Contenido

Modulación Σ–Δ en Control Automático
Ramón Silva Ortigoza, María Aurora Molina Vilchis (CIDETEC-IPN);
Hebertt Sira Ramírez (CINVESTAV-IPN);
Jesús Linares Flores (Universidad Tecnológica de la Mixteca). 3

Arquitectura de las Redes Ad-Hoc
María Aurora Molina Vilchis, Ramón Silva Ortigoza (CIDETEC-IPN);
Eleazar Bracho Molina (UAMI). 8

Sistema de Manufactura Flexible con Restricciones Temporales (Descripción)
José de Jesús Medel Juárez (CIC-IPN); Gabriel Hernández López,
Jacobo Sandoval Gutierrez (CICATA-LEGARIA-IPN). 14

Análisis de la Caracterización de los Identificadores por Radiofrecuencia RFID
Borja Becerril Dulce Lesly, Linares y Miranda R, Díaz Santos Fco. J., Garduño Medina J. A. García Rivero G., Gonzalez Mijangos J.A. (ESIME-ZACATENCO-IPN). 19

Mejora Continua para el Sistema de Comunicaciones
M. en C. Cirilo G. León Vega, M. en C. Luis Alejandro Iturri Hinojosa (ESIME ZACATENCO-IPN);
Ing. Ciro David León Hernández (CIDETEC-IPN). 25

Criptografía Cuántica: Un Nuevo Paradigma
María Aurora Molina Vilchis, Ramón Silva Ortigoza (CIDETEC-IPN);
Eleazar Bracho Molina (UAMI). 30

Modulación Σ–Δ en Control Automático

Ramón Silva Ortigoza
María Aurora Molina Vilchis
CIDETEC-IPN.
Hebertt Sira Ramírez
CINVESTAV-IPN.
Jesús Linares Flores
Universidad Tecnológica de la Mixteca.

La modulación Σ–Δ es una técnica de implementación basada en modos deslizantes que es extremadamente útil en la síntesis de leyes de control, diseñadas sobre la base de modelos promedios de sistemas conmutados. Con la ayuda del modulador Σ–Δ, las estrategias de control promedio, lineales o no lineales, se sintetizan apropiadamente en una manera conmutada. Debido a que la frecuencia de conmutación del modulador Σ–Δ es idealmente infinita, se propone una implementación práctica del mismo, la cual permite limitar la frecuencia de conmutación del circuito a un valor finito.

1. Introducción

La técnica de control por modos deslizantes [11] es quizá la mas sencilla y natural que se puede aplicar a los sistemas conmutados [11]. En este trabajo se propone una alternativa al uso de modos deslizantes conocida como modulación Σ–Δ. Esta técnica de implementación facilita la aplicación de técnicas de control lineales y no lineales, diseñadas sobre la base de modelos promedio, para sistemas con entradas conmutadas [3]. La modulación Σ–Δ es bastante popular en otras áreas diferentes a la teoría de control (principalmente comunicaciones, procesamiento de señales, conversión analógica a digital, etc.). La idea es contar con un bloque capaz de transformar señales continuas y acotadas en señales conmutadas, conservando una propiedad importante: que el comportamiento promedio de la señal discreta a la salida del modulador coincida exactamente con la señal continua a la entrada del mismo. La modulación Δ y sus variantes: modulación Σ–Δ, modulación Σ doble, modulación Σ–Δ bipolar, etc., fueron usadas durante las etapas iniciales de transmisión de voz en los vuelos espaciales y otras muchas áreas de digitalización de señales (véanse los libros de Norsworthy [4] y de Steele [10]). El uso de la modulación Σ–Δ en conjunto con modos deslizantes ha sido propuesto más recientemente (véase [7] y [8] aunque estos desarrollos tienen sus orígenes en [5]). Aplicaciones de la modulación Σ–Δ, en la síntesis de controladores diseñados sobre la base de modelos promedios de sistemas conmutados, se han desarrollado en [9].

2. Modulación Σ–Δ

Considerando el diagrama a bloques básico de la **Figura 1**, el cual hace referencia al diagrama a bloques de un modulador Σ–Δ usado en teoría de sistemas de comunicación y en esquemas de conversión análogo-digital, restringido a entregar valores del conjunto discreto {0,1}. El siguiente teorema resume la relación del modulador Σ–Δ con el control por modos deslizantes, cuando se establecen las funciones de entrada-salida del diagrama.

Teorema 1: Considere el modulador Σ–Δ mostrado en la **Figura 1**. Dada una señal $\mu(t)$ acotada y suficientemente suave, entonces la integral del error, $e(t)$, converge a cero en tiempo finito, t_h. Además, para cualquier valor inicial arbitrario, $e(t_0)$, existe un movimiento deslizante en la superficie de codificación perfecta, representado por $e = 0$, para todo $t > t_h$, siempre que la siguiente condición de codificación se satisfaga para todo t,

$$0 < \mu(t) < 1 \tag{1}$$

Demostración. De la **Figura 1**, las variables en el modulador Σ–Δ satisfacen las relaciones siguientes:

$$\dot{e} = \mu(t) - u \qquad u = \frac{1}{2}\left[1 + sign(e)\right] \tag{2}$$

Lo anterior genera que el producto $e\dot{e}$ esté definido por

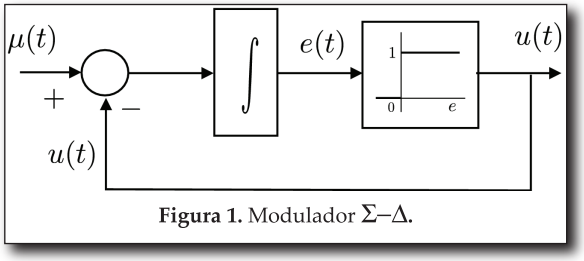


Figura 1. Modulador Σ–Δ.

$$e\dot{e} = e\left[\mu - \frac{1}{2}(1 + sign(e))\right]$$

$$= -|e|\left[\frac{1}{2}(1 + sign(e)) - \mu sign(e)\right]$$

Para $e > 0$ tenemos $e\dot{e} = -e(1-\mu)$, lo cual, de acuerdo con la condición (1) lleva a $e\dot{e} > 0$. Por otro lado, cuando $e < 0$, tenemos $e\dot{e} = -|e|\mu$. Entonces, existe un régimen deslizante en $e = 0$ para todo t después del tiempo t_h (véase [11]). Bajo condiciones ideales de deslizamiento, o codificación ideal, $e = 0$, $\dot{e} = 0$, tenemos que el valor equivalente de la señal de salida conmutada, u, denotada por $u_{eq}(t)$ satisface $u_{eq}(t) = \mu(t)$.

Un estimado del tiempo t_h se obtiene por inspección de las ecuaciones del modulador con los peores límites posibles para la señal de entrada μ en cada una de las dos condiciones: $e > 0$ y $e < 0$, junto con el valor correspondiente de u. Considere entonces $e(0) > 0$ en el tiempo $t = 0$. Tenemos que para todo $0 < t \le t_h$,

$$e(t) = e(0) + \int_0^t (\mu(\sigma) - u(\sigma))d\sigma$$

$$\le e(0) + t\left[\sup_{t\in[0,t]} \mu(t) - 1\right]$$

$$< e(0) + t_h\left[\sup_t \mu(t) - 1\right] \qquad (3)$$

Puesto que $e(t_h) = 0$, tenemos:

$$t_h \le \frac{e(0)}{1 - \sup_t \mu(t)} \qquad (4)$$

La salida promedio del modulador Σ–Δ, u_{eq}, produce idealmente la señal de entrada del modulador, $\mu(t)$, en un enfoque de control equivalente (véase [11]).

3. *Controladores Promedios y la Modulación* Σ–Δ

Suponiendo que tenemos un sistema no lineal suave de la forma $\dot{x} = f(x) + g(x)u$ con u siendo una señal de entrada de control continua que, debido a algunas limitaciones físicas, requiere ser acotada por el intervalo cerrado [0,1]. Supóngase, además, que hemos podido especificar un controlador de retroalimentación de salida dinámico de la forma $u = -k(y,\xi)$, $\dot{\xi} = \varphi(y,\xi)$ con características de desempeño en lazo cerrado deseables. Asuma, además, que para algunos estados iniciales razonables del sistema (y del controlador dinámico), los valores de la función de la señal de retroalimentación generada $u(t)$, son estrictamente acotados por el intervalo cerrado [0,1].

Si un requisito de implementación adicional nos impone ahora que la entrada control u ya no pueda tomar valores continuos en el intervalo cerrado [0,1], sino solo en el conjunto discreto {0,1}, la pregunta natural es: ¿Cómo podemos implementar el controlador continuo previamente deducido, para que se puedan recuperar, en un *sentido promedio*, las características deseables del controlador realimentado dinámico diseñado con base a las restricciones recientemente impuestas al actuador?

La respuesta se da claramente por las características de reproducción promedio de la señal de entrada en el modulador Σ–Δ previamente considerado, recordando que la señal de salida de tal modulador se restringe a tomar valores, precisamente, del conjunto discreto {0,1}. Entonces, si la salida del controlador continuo diseñado, denominado $u_{av}(t)$, se alimenta al modulador Σ–Δ propuesto, la señal de salida del modulador reproduce, en un sentido promedio, la señal de control requerida $u_{av}(t)$. La **Figura 2** muestra la implementación conmutada de un controlador de retroalimentación de la salida continuo, a través de un modulador Σ–Δ, que reproduce, en un sentido promedio, las características del controlador continuo diseñado.

En vista de los resultados anteriores, tenemos el resultado general siguiente, concerniente al control de sistemas no lineales a través de modos deslizantes sintetizados sobre la base de un controlador promedio y un modulador Σ–Δ. Solo se trata el caso del controlador realimentado dinámico para el problema de estabilización alrededor de un punto de equilibrio. Sin embargo, el resultado también puede extenderse a problemas de seguimiento de trayectorias.

Teorema 2: Considere el sistema no lineal n-dimen-

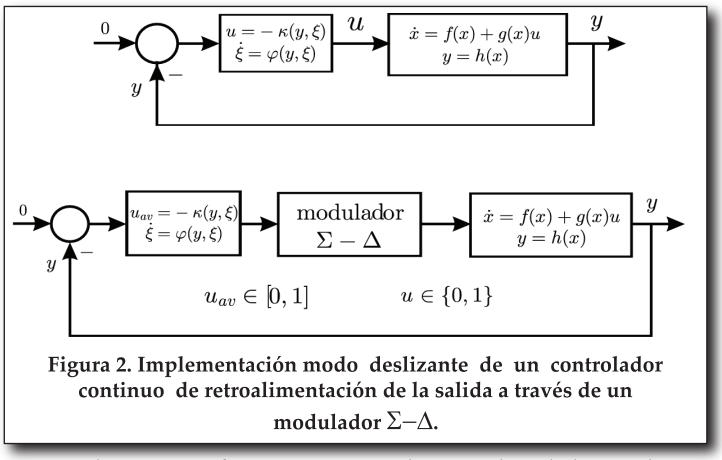


Figura 2. Implementación modo deslizante de un controlador continuo de retroalimentación de la salida a través de un modulador Σ–Δ.

sional suave $\dot{x} = f(x) + g(x)u$, con el mapa de salida escalar suave, $y = h(x)$. Asúmase que el controlador dinámico suave $u = -k(y,\xi)$, $\dot{\xi} = \varphi(y,\xi)$, con $\xi \in R^p$ localmente (globalmente, semiglobalmente) asintóticamente estabiliza el sistema hacia un estado de equilibrio constante deseado, denotado por X. Además, asúmase que la señal de control, u, es estrictamente acotada por el intervalo cerrado [0,1]. Entonces, el sistema en lazo cerrado

$$\dot{x} = f(x) + g(x)u$$
$$y = h(x)$$

$u_{av}(y, \xi) = -k(y, \xi, X)$

$$\dot{\xi} = \varphi(y, \xi, X)$$

$$u = \frac{1}{2}[1 + sign(e)]$$

$\dot{e} = u_{av}(y, \xi) - u$

exhibe una dinámica de deslizamiento ideal que es localmente (globalmente, semiglobalmente) asintóticamente estable al mismo punto de equilibrio constante, X, del sistema.

Demostración. La demostración de este teorema es inmediata al darse cuenta de que bajo la hipótesis hecha sobre la entrada de control promedio, u_{av}, el teorema anterior establece que un régimen deslizante existe sobre la variedad $e = 0$. Bajo las condiciones de invariancia: e = 0, $\dot{e} = 0$, que caracterizan la dinámica de deslizamiento ideal (véase Sira-Ramírez [6]), el control equivalente u_{eq}, asociado al sistema satisface que $u_{eq}(t) = u_{av}(t)$. Entonces, la dinámica de deslizamiento ideal se representa por:

$$\dot{x} = f(x) - g(x)\, u_{av}$$
$$y = h(x)$$

$u_{av}(y, \xi) = -k(y, \xi, X)$

$$\dot{\xi} = \varphi(y, \xi, X)$$

la cual se asume es localmente (globalmente, semiglobalmente) asintóticamente estable al punto de equilibrio deseado.

4. Realización Práctica del Modulador Σ–Δ

Idealmente, el modulador Σ–Δ conmuta a una frecuencia infinita, aunque tal demanda es imposible de llevar a cabo en la realidad. Una solución práctica para la realización de este modulador, operando a alta frecuencia de conmutación, pero finita, no afectaría los resultados principales notablemente. Para esto, se propone un modulador Σ–Δ basado en un *modulador por ancho de pulso* (MAP), que permite una frecuencia de conmutación finita seleccionada por el usuario. El diagrama a bloques del circuito que se propone se muestra en la **Figura 3**, mientras que en la **Figura 4** se muestra la implementación práctica. Esta realización práctica surge de reemplazar el bloque de conmutación del modulador Σ–Δ por un MAP clásico.

En referencia a la **Figura 3 y 4**, en la instrumentación del modulador Σ–Δ se distinguen cuatro bloques: un *restador,* un *integrador de señal*, un *generador de onda triangular* y un *MAP clásico*. El circuito generador de onda triangular se diseñó para producir una onda triangular de 40 kHz. Debido a que estos circuitos son de uso común, no se incluye la explicación de los mismos. En cambio, se recomienda al lector interesado revisar el libro presentado por Coughlin [2], donde cada uno de los bloques que conforman el diagrama de la **Figura 3** se explican en detalle.

En la **Figura 5** se muestra una fotografía del modulador que se implementó experimentalmente. En la **Figura 6** se presentan los resultados experimentales obtenidos en el prototipo desarrollado. Las pruebas se llevan a cabo de la siguiente manera: considerando el diagrama a bloques práctico del modulador Σ–Δ (**Figura 3**), la señal promedio $u_{av}(t)$ se hizo igual a 2.5 V (señal obtenida de una fuente de voltaje de CD), la señal resultante $u(t)$ es una señal conmutada de 40 kHz, la cual permite comandar apropiadamente el proceso de encendido y de apagado de sistemas conmutados.

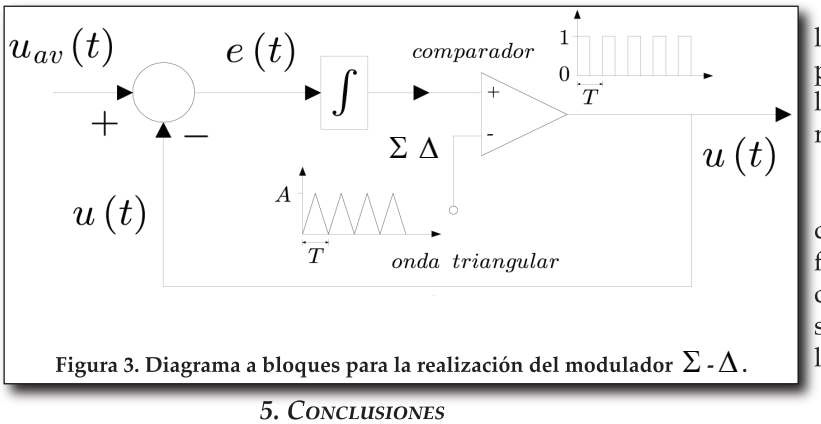


Figura 3. Diagrama a bloques para la realización del modulador Σ - Δ.

5. *Conclusiones*

En este trabajo se presentó la realización práctica de un modulador Σ–Δ, que se genera al reemplazar el bloque de conmutación del modulador Σ–Δ por un MAP clásico, lo cual permite que se obtenga una frecuencia finita de conmutación. La modulación Σ–Δ es propuesta como una manera de generar una señal lógica de frecuencia finita para ser usada como entrada a los dispositivos conmutadores de potencia y que al mismo tiempo se conserven las características cualitativas más relevantes del controlador diseñado con base a un modelo promedio.

