Contenido

3 **El Plagio Electrónico, ¿Necesidad del Alumno Promedio?**
Ing. Patricia Pérez Romero, Ing. Jesús Pimentel Cruz (CIDETEC-IPN).

Teoría del Caos en la Protección de la Información 7
M. en C. María Aurora Molina Vilchis, M. en C. Eduardo Vega Alvarado,
Dr. Ramón Silva Ortigoza, (CIDETEC-IPN).

12 **Robots Móviles: Evolución y Estado del Arte**
Ing. Victor Ricardo Barrientos, Ing. José Rafael García Sánchez,
Dr Ramón Silva Ortigoza, (CIDETEC – IPN)

Introducción a las Redes CAN. 1a. Parte. 18
Ing. Jesús Pimentel Cruz, Ing. Patricia Pérez Romero, (CIDETEC-IPN).

22 **La Visión Artificial en la Robótica**
Ing. Rogelio Rojas Hernández (UPIITA-IPN), Dr. Ramón Silva Ortigoza,
M. en C. María Aurora Molina Vilchis, (CIDETEC-IPN).

Tecnología Bluetooth para Sistemas de Monitoreo en Dispositivos PDA. (1a. Parte) 29
M. en C. Juan Carlos Herrera Lozada (CIDETEC–IPN), Jacobo Sandoval Gutiérrez,
Raziel Morón Corrales (CICATA LEGARIA-IPN)

35 **Licencias de Software: Antecedentes**
M. en C. Eduardo Vega Alvarado, Lic. Silvia Toledo Molano,
M. en C. María Aurora Molina Vilchis (CIDETEC–IPN)

polibits

¿Eres investigador, académico o estudiante de posgrado en el área de la Computación, Informática, Sistemas Digitales o Electrónica?

¿Deseas publicar los avances de tus investigaciones o desarrollos tecnológicos?

La revista **polibits** del CIDETEC-IPN te invita a publicar tus trabajos. **polibits** es una revista de difusión nacional en su formato impreso e internacional en su versión electrónica, ubicada en el site del CIDETEC:

www.cidetec.ipn.mx

Si deseas más información consulta el site anterior, en donde encontrarás los lineamientos básicos para publicar en nuestra revista, o consúltanos directamente en:

Consejo Editorial Revista **polibits**

E-mail: cidetec_si@ipn.mx

EDUCACION
CONSERVACION
INNOVACION
CIDETEC
IPN

El Plagio Electrónico, ¿Necesidad del Alumno Promedio?

Ing. Patricia Pérez Romero
Ing. Jesús Pimentel Cruz
Profesores del CIDETEC-IPN

Es indudable el valor que tienen las nuevas tecnologías de información y comunicación (TIC) en el campo de la educación. La inmensa cantidad de información disponible en medios digitales, el alcance y penetración de la televisión educativa, el uso de la computadora para realizar simulaciones y ejercicios interactivos, y sobre todo el alcance casi infinito de la Internet, son un claro ejemplo de como el avance tecnológico permite mejorar el proceso enseñanza-aprendizaje.

Sin embargo, la posibilidad de acceder a esta gran cantidad de información de muy diversa índole, implica aspectos no deseados respecto a su uso, como es el problema del plagio en la Internet (***WWW, World Wide Web***) por parte de la comunidad académica, y especialmente los alumnos.

La computación ha evolucionado a la par de varias generaciones de usuarios, llegando a un momento actual en donde la mayoría de usuarios se encuentran entre los 8 y 15 años de edad. Este tipo de tecnología los ha acompañado casi desde que nacieron, y ha sido asimilada por ellos de manera natural. Su habilidad con la Internet y el manejo de las computadoras aumenta con el tiempo, hasta un punto tal que es más sencillo plagiar información que realizar una investigación. Por ello es importante preguntarse ¿en verdad es el plagio en la ***WWW*** una necesidad del alumno promedio?

¿Qué entendemos por plagio?

Si consultamos el diccionario de la Real Academia Española en su versión Web e introducimos el término *plagiar*, obtenemos la siguiente definición: *Copiar en lo sustancial obras ajenas, dándolas como propias*.

El agregar el calificativo de *electrónico* implicaría que esta es la fuente de obtención; de este modo, entenderíamos por *plagio electrónico* a los materiales presentados como el fruto del trabajo personal que en realidad han sido copiados de forma parcial o total mediante procedimientos informáticos, sin mencionar su autoría original. El origen de estas fuentes es mayoritariamente la Internet, aunque también es una práctica común la copia de otros medios, tales como enciclopedias en CD-ROM, o presentaciones electrónicas de otros compañeros.

En este sentido, el vocablo *ciberplagio* [Fernández 2002] es un tanto más limitado, aludiendo únicamente a aquél plagio cuya fuente procede de la Internet.

¿Es un fenómeno nuevo presentar trabajos plagiados parcial o totalmente?

Por supuesto que no, siempre ha habido alumnos que han copiado de diversas fuentes, llámense libros, enciclopedias, trabajos de compañeros, etc.…; lo novedoso en este caso es la facilidad que supone la ***WWW*** para hacerlo. Con unos cuantos movimientos de ratón podemos disponer de una enorme cantidad de trabajos que representan éxito académico sin esfuerzo. Para esto existen varios métodos, entre los que podríamos mencionar:

- Ingresar directamente a un programa de búsqueda, e indicar el término o tema que se desea encontrar; la aplicación nos mostrará en fracciones de segundo una gran cantidad de resultados coincidentes con el criterio de búsqueda.

- Recurrir a alguno de los sitios de moda, donde se almacenan apuntes y trabajos que son cedidos por los estudiantes para que otros los puedan *aprovechar*. Suelen estar muy bien clasificados y el sistema de búsqueda es muy sencillo.

- Buscar en las páginas de congresos sobre el tema de interés, donde regularmente se hacen públicos los documentos íntegros de las conferencias.

Dada la abundancia de fuentes,

elaborar un trabajo-collage o híbrido a partir de varios de estos documentos no resulta complicado, dado que se reduce a operaciones de cortar y pegar.

Problema de difícil solución

Determinar el porqué existe un alto porcentaje de alumnos que plagian trabajos es un tema de difícil respuesta. Cuando se pide un trabajo de investigación, el estudiante en general entiende que debe buscar información sobre el tema, insertarla en un documento, y a lo más darle un formato atractivo para entregarlo al profesor como su creación; esto es válido para los alumnos, ya que toman como justificación el tiempo invertido en la búsqueda y edición de la información.

Naturalmente, los resultados de tan escaso acercamiento a la investigación son muy pobres y limitados, lo cual, aunado a una deficiente formación en la metodología de la investigación, produce trabajos de baja calidad que llegan a caer en lo burdo. El principal efecto negativo que genera en los estudiantes este robo intelectual, es que la intencionalidad pedagógica que está detrás de las tareas, trabajos e investigación solicitados a los alumnos para que desarrollen ciertas competencias y habilidades, como son los criterios de búsqueda, distinción entre información relevante y confiable de información poco útil o no válida, identificación de ideas principales, síntesis, reflexión y análisis, entre otros elementos, no se cumple adecuadamente.

Así, la pregunta obvia es: ¿cómo puede y/o proceder el docente cuando comprueba que ha recibido trabajos plagiados? En primer lugar, debe ***detectar*** la acción fraudulenta y, si lo considera pertinente, aplicar una ***sanción*** la cual debe quedar estipulada desde el inicio del curso, o aplicar la normatividad vigente, sí es que ésta existe. Sin embargo, posiblemente lo más importante por hacer sea ***prevenir.***

Como detectar el plagio

Existen numerosos indicativos que nos permiten dudar sobre la autoría de un trabajo presentado como original, entre los que podemos mencionar:

- Tiempos verbales no coincidentes en las oraciones.
- Diferentes estilos narrativos a lo largo del texto.
- Falta de conexión entre las ideas expuestas.
- Empleo de citas literales que no aparecen en las referencias.
- Ausencia de referencias aún cuando se citan varios autores.
- Numeración incorrecta de las imágenes o diagramas.
- Manejo de palabras de uso no común en nuestro entorno (ordenador, fichero, bucle, etc.)

Otro factor a considerar está relacionado con el conocimiento de los alumnos, ya que si bien en ocasiones se encuentran trabajos brillantes que son generados por alumnos sobresalientes, estos mismos trabajos pueden ser presentados por alumnos que no cubren ese perfil.

Si se presenta una sospecha de copia indebida, se recomienda repetir el proceso realizado por los alumnos, es decir, investigar la temática del trabajo con los motores de búsqueda de uso más generalizado en la Internet.

Actualmente existe una forma más cómoda para detectar trabajos copiados, mediante el empleo de un software diseñado para tal fin; entre las aplicaciones más populares de este tipo está ***Turnitin***, que es un programa diseñado por iParadigms a finales de los 90, originalmente para detectar el plagio en el mundo periodístico; la empresa cobra por una licencia anual 850 dólares, más una cuota por estudiante, la cual variará dependiendo del número de alumnos de la institución, requiriéndose cubrir un mínimo de 3,350 dólares, [Turnitin, 2007]. Su funcionamiento se basa en dos componentes: la utilización de una gran base de datos y, más recientemente, la búsqueda en la Internet. En ambos casos, el programa se encarga de buscar paralelismos o coincidencias del trabajo del alumno contra miles de fuentes. Con un funcionamiento similar existen otros programas en el mercado, tales como ***Eve2 (Essay Verification Engine)***, ***CopyCatch***; también los hay de carácter gratuito, pero su uso se destina a buscar plagios en códigos fuente, como son el ***MOSS*** y el ***JPlag*** [Condron, 2001].

La ventaja de tales sistemas reside en la comodidad para detectar los trabajos fraudulentos; sin embargo, también tienen inconvenientes, entre los que destacan:

- La mayoría de estos programas y servicios requieren el pago de una cuota.
- Su base de datos se limita a documentos en lengua inglesa.
- No verifican figuras, gráficos ni imágenes.

Aplicación de sanciones

A pesar de ya no ser tan reciente el problema del plagio electrónico o ciberplagio, las sanciones que muchas veces se tienen contempladas, (inclusive en los reglamentos de las instituciones educativas), aún tienen muchos huecos o ni siquiera están consideradas para este tipo de

situaciones. Sin embargo, se deben establecer medidas punitivas que disuadan al alumno de realizar conductas fraudulentas, considerando que esto no solo se presenta en casos de tareas o investigaciones escolares simples, sino que abarca ámbitos en una gama muy amplia, como serían el plagio de tesis, informes de investigaciones y productos de las mismas, ponencias en eventos académicos y científicos, etc., a todos los niveles.

Prevención

Más que detectar los plagios tenemos que prevenirlos, motivando al alumno a plasmar sus ideas y compartirlas, y enseñándolos a desarrollar las habilidades de análisis y síntesis para plantear propuestas concretas. Para ello es recomendable tomar en cuenta los siguientes puntos:

• ***El estudiante considera a la Internet como el único medio de búsqueda de información.*** Si bien es cierto que en la Internet es posible encontrar revistas, libros, periódicos y ponencias (entre otros muchos materiales), también es cierto que hay una amplía gama de fuentes alternativas para obtener información. Solicitarles que consideren en todas sus investigaciones al menos tres alternativas diferentes, con la libertad de seleccionar aquellas que puedan aportar mejores resultados a la investigación, es una buena manera de orientar a los alumnos a considerar un espectro más amplio de opciones para su investigación.

Algunas fuentes alternativas pueden ser: bancos de tesis en instituciones de educación superior; entrevistas personales con expertos y personalidades que por su experiencia y conocimientos aporten datos significativos; revistas y periódicos no digitalizados; memorias de congresos y foros académicos; programas de radio y televisión, etc., y sobre todas ellas la biblioteca tradicional.

• ***El estudiante considera que los resultados de su búsqueda en la Internet son verdaderos* per se**. Sin duda este es uno de los problemas relacionados con la investigación que se presenta con mayor frecuencia. La gran mayoría de los estudiantes creen que por el hecho de estar en la Internet, toda la información encontrada es válida. Tal y como sucede con otros medios, existen muy buenas referencias con sólido respaldo académico y metodológico, pero también existen páginas sin un sustento académico o de contenido. Por ello, es necesario inducir al estudiante a buscar todas las aristas de un punto de investigación y confrontar posturas, de modo que se pueda llegar a una posición propia a partir del análisis de los documentos encontrados.

• ***En la mayoría de los casos, el estudiante se limita a copiar y a pegar los textos sobre su trabajo con escasa o ninguna lectura analítica y reflexiva sobre su pertinencia.*** Este es un problema derivado de la deficiente formación metodológica, que de ninguna manera es justificable en los niveles medio superior y superior, y mucho menos en el posgrado. Existen dos maneras de abordar este problema; la primera se basa en la naturaleza misma de la tarea o investigación; si el trabajo se plantea en forma cerrada o teórica, mayor será la tendencia a copiar y pegar, ya que el estudiante encontrará textualmente la respuesta al trabajo solicitado. Por el contrario, si la tarea se solicita en un formato abierto tal como un ensayo, caso de estudio o análisis, la cita textual de párrafos pierde relevancia, pues lo que se evalúa es la aportación personal. Una segunda manera consiste en utilizar un formato estandarizado para los reportes de investigación, basándose en las técnicas metodológicas o en estándares internacionales, como el de la American Psychological Association (***APA***). Esto permite que el alumno se acostumbre a trabajar con el rigor científico, que es práctica común en los círculos de investigación.

• ***En términos generales, no se sabe buscar de manera eficiente en la Internet.*** Aunque en términos generales las nuevas generaciones son más diestras en el manejo de los sistemas computacionales, también es cierto que gran parte de las técnicas que se utilizan están basadas en la costumbre; esto se refleja en todos los ámbitos del ser humano, a tal grado que se describe al hombre *como un animal de costumbres*. De este modo, observamos que la mayoría sigue los mismos procedimientos de búsqueda, sin diferenciar tema o profundidad, recurriendo al buscador de moda o al que siempre ha usado. A este respecto, es conveniente capacitar a nuestros alumnos sobre las mejores prácticas de investigación en la Internet, ofreciendo un panorama general de las diferentes alternativas que ofrece el medio, así como enseñarlos a parafrasear las ideas y citar las referencias.

Conclusiones

Hoy en día, para los alumnos es fácil el navegar por la red y obtener información ya digerida y preparada, lo que ha ido generando una cultura del plagio cibernético cada vez más arraigada; los estudiantes pasan el tiempo copiando, reacomodando, combinando, y ajustando todo aquel material que encuentran, para así entregar un trabajo en donde su única aportación es su nombre (en ocasiones ni siquiera el formato). El plagio cibernético se ha vuelto

una adicción tan extendida como cualquier otra, y tan dañino para la sociedad en general porque convierte a gente aparentemente preparada en personas incapaces de responder ante los obstáculos que se le presentan. El problema se agudiza cuando los mismos profesores son quienes utilizan estas prácticas nocivas.

Por ello, la finalidad del presente trabajo es crear conciencia en la comunidad escolar, y en especial en los maestros, acerca de la gravedad que constituye el plagio en la ***WWW*** y de la importancia de llevar a cabo acciones para evitar su permanencia, así como impulsar una modernización del profesorado ante las nuevas tecnologías y sus problemáticas. De igual modo se invita a los estudiantes a mantener una ética computacional, tanto en su desempeño escolar como en su desarrollo extraescolar.

Para obtener más información sobre algunas de las consecuencias legales de estos actos se recomienda consultar la referencia [Téllez, 2005]

Referencias

[Area, 2002] Area, Manuel. (2002). *Sociedad de la Información, tecnologías digitales y educación*. http://www.cse.ull.es/tecedu/misc/temario/tema1/tema1.pdf.

[Baruchson, 2004] Baruchson-Arbib, S. y Yaari, E. (2004). *Printed versus Internet Plagiarism: A Study of Students Perception.* International Journal of Information Ethics, 1 (06/2004). Magazine *on-line*: http://www.ijie.org

[Campuzano, 1992] Campuzano Ruiz, Antonio. (1992). *Tecnologías audiovisuales y educación. Una visión desde la práctica*. Madrid: Akal.

[Condron, 2001] Condron, Frances. (2001). *Plagiarism and the Internet*. http://www.oucs.ox.ac.uk/ltg/reports/plag.html

[Dotinga, 2004] Dotinga, Randy. (2004). *Los espías electrónicos se ocupan de los* copiones (artículo de Wired News en español). http://us.terra.wired.com/wired/tecnologia/0,1157,25947,00.html

[Fernández 2002] Fernández Díaz y Sánchez Camargo (2002*). Conductas científicas censurables: una reflexión ante el plagio*. Universidad de las Américas, Puebla. México.

[Georgetown, 1999] Georgetown University (1999). *What is plagiarism?* http://www.georgetown.edu/honor/plagiarism.html

[Graham, 2003] Graham, Leah and Takis Metaxas, Panagiotis (2003). *Of Course it's True; I Saw It on The La Internet!* Communications of The ACM. Volume 46, Number 5.

[Real, 2001] Real Academia Española (2001). http://www.rae.es.

[Téllez, 2005] Téllez Valdés, Julio (2005). *Derecho Informático*, McGraw-Hill.

[Turnitin, 2007] http://www.turnitin.com/

[Universidad, 2004] Universidad de Palermo (2004). *Código de Ética y Conducta Universitaria*. http://www.palermo.edu.ar/la_up/eticayconducta.html.

University of Luton y CAA. *Technical Review of Plagiarism Detection Software Report*. http://www.jisc.ac.uk/uploaded_documents/luton.pdf

Teoría del Caos en la Protección de Información

M. en C. María Aurora Molina Vilchis ♦
M. en C. Eduardo Vega Alvarado
Dr. Ramón Silva Ortigoza ♣
Profesores del CIDETEC_IPN

En las últimas décadas ha surgido como una nueva corriente para la protección de información la Teoría del Caos. Partiendo del principio de Kerckhoff, en donde se establece que la robustez de un sistema de seguridad criptográfica reside en la dificultad para obtener la clave, entonces los métodos de generación de claves deben poseer ciertas propiedades de aleatoriedad. Para propósitos prácticos se han experimentado diversos métodos que proporcionan secuencias pseudo-aleatorias apropiadas; entre éstos se ubican los mapeos[1] caóticos. En este artículo se presenta el estado del arte de la Teoría del Caos en la generación de dichas secuencias, obtenidas a partir de los mapeos caóticos y sus aplicaciones en los diferentes tipos de protección de información multimedia y en las comunicaciones, especialmente las de espectro disperso.

