RISCE Revista Internacional de Sistemas Computacionales y Electrónicos

Enero-Mayo 2014
Número 1, Volumen 1, Año 6

ESCOM

IPN

Alejandro

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos; es una publicación bimestral del 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 Computo; 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. Certificado de reserva de Derechos al uso Exclusivo del título No. 04-2008-062613190500-203, ISSN en trámite. Los artículos son responsabilidad exclusiva del autor y no reflejan necesariamente el criterio de la institución, a menos que se especifique lo contrario. Se autoriza la reproducción total o parcial, siempre y cuando se cite explícitamente la fuente.

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

M. EN C. FERNANDO ARELLANO CALDERÓN
SECRETARIO GENERAL

M. EN C. DAFFNY ROSADO MORENO
SECRETARIO ACADÉMICO

DR. PRIMO ALBERTO CALVA CHAVARRIA
SECRETARIO DE INVESTIGACIÓN Y POSGRADO

ING. MARÍA EUGENIA UGALDE MARTÍNEZ
SECRETARIO DE SERVICIOS EDUCATIVOS

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

C.P. JOSÉ JURADO BARRAGÁN
SECRETARIO DE GESTIÓN ESTRATÉGICA

M. EN C. DELY KAROLINA URBANO SÁNCHEZ
SECRETARIO DE ADMINISTRACIÓN

LIC. JUDITH CLAUDIA RODRIGUEZ ZUÑIGA
DEFENSORA DE DERECHOS POLITÉCNICOS

ESCUELA SUPERIOR DE CÓMPUTO

DR. FLAVIO ARTURO SÁNCHEZ GARFIAS
DIRECTOR

LIC. ANDRÉS ORTIGOZA CAMPOS
SUBDIRECTOR ACADÉMICO

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

M. EN C. KARINA VIVEROS VELA
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

Índice 5

Proyecto de aulas digitales para preescolar. El Caso de los CENDIS del IPN. 6

Sistema de sugerencia y monitoreo de rutas abordo de taxis a través de dispositivos móviles con sistema operativo Android. 13

Modelo y Arquitectura para Votación sobre Medios Móviles 21

Arquitectura de Seguridad basada en Identificación y Autentificación para Cómputo Móvil 29

Non-Saturation Throughput of S-ALOHA Using the Time-Scale Decomposition Technique 39

Instrucciones para los autores 45

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 1, Año 6. Enero–Mayo 2014
Artículos con arbitraje

Proyecto de aulas digitales para preescolar. El Caso de los CENDIS del IPN.

Claudia Marina Vicario Solórzano
IPN – UPIICSA
cvicario@ipn.mx

Chadwick Carreto Arellano
IPN – ESCOM
ccarretoa@ipn.mx

Eduardo Bustos Farías
IPN – ESCOM
ebustosf@ipn.mx

Aide Rojas Pech
IPN – ESCOM
aiderojas93@outlook.com

Resumen – En este artículo se describe el desarrollo del proyecto de equipamiento de aulas digitales para preescolar en tres de los Centros de Desarrollo Infantil del Instituto Politécnico Nacional tanto en programas (se desarrollaron 18 interactivos que cubren los programas de la SEP para Preescolar I, II y III, que van dirigidos a niños de 3 a 6 años), la puesta en marcha de un repositorio digital de estos objetos de aprendizaje, así como la compra de tabletas, kits robóticos y de electrónica. La metodología pedagógica empleada corresponde al construccionismo de Papert.

Palabras clave – Tecnología educativa, Aprendizaje electrónico, Objetos de aprendizaje, Preescolar

Abstract – This paper describes the development of project about equipment digital classrooms for Preschool in three of the Pre-K Schools of the *Instituto Politécnico Nacional* in both software (18 interactive covering programs SEP Preschool I, II and III were developed described which are aimed at children aged 3-6 years), the launch of a digital repository of learning objects, as well as purchase of tablets, robotics and electronics kits. The pedagogical methodology corresponds constructionism of Papert.

Keywords – Educational technology, Electronic learning, learning objects, Preschool.

I. INTRODUCCIÓN

La increíble facilidad con la que los niños pequeños utilizan las nuevas tecnologías, como las tabletas y teléfonos inteligentes, de manera casi intuitiva deja sorprendidos a la mayoría de la gente, sobre todo a los que difícilmente pueden realizar una simple tarea, como mandar un correo electrónico o realizar una llamada, con este tipo de dispositivos.

Aprovechando esta habilidad innata en los niños, el Proyecto Horizon plantea que el uso de estas nuevas tecnologías puede ser de gran utilidad en la formación de nuevas estrategias y métodos en la generación de conocimiento, de enseñanza y aprendizaje. El Proyecto Horizon fue lanzado en 2002 como una iniciativa del New Media Consurtium (NMC) con el objetivo de ayudar a los educadores y líderes de opinión en la reflexión sobre el potencial de las tecnologías emergentes para la mejora de la educación.

II. MARCO CONTEXTUAL

En 2012, el CEO del NCM, Laurence F. Johnson, publicó en su informe anual información detallada sobre las nuevas tendencias del uso de la tecnología. Entre varias ideas que fueron presentadas en dicho

informe, se puede resaltar la siguiente: "La tecnología se ha convertido un medio para capacitar a los estudiantes un método para comunicarse y relacionarse con los demás, y es una parte ubicua y transparente de su vida". De esta idea, diferentes proyectos a lo largo de todo el mundo, se han dado la tarea de que los alumnos y docentes incorporen las Tecnologías de la Información– Conocimiento y Comunicación (TICC) en el proceso de la generación de conocimiento en los diferentes niveles educativos.

El Instituto Politécnico Nacional (IPN) no es indiferente a los cambios que se presentan en la forma en la que se desarrollan los procesos de aprendizaje en las escuelas, en los rápidos avances tecnológicos y en la necesidad de que el alumno sea autodidacta, por lo que desde enero de 2013 varios docentes que laboran en la Escuela Superior de Cómputo (ESCOM) y en la Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas (UPIICSA) en conjunto con la Asociación Mexicana para la Innovación en Tecnología Educativa A.C. (AMITE) realizan un proyecto de investigación, que lleva el nombre de "Portal de Recursos de Apoyo para Aulas Digitales de Preescolar," con el que pretenden realizar un diagnóstico de las necesidades en la infraestructura de las aulas y en la capacitación del personal docente para implementar interactivos educativos en tabletas, como un apoyo en el aprendizaje de los niños, a través de un repositorio digital y el equipamiento de los laboratorios de cómputo de los CENDIS que pertenecen al IPN.

El IPN cuenta con cinco Centros de Desarrollo Infantil (CENDI) ubicados en diferentes zonas del Distrito Federal, los cuales tienen el objetivo de proveer al niño de las condiciones necesarias para su desarrollo integral y adaptación al ambiente familiar, escolar y social mediante la formación de hábitos y actitudes deseables que lo habiliten como un ser seguro de sí mismo, para lograr que las madres trabajadoras desempeñen los labores propias del puesto asignado con la tranquilidad de que su hijo este en el lugar adecuado.

Hasta el momento no se ha documentado algún proyecto que plante alguna experiencia en el uso de dispositivos electrónicos como las tabletas para apoyar al proceso de aprendizaje en los niveles de inicial y preescolar en el sector de educación pública, que son los niveles abarcados por las instituciones educativas de los CENDI. El proyecto se enfocó a estos niveles de educación básica ya que en consideración de los colaboradores del proyecto es de los niveles menos atendidos, tanto a nivel nacional como dentro del IPN. Una prueba de ello, es que apenas en el 2004 se hizo una Reforma a la Educación Preescolar en la que se hizo obligatorio que los niños cursaran el tercer y último año de preescolar antes de ingresar al nivel de educación primaria y se presentaron las prácticas educativas que conformarían al programa educativo que rige este nivel educativo. En 2008 se hace obligatorio el primer año, formando parte de la educación básica en México.

III. MARCO TEÓRICO

En la actualidad existen ya varios recursos tecnológicos que ayudan a complementar la educación de los alumnos. Sin embargo, no existe una propuesta parecida a la presentada en el proyecto del IPN en colaboración con la AMITE para preescolar, puesto que otros recursos utilizan tecnología, que aún puede considerarse como tal, son ya atrasadas y no consideran la tendencia actual de las superficies interactivas, como las tabletas.

El hacer uso de las tabletas por encima de otras tecnologías, fue gracias a la extraordinaria habilidad

que tienen los niños en aprender a usarlas, en lo fácil que son de manejar, tanto para docentes como para el alumnado, y en la posibilidad que los niños tiene de poder hacer uso de la aplicación educativa desde su hogar. Además de las cualidades que se presentaron en el informe de 2012 del Proyecto Horizon:

"Las tabletas constituyen herramientas ideales para compartir contenido textual, videos, imágenes y presentaciones porque son más fáciles de utilizar. El acceso a diversidad de formatos, así como la posibilidad de producir materiales multimedia en red por parte de profesores y alumnos favorece el aprendizaje transversal de competencias digitales básicas. Las tabletas son un medio útil para fomentar el aprendizaje más allá de tiempos y espacios de clase".

Como ya se había mencionado, no se ha documentado el uso de tabletas como herramientas para la enseñanza y el aprendizaje en escuelas públicas, pertenecientes al sistema educativo mexicano, sin embargo, si se ha encontrado documentación al respecto de proyectos similares en otros países.

Uno de ellos, con el título de "Experiencia en la Escuela de Posgrado de la Universidad Peruana de Ciencias Aplicadas (UPC)" hace uso de las tabletas para sustituir el material impreso de los cursos y además incluir herramientas para la creación de escenarios de enseñanza– aprendizaje que creen nuevas formas de interacción entre el alumno y el profesor. Se diferencia con el proyecto IPN–AMITE en, además de enfocarse a diferentes niveles educativos, que el proyecto de la UPC hace uso de las tabletas para el acceso de materiales digitalizados y en el proyecto que se presenta en este artículo, tiene como propuesta el desarrollo de contenidos interactivos con los cuales el alumno pueda trabajar.

Otro ejemplo, es el proyecto realizado por la Universidad O'Higgins de Chile, nombrado como "UBOPad: Uso de Tablet en Apoyo a la Gestión Docente en el Aula", el cual se generó por la necesidad de llegar una mejor gestión de la información generada en el aula, como los estados de avance del programa en una asignatura, registro formal de actividades entre otros elementos asociados al desarrollo de la cátedra. El sistema UBOPad, permite llevar el control de asistencia, notas y temarios. Además, se encuentran conectados con un procedimiento central que lleva el control de los puntos antes señalados. Este proyecto se semeja con al Proyecto de los CENDIS del IPN en la forma de realización, puesto que en ambos proyectos se realizaron encuestas a los docentes para conocer su nivel de manejo y conocimiento de las TICC y las aplicaciones que fueron instaladas en las tabletas fueron desarrolladas por colaboradores de los mismos proyectos.

Pero sin duda el proyecto más novedoso y ambicioso, es el de las "Steve Jobs Schools" (Escuelas Steve Jobs) en Holanda. Sin duda, es una propuesta que cambia totalmente la forma de dar y tomar clases a nivel primaria. Todo se centraliza en el uso de las tabletas "iPad", de la marca Apple, para que los niños realicen todas sus actividades, desde llevar una agenda con las actividades que deben realizar en el día hasta trabajar en proyectos de clase de manera conjunta con otros alumnos y comunicarse con éstos en todo momento. El profesor toma el papel de entrenador (guía) en el proceso de aprendizaje de los alumnos dejándoles diferentes actividades que deberán ser realizadas en diferentes espacios dentro de la escuela, aportando información o ligas a contenido audiovisual interesante y útil en la red, así como llevar un seguimiento al progreso de los alumnos. Todas estas actividades se realizan

mediante diferentes aplicaciones que los niños, docentes y padres de familia instalan en sus tabletas.

IV. ESTRATEGIA METODOLÓGICA

Dejando atrás algunos de los proyectos que fueron tomados como referencia para el proyecto "Portal de Recurso de Apoyo para Aulas Digitales de Preescolar" elaborado por el IPN en colaboración con la AMITE, que es en el que se concentra el presente artículo, se describirá a continuación la estrategia metodológica que se empleó en la realización de dicho proyecto.

Primera Etapa: Organización del Equipo de Trabajo.

El equipo de trabajo se dividió en dos comisiones: la comisión pedagógica–estratégica y la comisión técnica. La primera se encargó de la interacción entre los CENDI y los investigadores para formular los aspectos a estudiar dentro de los planteles y así identificar los aspectos de mayor importancia para el desarrollo del estudio. De igual manera, fueron los encargados de la aplicación de encuestas con el fin de recolectar los datos necesarios para el análisis de las tecnologías y servicios informáticos disponibles en cada uno de los CENDI, de los recursos y modelos educativos que deberían de ocuparse, así como de la gestión de los recursos en los CENDI.

La comisión técnica se enfocó en la realización de la investigación de la información relativa a la infraestructura física de los CENDI para la instalación del nuevo hardware; a las características del hardware y software con el que se trabajará para el cumplimiento de los objetivos del proyecto y de las tecnologías alternas que permitan el cumplimiento de los mismos, mediante un monitoreo tecnológico. De igual forma, tuvieron la tarea llevar a cabo los acuerdos necesarios con la AMITE y los proveedores de la tabletas para revisar las posibilidades de transferencia tecnológica. Por otra parte, les fue delegado el labor de desarrollar el software necesario para los interactivos, el diseño del portal que se ocuparía como un repositorio de los interactivos y la implementación de los mismos en las tabletas y, además de poner en marcha dicho portal.