A diferencia del método tradicional MAP para llevar acabo el control de sistemas conmutados, en este trabajo se propuso una manera novedosa de sintetizar controladores diseñados sobre la base de modelos promedios para ejecutar de forma apropiada las órdenes de encendido-apagado de los interruptores de potencia (transistores).

Con la finalidad de mejorar el desempeño del modulador Σ–Δ, se propone como trabajo futuro el llevar a cabo la síntesis del bloque de comparación sin el uso de un MAP. Para esto, se propone implementar el modulador Σ–Δ con la ayuda de FPGA.

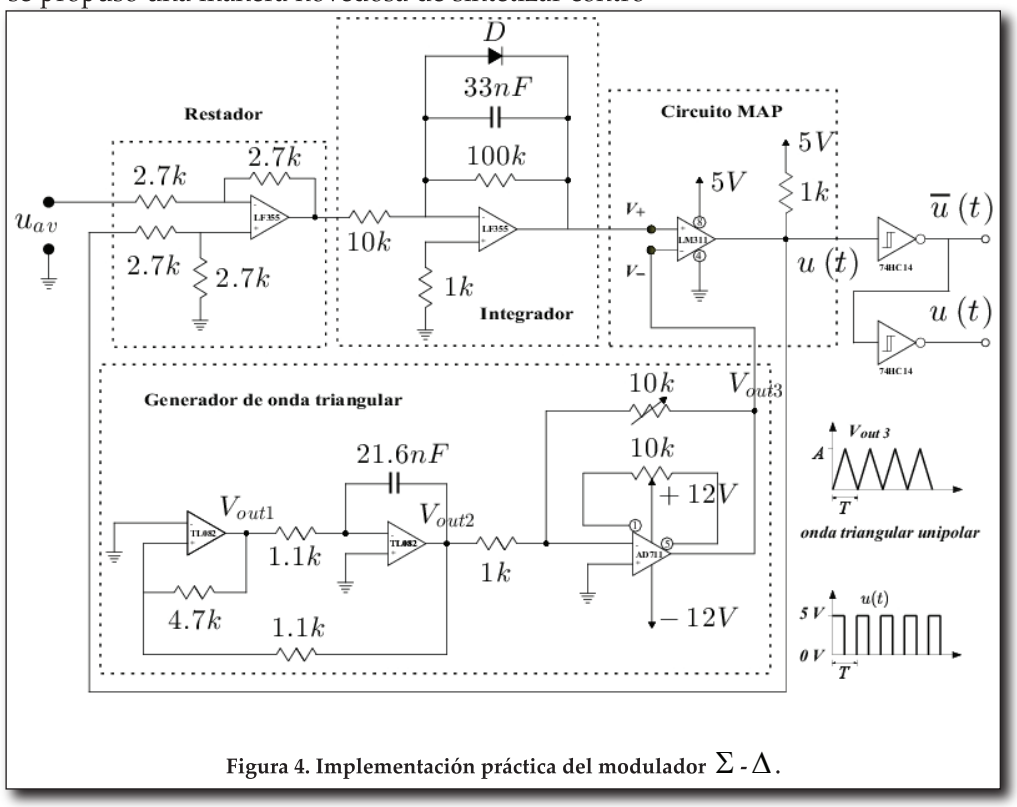


Figura 4. Implementación práctica del modulador Σ - Δ.

6. *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.

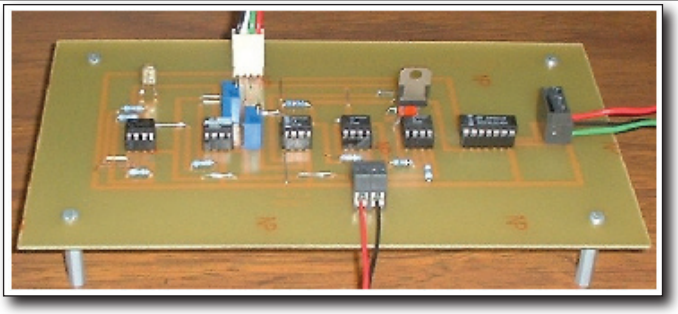


Figura 5. Fotografía del modulador Σ - Δ.

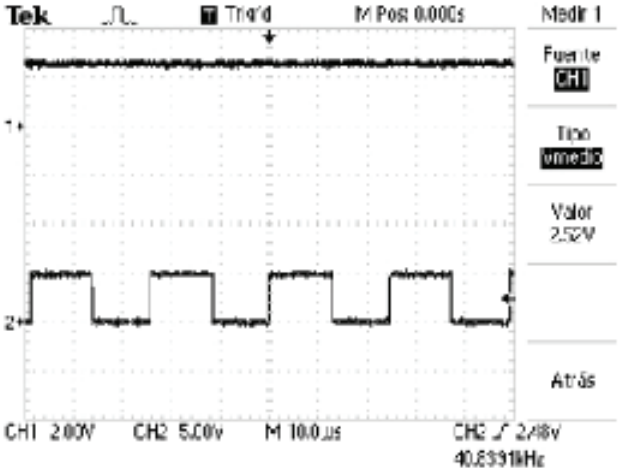


Figura 6. Resultados experimentales.

7. *Referencias*

[1] Batarseh I. (2004) Power electronics circuits. John Wiley and Sons, New York.

[2] Coughlin R.F., Driscoll F.F. (1982) Operational amplifiers and linear integrated circuits. Prentice Hall, Englewood Cliffs, New Jersey.

[3] Luckjiff G., Dobson I. (2005) Hexagonal Σ - Δ Modulators in Power Electronics. IEEE Trans on Power Electr 20:1075-1083.

[4] Norsworthy S., Schreier R, Temes G (1997) Delta-sigma data converters: theory, design, and simulation. IEEE Press, Piscataway, New Jersey.

[5] Sira-Ramírez H. (1987) Sliding Regimes in analog signal encoding and delta modulation circuits. Proc. 25th Annual Allerton Conference on Communications, Control and Computing. Vol. 1, pp. 78-87. University of Illinois at Urbana-Champaign, Ill.

[6] Sira-Ramírez H. (1988) Differential geometric methods in variable structure systems. Int J. of Control 48:1359-1391.

[7] Sira-Ramírez H. (2003) Sliding mode Δ modulators and generalized proportional integral control of linear systems. Asian J. of Control 5:467-475.

[8] Sira-Ramírez H., Silva-Ortigoza R. (2005) Sliding mode Σ–Δ modulation control of the boost converter. Asian J. of Control 7:1-7.

[9] Sira-Ramírez H., Silva-Ortigoza R. (2006) Control Design Techniques in Power Electronics Devices. Springer-Verlag, London.

[10] Steele R. (1975) Delta modulation systems. Pentech Press, London.

[11] Utkin V. (1978) Sliding modes and their applications in variable structure systems. Mir Publishers, Moscow.

Arquitectura de las Redes Ad-Hoc

Maria Aurora Molina Vilchis,
Ramón Silva Ortigoza
CIDETEC-IPN
Eleazar Bracho Molina
UAMI, Licenciatura en Computación

Desde el nacimiento de la tecnología de redes de computadoras a fines de la década de los sesenta, las actividades cotidianas del ser humano en la civilización contemporánea han incluido el uso intensivo y extensivo de estos sistemas de comunicación, estableciendo de este modo un vínculo estrecho entre la tecnología y la cotidianeidad. No obstante, entre las primeras redes y las actuales existe una gran brecha. Del paradigma multiusuario (muchos usuarios comparten un solo CPU), pasamos a otro, el de la computación personal (un solo usuario para un CPU). Hoy en día, el paradigma imperante es el de la computación sin infraestructura, en la que un solo usuario se conecta a muchos dispositivos de procesamiento; si a este último se le adiciona la cualidad de establecerse en el momento y en todo lugar, entonces nacen los conceptos de redes Ad-hoc y redes ubicuas. Sin embargo, cabe destacar que esto no sería posible sin la evolución de los dispositivos de comunicación móviles, tales como los teléfonos celulares, computadoras portátiles, organizadores electrónicos, etc. y de los esfuerzos que organismos como la IEEE han realizado para la generación de los estándares de soporte.

1. Redes Inalámbricas de Área local WLAN

Una WLAN (*Wireless Local Area Network*) de acuerdo a la IEEE [1], es un sistema de comunicación de datos implementado como extensión o alternativa de una red cableada, constituyendo el estándar para la realización de redes Ethernet sin hilos, por lo que es especialmente apropiada para la comunicación con dispositivos móviles. Esta tecnología esta estandarizada según la norma IEEE 802.11; sin embargo, el estándar dominante de WLAN (conocido también como Wi-Fi) es IEEE 802.11b. Dicho estándar señala que la transmisión-recepción de datos se realiza mediante tecnología de radio frecuencia utilizando como medio de propagación el aire, por lo que permite la movilidad del usuario dentro de un entorno de conexión de red. Otra de las ventajas de usar un sistema *wireless* se refiere a la portabilidad física de la infraestructura de la red, lo cual permite que el sistema se adapte a las necesidades típicas en las empresas, ya que utiliza transmisiones por medio de enlaces de radio de corto alcance, en la llamada banda ISM (*Industrial Scientific and Medical*), que incluye los rangos de 900Mhz, 2.4GHhz y 5Ghz. [2].

La configuración típica de una WLAN incluye uno o más puntos de acceso fijos conectados a una LAN mediante un cable de datos tradicional. El punto de acceso se difunde y recibe la información de los usuarios dentro de un rango de transmisión, denominado celda, por lo que todo el tráfico proveniente de las estaciones inalámbricas pasa a través de un punto de acceso para llegar a su destino. El usuario debe contar con un adaptador inalámbrico, de esta forma se elimina el enlace físico de la red tradicional permitiéndole conectarse directamente a un sistema de distribución sin cables ni hilos de interconexión.

2. Clasificación de las WLAN

Para hacer una clasificación de las WLAN se emplean criterios tales como: cobertura, servicios, componentes, etc., que nos ayuden a ubicar los diferentes tipos de redes que han surgido a partir de esta tecnología. Uno de ellos son las redes Ad-hoc, estas son redes punto a punto, donde varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utiliza en grupos de trabajo, reuniones, conferencias, etc. Las redes Ad-hoc [3], se dividen en MANET (*Movile Ad-hoc Network*),

Bluetooth, WSN (*Wireless Sensor Network*) y WSAN (*Wireless Sensor Actuator Network*). Bluetooth [4], se ha mostrado como una plataforma de soporte prometedora en las redes Ad-hoc, consolidándose como el estándar inalámbrico de corto alcance y bajo costo, especialmente dirigido para conectar dispositivos, tales como los PDA, las computadoras portátiles y los teléfonos móviles por medio de enlaces de radio. También opera en la banda ISM a 2.4 Ghz; esta es la tecnología usada por el grupo de trabajo IEEE 802.15.1, dedicado a las redes inalámbricas de área personal (WPAN); además emplea un esquema de funcionamiento orientado a conexión y basado en una configuración maestro-esclavo, en la cual un único maestro coordina el acceso al medio de hasta siete dispositivos esclavos mediante turnos de preguntas periódicas.

En este artículo se presenta la arquitectura básica de las redes Ad-hoc, resultado del análisis de las normas del Comité 802 de IEEE, respecto a las redes WLAN, de las cuales se originan. La sección 2 trata sobre el concepto de redes Ad-hoc, mientras que la sección 3 menciona la arquitectura de éstas en los niveles físico, enlace de datos y red. Y finalmente, la sección 4 describe el panorama en lo referente a los sistemas operativos y aplicaciones.

3. Redes Ad-hoc

La topología Ad-Hoc [5] es en la que no existe un nodo central, sino que cada dispositivo se comunica con todos los demás. Cada nodo, potencialmente móvil, forma parte de una red punto a punto, por lo que todos se encuentran en igualdad de condiciones, es decir, el transmisor o el receptor es siempre un punto de acceso. Lo anterior significa que los nodos participan en la toma de decisiones para el encaminamiento de los paquetes (ruteo); además, retransmiten paquetes entre los nodos que no tienen conexión inalámbrica directa. Estas redes pueden desplegarse de manera autónoma, organizarse y configurarse por si mismas, contando con la capacidad de combinarse con otras redes inalámbricas para conectarse a Internet mediante un punto de acceso (PA). Estas redes deben diseñarse tomado en cuenta las siguientes características: topología dinámica, distribución de carga de procesamiento de datos, manejo eficiente de energía y ancho de banda.

En general, el funcionamiento de una red Ad-hoc se describe considerando que: a) un nodo tiene que identificar los PA y las redes disponibles de acceso, b) la estación elige una red entre las que están disponibles y sigue un proceso de autenticación con el punto de acceso, c) la asociación permite que el PA y la estación intercambien información y capacidades.

Las redes Ad-hoc se asocian con frecuencia con las redes MANET (*Mobile Ad-hoc Networks*) ya que su tecnología de comunicación es ideal para un entorno totalmente móvil, en el que teléfonos celulares, PDA, dispositivos sensores, electrodomésticos, libros electrónicos, etc., se interconectan para cooperar y comunicarse de forma inteligente, para satisfacer las necesidades del usuario. Los fabricantes más importantes de esta tecnología son [3]: Dell, Gateway, IBM, NEC, Toshiba, Sony, Motorola, Ericsson, entre otros.

4. Arquitectura

4.1 Nivel físico

Dos organismos que estandarizan a las redes WLAN son IEEE y ETSI (*European Telecomunications Standards Institute*), y una alianza tecnológica llamada Home RF es quien las promueve. En IEEE la norma esta referida por la familia 802.11, de la que los estándares más usados hasta ahora, por orden de preferencia son: el 802.11b, el 802.11a, y el 802.11g. A continuación se describen dichos estándares:

802.11b (WiFi). Es el estándar más popular, a pesar de que la especificación fue aprobada al mismo tiempo que 802.11a en 1999. La técnica de modulación usada en 802.11b es DSSS (*Direct Sequence Spread Spectrum*), mientras que 802.11a utiliza OFDM (*Orthogonal Frecuency División Multiplexing*), dado que es mas sencillo implementar DSSS; compañías importantes tales como Cisco, Lucent, Agere Systems, Proxim y 3com han generado productos basados en 802.11b. El rango de frecuencia asignado para este estándar es de 2.4 a 2.48 Ghz, el cual esta disponible en todo el mundo para configuración de WLAN; además, las señales dentro de este rango pueden penetrar barreras físicas tales como muros y techos con mayor facilidad que las frecuencias más altas.

Este estándar cuenta con un certificado por la alianza WiFi, formalmente conocida como WECA (*Wireless Ethernet Compatibility Alliance*), y es seguro que los productos que funcionan bajo este estándar pueden interoperar con otros productos a nivel mundial. En teoría, para aplicaciones típicas de oficina, un PA que funciona sobre 802.11b puede comunicarse con dispositivos alejados hasta 100 m, pero mientras más alejado este el dispositivo

la velocidad de transmisión disminuye, y esto varia de acuerdo al fabricante, de tal forma que los dispositivos alejados hasta 30 m del PA tienen una velocidad de hasta 11Mbps. No obstante, a más de 30 m la velocidad cae hasta 5.5 Mbps sobre TCP y 7.1 Mbps sobre UDP.

Por otro lado, para dispositivos ubicados más allá de 65 m, la velocidad alcanza aproximadamente 1 Mbps, cuando el dispositivo se encuentra en el limite del área de cobertura del PA [6]. Adicionalmente, esta norma proporciona mecanismos de seguridad [4] en lo referente a la autenticación y cifrado por medio de WEP (*Wired Equivalent Privacy*), este protocolo emplea el algoritmo RC4 de RSA *Data Security* para cifrar transmisiones con la utilización de una clave secreta de 40 bits.

802.11a. Este estándar transmite en la banda de 5 Ghz, Sus dos principales ventajas son: a) Tiene una velocidad de transmisión de hasta 54 Mbps, ya que usa como técnica de modulación OFDM, por lo que no es compatible con las redes 802.11b. Esta velocidad es una gran ventaja tomando en cuenta que el ancho de banda esta disponible entre todos los usuarios que acceden al PA, y b) la banda utilizada no se encuentra tan congestionada como la de 2.4 Ghz, lo cual repercute en menor interferencia. Algunas de sus desventajas se deben a que las frecuencias de operación mayores cubren áreas pequeñas, lo cual significa que para mantener esa velocidad de transferencia se requieren varios PA para cubrir la misma área; a diferencia de 802.11b, 802.11a tiene una cobertura de 24 a 50 m.