Introducción

Con el origen de la Teoría del Caos, hace apenas unas tres décadas y con el descubrimiento de la sincronización del caos, se han formulado una gran cantidad de cifradores que de una u otra manera, y en general con poco rigor criptoanalítico, explotan las buenas propiedades de confusión y difusión de las aplicaciones caóticas [1]. Por ello, las señales resultantes de sistemas caóticos son impredecibles en la práctica a mediano y largo plazo, debido a la sensibilidad de las condiciones iniciales y a sus propiedades estadísticas aleatorias a pesar de ser generadas por algoritmos deterministas.

En los sistemas de seguridad de información resulta útil contar con secuencias binarias que puedan aplicarse a procesos que otorguen confidencialidad, privacidad o autenticidad. Para efectos prácticos, dichas secuencias deben cumplir con dos requisitos fundamentales: aleatoriedad e impredictibilidad. Entre las aplicaciones de estas secuencias resaltan las criptográficas, esteganográficas y canales subliminales [1]; su uso ha tenido buena aceptación por las propiedades estadísticas que poseen y su comportamiento *caótico*[2]. Las secuencias pseudo-aleatorias o aproximadamente aleatorias pueden generarse mediante la aplicación recursiva de *mapeos caóticos*.

En este artículo se presenta el estado del arte de las aplicaciones que tiene la Teoría del Caos en la protección de información, específicamente en criptografía, esteganografía y canales subliminales. Este documento consta de cinco secciones. La sección 2 trata de los conceptos fundamentales de la Teoría del Caos. En la sección 3 se detallan los trabajos más representativos para la generación de secuencias pseudo-aleatorias utilizando los principios de la Teoría del Caos. En la sección 4 se tratan los trabajos más relevantes de las aplicaciones de mapeos caóticos en la protección de información. Finalmente, en la sección 5 se presentan las conclusiones.

Teoría del Caos

El primer trabajo relacionado con los sistemas dinámicos fue presentado por el matemático francés Poincaré [3], quien con el estudio del movimiento planetario inventó nuevos métodos topológicos para estudiar soluciones para ciertas ecuaciones diferenciales; en lugar de usar los métodos basados en series, desarrolló el concepto de funciones automórficas, para resolver ecuaciones diferenciales lineales de segundo orden con coeficientes algebraicos, y de esta manera descubrió que las ecuaciones diferenciales admitían soluciones de una complejidad inimaginable hasta ese momento. Con este trabajo se reveló por primera vez que las ecuaciones diferenciales que describen fenómenos naturales

1 Dados dos conjuntos X y Y, el término mapeo significa que, para cada $x \in X$ le corresponde uno y solo un elemento $y \in Y$.

2 El caos en los sistemas se define como "el comportamiento inestable y no periódico de las soluciones de los sistemas dinámicos no lineales y deterministas".

pueden tener soluciones que se comportan en forma "caótica". Sin embargo, éste trabajo tuvo poco interés; a pesar de ello podemos decir que representa el origen de una nueva era para el estudio de las ecuaciones diferenciales.

En 1963 Lorenz [4] publicó un modelo matemático para describir la forma en la que el aire se mueve en la atmósfera terrestre. Observó, que si ocurrían alteraciones mínimas en los valores de las variables iniciales de su modelo primitivo, resultaban patrones climatológicos ampliamente divergentes. Esta sensible dependencia de las condiciones iniciales fue conocida después como el *Efecto Mariposa*[3]; aún cuando las fluctuaciones en las condiciones iniciales o intermedias de un proceso sean muy pequeñas, casi imperceptibles, pueden ser lo suficientemente poderosas como para provocar grandes alteraciones de los estados finales. Con este hecho se inicia el estudio moderno de la dinámica caótica. También dedujo algunas de las propiedades generales del caos como son: la dependencia y sensibilidad a las condiciones iniciales, la existencia de órbitas periódicas densas, los puntos periódicos, el acotamiento de trayectorias y la no linealidad, entre otras. Sin embargo, para los mapeos denominados caóticos, se consideran tres propiedades importantes:

a) Dependencia sensitiva.
b) Transitividad (órbita densa).
c) Conjunto denso de puntos periódicos.

Las propiedades ***a*** y ***b*** corresponden a un comportamiento irregular e impredecible, de aquí que concuerdan con las ideas intuitivas del caos; la propiedad ***c***, sin embargo, parece discrepar de las dos propiedades anteriores, al interpretarse como un comportamiento periódico, regular y predecible. No obstante, estos puntos periódicos son inestables, lo que significa que tan pronto como una órbita se acerca a un punto periódico, esta se empujará lejos en alguna otra parte. Por esta razón, en términos prácticos, el conjunto denso de órbitas periódicas no implica un comportamiento ordenado. Basándose en estas tres propiedades Devaney [2], planteó en 1989 la definición de Caos como sigue:

Sea V un intervalo. Decimos que f: V → V es caótica en V si:

a) *f tiene dependencia sensitiva en las condiciones iniciales,*
b) *f es transitiva y*
c) *los puntos periódicos son densos en V.*

Las tres propiedades se demuestran cuando se presentan una gran cantidad de iteraciones, dando origen al siguiente Teorema:

Si se tiene una función f, tal que:

f: [0,1] → [0,1], para muchas iteraciones *f* es caótica en [0,1].

Secuencias pseudo-aleatorias

En criptografía resulta muy útil contar con secuencias binarias que permitan aplicar procesos de transformación que otorguen confidencialidad, privacidad o autenticidad a la información que se transmite o se almacena. En este sentido, un trabajo muy referido es el realizado por Rueppel [4][5], quien en 1986 mostró la manera de analizar y diseñar secuencias para aplicaciones de cifrado en flujo. En su trabajo, utiliza el cifrador de Vernam como único cifrador incondicionalmente seguro; para que esto sea verdadero, es necesario que la secuencia de la clave sea finita y aleatoria, siendo necesario un algoritmo determinístico para su generación. Las secuencias generadas por este tipo de algoritmos se han catalogado como pseudo aleatorias, las que para usos criptográficos deben guardar ciertas propiedades que las hagan parecer verdaderamente aleatorias. Estas propiedades están contenidas en los llamados postulados de aleatoriedad que formuló Golomb [6] en 1967, los cuales se asocian con la aleatoriedad de secuencias finitas. No obstante, el cumplimiento de estos postulados no implica que una secuencia binaria necesariamente sea impredecible (condición asociada también a las secuencias verdaderamente aleatorias), pero al menos se asegura un comportamiento aleatorio adecuado.

Se define a las secuencias pseudo-aleatorias o ***PN*** (***Pseudo Noise***) como un conjunto de señales binarias periódicas de cierta longitud; para cada periodo la señal puede considerarse que se aproxima a una señal aleatoria (no siéndolo). Existen muchas y muy variadas aplicaciones de las secuencias en campos finitos cuyos términos dependen de forma sencilla de sus predecesores. Una ventaja computacional de estas secuencias reside en su facilidad para ser generadas mediante procedimientos recursivos.

En aplicaciones de comunicaciones un trabajo representativo es [7], donde se describen sistemas en los cuales la energía de la señal es dispersada sobre un gran ancho de banda; de esta manera se consiguen propiedades particulares. Esto proporciona inmunidad en el canal a interferencias intencionales y sin intención. Además de un mayor rechazo al ruido, existe la propiedad

3 Es un concepto que hace referencia a la noción de sensibilidad a las condiciones iniciales de la Teoría del Caos. Su nombre proviene de un antiguo proverbio chino: "el aleteo de las alas de una mariposa se puede sentir al otro lado del mundo".

de minimizar el efecto de propagación multitrayecto y, por supuesto, la posibilidad de comunicaciones con cierto grado de privacidad y de acceso aleatorio. Tanto el sistema de transmisión como el de recepción comparten un código idéntico para conseguir la demodulación y la recuperación de la señal útil. Esta tecnología tiene aplicaciones en telefonía celular, transmisión inalámbrica de datos, redes de comunicaciones personales, redes de computadoras inalámbricas, comunicaciones por satélite, sistemas de prueba y calibración, etc.

Una aplicación de secuencias pseudo-aleatorias para las marcas de agua se presenta en [8], donde se discute la viabilidad de codificar una marca de agua digital indetectable en una imagen estándar en escala de grises de ocho bits. La marca de agua es capaz de contener códigos de autenticación o autorización, o una leyenda esencial para la interpretación de la imagen. Esta capacidad se afronta para encontrar aplicación en una imagen etiquetada, para propósitos de autoría de derechos, protección falsificada, y control de acceso; sin una degradación apreciable en la imagen protegida. También se discuten dos métodos de implementación; el primero basado en la manipulación plana del bit menos significativo (***LSB, Less Significative Bit***), que ofrece decodificación fácil y rápida, y el segundo, que utiliza la suma lineal de la marca de agua a los datos de la imagen, y es más difícil de descifrar, ofreciendo seguridad inherente. En esta misma dirección en [9] se propone la construcción de marcas de agua a través de bloques arbitrarios de imagen al filtrar una secuencia ***PN***, por medio de un esquema de marca de agua para esconder información de derechos de autor en imágenes, empleando para ello un enmascarado visual para garantizar que la marca de agua incluida sea invisible y para aumentar al máximo la robustez de los datos ocultos. La marca de agua se construye para bloques arbitrarios de la imagen filtrándose una secuencia ***PN*** como un número de identificación del autor con un filtro que aproxima la frecuencia que enmascara características del sistema visual. Los resultados experimentales obtenidos en este caso, muestran que la marca de agua es robusta a varias distorsiones que incluyen ruidos blancos y de color; codificación JPEG a calidades diferentes y la segmentación de imágenes.

En el contexto de las comunicaciones inalámbricas, en [10] se hace referencia al uso de distintas capas de abstracción en un modelo de seguridad, una de las cuales considera la utilización de secuencias cifrantes ***PN*** en sistemas de espectro disperso, presentándose como una etapa en el mejoramiento de la protección de información durante su transmisión por el canal.

En los últimos años, se ha trabajado con el uso de secuencias cifrantes, como se describe en [11], en donde se proponen nuevos métodos de generación de verdaderas secuencias aleatorias a través de circuitos lógicos en los FPGA (*Field Programmable Gate Arrays*) y en ASIC (*Application Specific Integrated Circuits*), usando anillos osciladores de Fibonacci y de Galois, las secuencias binarias aleatorias generadas tienen inherentemente una alta velocidad y un índice de entropía muy alto y robusto en comparación con las propuestas anteriores para los generadores digitales de números aleatorios. Así también, se introduce un nuevo método para el post-proceso digital de datos aleatorios, basado en los circuitos lógicos síncronos no-autónomos con retroalimentación, y se presenta una técnica de reloj que controla el registro de desplazamiento de la retroalimentación lineal. El proceso posterior puede proporcionar extracción de aleatoriedad y aumento de la velocidad computacional segura de datos aleatorios de entrada. En la misma tendencia, pero con fines criptoanalíticos [12] propone dos métodos, uno para generar una secuencia pseudo aleatoria y otro para la predicción de la salida de un circuito generador de secuencias a partir de un hardware generador de números aleatorios. También se analiza este método para generar aleatoriedad, y como consecuencia de este análisis, se describe un método de ataque a este generador. Sin embargo, los diseños de hardware para la generación de números aleatorios y su evaluación no han sido tratados frecuentemente en las publicaciones. Esto significa un serio contraste, ya que por un lado está la importancia del hardware de generación de números aleatorios y su evaluación para aplicaciones de seguridad, y por otro lado, se manifiesta el poco interés que este tema ha encontrado en la literatura publicada.

Mapeos Caóticos

Las secuencias pseudo-aleatorias también pueden generarse por la aplicación recursiva de mapeos caóticos. Desde mediados de la década de los 90, se han presentado trabajos relacionados con la aplicación de la teoría del caos a la generación de secuencias cifrantes. Así, en [14] se presenta un esquema de comunicaciones de espectro disperso por salto de frecuencia usando sistemas caóticos. Se hace una descripción de una nueva familia de secuencias de salto en frecuencia generada para estos sistemas; dichas secuencias dan una dispersión uniforme sobre el ancho de banda total de la frecuencia, además de tener buenas propiedades de salto-correlación.

En aplicaciones criptográficas en [16] se aborda el problema de mezclar sistemas caóticos para las comunicaciones seguras con cifradores de flujo, con la mezcla de sistemas generadores de secuencias caóticas como métodos fidedignos para garantizar la confidencialidad; estas mezclas dan como resultado una secuencia que no tiene dependencia con la información cifrada. Los estados de salida generados por éste cifrador se aproximan al máximo teórico para las medidas de complejidad y la longitud del ciclo. Además se hace un análisis de la distribución de la función de entropía para un estado estable, así como de las secuencias de entrada de texto plano.

Un sistema digital caótico de comunicaciones, basado en un esquema *One-Time-Pad*[4] se propone en [19], donde la secuencia aleatoria se sustituye con una secuencia caótica generada por el circuito de Chua. En este sistema, se utilizó una estrategia impulsiva de control para sincronizar dos sistemas caóticos idénticos incluidos en el cifrador y el descifrador. Las longitudes de intervalos impulsivos son seccionalmente constantes, mejorando la seguridad del sistema. En [20] se explora la posibilidad de usar mapeos mezclados al diseño de cajas de sustitución (S-boxes) de acuerdo con Shannon [1], teniendo como expectativa que las propiedades buenas de difusión de tales mapeos serán heredadas por sus aproximaciones, por lo menos si el índice de convergencia es apropiado y las particiones asociadas son suficientemente buenas. En esta misma dirección en [21] se propone el diseño de secuencias binarias basadas en mapeos caóticos unidimensionales, donde se describen métodos simples de diseño de secuencias binarias caóticas con propiedades de autocorrelación exponencial y estadísticas. También emplea fragmentos monótonos unidimensionales sobre los mapeos y una función de umbral simple para generar estas secuencias, mostrando algunos diseños para este propósito.

Adicionalmente, en [22] se propone aplicar y extender los conceptos del exponente de Lyapunov y entropía a transformaciones sobre conjuntos finitos, afirmando que un sistema dinámico a tiempo discreto y con estados finitos es discretamente caótico si su exponente de Lyapunov discreto tiende a un número positivo (0 a ∞) cuando $M \rightarrow \infty$. También se discuten las aplicaciones del caos en criptografía, ya que los sistemas caóticos resultan muy atractivos a investigadores teóricos y prácticos. Recuérdese que en 1949, Shannon propuso este tipo de transformaciones en [23] por lo que no es sorprendente que cuando la Teoría del Caos floreció en las décadas de los años 80 y 90 del siglo pasado, pronto se propusieron varios criptosistemas basados en la discretización de transformaciones caóticas. Así mismo, se intenta formular el concepto de pseudo-caos o caos discreto, proponiendo como primera herramienta para medirlo al exponente de Lyapunov discreto. Adicionalmente en [24] se presenta una comparación entre la criptografía convencional y la caótica con re-inyección de la información (*message embedding*), así como una propuesta para resolver el problema de sincronización en la implementación digital de criptosistemas basados en el caos.

4 Término que empleó Vernam para un sistema criptográfico simple en el que se emplea una secuencia aleatoria de la misma longitud del texto plano.

Conclusiones

A partir del nacimiento de la Teoría del Caos, muchas disciplinas en la ciencia han visto aplicaciones convenientes en diferentes campos; no sorprende que en el terreno de la seguridad de la información tenga gran aceptación, por lo que en las últimas décadas, un gran número de trabajos importantes se han publicado sobre este tema, lo que refleja el gran interés sobre el mismo.

Los mapeos caóticos son la principal aportación que hace la Teoría del Caos a la protección de la información; dichos mapeos generan secuencias pseudo-aleatorias con propiedades estadísticas. Esto los convierte en uno de los mejores métodos para propósitos criptográficos, esteganográficos y de canales subliminales, donde se requieren secuencias cifrantes con muy buenas propiedades de impredictibilidad y aleatoriedad, además de ofrecer baja probabilidad de interceptación, sobre todo en las aplicaciones de canales subliminales.

Agradecimientos

♦ MAMV agradece el apoyo recibido del programa EDD del IPN.

♣ RSO agradece el soporte económico recibido de la Secretaría de Investigación y Posgrado del IPN (SIP-IPN), a través del proyecto 20071024 y del programa EDI, así como del Sistema Nacional de Investigadores (SNI-México).

Referencias

[1] Banks J., Dragan V., Jones A., *Chaos, a Mathematical Introduction,* Cambridge University Press. 2003. Pág. 168.

[2] Devaney R.L., *An Introduction to Chaotic Dynamical Systems*, Addison-Wesley, Redwood

[3] Freedman D. H., *Chaos Theory*, Boston.1998. Pág. 55.

[4] Rueppel, R. A., *Analysis and Design of Stream Ciphers*, Springer Verlag. 1986.

[5] Rueppel R.A.. Stream Ciphers. *Contemporary Cryptology - The Science of Information Integrity*, IEEE Press. 1992.

[6] Menezes, J. A., Van Oorschot, P.C., Vanstone, S.A., *Handbook of Appled Cryptography*, CRC,EUA, 1997.

[7] Simon, M. K., Omura, J. K., Scholtz, R. A. and Levitt, B. K., *Spread Spectrum Communication.* Vol. III, Computer Science Press, Rockville. 1985.

[8] Van Schyndel R.G., Tirkel A.Z., C.F. Osborne. *A Digital Watermark.* International Conference on Image Processing. 1994.

[9] Swanson M. D., Zhu B., Tewfik A. H., *Transparent Robust Image Watermarking.* SPIE Conf. on Visual Communications and Image Proc. 1996.

[10] Schaumont P., Verbauwhede I., *Domain-Specific Codesign for Embedded Security.* IEEE Computer Society, Volume 36, Issue 4. 2003.

[11] Golic J. D., *New Paradigms for Digital Generation and Post-Processing of Random Data.* Access Network and Terminals. Telecom Italia Lab. 2004.

[12] Dichtl M., *How to Predict the Output of a Hardware Random Number Generador.* Siemens AG, Corporate Technology. 2003.

