http://documentos.shellsec.net/otros/SeguridadWireless.pdf> [Consulta : Septiembre 2011]*

[9] *Saulo Barajas. Protocolos de seguridad en redes inalámbricas[En Línea] <http://www.govannom.org/seguridad/14-wifi-wireless-redes/139-protocolos-seguridad-redes-inalambricas.html> [Consulta: Noviembre 2011]*
[10] *Normas de Confidencialidad. [En Línea] < http://www.linksysbycisco.com/LATAM/es/privacypolicy > [Consulta: Octubre 2011]*
[11] *Seguridad Informática [En Línea] <http://www.slideshare.net/jemarinoi/seguridad-informtica-1125964 > [Consulta : Octubre 2012]*

Luis Enrique Hernandez Olvera es estudiante de la Maestría en Ciencias en Sistemas Computacionales Móviles. Es ingeniero en Sistemas Computacionales por parte de la Escuela Superior de Cómputo del Instituto Politécnico Nacional, sus líneas de investigación son: Seguridad en Redes Inalámbricas y Sistemas Móviles, Protocolos móviles y desarrollo de Aplicaciones Móviles para Android.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 4, Año 4. Enero 2012
Artículos con arbitraje

Sistema de control inteligente usando lógica difusa para regular las actividades de un sistema de información

Omar Del Rosario España, Rosaura Palma Orozco, José de Jesús Medel Juárez

Resumen - Los algoritmos utilizados por los sistemas manejadores de bases de datos actualmente se basan en aproximaciones por prueba y error para encontrar de forma automática los valores óptimos de afinación. Presentan problemas como la omisión del efecto de reconfiguración, y la omisión de los objetivos de desempeño definidos por el usuario. La presente investigación propone el uso de elementos de lógica difusa y bases de conocimiento en un sistema de control que tome en cuenta estos problemas.

Palabras clave – Afinación autonómica, Lógica Difusa, Control

I. INTRODUCCIÓN

El soporte de operación de la mayor parte de los sistemas de información son las bases de datos. Es posible tener grupos de servidores de aplicaciones para atender a la demanda creciente de usuarios de un sistema de información, sin embargo, todas las operaciones son soportadas por un solo sistema gestor de base de datos (SGBD). [3]

Las actividades de afinación del desempeño permiten ajustar las características de una base de datos a su uso particular, a la demanda de usuarios y a los requisitos de disponibilidad y tiempo de respuesta. Consisten en ajustar parámetros de rendimiento [1] para un caso particular en un momento en el tiempo [2].

Estas actividades consumen mucho tiempo y en algunos casos no es posible aplicar una metodología específica. Frecuentemente se hace necesario aplicar un enfoque holístico, es decir, afinar el sistema como un todo, lo que requiere de un conocimiento profundo acerca de los sistemas de información [3]. Los cambios en las condiciones de trabajo de las organizaciones necesariamente provocan realizar nuevamente estas actividades.

La afinación se complica con la ausencia de información histórica de diagnóstico para investigar problemas de desempeño al inicio de su ocurrencia. Esto alarga el tiempo necesario para llevar una base de datos a una operación óptima, pues en algunos casos es necesario replicar los problemas en un entorno controlado para poder realizar su diagnóstico.

Microsoft Research [4], IBM Labs [5] y Oracle Labs [6] han realizado avances en el objetivo de la Auto Afinación, propuesto por el *Technical Committee on Data Engineering* [7] en 2006. Los algoritmos utilizados se basan en la aproximación por prueba y error para encontrar los valores óptimos de afinación [8]. Sin embargo presenta el problema de que no se toma en cuenta el efecto de la reconfiguración, es decir, se asume que un cambio en la configuración posterior a los valores óptimos puede degradar el desempeño. Además, no toma en cuenta los objetivos de desempeño definidos por un usuario. Por ejemplo, se afina para dar respuesta a una base de datos de tipo transaccional [9]; pero si la misma atiende operaciones de tipo *data warehouse* [10] o de minería de datos [11], sólo es posible realizar la afinación para un tipo de operaciones en particular [8].

Se presenta una propuesta de aplicación de algoritmos adaptivos [12] para la afinación dinámica tomando en cuenta la experiencia del administrador. En particular se busca probar que es posible aplicar la teoría de control [13] a la afinación automática de bases de datos [14].

II. MÉTODO

Al abstraer las actividades de afinación de un SGBD [12] como una caja negra sometida a un proceso de control [1], se identifican variables a medir y ajustar, así como parámetros indicadores de una operación óptima. También se identifica

que el comportamiento del sistema cambia con el tiempo, es decir, es dinámico. Además, es necesario tomar decisiones de ajuste en parámetros de operación para mantener al sistema dentro de rangos de operación óptimos.
En la figura 1 se muestra el modelo de un sistema de control difuso.