802.11g. Este estándar trabaja en la banda de 2.4 Ghz y utiliza la misma técnica de modulación DSSS, puede alcanzar hasta 11 Mbps al igual que 802.11b, por lo que es de esperarse que exista compatibilidad entre ambos. Sin embargo, también es compatible con 802.11a, ya que para alcanzar velocidades de hasta 54 Mbps usa una modulación OFDM más eficiente, aún en la banda de 2.4 Ghz. En la práctica, una tarjeta de red 802.11g es compatible con un PA que funciona sobre 802.11b y una tarjeta de red 802.11b es compatible con un PA que funciona sobre 802.11g, la velocidad de transferencia máxima que se alcanzaría en ambos casos sería de 11 Mbps. Para alcanzar hasta 54 Mbps tanto la tarjeta de red como el PA tendrían que operar de acuerdo a 802.11g.

4.2 Nivel de enlace de datos

La capa MAC[1] según la especificación 802.15.3 soporta QoS (*Quality Of Service*) en servicios multimedia, para ello se emplea una supertrama MAC que consiste en un intervalo guía, un periodo CAP (*Contention Access Period*) y un periodo libre de contienda GTS (*Guaranteed Time Slots*). El límite entre los periodos CAP y GTS es dinámico y ajustable. El periodo CAP esta reservado para el envío de tramas de datos que no se especifican con QoS, por lo que se transmiten a manera de ráfagas o bien por un requerimiento de acceso al canal por parte de los dispositivos en la red. Hay dos tipos de mecanismos de acceso al medio: a) Protocolos con arbitraje (FDMA - *Frequency Division Multiple Access, TDMA – Time Division Multiple Access*) y b) protocolos de contienda (CSMA/CA – *Carrier Sense, Multiple Access, Collision Avoidance*), CDMA (*Code División, Multiple Access*) y el CSMA/CD (*Carrier Sense, Múltiple Access Collision Detection*), los cuales tienen similitudes al de Ethernet cableada, (IEEE 802.3).

En cuanto a las tarjetas de red más conocidas, están aquellas que vienen en formato PCMCIA (*Personal Computer Memory Card International Association)*, otros formatos son PCI, CompactFlash, SmartCard y casos como DELL, cuyos equipos usan tarjetas propietarias WLAN Dell™ TrueMobile [7]. La mayoría de las tarjetas que se venden actualmente son del tipo Orinoco (Lucent), Symbol HR y Prism 2 de Intersil. Todas ellas están soportadas por el driver orinoco_cs, incluido en el kernel 2.4.x de Linux, pero sólo para trabajar en modo *managed* o Ad-hoc, pues no soportan el modo *master* [8], de esta manera la configuración de las tarjetas de red en una red Ad-hoc es igual a nivel IP a la de una tarjeta Ethernet.

Las tarjetas inalámbricas tienen básicamente tres modos de trabajo:

1) Modo Ad-hoc, estas redes se construyen normalmente con computadoras con las tarjetas comunes y se configuran de forma que todas las computadoras de la red trabajen en modo punto a punto.

2) Manager, en este caso existe un servidor independiente al cual se conectan todas las computadoras. El *PA* entonces envía las tramas 802.11 a los destinatarios finales. Normalmente los *PA* soportan *roaming*, es decir los clientes pueden estar en movimiento e ir cambiando de punto de acceso de acuerdo a la potencia de la señal.

Los parámetros específicos más importantes para tarjetas inalámbricas son [7] [8]: identificador de red, frecuencia o canal, modo de trabajo, velocidad, clave de cifrado y potencia de transmisión.

4.3 Nivel de red

Los protocolos de encaminamiento se dividen en dos categorías [9]: proactivos[2] y reactivos[3]. Los protocolos proactivos utilizan tablas de ruteo, cuando hay un cambio, la información se envía a cada nodo para que actualice su tabla, este es el caso de OLSR (*Optimized Link State Routing).* No sucede así con los protocolos reactivos, que usan algoritmos de ruteo por estado del enlace para enviar frecuentemente información a los nodos informándoles sobre el estado de los enlaces con sus vecinos. A estos protocolos se les conoce también como protocolos de ruteo por demanda. En un principio, muchas propuestas de estos protocolos fueron evaluadas, sin embargo, hoy en día solamente cuatro de ellas han resistido la fuerte competencia, estas propuestas son [10]: AODV (*Ad-hoc On Demand Distance Vector*), DSR (*Dynamic Source Routing for Protocol Mobile Ad-hoc Networks*), OLSR (*Optimized Link State Routing Protocol*) y TBRPF (*Topology Broadcast based on Reverse- Path Forwarding*). De estas cuatro solo AODV y OLSR han alcanzado el nivel de RFC (*Request For Comment*), con los números 3561 para el primero y 3626 para el segundo.

AODV (Ad-hoc On-Demand Distance-Vector Routing Protocol)

El protocolo AODV esta basado en el algoritmo vector distancia DSDV (*Destination Sequenced Distance-Vector Routing Protocol*) [11] por lo que los nodos mantienen una tabla de encaminamiento para los destinos conocidos. Inicialmente esta tabla estará formada por sus vecinos, y solamente se le añaden destinos nuevos cuando es necesario. Es decir, cuando un nodo necesita comunicarse con otro que no está en su tabla, inicia un proceso de descubrimiento de ruta hacia el destino concreto. Cada nodo mantiene un contador propio de número de secuencia, el cual se incrementa constantemente para identificar las rutas obsoletas que conducen hacia él. De este modo, para cada destino del cual se asigna un número designado a una ruta en un nodo, este número se almacena en una tabla de encaminamiento junto con la dirección IP del siguiente salto. Una ruta expira si no se usa o reactiva dentro de un umbral de tiempo determinado.

DSR (Dynamic Source Routing)

El protocolo DSR se fundamenta en el encaminamiento desde el origen, es decir, los paquetes de datos incluyen una cabecera de información acerca de los nodos exactos que deben atravesar, ya que esta basado en algoritmos de estado de los enlaces, lo cual significa que cada nodo es capaz de guardar de la mejor manera las direcciones destino, por lo que se le considera reactivo. Además no requiere de mensajes periódicos, disminuyendo así la sobrecarga con mensajes de control. Por otro lado, posibilita obtener, con la solicitud de una ruta, múltiples caminos posibles hacia el destino, lo que permite el establecimiento de los enlaces unidireccionales sin problema, a diferencia de la mayoría de protocolos de ruteo en este tipo de redes. Así, cada nodo mantiene una memoria caché de rutas en la que se van almacenando las rutas obtenidas a través de procesos de descubrimiento de caminos, ya sean propios u obtenidos a través de escuchas en la red. En caso de ocurrir un cambio en la topología de la red la información es compartida a todos los nodos de la misma por medio de inundación.

OLSR (Optimized Link-State Routing Algorithm)

OLSR incorpora la filosofía utilizada en protocolos tradicionales de *estado del enlace*. En este algoritmo todos los nodos intercambian mensajes para formar una visión consistente de toda la red y así poder decidir el encaminamiento de paquetes. OLSR adolece del mismo problema que DSDV debido a la necesidad de intercambio de un gran número de mensajes periódicos (a menudo se dice que es proactivo por esta razón). Aquí el problema podría llegar a ser mayor, ya que además de mensajes a los vecinos, envía mensajes de control TC (*Topology Control*) que se retransmiten a todos los nodos de la red. Sin embargo, se ha conseguido una gran optimización en la retransmisión de estos mensajes con la incorporación de la técnica de retransmisión multipunto, a través de la cual, los mensajes sólo son retransmitidos por el mínimo número de nodos necesarios para alcanzar a todos los demás. Estos nodos son conocidos como Grupo de Retransmisores Multipunto (MPR's).

TBRPF ((Topology Broadcast based on Reverse- Path Forwarding)

El protocolo TBRPF proporciona el descubrimiento de la topología de manera completa de forma automática y al igual que OLSR se basa en el estado de los enlaces, siendo además un protocolo proactivo. Su funcionamiento consiste en almacenar la ruta más corta hacia

todos los posibles destinos, por lo que no hay retardos al establecer la ruta, esto significa que el tráfico de control y actualización de la topología es mínimo, siempre y cuando la movilidad de la red sea baja. Pero cuando el número de nodos aumenta, surgen otros problemas en la red.

5. Sistemas Operativos y Aplicaciones

5.1 Sistemas operativos

Para crear una red Ad-hoc se necesita de un adaptador o programas de ruteo; los más utilizados en la actualidad son el de Intel® Pro/Wireless LAN 2100 3A Mini PCI Adapter y el Winroute, con este último se puede crear un centro de comunicaciones con diversos sistemas de conexión para Internet, para casi cualquier dispositivo existente.

Entre los sistemas operativos que destacan para el modo Ad-hoc, podemos citar a Windows XP y Vista de Microsoft [12], para configuración en modo Ad-hoc. En ambos casos, para simular la conexión del cable cruzado entre 2 tarjetas de red se cuenta con los componentes para la conexión con Internet y de seguridad WEP.

Por otro lado, Windows CE de Microsoft [12] que es independiente de Windows XP o NT, se desarrolló para dispositivos móviles de 32 bits. Combina la compatibilidad y las pruebas a servicios de aplicación avanzados de Windows con soporte para múltiples arquitecturas de CPU y opciones incluidas de comunicación y redes que proporcionan una fundación abierta para una variedad de productos, con la finalidad de impulsar los dispositivos electrónicos del cliente, terminales Web, dispositivos de acceso a Internet, controladores industriales especializados, computadoras de bolsillo, dispositivos de comunicación incrustados e incluso consolas de video juegos. Esta plataforma modular permite a los diseñadores crear software para que la nueva generación de dispositivos móviles de 32 bits pueda integrarse con Windows e Internet. Otro sistema operativo para modo Ad-hoc es Symbian [13], producido por la alianza de varias empresas prominentes de telefonía celular, entre las que se encuentran Nokia, Sony Ericsson, Samsung y Siemens; el propósito inicial de este producto era crear un sistema operativo para terminales móviles capaz de competir con los sistemas operativos Palm o Windows Mobile de Microsoft.

5.2 Aplicaciones

Hoy en día las aplicaciones de las redes Ad-hoc más populares están basadas en Bluetooth, de tal forma que un dispositivo puede establecer una conexión instantánea con otra que esta dentro del rango. Algunos ejemplos son: hacer llamadas desde un auricular conectado remotamente a un telefono celular, conectar un reproductor MP3 a otros dispositivos para bajar música, instalar redes caseras para monitorear el aire acondicionado, el horno de microondas y restringir el acceso a Internet a menores, hacer llamadas a casa desde una ubicación remota para encender o apagar electrodomésticos, poner la alarma, monitorear actividades, etc.

Otros usos se dan en maniobras militares implementando una clase específica de redes Ad-hoc, llamadas WSN (*Wireless Sensor Network*), es el caso del FBCB2 (*Force XXI Battle Command, Brigade and Below*), que es un sistema digital basado en Ad-hoc para uso militar, este es un componente clave del sistema ABCS (*Army Battle Command System*) que consiste en la fusión de hardware y software que interconecta varias plataformas a través de la infraestructura de comunicaciones existente, llamada *Tactical Internet* construida por redes EPLRS (*Enhanced Position Location Reporting System*) [16] y SINCGARS (*Single Channel Ground and Airborne Radio System*) [17].

6. Conclusiones

La evolución de las redes se basa fundamentalmente en el desarrollo tecnológico de los dispositivos de comunicaciones móviles, así como de los desarrollos en materia de los sistemas operativos y las aplicaciones, hoy en día orientadas a las necesidades personales. El intercambio de información multimedia entre dispositivos facilita su almacenamiento, procesamiento y recuperación. Un pilar fundamental en la consolidación de cualquier tipo de red es el conjunto de estándares generados y por lo tanto avalados por organismos internacionales, tales como IEEE, ETSI y Home RF. El estudio de las redes Ad-hoc, igual que para cualquier tipo de red, puede realizarse a partir de su arquitectura, el conocimiento de las funciones del nivel fisico así como de los protocolos de los niveles MAC y red, lo que permite al estudioso del tema localizar los aspectos críticos y descubrir nuevas líneas de investigación, previendo así su futuro en el gran concierto de las redes de computadoras.

7. *Agradecimientos*

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

8. *Referencias*

[1] Chlamtec I., Corli M., and Liy J.J.N., "Mobile Ad-hoc networking: Imperatives and Challenges, Ad-hoc Networks", Vol 1, No.1, July 2003. pp 13-64.

[2] Nichols R.K., Panos C., "Seguridad para Comunicaciones Inalámbricas", Mc Graw Hill, México D.F., 2004, pp 362-363.

[3] John R. Vacca, "Wireless Data Demystified", Mc Graw Hill, USA, 2003.

[4] Cano J.C., Calafate C.T., Malumbres M. P., and Manzoni P., "Redes Inalámbrica Ad-hoc como tecnología de soporte para la computación ubicua", ver: www.grc.upv.es/calafate/downñload/main_novatica.pdf.

[5] Broch J., Maltz D.A., Johnson D.B., Hu Y., and Jtcheva C., "A performance comparison of multi hop wireless Ad-hoc network routing protocols", in 4th Annual ACM/IEEE Int/ Conf. on Mobile Computing and Networking, ACM Press, 1998, pp 85-97.

[6] Mallick M., "Mobile end Wireless Design Essentials". Wiley Publishing Inc, USA, 2003.

[7] Manuales Dell para win 2000 y Win XP, disponible en http://support.dell.com/support/edocs/network/p54164/sp/tasks.htm

[8] Galli Granada R., "Redes Wireless con Linux", ver http://bulma.net/body.phtml?nIdNoticia=1309

[9] Hong X., Xu K., and Gerla M, "Scalable Routing protocols for Mobile Ad-hoc Networks", Computer Science Departament, University of California, Los Angeles, August 2002.

[10] Villaseñor Garcia L. A., "Macromovilidad Ip para redes móviles Ad- hoc (MANETS)", ver: http://usuario.cicese.mx/~luisvi/Congresos/Presentacion-TI07.ppt#352,3,Introducción

[11] Pekins C., Belding R. E. and Das S., "Ad-hoc On Demand Distance Vector (AODV) Routing", RFC 3661, Jul.2003.

Sistema de Manufactura Flexible con Restricciones Temporales (Descripción)

José de Jesús Medel Juárez
CIC-IPN
Gabriel Hernández López, Jacobo Sandoval Gutiérrez
CICATA LEGARIA-IPN

Básicamente, los diseñadores de sistemas de manufactura flexible reconocen cuatro modelos definidos en el área de manufactura moderna. Sin embargo, desde hace algunos años la idea más ambiciosa respecto a estos procesos ha sido la Fábrica Flexible, en donde el objetivo principal está basado en la integración de todos los subprocesos a través de una planificación computacional, considerando en ello a todos los sistemas productivos que interactúan dentro del esquema de producción, de tal forma que dentro del sistema computacional el planificador considera variables de control acotadas por la interacción entre procesos, el volumen de producción y la variedad de productos. En este artículo, adicionamos las restricciones de tiempo como un recursos necesario dentro de los esquemas de planificación.

Palabras clave: *Sistemas de Manufactura Flexible, restricciones temporales.*

1. Introducción

Un Sistema de Manufactura Flexible (SMF) está integrado por máquinas-herramientas enlazadas mediante un esquema de manejo de materiales de manera automatizada y procesados lógicamente, es decir, es un sistema de producción de bienes constituido por celdas de producción[1].

En términos generales un SMF está compuesto por:

- Una o varias máquinas-herramienta de control numérico computarizado (MHCNC), que desempeña tareas de maquinado usando una lista de instrucciones en clave mediante una lógica digital. Ellas son vistas como los recursos compartidos, usados por varios subprocesos.
- El Diseño Asistido por Computadora (CAD); que se utiliza para la creación de objetos por computadora con capacidades interactivas y de graficación, por medio de las cuales las fases de este subproceso pueden hacerse visibles de una manera tridimensional. [1]
- Robot, el cual es un manipulador multifuncional reprogramable con varios grados de libertad, capaz de manejar materias, piezas, herramientas o dispositivos especiales según trayectorias variables programadas para realizar tareas diversas, colocando de una manera sincronizada los materiales a ser manufacturados en el lugar de trabajo según el ciclo a desarrollar. [2]
- Dispositivos de salida (actuadores neumáticos, electroneumáticos, hidráulicos y electrohidráulicos), los cuales son los medios que habilitan o sujetan las partes que integran al producto.
- Dispositivos de entrada, que son todos aquellos sensores que alimentan al sistema con una señal digital, proveniente de la presencia de una parte del producto, el inicio o el final de una operación.
- Sistema de control, montado dentro de una computadora central (SCC) y que se encarga de coordinar todas las operaciones del sistema de manufactura flexible registrando, realizando operaciones de planificación, de monitoreo y propiamente de control de los estados del sistema de producción.

