Advances in Computer Network Applications

Research in Computing Science

Series Editorial Board

Research in Computing Science es una publicación trimestral, de circulación internacional, editada por el Centro de Investigación en Computación del IPN, para dar a conocer los avances de investigación científica y desarrollo tecnológico de la comunidad científica internacional. **Volumen 142,** octubre 2017. Tiraje: 500 ejemplares. *Certificado de Reserva de Derechos al Uso Exclusivo del Título* No.: 04-2005-121611550100-102, expedido por el Instituto Nacional de Derecho de Autor. *Certificado de Licitud de Título* No. 12897, *Certificado de licitud de Contenido* No. 10470, expedidos por la Comisión Calificadora de Publicaciones y Revistas Ilustradas. El contenido de los artículos es responsabilidad exclusiva de sus respectivos autores. Queda prohibida la reproducción total o parcial, por cualquier medio, sin el permiso expreso del editor, excepto para uso personal o de estudio haciendo cita explícita en la primera página de cada documento. Impreso en la Ciudad de México, en los Talleres Gráficos del IPN – Dirección de Publicaciones, Tres Guerras 27, Centro Histórico, México, D.F. Distribuida por el Centro de Investigación en Computación, Av. Juan de Dios Bátiz S/N, Esq. Av. Miguel Othón de Mendizábal, Col. Nueva Industrial Vallejo, C.P. 07738, México, D.F. Tel. 57 29 60 00, ext. 56571.

Editor responsable: *Grigori Sidorov, RFC SIGR651028L69*

Research in Computing Science is published by the Center for Computing Research of IPN. **Volume 142**, October 2017. Printing 500. The authors are responsible for the contents of their articles. Printed in Mexico City, in the IPN Graphic Workshop – Publication Office.

Advances in Computer Network Applications

Arnoldo Díaz Ramírez
Carlos M. Tavares Calafate
Verónica Quintero Rosas
Juan Pablo García Vázquez (eds.)

Instituto Politécnico Nacional, Centro de Investigación en Computación
México 2017

ISSN: 1870-4069

Instituto Politécnico Nacional (IPN)
Centro de Investigación en Computación (CIC)
Av. Juan de Dios Bátiz s/n esq. M. Othón de Mendizábal
Unidad Profesional "Adolfo López Mateos", Zacatenco
07738, México D.F., México

http://www.rcs.cic.ipn.mx
http://www.ipn.mx
http://www.cic.ipn.mx

Indexed in LATINDEX, DBLP and Periodica

Printing: 500

Printed in Mexico

ISSN 1870-4069

Editorial

This volume of the "Research in Computing Science" journal is conformed by selected papers related to the computer networks theory and its applications. Computer networks, either wired or wireless, are becoming much more relevant nowadays. Social networks, video and audio streaming services, and electronic commerce, are examples of applications that are part of everyday life. However, it is expected that computer networks will be even more relevant in the near future, through applications of the Internet of Things, Smart Cities, Cyber-Physical Systems, or Software Defined Networks, to mention a few.

This volume contains ten papers, which were carefully chosen by the editorial board on the basis of the at least three reviews by the members of the technical program committee. The reviewers took into account the originality, scientific contribution to the field, soundness and technical quality of the papers. The acceptance rate was of 48% among the received submissions.

The papers of this volume address interesting topics regarding computer networks applications. The accepted papers cover topics ranging from Internet of Things, eHealth, performance evaluation of computer networks, cloud computing, security, vehicular networks, energy consumption, eLearning and image processing.

I would like to thank the members of Department of Computer Systems of the Instituto Tecnologico de Mexicali by their valuable support, the Organizing Committee, the Technical Program Committee, and the Red Temática de Sistemas y Redes de Próxima Generación del Conacyt. Also, I would also like to thank to the National Polytechnic Institute (IPN) and its Center for Computing Research (CIC) for the given support.

The entire submission, reviewing, and selection process, as well as preparation of the proceedings, were supported for free by the EasyChair system (www.easychair.org).