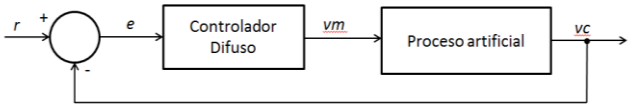


Figura 1: Modelo de un sistema de control difuso

Donde el proceso artificial es aquel que queremos controlar, el controlador difuso emite señales "vm" como acciones de control al proceso artificial que dependen de las condiciones iniciales "r" y del valor actual "vc". El controlador difuso es retroalimentado también por "vc" para obtener un valor de error o desviación "e" para emitir nuevamente señales "vm" al proceso artificial.
Si hacemos que el proceso artificial de la figura 1 sea un sistema manejador de bases de datos, las variables a controlar serían aquellas que permitan alterar el grado de optimización en la operación, las acciones de control estarían orientadas a ajustar los valores que mejoren el proceso y tomadas por el administrador de bases de datos, o el controlador difuso.
De esta forma se encuentran condiciones que permiten modelar un sistema de control que además de mantener a una base de datos dentro de rangos de operación óptimos, sea capaz de reaccionar rápidamente ante cargas de trabajo de diferente naturaleza y duración, así como tomar en cuenta las consecuencias de dichos ajustes para evitar reducir el desempeño.
En la figura 2 se muestra el modelo de control propuesto utilizando elementos de control con lógica difusa como método de toma de decisiones. Incorpora una base de conocimiento formada por reglas de inferencia acerca de las variables de entrada y salida resultado de la observación del comportamiento del sistema y la aplicación de conocimientos en su afinación. Al regular el control empleando la experiencia del administrador permite reducir el efecto de la reconfiguración, evitando los valores que pueden degradar el desempeño.
También se incorporan restricciones que el entorno impone a la operación del mismo. Esto permitirá que una misma base de datos pueda usarse para diferentes propósitos (procesamiento de transacciones, *data warehouse*, etc.) y cargas de trabajo (número de usuarios y operaciones). Incorporando estas restricciones como el tiempo de respuesta esperado, se toma en cuenta el entorno en el que opera el sistema.
En la presente investigación se han incluido para su control, las áreas de memoria de un sistema manejador de bases de datos Oracle 10g versión 10.2.0.1 [2].

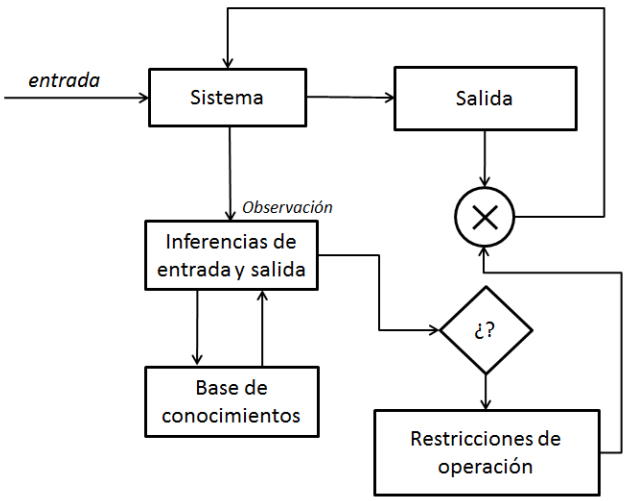


Figura 2: Modelo de control propuesto utilizando lógica difusa

Actualmente se genera la base de conocimiento, mediante la documentación y clasificación de las variables a controlar y sus rangos válidos de ajuste. Se identificarán los parámetros a evaluar para el ajuste óptimo y construirá un sistema de

información que permita mantener a una base de datos en condiciones de operación óptimas. La operación del sistema deberá igualar o superar los resultados de la prueba *TCP Benchmark C* [15] ejecutada en hardware comparable.