En general, los SMF cuentan con diferentes fallas, las cuales pueden ser clasificadas como recurrentes.

1.1 Fallas Recurrentes

Las fallas que tiene un SMF en su actuar repercuten en la calidad del producto, tales como los problemas de ensamble, exceso de material, deformaciones dimensionales, entre otras, y se les llama fallas de información, programación y operación.

1 Una celda de producción es la unidad de producción con alta autonomía de operación, integrada por máquinas para fabricar un tipo de pieza o producto.

La falla se define como el incumplimiento de una o varias de las especificaciones requeridas por el mundo físico con el cual interactúa el SMF [3]. Utilizando esta definición para el estudio de un SMF y considerando a la información en la programación y a la operación se tiene:

Una falla de información es la variación de resultados con respecto a lo establecido, mientras que una falla en programación es la falta de sincronización con el mundo físico. Por su parte, una falla en operación es cualquier incumplimiento en las especificaciones del sistema y del producto. Bajo el respaldo de todo lo anterior, se procede a plantear el siguiente análisis que fundamenta al tiempo real en los SMF.

1.2 Parámetros de una SMFTR

Para el ejemplo a desarrollar se toma como referencia un SMF en el cual se van a procesar dos productos, y que tiene operaciones atómicas que utilizan los mismos recursos y que permiten dar una respuesta sin que se pierdan las propiedades temporales por obstrucción entre ellas. Intrínsecamente requiere de cumplir con la sincronía, al igual que la entrega de cada uno de los productos, con una calidad que en promedio sea aceptable, dimensionalmente hablando.

El SMF utilizado está estructurado con tres estaciones: Almacén de Materia Prima (Robot SCARA ER-14 ESHED ROBOTEC, sistema sensorial y dispositivos electroneumáticos), Maquinados (centro de torneado, Centro de Fresado, Robot Antropomorfo IRB 140 ABB, sistema sensorial y dispositivos electro neumáticos) e Inspección/Ensamble (Robot Antropomorfo MK-2 ESHED ROBOTEC, sistema sensorial y dispositivos electroneumáticos), todas ellas en comunicación gracias a un sistema de red local CC-Link (Comunicación Central en línea), y como elemento de control operacional se

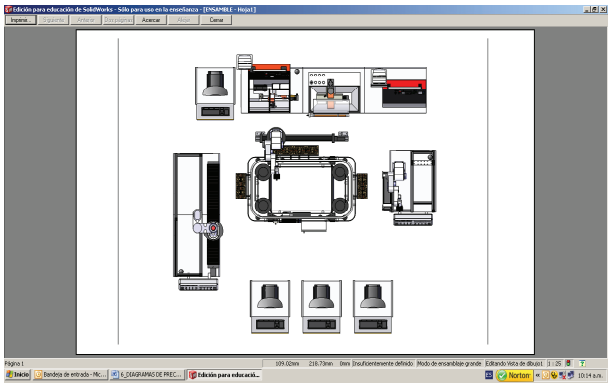


Figura 1.Esquema del SMF de la Escuela de Ingeniería de la Universidad Panamericana.



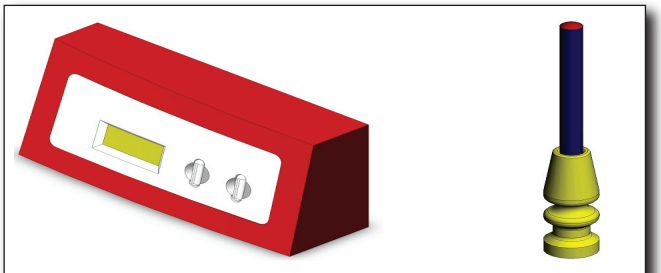
Figura 2. SMF de la Escuela de Ingeniería de la Universidad Panamericana.

tiene al Controlador Lógico Programable (PLC) el cual es programado con un lenguaje de alto nivel (Visual Basic). Cabe mencionar que cada estación cuenta con medios de información que muestran características de producción (Productos solicitados, tiempo de operación, etc.). (Ver **Figuras 1** y **2**).

Por tanto, y en consideración de las capacidades del SMF en términos de características geométricas, dimensionales, físicas y estéticas, los productos a fabricar son: 1) Maquinado y Ensamble de un Cronómetro y 2) Maquinado y Ensamble de un Porta-Plumas. (**Figura 3**).

Estos dos productos se desglosan por operaciones atómicas de cada producto, y además requieren de un tiempo determinado para su ejecución, el cual está determinado por la complejidad de la misma operación. En las tablas se observa su interacción con cada parte del sistema, además de los tiempos de ejecución de cada operación; sin embargo, para cuestiones de adaptabilidad de un control eficiente en un SMFTR es necesario considerar el flujo de proceso como un diagrama de precedencia integrado.

El cronómetro consta de dos partes: Contenedor y Reloj; mientras que el Porta-Plumas tiene Base y Pluma.



(a) **(b)**

Figura 3. a) Cronómetro y b) Porta-Plumas.

Productos	Partes del Producto	Estación				
		Almacén	Maquinados		Inspección y Ensamble	
			Torneado	Fresado	Inspección	Ensamble
Cronometro	Contenedor	■		■	■	■
	Reloj	■				■
Porta-Plumas	Base	■	■		■	■
	Pluma	■				■

Tabla 1. Desarrollo de manufactura de los dos productos en el SMF.

Su desarrollo en el proceso de manufactura se muestra en la **Tabla 1**. Realizando un estudio se obtuvieron los tiempos de cada operación (Ver **Tabla 2**). Es importante considerar que el tiempo de transporte a cada estación es de 5 s, por tanto para el Cronómetro se tiene un tiempo total de 173 s y para el Porta-Plumas es de 133 s.

En estas condiciones y para producción en línea, considerando que se requieren producir 100 Cronómetros y 100 Porta-Plumas, el tiempo de entrega sería tomando de referencia que la primera orden de producción es de los cronómetros, con un parcial de 4.80 hrs, y con 3.69 hrs. para el Porta-Plumas; así, el tiempo total de entrega es de 8.49 hrs.

Para las condiciones de un SMFTR que no sea de proceso en línea y en que toda acción corresponde a un proceso FIFO (FIRST INPUT/FIRST OUTPUT), además de poder tomar decisiones con base en la disponibilidad de los recursos, permitiendo que en todo momento el equipo este en operación, es decir un flujo combinado serie-paralelo, ejecutando n-duplas de operaciones. **Figuras 4** y **5**.

Con estas consideraciones, las cuales son las ideales de operación de un SMF, se tiene que el tiempo de entrega será el de producción del Cronómetro, es decir, 4.80 hrs., lo que representa una eficiencia del 43% en el sistema, y considerando que el SMF cuenta con sus componentes independientes y comunicados entre ellos a través de una red local CC-Link, en sincronía con el entorno gracias a sus I/O cumpliendo con respuestas aleatorias y temporales impuestas por el ciclo del proceso.

Las operaciones realizadas en el SMF tienen principio y fin, es decir están en un ciclo específico y combinado dentro del mismo sistema.

Productos	Partes del Producto	Estación					Tiempo Total
		Almacén	Maquinados		Inspección y Ensamble		
			Torneado	Fresado	Inspección	Ensamble	
Cronometro	Contenedor	5 s		108 s	8 s	32 s	153 s
	Reloj	■				■	
Porta-Plumas	Base	5 s	66 s		8 s	21 s	113 s
	Pluma	5 s				8 s	

Tabla 2. Desarrollo de manufactura de los dos productos en el SMF y tiempos de manufactura.

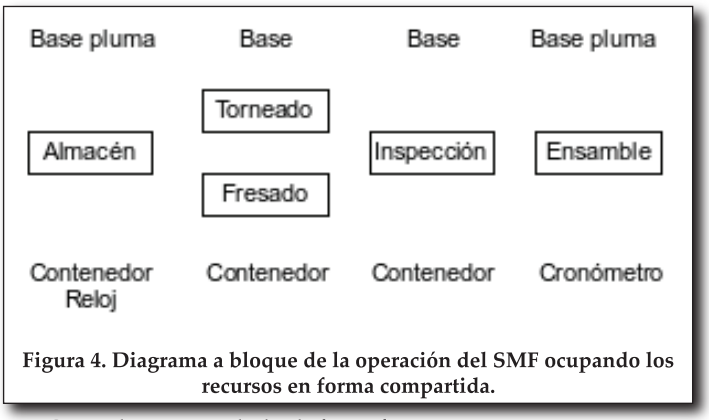


Figura 4. Diagrama a bloque de la operación del SMF ocupando los recursos en forma compartida.

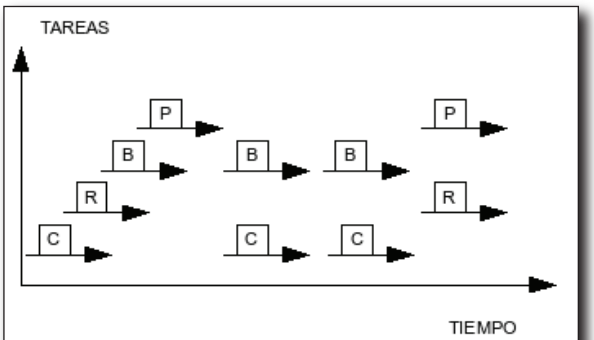
Complementando la definición anterior, se tiene que por ser un ciclo en especial también debe cumplir con un tiempo específico, y dentro de la manufactura esto es vital para lograr cumplir con los tiempos estándar de producción.

Finalmente, todas las proposiciones conducen a decir que el SMFTR está en sincronía en sus operaciones gracias a la respuesta de las E/S en forma aleatoria y temporales que se tienen cuando el sistema está en operación. Con esta fundamentación se dice que el comportamiento del sistema es el siguiente:

A. Interacción con el mundo real. Se está aplicando en un sistema de producción real y además en una operación cotidiana de la industria.
B. Respuestas correctas. La operación debe cumplir con las especificaciones técnicas y el sistema registra información verídica de lo sucedido en la operación.
X. Respuesta acotada en tiempo. Ya que cumple con un tiempo acotado; y esto se ejemplifica en la ecuación

$$T_{T_o} = T_i + T_e + T_{Rf1} + \ldots + T_{Rf6} \leq t_p$$

Donde:



C= Cronómetro; R = Reloj, B= Base y P= Pluma.

Figura 5. a) Ciclo de operación del SMF ocupando los recursos en forma compartida

T_{T_o} = Tiempo total de operación.
T_i = Tiempo de inicio.
T_e = Tiempo de ejecución.
T_{Rf1} = Tiempo de recuperación de falla 1.
T_{Rf2} = Tiempo de recuperación de falla 2.
T_{Rf6} = Tiempo de recuperación de falla 6.
t_p = Tiempo del ciclo del proceso

Sin embargo, para las condiciones del SMF con operaciones atómicas sincronizadas entre procesos, el tiempo total para la entrega de los productos de forma unitaria será el tiempo mayor de los procesos en forma independiente de los productos considerados, es decir:

$$T_{T_p} := \max\left\{T^i_{T_c}\right\}$$

y que contendrá a todos los demás procesos, de manera que globalmente el tiempo de todos los procesos se redujo tan solo al tiempo del proceso más largo; esto es siempre y cuando se logre la sincronía entre todas sus operaciones atómicas respecto a cada proceso.

Cuando el tiempo máximo es mucho muy grande respecto del tiempo necesario para realizar otro producto, es más conveniente que se realicen de manera independiente; por tanto es importante que dicha diferencia no sea mayor a un 30%. Con lo anterior contamos con la siguiente puntualización:

La Manufactura Flexible con restricciones de tiempo cuenta con sincronía entre todos los subprocesos constituida por la programación y la operación para obtener un tiempo de producción acotado y excelentes especificaciones de calidad.

2. *Conclusiones*

a. El Tiempo Real es determinante en las operaciones del Sistema de Manufactura Flexible.
b. Se cumplen con las condiciones del tiempo del proceso que son:
   - Interacción con el mundo real.
   - Respuestas correctas.
   - Respuesta acotada en tiempo.
   - Se maximiza el rendimiento de un SMF.
c. Se demuestra que por muy simples que sean las operaciones en el SMF, se requieren considerar las restricciones de tiempo.

d. Es inútil forzar de forma cualitativa las operaciones que se desarrollan en un SMF; es decir, un SMF debe contar con sistemas de registro de información que contribuyan a la adaptación y corrección de fallas en el sistema.

3. Referencias

[1] Gerard K. Boon, Alfonso Mercado. Automatización flexible en la industria; Difusión y producción de máquinas herramientas de control numérico en América Latina. LIMUSA NORIEGA. México 1990.

[2] The International Federation of Robotics. World Robotics 2001, Statistics, Market Analysis, Forecasts, Case Studies and Profitability of Robot Investment. United Nations.

[3] Pedro Guevara. José de Jesus Medel. Introducción a los Sistemas en Tiempo Real. Instituto Politécnico Nacional. México, 2003.

[4] Eduardo Oliva López. Sistemas Celulares de Producción. Instituto Politécnico Nacional. México. 2001.

[5] Gerard K. Boon, Alfonso Mercado. Automatización Flexible en la Industria; Difusión y producción de máquinas herramientas de control numérico en América Latina. LIMUSA NORIEGA. México 1990.

[6] Lee R. Nyman. Making Manufacturing Cells Work. Mc Graw Hill. USA 1992.

[7] Félix Sanz Adán, Julio Blanco Fernández. CAD/CAM, Gráficos, animaciones y simulación por computadora. THOMSON, España 2002.

[8] C Ray Asfahl. Robots and Manufacturing Automation. John Wiley and Sons, USA 1995.

[9] Geoffrey Boothroyd. Assembly Automation and Product Design. DEKKER, USA 1992.

[10] Tien-Chien Chang, Richard A. Wysk, "Computer-Aided Manufacturing", Segunda edición, Prentice Hall lnternationaI.1998.

[11] Holland, S.W., Rossol, L., and Ward, M.R., CONSIGHT-I: A Vision-Controlled Robot System for Transferring Parts Form Belt Conveyors, in Computer Vision and Sensor-Based Robots, (G.G. Dodd and L. Rossol, eds.), Plenum Press, NY, pp. ~81-97, 1979.

[12] Paul G. Ranky. The design and operation of FMS : flexible manufacturing systems, January 1984.

[13] MengChu Zhou. Modeling, Simulation, and control of flexible manufacturing systems, World Scientific, New Jersey Institute of Technology, USA 1999.

[14] Nigel R. Greenwood. Implementing flexible manufacturing systems, USA 1988.

Análisis de la Caracterización de los Identificadores por Radiofrecuencia RFID

Borja Becerril Dulce Lesly, Linares y Miranda R, Díaz Santos Fco. J., Garduño Medina J.A., García Rivero G., González Mijangos J.A.
ESIME-Zacatenco

Este artículo presenta el análisis de las características eléctricas y electromagnéticas de un sistema de identificación por radio frecuencia (RFID, *Radio Frequency IDentification*) y sus aplicaciones, así como las principales características, ventajas y desventajas de esta tecnología. Los sistemas de identificación por radio frecuencia se utilizan para la identificación de productos; su mayor aplicación esta en el control de inventarios en las tiendas de autoservicio, aunque actualmente se están desarrollando fuertemente en la identificación vehicular, y es esta aplicación en la que se basó este trabajo. Es de principal importancia conocer sus características para poder prevenir o corregir así los problemas de interferencia causado en y por los sistemas de identificación por radiofrecuencia.

Palabras clave: Radiofrecuencia, Identificadores, Lectores, Etiquetas, Tecnología activa, Tecnología pasiva, RFID.

1. Introducción

RFID es una tecnología que posee dos ventajas fundamentales: una gran capacidad para almacenar información y la posibilidad de capturar esa información sin necesidad de contacto físico ni visual entre el portador de los datos (etiqueta) y un dispositivo lector; en general, estos sistemas permiten recoger y almacenar electrónicamente la información, la cual puede ser empleada solo para identificación o bien para ser enlazada con una base de datos para una posterior utilización como es el caso del control vehicular.

Los sistemas RFID (identificadores por radiofrecuencia) están formados por los siguientes elementos básicos, estos se muestran en la **Figura 1**.