Segunda Etapa: Contacto con COCENDI y los CENDI.

En esta etapa del proyecto, algunos integrantes de la comisión pedagógica–estratégica contactaron a las autoridades de COCENDI para desarrollar el diagnóstico y la visita a los CENDI, con el propósito de dar a conocer las intenciones del estudio, los beneficios del mismo para los planteles, y obtener las facilidades para la recolección de los datos necesarios para los análisis descritos en la primera etapa, detallando el procedimiento para recabar dicha información.

Tercera Etapa: Generación de las Variables a Investigar.

La actividad de definir las variables a investigar fue desarrollada por la Dra. Claudia Marina Vicario Solórzano, consejera de la AMITE, quién decidió que la variables serían: la información general de las profesoras y directoras de los CENDI, que serían diferentes datos como su nombre, el puesto y las actividades que desempeñan, la antigüedad que tienen, entre otros; las tecnologías y servicios informáticos disponibles en los CENDI, tomando en cuenta el equipo informático con el que cuentan, su conectividad, seguridad y soporte, además de las opiniones de que tienen las profesoras acerca del equipo y servicios informáticos con los que se cuentan.

Otra de las variables es la infraestructura física, que incluye aspectos relacionados con el espacio físico, el mobiliario y las instalaciones donde se localizan los recursos informáticos que son utilizados para como apoyo para el aprendizaje de los niños. Por otra parte se deben investigar los modelos y recursos educativos basados en las TICC con las que cuenta el plantel, así como la articulación de las actividades diaria de los niños y los elementos de la Reforma Pedagógica de la Educación Preescolar y del Modelo Educativo Politécnico que se toman en las actividades basadas en las TICC.

Un concepto importante a considerar en la investigación es la cibercultura, la cual se refiere a la facilidad con la que los integrantes de una comunidad manejan las TICC, que se comuniquen de forma rápida y efectiva, y de igual manera, éstos colaboren activamente en proyectos conjuntos que generan conocimiento y bienestar a todos.

Por último, se debe investigar la gestión que se tiene en la adquisición de recursos y su procedimiento, así como las opiniones que tienen las profesoras acerca de las debilidades, fortaleza y oportunidades que se presentan en el CENDI en el que laboran.

Cuarta Etapa: Aplicación de las Encuestas.

Se visitó cada una de las escuelas de tal forma que la aplicación de los cuestionarios no interfiriera con las actividades académicas de las profesoras y directoras de los CENDI.

Con el análisis de la información que se recolectó de cada CENDI se pudo identificar las necesidades de los mismos respecto a servicios tecnológicos, equipamiento y capacitación.

Se pudo identificar que las profesoras no cuentan con los conocimientos necesarios para la enseñanza de la computación, que los programas y actividades que desarrollan los niños están desactualizados y no tienen la suficiente variedad para el aprendizaje de la computación, que no existe un acceso Internet en las computadoras que están destinadas al uso por parte de los alumnos y que todos los planteles carecen de la infraestructura adecuada para el equipo de cómputo, al mismo tiempo que éste es obsoleto por el software y hardware que lo componen. Además de que no hay capacitación para las profesoras y que ellas mismas consideran que los niños requieren de un nivel más elevado de enseñanza en computación para responder a las necesidades actuales, por fortuna, también expresan que tienen el interés de desarrollar una nueva forma de aprendizaje y apoyar la iniciativa en todo lo que esté a su alcance.

Con el análisis realizado de las necesidades de los CENDI, se llegó a la conclusión que además de los interactivos y sus respectivos guiones, es necesaria dar una capacitación acerca de las tecnologías con las que estarán en contacto alumnos, profesores y padres de familia. Adicionalmente se requiere fomentar, sobre todo en los padres de familia, una conciencia acerca de que el uso de las TICC favorece una enseñanza que fomenta el desarrollo de las competencias requeridas por la actual Sociedad del Conocimiento en la que vivimos.

Quinta Etapa: Elaboración de los Guiones Didácticos.

En esta etapa se elaboraron los guiones didácticos con la ayuda de expertos de la Sociedad Mexicana de Computación en la Educación (SOMECE). Dichos guiones ayudaron a la construcción de los interactivos para cada uno de los niveles de preescolar (I, II, III) cubriendo las competencias y campos formativos que se requieren, siendo éstos últimos acerca de: el desarrollo personal y social, el pensamiento matemático, exploración y conocimiento del mundo, apreciación artística, el

desarrollo físico y salud, y el lenguaje y comunicación.

Sexta Etapa: Elaboración de los interactivos.

La creación de los interactivos (que contienen recursos multimedia) estuvo a cargo de la AMITE con ayuda de alumnos becarios de la ESCOM. Se utilizó el Proyecto Descartes desarrollado por el Dr. José Luis Abreu (UNAM) para el proyecto LITE - CONNACYT 2013 (Laboratorio de Innovación en Tecnología Educativa).

Séptima Etapa: Elaboración de las Guías para el Profesor.

La elaboración de las guías para el profesor estuvo designada a la comisión pedagógica. Estas guías tienen el objetivo de explicar el funcionamiento de los interactivos para así hacer un uso correcto de los mismos.

Octava Etapa: Construcción del Portal.

El portal o repositorio, fue construido por colaboradores del proyecto por parte de la ESCOM. Dicho portal será un sitio web que podrá ser desplegado tanto en las tabletas como en cualquier PC. Además, en el repositorio se podrá desplegar una sección con los interactivos y sus funcionalidades, habrá un área de ayuda y otra que tendrá la función de ser como un portafolio de evidencias

Novena Etapa: Procedimiento de Compra del Equipo de Cómputo.

Se visitaron diferentes proveedores de tabletas, como Samsung y Microsoft, dónde se realizaron pruebas de la calidad de los productos, en cuanto a rendimiento y precio.

De igual forma se planea complementar el equipo de cómputo de las aulas digitales de los CENDI, con el material didáctico cómo Kits de robóticos y kits de electrónica

Etapa Actual del Proyecto.

Actualmente los colaboradores del proyecto están en espera de que el Fideicomiso del IPN compre los materiales solicitados y sean entregados a cada uno de los CENDI. Además, está en proceso el registro de derechos de autor para el IPN.

Trabajo a Futuro.

Lo que haría falta de realizar para cumplir los objetivos del proyecto sería: llevar a cabo la capacitación para profesoras y padres de familia sobre el uso de los materiales desarrollados, la entrega del reporte final para la AMITE y la aplicación de cuestionarios de satisfacción de los usuarios y de control de calidad.

V. CONCLUSIONES

Como conclusión del proyecto se puede comentar que se logró el diseño de recursos digitales para el nivel preescolar, la producción de los mismos con el apoyo del Laboratorio de Innovación en Tecnología Educativa (LITE) del DF y su disponibilidad a través de un portal. El total es de 18 interactivos de apoyo a 6 campos formativos orientados a los tres niveles de preescolar.

VI. AGRADECIMIENTOS

Este proyecto fue desarrollado con el financiamiento del Proyecto de Aulas Digitales para Preescolar entre la AMITE (Asociación Mexicana para la Innovación en Tecnología Educativa) y la Escuela Superior de Cómputo del Instituto Politécnico Nacional denominado Portal de Recursos de Apoyo para Aulas Digitales de Preescolar (E-KONETL

TAMACHTILKALI), así como los Proyectos financiados por la Secretaría de Investigación y Posgrado SIP 20130176 "Portal de Recursos de Apoyo para Aulas Digitales de Preescolar (E-KONETL TAMACHTILKALI)" y el SIP 20144081 "Un modelo de intervención basado en aprendizaje colaborativo apoyado en cómputo móvil en los CENDIS del IPN".

VII. BIBLIOGRAFÍA

Eléspuru, L., Dibós M., y Nazario J. "Gestión de contenidos a través de tabletas en los programas de postgrado: Experiencia en la Escuela de Postgrado de la Universidad Peruana de Ciencias Aplicadas (UPC)". Consulted in May 2014 at: http://www.altamira-peru.org/documentos/ponenciasv/LElespuru.pdf

Proyecto Horizon 2012. "Perspectivas tecnológicas: educación superior en Iberoamérica 2012-2017. Un Análisis Regional del Informe Horizon del NMC y la UOC". Consulted in May 2014 at: http://www.nmc.org/pdf/2012-technology-outlook-iberoamerica_SP.pdf

Silva, H. y Collao C., Ponencia UBOPad: "Uso de tablet en apoyo a la gestión docente en el aula". Chile: Universidad Bernardo O'Higgins, 2012.

Vicario, M. "Construccionismo. Referente sociotecmopedagógico para la era digital", Innovación Educativa, Vol.9, Número 47, México: IPN, 2009.

Steve Jobs School, 2013. "Portal Oficial de las Escuelas Steve Jobs". Consulted in May 2014 at: http://www.educationforanewera.com/#intro

VIII. AUTORES

Aide Rojas Pech
Estudiante de la carrera de Ingeniería en Sistemas Computacionales en la ESCOM IPN, becaria del sistema BEIFI 2014.

Claudia Marina Vicario Solórzano.
Doctorada en Pedagogía, directora fundadora del Centro de Formación e Innovación Educativa del IPN, profesora investigadora adscrita a la UPIICSA IPN

Chadwick Carreto Arellano.
Profesor –Investigador de la ESCOM - IPN, sus áreas de interés son: Comunicaciones Inalámbricas, Cómputo ubicuo, Cómputo Educativo, Seguridad Computacional.

Eduardo Bustos Farías.
Doctor en Ciencias Administrativas, Jefe del Departamento de Investigación de la ESCOM IPN.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 1, Año 6. Enero–Mayo 2014
Artículos con arbitraje

Sistema de sugerencia y monitoreo de rutas abordo de taxis a través de dispositivos móviles con sistema operativo Android.

Jiménez López Carlos Adrian
IPN – ESCOM
cjimenezl1001@alumno.ipn.mx

Negrete Juárez Francisco Javier
IPN – ESCOM
fjj.negrete@gmail.com

Euler Hernández Contreras
IPN – ESCOM
eulerconther@yahoo.com.mx

Jorge Cortés Galicia
IPN – ESCOM
jcortesg@ipn.mx

Resumen – En el presente TT se desarrollará una aplicación móvil, que servirá de apoyo a los usuarios que utilicen el transporte público tipo taxi, permitiéndoles por medio del escaneo de un código QR saber los datos correspondientes a la unidad. Además haciendo uso de la tecnología GPS, se le dará seguimiento al recorrido del usuario. La aplicación contará con la opción de sugerir rutas para el viaje, la cual puede ser utilizada u omitida; además de monitorear, se verificará que el taxi siga con la ruta planeada en caso contrario se le notificará esta situación al usuario. Si en algún momento el usuario se siente en peligro, la aplicación podría mandar una alerta, la cual contiene su posición inicial (dónde abordó el taxi), su posición actual, el historial del recorrido hasta ese momento y los datos del taxi.

Palabras clave – Alerta, Android, Aplicación Móvil, GPS, Sugerencia De Ruta, Transporte Público Tipo Taxi.

Abstract – At the present terminal work is going to be developed a mobile application, which will support users who use public transport type taxi, it will let them know taxi unit's data by means of the scanner of a QR code. Besides making use of GPS technology, it will be followed the user path. The application will have the option to suggest routes for travel, the route can be used or omitted; addition to monitoring, shall be ensured that the taxi follow the planned route otherwise this situation will be notified to the user. If at any time the user feels in danger, the application might send an alert, which contains the initial position (where the taxi was approached), her/his current location, travel history so far and taxi data.

Keywords – Alert, Radar applications, Cellular phones, transport.

I. Introducción

En la ciudad de México cada día más de seis millones de personas hacen uso de los servicios del transporte público, dentro del cual hay 130 mil taxis a disposición, lo cuales son operados por 190 mil conductores (debido a que una unidad puede tener

dos choferes), que poseen la licencia tarjetón tipo B1 para operar en sitios y bases autorizados. [1]

Del 2006 al 2010 se registró un incremento del 139% en el número de asaltos a bordo de taxis que se denunciaron, pues pasaron de 772 a 1850.

En 2010 se registraron 1850 víctimas de la delincuencia en este sistema de transporte [2], mientras que en 2011 bajo a 1038 víctimas [3], finalmente en el año más reciente la cifra es de 640 víctimas con violencia más otras 96 sin violencia, dando un total de 736 víctimas durante el 2012 [4]. Esto de acuerdo a los datos de los informes de la Procuraduría General de Justicia del Distrito Federal.

El asalto en taxis con violencia representa el 0.36% de los delitos del fuero común que se cometieron en la ciudad en 2012, por lo que las autoridades lo consideran de "alto impacto social" porque afecta los bienes patrimoniales de las personas, mientras que el robo sin violencia representa el 0.06% y es considerado de "bajo impacto social". [4]

En 2010 *"las delegaciones Cuauhtémoc, Benito Juárez, Miguel Hidalgo y Gustavo A. Madero concentraron 66% de asaltos a bordo de taxis, lo cual se debe, explicó Gamaliel Martínez, director general de Políticas y Estadística Criminal de la PGJDF, a que en ahí se concentra una gran cantidad de población flotante, es decir, por el número de personas y actividades que se llevan a cabo.*

En contraste, Magdalena Contreras, Cuajimalpa, Tláhuac y Milpa Alta, concentraron sólo 2% de asaltos". [5]

Actualmente las delegaciones que tienen el número más alto de delitos de alto y bajo impacto social son Cuauhtémoc, Iztapalapa y Gustavo A. Madero con 29057, 28816 y 20510 respectivamente. [4]

"Datos de la PGJDF revelan que el 98% de robos ocurre cuando la persona viaja sola. El 58% son mujeres, 40% son hombres y sólo en 2% de los casos viajaban más de dos personas.