III. DISEÑO DE LAS PRUEBAS

Se empleará la metodología *TPC-C* y *TPC-H* del *Transaction Processing Performance Council TPC [15]*, que permite evaluar el rendimiento de bases de datos independientemente del SGBD, sistema operativo y hardware utilizado en términos de dos indicadores de calidad: Tiempo de respuesta y Número de transacciones por minuto (tpmC).
El *TPC* [16] es un organismo dedicado a estandarizar las mediciones de desempeño en bases de datos desde 1988. Entre sus miembros se encuentran los principales fabricantes de hardware de servidores, así como los principales manejadores de bases de datos. Sus pruebas son auditadas por organismos externos para su aceptación.
Se empleará la herramienta *Quest Benchmark Factory* en su versión 9.0 que permite realizar la prueba de benchmarking según las especificaciones de *TPC-C* y *TPC-H [17]*. La herramienta permite la creación de una base de datos estándar con las características requeridas en diferentes manejadores de bases de datos, ejecuta la carga de transacciones simulando la conexión de usuarios concurrentes en diferentes intervalos y realiza la medición de las actividades del benchmark. La consistencia de resultados se mantiene pues la prueba se aplica manteniendo la carga de usuarios en un intervalo de tiempo controlado [17].
El equipo donde se ejecutará la prueba es una computadora portátil con las siguientes características: Procesador Intel Core i7 2630QM@2GHz, 8GB de RAM DDR3 1333MHz, SSD 128GB SV100S2128G.
Se realizarán tres procesos de benchmarking manteniendo siempre la misma configuración de hardware, parámetros de operación del sistema operativo y condiciones iniciales del manejador de base de datos.
Protocolo de Ejecución de las pruebas
1. Instalar y configurar con los parámetros recomendados por el fabricante el manejador de base de datos *Oracle* versión 11.2.0.1 en un sistema operativo *Oracle Linux* versión 6.0
2. Crear una base de datos estándar *TPC-C* y *TPC-H* con un tamaño de 80 GB (Base de Datos de Referencia).
3. Realizar un benchmark con la configuración inicial recomendada por el fabricante. Se emplea el motor de afinación por defecto de que dispone el manejador.
4. Registrar los resultados obtenidos como CONTROL.
5. Restablecer la Base de Datos de Referencia al momento inmediato anterior al paso 3 y reiniciar la instancia de base de datos.
6. Realizar un benchmark con la configuración inicial recomendada por el fabricante. Se emplea el motor de afinación diseñado.
7. Registrar los resultados obtenidos como PRUEBA 1.
8. Restablecer la Base de Datos de Referencia al momento inmediato anterior al paso 3 y reiniciar la instancia de base de datos.
9. Realizar los ajustes necesarios al modelo.
10. Realizar un benchmark con la configuración inicial recomendada por el fabricante. Se emplea el motor de afinación diseñado.
11. Registrar los resultados obtenidos como PRUEBA 2.
12. Fin de la prueba.

IV. CONCLUSIONES

Se han analizado las características y actividades de un sistema de control y se han comparado con los elementos de un SGBD y sus actividades de afinación identificando en ambos casos un elemento a controlar, y variables que deben ser ajustadas para obtener en un elemento de control una operación óptima. En esta comparación se han encontrado similitudes en su operación que permiten aplicar los mecanismos de la teoría de control en su afinación. De esta forma se propone un modelo (fig. 2) para la aplicación del control utilizando lógica difusa para la afinación de bases de datos.
Se han encontrado puntos de mejora respecto de los métodos actuales de afinación automática como consecuencia de la incorporación de elementos de lógica difusa y bases de conocimiento a un sistema de control como afinador automático de desempeño: reducción del efecto de reconfiguración al incorporar la experiencia del administrador; y el tomar en cuenta las restricciones del entorno, al incorporar estas restricciones como parte de las reglas difusas.

Referencias

[1] Oracle Corporation. “Performance Features in Oracle 11g”, 2009.
[2] Oracle Corporation. “Oracle Database Performance Tuning Guide 10g Release 2 (10.2)”, 2008.

[3] IBM Corporation. “Relational Database Design and Performance Tuning for DB2 Database Servers", 2004.

[4] Microsoft Corporation, http://research.microsoft.com/enus/projects/autoadmin/. “Microsoft Research AutoAdmin Project”, 2011.

[5] Sam Lightstone, Guy M. Lohman, Peter J. Haas, Volker Markl, Jun Rao, Adam Storm, Maheswaran Surendra, and Daniel C. Zilio. “Making DB2 products self-managing: Strategies and experiences”. Bulleting of the Technical Commttee on Data Engineering, sep 2006.

[6] Benoit Dageville and Karl Dias. “Oracle's self-tuning architecture and solutions”. Bulleting of the Technical Commttee on Data Engineering, sep 2006.

[7] Sam Lightstone. “Letter from chair of the working group on self-managing database systems". IEEE Data Eng. Bull., pages 4-5, 2006.

[8] Marc Holze and Norbert Ritter. “System models for goal-driven self-management in autonomic databases”. Data & Knowledge Engineering, pages 685-701, 2011.

[9] Tanya Puntti. http://www.hypergurl.com/blog/databases/transaction-processing.html “Transaction Processing in Large Database Systems”. Central Queensland University.

[10] Mendez, A., Mártire, A., Britos, P. , Garcia-Martínez, R. “Fundamentos de Data Warehouse”.Centro de Actualización Permanente en Ingeniería del Software, Instituto Tecnológico de Buenos Aires, Argentina 2003

[11] Jiawei Han, Micheline Kamber. “Data Mining: Concepts and Techniques” 2nd Edition University of Illinois at Urbana-Champaign Elsevier 2006

[12] Romero Urbueta Parrazales, José de Jesús Medel Juárez, Rosaura Palma Orozco. “Control Difuso usando Sistemas Digitales”. McGraw-Hill, 2010.

[13] Juan Carlos García Infante, José de Jesús Medel Juárez, and Rosaura Palma Orozco. Sistemas con Lógica Difusa". McGraw-Hill, 2010.

[14] Sanjay Agrawal, Nicolas Bruno, Sujarit Chaundhuri, and Vivek Narasayya. “Autoadmin: Self-tuning database systems technology”. Bulleting of the Technical Commttee on Data Engineering, 29(3), sep 2006.