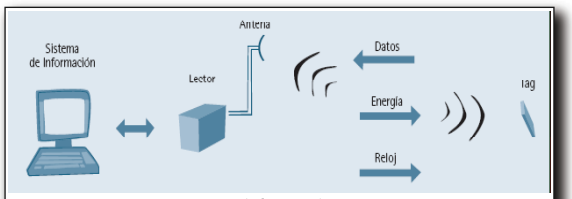


Figura. 1. Principio básico de un sistema RFID.

- Un circuito integrado con antena o etiqueta inteligente, colocado en el objeto a identificar; en este caso, el parabrisas del auto constituye el dispositivo de transporte de datos del sistema RFID, que está compuesto por un sistema base de lectura y una antena que transmite la información. Estas pueden incluir un circuito electrónico con suministro propio de energía (dispositivo activo); o bien recibir energía de la señal de radio para transmitir los datos que se encuentran en su memoria (dispositivo pasivo); también existen dispositivos con batería que solo utilizan para dar energía al circuito integrado y no para la transmisión (dispositivo semi-pasivo).

- El lector RFID que, dependiendo de la tecnología utilizada y de la aplicación, puede ser un dispositivo sólo de lectura con una única reprogramación de usuario, o de lectura / escritura, que permite múltiples reprogramaciones de usuario y recupera dicha información de manera remota, múltiple y sin necesidad de línea visual para generar su función. El lector contiene un módulo de acoplamiento por radiofrecuencia con las etiquetas a través de una antena (transmisor y receptor), una unidad de control y una terminal serial RS232, RS485 o infrarrojo para la comunicación con un panel de control o una computadora. Esto proporciona una mayor seguridad en los datos, ya que permite aplicar algoritmos de detección y corrección de errores, de autenticación y encriptación; también existen mecanismos anticolisión que permiten realizar múltiples lecturas de forma simultánea.

Los dispositivos de los que depende la tecnología para esta aplicación son los siguientes:

- Sensor de masa metálica.
- Barreras ópticas.
- Sensor de altura.
- Video cámara.
- Antena RFID.
- Contadores de ejes.
- Contadores de ruedas dobles.
- Semáforos.
- Cartelera variable.

Un esquema de la tecnología de identificación por radiofrecuencia para la aplicación de identificación vehicular se muestra en la **Figura 2**.



Figura 2. Identificación vehicular con tecnología RFID.

Las principales ventajas de utilizar esta tecnología para la identificación vehicular son:

- Operación manos libres, sin detención.
- Reducción del tráfico en entradas y salidas.
- Mayor seguridad personal.
- Control de la autorización de seguridad mediante identificación.
- Accesible en precio, fácil instalación y mantenimiento.
- Procesamiento automático en puertas remotas o sin atención de personal.
- Rastreo automático del inventario.
- Sistema flexible que se adecua a los requerimientos en cuanto a distancia y velocidad.
- Disminución de emisiones, ya que el vehículo pasa por las entradas o portales sin detenerse ni encender el vehiculo nuevamente.

2. *Método*

Como continuación del proceso de caracterización de un sistema RFID se efectuaron pruebas de campo y laboratorio (cámara anecoica), mostrando el esquema de

Parámetro	Nominales	Medidos
Impedancia	50 Ohms	50 Ohms ±2 Ohms
ROE, Relación de onda estacionaria (SWR)	1.1	1.3 ±0.3
Ganancia	12 dBi	12 dBi ±2 dBi

Tabla 1. Parámetros de lectoras de la tecnología RFID.

calibración. La medición de los parámetros eléctricos y electromagnéticos se realizó con la calibración del sitio de pruebas a 2 m de distancia entre antenas, parámetros de transmisión S21 y potencia de 0 dB.

Las mediciones que se efectuaron fueron las pruebas de velocidad con intervalos de 40 a 60 Km/h y de 80 a 120 Km/h; esto fue para verificar el funcionamiento de los sistemas bajo operación real, así como la comprobación del área de cobertura en la cual las lecturas del sistema RFID son correctas. De igual forma se realizaron pruebas de inmunidad a campos electromagnéticos, con el fin de conocer los niveles de potencia que pueden llegar a afectar el correcto funcionamiento del sistema.

De las mediciones presentadas en el articulo:

- Impedancia.
- Ganancia.
- Patrón de radiación.
- Directividad.
- Polarización.

podemos definir la interpretación con respecto a la aplicación de identificación vehicular, lo cual se muestra en los resultados del presente artículo.

Parámetros	Nominal	Medida
Impedancia	50 Ohms	50 Ohms ±2 Ohms
Potencia	30 dBm (1 Watt)	32.5 dBm ±1 dBm

Tabla 2. Parámetros de los cables coaxiales utilizados para la conexión lector-antena de la tecnología RFID.

Parámetro	Valor Nominal	Medida
Impedancia	50 Ohms	50 Ohms ±2 Ohms
Pérdidas	0.1 dB/m	0.12 dB/m ±0.02 dB/m

Tabla 3. Parámetros de la antena de tipo parche para lectoras de la tecnología RFID.

Parámetro	Nominales	Medidos
Impedancia	50 Ohms	50 Ohms
ROE, Relación de onda estacionaria	1.1	1.3 ±2
Ganancia	6 dBi	6 dBi ±1 dBi

Tabla 4. Parámetros de la antena de tipo yagi para lectoras de la tecnología RFID.

Los datos de parámetros eléctricos obtenidos en las pruebas se presentan en las **tablas 3** y **4**.

El montaje para las pruebas mencionadas se muestra en la **Figura 3**; se colocó el sistema RFID en el sitio de pruebas con una estructura para la antena a 3.5 m de altura y 20º de inclinación con respecto a la horizontal.

3. *Distribución de la señal radioeléctrica*

El procedimiento consistió en marcar un sistema de coordenadas X, Y en el sitio destinado para pruebas en espacio libre, cubriendo un área de 8 por 12 m con divisiones cuadriculadas de $1m^2$; después se conectó la antena Hiperlog con un atenuador (para protección) de 40 dB al radiorreceptor R&S y se hizó un barrido de frecuencia de 900 a 1000 MHz, colocando la antena en cada punto de prueba de acuerdo a las coordenadas trazadas, posteriormente tomar la lectura del radioreceptor, cuyos resultados se muestran en la **Figura 4**.

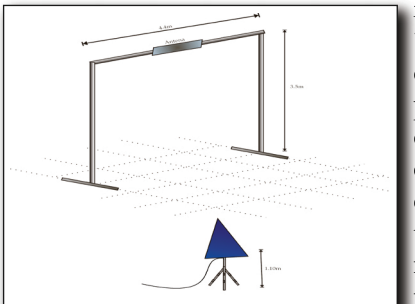


Figura 3. Colocación de la antena.

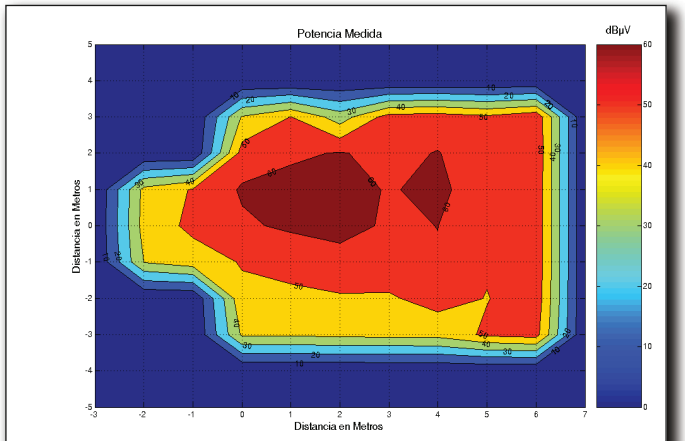


Figura 4 . Distribución de la señal radioeléctrica por un lector RFID.

A partir de los datos obtenidos en la prueba es posible determinar la potencia emitida por el lector del sistema RFID. Para la medición fue utilizada una antena con un factor de 25 dB/m , un cable con una atenuación de 3 dB y un atenuador de protección de 40 dB; el campo eléctrico promedio máximo obtenido es de 123 dB µV/m. Aplicando la fórmula de Friis se obtiene aproximadamente la potencia emitida por el lector del sistema de RFID, de ≈ 1.5 = 3.8 dBm y la ganancia numérica de la antena es de 4 ≈ 6 dB.

4. *Identificación de vehículos*

Los vehículos se hicieron pasar diez veces dentro de la zona iluminada por la antena del lector de la tecnología RFID. Los sistemas que se instalaron leyeron las etiquetas tanto a 40 km/h como a 60 km/h. En el primer caso se tuvieron repeticiones de lecturas de la etiqueta, máximas de 104 y mínimas de 32; en el segundo caso las repeticiones de lecturas máximas fueron de 82 y lasdmínimas de 20. Esto permite afirmar que el número de lecturas disminuye conforme aumenta la velocidad. El objetivo de esta prueba es la detección de las etiquetas cuando los vehículos circulan en la zona de iluminación de la antena a velocidades de 40 km/h y 60 km/h. Los resultados del número de lecturas registradas cada vez que el vehículo pasa por la zona de cobertura se muestran en la **Tabla 5**.

Los resultados de la **Tabla 5** se presentan en una gráfica de barras en la **Figura 5**, y la representación del promedio del número de lecturas se muestra en la **Figura 6**.

#Vueltas	40km/h	60km/h
1	59	54
2	64	58
3	67	61
4	67	56
5	67	62
6	47	39
7	35	33
8	30	39
9	33	32
10	37	40
Prom. No. de lecturas	$\bar{x} = 50.6$	$\bar{x} = 47.4$

Tabla 5 . Número de lecturas de la etiqueta de tecnología RFID a la velocidad de 40Km/h y 60Km/h.

Una representación con mayor detalle de las lecturas registradas de las etiquetas respecto a las velocidades de 40 km/h y 60 km/h se llevó a cabo normalizando dichas lecturas y graficándolas para cada paso (muestras) del vehículo en la zona de cobertura de la antena del lector del sistema de RFID. Estas gráficas se muestran en la **Figura 7**, en donde la barra de color café indica la desviación estándar para un promedio de lecturas de 50.6 para 40 km/h y de 47.4 para 60 km/h.

Las pruebas de baja velocidad se repitieron en el intervalo de 80 a 160 Km/h, con el mismo procedimiento de medición, obteniendo resultados similares a los anteriores, es decir las lecturas fueron satisfactorias para esas velocidades.

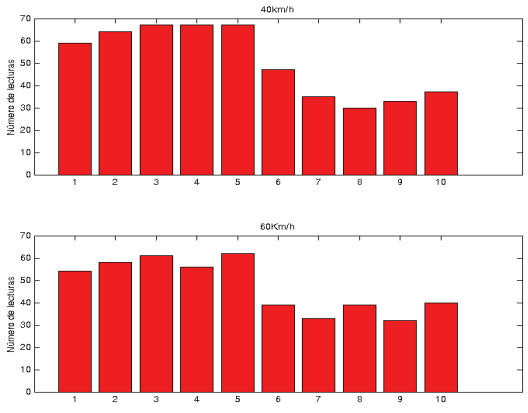


Figura 5 . Gráfica del número de lecturas de la etiqueta de la tecnología RFID a velocidades de 40 km/h y 60 km/h.

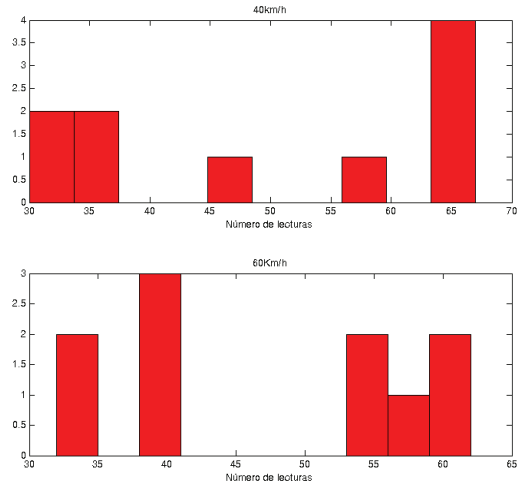


Figura 6 . Histograma del número de lecturas promedio de la etiqueta de la tecnología RFID a velocidades de 40 km/h y 60 km/h.

5. *Funcionalidad respecto a señales interferentes*

Uno de los problemas críticos en cualquier sistema de radiocomunicación es la interferencia y para el caso de la tecnología RFID, es importante analizarla con el objetivo de conocer los niveles de campo eléctrico al cual puede funcionar sin problema.

La medición del número de lecturas en presencia de una señal de interferencia se realiza para conocer que tan inmunes son los sistemas de identificación por radiofrecuencia, y que nivel de potencia se requiere para bloquearlos. El procedimiento de medición es el siguiente:

Se colocó la etiqueta en el simulador de parabrisas, ajustado a una altura de 80 cm del nivel del piso de la cámara anecoica, y se alineó una antena Hyperlog con la etiqueta a una distancia de 2.30 m. Se conectó la antena Hyperlog al generador de señales R&S 9 KHz-2.2 GHz SML 02, el cual se encuentra en el exterior de la cámara anecoica. Posteriormente se envió la señal de interferencia con el generador fijado a la frecuencia de operación del lector, variando la potencia con incrementos de 1 dBm, y se registró el número de lecturas realizadas por el lector; la variación de potencia se finaliza cuando el lector termina de registrar lecturas debido a la información de la etiqueta, en caso de que el lector deje de registrar lectura a 1 dBm se deberá disminuir la potencia a 0.1 dBm avanzando cada 0.1 dBm y registrar el valor de potencia a la cual ya no se registre lectura.

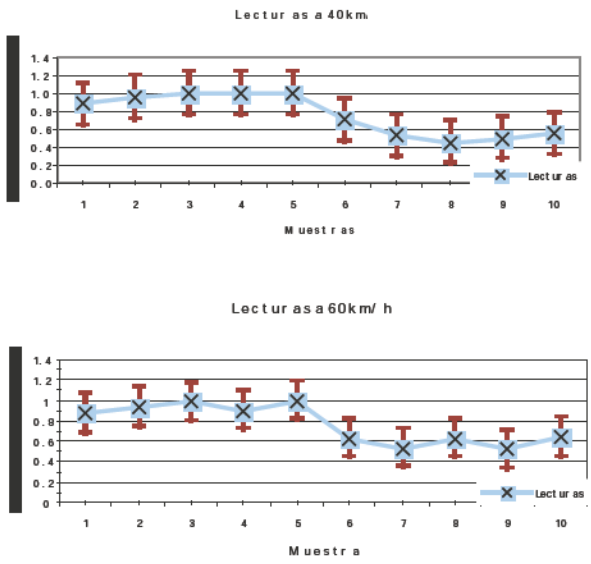


Figura 7. Gráfica de la desviación estándar del número de lecturas de la etiqueta de la tecnología RFID a velocidades de 40km/h y 60km/h.

En esta prueba se emitió una señal dirigida hacia la etiqueta con frecuencia igual a la de la portadora del sistema de RFID (915 MHz), con una separación entre fuente interferente y etiqueta de 0.5 metros. Para esto se utilizó un generador de radiofrecuencia con opción de modulación en AM y FM, una antena semi-logarítmica con ganancia de 5 dBi y factor de antena de 27 dB/m., mientras que el cable coaxial usado presentó una pérdida de 3 dB. Los niveles de campo eléctrico que mostraron un bloqueo a la respuesta de identificación de la etiqueta (número de lecturas) se muestran en la **Tabla 6**.

Los niveles a los cuales se interfiere la tecnología RFID pasiva están más allá de los límites especificados por las Normas Internacionales de Compatibilidad Electromagnética CISPR22, por lo que la tecnología pasiva RFID es segura de operar en un ambiente electromagnético típico de una ciudad donde se han reportado niveles considerables de potencia de radiación.

Para la tecnología RFID activa se probaron sistemas de 915 MHz y de 433 MHz, los cuales se sometieron a pruebas de alcance, potencia isotrópica radiada emitida por la etiqueta y nivel de campo eléctrico al cuál pueden ser interferidos. El nivel de potencia isotrópica radiada se presenta en la siguiente tabla.

Sistema	P (PIRE)
1	42 μW
2	39.4 μW

Tabla 6. Potencia isotrópica radiada

Sistema	Campo Eléctrico
1	86 dB μV/m
2	94 dB μV/m
3	96 dB μV/m
4	90 dB μV/m

Tabla 7. Señal interferente.

Con respecto al campo eléctrico de la señal interferente se consideró el mismo para ambas mediciones que es de 8.5 dB μV/m .