Las estadísticas de 2010 señalan que los atracos son menos violentos, pues las denuncias muestran que sólo 5% de los casos hubo agresiones físicas y en 2% hubo agresión de tipo sexual.

En 58% de los asaltos participaron dos personas adicionales al chofer, lo que explica Gamaliel Martínez, que se trata de bandas delictivas.

De acuerdo con la Secretaría de Seguridad Pública, los días martes y viernes de las 18:00 horas a la medianoche ocurre la mayor incidencia de robos".[5]

Algunas de las acciones tomadas por el gobierno del Distrito Federal para combatir este tipo de delitos son la regularización del padrón y la portación de los tarjetones [5], además de que tres mil taxistas portarán una calcomanía con los teléfonos 066 y 01 800 00 PGJDF (74533) para que usuarios denuncien si se llegase a suceder algún ilícito en la unidad. [1]

II. METODOLOGÍA

El sistema Taxi Tracking está constituido por 8 módulos de los cuales 3 realizan la mayoría de la funcionalidad: Implementación del código QR, Rutas y el módulo de Estimación de Distancia y Costo.

El módulo de la implementación del código QR abarca básicamente la generación, lectura (que se hace a través de la cámara del dispositivo móvil) y

[1] La licencia tarjetón tipo B, es un tipo de permiso solicitado para poder manejar un taxi, y así poder ser registrado. Se podrá obtener con vigencia de 2 y 3 años. Su costo es de $778 por 2 años y $1170 por 3 años.

procesamiento de un código QR. A continuación damos una explicación de lo que es esta tecnología y la manera en que se ocupó.

Código QR

Un código QR es un módulo para almacenar información en una matriz de puntos o un código bidimensional creado por la compañía japonesa Denso Wave, en 1994. Se caracteriza por los tres cuadrados que se encuentran en las esquinas y que permiten detectar la posición del código al lector. La sigla «QR» se deriva de la frase inglesa *Quick Response* (Respuesta Rápida en español).

El código QR (ver figura 1) es capaz de manejar todo tipo de datos, como los caracteres numéricos y alfabéticos, kanji, kana, hiragana, símbolos binarios y códigos de control. Hasta 7089 caracteres se pueden codificar en un símbolo. Nuestro sistema guardará únicamente información alfanumérica en el código, ésta será: la clave única del operador.

El código QR es omnidireccional y de lectura de alta velocidad. El código QR lleva a cabo esta tarea a través de los patrones de detección de posición situados en las tres esquinas del símbolo. Estos patrones de detección de posición garantizan una lectura estable, evitando los efectos negativos de la interferencia de fondo. [6]

Figura 1. Código QR.

El módulo de rutas se encarga de cómo su nombre lo dice la "gestión" de rutas, es decir, sugerir y monitorear las rutas que el usuario recorre. Complementando este módulo, tenemos el módulo de estimación de costo y distancia que se encarga de simular un taxímetro virtual dentro de la aplicación móvil. Ambos módulos ocupan la tecnología GPS junto con las Apis de google para su funcionamiento. A continuación se habla sobre estas tecnologías y se describe el funcionamiento de un taxímetro normal y nuestro taxímetro virtual.

Sistema de posicionamiento global (GPS)

La implementación del programa NAVSTAR, GPS (*Navigation System Timing And Ranging, Global Positioning System*) fue efectivamente iniciada en diciembre de 1973. El 22 de febrero de 1978 fue lanzado el primer satélite de una serie de cuatro.

La responsabilidad del desarrollo y mantenimiento del sistema recae en el Departamento de Defensa de los Estados Unidos, División Sistema Espacial. Esa dependencia se debía a que el sistema fue concebido, igual que **Transit**, para uso militar.

GPS es un sistema que tiene como objetivo la determinación de las coordenadas espaciales de puntos respecto de un sistema de referencia mundial. Los puntos pueden estar ubicados en cualquier lugar del planeta, pueden permanecer estáticos o en

movimiento y las observaciones pueden realizarse en cualquier momento del día.

Para la obtención de coordenadas el sistema se basa en la determinación simultánea de las distancias a cuatro satélites (como mínimo) de coordenadas conocidas. Estas distancias se obtienen a partir de las señales emitidas por los satélites, las que son recibidas por receptores especialmente diseñados. Las coordenadas de los satélites son provistas al receptor por el sistema. [7]

Bases de funcionamiento

Se sabe que la Tierra es un planeta de forma casi esférica que ha sido representado de muchas formas según distintos métodos cartográficos. De ellos, el más preciso es el modo esférico, ya que se ve a la tierra como una esfera perfecta lo que idealiza las condiciones en las que se realizan los cálculos matemáticos.

A partir de esta idea se divide la esfera en "gajos" basándose en circunferencias verticales denominadas meridianos, que pasan por los polos; y en discos horizontales, a partir de circunferencias paralelas al ecuador, denominadas paralelos. Dichas circunferencias permiten definir cualquier posición de un punto en la superficie terrestre a partir de su distancia angular al Meridiano Greenwich y al Ecuador.

Conociendo la latitud y longitud para dos puntos cualquiera del globo, podemos trazar la línea más corta que los une a través de la superficie del planeta y conocer nuestra referencia de posición.

La **Latitud** es la distancia que existe entre un punto cualquiera y el Ecuador, medida sobre el meridiano que pasa por dicho punto.

La **Longitud** es la distancia que existe entre un punto cualquiera y el Meridiano de Greenwich, medida sobre el paralelo que pasa por dicho punto (véase figura 2 [8]).

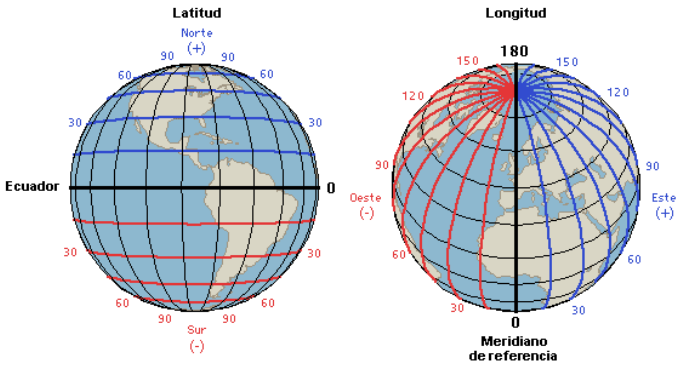


Figura 2. Longitud y latitud.

Sistema GPS - Constitución

Está constituido por tres segmentos fundamentales:

- Espacial
- De control
- Del usuario

Segmento espacial

Se puede observar en la figura 3 la disposición aproximada que tienen los satélites de la constelación NAVSTAR, GPS que integran el segmento espacial.

Debido a que la vida útil de un satélite llega a término por envejecimiento de los paneles solares, falta de capacidad de los acumuladores, averías no reversibles en los sistemas electrónicos o agotamiento del combustible de maniobra, se planificó su reemplazo en bloques [9].

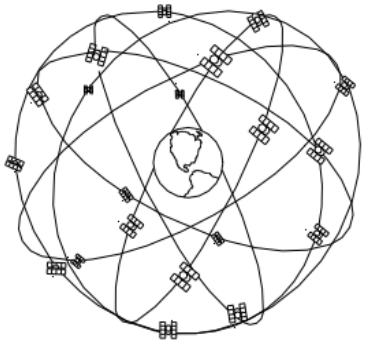


Figura 3. Segmentación espacial.

Segmento usuario

Está constituido por los instrumentos utilizados para recepcionar y procesar la señal emitida por los satélites.

Estos instrumentos están integrados esencialmente por una antena y un receptor. Un equipo complementario es usado, en ocasiones, para transferir datos entre receptores (ver figura 4).

Figura 4. Estaciones de control.

La **antena** está conectada por cable al receptor o en otros casos forman una sola unidad. Las coordenadas que se calculan corresponden al centro radioeléctrico de la antena.

El **receptor** consta de un mínimo de 4 canales (generalmente 10 ó 12) que permiten recepcionar y procesar simultáneamente la señal de cada satélite.

Posee además un oscilador de cuarzo que permite generar la frecuencia de referencia para realizar la observación.

Un **microprocesador** interno con el software correspondiente calcula las coordenadas de la antena y la velocidad y acimut si el aparato está en movimiento.

Posee además una memoria para almacenar observaciones. La capacidad de esta memoria varía de acuerdo al tipo de receptor, pudiendo llegar a almacenar información durante varias decenas de horas.

Todo equipo adiciona una unidad de alimentación eléctrica que deberá brindar al receptor la autonomía necesaria.

Los equipos están en continuo desarrollo y su evolución es comparable a la experimentada en informática durante las últimas décadas para los ordenadores personales. [7]

Google maps

Los servicios de cartografía de Google se han convertido en algunos de los más populares usados por los usuarios y desarrolladores para sus aplicaciones, uno de estos servicios es *Google Maps* (ver figura 5 [10]), el cual es un servidor de aplicaciones de mapas en la web.

Google Maps ofrece la visualización de los mapas a través de una vista alternativa vía satélite con imágenes de alta resolución (máxima ampliación) para la mayor parte del territorio de Canadá y Estados Unidos y en forma parcial para países como Francia, Irlanda, Italia, Irak, Japón, Bahamas,

Kuwait, México, Holanda, etc. Las imágenes que muestra Google Maps son tomadas vía satélite en su mayoría y otras son tomadas por aviones que vuelan alrededor de una altura de 10.000 metros.

Este servicio está desarrollado casi en su totalidad con Java Script y XML. Google Maps lanzó su API (*Application Programming Interface - Interfaz de Programación de Aplicaciones*) en Junio del 2005.

La API lanzada por Google Maps también hace posible la integración de este servicio en dispositivos móviles con sistema operativo **Android**. Una de las novedades que ofrece *Google Maps* en dispositivos móviles es la integración de *Google Places*. Para la versión 5.12, Google Maps logra disminuir el uso de memoria y la conexión a internet necesaria para garantizar un buen resultado en la aplicación. [10]

Figura 5. Google maps.

Funcionamiento Taxímetro "Normal"

Un taxímetro funciona a base del llamado Tacómetro (véase figura 6), el cual a su vez funciona detectando el movimiento de las llantas, dependiendo del modelo también puede llevar sus mediciones con cada "chispazo" producido por el motor. Es así que, con estos datos, el taxímetro opera aumentando una tarifa cada que el taxi recorre 250 metros o cuando pasan 45 segundos después del último aumento.

Figura 6. Tacómetro

Funcionamiento Taxímetro "Virtual"

El algoritmo del taxímetro funciona con datos del movimiento del taxi, es decir, cuando el dispositivo con la aplicación Taxi Tracking comienza a hacer el viaje éste actualiza su posición, por mínima que ésta sea. Al actualizar el primer punto acciona el cronómetro, y empieza el conteo del tiempo; es así que, una variable se actualiza cada 45000 milisegundos o cada 250 metros recorridos, esto lo hacemos posible gracias al evento "*requestlocationupdates*" el cual es un escuchador que se acciona dependido de los parámetros que se le envíen. Cada que se hace este evento el total se va actualizando: sumando la cantidad inicial conocida como "Banderazo" con la tarifa; cada que el evento es llamado suma una Bandera de cobro la cual va aumentando de uno en uno, y esto permite simular lo que hace el taxímetro para marcar el precio.

III. RESULTADOS

A continuación en las figuras 7, 8 y 9 mostraremos los resultados que dieron las pruebas de la aplicación **Taxi Tracking**, se muestra el reporte de la consola de las aplicaciones de Google, la cual utilizábamos para la implementación de los mapas.

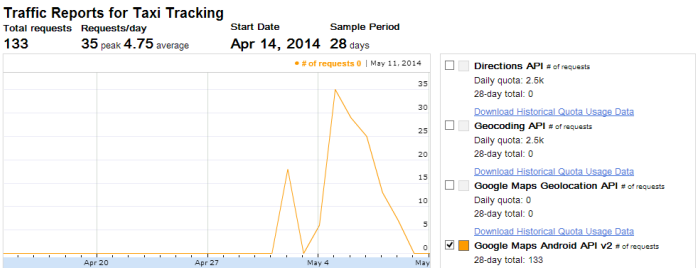


Figura 7. Reporte de tráfico

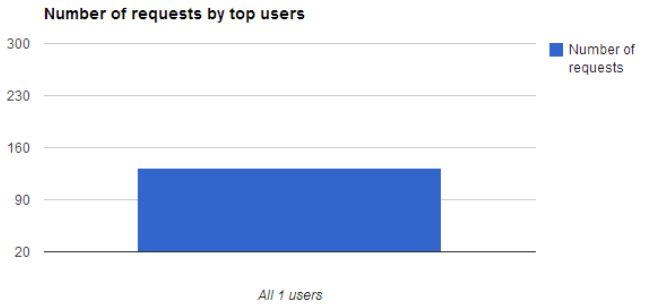


Figura 8. Peticiones

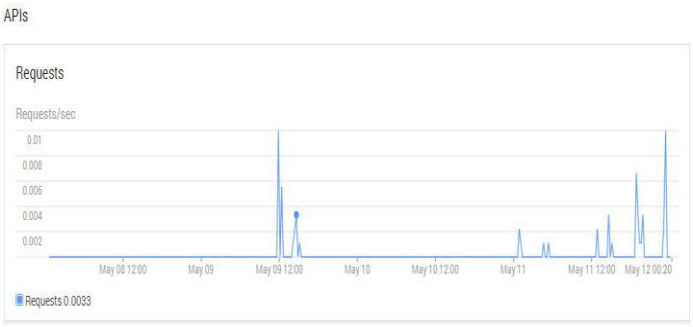


Figura 9. Gráfica peticiones

En la figura 10, observamos el reporte del tráfico de peticiones, que se generó a partir de las primeras pruebas de la API.