Arnoldo Díaz Ramírez
Guest Editor
Tecnológico Nacional de México,
Instituto Tecnológico de Mexicali,
Mexico

October 2017

ISSN 1870-4069

Table of Contents

Page

ISSN 1870-4069

Detección y extracción automática de eventos S1, S2, S3 y S4 en sonidos del corazón

P. Mayorga[1], G. Chavez[1], V. Arguelles[1], C. Druzgalski[2], V. Zeljkovic[3]

[1] Instituto Tecnológico de Mexicali, Depto. de Posgrado, Mexicali, México

[2] California State University, Elec. Eng. Dept., Long Beach, CA, USA

[3] The Lincoln University, CPES Dept., PA, USA

christopher.druzgalski@csulb.edu

Resumen. Debido a la limitación de los rangos de frecuencia en la percepción humana, las enfermedades cardiacas son difícilmente detectadas solo por auscultación con estetoscopio clásico. En muchos de los casos resulta en un diagnóstico tardío, y además de esto las técnicas actuales no logran ser suficientes o los equipos son sofisticados y costosos. Diversas propuestas han surgido en la literatura para otros eventos acústicos como la voz, estos se apoyan en transformadas de Hilbert-Huang, y detección de eventos. Por lo que en el presente artículo se propone un método novedoso de detección automática de eventos en señales HS. La propuesta en este trabajo está basada en Detección de Actividad de Voz, Modelos Mezclados Gaussianos (VAD-GMM), y la transformada de Hilbert (HT). Los resultados son alentadores logrando hasta un 97% de eficiencia en la clasificación mediante Modelos Ocultos de Markov (HMM), para eventos de S1, S2, S3 y S4 en sonidos del corazón (HS).

Palabras clave: Sonidos del corazón (HS), detección de actividad de voz (VAD), modelos mezclados gaussianos (GMM), transformada de Hilbert (HT).

Detection and Automatic Extraction of Events S1, S2, S3 and S4 in Heart Sounds

Abstract. Because the human hear has limitations in some perception ranges, the cardiac diseases are hardly detected by traditional methods of auscultation. In many cases it results in a late diagnosis, and also the current techniques can not be enough, even sophisticated equipment's are too expensive to be used in simple medical offices. Some proposals have arisen in the literature for acoustic events such as the voice, these are based on Hilbert-Huang transform, and event

detection. Therefore, in the present paper we propose a novel method of automatic detection of events in Heart Sounds (HS), signals. Our proposal is based on Voice Activity Detection (VAD), implemented with Mixed Gaussian Models (VAD-GMM) and the Hilbert Transform (HT). The results are motivated, because the efficiency in classification using Hidden Markov Models (HMM), for S1, S2, S3 and S4 events in heart sounds has reached 97%.

Keywords: Gaussian mixed models (GMM), heart sounds (HS), Hilbert transform (HT), voice activity detection (VAD).

1. Introducción

El uso de la tecnología ha facilitado y mejorado los procesos en la medicina. Tal es el caso de la auscultación cardiaca y respiratoria, la cual por medio del avance de la tecnología ha logrado mejorar las técnicas de auscultación aplicando el estetoscopio, y de esta manera tener una mejor percepción de los sonidos cardiopulmonares. Una alternativa en la reducción de ruido es el filtrado (pasa banda, pasa baja, pasa altas), que permite eliminar frecuencias no necesarias y que afectan la detección de los eventos S1 y S2 [1]. Sin embargo, las limitaciones con los que se cuenta en los centros de atención medica han originado propuestas como grabaciones de sonidos cardiacos utilizando micrófonos con condensador, es decir, convirtiendo los estetoscopios tradicionales en estetoscopios digitales, con ello se facilita el acceso a consultorios y centros de investigación que cuenten con recursos limitados [1]. En la actualidad existen distintos niveles de atención médica [2], algunos básicos y otros más especializados; los niveles de atención médica básicos cuentan con cierta funcionalidad, implicando al menos equipo como un estetoscopio. Además, por normatividad se debe contar con una computadora para el expediente electrónico del paciente [3, 4], lo cual es asequible.