6. Conclusiones

Como a cualquier sistema de radiocomunicación, uno de los problemas básicos que afecta a la tecnología RFID es la interferencia electromagnética; en este caso, los sistemas activos son más sensibles a interferencias en un promedio de 10 dB, lo que implica que pueden ser bloqueados para no identificar la etiqueta y además no requieren de fuentes interferentes direccionales, que es lo que se requiere para el caso de la tecnología pasiva.

Como conclusión general, la Tecnología RFID pasiva es adecuada para la aplicación de identificación vehicular, sobre todo con la estructura de instalación que se utilizó para las pruebas, ya que es robusta a interferencias y tiene una cobertura que puede cumplir con expectativas que se requieran.

6.1 Tecnología RFID pasiva

Para la tecnología pasiva se especificó un alcance típico de entre cuatro y siete metros; con una cobertura para las dimensiones normalizadas de un carril en carretera, los resultados indican que la tecnología RFID pasiva es factible de implementarse en la aplicación de identificación vehicular, siempre y cuando se respete la línea de vista lector-etiqueta. Las mediciones de las distancias de detección especificadas fueron satisfactorias e incluso se rebasaron, debido a que los sistemas utilizados presentaban potencias mayores a lo que especifican las normas internacionales para las bandas de frecuencia no licenciadas de 860 MHz - 960 MHz (>4W PIRE).

6.2 Tecnología RFID activa

De acuerdo a los resultados de las pruebas, la tecnología RFID activa es factible para identificación vehicular. El alcance de esta tecnología es mayor de 50 m y no requiere de línea de vista, aunque las mediciones se realizaron a una distancia de 8 m. Todo esto se debe porque es una tecnología de radiofrecuencia de alta sensibilidad (>-75 dBm).

7. Referencias

[1] Klaus Finkenzeller, Giesecke y Devrient GmbH (2003) *RFID HANDBOOK Fundamentals and Applications in Contlactless Smart Cards and Identification, 2nd edition*, John Wiley & Sons, Gran Bretaña, ISBN 0-470-84402-7.

[2] http://www.rfidjournal.com/article/ articleview/1323

[3] N. Raza.; V. Bradshaw.; M. Hague.(25 Oct. 1999) "Applications of RFID technology," RFID Technology (Ref. No. 1999/123), IEE Colloquium Page(s):1/1 - 1/5

[4] Design antenna Microchip Technology Inc DS00710c pag-14. pdf 2003

[5] Radio Frequency Identification Technology (RFID) © IEE 2005

[6] 2005, EM Microelectronic-Marin SA, www.em-microelectronic.com, Pidhget web service

Mejora Continua para el Sistema de Comunicaciones

M. en C. Cirilo G. León Vega
M. en C. Luis Alejandro Iturri Hinojosa
ESIME ZACATENCO
Ing. Ciro David León Hernández
CIDETEC

Los sistemas de comunicación se utilizan para enviar información de un lugar a otro a través de diferentes medios, tales como el espacio, la fibra óptica y el cableado metálico. Entre los sistemas más comunes tenemos la televisión, radio, infrarrojo, satelital, telefónico, y voz sobre IP. El objetivo es mejorar continuamente la forma de hacer llegar al destinatario la información generada por la fuente, de manera rápida, segura, veraz y a bajo costo. Para detectar la problemática de los sistemas de comunicaciones en México utilizamos el Modelo Hazan Ozbeckhan , el cual consta de cinco etapas:

1.- Proyección de Referencia, en la cual se detecta la problemática del sistema utilizando las Técnicas de Kawakita Jiro (TKJ), la Jerarquización Analítica y el Principio de Pareto.

2.- Planeación Normativa, donde se plantea la misión del sistema incluyendo metas y objetivos.

3.- Planeación Estratégica, que plantea cómo dar solución a los problemas detectados.

4.- Planeación Organizacional, donde se proponen los recursos con los que se resolverá la problemática.

5.- Evaluación, la cual permite conocer lo que es factible hacer.

Aplicando las técnicas anteriores se detectaron los principales problemas del sistema de comunicaciones, concluyéndose que es necesario ajustar periódicamente el Modelo debido a la velocidad de los cambios tecnológicos.

1. Introducción

Las comunicaciones que se utilizan para transmitir datos, imágenes y video han venido evolucionando en forma acelerada, de ahí la importancia del desarrollo de las comunicaciones de nuestro país; por ello es de suma importancia conocer cuales son los principales problemas que estancan el avance de las mismas, ya que si se detectan los problemas se puede implementar una propuesta de solución. Este trabajo no pretende dar una solución ni tampoco es el único método para detectar problemas, más bien es una herramienta para una mejora continua en el desarrollo de este campo por lo que cada institución, grupo o persona debe adecuar este Modelo de acuerdo a sus necesidades y subsistemas concretos.

2. Estructura del Modelo de Planeación de Hazan Ozbeckhan[1]

2.1 Problemática

La problemática constituye una ayuda para poder ver claramente cuál es el objeto focal, definido éste como el sistema en el cual se está interesado, es decir, la parte sobre la cual pueden ejercer control los que llevan a cabo la planeación.

Dentro de la primera fase se empleará la Técnica Kawakita-Jiro (TKJ), clasificando la problemática por grupos, el modelo de decisiones de Jerarquización Analítica, el Principio de Pareto y la Técnica de Ishikawa aplicadas durante esta fase del modelo.

1 Hazan Ozbeckhan, Thoughts on the Emergin Methodology of Planing, in systems and Management Science , Wiley, USA, 1974.

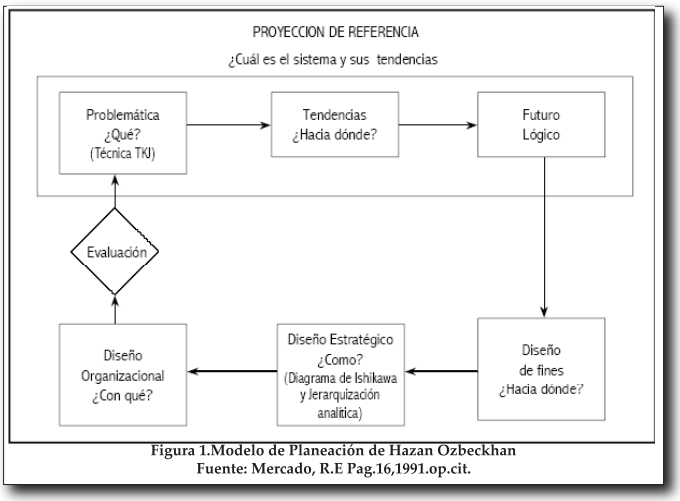


Figura 1.Modelo de Planeación de Hazan Ozbeckhan
Fuente: Mercado, R.E Pag.16,1991.op.cit.

2.2 Proyección de Tendencias y Futuro Lógico.

Esta parte, conjuntamente con la definición del sistema de interés y su problemática, es lo que se denomina *Proyección de Referencia*. La fase de proyección implica el pronóstico a través de una serie de datos estadísticos históricos, o bien de tendencias detectadas en forma cualitativa con base en una consulta de expertos. A través ésta, se pretende conocer cuál sería el estado o dimensión de un problema en un futuro específico; dicho estado es lo que se ha denominado futuro lógico, y representa el futuro más probable o natural.

3. Planeación

3.1 Planeación Normativa

La tarea esencial en esta fase del proceso de planeación consiste en la definición precisa de los fines que persigue el sistema.

3.2 Planeación Estratégica

Una vez que se ha determinado la problemática pertinente, con el grado de detalle necesario y se han diseñado los fines que se pretende alcanzar en forma participativa, se tiene una idea más clara del esfuerzo que será necesario para transformar el sistema del estado actual hacia el que se desea. Es posible comenzar ahora con una estimación de costos, horas-hombre, inversiones, reestructuraciones, etc. La forma de utilizar estos recursos deberá ser eficaz, eficiente y coherente.

3.3 Planeación Organizacional

Una vez definido el qué hacer y el cómo hacer, el modelo de planeación lleva a la pregunta ¿con qué recursos debe contarse para que el sistema se transforme a la manera deseada con el diseño de estrategias?. Esta parte cierra el ciclo del método global de planeación, y la ejecución de las acciones comenzará a transformar el sistema de la manera prevista si todo fue bien diseñado.

3.4 Evaluación

La etapa de evaluación se refiere al hecho de establecer el sistema de información idóneo al proceso, el cual será capaz de detectar en la forma más frecuente posible los valores de las variables más relevantes, con objeto de percibir a tiempo desviaciones a los valores deseados y efectuar las correcciones idóneas. La frecuencia para evaluar el comportamiento del sistema puede balancearse en función de los costos de las observaciones y el costo de las desviaciones. Como se observa, este concepto de planeación es integral, participativo, continuo y retroalimentado.

4. Aplicación del Modelo de Planeación de Hazan Ozbeckhan

En el caso de las telecomunicaciones se pretende aplicar este modelo el cuál permitirá el funcionamiento adecuado para el desarrollo de las mismas, así como la calidad que asegure la satisfacción plena a sus usuarios nacionales e internacionales.

De acuerdo con el modelo de planeación de Hazan Ozbeckhan nos avocamos a considerar cada fase del mismo.

5. Aplicación de la Técnica Kawakita-Jiro

5.1 Identificación de la Problemática

Para realizar esta técnica se elaboró un cuestionario que se envió a los expertos para detectar la problemática de las comunicaciones; una vez obtenidas las respuestas de un total de 50 cuestionarios se detectaron 31 problemas, dado que había respuestas similares.

Primero se discutió si estaban planteados adecuadamente, es decir, que no fueran soluciones, causas, etc., enseguida se modificaron los enunciados en los cuales existía confusión, o no estaban bien planteados, para ello se pidió a los autores que hicieran las aclaraciones correspondientes. Una vez reclasificados, los problemas quedaron como se muestra en la **tabla 1**.

5.2 Jerarquización de Problemas

Los problemas fueron evaluados por un programa de cómputo llamado Sistema Integral de Toma de Decisiones y Jerarquización Analítica, en donde se obtuvo la importancia esencial de cada uno en una comparación pareada de acuerdo a la **tabla 1**.

Mediante el programa se obtuvieron los porcentajes de importancia relativa de los 6 problemas básicos, los cuales se representaron cond la letra Y; el programa los calcula en relación a la importancia e intensidad que cada participante le asigne a los diferentes pares de combinaciones (Y1Y2, Y1Y3, Y1Y4, Y1Y5, Y1Y6, Y2Y3, Y2Y4, Y2Y5, Y2Y6, Y3Y4, Y3Y5, Y3Y6, Y4Y5, Y4Y6, Y5Y6) y el árbitro debe ponderar la importancia relativa del elemento preferido dentro de la comparación pareada, con base en la escala de calificaciones mostrada en la tabla I; los 31 problemas del estrato inferior se representan por la letra X y sus porcentajes de importancia relativa son calculados por el programa de la misma forma. La suma de los porcentajes de importancia relativa de cada uno de los problemas Y nos da el 100% de importancia absoluta de la problemática Z, de la misma forma la suma de los porcentajes de las X correspondientes nos da el 100% de las importancia relativa de cada problema Y.

Problemática	Importancia Relativa %	Importancia Absoluta %
Y_1 Políticas de las telecomunicaciones	**23**	
X_{11} Política de las comunicaciones nacionales	60	0.60*0.23*100=13.080
X_{12} Política de las comunicaciones regionales	25	0.25*0.23*100=05.750
X_{13} Política de las comunicaciones mundiales	15	0.15*0.23*100=03.450
Y_2 Reglamentación de las telecomunicaciones	**19**	
X_{21} Normatividad nacional	50	0.50*0.19*100=09.500
X_{22} Normatividad regional	35	0.35*0.19*100=06.650
X_{23} Normatividad mundial	25	0.25*0.19*100=04.750
Y_3 Seguridad en la información	**18**	
X_{31} Ataques de virus	55	0.55*0.18*100=09.900
X_{32} Participación de hackers	30	0.30*0.18*100=05.400
X_{33} Eficiencia en los sistemas de comunicaciones	15	0.15*0.18*100=02.700
Y_4 Poco crecimiento en la industria de las telecomunicaciones	**17**	
X_{41} Dificultad de adaptación de las empresas para renovarse en las tecnologías	15	0.15*0.17*100=02.550
X_{42} Integración de servicios	14	0.14*0.17*100=02.380
X_{43} Escasez de servicios	12	0.12*0.17*100=02.040
X_{44} Calidad en los productos	11	0.11*0.17*100=01.870
X_{45} Costos elevados	11	0.11*0.17*100=01.870
X_{46} Baja calidad en algunos servicios	10	0.10*0.17*100=01.700
X_{47} Incompatibilidad de servicios	10	0.10*0.17*100=01.700
X_{48} Coordinación entre los productores de internet en México para ofrecer al usuario una red segura	9	0.09*0.17*100=01.530
X_{49} Bajo impacto de servicios de banda ancha y televisión por cable en el país	8	0.08*0.17*100=01.360
Y_5 Capacitación	**14**	
X_{51} Baja autoestima en el personal de trabajo	40	0.40*0.14*100=05.600
X_{52} Deficiencia en la capacitación de personal	30	0.30*0.14*100=04.200
X_{53} Deficiencias de conocimientos del personal a nivel ingeniería y de otras áreas	20	0.20*0.14*100=02.800
X_{54} Empresas sin departamentos de investigación	10	0.10*0.14*100=01.400
Y_6 Infraestructura inadecuada principalmente en zonas rurales y ciudades pequeñas	**9**	
X_{61} Áreas	55	0.55*0.09*100=04.950
X_{62} Equipo	25	0.25*0.09*100=02.250
X_{63} Material de trabajo	20	0.20*0.09*100=01.800

Tabla I.- Importancia Relativa y Absoluta de la Problemática.

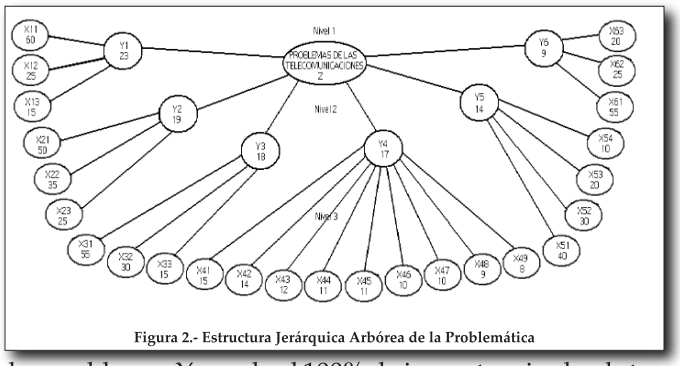


Figura 2.- Estructura Jerárquica Arbórea de la Problemática

Los porcentajes obtenidos por el programa Sistema Integral de Toma de Decisiones y Jerarquización Analítica, se muestran en la **tabla 1**.

La **figura 2** muestra la estructura jerárquica arbórea que se encuentra dividida en tres niveles: el primer nivel consiste en la problemática total de las telecomunicaciones (Z), el segundo nivel está conformado por los seis problemas agrupados por la letra (Yi) dentro de los cuales se encuentran los treinta y un problemas representados por la letra (Xij), la gráfica termina en el tercer nivel debido a que cada uno de los elementos del mismo ya no se puede dividir en otros problemas a considerar.

5.3 Principio de Pareto

El Principio de Pareto (Principio 20-80), mismo que se puede observar en la ultima columna de la **tabla 2** y en la grafica de la **figura 3**, establece que si tomamos en consideración el 20% de los problemas más importantes, y sumamos la importancia absoluta de cada uno de ellos, obtenemos aproximadamente el 80% de la importancia absoluta de la problemática total. Esto quiere decir que basta con solucionar el 20% de los problemas principales para no gastar esfuerzos y recursos en los demás, pues su impacto en la problemática total es bajo.

5.4 Técnica de Ishikawa

Esta técnica conocida también como esqueleto de pescado se utilizó para encontrar las causantes de los problemas, para ello se revisaron los cuestionarios de los expertos y con el auxilio de la técnica TKJ se detectaron dichos causantes. Posteriormente, se procedió a hacer un resumen, obteniéndose un total de siete causas específicas por problema.