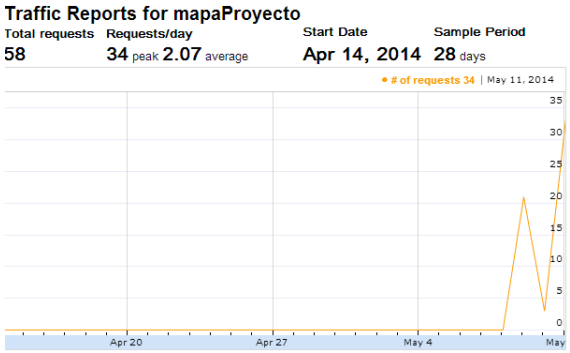


Figura 10. Reporte de tráfico de las primeras pruebas

IV. CONCLUSIONES

Taxi Tracking fue un proyecto que constó de dos partes, una parte web, la cual se trataba de la administración de información y peticiones, y una móvil, que era la que principalmente interactuaba con el usuario, y a partir de esto podemos decir que la interacción de la parte móvil con la parte web fue llevada a cabo de manera exitosa gracias a los distintos elementos en peticiones tipo JSON que se hacían entre cada una de ellas.

Después de haber realizado Taxi Tracking en su versión móvil, podemos concluir que el sistema operativo Android es muy "maleable", y las aplicaciones se pueden implementar de una manera muy práctica pues sus interfaces de desarrollo son muy cómodas y funcionales. Por otro lado, su arquitectura interna es muy especial, pues a pesar de que dicha arquitectura lo hace muy central, permite una gran compatibilidad con las aplicaciones que se desarrollan en él.

En Taxi Tracking también se utilizaron aplicaciones de Google debido a que los servidores de Google contienen las bases de datos Geoespaciales más completas que existen en la actualidad. El manejo de estas APIS fue muy importante al momento de crear mapas, trazar rutas e inclusive de obtener la dirección del usuario en el uso de botón de pánico.

El uso de la consola para acceder a los recursos es muy conveniente, pues además de proporcionar bitácoras con los reportes del uso de Taxi Tracking, éstas ayudaron a tener una visión más acertada y control sobre las pruebas que se realizaron.

Finalmente, y con base en el resultado de las encuestas, podemos concluir que el objetivo de desarrollar una aplicación para el uso seguro de taxis se cumplió, pues a pesar de que en un principio los usuarios tuvieron algunos problemas para el uso de la aplicación, al final de las pruebas expresaron que les parecía buena la aplicación y que fue una buena idea realizar su implementación.

V. RECONOCIMIENTOS

Los Autores agradecen a la Escuela Superior de Cómputo del Instituto Politécnico Nacional por el apoyo recibido y las facilidades otorgadas para el desarrollo del presente trabajo terminal.

VI. BIBLIOGRAFÍA

[1] C. Bolaños, "Taxistas prevendrán los delitos.," El Universal, vol. Metrópoli., 19 February 2011.

[2] Agencias del Ministerio Público (SAP - INCOL - SUI), «Informe Estadístico Delictivo en el Distrito Federal,» 2010.

[3] Agencias del Ministerio Público (SAP - INCOL - SUI), «Informe Estadístico Delictivo del Distrito Federal,» 2011.

[4] Agencias del Ministerio Público (SAP - INCOL - SUI), «Informe Estadístico Delictivo del Distrito Federal.,» 2012.

[5] H. De Mauleón and J. Robles, "Crecen 139% asaltos en taxis en cinco años.," El Universal, vol. Metrópoli., 02 March 2011.

[6] "DENSO WAVE INCORPORATED," [Online]. Available: http://www.qrcode.com/en/. [Accessed 12 September 2013].

[7] E. Huerta, A. Mangiatierra and G. Noguera, GPS Posicionamiento Satelital, Universidad Nacional de Rosario, 2005.

[8] "Latitud y Longitud," [Online]. Available: http://sistemaposicionamientogps.com/latitud-y-longitud/. [Accessed 12 September 2013].

[9] L. Letham, GPS made easy., Barcelona.: Paidotribo., 2001.

[10] Google, "Official Blog," [Online]. Available: http://googleblog.blogspot.mx/. [Accessed 10 September 2013].

VI. AUTORES

Euler Hernández Contreras

Egresado de la Licenciatura en Computación de la Universidad Autónoma del Estado de Hidalgo, con una especialidad en Ingeniería de Software y una primera maestría en Bases de Datos por la misma Universidad, tiene una segunda maestría por parte del CIC - IPN en Ciencias Computacionales. Ha sido Presidente de la Academia de Ingeniería de Software del Departamento de Ingeniería en Sistemas de la ESCOM-IPN; actualmente se desempeña como Jefe del Departamento de Posgrado de la SEPI ESCOM - IPN. Sus áreas de interés son los Sistemas de Bases de Datos, *Big Data y Bussiness Intelligence*.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 1, Año 6. Enero–Mayo 2014
Artículos con arbitraje

Modelo y Arquitectura para Votación sobre Medios Móviles

Sandra I. Bautista Rosales
IPN – ESCOM
sibauros@hotmail.com

Chadwick Carreto Arellano
IPN – ESCOM
ccarretoa@ipn.mx

Luis E. Hernández Olvera
IPN – ESCOM
luishernandez_2605@hotmail.com

Resumen – La democracia es un campo en el que el avance de la tecnología ha impactado a través de diversos medios electrónicos, convergiendo en lo que se ha denominado "voto electrónico". Existen países que han implementado este tipo de voto por medio de modelos de votación electrónica que se apegan a la legislación de cada uno de ellos y que consideran dispositivos especializados únicamente para la recepción del sufragio. Sin embargo, aunque ya existen muchos avances tecnológicos en la emisión y recepción del voto, aún no se ha considerado un modelo que pueda aplicarse a dispositivos móviles que le brinde a los electores la posibilidad de emitir su opinión desde cualquier lugar en el que se encuentren y con la certeza de que las garantías procedimentales y los principios del voto serán respetados.

Palabras clave – Voto electrónico, Seguridad, Autenticación, firma digital, dispositivos móviles.

Abstract – Democracy is a field in which the advancement of technology has impacted through various electronic media, converging in what has been called "electronic voting". There are countries that have implemented this type of vote by electronic voting models that adhere to the laws of each and consider specialized devices solely for the reception of suffrage. However, although there are many technological advances in the emission and reception of the vote, has not been considered a model that can be applied to mobile devices that gives voters the opportunity to express its view from wherever they are in and with the certainty that procedural safeguards and principles of the vote will be respected.

Keywords – Digital control, Information security, Authentication, Digital signatures, cell phone,

I. INTRODUCCIÓN

Con el avance de las nuevas tecnologías de la información y la comunicación, sobre todo el Internet, se ha potencializado el flujo de información a niveles impresionantes que ha llegado a producir cambios sociales.

Estos cambios han provocado que la democracia se transforme, los procesos electorales se envuelvan en el flujo de información y la toma de decisiones se facilite; y así todo concurre para considerar la inserción del voto electrónico [2].

Existen países que han ido introduciendo el voto electrónico en sus diferentes procesos electorales de acuerdo con diversos modelos de votación que se apegan al sistema político de cada uno de ellos. Sin embargo, todos estos modelos de votación incluyen dispositivos especializados en la recepción del voto y aún no se ha considerado optar por dispositivos propios de los usuarios, por ejemplo los dispositivos móviles, para emitir el sufragio.

Por otra parte, el avance continuo de los dispositivos móviles y su capacidad de conectividad con las redes inalámbricas les permite a los usuarios estar comunicados en cualquier momento y desde cualquier lugar; lo que nos lleva a uno de los principales retos que tiene que cumplir toda votación electrónica llevada a cabo por este medio, es decir, proveer seguridad al mandar datos por medio del aire, ya que es uno de los canales de propagación más inseguros para transmitir, por lo que es necesario hacer uso de modelos de seguridad adecuados para cubrir esta necesidad [10]. Esta es la razón por la que éste trabajo está enfocado en desarrollar un Modelo y una Arquitectura de Votación Electrónica Móvil el cual le permitirá al usuario emitir su voto por medio de un proceso de identificación y autentificación a través de su dispositivo móvil, desde cualquier lugar en el que se encuentre, siempre y cuando cuente con una conexión a Internet.

A continuación en la Sección II se brindará un marco teórico donde se abordarán algunos de los conceptos más importantes para el presente trabajo, así como los aspectos que involucra el voto electrónico; en la Sección III se plantea el problema en base a los antecedentes abordados en el marco teórico y se define la problemática a resolver; en la sección IV se describe el modelo propuesto para dar solución a la problemática planteada y finalmente en la sección V se presentan las conclusiones y el trabajo a futuro.

II. MARCO TEÓRICO

Siendo el voto la expresión pública o secreta de una preferencia ante una o más opciones [1], se puede decir que el voto electrónico (VE) tiene el mismo objetivo, con la excepción de que se emplean mecanismos electrónicos para realizarlo por lo que se pueden identificar dos aspectos del mismo [2]:

a) VE en *sentido amplio*: es todo mecanismo de elección en el que se utilicen los medios electrónicos o cualquier tecnología en las distintas etapas del proceso electoral, principalmente el acto efectivo de votar.

b) VE en *sentido estricto*: es el acto preciso en el que el emitente del voto deposita o expresa su voluntad a través de medios electrónicos (urnas electrónicas) o cualquier otra tecnología de recepción de sufragio.

Teniendo en cuenta esta clasificación, el presente trabajo considerará el voto electrónico en el sentido amplio, lo que lleva a definir algunos conceptos básicos para este aspecto.

Existen diversos sistemas de voto electrónico que actualmente ya son utilizados en diferentes países, principalmente los occidentales; de manera general se identifican tres tipos de sistemas principales y un cuarto [2] que va en proceso de adoptarse por ser más reciente. Los sistemas antes mencionados son:

1) Mediante tarjeta perforada. El elector recibe una tarjeta, en la cual debe perforar su opción por medio de un aparato. Este sistema es un tanto problemático, pues la precisión de la perforación depende del usuario y podrían no contarse adecuadamente la perforación de cada tarjeta. Este es un sistema obsoleto, pero aún lo continúan empleando.

2) Mediante un aparato lector. El votante realiza marcas con un bolígrafo en una papeleta, para que después éstas puedan ser introducidas en un aparato lector y se cuente el voto. El votante no entra en contacto directo con la tecnología, pero sí su papeleta.
3) Mediante aparatos de grabación directa. Usan aparatos similares a un cajero automático, el elector establece su preferencia por medio de una pantalla táctil o un teclado. Puede que el mismo aparato registre el voto o que el voto se grabe en un soporte externo. Tras emitir su voto, el votante utiliza su tarjeta a modo de una papeleta tradicional, introduciéndola en una urna, que a su vez será un aparato lector de tarjetas magnéticas, y que realizará el recuento.
4) Voto electrónico remoto. Es el que provee que el votante no deba desplazarse hasta el colegio electoral y pueda emitir su voto a través de la red (puede ser interna o desde cualquier plataforma conectada a Internet).

Será este último tipo de sistema el que se tome en cuenta para la propuesta del modelo de votación.

La ***seguridad*** en general, se refiere al cumplimiento de los servicios de seguridad que se listan a continuación [3]:

- **Confidencialidad.** Garantiza que la información privada pueda ser accedida únicamente por las entidades autorizadas.

- **Integridad de los datos**. Se refiere a la protección de los datos de tal manera que no puedan ser modificados, destruidos o extraviados de una manera maliciosa o accidental.

- **Autenticación**. Es un servicio relacionado con la identificación de identidades o de datos. La autenticación de una entidad es la confirmación de su identidad, es decir, una comprobación de que es quien dice ser. La autenticación de datos se refiere a la validez de los datos, lo que implica la integridad de los mismos.

- **No rechazo**. Asegura que el remitente de cierta información no pueda rechazar/negar su transmisión o contenido y que el receptor no pueda negar su recepción o contenido.

La ***firma digital*** es un esquema matemático que garantiza la privacidad de la conversación, la integridad de los datos, la autenticidad del mensaje/emisor digital y el no repudio del remitente [4]. También se puede decir que es un método criptográfico que asocia una identidad, ya sea de una persona en particular o de un equipo a un mensaje enviado a través de transmisión por la red.

La ***firma a ciegas*** es una clase de firma digital producida para mensajes que se mantienen ocultos para el signatario y por lo tanto una tercera entidad solicita la firma [5]. Este concepto fue introducido por Chaum con la finalidad de garantizar anonimato en los sistemas de pago electrónico [6], pero actualmente también se le ha dado uso en los sistemas de votación electrónica. Las firmas a ciegas requieren de dos entidades, el usuario quien solicita la firma y el signatario quien firma el mensaje.

De manera general, un sistema de votación electrónica por Internet debe cubrir con todos los requisitos funcionales del proceso electoral, así como los servicios de seguridad necesarios para protegerse de ataques potenciales provenientes de la red. Algunos de los requisitos esenciales son los siguientes [5]:

- *Autenticación*: sólo los votantes incluidos en el padrón electoral serán autorizados para emitir su voto.
- *Anonimato y no coerción*: nadie debe ser capaz de determinar el valor del voto ni de vincularlo con el votante.
- *Unicidad*: ningún votante debe votar más de una sola vez.
- *Verificación y auditoría*: debe ser posible verificar que al final del proceso electoral, todos los votos fueron contados correctamente.