[13] Nokolaidis N., Tsekeridou S., Solachidis V., *Applications of Chaotic Signal Processing Techniques to Multimedia Watermarketing.* Aristotle University of Thessaloniki. 2002.

[14] Cong L. , Songgeng S., *Chaotic Frequency Hopping Sequences.* Nanjing Inst. of Communications. 1998.

[15] Tsekeridou S., Nikolaidis N., Tefas A., *Theoretic Investigation of the Use of Watermark Signals Derived from Bernoulli Chaotic Sequences.* Department of Informatics Aristotle University of Thessaloniki. 2003.

[16] Philip N. S., Babu J., *Chaos for Stream Cipher.* ADCOM 2000, Tata McGraw Hill. 2001.

[17] Tefas A., Nikolaidis A., Pitas I., *Statistical Analysis of Markov Chaotic Sequences for Watermarking Applications.* Department of Informatics, Aristotle University of Thessaloniki. 2001.

[18] Masuda N., Aihara K.. *Cryptosystems With Discretized Chaotic Maps.* IEEE. Fundamental Theory and Applications, Vol. 49, No. 1. 2002.

[19] Li Z., Li K., Wen Ch., and Chai S.Y., *A New Chaotic Secure Communication System.* IEEE Transactions on Communications, Vol. 51, No. 8. 2003.

[20] Szczepanski J., Michalek T., Kocarev L. *Cryptographically Secure Substitutions Based on the Approximation of Mixing Maps.* IEEE Regular Papers, Vol. 52, No. 2. 2005.

[21] Tsuneda A., *Design of Binary Sequences With Tunable Exponential Autocorrelations and Run Statistics Based on One-Dimensional Chaotic Maps.* IEEE Regular Papers, Vol. 52, No. 2. 2005.

[22] Amigó J. M., Szczepanski J., *Caos Discreto y Criptografía*. CIBSI' 05, Valparaíso-Chile. 2005.

[23] Shannon, C. E. *Communication theory of secrecy systems*. Bell Syst. Techn. J., Págs. 656 – 715. 1949.

[24] Amigó J. M., Hernández A., Millérioux G., *Criptografía caótica con reinyección de la información.* CIBSI' 05, Valparaíso-Chile. 2005.

Robots Móviles: Evolución y Estado del Arte

Víctor Ricardo Barrientos Sotelo.
José Rafael García Sánchez.
Dr. Ramón Silva Ortigoza.♣
Profesor del CIDETEC-IPN

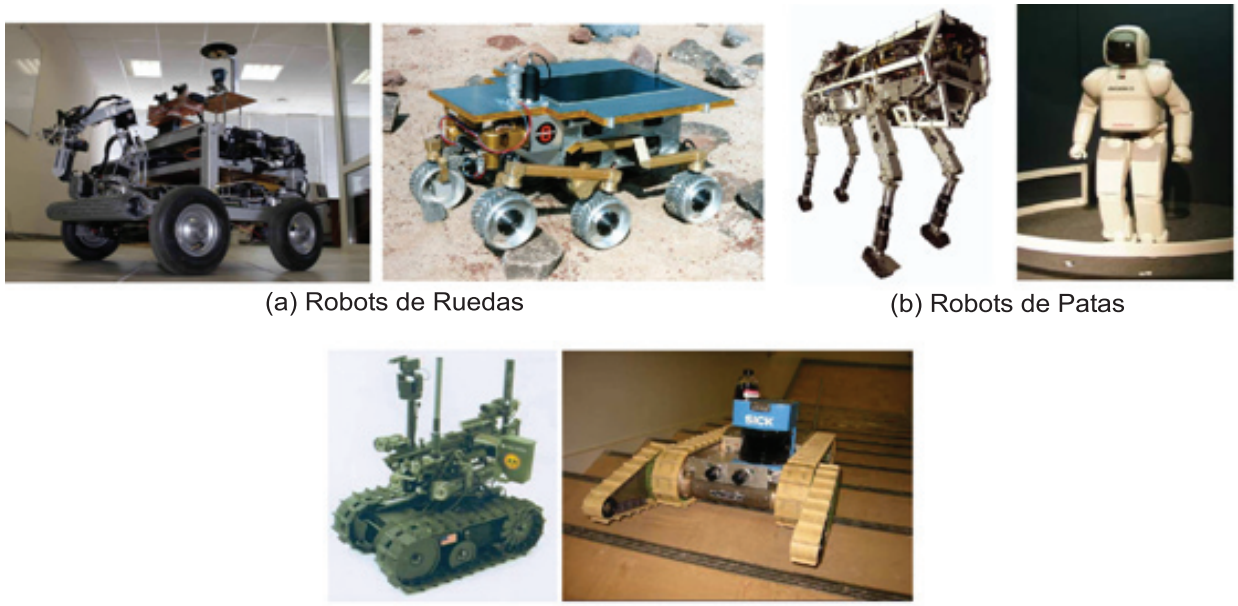
La robótica es una ciencia que ha acompañado al ser humano durante su evolución, compaginándose con nuestra vida cotidiana y brindando un desarrollo vertiginoso en sus distintos campos de aplicación, partiendo desde robots manipuladores, robots de entretenimiento y de servicio, hasta robots móviles. Este trabajo pretende ser una introducción a la robótica móvil. Aquí se abordan tanto una revisión del estado del arte sobre los diversos aspectos a considerar para el diseño de un robot móvil, como los desarrollos más relevantes que han ido aportando las bases del conocimiento en esta rama de la robótica, siempre en la búsqueda de una autonomía total en los robots móviles.

Evolución de la robótica móvil

En civilizaciones antiguas, tales como la griega, se hablaba de seres mecánicos con vida que eran movidos por mecanismos basados en poleas y bombas hidráulicas. Sin embargo, el concepto de robot como tal, comenzó a hilvanarse en la civilización árabe, donde se le dio sentido a dichos mecanismos para confort del ser humano. La robótica nace como ciencia a partir del siglo XX, hacía la década de los cuarenta. Los orígenes de la misma, datan del siglo XVIII con la construcción de autómatas humanoides por Vaucanson y los Jaquet-Droz. Si bien con el paso del tiempo se desarrolló un gran numero de figuras dotadas de partes móviles, fue gracias a la revolución industrial en los albores del siglo XIX (históricamente el hito más importante en el desarrollo de nuevas tecnologías) que se impulsó el crecimiento de las diferentes áreas científicas y la creación de nuevos dispositivos aplicables a distintos rubros (i.e. construcción, milicia, aeronáutica, transporte, etc.), que posteriormente convergieron en la concepción de la robótica. En 1921 el escritor checo Capek, en su obra dramática ***Rossum´s Universal Robots*** (**R.U.R.**), acuñó el término ***robot***, a partir de la palabra checa ***robota***, que significa servidumbre o trabajo forzado. Por su parte, Asimov, introdujo por primera vez el término *robótica* en la historia Runaround de su obra ***I, Robot***, incluyendo en ese mismo trabajo las tres leyes de la robótica. Como consecuencia de los trabajos que hasta entonces se habían realizado, aunado al éxito de las obras mencionadas, la robótica acaparó la atención, no solo de aficionados a la ciencia ficción, sino también de mayor cantidad de investigadores que fueron adentrándose en el estudio de la misma. De esta forma, surgió la necesidad de establecer el concepto de un robot, que puede denotarse como *un sistema electromecánico reprogramable, que permite realizar diferentes tareas repetitivas que requieren un grado elevado de precisión.* Existe toda una gama de formas y aplicaciones para los robots, dependiendo de la tarea que deban realizar; de esta forma se pueden considerar diferentes criterios para su clasificación, como son: su arquitectura, su generación, el nivel de inteligencia, el nivel de control o el nivel de su lenguaje de programación. Dentro de la clasificación por su arquitectura se encuentran los robots móviles, de los cuales a continuación se da una amplia revisión.

A partir de las década de los setenta - setenta, la investigación y diseño de robots móviles creció de manera exponencial; por ejemplo, Nilsson en el SRI desarrolló el robot ***Shakey***, siendo este el primer mecanismo en hacer uso de la inteligencia artificial para controlar sus movimientos. También destacan el ***Newt***, desarrollado por Hollis, y ***Hilare***, desarrollado en el LAAS[1] en Francia. En el Jet Propulsion Laboratory[2] (JPL) se desarrolló el ***Lunar Rover***, diseñado particularmente para la exploración planetaria. A finales de esa década, Moravec desarrolló el ***Stanford Cart***, capaz de seguir una trayectoria delimitada por una línea

1 Acrónimo de Laboratorio de Análisis y Arquitectura de Sistemas.
2 Centro de investigación con sede en EE.UU. y actualmente perteneciente a la NASA.



(a) Robots de Ruedas (b) Robots de Patas

(c) Robots de Orugas

Figura 1: Tipos de locomoción en un robot móvil

establecida en una superficie, en la Universidad de Stanford. En 1983, ***Raibert*** fue desarrollado en el MIT[3], un robot de una sola pata diseñado para estudiar la estabilidad de estos sistemas y brindar un conocimiento más profundo acerca de este tipo de locomoción. A principios de la década de los noventa, Vos et al. desarrollaron un robot "uniciclo" (una sola rueda, similar a la de una bicicleta) en el MIT. Años más tarde, en 1994, el Instituto de Robótica CMU[4] desarrolló a ***Dante II***, un sistema de seis patas cuyo propósito fue tomar muestras de gases en el volcán Spurr, situado en Alaska. En 1996, también en el CMU, se desarrollo el ***Gyrover***, un mecanismo ausente de ruedas y patas, basado en el funcionamiento del giroscopio, por lo que la precisión de sus movimientos y su estabilidad eran muy elevadas. Ese mismo año se desarrolló en el MIT el ***Spring Flamingo***, robot que emulaba el movimiento de un flamingo, diseñado para implementar técnicas eficaces de control en la posición de los actuadores (patas), para describir el movimiento del mismo y para ejecutar diversos algoritmos de desplazamiento. Por su parte, en 1997 la NASA[5] envío a Marte un dispositivo móvil teleoperado llamado ***Sojourner Rover***, dedicado a enviar fotografías del entorno de dicho planeta. Ese mismo año, la empresa japonesa HONDA, dio a conocer el robot ***P3***, el primer humanoide capaz de imitar movimientos humanos. Al siguiente año, en la Universidad Waseda de Japón, se da a conocer el ***WABIAN R-III***, un robot humanoide para fines de investigación sobre el movimiento del cuerpo humano. En 1999 en el CMU, Zeglin propuso un nuevo diseño de robot con una pata llamado ***Bow Leg Hopper***, un diseño que por su naturaleza permite almacenar la energía potencial de la pata, ya que es una articulación de forma curva que al dar cada paso comprime un sistema de resorte y de esta forma el consumo de energía es mínimo, permitiendo un ahorro significativo de la misma. En el 2006, Hollis et al. desarrollaron a ***Ballbot***, un sistema holónomo cuyo movimiento es proporcionado por una esfera ubicada en la parte inferior de la estructura; el control de la esfera, es similar al de un ratón de computadora, empleando encoders para determinar cada posición de la misma. Sin embargo, el estudio de este tipo de robots con una esfera, fue iniciado por Koshiyama y Yamafuji en 1991. Actualmente los robots teleoperados ***Spirit Rover*** y ***Opportunity Rover***, se encuentran explorando la superficie del planeta Marte en busca de mantos acuíferos.

3 Siglas de Massachussets Institute of Technology.

4 Acrónimo de Carnegie Mellon University.

5 Siglas de National Aeronautics and Space Administration.

Estado del arte

Como se ha visto hasta este punto, las aplicaciones de los robots móviles son muy amplias. Otros ejemplos son: exploración minera, exploración planetaria, misiones de búsqueda y rescate de personas, limpieza de desechos peligrosos, automatización de procesos, vigilancia, reconoci-

miento de terreno, asistencia médica, exploración marítima, entretenimiento, investigación y desarrollo, investigación militar, agricultura, inspección, transporte, etc.

Un robot móvil se define como *un sistema electromecánico capaz de desplazarse de manera autónoma sin estar sujeto físicamente a un solo punto. Posee sensores que permiten monitorear a cada momento su posición relativa a su punto de origen y a su punto de destino. Normalmente su control es en lazo cerrado. Su desplazamiento es proporcionado mediante dispositivos de locomoción, tales como ruedas, patas, orugas, etc.*

Los robots móviles se clasifican por el tipo de locomoción utilizado; en general, los tres medios de movimiento son: por ruedas [1], por patas [2] y por orugas [3]. Si bien la locomoción por patas y orugas ha sido ampliamente estudiada, el mayor desarrollo está en los Robots Móviles con Ruedas (***RMR***), esto es debido a las ventajas que presentan las ruedas respecto a las patas y a las orugas. Dentro de los atributos mas relevantes de los RMR, destacan su eficiencia en cuanto a energía en superficies lisas y firmes, a la vez que no causan desgaste en la superficie donde se mueven y requieren un número menor de partes, normalmente menos complejas en comparación con los robots de patas y de orugas, lo que permite que su construcción sea más sencilla. La **Figura 1** muestra los distintos tipos de locomoción.

En lo referente a las partes de las que se compone un RMR, se tiene un arreglo cinemático y un sistema de actuadores, que dotan de movimiento a la estructura cinemática. Ambos sistemas están íntimamente ligados y son dignos de estudiarse en conjunto; no obstante, se ha logrado un mayor avance en el estado del arte al estudiarlos por separado.

Existen diferentes configuraciones cinemáticas para los RMR [4], éstas dependen principalmente de la aplicación hacia donde va enfocado el RMR; no obstante, en general se tienen las siguientes configuraciones: Ackerman, triciclo clásico, tracción diferencial, skid steer, síncrona y tracción omnidireccional, véase la **Figura 2**.

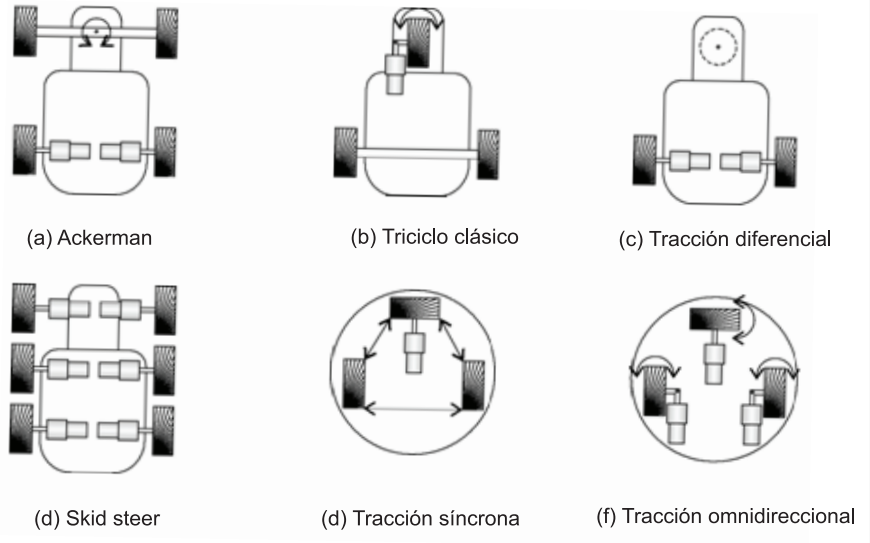


Figura 2: Configuraciones de los RMR

Dependiendo de su configuración cinemática, los RMR utilizan cuatro tipos de ruedas para locomoción [5], estas son: omnidireccionales, convencionales, tipo castor y ruedas de bolas, véase la **Figura 3**. Con el objeto de hacer más tratable el problema del modelado en las configuraciones cinemáticas, se suelen establecer algunas suposiciones de diseño y de operación. Dentro de las suposiciones de diseño generalmente se toman tres; la primera va dirigida a considerar que las partes dinámicas del RMR son insignificantes i.e., que no contiene partes flexibles, de esta manera pueden aplicarse mecanismos de cuerpo rígido para el modelado cinemático. La segunda limita que la rueda tenga a lo más un eslabón de dirección, con la finalidad de reducir la complejidad del modelado. La tercera es asumir que todos los ejes de dirección son perpendiculares a la superficie, de esta manera se reducen todos los movimientos a un solo plano. Por otra parte, respecto a las suposiciones de operación, al igual que en las de diseño, se toman tres. Una de ellas descarta toda irregularidad de la superficie donde se mueve el RMR. Otra, considera que la fricción de traslación en el punto de contacto de la rueda con la superficie donde se mueve, es lo suficientemente grande para que no exista un desplazamiento de traslación del móvil. Como complemento a lo anterior, una tercera suposición de operación establece que la fricción rotacional en el punto de contacto de la rueda con la superficie donde se mueve, es lo suficientemente pequeña para que exista un desplazamiento rotatorio.

Relativo a los actuadores utilizados para dotar de movimiento a los RMR, es común que se utilicen motores. Existe una gama bastante amplia dependiendo de su empleo; los más utilizados en la robótica móvil son los motores de corriente directa (CD), por el argumento de

Figura 3: Tipos de Ruedas

que su modelo es lineal, lo que facilita enormemente su control, y específicamente los de imán permanente debido a que el voltaje de control es aplicado al circuito de armadura y el circuito de campo es excitado de manera independiente. Hablando de motores de CD de imán permanente, se tienen dos tipos: con escobillas y sin escobillas. Ambos tipos de motores brindan ventajas semejantes, sin embargo, los motores sin escobillas tienen algunas ventajas significativas sobre los motores con escobillas, como por ejemplo: a) al no contar con escobillas, no se requiere el reemplazo de estas ni mantenimiento por residuos originados de las mismas, b) no presentan chispas que las escobillas generan, de esta forma se pueden considerar más seguros en ambientes con vapores o líquidos flamables, c) la interferencia causada por la conmutación mecánica de las escobillas se minimiza considerablemente mediante una conmutación electrónica, d) los motores sin escobillas alcanzan velocidades de hasta 50,000 rpm comparadas con las 5,000 rpm máximas de los motores con escobillas. A pesar de que estas ventajas parecieran inclinar la balanza a favor de los motores sin escobillas, existen desventajas cruciales que pueden cambiar la tendencia: a) en los motores sin escobillas no se puede invertir el sentido de giro cambiando la polaridad de sus terminales, esto agrega complejidad y costo a su manejo, b) los motores sin escobillas son mas caros, c) se requiere un sistema adicional para la conmutación electrónica, d) el controlador de movimiento para un motor sin escobillas es mas costoso y complejo que el de su equivalente con escobillas.