Problemas en orden de importancia	Elemento	Importancia Absoluta (IA)100%	Suma de Pareto 100%
Política de las comunicaciones nacionales	**X11**	**.1308**	**0.1308**
Ataques de virus	**X31**	**.0990**	**0.2298**
Normatividad nacional	**X21**	**.0950**	**0.3248**
Normatividad regional	**X22**	**.0665**	**0.3918**
Política de las comunicaciones regionales	**X12**	**.0575**	**0.4488**
Baja autoestima en el personal de trabajo	**X51**	**.0560**	**0.5048**
Participación de hackers	**X32**	**.0540**	**0.5588**
Áreas	X61	.0495	0.6083
Normatividad mundial	X23	.0475	0.6558
Deficiencia en la capacitación de personal	X52	.0420	0.6978
Política de las comunicaciones mundiales	X13	.0345	0.7258
Deficiencias de conocimientos del personal a nivel ingeniería y de otras áreas	X53	.0280	0.7538
Eficiencia en los sistemas de comunicaciones	X33	.0270	0.7808
Dificultad de adaptación de las empresas para renovarse en las tecnologías	X41	.0255	0.8063
Integración de servicios	X42	.0238	0.8301
Equipo	X62	.0225	0.8526
Escasez de servicios	X43	.0204	0.8730
Calidad en los productos	X44	.0187	0.8917
Costos elevados	X45	.0187	0.9104
Material de trabajo	X63	.0180	0.9284
Baja calidad en algunos servicios	X46	.0170	0.9454
Incompatibilidad de servicios	X47	.0170	0.9624
Coordinación entre los productores de internet en México para ofrecer al usuario una red segura	X48	.0153	0.9777
Empresas sin departamentos de investigación	X54	.0140	0.9917
Bajo impacto de servicios de banda ancha y televisión por cable en el país	X49	.0081	0.9998

Tabla II.- Importancia Absoluta y Suma de Pareto de Mayor a Menor Importancia

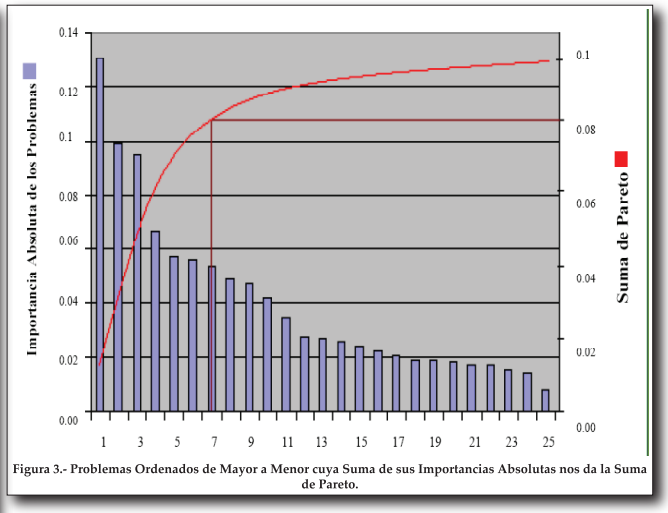


Figura 3.- Problemas Ordenados de Mayor a Menor cuya Suma de sus Importancias Absolutas nos da la Suma de Pareto.

Relación de Problemas con sus Causas Específicas:

Política de las comunicaciones nacionales:
- Información a la población del desarrollo de las telecomunicaciones.
- Capacitación para el uso de las telecomunicaciones a la población.
- Falta de comunicación en algunas comunidades del país.
- Proteccionismo de las compañías nacionales.

Ataques de virus:
- Descuido de los programadores.
- Falta de vacunas.
- Falta de cuidado de los usuarios.

Normatividad nacional:
- Fraudes.
- Publicidad inadecuada
- Afectación a empresas de audio y video.
- Escaso desarrollo de las telecomunicaciones.

Normatividad regional:
- Incompatibilidad en los servicios.
- Publicidad inadecuada.
- Afectación a empresas de audio y video.
- Escaso desarrollo de las telecomunicaciones.

Política de las comunicaciones regionales:
- Información a la población del desarrollo de las telecomunicaciones
- Capacitación para el uso de las telecomunicaciones a la población.
- Existe falta de comunicación en países de América Latina.
- Proteccionismo de las compañías nacionales.

Baja autoestima en el personal de trabajo:
- Falta de incentivos en el trabajo.
- Poca interactividad personal en el trabajo.
- Información de los objetivos y metas de la empresa.

Participación de *hackers*:
- Aprovechan los errores de la programación.
- Piratería de programas.
- Programación inadecuada de los programas.

Y así sucesivamente de la misma forma se van encontrando las causantes generales y específicas de cada uno de los problemas mencionados.

En la **figura 4** se presenta un ejemplo de los esquemas de Ishikawa con sus causantes generales.

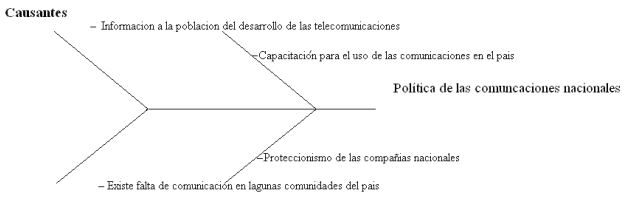


Figura 4. Ejemplo de esquemas de Ishikawa con sus causantes generales.

6. Conclusiones

El resultado obtenido de la información derivada de los cuestionarios que fueron aplicados a un grupo de expertos y funcionarios en el área de las comunicaciones fue de siete problemas principales, a partir de los cuales se derivan otros que están contenidos en ellos. Estos resultados van a depender de las personas a quienes se les aplique la encuesta, de la información recabada, de las necesidades de cada instancia, etcétera; ya que abordar el problema de forma general de las comunicaciones es diferente cuando se analiza un sistema especifico; por lo tanto, se recomienda a los usuarios del modelo que utilicen las técnicas y la metodología en forma rigurosa.

7. Referencias

[1] David Goodman "One Stepan at Time", Agosto de 1995, pp. 847.

[2] William W. Arnold, "Lessons of Value -Driven

[3] Leandership", Healthcare Executive, Julio Agosto, 1995, pp. 12 y 15.

[4] Marke Suchman, "Managing Legitima Strategic and Institutional Approaches", Academy of Magnament Review 20, No.3(1995); pp. 571-610.

[5] Eduard A. Robinson, "Americas Most Admired-Companies", Fortune, 3 de marzo, 1997, pp. 68-75.

[6] David Greising, "It Hurt So Good at Delta", Bussiness Week, Diciembre, 1995, pp. 106-107.

[7] Robert L. Simision, Oscar Suris, "Alex Trorman Goal: Its Make Fordasol in World Sales", Wall Street Journal, 18 de Julio, 1993, pp.A1-A8.Ackoff, Russell

[8] L. On Purposeful Systems, Travistock, London, 1972.

[9] Ackoff, Russell L. Planeación de Empresas. Limusa, México, 1986.

[10] Ackoff, Russell L. Redesigning the Future. Wiley, NY, 1974.

[11] Ackoff, Russell L. Scientific Method: Optimizing Applied Research Desicions. Wiley, N. V., 1982.

[12] Barojas, P.E., Modelo de Programación por Metas y Jerarquización para la Asignación Óptima de Recursos Económicos, Tesis: Maestría., S.G.I. ESIME, IPN, 1986.

[13] De la Vega Lezama, F. C. Un Paso Hacia el Método Científico. México, IPN, 28ª Edición, 1994.

[14] Fickers, Sir Geoffrey. Toward a Sociology of Management. Basic Books, N.Y. 1968.

Criptografía Cuántica: Un Nuevo Paradigma

Maria Aurora Molina Vilchis
Ramón Silva Ortigoza
CIDETEC IPN
Eleazar Bracho Molina
UAMI, Licenciatura en Computación.

La criptografía cuántica, a diferencia de la criptografía clásica, resuelve los problemas de cifrado de los mensajes para ocultar la información, así como la distribución de la clave, donde cada bit puede estar en un estado discreto y alternativo a la vez; la unidad fundamental de almacenamiento es el bit cuántico, cada uno de los cuales puede tener múltiples estados simultáneamente en un instante determinado, con lo que se reduce el tiempo de ejecución de algunos algoritmos de miles de años a apenas segundos.

La criptografía cuántica está basada en las interacciones del mundo sub-atómico, y tiene elementos como el bit cuántico, las compuertas cuánticas, los estados confusos, la tele transportación cuántica, el paralelismo cuántico y la computación cuántica.

Podemos decir que los métodos actuales de encriptación se basan en operaciones matemáticas, que modifican el mensaje para ocultar su significado, hasta que el destinatario que conoce las claves invierte el proceso y redescubre el mensaje. La fragilidad de este método radica en la transmisión de las claves, que pueden ser interceptadas en el trayecto, sin que el emisor y el receptor lo sepan. La criptografía cuántica supera en teoría ambas limitaciones, ya que la información se sitúa en las partículas de luz o fotones que son emitidos, de uno en uno, en un estado previamente conocido por el destinatario, quien de esta forma puede recuperar el mensaje. Si uno de los fotones es interceptado, su estado queda alterado y el receptor detecta el ataque al mensaje.

Criptografía es la ciencia matemática de las comunicaciones secretas, con una larga y distinguida historia de uso militar y diplomático que se remonta a los antiguos Griegos. Fue un elemento importante y decisivo durante la segunda guerra mundial, y hoy en día su uso es muy común y necesario, para brindar seguridad en las transacciones comerciales, comunicaciones, y privacidad; que se llevan a cabo mediante la Internet. Dados M y f, donde M es un mensaje y f una función de encriptación, tenemos $C = f(M)$, C entonces es el mensaje encriptado. C es enviado al receptor mediante un canal público, este obtiene el mensaje original con f^{-1}, haciendo $M = f^{-1}(C)$. Si f^{-1} es conocido y C es interceptado en el canal público, entonces se puede obtener M. La seguridad de f depende de la dificultad con que pueda obtenerse f^{-1}.

La factorización es un aspecto muy importante en la criptografía moderna, debido a que la seguridad del mecanismo de criptografía RSA de clave pública se basa en la dificultad de factorizar números grandes. El mejor algoritmo para hallar los factores aún sigue siendo el de las divisiones sucesivas. Así M, R_1 y R_2, mediante el mecanismo de RSA se define una función p, tal que $C_1 = p(Q_1, P_1, M_1)$ y $C_2 = p(Q_2, P_2, M_2)$, donde P_1 y P_2 son claves públicas generadas en base a Q_1 y Q_2 que son claves privadas pertenecientes a A y B respectivamente. A y B comparten sus respectivas claves públicas P_1 y P_2, y ambos pueden obtener y descifrar sus mensajes mediante p^{-1}, de tal modo *que* $M_1 = p^{-1}(Q_1, P_1, M^1)$ y $M_2 = p^{-1}(Q_2, P_2, M_2)$.

El tiempo que requeriría el realizar la factorización se estima en aproximadamente $4x10^{16}$ años. Sin embargo en 1994 se logró desarrollar un algoritmo, usando recursos en redes, donde la factorización únicamente tomo 8 meses, el equivalente a 4,000 MIPS-años. [Hughes94]. Se estima que los algoritmos cuánticos de factorización realizarían este cálculo en segundos. Utilizando claves privadas, es posible – al menos en teoría – tener un algoritmo de encriptación imposible de romper. El emisor cada vez que envía un mensaje M, genera aleatoriamente una diferente clave privada P, y mediante una función de encriptación E se codifica el mensaje de tal modo que $C = E(P, M)$. El receptor necesita la clave privada P para poder realizar el proceso inverso $M = E^{-1}(P, C)$. Actualmente, este mecanismo es utópico, debido a la gran dificultad que surge en la distribución de la clave privada P, debido a que necesita un canal muy seguro para su entrega.

La criptografía cuántica hace posible la distribución de la clave privada P. Esta clave es transmitida mediante un canal cuántico. Cualquier intento de medir P será

detectado, debido a que es imposible observar un *qubit* (bit cuántico) sin dejar rastro.

Este artículo presenta una introducción al nuevo paradigma en la criptografía de cara a la computación cuántica. En la sección 2 describe *grosso modo* los fundamentos de la criptografía cuántica. En la sección 3 se describe el criptosistema cuántico. Por último, en la sección 4 se listan las principales empresas comerciales que actualmente están incursionando en este nuevo campo de la criptografía.

2. Fundamentos de la Criptografía Cuántica

La comunidad científica dedicada a investigar tópicos en el ámbito de la criptografía cuántica, ha logrado enormes avances teóricos, al demostrar que es posible reducir drásticamente los recursos computacionales requeridos en la ejecución de algoritmos. Los algoritmos requieren un inmenso poder de cómputo aún en las computadoras más avanzadas de la actualidad. Algoritmos matemáticos tales como la búsqueda de números primos, y algoritmos de manejo de información tales como la búsqueda en bases de datos no ordenadas han sido teóricamente desarrollados con mucho éxito, utilizando los fundamentos de la criptografía cuántica.

La teoría de la criptografía cuántica está basada en las interacciones del mundo atómico y en futuras implementaciones de las computadoras cuánticas. Dichas computadoras aún están en los laboratorios de investigación pero ya se tienen resultados alentadores, como el desarrollo de la computadora Cuántica de cinco qubits desarrollada por Steffen et al [Steffen01].

2.1 Fundamentos de la Criptografía Cuántica

La Criptografía cuántica se basa en las propiedades de la interacción cuántica entre las partículas subatómicas, tales como la superposición simultánea de dos estados en una sola partícula subatómica. Esta propiedad fundamental de la interacción cuántica, es ampliamente aprovechada para el desarrollo teórico de los algoritmos cuánticos, logrando una capacidad de procesamiento exponencial.

La superposición Cuántica permite mantener simultáneamente múltiples estados en un bit cuántico, es decir "0" y "1" a la vez; a diferencia del bit – elemento fundamental en la criptografía actual – que únicamente es capaz de mantener un estado discreto alternativo a la vez, el "0" o "1" lógico. La criptografía cuántica aprovecha la superposición cuántica para lograr el paralelismo cuántico y el paralelismo cuántico masivo. Cualquier interacción con el mundo subatómico producirá un cambio en este, es decir, cualquier medición o lectura traerá indefectiblemente un cambio. Este fenómeno cuántico es aprovechado en la tele transportación cuántica para la transmisión de qubits, y asimismo es utilizada como mecanismo de seguridad en la criptografía cuántica.

2.2 Elementos básicos de la Criptografía cuántica

2.2.1 El bit cuántico "qubit"

El elemento básico de la criptografía cuántica es el bit cuántico o qubit[1] (*quantum bit* por sus siglas en inglés), un qubit representa ambos estados simultáneamente, un "0" y un "1" lógico, dos estados ortogonales de una sub partícula atómica, como es representada en la figura 1. El estado de un qubit se puede escribir como $\{|0\rangle, |1\rangle\}$, describiendo su múltiple estado simultáneo.

Un vector de dos qubits representa simultáneamente los estados 00, 01, 10 y 11; un vector de tres qubits, representa simultáneamente los estados 000, 001, 010, 011, 100, 101, 110, y 111; y así sucesivamente. Es decir, un vector de n qubits representa a la vez 2^n estados.

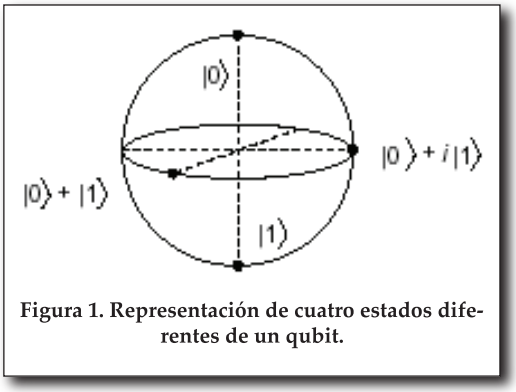


Figura 1. Representación de cuatro estados diferentes de un qubit.

Cualquier sistema cuántico con dos estados discretos distintos puede servir como qubit, un espín de electrón que apunta arriba o abajo, o un espín de fotón con polarización horizontal o vertical. En la figura anterior se tiene una representación gráfica de cuatro diferentes estados basado en el espín de un núcleo atómico, por lo que puede ser usado como un qubit. Un qubit no puede ser clonado, no puede ser copiado, y no puede ser enviado de un lugar a otro.

1 "qubit" término acuñado por Schumacher en 1995.