Otros requisitos propuestos por [7] son:

- *Precisión*: Se debe evitar que el voto emitido sea alterado, duplicado o eliminado por cualquier persona. Cada voto legítimo debe ser contabilizado correctamente.

- *Simplicidad*: El proceso de votación debe ser lo más simple posible. En otras palabras, una interfaz de elección electrónica amigable al usuario y que no necesite aprender técnicas complejas y cualquier equipo adicional.

III. PLANTEAMIENTO DEL PROBLEMA

Los avances tecnológicos aunados a las técnicas criptográficas han sido un factor para la paulatina inserción del voto electrónico dentro de los sistemas tradicionales de sufragio. El Internet y diversos dispositivos electrónicos facilitan la captura, recepción y transmisión del voto, ofreciendo así un proceso más cómodo y eficiente para todos los participantes.

No obstante, el nuevo sistema de votación que se deriva del voto electrónico, es decir, el e-voting remoto acarrea también ciertos problemas o riesgos adicionales a los que ya existen en el sistema tradicional. Por ejemplo, la autenticación del usuario, ya que debe de ser identificado para tener los respectivos permisos para votar y a su vez guardar su anonimato al momento de emitir su voto.

Otro problema viene de considerar el Internet como el principal medio de transmisión, pues es necesario implementar los esquemas de seguridad para votaciones electrónicas que ofrezcan seguridad al sistema y confidencialidad a los votantes.

Ya que generalmente el voto es capturado electrónicamente y enviado a una urna electrónica para ser contabilizado al finalizar el periodo de votación, la auditoria se convierte en otro problema, ya que no hay una garantía de que esos votos que van siendo almacenados no sean alterados mientras finaliza la elección.

En la actualidad hay muchos protocolos y esquemas de votación electrónica que van de acuerdo a ciertos modelos de votación. Por ejemplo, "Un esquema verificable del voto electrónico por Internet" [7] proporciona un esbozo de cómo dar seguimiento al proceso de la votación, especificando 4 fases, a saber, fase de registro, autenticación, votación y conteo, además propone cinco entidades participantes: Votantes, Autoridad Certificadora, Centro de autenticación, Centro de supervisión y Centro de conteo, siendo la mayor aportación de este trabajo la verificabilidad.

Otro trabajo titulado "Un Protocolo Seguro de Voto Electrónico para las Elecciones Generales" [8] propone un centro de voto que está compuesto por cuatro pasos con los que navega a través de cinco módulos.

Un tercer protocolo es "Un Mecanismo de Votación Anónima basado en el Protocolo de Intercambio de Claves" [9], éste hace uso de la firma a ciegas y del protocolo de Diffie-Hellman para el intercambio de

llaves entre el votante autenticado y el servidor encargado de recibir el mensaje correspondiente al voto. Una de las desventajas de este protocolo es que no permite al votante verificar que su voto haya sido contado correctamente.

En la tabla I podemos observar la comparativa de las diferentes propuestas de modelos de votación

TABLA I.

TABLA I.
COMPARATIVA DE MODELOS DE VOTACIÓN ELECTRÓNICA

	Protocolos			
Requerimientos	**Protocolo de Liaw [8]**	**Protocolo de Chang-Lee [9]**	**Protocolo de Chun-Ta Li [7]**	**Modelo propuesto**
Precisión	✓	✓	✓	✓
Simplicidad	X	✓	✓	✓
Apegado a la Ley	✓	✓	✓	✓
Verificabilidad	✓	X	✓	✓
Privacidad	✓	✓	✓	✓
Esquema sobre Internet	✓	✓	✓	✓
Basado en redes inalámbricas	No especifica	No especifica	No especifica	✓
Contemplan dispositivos móviles	X	X	X	✓

IV. MODELO PROPUESTO

Con los modelos de votación electrónica que se han propuesto hasta el momento, se puede observar que la mayoría toma en cuenta lugares específicos para que el elector acuda a emitir su voto y/o contemplan dispositivos dedicados a la recepción y conteo del voto. Es verdad que ya existen modelos planteados para un esquema basado en Internet, pero sus descripciones en cuanto al tipo de comunicación que emplearan son muy vagas o casi nulas y dichos modelos se enfocan principalmente en el acto efectivo de votar, dejando de lado las especificaciones y protocolos que se deben de seguir al hacer uso de una red alámbrica o inalámbrica.

En cuanto a la seguridad, la mayor parte de los protocolos propuestos usan relativamente mecanismos sencillos de autenticación, por ejemplo, tarjetas inteligentes y/o una comprobación de que el votante se ha registrado previamente en una base de datos, por lo cual es necesario hacer uso de distintos mecanismos de autenticación para poder brindar confiabilidad en el sistema de votación.

Por otra parte, los modelos de votación electrónica ya propuestos solamente mencionan que las diferentes entidades gubernamentales deben participar y vigilar que el proceso de la votación se realice correctamente, pero dichos modelos no contienen un apartado dedicado a la parte legislativa que es aplicada en cada una de las naciones democráticas.

La importancia de llevar la votación electrónica a un esquema móvil es de vital importancia, ya que brindaría a los votantes un modelo de votación mucho más conveniente para ellos, haciendo uso de las bondades que brindan sus propios dispositivos móviles, es decir, permitirles emitir su voto desde cualquier lugar en dónde se encuentren (y esté disponible una red inalámbrica), sin necesidad de trasladarse a un lugar donde se encuentre algún dispositivos especializado en recibir o contabilizar el voto.

El modelo propuesto es una alternativa que se podría ir adoptando en las diversos países democráticos, ya que además de brindarle beneficios a los votantes al romper con las barreras geográficas, también es conveniente para las entidades encargadas de gestionar todo el proceso de la votación, pues evitaría gastos innecesarios en material (papel, bolígrafos e incluso dispositivos especializados que pueden llegar a ser muy costosos) y la mayor parte de los esfuerzos se podrían enfocar en garantizar la seguridad del sistema y del votante.

El Modelo de Votación Electrónica Móvil propuesto, consta de cuatro capas como se observa en la Fig. 1

Figura 1. Modelo propuesto de Votación Electrónica Móvil

Cada capa está enfocada a diversos aspectos y fases dentro del proceso de votación, a continuación se describe cada una:

A. ***Facultad o derecho de ejercer el voto***: Se refiere primeramente al proceso de registrar a los votantes que cumplen con los requisitos básicos para poder votar, de esa manera se les otorgará un nombre de usuario y contraseña para después hacer uso de ellos en el proceso de identificación del votante.
B. ***Principios que rigen el voto***: En esta capa se especifican el proceso de autenticación del votante, la cual se realizará por medio de la Firma Electrónica y la implementación del algoritmo de encriptación RSA para autenticarse a través de su dispositivo móvil, además de especificar los principios del voto, como son el sufragio universal, libre, igual y secreto, por mencionar algunos.
C. ***Garantías Procedimentales***: Esta capa involucra la emisión de documentos, certificados, por ejemplo el certificado de autenticación de usuario; también se especifican los aspectos legislativos que regirán el proceso de la votación y se definen las reglas de acuerdo con la legislación del país o de la entidad organizadora de la votación.
D. ***Garantías de Servicios***: En esta capa se especifican las garantías con las que debe cumplir cada procedimiento especificado dentro de la votación, por ejemplo la transparencia, la verificación de la autenticación, verificación del voto emitido por medio de un certificado digital, la integridad de la información, comunicación segura en el envío de datos a través de la implementación del algoritmo AES, entre otros.

Cada capa tratará de cubrir una de las cuatro características esenciales del voto tradicional que también se deben aplicar al Voto Electrónico sobre medios móviles, como se enlistan a continuación:

- ***Universal***, porque el derecho al voto es inherente a todos los ciudadanos, sin más restricción que cumplir las condiciones que establece la entidad que organiza.
- ***Libre***, porque el ciudadano vota por la opción de su preferencia de manera consciente e informada, sin que persona alguna ejerza presión o lo condicione de alguna manera.
- ***Secreto***, porque el ciudadano emite su voto privado, y ninguna persona puede requerirle información sobre el sentido del mismo.
- ***Directo***, porque el ciudadano acude a votar personalmente.

Para verificar la funcionalidad del Modelo de Votación Electrónica, se cuenta con un caso de estudio que consiste en una Urna Electrónica Móvil que será implementada sobre la Arquitectura que se

muestra en la Fig. 2, donde también se aprecia en qué parte de la Arquitectura se implantará cada capa del Modelo propuesto.

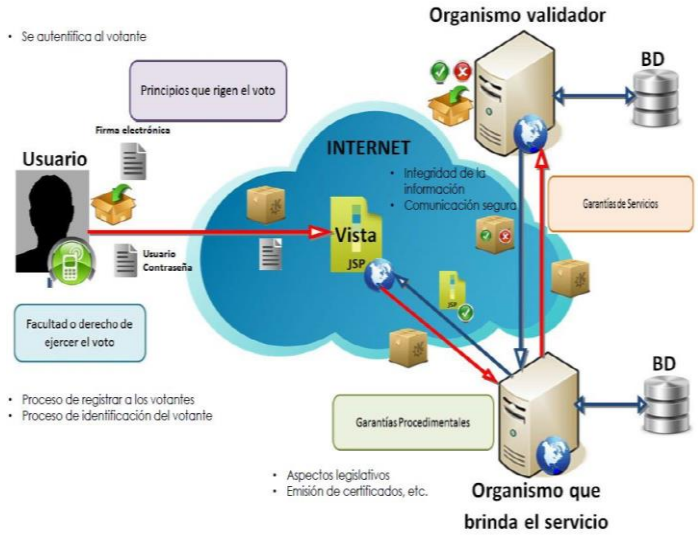


Figura 2. Descripción de cada capa del Modelo en la Arquitectura propuesta.

V. CONCLUSIONES Y TRABAJO A FUTURO

En el presente trabajo se describió la propuesta y avance de un Modelo de Votación Electrónica aplicado principalmente a las redes Inalámbricas y Sistemas Móviles. Como se pudo observar, el Modelo se basa en cuatro capas para cubrir los diferentes aspectos que se deben de considerar en el Voto Electrónico. Pretende como aportación el poder garantizar no solamente la identificación y autenticación del votante, sino también pretende lograr la protección de la identidad del usuario, así como la seguridad de los votos emitidos. Por otro lado, con la implementación del Modelo en la Arquitectura se brindará transparencia a lo largo de todo el proceso y no solamente al finalizar la votación.

Actualmente se está trabajando en validar el mecanismo de Autenticación de usuarios de la Urna Electrónica Móvil (caso de estudio) el cual es una parte de un Modelo de Seguridad en Redes Móviles que la firma electrónica del usuario para su funcionamiento [12] y en la aplicación para el usuario en el sistema operativo Android.

VI. AGRADECIMIENTOS

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

VII. BIBLIOGRAFÍA

[1] Real Academia Española, Diccionario de la lengua española, 22ª ed. 2010. [en línea] disponible en: <http://lema.rae.es/drae/>. [Consultado el 12 de septiembre 2012].

[2] Téllez Valdés, Julio. El voto electrónico, México, Tribunal Electoral del Poder Judicial de la Federación, 2010. [en línea] disponible en: <http://www.te.gob.mx/documentacion/publicaciones/Temas_selectos/14_voto.pdf> [Consultado el 04 de octubre 2012].

[3] F. Rodríguez-Hernríquez, N.A. Saquip, A. Díaz Pérez, C. K. Koc. Cryptographic Algorithms on Reconfigurable Hardware (Signals and Comminication Technology). Springer Verlag, New York, Inc., 2006.

[4] Kaur, R. Digital Signature. Guru Nanak Dev University, India. International Conference on Computing Sciences, 2012.

[5] M. de L. López García. Diseño de un protocolo para votaciones electrónicas basado en firmas a ciegas definidas sobre emparejamientos bilineales. Centro de Investigación y Estudios Avanzados del Instituto Politécnico Nacional. México, 2011.

[6] D. Chaum, R. L. Rivest and A. Sherman. Crypto 82 in Advances in Cryptology 1981 to 1997, Vol. 1440 of Lecure Notes in Computer Science, p. 13-19. Springer Berlin, 1999.

[7] Chun-Ta Li, Min-Shiang Hwang, Yan-Chi Lai. A verifiableElectronic Voting Scheme over the Internet. Sixth International Conference on Information Technology: New Generations, Las Vegas Nevada, April 2009.

[8] H. T. Liaw. A secure electronic voting protocol for general elections. Computers & Security, 2004.

[9] C.C. Chang and J. S. Lee. An anonymous voting mechanism based on the key exchange protocol. Computers & Security, 2006.

[10] Mudhakar Srivatsa. Who is Listening? Security in Wireless Networks. IEEE-International Conference on Signal processing, Communications and Networking, Madras Institute of Technology, Anna University Chennai, India, pp. 167-172, 2008.

[11] Gentles, Donovan and Sankaranarayanan. Biometric Secured Mobile Voting. Kingston, Jamaica, 2011.

[12] Hernández O. Luis E. Modelo de Seguridad para Redes Aplicado a Dispositivos Móviles. Escuela Superior de Cómputo, Instituto Politécnico Nacional, 2013.

[13] L. Bass, P. Clements, R. Kazman, Software Architecture in Practice, 2nd Edition, Addison Wesley, 2003.

VIII. AUTORES

Sandra Ivette Bautista Rosales

Estudiante de la Maestría en Ciencias en Sistemas Computacionales Móviles e ingeniero en Sistemas Computacionales por parte de la ESCOM - IPN, sus líneas de investigación son: Seguridad en Redes Inalámbricas y Sistemas Móviles, Protocolos móviles y desarrollo de Aplicaciones Móviles para Android.