Dentro de la robótica móvil, los factores más importantes e imperativos a considerar, son los concernientes al posicionamiento, seguimiento de trayectoria y evasión de obstáculos. Respecto a esto, se han llevado a cabo diversas investigaciones cuyos resultados han permitido un avance significativo pero no total en estos 3 aspectos. Algunos trabajos que han contribuido de manera importante a estos puntos, se mencionan en los siguientes párrafos.

Acerca del posicionamiento se han llevado a cabo distintos análisis empleando sensores ultrasónicos para la navegación de los robots. Por ejemplo en [6], se presentan distintos métodos para la implementación de sensores que permitan al robot móvil conocer su posición dentro del ambiente de trabajo, estudiando los distintos tipos de sensores y abarcando el problema de posicionamiento en forma general. De igual forma, en [7] se aborda el problema de estimación del posicionamiento de un robot móvil, mediante la cuantificacion de errores de odometría[6] de tipo sistemáticos. En [8] se integran dos métodos de mapeo para la navegación de un robot dentro de un ambiente cerrado y estructurado, mapeo enrejado bidimensional y mapeo topológico, logrando una mayor precisión y eficiencia en el desplazamiento del robot.

Respecto al seguimiento de trayectoria, se propone en [9], un esquema de control para un robot móvil tipo trailer multiarticulado para abordar el seguimiento de trayectorias, integrado por tres diferentes leyes que proporcionan al sistema la capacidad de seguir trayectorias en forma global. En [10], para el seguimiento de trayectoria, se propone una estrategia de control jerarquizada en dos niveles, un lazo interno compuesto por un controlador PID asociado a los motores del robot y

6 Medida de la posición de un robot móvil de forma relativa en base a un origen en el plano cartesiano, emplea encoders para calcular la rotación y orientación de las ruedas.

un lazo externo asociado al modelo cinemático del robot que se encarga de generar los perfiles de velocidad para cada motor, considerando la inductancia de cada uno igual a cero. En [11] se realiza el seguimiento guiado por los movimientos del ojo dentro de su orbita (electrooculografía) brindando la ventaja de ser fácilmente operado por personas con discapacidades físicas.

En lo que respecta a la evasión de obstáculos, existen distintos métodos para llevar a cabo esta tarea. Los más relevantes son: por detección de bordes [12], por descomposición en celdas [13], construcción de mapas [14] y campos potenciales [15]. En el método por detección de bordes, el algoritmo implementado permite que el robot detecte los bordes verticales de un posible obstáculo. El método por descomposición en celdas, divide en celdas el espacio de trabajo del robot en un plano bidimensional, a cada celda se le asigna un valor que permite saber si existe dentro de la misma algún obstáculo. En el método por construcción de mapas, el algoritmo implementado permite crear un grafo que conecta cada punto del espacio libre de trabajo (espacio libre se refiere al espacio de trabajo en el que la incidencia de obstáculos es nula), facilitando la generación de un camino que permita al robot navegar desde su punto inicial a su punto final eliminando la incertidumbre de posibles obstáculos. Respecto al método de campos potenciales artificiales, fue desarrollado por Khatib y se supone al móvil como una partícula puntual y de igual forma, los obstáculos que lo rodean se consideran como partículas que ejercen una fuerza de repulsión sobre el móvil, mientras que, su punto de arribo, es una fuerza atractiva, consiguiéndose de esta forma establecer un campo potencial que representa el ambiente en el que debe de seguir su trayectoria el robot.

Los resultados que se han reportado en la literatura, sugieren un avance significativo y sólido en la búsqueda de la autónomia. No obstante, continua latente un amplio margen en la investigación de la robótica móvil, que se ira reduciendo paulatinamente mientras nuevos estudios se vayan sucediendo.

Conclusiones

Desafortunadamente en México, la investigación en robótica no ha tenido suficiente apoyo y muchos de los desarrollos se estancan tan solo en el diseño y a lo más en la construcción de prototipos. Sin embargo, a nivel internacional los logros han sido impresionantes, teniendo como principal exponente a Japón, país en donde se pueden encontrar diversos tipos de robots incorporados totalmente a la vida cotidiana, entre los que se pueden mencionar androides con capacidades de movimiento y comportamiento inimaginables, robots de servicio y soporte a personas discapacitadas, además de las plantas industriales totalmente automatizadas en donde la intervención humana es casi nula, solo por mencionar algunos. Por otro lado, no menos importantes, institutos de investigación tales como el CMU, el MIT, la NASA, etc. han logrado una importante autónomía en plataformas móviles y en configuraciones alternas como los robots de péndulo invertido, robots con una sola rueda, robots balanceados en una esfera, robots con patas y robots modulares, entre otros. De esta manera, al poseer un vasto campo de aplicación, la robótica móvil continua en pleno desarrollo, cuya única limitante de crecimiento es la imaginación.

Agradecimientos

♣ RSO agradece el soporte económico recibido de la Secretaría de Investigación y Posgrado del IPN (SIP-IPN), a través del proyecto 20071024 y del programa EDI, así como del Sistema Nacional de Investigadores (SNI-México).

Referencias

[1] P. F. Muir and C. P. Neuman, "Kinematic modeling of wheeled mobile robots", *Journal of Robotic Systems,* vol. 3, pp. 281-340, 1987.

[2] M. H. Raibert, H. Brown, M. Chepponis, E. Hastings, J. Koechling, K. N. Murphy, S. S. Murthy and A. Stentz, "Dynamically stable legged locomotion", Robotics Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU-RI-TR-83-20, 1983.

[3] T. Iwamoto, H. Yamamoto and K. Honma, "Transformable crawler mechanism with adaptability to terrain variations", in *Proc. 1983 International Conference on Advanced Robotics Conf.,* Tokyo, Japan, pp. 285-292.

[4] A. Bano Azcon, "Análisis y diseño del control de posición de un robot móvil con tracción diferencial", Tesis profesional, LEscola Tecnica Superior dEnginyeria (ETSE) de la Universitat de Valencia, 2003.

[5] K. Goris," Autonomous mobile robot mechanical design", These elektrotechnisch ingenieur, Vrije Universiteit Brussel, 2005.

[6] J. Borenstein, H. R. Everett and L. Feng, "Where am I? sensors

and methods for mobile robot positioning", *The University of Michigan,* April 1996.

[7] J. Borenstein and L. Feng. "UMBmark: A benchmark test for measuring odometry errors in mobile robots", *SPIE Conference on Mobile Robots,* Philadelphia, October 22-26, 1995.

[8] A. Bucken and S. Thrun, "Learning maps for indoor mobile robot navigation", *Carnegie Mellon University,* Pittsburgh, April 1996.

[9] J. M. Albarran Jimenez. "Diseño, construcción y control de un robot móvil multiarticulado", Tesis de Doctorado, Departamento de Ingeniera Eléctrica, Sección Mecatrónica, CINVESTAV, Mexico, 2003.

[10] T. Salgado Jimenez. "Diseño, construcción y control en tiempo real de un robot móvil", Tesis de Maestría, Departamento de Ingeniera Eléctrica, Sección Mecatrónica, CINVESTAV, Mexico, 1999.

[11] R. Barea, L. Boquete, M. Mazo, E. Lopez, L.M. Bergasa. "Guiado de robots móviles utilizando electro-oculografia", Universidad de Alcalá,Madrid España.

[12] J. L. Crowley. "World modeling and position estimation for a mobile robot using ultrasonic rangin", *IEEE International Conference on Robotics and Automation,* Scottsdale, Arizona, pp. 674-680, May 14-198, 1989.

[13] J. T. Schwartz and M. Sharir. "On the piano movers problem: II. General technique for computing topological properties of real algebraic manifolds", *Advanced in applied Mathematics,* Vol. 1, No. 4, pp. 293-351.

[14] N. Nilsson. "A mobile automaton: an application of artificial intelligence techniques"., *Proceedings of the International Joint Conference on Artificial Intelligence,* pp. 509-520, 1969.

[15] O. Khatib. "Real-Time obstacle avoidance for manipulators and mobile robots", *IEEE International Conference on Robotics and Automation,* St. Louis, pp. 500-505 March 25-28, 1985.

Introducción a las Redes CAN 1a. Parte

Ing. Jesús Pimentel Cruz
Ing. Patricia Pérez Romero
Profesores del CIDETEC-IPN

Este artículo se presenta como el primero de una serie de trabajos sobre el protocolo ***CAN*** (***Controller Area Network***), los cuales abarcaran desde los aspectos básicos en dicho protocolo hasta su implementación y comunicación en dos tarjetas de hardware, las cuales están diseñadas con microcontroladores *PIC* y *AVR*.

Longitud del Bus	Velocidad en Bits/seg	Tiempo Máximo de Transmisión
Hasta 25 mts.	1Mbit/s	129 μs
Hasta 100 mts.	500 Kbit/s	258 μs
Hasta 500 mts.	125 Kbit/s	1032 μs
Hasta 1000 mts.	50 Kbit/s	2580 μs
Mensaje para CAN2 de 129 bits de longitud		

Tabla 1

Introducción

El sistema CAN consta de un mecanismo de comunicación serial multiplexado, en el cual la entrega a tiempo de un mensaje es mucho más importante que el ancho de banda; las redes que trabajan con CAN lo hacen a diferentes velocidades, considerando una serie de recomendaciones practicas, tal comose indica en la **Tabla 1**. Este tipo de redes se utilizan para trabajo en ambientes muy hostiles, destacándose por ser muy robustas y seguras; originalmente fueron desarrolladas por el consorcio alemán BOSH GmbH para el intercambio de información en tiempo real entre piezas automotrices, con el objetivo de conseguir automóviles más seguros y confiables, al mismo tiempo que tuvieran una eficiencia mayor en el consumo de combustible y un menor peso. Actualmente, esta tecnología se utiliza ampliamente en la industria automovilística, pero sus aplicaciones se están extendiendo rápidamente a otros mercados, como son la industria eléctrica ó aquellos procesos de transformación con alta posibilidad de fallas críticas.La existencia de un estándar del *bus* CAN a nivel mundial posibilita que unidades de control de diferentes fabricantes se puedan comunicar entre si.

Generalidades del Bus CAN

La funcionalidad específica del Bus CAN se puede interpretar, en términos del modelo OSI, como un protocolo de dos capas, mostrado en la **Figura 1.**

• Capa Física: se usa generalmente para implementar redes CAN en una línea de bus con dos cables de conducción diferenciados.

• Control de Acceso al Medio: se contemplan tramas y arbitrajes, corrección de errores, detección y bandera de error.

• Control de Enlace Lógico: incluye aspectos de transferencia de datos, petición remota, filtrado de mensajes, notificación de sobrecarga y recuperación.

Se tiene acceso al bus serial multimaestro con un esquema CSMA/CD, (*Carrier Sense Multiple Access / Collision Detection*, Acceso Múltiple con Detección de Portadora/Detección de Colisiones) por lo que es posible que varios nodos intenten transmitir al mismo tiempo en cualquier momento, y por lo mismo se pueden dar colisiones entre mensajes simultáneos; sin embargo, cada mensaje lleva una identificación que establece su prioridad, obteniendo el acceso al bus el de mayor jerarquía, mientras que los de menor nivel esperan a que el bus se encuentre libre, mediante un arbitraje de Bus (*Bus Arbitration*).

El Bus CAN es un protocolo con prioridad al mensaje y no a la dirección; esto significa que los participantes no tienen una dirección y el mensaje se envía a todos los nodos de la red CAN. Son estos nodos los que deciden, con base en una identi-

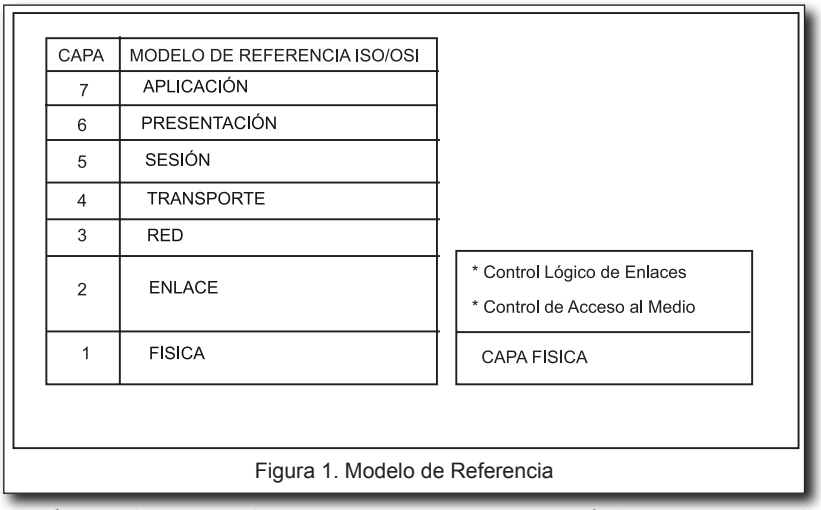


Figura 1. Modelo de Referencia

ficación, si el mensaje les sirve para procesarlo o lo desechan; así, si un nodo envía un mensaje, dicho mensaje no incluye un campo de nodo destino, dado que todos los nodos escuchan el canal, y en un momento dado varios de ellos pueden aceptar la transmisión. Las identificaciones las asigna el usuario CAN según lo crea conveniente, teniendo que cumplir algunas reglas, como la de que dos nodos no pueden transmitir con la misma identificación.

Trama de Datos

Los mensajes CAN constan de celdas donde se envían datos e información de acuerdo a las especificaciones que marca el protocolo; ver **Figura 2**, el formato del paquete incluye los campos siguientes:

• SOF (*Start of Frame*, Inicio de Trama), inicio de trama, consta de un bit siempre dominante, que indica el inicio del mensaje.

• Arbitraje, este campo es el que concede prioridad a un mensaje o a otro (dominante o recesivo); en el formato estándar tiene once bits de identificación, seguidos del bit RTR (*Remote Transmisión Request*, Petición de Transmisión Remota), que en este caso será dominante. En el formato extendido son los once bits de identificación base y dieciocho bits adicionales, y el bit SRR (*Subsitute Remote Request*, Petición de Sustituto Remoto) sustituye al RTR, siendo *recesivo.* Ver **Figura 3**.

• Campo de Control.- Este grupo está formado por dos bits reservados y cuatro bits adicionales que indican el numero de bytes de datos; el primero de estos bits, r1 (IDE, *Identifier Extension*, Extensión de Identificación) se utiliza para indicar si la trama es estándar (IDE dominante) o extendida (IDE recesivo), el segundo de estos, r0, es siempre recesivo. Los cuatro bit del DLC (*Data Length Code*, Código de Longitud de Datos), indican, en binario, el número de bytes de datos en el mensaje.

• CRC (*Cyclic Redundance Code*, Código de Redundancia Cíclica), el código de esta celda, se utiliza para verificar si se han producido errores.

• ACK (*Acknowledge,* Reconocimento) este campo de dos bits (*SLOT,* Ranura *y Delimiter,* Delimitador*)* indica si el mensaje ha sido recibido correctamente. El nodo transmisor envía los dos bits como recesivos, mientras que el nodo que lo reciba contestará enviando un bit dominante en el campo SLOT si ha recibido de manera correcta un mensaje válido.

Figura 2 Trama de Datos

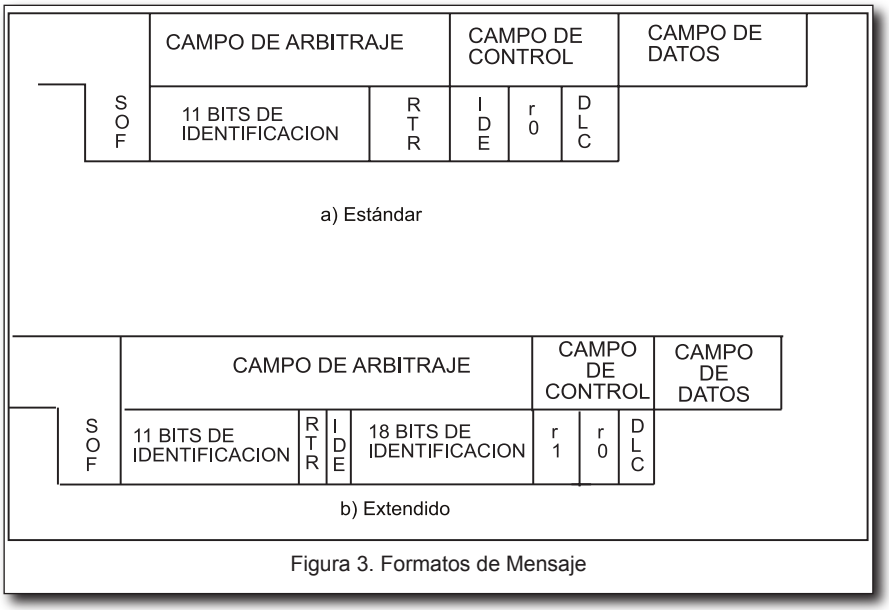


Figura 3. Formatos de Mensaje

• EOF (*End of Frame*, Fin de trama), consiste en una bandera de siete bits recesivos, en forma sucesiva, que indican el final de la trama.

• IFS (*InterFrame Space*, Espacio entre Tramas), esta consta de al menos tres bits recesivos, y durante su vigencia ningún nodo tendrá permiso para iniciar transmisiones.

Trama Remota

Los nodos pueden requerir información de otros nodos, por ello, si alguno realiza una petición en este sentido, el nodo que tiene la información envía un mensaje con la repuesta, misma que puede ser recibida por quien la solicitó y por cualquier otro nodo interesado.

El mensaje de petición remota tiene el formato que se muestra en la **Figura 4**. Este tipo de mensajes se envían con una trama que incluye la identificación del nodo requerido, a diferencia con los mensajes de datos, el bit RTR toma valor recesivo y no hay campo de datos. En el caso de que se envíe un mensaje de datos y de petición remota con la misma identificación, la trama de datos ganará el acceso al bus, ya que su RTR tiene valor dominante.