Desafortunadamente, el estetoscopio presenta varios retos, como el ruido ambiental y el traslape de los Sonidos del Corazón (HS), con los Sonidos del Pulmón (LS). Debido a esto, la percepción de sonidos cardiacos queda restringida a la capacidad y experiencia del médico, y puesto que hay frecuencias fuera de los rangos auditivos humanos se dificulta diagnosticar con certeza la existencia de alguna enfermedad [5]. Debido a lo anterior, es necesario un sistema que no dependa del oído humano, que pueda detectar y clasificar sonidos cardiopulmonares por métodos automatizados y computarizados. Algunas aproximaciones son dirigidas a enfermedades endémicas, en donde se utilizan las características acústicas de la tos y crepitaciones para reforzar vectores de Coeficientes Cepstrales en Frecuencia Mel (por sus siglas en inglés, MFCC), aplicando ondículas (Wavelets), [6]. Otros trabajos se destinan al análisis y monitoreo de las ondas sonoras del corazón [7]. Otros autores mencionan que, si bien el uso de estetoscopio es una herramienta de bajo costo, los movimientos de los pacientes sobre todo en niños contaminan los registros de los sonidos [8]. En [9], se propone un algoritmo basado en un método de doble umbral para una detección robusta de los sonidos cardiacos S1 y S2.

La señal original del sonido del corazón (HS), es filtrada aplicando una ventana de Hamming. La envolvente de sonido cardiaco se extrae mediante la Transformada de

Tabla 1. Características principales en sonidos HS.

Sonido	Punto de auscultación	Frecuencia	Características	Duración	Forma de auscultación
S1	Mitral con mayor intensidad que el tricúspide	30- 120 Hz	Causado por la sístole	0.08 – 0.16seg. (0.14seg)	Diafragma del estetoscopio
S2	Mitral	70-150 HZ	Por el cierre valvular aórtico	0.06 – 0.12seg. (0.11seg)	Diafragma del estetoscopio
S3	Mitral	27-70 Hz	Diástole por disfunción ventricular	0.04 - 0.08seg	Campana del estetoscopio
S4	Mitra l	10-50 Hz	Ruido auricular por tensión en válvulas	0.06 – 0.08seg	Campana del estetoscopio

Hilbert-Huang (HHT), y se segmenta el sonido cardiaco por el método de doble umbral [9]. En [10], se presenta un método de baja complejidad para la detección del primer y segundo sonidos del corazón (S1 y S2), y los períodos de sístole y de diástole sin necesidad de utilizar una referencia electrocardiográfica.

El algoritmo utiliza el Modo de Descomposición Empírica (EMD, de sus siglas en inglés), que produce envolventes de intensidad de los principales sonidos del corazón en el dominio del tiempo [10]. En otro estudio [11], se sugiere un método de localización para S1 y S2, basado en un algoritmo que implica el filtrado en frecuencia, detección de energía, y la duración de intervalo. La exactitud de la localización se evaluó comparando el algoritmo con el método de localización basado en transformar de Hilbert tradicional [11].

En [12], se propone un método automático para segmentación y análisis de detección de pico en patrones de Sonidos Cardíaco (HS), con especial atención a las características de las envolventes de HS y teniendo en cuenta las propiedades de la Transformada de Hilbert (HT). Con esto se aplica la Transformada de Hilbert Modificada en Tiempo Corto (STMHT), para segmentar y localizar automáticamente los puntos pico para HS mediante cruce por cero de la STMHT [12].

A través del uso de Coeficientes Cepstrales en Frecuencia Mel (MFCC), se obtienen las características más importantes de los eventos, así como la Detección de Actividad de Voz (VAD), la cual es una herramienta que puede facilitar la detección de actividad y silencio [13]. Por otra parte algunos autores proponen la extracción de características principales por medio de la Transformada Rápida de Fourier (FFT), para llevar a cabo la clasificación [14].