Chadwick Carreto Arellano.

Profesor –Investigador de la ESCOM - IPN, sus áreas de interés son: Comunicaciones Inalámbricas, Cómputo ubicuo, Cómputo Educativo, Seguridad Computacional.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 1, Año 6. Enero–Mayo 2014
Artículos con arbitraje

Arquitectura de Seguridad basada en Identificación y Autentificación para Cómputo Móvil

Sandra Andrea Anízar González
IPN – ESCOM
heladodefresaconmermelada@hotmail.com

Chadwick Carreto Arellano
IPN – ESCOM
ccarretoa@ipn.mx

Alfonso Fernandez Vázquez
IPN – ESCOM
alfonso.fernandez.v@gmail.com

Resumen – Se busca establecer una identificación digital que permita la autenticación del usuario y que pueda ser transportable, identificable y no modificable en un dispositivo móvil, esto conjuntando diversas tecnologías de seguridad, entre ellas: cifrado asimétrico, firma digital, usuario y contraseña, las cuales puedan ser aplicables sobre dispositivos y medios con pocas capacidades de procesamiento y recursos limitados.

Palabras clave – Cómputo móvil, seguridad, Identificación, autentificación.

Abstract – This paper seeks to establish a digital ID that allows user authentication and can be transportable, identifiable and unchanging on a mobile device, this putting together different security technologies, including: asymmetric encryption, digital signature and *password*, which may be applicable to devices with low processing capabilities, and limited resources.

Keywords – Computer mobile, security, identification, authentication.

I. INTRODUCCIÓN

En la actualidad dentro de cualquier sociedad, es necesario que se tenga la adecuada manera de poder identificar a cada uno de los integrantes que la conforma, de manera que al portador de la identificación se le pueda permitir el acceso a recursos, servicios, instituciones y beneficios de manera segura, así como aplicar diversas normas y otorgarle obligaciones.

Es por esta causa, que surge la necesidad de establecer métodos de identificación y autenticación que no solo consten de una credencial, o una contraseña, si no que involucren un conjunto de datos únicos del individuo con un medio de transmisión digital, que mantenga segura la información del usuario, así como a él mismo.

Este concepto se conoce actualmente como ID digital o Identificaciones Digitales, las cuales permiten almacenar información valiosa y disponible para los sistemas de identificación, permitiendo una identificación diversos aspectos y un nivel de información confidencial del usuario, con el propósito de brindarle servicios y otorgarle privilegios.

En el presente trabajo de tesis se propone una arquitectura de seguridad basada en identificación y autentificación para cómputo móvil (ASIACM) con la que se pretende obtener una ID digital de tal

manera que se logre que un individuo pueda tener acceso a diversos servicios en red basados en un método de autenticación. Debido a esto, la ID digital dispondrá de diversos factores de autenticación, con el análisis de información privada, la cual es validada por una tercera instancia de verificación confiable, así como información biométrica, garantizando al usuario entre diversas cosas un medio de identificación y autentificación confiable y de fácil manejo.

II. SEGURIDAD

Existen diversos medios de identificación en la vida cotidiana, como por ejemplo: el lenguaje, tatuajes, documentos con firma manuscrita, documentos con fotografía, escritura, forma de caminar o vestir, entre otros. Pero estos medios nos permiten identificar a una persona o suponer que es la que se piensa, por lo que no se pueden utilizar para poder asegurar cosas como una cuenta bancaria, el acceso a la casa u oficina, o identificarnos ante una persona del gobierno.

Por tal motivo, alrededor del mundo, cada país intenta contar con mínimo un medio de identificación oficial entre sus ciudadanos. En México existen varios de ellos como el pasaporte, la cartilla militar, y principalmente la credencial de elector del Instituto Federal Electoral, otorgada sólo a los ciudadanos mayores de 18 años, que sirve como identificación en el momento de ejercer el derecho al voto así como en la mayoría de los servicios y trámites. 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.

En este tipo de identificaciones, además de que pueden ser falsificadas, también tienen puntos de vulnerabilidad en caso de que la identificación fuera robada o extraviada. Tal es el caso de que no permiten la autenticación del portador, por lo cual cualquier persona maliciosa que la tenga en su poder, puede hacerse pasar por el dueño. Otro inconveniente, es el alto número de información que contiene del dueño, pues puede que está sea una herramienta de extorsión.

Es por lo anterior, que surge la necesidad de establecer nuevos métodos de identificación que permitan a su vez la autenticación de personas y que no solamente consten de una credencial o de alguno de los métodos mencionados anteriormente, sino que, involucren tecnología informática.

Aunque se tiene que tener en cuenta que no existe un sistema que pueda validar tener el 100% de seguridad, puesto que existen diversos tipos de personas maliciosas que buscan la manera de realizar actividades como:

- Robo o daños en el *hardware*
- Robo o daños en la información
- Interrupción de algún servicio.

A partir de este punto, se hablará de cómo se busca la manera de evitar el robo o daños en la información con la ayuda de métodos de identificación y autenticación digital [1].

Los factores o métodos de autenticación están en función de lo que se utiliza para validar al usuario y pueden utilizarse de manera individual o conjunta [2]. Estos factores deben de cumplir con los principios básicos de la seguridad de la información, que en conjunto forman la Tríada CIA (*Confidentiality*, *Integrity*, *Availability*), éstos son: Confidencialidad: para prevenir la divulgación de información a personas o sistemas no autorizados; Integridad: busca mantener los datos libres de modificaciones no autorizadas, es decir,

modificaciones o eliminación de datos importantes; Disponibilidad: cuando la información puede encontrarse a disposición de quienes deben acceder a ella [3].

Para ello, se tienen tres factores de autenticación:

1) *Factor por conocimiento*:
   Apoyado en información que sólo para el usuario legitimo es conocida. Como por ejemplo el uso del *password*.

2) *Factor por pertenencia*:
   Basada en algo que posee el usuario. Por ejemplo, el *Token* de seguridad.

3) *Factor biométrico*:
   Este factor, está basado en alguna característica física del usuario o un acto involuntario. De los más utilizados son los biométricos de huella digital y reconocimiento facial.

Otro punto importante, es que 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, el cual tiene como objetivo el mantener la privacidad de la comunicación entre un emisor (persona que envía un mensaje) y un destinatario o receptor autorizado (persona que recibe el mensaje) [4].

Existen dos tipos de biométricos:

A. Cifrado *Asimétrico*
   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.

B. Cifrado *Simétrico*
   Se basa en la privacidad de su clave secreta ya que es la misma para el cifrado que para el descifrado. En este esquema de cifrado se tiene dos características muy importantes; la primera es una clave secreta(k1); que se usa en la entrada de un algoritmo cuyas operaciones elementales son la sustitución para causar una confusión y una transposición (reordenamiento) o permutación con el fin de manejar una difusión en cada elemento del texto claro.

También existen las firmas digitales, las cuales son un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje, y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador, garantizando la autenticación de origen y el no repudio.

Como los esquemas de firma digital suelen ser lentos en su transmisión, y a veces, la longitud de la firma es similar o mayor al mensaje, en la práctica de utiliza la función *Hash* antes de firmar el documento. Esta función consiste en aplicar a un mensaje de longitud variable, una representación de longitud fija del propio mensaje, que se denomina valor hash, el cual al ser único, se puede averiguar si sufrió alguna alteración en la transacción [5].

III. CÓMPUTO MÓVIL

El enfoque de la comunicación móvil, inicialmente se basaba en la transmisión de voz, posteriormente en el envío y recepción de datos, y hoy en día gracias a la conexión con que la mayoría cuenta a Internet, los dispositivos móviles nos ofrecen diversos servicios como, transacciones bancarias, mail, redes sociales, agendas y más.

Se considera un ambiente de cómputo móvil si soporta una o más de las siguientes características [6]:

1) Movilidad del usuario
El usuario debe ser capaz de moverse de una ubicación física a otra y usar el mismo servicio.

2) Movilidad de red
El usuario puede desplazarse de una red a otra y utilizar el mismo servicio.

3) Movilidad del portador
Debe ser posible moverse de un portador a otro y utilizar el mismo servicio.

4) Movilidad del dispositivo
El usuario puede cambiar de un dispositivo a otro y seguir utilizando el mismo servicio.

5) Movilidad de sesión
Una sesión de usuario debería ser capaz de desplazarse de un entorno a otro.

6) Movilidad de huésped (*host*)
El dispositivo de usuario puede ser cliente o servidor.

Utilizando tecnologías mencionadas anteriormente, y el computo móvil, es que se crean diversos sistemas & arquitecturas científicas que conjuntan fases de autenticación para formar una ID digital y son implementadas en dispositivos móviles, como: *Two Factor Authentication Using Mobile Phones* [8], *Enhanced Authentication Services for Internet Systems using Mobile Networks* [9], *ESET Secure Authentication* [10] entre muchos otros de empresas especializadas.

Por lo que la problemática entonces no es el hecho de la identificación digital en los dispositivos móviles, si no la necesidad de mecanismos y modelos de seguridad que permitan brindar esquemas de autenticación a los medios móviles de una manera más completa, y que así mismo, sean usables, adaptables y flexibles, para garantizar seguridad recíproca entre el prestador del servicio y el usuario móvil.

En base a lo anterior, y observando las diferentes propuestas que existen hoy en día, se le suma la necesidad de crear una identificación digital, que permita la autenticación del usuario por medio de dispositivos móviles, permitiendo de tal modo, tener acceso a diferentes recursos, no necesitar de un dispositivo extra, tener movilidad y poder autenticarse de manera segura cuando y donde quiera.

Y qué mejor que crear una ID digital, que te permita tener factores de posesión y de conocimiento, más un certificado digital, más la validación de información privada por una tercera instancia gubernamental, más la creación de una firma digital, más un factor biométrico que en diferentes predicciones como la de Gartner, Deloitte, DualShield, IDC, entre otras, aseguran que tal factor se impondrá en los dispositivos móviles a partir del 2014 [11].

IV. ARQUITECTURA PROPUESTA (ASIACM)

La arquitectura de identificación y autenticación para cómputo móvil propuesta en el presente trabajo, pretende resolver la problemática descrita anteriormente, al conjuntar los tres factores de autenticación:

Esto, con la creación de una identificación digital del usuario (ID digital), formada a partir del uso de diversas tecnologías como el cifrado con RSA,

función MD5, certificados digitales y firma digital, con perfiles únicos del usuario:

A. Perfil privado
   Información privada del usuario con la que se establece el factor de conocimiento en la arquitectura ASIACM.

   El usuario tendrá que llenar un formulario con información relevante pero privada de él. Como por ejemplo: Nombre(s), apellido paterno, apellido materno, sexo, fecha de nacimiento, entidad Federativa en la que nació, Cedula profesional, cartilla, No. de identificación para votar, teléfono celular, No. de licencia, CURP, No. de Seguro Social, RFC.

   La selección de estos dependerá de la aplicación que se le quiera dar y hacia qué servicios va dirigida. Entre ellos, los dos importantes son: Nombre completo, para poder solicitar información de este, y a su vez, permitir su registro a la arquitectura una sola vez; también el teléfono celular, puesto que de alguna manera se tiene que tener contacto con el usuario una vez que esté se dio de alta en la arquitectura ASIACM por cualquier cuestión. Se tiene que anexar la clave del área en donde se encuentra para que este sea válido.

   Otra cosa requerida forzosamente, es el uso de un *password*, el usuario lo elige, pues es uno de los medios por el cual se tendrá acceso a su ID-digital para poder ser identificado y autenticado. Sus características son: Tamaño mínimo de 8 caracteres de longitud; Al menos un carácter tiene que ser letra mayúscula, un carácter tiene que ser letra minúscula, un carácter tiene que ser un número, un carácter tiene que ser un carácter especial de los 60 disponibles en la mayoría de los dispositivos móviles.

B. Perfil público
   Validación del perfil privado por terceras instancias.

   Cabe mencionar, que la importancia de la creación de este perfil, radica en que solamente se le asignará la identificación digital, a personas que de alguna manera pueden validar su existencia/pertenencia a algún grupo o país por una tercera instancia de verificación y utilizar tal información como la parte pública de la ID-Digital.

   Utilizando los ejemplos de la información que puede ser pedida para el perfil privado, se puede comparar tal información con bases de datos como, IFE (Instituto Federal Electoral) ahora INE (Instituto Nacional Electoral) únicamente para personas mayores de edad. O la del CURP (Clave Única de Registro de Población) para cualquier persona registrada.

C. Perfil biométrico
   Es un servicio asociado a la información única de usuario, con la que se establece un factor de identidad. En ese aspecto, se pude seleccionar el uso de cualquier biométrico, siempre y cuando, el dispositivo móvil no requiera de un sensor extra para su uso, pues de ese dispositivo móvil, se envía la información al servidor, en donde se realiza el proceso de obtención de patrones biométricos.

Tal ID digital, consta del conjunto de documentos electrónicos, tales como llave privada, texto plano cifrado, firma digital y certificado digital. La cual una vez creada, se almacena en el dispositivo móvil

del usuario buscando que no genera un peso fuerte de almacenamiento para el móvil.

La información del usuario se tiene que mantener de forma íntegra y sobre todo confidencial, una vez que un usuario se da de alta y finalizó la generación de una ID digital, esta ID digital no se almacena, pues esto sería un punto vulnerable de la arquitectura, por lo que únicamente se contara con registro de datos primarios como, nombre, teléfono, firma digital y código hash.