Trama de Error

Esta trama, mostrada en la **Figura 5**, es generada por cualquier nodo que detecte un error, y consiste de dos campos: indicación de de error (*error flag*) y delimitador de error (*error delimiter*), el cual consta de ocho bits recesivos continuos y permite a los nodos reiniciar la comunicación tras el error.; la indicación va a depender del estado de error del nodo que detecte dicha condición.

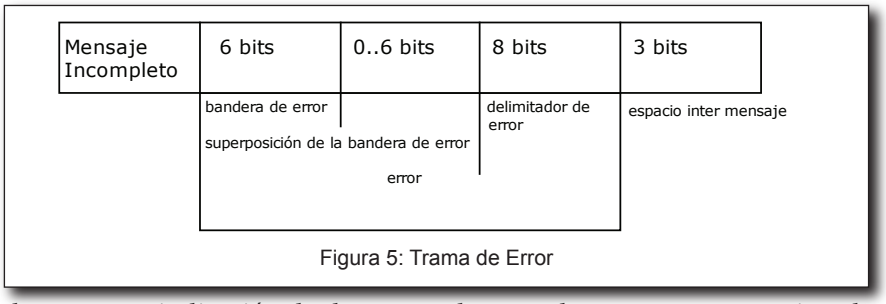


Figura 5: Trama de Error

Si un nodo en estado de error *Activo* detecta otro error en el bus, interrumpe la comunicación del mensaje en proceso, generando un nuevo mensaje de error activo, que consiste en una secuencia de seis bits dominantes sucesivos. Esta secuencia no cumple con la regla de relleno de bits y genera la trama de error en otros nodos, por lo tanto el error puede extenderse de seis a doce bits dominantes sucesivos. Se espera la llegada de un campo de limitación de error formado por los ocho bits recesivos, entonces la comunicación se reinicia y el nodo que había sido interrumpido comienza nuevamente la transmisión del mensaje.

Si un nodo en estado *pasivo* detecta un error, el nodo transmite un indicador de error pasivo, seguido nuevamente por el campo delimitador de errores. El indicador de error de tipo pasivo consiste de seis bits recesivos seguidos y por lo tanto la trama para este tipo de nodos es de catorce bits recesivos; por ello, la trama de error de tipo pasivo no afecta a nodo alguno en la red, excepto cuando el error es detectado por el mismo nodo que ésta transmitiendo. En este caso, los demás nodos detectan una violación a las reglas de relleno y transmitirán a la vez una trama de error.

El relleno de bits consiste en que cada cinco bits de igual valor se introduce uno de valor inverso. Al ser señalada una trama de error de la forma apropiada, cada nodo transmite bits recesivos

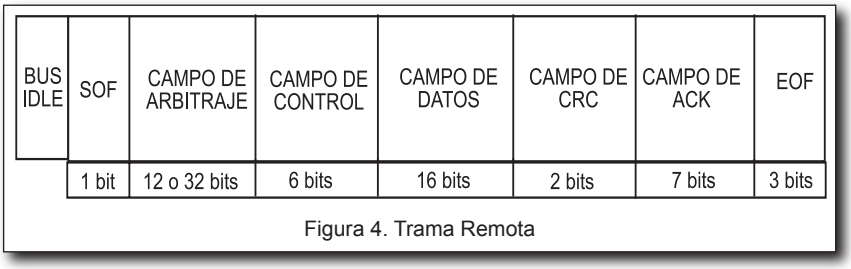


Figura 4. Trama Remota

Implementación de controladores CAN

Existen tres tipos de arquitecturas en microcontroladores: Controlador CAN Autónomo (*Stand-Alone CAN Controller)*, Controlador CAN Integrado (*Integrated CAN Controller)* y Nodo CAN de Circuito Único (*Single-Chip CAN Node)*.

Controlador CAN Autónomo

Es la arquitectura más simple, para llevar a cabo una comunicación en una red CAN se requiere:

1. Un microcontrolador.

2. Un controlador CAN para introducir el protocolo, el filtro de mensajes y todo lo necesario para las comunicaciones. Un ejemplo es el dispositivo MCP2510.

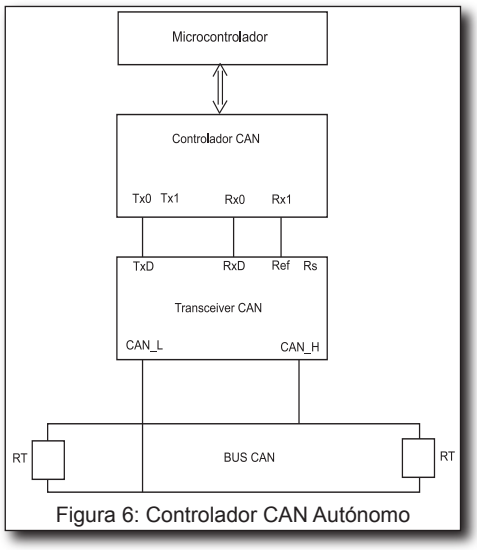


Figura 6: Controlador CAN Autónomo

3. Un transceiver CAN, esto es, un transmisor/receptor; por ejemplo, el MCP2551 desarrollado por Microchip. **Figura 6**.

Controlador CAN Integrado

Este tipo de arquitectura consiste en un microcontrolador que incluya, no sólo sus características propias sino además un módulo con la funcionalidad de un microcontrolador CAN. El transceiver se sitúa de manera separada como se puede observar en **Figura 7**.

Nodo CAN en un solo Circuito

Se trata de un chip que incluye en su interior los tres elementos necesarios para llevar a cabo las comunicaciones en un entorno CAN, ver Figura 8.

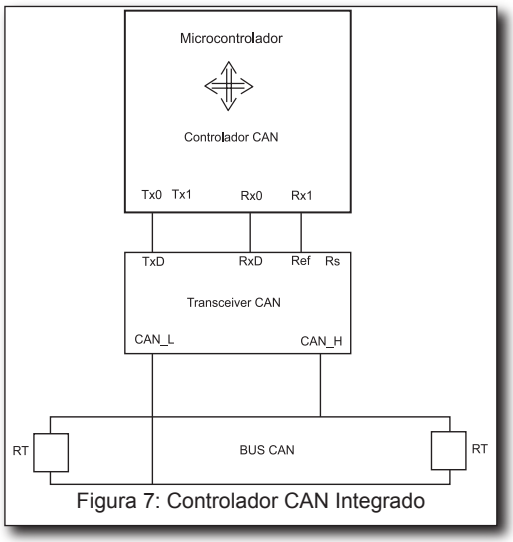


Figura 7: Controlador CAN Integrado

Bibliografía:

[1] Pfeiffer Ayre, Olaf; Keydel, Christian. *Embedded Networking*.RTC Books.

[2] Bosch GmbH, Robert. *CAN Specification version 2.0*

[3] Chamú Morales, Carlos Antonio. *Desarrollo de un sistema educativo para la enseñanza del protocolo de comunicaciones CAN.* Universidad Tecnológica de la Mixteca.

[4] Etschberger, Konrad. Controller Area Network: *Basics Protocols, Chips and Applications*; IXXAT Automotion GmbH.

[5] Lawrenz, Wolfhard. *CAN System Engineerin: From Theory to Practical Applications*. Springer

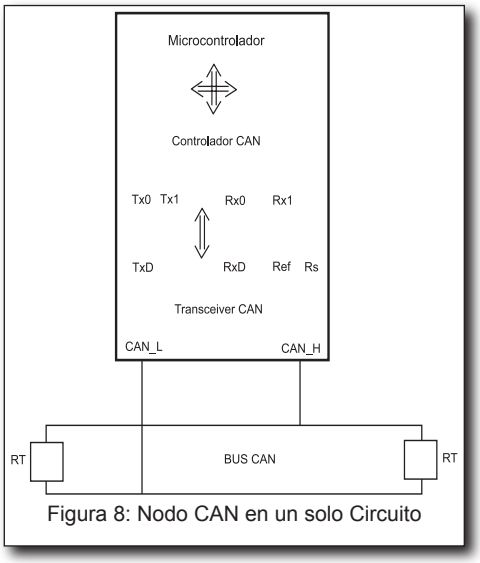


Figura 8: Nodo CAN en un solo Circuito

La Visión Artificial en la Robótica

Ing. Rogelio Rojas Hernández
UPIITA
Dr. Ramón Silva Ortigoza ♣
M. en C. María Aurora Molina Vilchis. ♦
Profesores del CIDETEC

El vertiginoso avance de las computadoras ha permitido que la visión artificial se incorpore a una gran cantidad de disciplinas, apoyando e incluso sustituyendo a los sistemas que antaño se utilizaban. Este trabajo tiene como finalidad presentar un panorama general de las bases, trabajos, proyectos y avances sobre la visión artificial en aplicaciones de robótica.

Introducción

Con la cantidad de información disponible actualmente, no es de extrañar el enorme número de referencias sobre robots a la que una persona puede acceder (basta teclear *robot* en el popular buscador Google y se obtendrán mas de 78 millones de enlaces). Sin embargo, pocas veces alguien puede explicar lo que verdaderamente son estos artefactos en el mundo real.

La palabra ***robot*** viene del vocablo checo *robota*, que significa "servidumbre", "trabajo forzado" o "esclavitud"; el término fue utilizado por primera vez por Karel Capek en su novela ***R.U.R***. (*Rossum's Universal Robots*). Fue un científico y divulgador de la ciencia, Isaac Asimov, quien introdujo por primera vez el término robótica con el sentido de disciplina científica encargada de construir y programar robots [1]; pero en definitiva no fue la comunidad científica y académica la que difundió de forma masiva este concepto.

Hollywood, como industria cinematográfica, ha hecho una gran labor en cuanto a la divulgación de la idea de un robot. La amplia filmografía realizada recurriendo a este tema proporciona una imagen mental de lo que son estos artefactos. Así pues, cualquiera sabe quienes son *C3PO* o *R2D2* (curiosamente mexicanizado como Arturito) e identifica claramente que son robots (ver la **Figura 1**).

Figura 1: C3PO y R2D2, robots emblemáticos de nuestra cultura.

Estos robots imaginarios están aún lejanos de lo que realmente existe, pero nos dan la idea de lo que es un robot; aunque ésta no es estrictamente correcta, es una idea al fin, que es lo importante. Afinar esta imagen mental y convertirla en un concepto general y universal es bastante complicado; lo cierto es que aún no nos hemos puesto de acuerdo del todo.

En este artículo se presenta un panorama de los elementos, desarrollo y aplicaciones de la visión artificial, específicamente en el campo de la robótica. El documento consta de seis secciones; en la Sección 2 se define lo que se puede calificar como un robot. En la Sección 3 se introduce al lector a las posibilidades de interacción con las que puede contar un robot. En la Sección 4 se detallan los conceptos fundamentales de la visión artificial. En la Sección 5 se tratan los trabajos más relevantes sobre la aplicación de la visión artificial en robótica y, finalmente, en la Sección 6 se presentan las conclusiones.

Definiendo un robot

Existen suficientes definiciones como para llenar una biblioteca entera, pero tomando una de las más aceptadas se considera que los robots son dispositivos mecánicos capaces de realizar tareas

(a) Androide (b) Móvil (c) Zoomórfico (d) Poliarticulado

Figura 2: Distintas Formas de Robot

que podrían desempeñar los seres humanos. Bajo esta definición, las máquinas que intervienen en una cadena de ensamblaje de automóviles son robots, aun cuando no son muy inteligentes en apariencia; hoy en día a estas máquinas las llamamos robots industriales.

Desde inicios de la década de los 90 y dependiendo del país, han aparecido con rapidez nuevos robots más inteligentes. A estos se les ha dotado de capacidades perceptivas (vista, oído y tacto principalmente), aunque reducidas en comparación con las capacidades de los seres vivos. Estas nuevas máquinas, que en apariencia son más inteligentes y que se suelen adaptar a entornos cotidianos, se denominan por lo general robots de servicio o robots inteligentes. Pero al analizarlos cuidadosamente, muchos robots de servicio no son tan inteligentes como parecen, e inclusive existen robots industriales desarrollados años atrás, que realizan tareas mucho más complicadas.

Como sociedad, ¿que es un robot?

Habitualmente se debate sobre que máquina es un robot y cual no lo es, porque realmente es complicado llegar a un acuerdo cuando el tema es tratado por el público general. La batidora, un electrodoméstico común, realiza una función que puede llevarse a cabo por un ser humano, y siguiendo estrictamente la definición, la batidora es un robot aún cuando no sea más que una herramienta eléctrica. De hecho, se pueden encontrar a la venta robots de cocina cuya única capacidad es triturar alimento.

También existen ejemplos de máquinas que se transforman en robots; un automóvil es una máquina, así está definido hoy en día [2]. Sin embargo, al combinarlo con un sistema informático, electrónico y mecánico que lo controle y le permita llegar a un destino sin la intervención de un ser humano, se convierte en un robot. Evidentemente, en las sociedades mas desarrolladas tecnológicamente, una batidora no se considera un robot, si se le compara con los robots de última generación que se conocen. En realidad, se trata de un problema de contraste social; en el año 1985 nadie ponía en duda que una batidora fuera un robot de cocina y ahora resulta increíble decir que tanto una batidora como un humanoide son robots. Quizás en el año 2030 el conductor robotizado de un auto sea tan poco llamativo para el público como una batidora en el presente.

Lo más curioso de esta discusión es que no podemos definir a conciencia lo que es un robot, pero si los hemos clasificado en cuatro formas, básicamente diferenciados por sus capacidades [3].

1. Androides: son robots que imitan la forma y comportamiento humano; suelen ser solo de experimentación, pero existen a la venta modelos cuya función es ser juguete o una mascota. La principal limitante de este modelo es la implementación del equilibrio a la hora del desplazamiento, pues es bípedo (ver la **Figura 2(a)**).

2. Móviles: se desplazan mediante una plataforma rodante (ruedas u orugas); estos robots aseguran el transporte de piezas de un punto a otro (ver la **Figura 2(b)**).

3. Zoomórficos: logran la locomoción imitando a los animales. Estos robots son utilizados en ambientes específicos, tales como el estudio de volcanes o la exploración espacial (ver la **Figura 2(c)**).

4. Poliarticulados: suelen imitar un brazo humano, con algunas variantes y/o limitantes. Su utilidad es principalmente industrial, para desplazar elementos que requieren fuerza y cuidado en su manejo (ver la **Figura 2(d)**).

Los sentidos de un robot

En un ser humano, un sentido es una fuente de información sobre el mundo que lo rodea, para que en base a dicha información el cerebro tome una decisión. Los sentidos proveen datos sobre temperatura, luz, sonido, fuerza, olor, sabor, etc.; vista, tacto, oído, gusto y olfato son los sentidos que tradicionalmente se asocian a una persona, aunque popularmente se acepta la existencia de otros sentidos como la empatía, la telepatía y otras clases de percepción extrasensorial.

Extrapolando la misma idea a los robots, ya se dispone de la tecnología para dotarlos de tales sentidos, mediante el uso de computadoras que sustituyen al cerebro, y micrófonos, cámaras, sensores, etc. que sustituyen a los ojos, la piel, los oídos, la lengua y la nariz. En general, resulta demasiado costoso e impráctico para los proyectos que se requieren y/o desarrollan dotar a un robot con los mismos sentidos con los que cuenta un ser humano; estas condiciones se presentan debido a lo corto que suelen ser los tiempos y presupuestos, y a que los robots normalmente se desempeñan en ambientes específicos y/o controlados, que solo requieren de algún sentido en especial, incluso más desarrollado que su contraparte humana.

La visión artificial

Si solo se va a incorporar un sentido al robot, la selección se inclinará naturalmente hacia el que más información proporcione sobre el ambiente; en general, la información que suele requerirse son dimensiones físicas (tamaño, volumen, posición, velocidad, aceleración, dirección, etc.), por lo que el sentido seleccionado suele ser la vista.

Una imagen puede suministrar mayor cantidad de información sobre las dimensiones de un lugar, un objeto o una persona, que la que podría obtenerse a través de un olor, un sonido, un sabor o una textura. En adelante se utilizarán los términos imagen e imagen digital de forma indistinta, puesto que las tecnologías utilizadas para dotar de vista a los robots solo pueden utilizar imágenes digitales.

La tecnología que se encarga de dotar del sentido de la vista a un robot se denomina ***visión artificial*** o visión por computadora, y su propósito es "entender" las características de una imagen y en consecuencia generar una acción. No se debe confundir la visión artificial con el procesamiento digital de imágenes (PDI); el PDI es un conjunto de técnicas que se aplican con el objetivo de mejorar la calidad ó facilitar la búsqueda de información en una imagen digital. El PDI es lo que suelen aplicar los laboratorios fotográficos al corregir "ojos rojos", montar escenarios, restaurar, etc. La visión artificial está profundamente apoyada en el PDI, pero de ninguna forma son lo mismo. El proceso de obtener información a través de la visión artificial para la toma de una decisión puede esquematizarse como muestra la **Figura 3**.

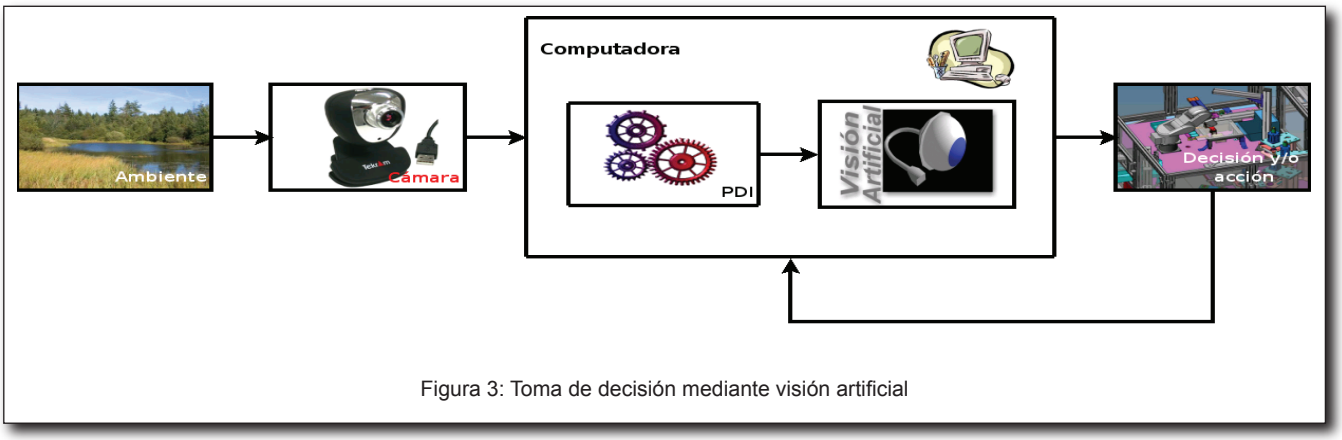


Figura 3: Toma de decisión mediante visión artificial

Ambiente

El ambiente es simplemente el lugar donde el robot desarrollará sus actividades. Puede ser una nave industrial, un laboratorio, una mesa de pruebas, etc.