Los sonidos HS patológicos interfieren de manera más significativa en LS que un HS normal y son más difíciles de percibir mediante el oído. Por lo cual, aquí se propone la detección de eventos de S1, S2 en señales HS con presencia de S3 y S4. Por medio de la transformada de Hilbert que facilita y permite la detección de puntos extremos (máximos y mínimos). Además, con el apoyo de las técnicas de VAD que, a su vez

están basadas en modelos GMM se efectúa la extracción automática, lo cual se mostrará a lo largo de este trabajo.

2. Detección de S1, S2, S3 y S4

Los sonidos cardiacos se componen de dos sonidos principales S1 y S2, y en ocasiones especiales se presentan dos ruidos simultáneamente denominados ruidos cardiacos patológicos S3 y S4. El primer sonido S1 y el segundo sonido S2, son producidos por la abertura de las válvulas atrio ventriculares y el cierre de la válvula semilunar, respectivamente y viceversa. Los sonidos S3 y S4 ocurren al final de S2 debido a la vibración del flujo sanguíneo dentro de los ventrículos, el cuarto sonido S4 se encuentra justo antes de S1 debido a la contracción de la aurícula [15]. La **Tabla 1**, contiene los datos más relevantes en cuanto a duración, frecuencia y otras características de HS:

3. Métodos y materiales

En esta sección se explican las técnicas y señales empleadas para llevar a cabo la detección de eventos de S1, S2, S3 y S4 en señales HS; particularmente, al final se describe la técnica VAD-GMM que se está proponiendo en este trabajo.

3.1. Vectores acústicos MFCC, cuartiles y PCA

En MFCC, los sonidos son parametrizados, haciendo un preénfasis con filtros FIR, seguido por una ventana Hamming aplicada a cada trama [16-19]. En este trabajo, se aplicó una tasa de 120 tramas por segundo con el 50% de traslape en señales HS, a las cuales se aplica la Transformada Rápida de Fourier (FFT); posteriormente, se obtiene el módulo y se multiplica por un banco de filtros donde sus rangos de frecuencia y frecuencias centrales están distribuidos en la escala de Mel. A esto le sigue una etapa de logaritmo de la energía obtenida de cada filtro y posteriormente la transformada inversa de Fourier. El resultado final es un vector de características llamado MFCC [13, 20, 21].

El Cuartil q_p, de una variable aleatoria está definido como el número q más pequeño, tal que la función de distribución acumulativa es mayor o igual a una probabilidad p, donde p se encuentra entre $0 < p < 1$. Esto se puede definir con la función de densidad de probabilidad continua $f(x)$ a través de (1):

$$p \int_{-\infty}^{q} f(x)dx \, . \tag{1}$$

La estacionariedad está relacionada con la duración de los eventos, por lo cual el tamaño del vector se seleccionó de una duración menor al evento [14].

En el cálculo de los cuartiles, el primer paso es la lectura de la señal, partiendo de archivos *.wav; posteriormente, se aplica la FFT por cada trama. Cumpliendo con un principio básico para una función de densidad de probabilidad, la distribución espectral se normaliza como en (2):

$$F_N(f) = \int_{-\infty}^{\infty} \frac{f(t)e^{-j2\pi ft}dt}{area(F(f))}, \quad (2)$$

Un ejemplo particular de Cuantiles son los Cuartiles, calculados aquí mediante (3), cuyos valores frecuenciales f0.25, . . ., f0.75 corresponden a cada uno de los respectivos coeficientes cuartílicos [22]:

$$A_{0.25} = \int_{-\infty}^{f_{0.25}} F_N(f)df\ , \ldots, A_{0.75} = \int_{-\infty}^{f_{.75}} F_N(f)df\ , \quad (3)$$

Uno de los propósitos del análisis de componentes principales (PCA), es reducir la dimensionalidad de p a d, en donde $d<p$, y al mismo tiempo conservar la mayor cantidad posible de varianza de los datos originales [23, 24]. En este trabajo, la idea es aplicar PCA para obtener una representación disminuida en dimensión de los vectores de características, pero sin menoscabo de la eficiencia. Al utilizar PCA, se transforman los datos a un nuevo grupo de coordenadas o variables, las cuales son una combinación lineal de las variables originales. Además, las observaciones en el nuevo espacio de componentes principales no están correlacionadas. Esto se hace con el propósito de obtener información útil para comprender los datos u observaciones en el nuevo espacio [25].