[15] TPC Benchmark C full disclosure report for ProLiant ML350T03 X2.8/533 512 SA641 using Oracle DB v.10.2.0.1 and Microsoft Windows Server 2003 Standar Edition", Apr 2004.

[16] Sitio oficial del Transaction Processing Performance Council TPC http://www.tpc.org consultado el 5 de septiembre de 2011.
[17] Sitio oficial del fabricante Quest Software –Benchmark Factory http://www.quest.com/benchmark-factory/ consultado el 6 de diciembre de 2011.

Omar Del Rosario España. (D.F., México, 1980) Estudiante de la Maestría en Sistemas en Cómputo Móvil, en la Escuela Superior de Cómputo del Instituto Politécnico Nacional, D.F. México. Desde 2005, Ingeniero en Sistemas Computacionales de la Escuela Superior de Cómputo del Instituto Politécnico Nacional.
Desde 2011 asesor de seguridad y tecnología de la información TI para la División de Sistemas de Información de la Secretaría de Administración en el Instituto Politécnico Nacional y Administrador de Infraestructura de TI de la Comisión de Operación y Fomento de Actividades Académicas del Instituto Politécnico Nacional. Por cuatro años fue jefe del Departamento de Afinación de Bases de Datos y Auditoría Informática en el Centro Nacional de Cálculo de la Coordinación General de Servicios Informáticos del Instituto Politécnico Nacional.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 4, Año 4. Enero 2012
Artículos con arbitraje

Arquitectura de seguridad basada en identificación y autenticación para cómputo móvil

Sandra Anízar González[1], Chadwick Carreto Arellano[2]
Instituto Politécnico Nacional
ESCOM-SEPI
Distrito Federal, México
sanizarg0400@alumno.ipn.mx[1], ccarretoa@ipn.mx[2]

Resumen-*Desde siempre, la seguridad ha sido un requisito indispensable para toda sociedad humana, por lo que, contar con un método de identificación que no solo este conformado por un típico par usuario y contraseña, sino que además permita la autenticación del usuario, es cada vez más necesario. Al mismo tiempo, tomando en cuenta que hoy en día es más común la autenticación de usuarios en dispositivos móviles que en máquinas de escritorio.En éste trabajo, se propone una arquitectura de seguridad para cómputo móvil, que conjunta diversas tecnologías: cifrado asimétrico, firma digital, usuario y contraseña ;junto con tres módulos de información pertenecientes al usuario: pública, privada y biométrica, creando una identificación digital que podrá ser utilizada en diferentes servicios para la autenticación de usuarios evitando entre diversos problemas, el no repudio y el robo de identidad.*
Palabras clave: ***Cómputo móvil, seguridad, identificación digital, autentificación, biometría.***

Abstract- O*ver time, the security has been a prerequisite for all human society, therefore, having a method of identification that which not only consists of a username and password, but also allows the user authentication, is increasingly most needed. At the same time, considering that nowadays is more common user authentication on mobile devices than on desktop machines. In this paper we propose a security architecture for mobile computing that combines several technologies: asymmetric encryption, username and password, digital signature; along with three modules of information belonging to the user: public, private and biometric, for getting a digital identity that can be used in diverse services for user authentication and so avoiding problems like the non-repudiation and identity theft .*
Keywords: ***Mobile computing, security, digital ID, authentication, biometric.***

1. Introducción

Es esencial que dentro de toda sociedad humana esté presente la necesidad de identificar a cada uno de los integrantes que la conforma de manera que, al portador de la identificación se le puedan aplicar diversas leyes, otorgar obligaciones, así como permitir el acceso a recursos, servicios, instituciones y beneficios de manera segura.

Alrededor del mundo, cada país intenta contar con mínimo un medio de identificación oficial entre sus ciudadanos. En México existen varios de ellos como la cédula de identidad ciudadana, el pasaporte y la cartilla militar, pero principalmente existe la credencial de elector del Instituto Federal Electoral, otorgada sólo a los ciudadanos mayores de 18 años, y que sirve como identificación en el momento de ejercer el derecho al voto así como en la mayoría de los servicios y tramites. Ésta identificación cuenta con la siguiente información del titular: nombre completo, domicilio, edad, sexo, folio, año de registro, clave de elector, firma, fotografía y huella del dedo índice, entre otras.

Analizando lo anterior, existen puntos de vulnerabilidad si tal identificación es extraviada o robada:

- No permite la autenticación del portador, por lo cual cualquier persona maliciosa que la tenga en su poder, puede hacerse pasar por el dueño, perjudicándolo en muchos sectores.
- El alto número de información que contiene, pues puede que está sea una herramienta de extorsión y secuestro por el crimen organizado.