Cámara

En visión artificial la cámara es el elemento que reemplaza al ojo humano. La cámara tiene como propósito convertir la luz presente en el lugar de trabajo, en una señal eléctrica que una computadora

pueda utilizar. Las cámaras ya no resultan extrañas, debido a la gran cantidad de modelos disponibles en el mercado, pero cabe mencionar que en el ambiente científico e industrial no cualquier tipo de cámara resulta útil para los fines que se persiguen. Los dispositivos que se han diseñado específicamente para las tareas en los ambientes antes mencionados son denominados cámaras de visión artificial. Las cámaras de visión artificial son mas sofisticadas que las convencionales, ofreciendo un completo control de los tiempos y señales de la cámara [4], [5]. Existen infinidad de marcas y modelos de este tipo de dispositivos, cada uno especializado en alguna necesidad, pero todas basadas en dos tecnologías para transformar la luz en una señal eléctrica: CCD y CMOS.

Tecnología CCD

Un CCD (***Charge-Coupled Device***, Dispositivo de Cargas Eléctricas Interconectadas) es un circuito integrado que contiene un número determinado de condensadores enlazados o acoplados. Bajo el control de un circuito interno, cada condensador puede transferir su carga eléctrica a uno o a varios de los condensadores que estén a su lado en el circuito impreso. El CCD es uno de los elementos principales de las cámaras fotográficas y de video digitales; en éstas, el CCD trabaja conjuntamente con células fotoeléctricas diminutas que registran la imagen, formando así el sensor. Desde allí, la imagen es procesada por la cámara y registrada en la tarjeta de memoria. La capacidad de resolución o detalle de la imagen depende del número de células fotoeléctricas, dicho número se expresa en píxeles; dichos píxeles registran tres colores diferentes: rojo, verde y azul (***RGB***, del inglés Red, Green, Blue), por lo cual tres píxeles, uno para cada color, forman un conjunto de células fotoeléctricas capaces de captar cualquier color en la imagen. Para conseguir esta separación de colores la mayoría de las cámaras del tipo CCD utilizan un filtro de Bayer [6], que proporciona una trama para cada conjunto de cuatro píxeles, de forma que un píxel registra luz roja, otro luz azul y dos más se reservan para la luz verde (por imitación al ojo humano, que es más sensible a la luz verde).

Tecnología CMOS

Un ***Active Píxel Sensor*** (***APS***) es un sensor que detecta la luz basado en tecnología CMOS y por ello es más conocido como sensor CMOS. Gracias a esta tecnología de construccción es posible integrar más funciones en un chip sensor, tales como control de luminosidad, corrección de contraste, conversión analógico-digital, etc. El APS, al igual que el sensor CCD, se basa en el efecto fotoeléctrico, ya que está formado por numerosos fotodiodos, uno para cada píxel, que producen una corriente eléctrica que varía en función de la intensidad de luz recibida. En el CMOS, a diferencia del CCD, se incluye un conversor digital en el propio chip y se incorpora un amplificador de la señal eléctrica en cada fotodiodo mientras que en un CCD se tiene que enviar la señal eléctrica producida al exterior y amplificarla. Al igual que ocurre con el CCD, los fotodiodos captan únicamente intensidad lumínica, para lo que se suele emplear nuevamente el filtro de Bayer [6] para la distinción de los colores. Mediante este filtro, unos fotodiodos recogen solo la luz roja, otros la luz verde y unos mas la luz azul.

Computadora

En un sistema de visión artificial la computadora es la encargada de recibir y procesar la información que proviene de la cámara. El término computadora aplica para el típico CPU con su monitor, teclado, ratón, etc., y para computadoras pequeñas especializadas basadas en dispositivos FPGA, DSP y microcontroladores. En la computadora se llevará a cabo la etapa de PDI y de visión artificial.

PDI

El análisis humano de imágenes u objetos presenta dificultades, pues el proceso de inspección visual consume una gran cantidad de tiempo y está sujeto a interpretaciones incoherentes e incompletas. El PDI, que comprende la manipulación por computadora de imágenes reales, resuelve estos problemas al poder automatizar el proceso de extracción de información útil de los datos contenidos en la imagen, y también permite perfeccionar la imagen, corregir distorsiones, etc. El PDI se efectúa dividiendo la imagen en un arreglo rectangular de elementos; cada elemento de la imagen así dividida se conoce como píxel.

El siguiente paso consiste en asignar un valor a la luminosidad promedio de cada píxel; así, los valores de cada píxel, junto con las coordenadas que indican su posición, definen completamente a la imagen. Todos estos números se almacenan en la memoria de una computadora. A continuación se alteran los valores de luminosidad mediante operaciones o transformaciones matemáticas, para resaltar los detalles de la imagen que sean convenientes. Al final se obtiene la representación de estos píxeles en un monitor, una fotografía impresa, etc.

La utilidad del procesamiento de imágenes es muy amplia y abarca muchos campos. Como aplicaciones típicas tenemos: detección de presencia de objetos, inspección visual automática, obtención de características geométricas y color de objetos, restauración de imágenes y mejoramiento en la calidad de las mismas. También se aplica en imágenes para diagnóstico médico, o en tomas aéreas empleadas para realizar exámenes del terreno, con el fin de analizar los recursos naturales, las fallas geológicas, etc. [7].

Visión Artificial

Cuando el PDI termina de optimizar la información de la imagen, la visión artificial entra en acción. Los objetivos típicos de la visión artificial incluyen:

- Reconocimiento de ciertos objetos en imágenes, por ejemplo, rostros humanos.
- La evaluación de los resultados; por ejemplo, obtener las dimensiones de un objeto proveniente de una máquina CNC y comprobar que cumpla con las especificaciones de diseño.
- Registro de diferentes imágenes de una misma escena u objeto; por ejemplo, hacer concordar un mismo objeto en diversas tomas.
- Seguimiento de un objeto en una secuencia de imágenes. Se suele utilizar para medir posición, velocidad y aceleración.
- Mapeo de una escena para generar un modelo tridimensional; tal modelo puede ser usado por un robot para navegar por la escena.
- Estimación de las posturas tridimensionales de humanos.

Estos objetivos se consiguen por medio de reconocimiento de patrones [8], aprendizaje estadístico [9], geometría de proyección [9], procesado de imágenes [10], teoría de gráficos [11] y otras técnicas.

Logros y avances de la visión artificial en el campo de la robótica

Los logros alcanzados por la visión artificial son notables; entre todos ellos destacan por su complejidad los del robot ASIMO, pero existen también desarrollos de autos robot y sistemas de control de calidad, entre muchos otros.

A S I M O

ASIMO (***Advanced Step in Innovative Mobility***), es un robot humanoide creado por la empresa Honda, capaz de moverse, interactuar con seres humanos y ayudarles; es una de las mayores

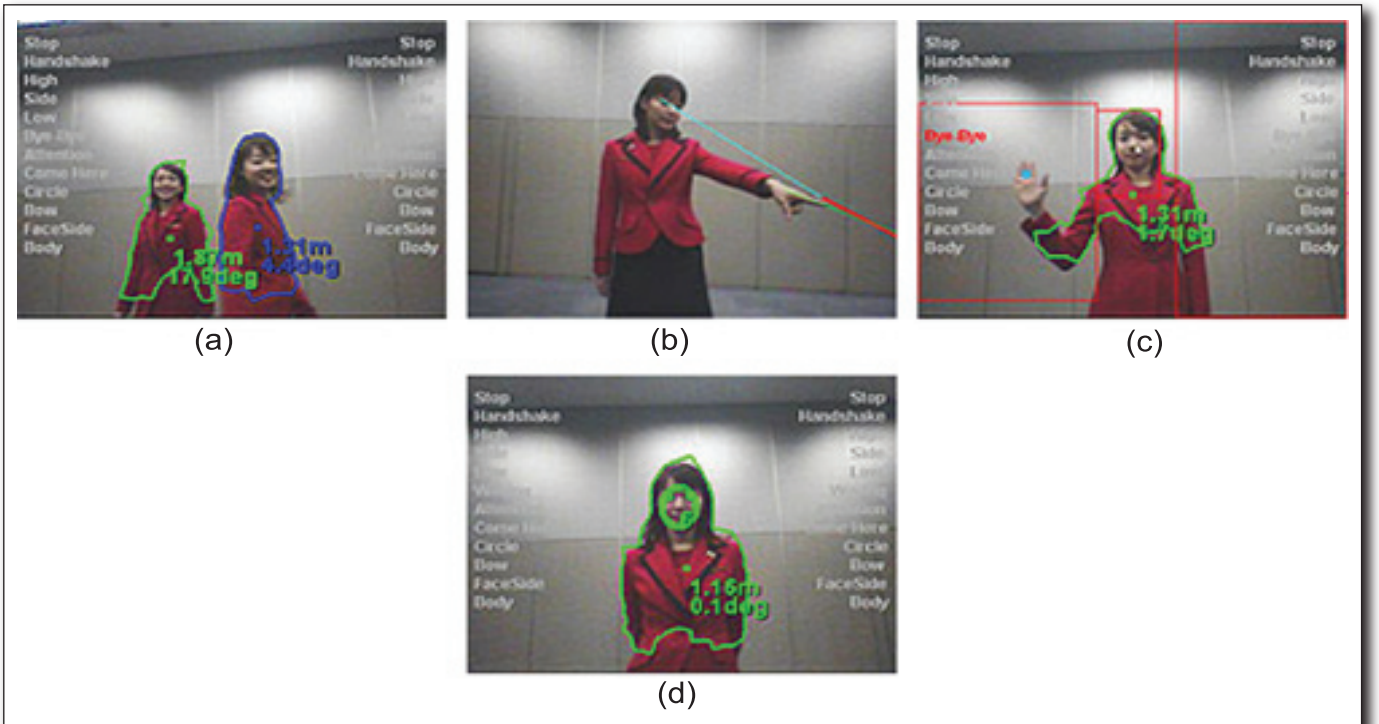


Figura 4: La visión artificial de ASIMO

proezas tecnológicas hasta ahora vistas. Aunque todavía se está lejos de poder atribuir roles concretos a los robots humanoides, estos podrían utilizarse, por ejemplo, para incrementar la autonomía de las personas con capacidades diferentes y personas mayores. Evidentemente, todavía tienen que transcurrir muchos años hasta que se pueda cumplir este objetivo, pero algunas empresas en Japón ya utilizan los servicios de ASIMO para funciones promocionales, como la recepción de visitantes.

La visión artificial que ASIMO incorpora puede determinar la distancia y dirección de movimiento de múltiples objetos o personas (ver la **Figura 4(a)**), es capaz de reconocer gestos como señalar objetos (ver la **Figura 4(b)**) y saludar (ver la **Figura 4(c)**), y además puede reconocer a una persona por sus rasgos faciales (ver la **Figura 4(d)**) [12].

Stanley

Stanley es un auto robot capaz de conducirse solo. Se trata de un VW Passat cuya dirección, acelerador y frenos están controlados completamente por una computadora (ver la **Figura 5**). Creado por un equipo de la Universidad de Stanford, ganó un premio de dos millones de dólares al lograr atravesar 212 kilómetros del desierto de Mojave, EU, guiado sólo por radares, dispositivos láser, y cámaras montadas en la carrocería. La visión artificial de Stanley, le permite evadir los objetos que se encuentran en su camino y estimar la calidad del terreno para determinar la velocidad de avance adecuada [13].

Figura 5:Auto robot Stanley.

Sistema de control de calidad para el laboratorio CIM de la UPIITA-IPN

Un laboratorio de manufactura integrada por computadora (**CIM**), consiste de una celda flexible de manufactura[1], y el software de integración de administración para simular un ambiente real. El propósito de este laboratorio es complementar el proceso de enseñanza en las aulas a los estudiantes de ingeniería en sistemas modernos de manufactura e información gerencial.

Todo proceso de manufactura cuenta con un control de calidad, y en el laboratorio CIM de la UPIITA-IPN, dicho control se lleva a cabo mediante visión artificial. El proceso es bastante sencillo, ya que solo se fabrican dos piezas simples: un cilindro de aluminio y un cubo de acrílico (ver las **Figuras 6(a)** y **6(b)**); dichas piezas forman un ensamble en forma de T invertida. La visión artificial debe determinar si ambas piezas cumplen con las dimensiones que el diseño especifica; si es así, se ensamblan mediante un robot poliarticular, de lo contrario son desechadas (ver **Figura 6(c)**).

Todo el software que lleva a cabo el control de calidad fue desarrollado por alumnos de ingeniería mecatrónica de la UPIITA-IPN, al realizarse un proceso de rediseño, actualización y mantenimiento mayor en el laboratorio CIM [14].

Conclusiones

La visión artificial es un campo sumamente fértil para el desarrollo de nuevos proyectos y aplicaciones, tanto en la industria, la academia y la vida diaria. Adicionando la robótica, es posible

Figura 6: Visión artificial en el laboratorio CIM de la UPIITA

1 Se considera flexible debido a que puede fabricar prácticamente cualquier elemento mecánico, a través de su maquinaria CNC.

producir resultados extraordinarios. Prácticamente no existen límites para lo que pueden lograr estas disciplinas unidas, desde artefactos que poseen tecnología de punta, con intenciones de incorporar la robótica a la vida diaria de la humanidad, hasta pequeñas aplicaciones escolares con fines puramente didácticos. Para finalizar, es conveniente mencionar que existe una condición muy alentadora en el desarrollo de estas disciplinas: lo único que puede limitarlas es la falta de ingenio, algo que afortunadamente a los mexicanos nos sobra.

Agradecimientos

♣ RSO agradece el soporte económico recibido por la Secretaría de Investigación y Posgrado del IPN (SIP-IPN), a través del proyecto 20071024 y del programa EDI, así como del Sistema Nacional de Investigadores (SNI-México).

♦ MAMV agradece el apoyo recibido del programa EDD del IPN.

Referencias

[1] http://es.wikipedia.org/wiki/IsaacAsimov

[2] Real Academia Española, Diccionario de la Lengua Española, Espasa Calpe, 22va ed, 2002.

[3] J. Craig, Robótica, Prentice Hall, 3ra ed, 2005.

[4] www.infaimon.com/catalogo/industria/index.html

[5] www.ni.com

[6] http://es.wikipedia.org/wiki/MosaicodeBayer

[7] J. González, *Visión por computador*, Paraninfo, Madrid, España, 2000.

[8] J. L. Díaz de León Santiago, *Reconocimiento de patrones: avances y perspectivas*, IPN-CIC, México, 2002.

[9] D. M. Gómez Allende, *Reconocimiento de formas y visión artificial*, RA-MA, 1994.

[10] G. J. Awcock, *Applied image processing*, McGraw Hill, New York, EU, 1996.

[11] O. Ore, *Teoría y aplicaciones de los gráficos*, Norma, Cali, Colombia, 1963.

[12] http://world.honda.com/ASIMO/technology/intelligence.html

[13] http://cs.stanford.edu/group/roadrunner//old/index.html

[14] A. Vázquez, J. Cruz, R. Rojas, *Reacondicionamiento e implementación de un sistema de control de calidad para el módulo de visión artificial del CIM*, IPN-UPIITA, México, 2006.

Tecnología Bluetooth para Sistemas de Monitoreo en Dispositivos PDA 1a. Parte

M. en C. Juan Carlos Herrera Lozada
Profesor del CIDETEC
M. en C. Jacobo Sandoval Gutiérrez,
Ing. Raziel Morón Corrales
CICATA LEGARIA

El estándar de comunicación ***Bluetooth*** es una norma abierta que posibilita la conexión inalámbrica (*Wireless*) de corto alcance para voz y datos entre dispositivos móviles y/o periféricos de uso común, a través de una banda disponible a nivel global (2.4 GHz) y mundialmente compatible.

En este documento se da una breve revisión al protocolo *Bluetooth* y se vislumbran las perspectivas sobre dicha tecnología; lo anterior en aras de conseguir una comunicación de esta naturaleza como objetivo de un proyecto de investigación para controlar un módulo *Bluetooth* mediante un microcontrolador, de manera que podamos comunicar un dispositivo PDA con éste.

Antecedentes

A finales del siglo XX, una de las más importantes revoluciones tecnológicas se relaciona con la computadora personal, que ha ido de la mano con otras innovaciones, como lo son los teléfonos celulares y los asistentes digitales personales (**PDA**) o computadoras de bolsillo, entre otras. Los teléfonos celulares y los PDA han tenido un auge de uso muy importante en todo el mundo, debido a su movilidad y portabilidad, aunado a la transmisión de datos en las comunicaciones y el intercambio de información.

En las áreas de las tecnologías de la información y de las comunicaciones, se han aprovechado las innovaciones en transceptores, circuitos integrados y antenas, así como los nuevos algoritmos convertidos en software, para construir dispositivos cada vez más eficientes, robustos y a menor precio, dirigiendo los esfuerzos hacia la comunicación inalámbrica.

La clave de todas estas nuevas herramientas es el desarrollo de las nuevas tecnologías de *Transmisión Inalámbrica de Datos (**DoW - Data over Wireless**)* que implican la utilización del espectro electromagnético en determinadas frecuencias reguladas por normas internacionales y adoptadas en cada país por las instancias correspondientes; en México se regula a través de la *Comisión Federal de Telecomunicaciones (COFETEL).*

El uso que se da a cada protocolo depende en gran medida de la demanda de datos y la distancia de transmisión; por esta razón existen diferentes protocolos que se complementan para realizar tareas sin cables. En consecuencia, podemos incrementar la productividad de manera cuantitativa en diferentes actividades, desde tareas en nuestra vida diaria hasta procesos industriales y de servicio.