3.2. Modelos mezclados Gaussianos (GMM) y ocultos de Markov (HMM)

Un modelo GMM es una tripleta Λ compuesta por las medias, covarianzas y ponderaciones. El modelado GMM se sirve del algoritmo EM para calcular las tripletas $\Lambda_i = \{m_i, \vec{\mu}, \Sigma_i\}$. La media $\vec{\mu}$, representa el promedio de todos los vectores, mientras que la matriz de covarianza Σ_i, modela la variabilidad de las características en una clase acústica [26]:

$$p(\vec{x}|\Lambda) = \sum_{i=1}^{M} m_i b_i(\vec{x}). \quad (4)$$

En la ecuación (4), $\vec{x}$ es un vector MFCC o Cuartílico, b_i ,$\forall_i = 1, \ldots, M$, son las densidades componentes y m_i , $\forall_i = 1, \ldots, M$ son las ponderaciones de cada densidad en el modelo. Cada densidad componente es una función Gaussiana D-dimensional [17, 20]. Cada densidad Gaussiana contiene los parámetros representados como en (5). Específicamente, aquí se calculó un modelo GMM para cada evento y/o ruido-silencio:

$$b_i(\vec{x}) = \frac{1}{(2\pi)^{D/2}|\Sigma_i|^{1/2}} exp\left[-\frac{1}{2}(\vec{x} - \vec{\mu})^T \sum_{i}^{-1}(\vec{x} - \vec{\mu})\right]. \quad (5)$$

Un HMM es un autómata finito basado en estados que no son directamente observados. En esta metodología, cada estado está constituido por un GMM, el cual

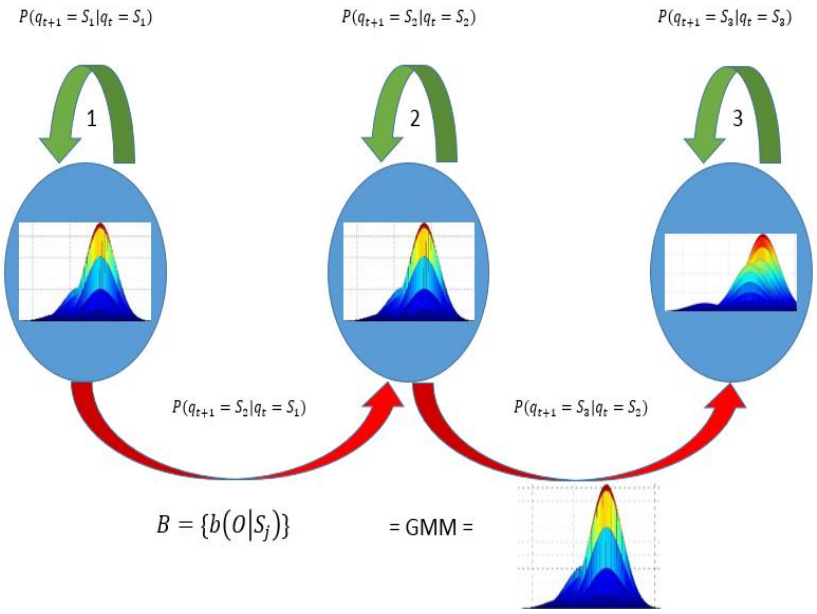


Fig. 1. Modelo HMM.

modela las observaciones correspondientes a ese estado. Un HMM, también es una tripleta $\boldsymbol{\lambda} = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$, donde A es la matriz que regula las transiciones de estado a estado, B (un GMM), es la función de probabilidad que determina si un vector pertenece a un estado determinado y $\boldsymbol{\pi}$ da la probabilidad de iniciar en alguno de los estados. Formalmente, HMM está definido con más precisión en [27, 28], y es entrenado con el algoritmo EM. En el caso de los experimentos de este estudio, las observaciones pueden ser vectores acústicos MFCC, Cuartiles.