Es por esto, que se necesita de un método de identificación y autenticación que no solo conste de una credencial, más bien, que conjunte datos únicos del individuo (personales, académicos, de salud, financieros y hasta biométricos) con un medio de transmisión digital, que mantenga segura la información del titular, así como a él mismo. A esto se le conoce como identidad digital.

Si a todo lo anterior le sumamos que el uso de la autenticación de usuarios es más común en dispositivos móviles que en maquinas de escritorio por el creciente número de servicios móviles en el mundo, y sabiendo que la identificación de personas es y será un tema de investigación y desarrollo importante junto a la constante evolución de las sociedades humanas, en este trabajo se propone una arquitectura de seguridad basada en identificación y autentificación para cómputo móvil de la que se obtendrá una ID digital con la que se pretende lograr que el individuo pueda tener acceso a diversos servicios web donde y cuando sea necesario un método de identificación y autenticación, ya que para ésta ID digital, se combinan tecnologías de seguridad con el análisis de información biométrica, pública y privada.

A continuación, en la sección II se dan a conocer algunos de los antecedentes para el desarrollo del trabajo, en la sección III se describe la arquitectura propuesta así como las características de los elementos y módulos que la componen, finalmente en la sección IV se muestra las conclusiones del trabajo.

II. Antecedentes

Desde siempre el hombre se a preocupado por restringir el acceso a sus bienes materiales y a su información manteniéndolos seguros. Y a seguro nos referimos a la cualidad de seguro refiriéndose a libre y exento de todo peligro, daño o riesgo [1]. Esto nos lleva a dos básicas definiciones para este trabajo, la identificación y la autenticación.

Como la acepción más común de la palabra identificación, se encuentra que es el acto de identificar, reconocer o establecer los datos e información principal sobre una persona, lo que la ha hecho crucial para la sociedad desde el comienzo de la civilización hasta nuestros días, usada en los sectores financieros, de salud, de transporte, de entretenimiento, cumplimiento de la ley, seguridad, control de acceso, control migratorio, gobierno, comunicación entra otros [2].

Y como autenticación nos referimos, es la verificación de la identidad de una persona o de un proceso, para acceder a un recurso o poder realizar determinada actividad [3].

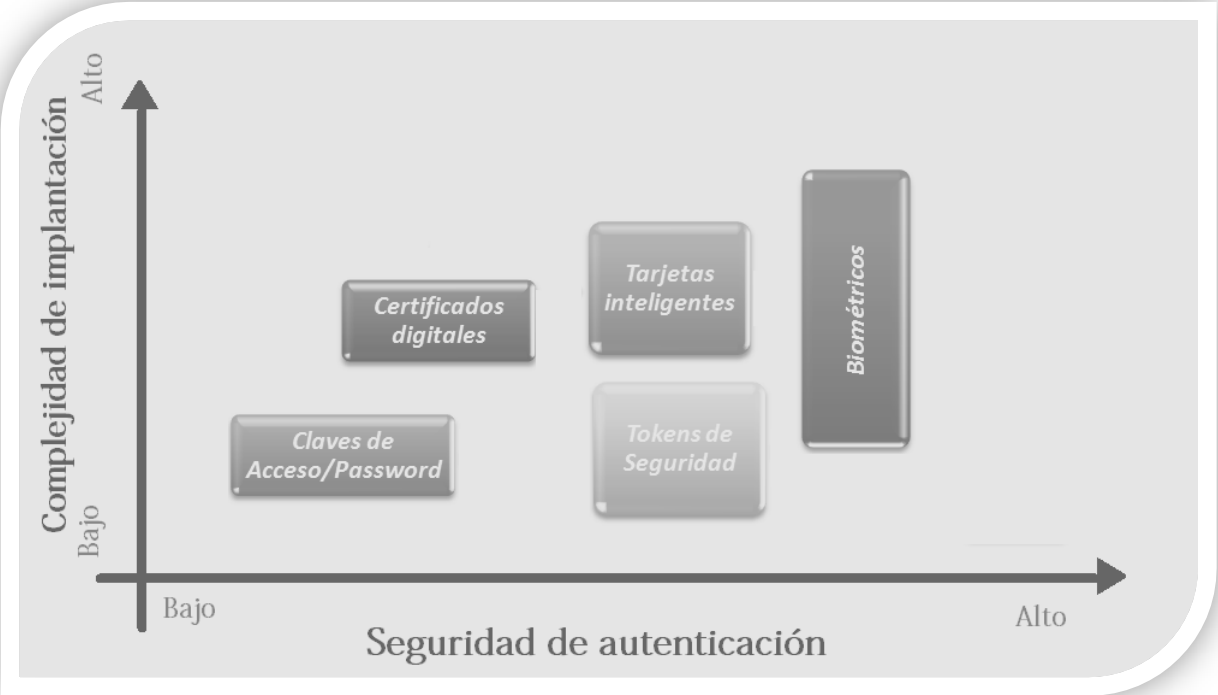
Estas dos son utilizadas para entre muchas cosas, garantizar el no repudio, el cual es la condición en la que quien realiza alguna acción no puede negar la validez del resultado del proceso que se utilizó para autenticar la información [4].