Se utilizaran reportes, en los cuales, se podrá visualizar la hora, el día y la acción que realizo el usuario (creación ID digital, autentificado, no autentificado, certificado expirado) a manera de bitácoras que permitan fortalecer el ámbito del no repudio y tener una mejor administración de los usuarios.

En la figura 1, podemos observar de una manera más esquemática el funcionamiento de la propuesta de arquitectura ASIACM, así como sus módulos que la conforman, las instancias externas de verificación y la base de datos.

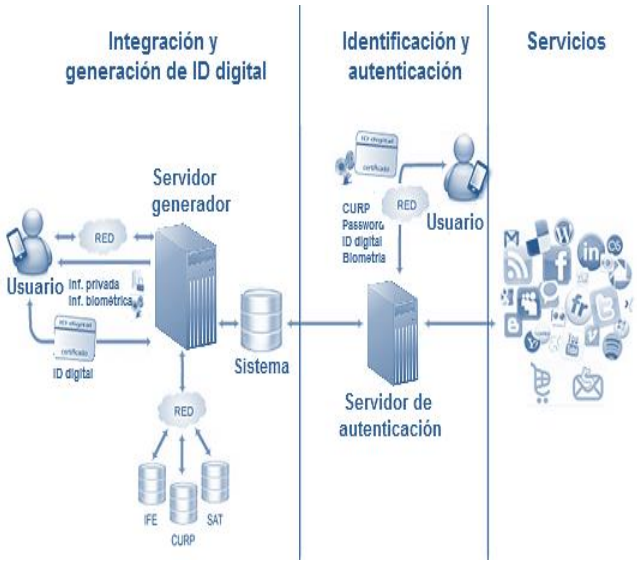


Fig. 1. Representación de la arquitectura de seguridad basada en identificación y autentificación para cómputo móvil (ASIACM). Fuente: Propia

Como se puede observar en la figura 1, se tienen contemplados el módulo de integración y generación de ID digital y el módulo en donde se identifica y autentifica al usuario.

A. Módulo Integración y generación de ID digital.

En estas etapas, se le pide al usuario que introduzca su información privada, y sólo procederá al siguiente paso cuando tal información sea validada por una tercera instancia. Cabe mencionar que al ser una arquitectura, se le pueden agregar diversas instancias que avalen la información que el usuario brinda, evitando así, que se generen ID`s de personas ficticias o diversos problemas más. Para el presente trabajo de tesis, se validan los datos con el uso de la base de datos de las instancias externas de validación por medio de la red, siendo esto parte de la información pública del usuario. De tal base de datos se extrae la información pública del usuario.

Una vez que ya se tiene la información anterior con su validez, se pide al usuario que introduzca su información biométrica para que en se conjunte la información obtenida y con la aplicación del cifrado asimétrico RSA, 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.

B. Módulo Identificación y Autenticación

En ellas 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 con la función MD5, que el certificado aun no caduque y que la información que introduzca sea la misma y que coincida tal información con el

registro almacenado en la base de datos, así como también deberá de coincidir la información biométrica, permitiendo cancelar la autenticación en el momento en que alguna de estas capas no coincida. Todo esto para que una vez que se autentifique el usuario, este pueda acceder a sus servicios en donde se le solicite ser identificado y autentificado.

También se considera la acción de borrar usuario y de visualizar reportes en donde se pueda visualizar las veces que el usuario ha querido autentificarse con éxito, y si en algún momento existió algún tipo de error en el proceso.

V. CARACTERÍSTICAS DE LA ARQUITECTURA

1) 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, de las que depende el biométrico a utilizar,

2) Robusto:
Considerando la información conformada por tres perfiles o fases de seguridad: Privada, pública y biométrica.

3) Validación con terceras instancias:
Con el fin de que los usuarios de la arquitectura, existan dados de alta en alguna dependencia de gobierno como el INEI, SAT, o que tengan un CURP validado. Esto para evitar que se creen identificaciones falsas o que los usuarios tengan más de una en su poder y con información diferente.

4) Flexible a cambios

La arquitectura, tiene la flexibilidad de ajustarse a cambios en cuanto a sus perfiles. Para comprender esto, utilicemos el ejemplo de que la arquitectura es utilizada para el voto en línea en México, para esto se necesitarían los siguientes perfiles:

- **Perfil privado**: se solicita al usuario, su nombre, entidad federativa, fecha de nacimiento, dirección.

- **Perfil público**: La instancia de validación que se utilizaría, sería la validación con la BD del INE (Instituto Nacional Electoral) con el debido permiso de esta, solamente para que valide que los datos que el usuario introdujo en el perfil privado pertenecen a una persona perteneciente a él.

- **Perfil biométrico**: En este particular ejemplo, se podría utilizar el biométrico de rostro, el cual pidiera al usuario una fotografía de su credencial para votar, así como de su rostro justo en el momento en el que se está creando la ID digital, esto para comprobar y validar primeramente que el dueño de la identificación es el próximo dueño a la ID digital. También se podría añadir un segundo biométrico de huella digital, para validar de igual forma que el biométrico anterior, la información de la credencial para votar como la del usuario. El único requerimiento extra que tendría que tener el dispositivo móvil, es un sensor para capturar la huella digital.

Estos perfiles cambiarían radicalmente, si el usuario es menor de edad y no cuenta con credencial para votar. Por lo que se tendrían que acomodar nuevos perfiles dependiendo de los usuarios que necesiten de su ID digital, y del

proceso que se quiere realizar después de la autenticación.

5) Identificación
Para la identificación del usuario, se utiliza información pública que anteriormente ya fue validada por una tercera instancia de validación y que confirman la existencia del usuario en instancias del gobierno; y un *password* que el al momento de crear su ID digital, introduce con un mínimo de: 8 caracteres de longitud, un carácter en mayúscula, un carácter en minúscula, un numérico y un símbolo especial. Esta información, primero se verifica si existe en la BD, pues de lo contrario el usuario no puede ser identificado.

6) Movilidad
Al ser una arquitectura de seguridad móvil, obtiene mayor portabilidad y sencillez que las que son empleadas para las máquinas de escritorio.

7) Seguridad de información
Si por algún motivo el usuario perdiera su dispositivo móvil, la persona que lo encuentre no podrá acceder a la información, ni mucho menos tener acceso a servicios del usuario, puesto que la información contenida en el dispositivo, se encuentra encriptada y para desencriptar se necesita de la llave privada almacenada en la BD de usuario, y para poder tener acceso a ella primero se tiene que identificar y autentificar al poseedor del móvil utilizando información pública, *Password* y biometría.

8) Autenticación de usuario:
Utilizando tecnologías como criptografía, firma digital, certificados digitales, con los perfiles privados, públicos y biométricos del usuario, una característica principal de la Arquitectura ASIACM es la Autenticación de usuarios validados por una tercera instancia, la cual verifica que a la ID digital del usuario que se almacena en el dispositivo móvil, no tenga cambios y que pertenezca a la persona que se quiere autentificar, una vez que esta primero se identifique y después introduzca su información biométrica.

9) No repudio:
Con el uso de firmas digitales, biométrico e información privada que solamente el usuario conoce, al momento de identificar y autentifica al usuario, este no puede negar el acceso la autenticación. Aparte de que se actualizan los reportes cada vez que el usuario: pretenda acceder a la autentificación, de forma satisfactoria o que otra persona quiso acceder a ella sin obtener la validación.

10) Comparación biométrica
A diferencia de los biométricos simples, que para autentificar al usuario comparan su patrón biométrico con todos los usuarios almacenados en la BD, la comparación biométrica que se realiza con esta arquitectura ASIACM, solamente compara la información biométrica que el usuario contiene en su ID digital debidamente encriptada, con la información biométrica que el usuario otorga justo en el momento de la autentificación, agilizando el proceso de autentificación.

VI. CONCLUSIONES

En este trabajo se tuvo por objetivo la creación de una arquitectura que contempla tres tipos de información única del usuario: pública, 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 que es almacenada en el móvil del usuario y permite a este, el acceso a sus servicios tales como cuentas bancarias, redes sociales y más.

Al autenticar al usuario y al tener un registro de las entradas exitosas de él, así como sus intentos fallidos, se establece el no repudio, ayudando a las empresas y personas al confiar más entre ellos.

Entre las principales ventajas que se logran, es la conjunción de las tecnologías de seguridad, necesarias y eficaces, con los tres tipos de información del usuario (privada, púbica y biométrica). Demostrando que la autenticación multifactor, con validaciones de terceras instancias, permiten tener un nivel de seguridad más al de arquitecturas actuales.

VII. BIBLIOGRAFÍA

Basic format for books:

[1] Rick Lehtinen,Deborah Russell,G. T. Gangemi. (2006). Computer Security Basics. USA: O'Reilly Media.

[2] Gollmann D. (1999).Computer Security. John Wiley & Sons, Chichester,New York.

[3] Pilar Lasala Calleja. (2013). Derecho y tecnologías avanzadas. España: Prensas de la Universidad de Zaragoza.

[4] Alfred J. MenezesPaul C. van Oorschot, & Scott Vanstone. (1997). Handbook of Applied Cryptography. Estados Unidos: CRC Press.

[5] Carolina M. Laborde. (2008). Electronic Signatures in International Contracts. European University Studies: Peter Lang.

[6] A.K. Talukder, H. Ahmed, R.R. Yavagal (2010), Mobile Computing: Technology Applications and Service Creation (2a edición), India: Tata McGraw-Hill.

[7] Asoke K. Talukder, Manish Chaitanya. (2008). Architecting Secure Software Systems. Estados Unidos: CRC Press.

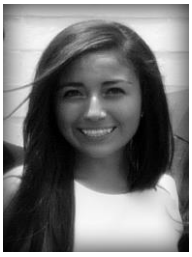
[8] Fadi Aloul, Syed Zahidi, & Wassim El-Hajj . (2009). Two Factor Authentication using Mobile Phones. International Conference on Computer Systems and Applications, 641-644.

[9] Mark Looi (2001), Enhanced Authentication Services for Internet Systems using Mobile Networks, Australia: Global Telecomunication Coference, 3468-3472.

[10] Enjoy Safer Technology (2014), ESET Secure Authentication. Disponiple en: http://descargas.eset.es/templates/fichas_productos/ESET_Secure_Authentication.pdf

[11] IDC, (2013). Nuevas tendencias tecnológicas han entrado al 2013. Sitio web: http://mx.idclatin.com/releases/news.aspx?id=1433.

VIII. AUTORES



Sandra Anízar González
Estudiante de la Maestría en Sistemas de Cómputo Móvil, en la ESCOM – IPN. Desde 2011, Ingeniero en Sistemas Computacionales de la ESCOM - IPN. Línea de investigación: Desarrollo de sistemas para el cómputo móvil - Seguridad.

Chadwick Carreto Arellano.
Candidato a Doctor en Ciencias Computacionales por el CIC – IPN. Forma parte de la Sección de Estudios de Posgrado e Investigación, Departamento de Programación y

Desarrollo de Sistemas y Academias de Ingeniería de Software, Sistemas Operativos y Redes en la ESCOM - IPN.

Alfonso Fernandez Vázquez.
Doctor en Ciencias de la Electrónica en Instituto Nacional de Astrofísica, Óptica y Electrónica. Forma parte de la Sección de estudios de posgrado e investigación en ESCOM - IPN. Líneas de investigación: Comunicaciones digitales y procesamiento de señales.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 1, Volumen 1, Año 6. Enero–Mayo 2014
Artículos con arbitraje

Non-Saturation Throughput of S-ALOHA Using the Time-Scale Decomposition Technique

M. Gutierrez-Begovich
IPN – ESCOM
lgutierrezb0200@alumno.ipn.mx

M. E. Rivero-Angeles
CIC IPN
mriveroa@ipn.mx

Resumen – *Slotted* ALOHA (S-ALOHA) protocolo de acceso aleatorio es un protocolo ampliamente utilizado para la transmisión de paquetes cortos en redes inalámbricas. La mayoría de los trabajos consideran ya sea un modelo de población infinita, donde el impacto del protocolo de retroceso no se puede evaluar de forma adecuada o un modelo de población finita, donde se fija el número de nodos. En este artículo*, se propone una combinación de ambos modelos utilizando la técnica de descomposición de escala de tiempo. Esta metodología permite estudiar el sistema en condiciones más realistas donde la dinámica de los usuarios que entran y salen del sistema se refleja en el rendimiento del sistema, así como el impacto del protocolo de retardo de envío. Además, permite el estudio del sistema en condiciones de no-saturación. La metodología propuesta se divide el análisis en dos partes: a nivel de paquetes y a nivel de conexión. Este análisis hace que los resultados adecuados cuando la escala de tiempo de las estadísticas a nivel de paquetes y de nivel de conexión son diferentes. Por otro lado, cuando estas escalas son similares, la metodología propuesta ya no es la adecuada para realizar el análisis.

Palabras clave – S-ALOHA, condiciones de no saturación, infinito y finito modelo de población, la descomposición de escala de tiempo

Abstract – Slotted ALOHA (S-ALOHA) random access protocol is a widely used protocol mainly for the transmission of short packets in wireless networks. Most papers consider either an infinite population model where the impact of the backoff protocol cannot be adequately evaluated or a finite population model where the number of nodes is fixed. In this letter*, a combination of both models is proposed using the time-scale decomposition technique. This methodology allows to study the system under more realistic conditions where the dynamics of users enter and leaving the system are reflected on the performance of the system as well as the impact of the backoff protocol. Also, it allows studying the system in non-saturation conditions. The proposed methodology divides the analysis in two parts: packet-level and connection-level. This analysis renders suitable results when the time scale of the packet level and connection level statistics are different. On the other hand, when these scales are similar, the proposed methodology is no longer suited.