Servicios de Transmisión Inalámbrica

A continuación, se procederá a comentar algunos aspectos formales de la comunicación sin cables en servicios *DoW*.

Telefonía celular

El sistema de telefonía celular, también conocido como sistema de telefonía móvil, está conformado por dos grandes bloques: una red de comunicaciones (red de telefonía móvil) y las terminales (teléfonos móviles) que permiten el acceso a dicha red. Este tipo de servicio se clasifica por la capacidad de datos que transmite en un enlace de comunicación.

La primera generación de telefonía móvil surgió en 1979, basada en el uso de radioteléfonos comerciales, caracterizándose por ser completamente analógica y estrictamente para voz. La calidad en los enlaces de comunicación era muy pobre, con una velocidad de 2400 baudios. En cuanto a la transferencia entre celdas, ésta era muy imprecisa ya que denotaba una baja capacidad, basada en *FDMA* (*Frequency Division Multiple Access*

– Acceso Múltiple por División de Frecuencia) y además, la seguridad no existía. La tecnología que trató de estandarizar y predominar esta generación fue *AMPS* (*Advanced Mobile Phone System* –Sistema Avanzado de Telefonía Móvil).

La segunda generación surgió en 1990, siendo de carácter digital y permitiendo transmitir datos y voz, además de ofrecer el servicio de *roaming*. A esta generación se le denominó *TDMA (Time Division Multiple Access* – Acceso Múltiple por División de Tiempo) que trabaja en los 800 MHz, con 30 KHz a 14.4 Kbps y que a su vez se subdivide en dos variantes principales: *Global System Mobile (GSM* – Sistema Global Móvil) el más conocido por la cantidad de usuarios a nivel mundial, trabaja en 800, 1800 y 1900 MHz con canales de 200 KHz a 14.4 Kbps y 8 ranuras de tiempo; *CDMA-One (Code Division Multiple Access* – Acceso Múltiple por División de Código) que trabaja en 800 y 1900 MHz con un canal de 1.25 MHz, usando de 9 a 14 canales para alcanzar hasta 115.2 Kbps.

Cabe mencionar que existe un intermedio entre la segunda y la tercera generación, aportando principalmente el servicio *General Packet Radio Services (GPRS* – Servicio General de Paquetes de Datos por Radio) que soporta desde 56 hasta 114 Kbps,

La tercera generación se caracteriza por la convergencia de voz y datos con acceso inalámbrico a Internet suministrando una alta tasa de transmisión de datos para aplicaciones multimedia, principalmente música, video (movimiento y videoconferencia) e imágenes. Esta generación alcanza hasta 144 kbps, donde se encuentran los servicios *CDMA 2000-1x, 1xEV, EDGE (Enhanced Data Rates for Global Evolution* – Transferencia Mejorada de Datos para una Evolución Global), *W-CDMA y* la propia *3G*, que en un futuro cercano se piensa alcanzará velocidades de hasta 384 kbps.

Redes inalámbricas

La movilidad y la seguridad de información cada vez se vuelven más imprescindibles para los usuarios, por esta razón se han desarrollado redes de datos que cubran estos requisitos.

Wireless - Fidelity (Wi-Fi – Fidelidad Inalámbrica) es una tecnología basada en el estándar *IEEE 802.11* de tercera generación, que trabaja en un espectro de onda de 2.4 GHz y con velocidades de 11 Mbps y 54 Mbps, estableciendo una área de cobertura de alrededor de 300 metros. Por tratarse de una señal de microondas, esta puede verse afectada por diversos factores y obstáculos en su camino, tales como paredes muy gruesas, edificios, techos de metal, etc., razón por la cual existen dispositivos para mantener y mejorar la recepción de la señal.

Los subestándares de Wi-Fi que actualmente se están explotando en el ámbito comercial son: *802.11b* y *802.11g*. El primero de ellos, en uso desde 1999, actualmente es el más extendido; opera en la banda de los 2.4 GHz y alcanza una velocidad máxima de 11 Mbps. El segundo subestándar, surgió en 2003, sobre la banda de los 2.4 GHz y con una velocidad máxima de 54 Mbps.

Para la transmisión y recepción de información, *Wi-Fi* utiliza la técnica *Orthogonal Frequency Division Multiplexing (OFDM* – División Multiplexada de Frecuencia Ortogonal) y para la seguridad de la información utiliza una encriptación *Wired Equivalency Privacy (WEP* – Equivalencia de Privacidad Cableada) basada en el algoritmo de encriptación *RC4*.

Esta tecnología nos proporciona una ventaja muy grande de movilidad y transmisión de datos seguros, sin necesidad de instalación ni configuración especial sobre los equipos que deseen intercambiar grandes cantidades de datos.

Otro servicio de red *wireless* es *Wi–Max;* esta tecnología se basa en el estándar *IEEE 802.16*, y puede alcanzar una velocidad de 100 Mbps en un canal con un ancho de banda de 28 MHz en el rango de 10 a 66 GHz, y de 70 Mbps en bandas menores a 11GHz, con una cobertura de 40 a 70 km, utilizándose principalmente para enlaces punto-multipunto; es decir, para conectar una red a distancia con un proveedor de servicios de Internet, siendo una alternativa a las conexiones de cable o fibra óptica.

Identificación inalámbrica por radio frecuencia

La identificación de productos en las cadenas de suministros estaba controlada en su totalidad por los populares códigos de barras; en la actualidad dicha tarea es complementada por los sistemas de Identificación por Radio Frecuencia *(RFID – Radio Frequency IDentification)* que utilizan un sistema de localización inalámbrico para automatizar los procesos de identificación. Su rango de trabajo está estandarizado bajo las normas EPC 125 kHz a 134 kHz, 13.56, 860 , 960 MHz y 2.45 GHz, y con alcance hasta 50 metros.

Tecnología *Infrared* (*IR*)

Esta tecnología ha sido ampliamente utilizada, en aplicaciones tales como controles remotos, PDA, computadoras portátiles, entre algunas otras. La comunicación es fácil cuando los dispositivos envían datos, y solamente deben contar con un puerto IR, sin necesidad de cables con adaptadores especiales, siendo

esté el objetivo de IR; sin embargo, tiene limitantes por la velocidad de transmisión, así como la enorme desventaja de que los puertos deben encontrarse en línea de vista entre sí, para poder completar la comunicación.

Bluetooth

Varios de los principales fabricantes de computadoras y telecomunicaciones (*Ericsson, Nokia, IBM, Toshiba),* formaron el Grupo de lnterés Especial en la Tecnología *Bluetooth (Bluetooth SIG - Special Interest Group)* el 20 de mayo de 1998, con el objetivo de crear un estándar libre para comunicación inalámbrica de corto alcance, normalizado sobre el protocolo *IEEE 108.15*.

El nombre dado al estándar fue tomado de un rey danés del siglo X llamado *Harald Blaatand* (*Bluetooth* en inglés), debido a que él simbolizó la unidad entre diferentes grupos de personas.

Principales características

Bluetooth utiliza una comunicación omnidireccional, es decir, la señal se propaga igualmente en todas direcciones, de manera similar a la tecnología *Wi–Fi*, tal como lo muestra la comparación de la **Figura 1**. Por lo tanto, esta comunicación no solamente se limita a un enlace punto a punto, sino que también se pueden crear pequeñas redes LAN, y así mismo podrían realizarse conexiones a Internet.

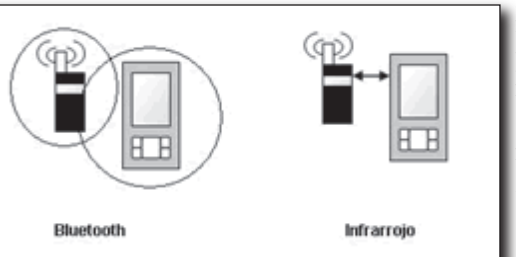


Figura 1. Espectro de propagación de *Bluetooth* e Infrarrojo.

Bluetooh opera en una banda de uso libre (sin licencia) de 2.4 GHz (2402 Hz – 2480 Hz), con un ancho de canal de 1 MHz, lo que resulta en un total de 79 canales. Las versiones de *Bluetooth* actuales hacen referencia a una *clase 1* que puede conseguir distancias de hasta 200 metros, y una *clase 2* que se limita a menos de 10 metros.

A diferencia de otras tenologías *DoW* que emplean el método de Espectro Esparcido (*Spread-spectrum)*, *Bluetooth* cambia su frecuencia con una pseudo-aleatoriedad de 1600 veces por segundo; de esta forma el canal se convierte en insensitivo, ya que si algún paquete llega a ser interrumpido éste vuelve a ser enviado en otra frecuencia en la que difícilmente podrá ser nuevamente interferido, llamando a esta tecnología de Saltos de Frecuencia Aleatorios (*Frequency-Hopping)*, como se muestra en la **Figura 2.**

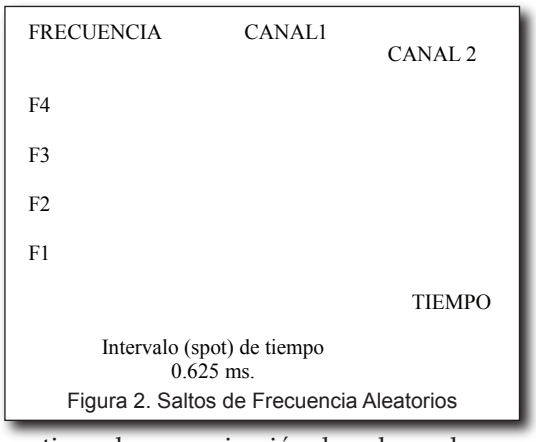


Figura 2. Saltos de Frecuencia Aleatorios

Un canal de *Bluetooth* siempre consiste de un maestro y uno o más esclavos; el maestro frecuentemente es quien inicia la conexión y decide sobre un esquema de esperanzas relacionado sobre el reloj interno, y el esclavo calcula un *offset* (desplazamiento) el cual es la diferencia entre los relojes maestro y esclavo. Esto determina la frecuencia a la que se espera el salto. Los canales de *uplink* y *downlink* (enlace activo e inactivo, respectivamente) para un solo componente son multiplexados en el tiempo y consecuentemente utilizan el mismo esquema de salto de frecuencia a 1MHz.

La eficiencia de comunicación bidireccional de datos se logra mediante dos tipos de comunicación de enlace; el primero es un enlace síncrono de comunicación llamado *Synchronous Connection-Oriented (SCO*–Conexión Orientada Síncrona*)*, que es especialmente deseable para servicios por circuitos de interrupción, donde se requiere un retardo mínimo y una alta razón de calidad del servicio (*QoS – Quality of Services)*. Estos canales ofrecen la misma velocidad en ambas direcciones y conocen exactamente cuando recibirán el próximo paquete, siendo óptimos para transmisiones constantes en los intervalos de tiempo (*slots*) en toda la sesión.

El segundo enlace, conocido como *Asynchronous Connection-Less (ACL* – Conección Débil Asíncrona*)* se utiliza para transferir datos y servicios asíncronos, mediante un esquema de poleo en la transmisión, formando una colección de hasta 8 unidades *Bluetooth* donde la unidad maestra controla la transmisión y el esquema de salto. El *master* regula las transmisiones de los esclavos. El tipo de enlace depende en gran medida de la calidad de transmisión que se quiera lograr, esto se observa de manera más detallada en la **Figura 3**.

Para transmitir la voz existen dos métodos de codificación analógica a digital; el primero es la Módulación por Codificación de Pulso *(PCM - Pulse Code Modulation)*. Esta técnica

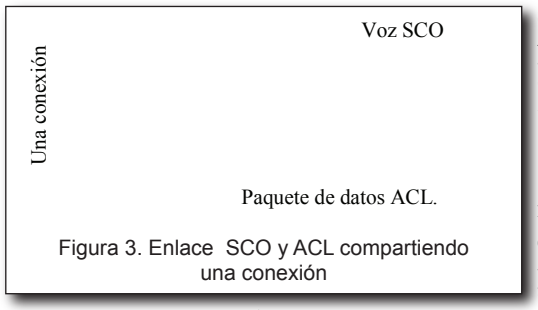


Figura 3. Enlace SCO y ACL compartiendo una conexión

nos proporciona 64 Kbps. La segunda técnica es llamada Curva Delta Continuamente Variable *(CSVD - Continuously Variable Slope Delta)*, que utiliza una técnica de un bit de longitud y con menor interferencia, ideal para ambientes *wireless* de sólo 8 Kbps. *Bluetooth* dispone de un mecanismo para el ahorro de energía, conservando la vida de la batería; las especificaciones del protocolo clasifican a los dispositivos en tres de acuerdo a su energía de operación, tal como se muestra en la **Tabla 1**.

Clase Potencia	Salida Máxima	Potencia
1	100 mW	-20 dBm
2	2.5 mW	-4 dBm
3	1.0 mW	-0 dBm

Tabla 1. Clases de potencia *Bluetooth*

1.- *Sniff Mode (*Modo olfateado*)*. En este modo se actualiza de acuerdo al ambiente en el que se está operando.

2.- *Hold Mode (*Modo Sostenido*)*. El reloj continúa operando, liberándose de la sincronización con el master.

3.- *Park Mode (*Modo estacionado*)*. Es similar a Hold Mode, solamente que este no retiene la dirección al cambiar de modo.

Una red *Bluetooth* debe contar con un software, que opera como *firmware* en el que se provee soporte para funciones de configuración, autentificación, conexión, envio, recepción, detección de errores y corrección; además cuenta con tres tipos de seguridad: *modos 1, 2 y 3*.

El *modo 1* representa un modo no seguro de operación, esto quiere decir que no tiene procedimientos de seguridad. En el *modo 2* se establece la posibilidad de comunicarse con dispositivos que no cuenten con seguridad y a su vez proporciona un nivel mínimo, si esto se requiere; en el *modo 3* se implementa la seguridad antes de iniciar los enlaces de operación.

La arquitectura de seguridad en *Bluetooth* es flexible, ya que permite enlaces sin autentificación o con *Personal Identification Number (PIN* Número de Identificación Personal*)*, esto es una validación para que los dispositivos se comuniquen, lográndose con la autentificación, autorización y la encriptación de los datos.

Funcionamiento de Bluetooth

Para establecer la conexión, primero el dispositivo *Bluetooth* debe ser encendido, cuando ocurre esto el equipo se pone en modo *standbye*, esperando mensajes de forma periódica en el espectro *RF* cada 1.28 s, sobre un conjunto de 32 saltos de frecuencia definidos por él mismo; después, si algún dispositivo está presente, recibe una instrucción de enlace, y si la dirección es conocida se transmite un mensaje *PAGE (*página*)*, en caso contrario se envía un mensaje de *INQUIRY (*exploración*)*.

El esquema más simple de conexión ocurre cuando dos dispositivos necesitan comunicarse uno con otro y se denomina *PICONET*. Este es un enlace punto a punto donde se requiere un dispositivo maestro y otro esclavo; además, si existe un dispositivo maestro y uno o más esclavos (punto a multipunto) en una red *ad hoc*, ésta también se considera como PICONET, tal como se muestra en la **Figura 4**.

Una red PICONET se limita únicamente a 8 dispositivos al mismo tiempo, aunque se pueden tener más esclavos, no simultáneos pero sí con la posibilidad de comunicarse; a estos elementos se les refiere como *Parked (*estacionados*)*. A cada esclavo activo se le asigna una dirección de 3 bits, mientras que los esclavos *parked* tienen 8, siendo un máximo de 256 dispositivos esclavos en *parked*.

Como se mencionó anteriormente, el enlace se logra con mensajes de *PAGE* o *INQUIRY*, y cuando el dispositivo entra en modo de operación *PAGE* se transmite una secuencia de 16 mensajes idénticos sobre 16 diferentes saltos de frecuencia, y si el esclavo no responde dentro de ese lapso el maestro vuelve a enviar la misma secuencia sobre las 16 frecuencias restantes. En el caso de *INQUIRY*, se establece que es un dispositivo desconocido que ha entrado a un nuevo ambiente *Bluetooth*; es similar a *PAGE*, pero utiliza un poco más de tiempo para poder ser reconocido, y el tiempo máximo de alcance de un maestro a un esclavo es de 5.12 segundos.

Existen algunas variaciones de PICONET, como por ejemplo SCATTERNET, que infiere hasta ocho

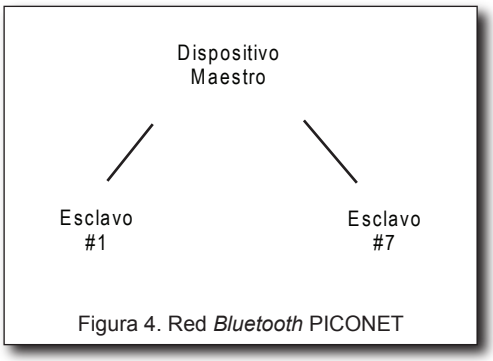


Figura 4. Red *Bluetooth* PICONET

PICONET que están cerca, sobre una misma área de cobertura *wireless*, como se muestra en la **Figura 5**.

Errores de conexión

Existen tres esquemas para corrección de errores, los dos primeros utilizan *Forward Error Correction (FEC* – Corrección de Error Frontal*)* que es un esquema de redundancia suficiente para corregir el menor número de bits, mientras que el tercero, *Automatic Retransmission Request (ARQ* – Solicitud de Retransmisión Automática), funciona validando los paquetes a través de un algoritmo CRC que se compara entre el calculado y el transmitido.

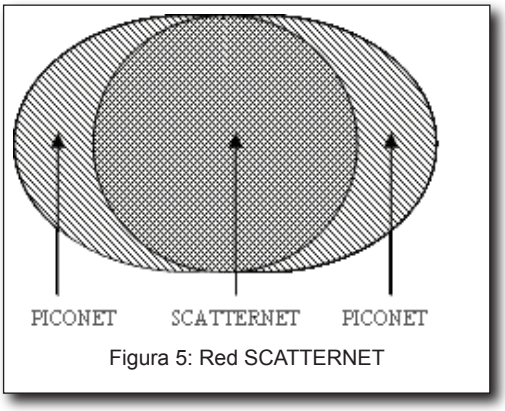


Figura 5: Red SCATTERNET

Perspectivas Actuales

Con la aparición de diferentes plataformas en dispositivos móviles, específicamente tipo PDA (vistos como computadoras de bolsillo) y Smartphones, es posible considerar al protocolo *Bluetooth* de corto y largo alcance con dos posibles vertientes: aplicaciones residentes *(software)* para el manejo e intercambio de información multimedia o documental entre dos o más dispositivos de las mismas características y, por otra parte, aplicaciones que permiten conectar al dispositivo móvil con alguna realización hardware externa, como sería un microcontrolador.