Los principios básicos de la seguridad de la información son:

- Confidencialidad: propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
- Integridad: propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.
- Disponibilidad: cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones [5].

A estos principios también se les conoce como la Tríada CIA, del inglés: "Confidentiality, Integrity, Availability" y existen diversos tipos de personas maliciosas que buscan dañarlos como los hacker.
Es por eso que es necesario verificar que el portador de la identificación es quien dice ser y para eso, existen diferentes tecnologías que apoyan el mecanismo de autentificación de usuarios tales como certificados digitales, claves de acceso/password, tarjetas inteligentes, tokens de seguridad, biométricos entre otros. En la Fig. 2.1 se muestran estas tecnologías así como su relación con la complejidad de implantación.

Fig. 2.1 Tecnologías que apoyan el mecanismo de autentificación



Lo malo en ellas, es que individualmente generan problemas de seguridad como:

- La contraseña pueden ser vulnerable al espionaje o robo de las mismas.
- Son comúnmente falsificables.
- Robo y clonación de tarjetas inteligentes.
- No autorizan a los individuos, sino a los tokens y por lo tanto no prueba quien es la persona que lo tiene.
- Los biométricos todavía son caros y requieren hardware especializado.

Al hablar hoy día de sistemas de comunicación segura, se introduce una herramienta que maneje la seguridad de redes y comunicaciones y esta es el cifrado, cuyo principio es mantener la privacidad de la comunicación entre un emisor (persona que envía un mensaje) y un destinatario o receptor (persona que recibe el mensaje).

En este esquema de cifrado se tienen dos aspectos de importancia; el primero es el uso de una clave pública (k1) y una privada (k2); una es usada para el cifrado y otra para el descifrado, la seguridad está en la longitud de las claves y el costo computacional para romper el cifrado. El segundo aspecto es el uso de un algoritmo de cifrado; el algoritmo realiza diferentes transformaciones en el texto claro, si el emisor envía un mensaje privado al receptor, para cifrar el algoritmo usa la clave pública del receptor y el receptor lo descifra usando su clave privada; ejemplos de estos algoritmos son el RSA y el Gamal [6]. El esquema de este cifrado se muestra en la Fig. 2.2.

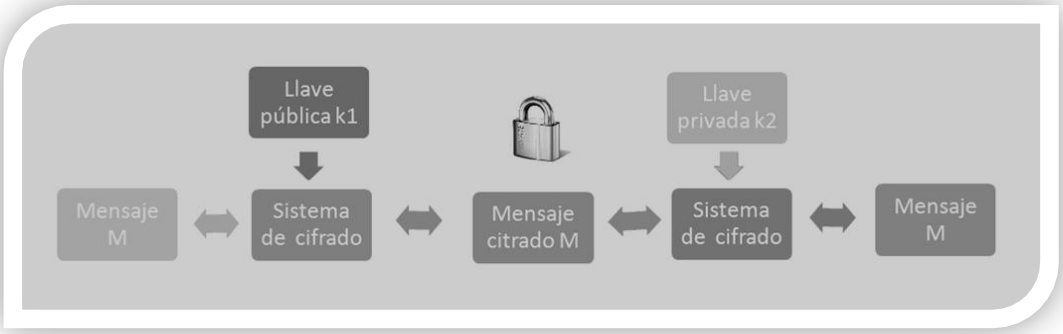


Fig.2.2 Cifrado Asimétrico

Utilizando estas tecnologías antes mencionadas, existen diversos sistemas & arquitecturas que las conjuntan para así formar una ID digital y que son implementadas en dispositivos móviles.[7] Los podemos dividir en los que utilizan:

- Únicamente biometría: necesitan un dispositivo especial del cual extraer la información biométrica de los usuarios, después son encriptados [8][9].
- Información personal & GSM: Necesitan del software instalado en el teléfono móvil del cliente, software de servidor, y de un módem GSM conectado al servidor [10].
- Información biométrica y personal. . Toma en cuenta diversos factores importantes en el tema de la autenticación de usuarios, pues tiene en cuenta tres aspectos que sirven como candados: el token, contraseña y biometría [11].

III. Propuesta de Arquitectura de seguridad basada en identificación y autenticación para cómputo móvil

Con el fin de evadir la problemática de la identificación y autenticación en el cómputo móvil, se propone conjuntar diversas tecnologías de seguridad como: el cifrado asimétrico, la firma digital, el par usuario/contraseña, certificados digitales, entre otros; con tres tipos de información pertenecientes al usuario: pública, privada y biométrica, creando una identificación digital que podrá ser utilizada en diferentes servicios para la autenticación de usuarios como se muestra en la Figura 3.1.