* Corresponding author: Mario Eduardo Rivero-Angeles, Ph.D., professor, research fields: telecommunications, computer networks, cellular systems, wireless sensor networks, P2P networks. E-mail: mriveroa@ipn.mx.

Note: A fuller version of this paper was first submitted in David Pubishing - Journal of Mechanical Engineering and Automation: 4 (2014) 116-122.

Keywords – S-ALOHA, non-saturation conditions, infinite and finite population model, time-scale decomposition.

I. INTRODUCTION

Slotted ALOHA (S-ALOHA) random multiple access strategies are widely used in data and cellular networks because it is the simplest protocol, since it does not require any information about the channel conditions, and its implementation is straightforward [1]. This protocol is the basis of the access in both TDMA/FDMA and CDMA cellular systems [2, 3], Split Channels control schemes [4] and LTE [5]. Also, given the rapid development in Wireless Sensor Networks (WSN), it can be used as an alternative to the CSMA based protocols that consume much more energy due to the channel sensing functions. In S-ALOHA, users that arrive to the system trying to reserve a data channel simply wait for the beginning of the next time slot and transmit their packet. If more than one user attempts to transmit a packet, then a collision occurs. If only one packet transmission attempt occurs in a time slot then it is received without any errors and the base station replies to the mobile with a positive acknowledge (ACK). For high offered loads, the amount of collisions increases drastically due to the lack of a central access coordination entity and the random nature of the arrivals; then very few users can actually have access to the traffic data channels, rendering a very low average data rate for the system.

Previous works in this area, consider either an infinite population model or a finite population model. In the former, it is not possible to know the fraction of the total arrival rate that corresponds to backlogged packet transmissions. Consequently, it is not possible to know the effect of the collision resolution (or backoff) protocol. In the latter, the number of users is considered to be fixed. This assumption closely matches conditions in a local area networks (LANs), but do not match conditions in a cellular system or WSN where nodes typically transmit sporadically. Hence, in WSNs it is rare to find all nodes in the network reporting their data simultaneously. In the case of cellular systems, users enter and leave in a stochastic manner. Another common assumption in previous works is that the system is in saturation conditions, where nodes always have a packet to transmit. This has been usually considered as the worst-case scenario. However, in wireless systems (cellular, local or sensor networks), it is highly unlikely that all subscribed users or nodes have always a packet ready for transmission. In this work, we focus on the use of S-ALOHA in wireless networks where a high number of users/nodes enter and leave the system at different instants. As such, an infinite population model and non-saturation conditions are assumed. These conditions are typical in cellular systems and WSNs.

In a more detailed discussion on the infinite population model, each packet can be considered as if it belongs to a different user. Hence, each newly arrived packet can be assigned to an idle user, i.e. one that does not have a packet ready to transmit [9]. Observing the channel over time, each packet is scheduled to be transmitted at a given time (scheduling points). The scheduling points include both the generation times of new packets and the retransmission times of previously collided packets [12]. Therefore, the Poisson process considers a total traffic load G. This total traffic load corresponds to the sum of the new packet arrival rate GN and the arrival rate of the retransmitted packets, GR. The main problem with this approach is that the specific values of GN and GR are unknown, and the only parameter used for the analysis is G. Hence, this

model does not provide any insight into the dynamics of the system because the value of G is related neither to the particular backoff policy nor to its parameters. In particular, since backlogged packets are no different from new packets, then an access delay analysis is not feasible because the time between retransmissions of backlogged packets is not reflected on the total arrival process. Additionally, in a real system, the number of backlogged packets is time-variant; therefore, the value of the total traffic load G also changes. Thus, this leads to a feedback effect, generating further changes in the number of backlogged packets. These changes are not reflected on the infinite model with a constant value of the total traffic load. In summary, the conventional infinite population model does not allow to study in detail the effect of backlogged packets for a particular backoff scheme.

In this work, we study the performance of the S-ALOHA protocol in non-saturation conditions for an infinite population model using the time-scale decomposition technique that allows studying in detail the effect of the retransmissions under the Geometric Backoff (GB) protocol. The proposed analysis corresponds to a combination of the infinite population model and finite population model. Indeed, the performance of the system is sensitive to both arrivals and departures of users as well as the backoff protocol. However, this methodology is an approximation of the practical system since it is only suited when the time scales at the packet level is much higher than the time scale at the packet level. This assumption is accurate in most cellular and wireless sensor networks, where the user/node arrival is in the order of seconds, while the packet transmissions are in the order of miliseconds.

II. TELETRAFFIC ANALYSIS

It is considered that the average time between user arrivals is in the order of seconds while the packet transmission is in the order of a few milliseconds. Therefore, it is possible to use the time-scale decomposition technique [6]-[7] to separate the analysis into two parts: connection level and packet level analyses. As such, analysis at the packet level can be performed considering that the total number of users in the system is fixed. This results in a very manageable analysis in terms of the number of state variables needed at the packet level. Indeed, the Markov chain for the packet level analysis only considers the number of users attempting a packet transmission. On the other hand, at the connection level, the total number of users varies according to a Poisson arrival processes and exponentially distributed session times. Therefore, a continuous time analysis is preferred in this case.

A. Packet level analysis:

At this level, the number of nodes in the system is considered to be constant, M. Let the number of slots be sequentially numbered and $N(k)$ represents the number of packets in the backlogged state at the beginning of the k slot. $N(k)$ depends on the number of packets in the $(k-1)^{th}$ slot and the number of packets that moved from the new state to the backlog state or a single backlogged packet successfully transmitted within that slot. Since state transitions are independent of the events in previous slots, this system can be modeled using a Markov chain as that depicted in [1] where the random variable $N(k)$ corresponds to the state of the chain. In this Markov chain, all states communicate each other; hence, it is an ergodic chain. Hence a steady state distribution exists. New packets are transmitted with probability σ while backlogged packets are retransmitted with probability τ in each time slot. Let

π_i be the steady state probability of finding the system in state i. Then, the Markov chain can be solved using [9]: and using the normalization equation , where and are the steady state probability vector and probability transition matrix respectively with elements given by:

(1)

These transition probabilities can be explained as follows: Considering that the system has i backlogged packets in a given time slot, 1) There cannot be more than one packet transmission in the current time slot. As such, there cannot be less than $i-1$ packets in the following time slot. 2) The case where a transmission is successful, the system goes to $i-1$ packets in the following time slot. This happens when only one backlogged packet is transmitted. 3) When there are none or more than one transmissions of backlogged packets or only one new packet is transmitted, the system remains in state i. 4) When a new packet collides with one or more backlogged packets, the system goes to state i $i+1$. 5) When j new packets transmit, the system goes to state $j-i$.

This chain is numerically solved. Finally, the throughput is equivalent to the probability that one packet is transmitted in a time slot and this probability depends on the number of packets in the backlogged state, and the number of users in the system n, then:

(2)

The probability of having only one transmission in a time slot when there are i packets in the backlog state, $S(i)$, is equal to the probability that either only one new packet is transmitted or only one backlogged packet is retransmitted, then:

(3)

As it can be seen, the throughput has a very strong dependence on both the transmission and retransmission probabilities σ and τ respectively.

B. Connection level analysis

At this level, we capture the Poisson arrivals and departures, typically assumed in the infinite population model. Hence, a Continuous Time Markov Chain (CTMC) is proposed. In this case, users arrive to the system with rate λ and users remain connected for an exponentially distributed time with mean $1/\mu$. As such, a conventional birth-death process is considered. Let $W(t)$ be a CTMC with $W(0)=0$ and feasible states given by. The transition rates in state $W(t)=M$ due to a user arrival is given by λ in which case it goes to the immediate upward state $M+1$. On the other hand, the system goes to the neighbor downward state $M-1$ with rate $i\mu$ in case of a user departure. From this description it is easy to see that the steady state probability of being in state i is given by where $a=\lambda/\mu$ corresponds to the traffic load. In this infinite model there is no limit on the number of users that can arrive to the system. As such:

(4)

However, in order to compare this mathematical model with simulation results, a maximum number of nodes, v, is considered. Hence:

(5)

Finally, the throughput in non-saturation conditions can be calculated as follows:

(6)

Note that the conventional infinite population model does not show this dependency between the retransmission probability and the throughput. On

the other hand, the finite population model usually does not consider the new packet arrival rate.

III. NUMERICAL RESULTS

In this section, the accuracy of the mathematical model is evaluated comparing to simulation results. In Figs. 1 and 2 we compare the accuracy of the proposed analytical model to simulation results for different system conditions. It can be seen that the decomposition technique is accurate when the difference in time scales of the connection level and packet level are high, i.e., high values of τ and σ. In these scenarios, the (re)transmission probability is high, which renders low packet transmission times. Hence, packets are transmitted much faster than the arrival of new users. As such, the connection level statistics can be considered to be rather stable, i.e., the number of users with an active session remains almost unchanged during the transmission of a packet. Then the decomposition methodology is most accurate. On the other hand, when packet (re)transmission times are high (low values of σ and τ), the user arrival times are in a similar time scale. Indeed, in these conditions, during a packet transmission, the number of users in the system is highly likely to change. Hence, the time-scale decomposition technique no longer renders accurate results.

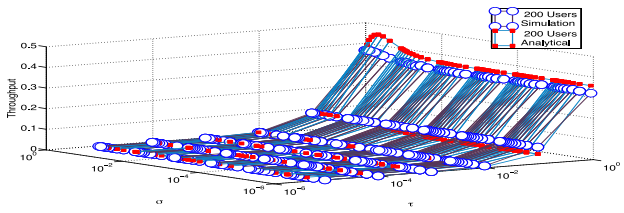


Fig 1. Throughput for S-ALOHA in non-saturation conditions for different values of λ and τ (σ=τ, μ=1), 200 users.

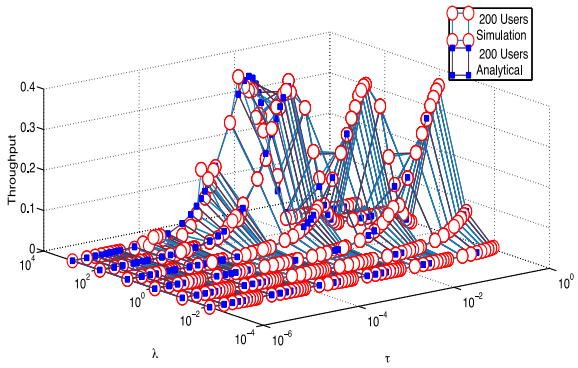


Fig 2. Throughput for S-ALOHA in non-saturation conditions for different values of σ and τ (λ=1, μ=1), 200 users.

Also, comparing Figs. 1 and 2 can draw an important conclusion. In Fig. 1. both transmission and retransmission probabilities are considered to have the same value. Hence, no differentiated access is considered in this case. It can be seen that the maximum throughput is around 0.4. Conversely, when the values of σ and τ are different, the maximum achievable throughput is increased to around 0.5, which is a considerable increase. As such, it can be concluded that a system can render a better performance by carefully selecting the transmission and retransmission probabilities with the same conditions of the traffic load and maximum number of users. Specifically, the value of the retransmission probability has a higher effect on the performance of the system than the new packet transmission τ.

IV. CONCLUSIONS

In this work, the S-ALOHA random access protocol is studied under the infinite population model where the impact of the backoff protocol is reflected on the system performance. Also, non-saturation conditions are assumed. The system is studied using the time-scale decomposition technique, that allows separating the analysis in two main parts: packet-level and connection-level analysis. By applying this

methodology, it is simple to consider the dynamics of users enter and leaving the system in order to transmit their packets. We believe that this reflects more realistic systems such as cellular and wireless sensor networks. Numerical results clearly shows that the (re)transmission probabilities have an important impact on the throughput of the system, which cannot be perceived considering the conventional infinite population model. Conversely, the model also reflects the impact on the traffic load, which cannot be perceived by using the conventional finite population model. Finally, this methodology can be used to study more complex systems such as the IEEE 802.11 that works under the CSMA/CA protocol, where the finite population model in saturation conditions is usually assumed.

Acknowledgments: This work was partly supported by IPN (under project 200120107).

V. BIBLIOGRAPHY

(1) R. Rom and M. Sidi, *Multiple Access Protocols. Performance and Analysis*. Berlin, Germany: Springer-Verlag, 1990, pp. 47–103.

(2). C. Schlegel, R. Kempter, and P. Kota, "A novel random access method using CDMA," *IEEE Trans, on Wireless Commun.*, vol. 5, no. 6, pp. 1362-1370, June 2006.

(3) Y. Yang and T.-S. P. Yum, "Analysis of Power Ramping Schemes for UTRA-FDD Random Access Channel," *IEEE Trans. Comm.*, vol.4, no.6, pp.2688-2693, Nov. 2005.

(4) J. Deng, Y.S. Han, and Z. J. Haas, "Analysis split channel medium access control schemes," *IEEE Trans, on Wireless Commun.*, vol. 5, no 5, pp. 967-971, May 2006.

(5) LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification, 3GPP TS 36.321 version 10.3.0 Release 10.

(6) S. Ghani, M. Schwartz, "A decomposition approximation for the analysis of voice/data integration," IEEE Trans. on Commun., vol. 42, no. 7, pp. 2441-2452, Jul. 1994.

(7) D. Mitra, M. I. Reiman, "Robust dynamic admission control for unified cell and call QoS in statistical multiplexers," IEEE J. Select. Areas Commun., vol. 16, no. 5, pp. 692-707, Jun. 1998

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 —[ ]l. 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