En este segundo caso se trabaja con sistemas básicos de adquisición y monitoreo de señales; es decir, a través del microcontrolador se establece una comunicación inalámbrica vía *Bluetooth* con el *PDA* o el *Smartphone*, para que éste reciba la información, la procese, la almacene de ser necesario y pueda elaborar gráficas para un análisis más concreto en un sistema de supervisión.

Cabe mencionar que, dadas las propiedades de la tecnología *Bluetooth*, es posible realizar la comunicación de manera serial entre sólo dos dispositivos entrelazados, que es el caso de este artículo, o bien crear una red que puede soportar varios dispositivos interactuando. La **Figura 6** hace referencia a la aproximación de integración del prototipo. Obsérvese que el PDA debe incluir la funcionalidad *Bluetooth*.

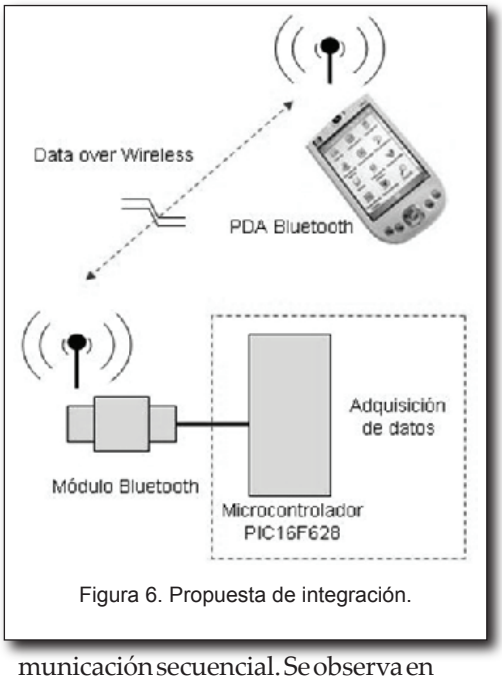


Figura 6. Propuesta de integración.

Para la alternativa del módulo *Bluetooth*, entre varias opciones, es posible usar un adaptador de RS-232 a *Bluetooth* comercial, un convertidor de alcance considerable, que soporta la transmisión de voz y datos; el dispositivo consta de tres partes: un controlador de banda base, una memoria flash y una interface de radio que funciona entre 2.4 y 2.5 GHz, cumpliendo con la *versión 1.1* del protocolo y permitiendo configurar la velocidad de transferencia en la contraparte serial desde 2,400 hasta 9,600 baudios con un conector macho DB9. El Módulo para este prototipo se muestra en la **Figura 7**, el cual consta de una serie de interruptores que permiten configurar la velocidad de transmisión, que en el caso particular de este proyecto es de 2400 baudios, soportados por el microcontrolador.

La idea de utilizar el convertidor *Bluetooth* a serial RS-232 está basada en la facilidad con la que el microcontrolador puede implementar esta comunicación secuencial. Se observa en la **Figura 6** que el microcontrolador sugerido se debe programar con una funcionalidad serial, como si se fuera a comunicarse con el protocolo RS-232 alambrado, siendo transparente para éste la conversión *Bluetooth* que realizará el adaptador.

En dependencia con el Sistema Operativo del PDA, será necesario buscar una herramienta adecuada para programar la aplicación; se propone C#, Visual Basic o J2ME. Las primeras aproximaciones se han realizado en C# 2.0.

Conclusiones

En este documento se presentó una revisión básica de las tecnologías *Data over Wireless*, enfocándonos al protocolo *Bluetooth*, actualmente utilizado en la mayoría de los dispositivos móviles, dada su facilidad de conexión, seguridad de transferencia, alta velocidad e infraestructura.

La idea básica de este artículo es sentar las condiciones iniciales para acoplar un módulo de comunicación

Figura 7: Adaptador *Bluetooth* a RS-232, marca IOGEAR

Bluetooth a un microcontrolador, y de esta manera acceder a un PDA también con puerto *Bluetooth* e intercambiar información, formando así un sistema inalámbrico de adquisición y monitores de datos.

En artículos posteriores se abordará la implementación del sistema completo.

Bibliografía.

[1] Gilbert Held, ***"Data Over Wireless Networks Bluetooth, WAP, and Wireless LAN´s"*** McGraw-Hill U.S.A 2001.

[2] Christoffer Andersson. ***"GPRS and 3 Wireless Applications"***, John Wiley & Sons, Inc. USA 2001.

[3] Comisión Federal de Telecomunicaciones COFETEL, www.cofetel.gob.mx

[4] J. Sandoval, F. Martínez. ***"Diseño de un sistema RFID activo tipo GEN2 sobre UHF de 433 MHz en modulación ASK de bajo costo"***, 4º Congreso Internacional en Innovación y Desarrollo Tecnológico, México, 2006, IEEE.

[5] Herrera Juan, Morales Mario, Sandoval Jacobo, Ilizaliturri Ian. ***"Perspectivas Actuales de la Tecnología RFID"***. VIII Simposium Internacional, Aportaciones de las Universidades a la docencia, la investigación, la tecnología y el desarrollo. ESIQIE – CIDETEC, IPN, México, D.F. 2006.

[6] Herrera Juan, Gonzáles Juan, Cruz Agustín. ***"Programación de Dispositivos de Cómputo Móviles"***. POLIBITS, Año XV, Vol. 1, Número 31, Enero – Junio de 2005. CIDETEC, México, D.F.

[7] Herrera Juan, Gonzáles Juan, Cruz Agustín. ***"Una Alternativa para el Control de Motores Convencionales de CD en una Computadora de Bolsillo"***. Congreso Internacional de Electrónica Electro2006, Instituto Tecnológico del Estado de Chihuahua, Chihuahua, México.

Licencias de Software: Antecedentes

M. en C. Eduardo Vega Alvarado
Lic. Silvia Toledo Molano
M. en C. Ma. Aurora Molina Vilchis
Profesores del CIDETEC-IPN

Software es un término general que se aplica a las diversas clases de programas (*conjuntos de instrucciones*) que dirigen a una computadora y a sus dispositivos relacionados para llevar a cabo una tarea específica [1]; eventualmente, esta definición se puede ampliar para incluir a la documentación relativa al funcionamiento y uso de tales programas (*manuales*) [5].

Cuando se desarrollaron las primeras computadoras electrónicas, los pioneros en el campo no previeron que aparecería una actividad denominada programación de computadoras; sin embargo, a partir de la década de 1990 el desarrollo y mercadeo del software superó por mucho al del hardware, el cual para entonces se había convertido en un producto barato de producción en masa [2]. Como resultado de esta enorme expansión, las licencias de derechos son cada vez más importantes como mecanismos para protección del software, y en muchas ocasiones se vuelven un punto de conflicto, debido principalmente al desconocimiento general sobre las mismas.

En el presente artículo se describe de manera objetiva a los antecedentes y a las diferentes opciones para licenciar software, considerando tanto la óptica del programador como la visión de los distribuidores de programas y el sentir del usuario final.

Historia

Las primeras computadoras electrónicas digitales surgen a finales de la segunda guerra mundial, básicamente como calculadoras de alto rendimiento; como consecuencia de esta especialización, la programación tanto de sistemas como de aplicaciones simplemente no existía. En 1951, la aparición de la *UNIVAC* (*Universal Automatic Computer*) marca un hito al ser el primer equipo pensado para su venta como una computadora de propósito general (universal); a partir de entonces comienza a tomar fuerza la idea de que una misma computadora pueda realizar tareas totalmente diferentes, únicamente cambiando su secuencia de órdenes (programa). Así van surgiendo los sistemas operativos, los lenguajes de programación y los compiladores, dando origen a la programación de sistemas, en una dinámica que se mantiene hoy en día.

El enfoque de comercialización aplicado inicialmente consideraba a los programas y a los equipos como sistemas completos, bajo un esquema propietario, por lo que sus partes no se distribuían de forma independiente; no existían entonces proveedores de aplicaciones ni se pensaba siquiera que un equipo ejecutara programas de otro fabricante. Sin embargo, en diciembre de 1968, bajo la presión del gobierno de Estados Unidos, IBM anunció que al año siguiente *desincorporaría* el software; esto es, lo vendería por separado en lugar de combinar su costo con el de los sistemas físicos. El software permanecería etéreo, pero ahora podría comprarse y venderse. El efecto de esta decisión era abrir el campo del software a la competencia comercial, la cual se vería alimentada por la fuerza del mercado libre [2].

Como consecuencia de esta medida, comenzó un debate aún vigente sobre si el software debe considerarse como propiedad intelectual y, en consecuencia, en que términos deben generarse las licencias para su uso, distribución, modificación y copia, entre otros aspectos; incluso la discusión se extiende al análisis sobre la patentabilidad del software, ya que algunos lo consideran como un desarrollo y para otros es una invención.

La selección de un tipo de licencia de software no es un asunto simple, dado que hay muchos detalles involucrados, e incluso el decidir que licencia utilizar para un proyecto particular puede ser un proyecto por si mismo [8]. Es fundamental considerar el punto de vista del interesado, esto es, si es creador, distribuidor o

usuario ya que incide directamente en su percepción respecto a que aspectos del software se deben proteger mediante una licencia. En general, las opciones para licenciar software contemplan dos alternativas:

1. Las licencias propietarias

2. El software libre y de fuente abierta (*FOSS*, *Free and Open Source Software*).

Software Propietario

El término *propietario* describe una tecnología o producto que pertenece exclusivamente a una compañía, la cual conserva en secreto el conocimiento acerca de dicha tecnología o del funcionamiento interno del producto [1]. Incluso la mayoría de los programas propietarios solo funcionan adecuadamente si se utilizan con otros productos de la misma compañía; Microsoft es considerado como el mejor ejemplo de ello, siendo el caso Windows – Office totalmente representativo.

En el caso del software propietario, lo único que generalmente permiten las licencias es el uso de la aplicación, prohibiendo o limitando severamente cualquier otro permiso sobre el producto. Por lo mismo, la copia o distribución ilegal de los programas se ha convertido en una preocupación permanente para los poseedores de las licencias, tal como lo muestra la afirmación siguiente [4]:

La magnitud de la piratería cometida contra toda clase de contenidos digitales tales como música, software y películas se ha vuelto monstruosa. Este problema tiene enormes repercusiones económicas y ha sido causa de cierta parálisis en la creatividad ¿porqué crear si no se recibe recompensa por el esfuerzo?.

La polémica respecto al software propietario aumenta cuando se consideran aspectos tales como:

• el valor de la propiedad intelectual, suponiendo que dicha propiedad sea éticamente correcta, en otra palabras ¿cuánto valen los conocimientos aplicados en un programa?

• la creación y sostenimiento de monopolios y oligopolios en una época donde la ley de la oferta y la demanda, la libre competencia y la apertura de mercados son la base de la organización económica mundial, y

• la falta de capacidad de compra en sectores amplios de usuarios, especialmente en los países en vías de desarrollo, que impide la adquisición de estos productos y propicia la pirateria.

Software Libre

Richard Stallman, un investigador del Laboratorio de Inteligencia Artificial del MIT, inició en 1984 el proyecto *GNU* (*GNU is Not Unix*), con la idea de desarrollar un sistema operativo bajo el esquema de software libre. Stallman inició su proyecto porque sentía que el conocimiento que constituye a un programa ejecutable (esto es, el código fuente) debe ser libre; mientras los fabricantes de software veían un conjunto de secretos industriales que debían protegerse celosamente, Stallman veía conocimiento científico que debía ser compartido y distribuido [3].

Stallman provenía de un ambiente de programadores, acostumbrados a compartir sus desarrollos entre sí. Estos grupos de trabajo no eran un concepto nuevo; si bien se habla de ellos como un movimiento que aparece en la década de los setenta, sus orígenes se remontan a 1955 cuando surge el grupo SHARE, formado por usuarios de sistemas IBM 701 con la finalidad de compartir sus experiencias en la programación de tales equipos [2].

Inicialmente, el proyecto GNU avanzó hasta la implementación de herramientas para la construcción de aplicaciones, tales como bibliotecas de funciones, editores de texto y compiladores; sin embargo, el desarrollo del sistema operativo base no tuvo mayor progreso hasta la aparición del kernel de Linux. El sistema operativo libre Linux inició una de las mayores revoluciones en la historia de la computación cuando brotó de los dedos de un estudiante finlandés llamado Linus Torvalds, hace ya 15 años. Actualmente, Linux encabeza ahora ventas anuales de hardware, software y servicios por al menos 15 mil millones de dólares [6]. Este hecho demuestra lo establecido por el propio Stallman, respecto a que software libre no es sinónimo de gratuito, así como tampoco existe contraposición entre el mismo software libre y el software comercial [7]:

Contrastar el software libre (o fuente abierta) con el software "comercial" es un segundo malentendido […] Software comercial significa software desarrollado por un negocio. Muchos programas libres (y de fuente abierta) importantes, incluyendo a OpenOffice y MySQL, son comerciales.

A pesar de su éxito, el desarrollo futuro del software libre y de fuente abierta enfrenta algunos obstáculos, entre los que destacan:

• Hardware secreto: los fabricantes de HW tienden a mantener en secreto las especificaciones de sus productos, dificultando la escritura de manejadores (*drivers*) para dar soporte a nuevos dispositivos.

• La existencia de bibliotecas de desarrollo que no son software libre, principalmente para programar interfaces con el usuario.

• Las patentes de software, que impiden utilizar estructuras y algoritmos en aplicaciones fuera del software propietario hasta por veinte años.

Licencias de Productos Derivados

Un punto que normalmente no se toma en cuenta respecto a las licencias es el estatus de los productos derivados o generados al utilizar algún software en particular, cuando tales productos tienen la forma de programas, bibliotecas de funciones o incluso estructuras de datos con formatos especiales. La mayoría de las herramientas para diseño de estas aplicaciones incluyen previsiones al respecto en sus licencias, por lo que las alternativas para los productos generados están ya definidas, por lo que es muy fácil infringir alguna ley por ignorancia. Es conveniente recordar que, de acuerdo a las normas generales del derecho, el desconocimiento de una ley no justifica su incumplimiento.

Conclusiones

Es importante destacar que el debate en el caso del software no es sobre la aplicación o no de licencias, sino sobre las características que estas deben cumplir; el pensamiento general es que todo programa debe estar cubierto por una licencia derivada de los derechos de autor. Cada tipo de licencia tiene un enfoque especial orientado a la protección de aspectos específicos del software; así, mientras algunos piensan en conservar la propiedad intelectual, otros se avocan a asegurar la libertad en todos los aspectos relacionados con la interacción usuario – producto: uso, copia, distribución y modificación, sin que esta libertad conduzca a una pérdida de derechos para el autor.

Evidentemente cada tipo de licencia tiene ventajas y desventajas, y es imposible determinar si alguna es mejor que otras sin considerar una serie de factores, que en muchos casos incluyen aspectos económicos, legales e incluso sociales de gran complejidad. La selección de licencias debe hacerse analizando caso por caso, y dadas las características de la economía actual, el enfoque más adecuado parece ser la incorporación de sistemas abiertos, donde el aspecto comercial no se anteponga a la difusión del conocimiento, sino que se complementen.

En este artículo se presentó un panorama general sobre las licencias de software, con la idea de iniciar una serie de trabajos al respecto; posteriormente se tratarán en detalle las licencias específicas y sus implicaciones económicas, legales y sociales, así como una serie de criterios para la selección de la licencia adecuada en un caso específico.

Referencias

1. Thing, L., *The Whatis?com's Encyclopedia of Technology Terms.* Que Publishing, 2002.
2. Ceruzzi, P., *A History of Modern Computing, 2nd Edition*. Cambridge: MIT Press, 2003.
3. DiBona, C., *Open Souces, Voices from the Open Source Revolution*. O'Reilly & Associates, 1999.
4. Eilam, E., *Reversing, Secrets of Reverse Engineering*. John Wiley & Sons, 2005.
5. Téllez, J., *Derecho Informático, 3ª Edición.* McGraw Hill, 2004.
6. Lyons, D., Toppling Linux, *Forbes Global 2.18*, Octubre 30, 2006, p92.
7. Stallman, R., A Note from Richard Stallman (Letter to the Editor), *Technology Review 110.3*, Cambridge, Mayo – Junio 2007, p8.
8. St. Laurent, A., *Understanding Open Source & Free Software Licensing*, O'Reilly & Associates, 2004.

OBSERVACIONES

Si te interesa contribuir con algún comentario o sugerencia, el Consejo Editorial de la Revista Polibits agradecerá utilices este espacio, y lo remitas a:

Centro de Innovación y Desarrollo Tecnológico en Cómputo
Consejo Editorial Revista POLIBITS
Av. Luis Enrique Erro s/n, Unidad Profesional Adolfo López Mateos,
Zacatenco, Deleg. Gustavo A. Madero, C.P. 07738, D.F.,

Teléfono 5720-6000 ext.52513.
mail *cidetec_si@ipn.mx*

Si tu contribución es un artículo, favor de enviarlo por e-mail y anexar los siguientes datos: Nombre del autor, Grado Académico e Institución o Empresa de procedencia. Puedes consultar la página www.cidetec.ipn.mx para consultar los formatos de archivo para tu envío.

10º Aniversario

1997 - 2007

30 de mayo

INSTITUTO POLITÉCNICO NACIONAL
IPN
Centro de Innovación y Desarrollo Tecnológico en Cómputo
CIDETEC
IPN
10º Aniversario
3er Congreso Internacional: Tendencias Tecnológicas en Computación 2007
12 al 16 de Noviembre
Conferencias y Talleres
"Unidad Profesional Adolfo López Mateos", Av. Juan de Dios Bátiz s/n, casi esq. Miguel Othón de Mendizábal, Edificio CIDETEC. Colonia Nueva Industrial Vallejo, Delegación Gustavo A. Madero C.P 07700, México D.F
www.ipn.mx
www.sep.gob.mx
SECRETARÍA DE EDUCACIÓN PÚBLICA
SEP