Esta arquitectura de identificación y autentificación, estará compuesta por dos módulos:

- Generación de ID digital: En este modulo se le pedirá al usuario que introduzca su información pública, y sólo procederá al siguiente paso cuando tal información sea validada por una tercera instancia, después se le pedirá la información privada y al final su información biométrica. Se conjuntará la información obtenida y con la aplicación del cifrado asimétrico, el MD5, la generación de una firma digital y la obtención de un certificado digital, se genera la ID digital, la cual posteriormente es guardada en un dispositivo móvil y así, se está lista para ser utilizada.
- Validación: En este modulo se verifica que la persona que tiene en su poder el dispositivo móvil es la misma que genero su ID digital, al checar que la información no esté modificada, que el certificado aun no caduque y que la información que introduzca sea la misma.

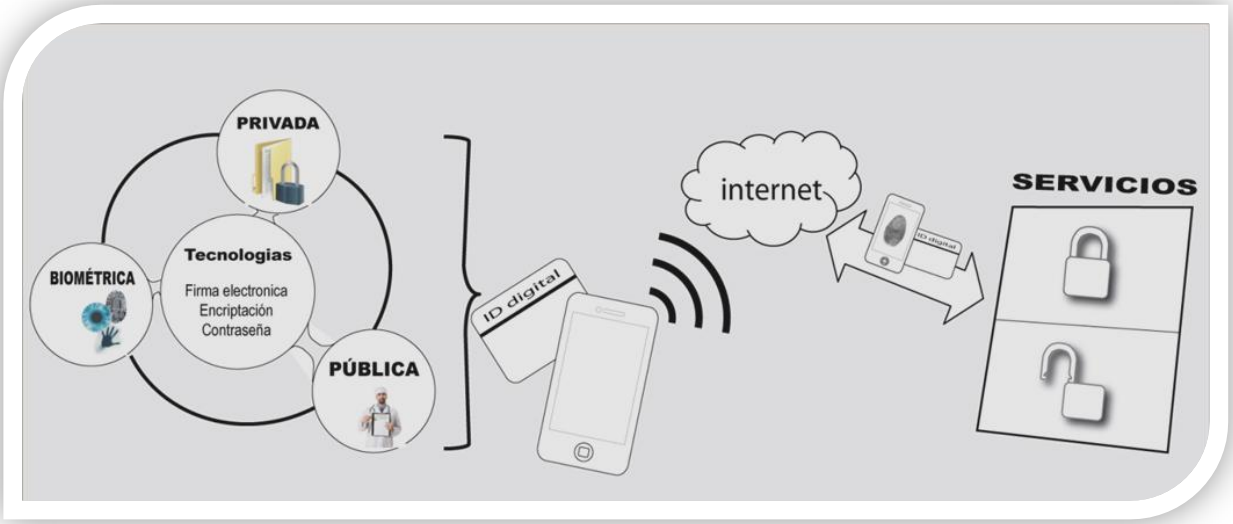


Fig. 3.1 Representación de la arquitectura de seguridad basada en identificación y autentificación para cómputo móvil.

Las principales características que se tienen de este trabajo son:

- Sencillez: Al eliminar la complejidad de uso de sus interfaces y sea apto para cualquier tipo de usuario que tenga en su poder un dispositivo móvil con ciertas características especiales, capaces de soportar la biometría adecuada para esta propuesta.
- Robustibilidad: Considerando la información conformada por tres fases de seguridad: Personal, pública y biométrica.
- Movilidad: Al ser una arquitectura de seguridad móvil, obtiene mayor portabilidad y sencillez que las que son empleadas para las maquinas de escritorio.
- Seguridad de información: si por algún motivo el usuario perdiera su dispositivo móvil, la persona que lo encuentre no podrá acceder a tu información, puesto que para tener acceso a ella se necesita de la información privada y biométrica.

IV. Conclusiones

Hoy en día es indispensable contar con un sistema de identificación que permita la autenticación de usuarios por medio de los dispositivos móviles para poder acceder de manera segura a los diferentes servicios web. Por lo que mientras más información contenga tal identificación digital y más candados (tecnologías de seguridad) se utilicen, se obtendrá una gran ventaja ante las personas maliciosas del mundo exterior que quieren tener acceso a la información del usuario.
Es por eso que en este trabajo se propone la creación de una arquitectura que contemple tres tipos de información única del usuario: publica, privada y biométrica. A éste conjunto de información se le adjunta diversas tecnologías como criptografía asimétrica, MD5, firma digital y certificado digital, permitiendo crear una ID digital, completa y segura.