Al igual que en el caso de los modelos GMM, es convencional expresar los modelos HMM como tripletas (A, B, π). Un ejemplo de modelo HMM para señales acústicas se muestra en la **Fig. 1**.

El entrenamiento o aprendizaje de los parámetros HMM, dado un conjunto o secuencia de observaciones $\{O_i\}$, es típicamente efectuado aplicando el algoritmo Baum-Welch [28], el cual determina los parámetros maximizando la *verosimilitud* o probabilidad $P(O_i|\lambda)$. En la etapa de evaluación, se requiere calcular $P(O|\lambda)$, dado el modelo λ y una secuencia O de observaciones; aquí se aplicó algoritmo de forward-backward [28].

La arquitectura HMM fue de tipo izquierda-derecha (*Bakis*), como lo muestra la Figura 1. Aquí, el vector π denota las probabilidades iniciales (*a priori*), de estar en alguno de los estados q; los valores $a_{i,j}$ son las probabilidades de transición entre estados, mientras que $b_i(O)$, es la probabilidad de que la observación O (vector acústico), haya sido emitido en el estado q_i (para este caso un GMM). Se puede destacar que las probabilidades de transición y de estado inicial, fueron inicializadas aleatoriamente.

3.3. Transformada de Hilbert

La transformada de Hilbert de una señal produce un adelanto de fase en π/2, radianes. Cuando una señal es causal en un dominio, ya sea tiempo o frecuencia, la parte real y la imaginaria en el otro dominio están vinculadas por la transformada de Hilbert [29]. Se define la transformada de Hilbert como la convolución de *f(t)*, con la función -1/πt:

$$HT\{f(t)\} = f(t) * \frac{-1}{\pi t} = \frac{-1}{\pi}\int_{-\infty}^{\infty} \frac{f(\tau)}{t-\tau} d\tau. \quad (6)$$

Convolucionar en tiempo por -1/ πt, es equivalente a multiplicar en frecuencia por *i*sign(w)*, es decir no se modifica el espectro en amplitud, solo se efectúa un corrimiento π/2 para frecuencias positivas y de -π/2 para frecuencias negativas. Si escribimos la función exponencial compleja de la siguiente forma:

$$e^{i\omega t} = \cos \omega t + i \sin \omega t = \cos \omega t - iHT\{\cos \omega t\}. \quad (7)$$

Podemos generalizar esta idea y crear una función compleja a partir de una función real, cuya parte imaginaria tenga un retardo en fase de 90° respecto de su parte real, es decir:

$$g(t) = f(t) - iHT\{f(t)\}. \quad (8)$$

La función *g(t)* es conocida como función analítica asociada a *f(t)*. Dada una función en tiempo cuya parte imaginaria sea igual a menos la transformada de Hilbert de su parte real, su transformada de Fourier será causal. Análogamente, si una función temporal es causal, la parte real e imaginaria de su transformada de Fourier estarán vinculadas por la transformada de Hilbert. De aquí, se define a la envolvente *E(t*) de una función f(t), como el módulo de su función analítica:

$$E(t) = |g(t)| = \sqrt{f(t)^2 + HT\{f(t)\}^2}. \quad (9)$$

3.4. VAD-GMM

Los detectores de actividad de voz (VAD), son fundamentales en el uso eficiente de ancho de banda [30], por lo cual resulta útil en señales HS y LS. Aquí se propone una versión de VAD basada en Modelos Mezclados Gaussianos (GMM), a diferencia de los modelos de VAD tradicionales, aquí se toman como referencia los sonidos cardiacos. Estos permiten detectar los segmentos activos de interés en las señales relacionadas con patologías cardiacas. Mediante VAD y cálculo de umbrales se extrajo automáticamente cada uno de los eventos de las señales HS.