2.2.2 Compuertas Cuánticas

Las compuertas lógicas son operaciones unarias sobre qubits. La compuerta puede ser escrita como $P(\theta)=|0\rangle\langle 0| + \exp(i\theta) + |1\rangle\langle 1|$, donde $\theta = \omega t$. A continuación algunas compuertas Cuánticas elementales [Steane97]:

$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ = identidad
$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$ = NOT
$Z \equiv P(\pi)$
$Y \equiv XZ$
$H \equiv (1/\sqrt{2})[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]$

Donde I es la identidad, X es el análogo al clásico NOT, Z cambia el signo a la amplitud, y H es la transformación de Hadamard. Esas compuertas forman uno de los más pequeños grupos de la criptografía cuántica. La tecnología de la física Cuántica puede implementar esas compuertas eficientemente. Todos, excepto el CNOT, operan en un simple qubit; la compuerta CNOT opera en dos qubits. Una compuerta de dos qubits en especial interesante, es la conocida como "U controlada", [Steane97] $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U$ son operadores actuando sobre dos qubits, donde I es la operación de identidad sobre un qubit, y U es una compuerta. El estado del qubit U es controlado mediante el estado del qubit I. Por ejemplo, el NOT controlado (CNOT) es:

$|00\rangle \rightarrow |00\rangle$; $|01\rangle \rightarrow |01\rangle$; $|10\rangle \rightarrow |11\rangle$; $|11\rangle \rightarrow |10\rangle$

2.2.3 *Procesamiento*

La capacidad computacional de procesamiento paralelo de la criptografía cuántica, es enormemente incrementada por el procesamiento masivamente en paralelo, debido a una interacción que ocurre durante algunas millonésimas de segundo. Este fenómeno de la mecánica cuántica es llamado *entanglement*. Debido a esto es que dos partículas subatómicas permanecen indefectiblemente relacionadas entre sí, si han sido generadas en un mismo proceso; por ejemplo, la desintegración en un positrón y un electrón. Estas partículas forman subsistemas que no pueden describirse separadamente. Cuando una de las dos partículas sufre un cambio de estado, repercute en la otra. Dicha característica se desencadena cuando se realiza una medición sobre una de las partículas [White00].

2.2.4 Tele transportación Cuántica

La tele transportación Cuántica es descrita por Stean [Steane97] como la posibilidad de "transmitir qubits sin enviar qubits". En la criptografía tradicional, para transmitir bits, estos son clonados o copiados y luego enviados a través de diferentes medios como el cobre, fibra óptica, ondas de radio y otros. En la criptografía cuántica no es posible clonar, copiar, o enviar qubits de un lugar a otro como se hacen con los bits.

Si enviamos un qubit $|\varnothing\rangle$ donde $\varnothing$ es un estado desconocido, el receptor no podrá leer su estado con certidumbre; cualquier intento de medida podría modificar el estado del qubit, por lo tanto se perdería su estado, imposibilitando su recuperación. La tele transportación Cuántica, resuelve este problema; esta se basa en el *entanglement* para poder transmitir un qubit sin necesidad de enviarlo. El emisor y el receptor poseen un par de qubits "enredados" (*entangled*). Entonces el qubit es transmitido desde el emisor, desaparece del emisor y el receptor tiene el qubit tele transportado. Este fenómeno es posible debido a un mecanismo conocido como el efecto EPR[2]. En la tele transportación Cuántica primero dos qubits E y R son "enredados" y luego separados, el qubit R es ubicado en el receptor y el qubit E es ubicado en el emisor junto al qubit original Q a ser transmitido; al realizar la lectura del estado de los dos qubits Q y E, estos cambian su estado a uno aleatorio debido a la interacción. La información leída es enviada al receptor, donde esta información es utilizada para un tratamiento que es aplicado al qubit R, siendo ahora R una réplica exacta del qubit Q [Nayak02] [Ambainis02].

2.2.5 El paralelismo cuántico

La superposición Cuántica permite un paralelismo exponencial o paralelismo cuántico en el cálculo, mediante el uso de las compuertas lógicas de qubits. [Steffen01] Los qubits, a diferencia de los bits, pueden existir en un estado de superposición, representado por $a|0\rangle + b|1\rangle$, donde a y b son números complejos que satisfacen la relación $|a|^2 + |b|^2 = 1$.

Dada una compuerta lógica de un qubit *f*, que transforma el estado $|a|$ en el estado $|f(x)|$, cuando el qubit de entrada tiene en el estado $(1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$ [Steffen01] una superposición igual de $|0\rangle$ y $|1\rangle$.

Por linealidad de la mecánica Cuántica [Steffen01], la compuerta lógica *f* transforma el estado del qubit a

$$(1/\sqrt{2})|f(0)\rangle + (1/\sqrt{2})|f(1)\rangle$$

2 La "correlación de Einstein-Podolsky-Rosen (EPR)" o *entanglement*, ha sido al menos en parte conocido desde los 1930s cuando fue discutido en un famoso paper por Albert Einsten, Boris Podolsky, y Nathan Rosen

El estado resultante es la superposición de los 2 valores de salida, siendo *f* evaluado para los 2 valores de entrada en paralelo. Para una compuerta lógica *g* de 2 qubits, que tienen dos qubits de entrada en superposición de $|0\rangle$ y $|1\rangle$, tendríamos una superposición de 4 estados $c_0|\mathbf{0}\ \rangle + c_1|\mathbf{0}\ \rangle + c_2|\mathbf{0}\ \rangle + c_3|\mathbf{1}\ \rangle$.

La compuerta lógica *g* transforma el estado de entrada a $c_0|g(\mathbf{0}\ )\rangle + c_1|g(\mathbf{0}\ )\rangle + c_2|g(\mathbf{0}\ )\rangle + c_3|g(\mathbf{1}\ )\rangle$ [Steffen01] así *g* es evaluado en un solo paso para 4 valores de entrada. En una compuerta lógica *h* de 3 qubits, se tienen 3 qubits de entrada en superposición de $|0\rangle$ y $|1\rangle$, juntos hacen una superposición de 8 estados, que son evaluados en paralelo. Por cada qubits adicional la cantidad de estados se duplica.

3. Criptosistemas Cuánticos

La Criptografía cuántica es propuesta a principios de los 70 por Stephen Weisner, denominada *Conjugate Coding* y publicada eventualmente el 1983. Bennet y Brassard, quienes compartían ideas de Weisner, proponen el protocolo para la criptografía cuántica denominado "BB84" en 1984. No fue sino hasta 1989, en un laboratorio del Centro de Investigaciones de IBM (*International Business Machines*), que el primer prototipo experimental basado en este protocolo fue operable, la primera transmisión de señales Cuánticas fue a una distancia de 32 cm. En 1995, investigadores de la Universidad de Ginebra lo consiguieron utilizando una fibra óptica de 23 kilómetros de longitud. En 1997, Zbinden et al [Zbinden98] lograron distribuir Cuánticamente una clave a través de 23 Km de fibra bajo el lago Génova. Más adelante, el laboratorio de Los Álamos logró una distancia de 50 kilómetros.

Actualmente, ingenieros de la compañía Toshiba en Gran Bretaña han conseguido enviar un mensaje a más de 100 kilómetros por un cable de fibra óptica utilizando criptografía cuántica a la velocidad de 2 kilobits por segundo, lo que permitirá comercializar esta tecnología, incluso podría utilizarse la QKD (*Quantum Key Distribution*).

Los sistemas criptográficos cuánticos aprovechan el Principio de Incertidumbre de Heisenberg, el cual al medir un sistema cuántico en general lo perturba, ofreciendo información distinta a la de su estado antes de la medida. El escuchar detrás de las puertas en un canal de comunicaciones cuántico causa un disturbio inevitable. Los elementos del intercambio de información del quantum son observaciones del mismo; los fotones son puestos típicamente en un estado particular por el remitente y después observados por el destinatario. Debido al principio de incertidumbre, cierta información del quantum ocurre como conjugaciones que no se puedan medir simultáneamente. Dependiendo de cómo se realiza la observación, diversos aspectos del sistema pueden ser medidos – por ejemplo, las polarizaciones de fotones se pueden expresar en cualquiera de tres diversas bases: rectilíneo, circular y diagonal – pero observado en una base seleccionada al azar.

Así, si el receptor y el remitente no concuerdan en que base de un sistema del quantum están utilizando, el receptor puede destruir la información del mensajero sin ganar cualquier cosa útil. Éste, entonces, es el acercamiento total a la transmisión del quantum de la información: el remitente lo codifica en estados del quantum, el receptor observa estos estados y entonces, por la discusión pública de las observaciones, el remitente y el receptor convienen un cuerpo de la información que comparten (con probabilidad arbitrariamente alta). Su discusión se ocupa de los errores, mismos que se pueden introducir por ruido al azar o por *eavesdroppers*, pero debe ser en general para no comprometer la información. Mientras que la criptografía clásica emplea varias técnicas matemáticas para restringir a los indiscretos, en la teoría Cuántica la información es protegida por las leyes de la física. En la criptografía clásica una seguridad absoluta de la información no puede ser garantizada, mientras que el principio del enredo y la incertidumbre de Heisenberg se puede explotar en un sistema de la comunicación segura.

La criptografía del quantum proporciona los medios para que dos participantes intercambien una llave de codificación sobre un canal privado con completa seguridad. Hay por lo menos tres tipos principales de Criptosistemas para la distribución de llaves, estos son: **a)** Criptosistema con la codificación basada en dos observadores que no conmutan, propuestos por S. Wiesner, C.H. Bennett y G. Brassard, **b)** Criptosistema con la codificación construida sobre el enredo del quantum y el teorema de Bell, propuesto por A.K. Ekert, y **c)** Criptosistema con la codificación basada en dos vectores no ortogonales, propuestos por C.H. Bennett.

3.1 Criptosistema de quantum

El criptosistema de quantum se puede explicar con el ejemplo siguiente: el sistema incluye un transmisor y un receptor; un remitente puede utilizar el transmisor para enviar los fotones en una de cuatro polarizaciones:

0°, 45°, 90° o 135°, mientras que un recipiente en el otro extremo utiliza el receptor para medir la polarización. Según las leyes mecánicas del quantum, el receptor puede distinguir entre las polarizaciones rectilíneas (0° y 90°), o puede ser configurado rápidamente de nuevo para discriminar entre las polarizaciones diagonales (45° y 135°), pero nunca distinguir ambos tipos. La distribución dominante requiere varios pasos: el remitente envía los fotones con una de las cuatro polarizaciones que se liguen al azar; para cada fotón entrante, el receptor elige al azar el tipo de medida, rectilíneo o diagonal. El receptor registra las medidas y las mantiene secretas. El receptor posteriormente anuncia públicamente el tipo de medida (no los resultados) y el remitente dice al receptor que medidas estaban del tipo correcto. El remitente y receptor guardan todos los casos en los cuales las medidas del receptor son del tipo correcto. Estos casos se traducen en trozos (unos y ceros) y de tal modo se convierte en una llave. Un *eavesdropper* esta limitado para producir errores a esta transmisión , por que no sabe por adelantado el tipo de polarización de cada fotón, y la mecánica del quantum no permite que adquiera valores agudos de dos observadores que no conmuten (polarizaciones rectilíneas y diagonales). Los dos usuarios legítimos prueban el quantum para escuchar detrás de la puerta, revelando un subconjunto de azar de trozos dominantes y comprobando (en público) la tasa de error. Aunque no pueden evitar escuchar detrás de las puertas, un *eavesdropper* nunca los engañará, porque el esfuerzo sutil y sofisticado de golpear ligeramente el canal será detectado.

3.2 Criptosistema del enredo del quantum y el teorema de Bell

La idea principal de este criptosistema está basada en una secuencia de los pares correlacionados que la partícula genera, con un miembro de cada par que es detectado por cada partido (por ejemplo, un par de los fotones supuestos de Einstein Podolsky-Rosen, que polarizaciones son medidas por los partidos). Un *eavesdropper* en esta comunicación tendría que detectar una partícula para leer la señal, y retransmitirla en la orden para que su presencia siga siendo desconocida. Sin embargo, el acto de la detección de una partícula de un par destruye su correlación del quantum con la otra, y los partidos pueden verificar fácilmente si esto ha sido hecho, sin revelar los resultados de sus propias medidas, por el excedente de la comunicación en un canal abierto.

4. Compañías Comerciales Relacionadas

La criptografía cuántica teóricamente ha logrado evolucionar de forma satisfactoria y tiene definidos sus fundamentos con base en la interacción subatómica y sus elementos como el bit cuántico, compuertas Cuánticas, tele transportación de código, paralelismo cuántico y encriptación Cuántica. [Steane97] [Bennett98]. Aunque no se ha logrado implementar una comunicación Cuántica aún, se tienen grandes avances como la definición de una arquitectura Cuántica ampliamente aceptado por los investigadores [Oskin02], la implementación de pequeños prototipos como la computadora de 5 bits cuánticos desarrollada por Steffen et al [Steffen01], y el desarrollo de tecnologías Cuánticas comerciales [Johnson02a].

Las principales compañías que actualmente están realizando estrategias de desarrollo y comercialización con la criptografía cuántica son:

- MagiQ Technologies
- IdQuantique
- BBN Technologies
- D-Wave Systems
- IBM
- Hewlett-Packard,

IdQuantique quien actualmente tiene en el mercado el generador de números aleatorios cuánticos. En el futuro se espera que la criptografía cuántica, esté completamente desarrollada (aproximadamente entre el 2020 a 2025), y tome el lugar de las Criptografías actuales. Una muestra de lo que ocurrirá es *Magiq*, la primera empresa que lanzará al mercado tecnología de Encriptación Cuántica, capaz de codificar flujos de datos y enviarlos a altas velocidades por las troncales de Internet, de forma similar a los trabajos experimentales desarrollados por Prem Kumar y Horace Yuen, profesores de la Universidad Northwestern [Johnson02a] [Johnson02b].

5. Conclusiones

Dos limitaciones importantes enfrenta la implementación de la criptografía cuántica: 1) la presencia de elementos en estado líquido y gaseoso en el proceso de interacción subatómica, que hacen muy difícil el lograr modelos donde intervengan miles de bits cuánticos. 2) no se puede realizar una lectura sin producir cambios en ella, limitación dada por la naturaleza de las interacciones

con los elementos subatómicos. Estos cambios son impredecibles y se propagan a lo largo de todo el sistema, por lo que es necesario integrar complejos mecanismos de corrección de errores que agregan sobrecarga en proporciones exponenciales. No obstante, en las próximas décadas serán realidad y de uso cotidiano los criptosistemas cuánticos en las redes como la Internet, gracias a los avances tecnológicos de la computación cuántica.

Agradecimientos

MAMV agradece el apoyo recibido del programa EDD del IPN.

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).

Referencias

[Ambainis02] Ambainis, A., Smith, A., Yang, K., "Extracting Quantum Entanglement", in Proceedings of the 17th IEEE Annual Conference on Computational Complexity" (2002).

[Bennett98] Bennett, C., Shor, P., "Quantum information theory", in Information Theory, IEEE Transactions (Volume: 44 Issue: 6 , Oct. 1998), Page(s): 2724 -2742.

[Beth00] Beth, T., "Quantum Computing: An Introduction", in ISCAS 2000 – IEEE International Symposium on Circuits and Systems (May 28-31, 2000, Genova, Switzerland).

[Hughes94] Hughes, R., J., "Quantum Cryptography", (1994).

[Johnson02a] Jonson, R., "Magiq employs quantum technology for secure encryption", in EETIMES, http://www.eetonline.com/at/news/OEG20021105S0019 (November 6, 2002).

[Johnson02b] Jonson, R., "Quantum encryption secures high-speed data stream", in http://www.eetonline.com/at/news/OEG20021107S0031 (November 8, 2002).

[Keyes01] Keyes, R., "Fundamental limits of silicon technology", in Proceedings of the IEEE (Volume: 89 Issue: 3, March 2001), Page(s): 227 -239.

[Nayak02] Nayak, A., Salazman, J., "On Communication over an Entanglement-Assisted Quantum Channel", in Proceedings of the 34th Annual ACM Symposium on Theory of Computing (2002).

[Oskin02] Oskin, M., Chong, F., Chuang, I., "A Practical Architecture for Reliable Quantum Computers", in Computer (Volume: 35 Issue: 1, Jan. 2002), Page(s): 79 -87.

[Steane97] Steane, A., "Quantum Computing", in Department of Atomic and Laser Physics (University of Oxford, , England, July, 1997).

[Steffen01] Steffen, M., Vandersypen, L., Chuang, I., "Toward Quantum Computation: A Five-Qubit Quantum Processor", in IEEE MICRO (Volume: 21 Issue: 2, March-April 2001). Page(s): 24 -34.

[Svennson01] Svennson, C., "Future of CMOS – physical limits, trends, and perspectives", in QNANO Workshop (2001).

[White00] White, A., James, D., Munro, W., Kwiat, P., "Measuring entanglement and entanglement measures", in Quantum Electronics and Laser Science Conference (2000), Page(s): 163 -163.

[Zbinden98] Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., Zbinden, H., "Automated 'plug and play' quantum key distribution", Electronics Letters (Volume: 34 Issue: 22 , 29 Oct. 1998), Page(s): 2116 -2117.