Referencias

[1] Real academia española, Diccionario de la lengua española, 22ª edición, 2001.
[2] Roger Clarke, Human Identification in Information Sytems, Management Challenges and Public Policy Issues, Information Technology & People, 1994.
[3] Joseph Migga Kizza, Computer Network Security, páginas 233-256,2005.
[4] Morrie Gasser, Building a Secure Computer System Van Nostrand Reinhold, Nueva York, Estados Unidos, 1988.
[5] Rick Lehtinen,Deborah Russell,G. T. Gangemi, Computer Security Basics: O'Reilly Media, 2ª edición, 2006.
[6] Joseph Migga Kizza, Computer Network Security, páginas 233-256, 2005.
[7] Alfred J. Menezes, Paul C. van Oorschot y Scott Vanstone, Handbook of Applied Cryptography, CRC Press, Nueva York, 1997.
[8] Brian Chess y Brad Arkin The Case for Mobile Two-Factor Authentication, IEEE Security &Privacy, volúmen: 9, páginas: 81-85, 2011.
[9] Fadi Aloul, Syed Zahidi, Wassim El-Hajj Two Factor Authentication using Mobile Phones, International Conference on Computer Systems and Applications, páginas: 641-644, 2009.
[10] Daesung Moon, Sungju Lee, Seunghwan Jung, Yongwha Chung, Mutual Authentication using Fuzzy Fingerprint Vault, International Conference on Computational Intelligence and Security, páginas: 878–881, 2006.
[11] Esla Timothy Anzaku, Hosik Sohn, Yong Man Ro., Multi-Facto authentication Using Fingerprints and User-Specific Random Projection 12th International Asia-Pacific Web Conference, 2010.

Instrucciones para los autores

Los artículos que se someten a **RISCE** deben contener resultados inéditos y originales, no haber sido publicados con anterioridad ni haber sido sometidos simultáneamente a otra revista científica. Si el artículo ha sido presentado, sometido o publicado en alguna otra parte, deberá informarse al coordinador editorial. Los artículos deben ajustarse a las siguientes especificaciones:

- Idioma Inglés (anexar un resumen y palabras clave en español)
- Idioma Español (anexar un resumen y palabras clave en Inglés)
- Procesador de texto admitido: MS-Word.
- Tamaño de página: carta , utilizar un solo lado de la hoja. Máximo 10 páginas.
- Márgenes: izquierdo 2.5 cm y derecho 2 cm., superior 2.5 cm e inferior 2.5 cm.
- Autores: primer nombre seguido de los dos apellidos (sin abreviaturas), abajo: afiliación y e-mail.
- Tipo de letra del texto regular: Times o Times New Roman de 10 pt (título original 22 pt; secciones 11.5 pt, subsecciones 11.5 pt, en negritas).
- Texto: a una columna y con espaciado sencillo (renglón seguido).
- Resumen/Abstract: entre 70 y 150 palabras, colocado al principio del texto, seguido del de Español o inglés según sea el caso.
- Palabras clave/Keywords: colocadas después del resumen en negritas, y no más de 10.
- Imágenes y fotografías: deben ser de alta calidad, con colores bien definidos y contrastantes, en mapa de bits (no sectorizadas) en formato JPG e incrustadas en el texto de forma que se puedan manipular independiente.
- Fórmulas: Deberán de presentarse en formato de tabla sin bordes, centradas y la numeración de c/u justificada a la derecha con negritas en mapa de bits, no vectorizadas.
- Pies de figura. Deben mencionarse dentro del texto y numerarse de manera consecutiva con un tipo de letra Times New Roman 9 puntos
- Cabecera de tabla. Deberá presentase en la parte superior de la tabla un numeración consecutiva y descripción con tipo de letra Times New Roman 9
- Referencias:

En cualquier caso el nombre del autor del artículo o publicación web deberá mostrarse al principio. Deberán ordenarse conforme aparezcan dentro del texto encerradas entre paréntesis cuadrado —[ ]‖. A continuación algunos ejemplos:

[1]. Baldonado, M., Chang, C.-C.K., Gravano, L., Paepcke, A.: The Stanford Digital Library Metadata Architecture. Int. J. Digit. Libr. 1 (1997) 108–121

[2+. Bruce, K.B., Cardelli, L., Pierce, B.C.: Comparing Object Encodings. In: Abadi, M., Ito, T. (eds.): Theoretical Aspects of Computer Software. Lecture Notes in Computer Science, Vol. 1281. Springer-Verlag, Berlin Heidelberg New York (1997) 415–438

[3]. van Leeuwen, J. (ed.): Computer Science Today. Recent Trends and Developments. Lecture Notes in Computer Science, Vol. 1000. Springer-Verlag, Berlin Heidelberg New York (1995)

[4]. Michalewicz, Z.: Genetic Algorithms + Data Structures = Evolution Programs. 3rd edn. Springer-Verlag, Berlin Heidelberg New York (1996)

Instrucciones:

Enviar el archivo en extenso a la siguiente dirección electrónica: ebustosf@gmail.com

Los revisores técnicos le harán llegar sus observaciones y modificaciones, las cuales deberá realizar y reenviar el archivo corregido al correo arriba mencionado.

El comité editorial se comunicara mediante correo electrónico indicándole la aceptación o rechazo del artículo.

Se le solicitará autorización para publicación; en caso de aceptar se le indica la cuenta donde debe hacer el depósito por cobro de publicación y el costo, el cual no debe exceder de $1000.00 pesos mexicanos.

Reserva de Derechos 04-2008-062613190500-203