En la primera etapa del experimento se utiliza un corpus de señales HS a las cuales se les aplica blanqueado, centrado y filtrado. Específicamente, se aplicó un filtro pasa bajas Butterworth de orden 7 y frecuencia de corte 150Hz, con el fin de suprimir ruido. A partir de estas señales se efectuaron recortes manuales obteniendo un nuevo corpus de señales que contienen un solo evento (S1, S2, S3 o S4 según sea el caso).

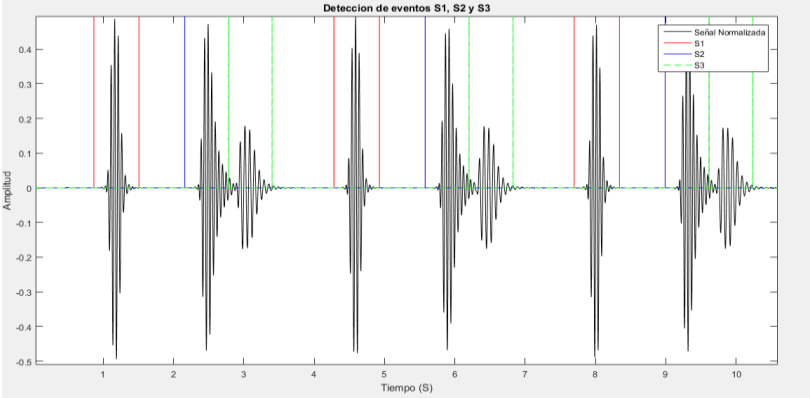


Fig. 2. Detección de eventos S1, S2 y S3 en señal Hs.

Con este nuevo corpus se calcularon los vectores acústicos para calcular modelos GMM correspondientes a cada evento, estos modelos GMM fueron utilizados para la implementación del método VAD propuesto. VAD se aplica para determinar zonas de actividad (correspondientes al evento), y zonas de no actividad (ruido o silencio).

Los vectores acústicos calculados por clase fueron MFCC (en S1, S2, S3 y S4), otra clase que se define aquí es la compuesta por ruido o silencio. Para MFCC se aplicó una tasa de 120 tramas por segundo, 13 coeficientes por vector. Posteriormente, se le aplicó PCA para obtener una representación mejorada, de la cual se utilizan únicamente los primeros 4 coeficientes.

Aplicando los modelos GMM sobre la señal se determina si el vector corresponde a actividad (asignando un 1), o a silencio (asignando un 0). Una vez que se determina la zona de actividad y no actividad esta se multiplica por la señal original obteniendo una nueva señal con solo actividad. A esta nueva señal se le extrae la envolvente por medio de la transformada de Hilbert, la cual es suavizada con un filtro Butterworth de orden 5 y frecuencia de corte de 8 Hz.

Para determinar S1, S2 y S3 o S4 es necesario calcular umbrales, los cuales son obtenidos con base en las amplitudes de los eventos correspondientes.

4. Resultados

Los resultados fueron obtenidos con particiones logradas con validación cruzada. Para medir la eficiencia de la propuesta se efectuó clasificación con los eventos con nuevos corpus de señales obtenidos por detección automática. Para lo anterior se efectuaron experimentos de clasificación aplicando Modelos Ocultos de Markov (HMM), sobre el nuevo corpus de señales. Aplicando detección automática VAD-GMM se obtiene la Fig. **2** y Fig. **3**, así mismo esto arroja los índices de inicio y fin de cada evento para su extracción. Para el primer y segundo experimento de clasificación se utilizó una base de datos de 20 señales de S1, S2 y S3 a su vez 20 señales de S1, S2 y S4, las cuales fueron extraídas automáticamente con VAD-GMM.

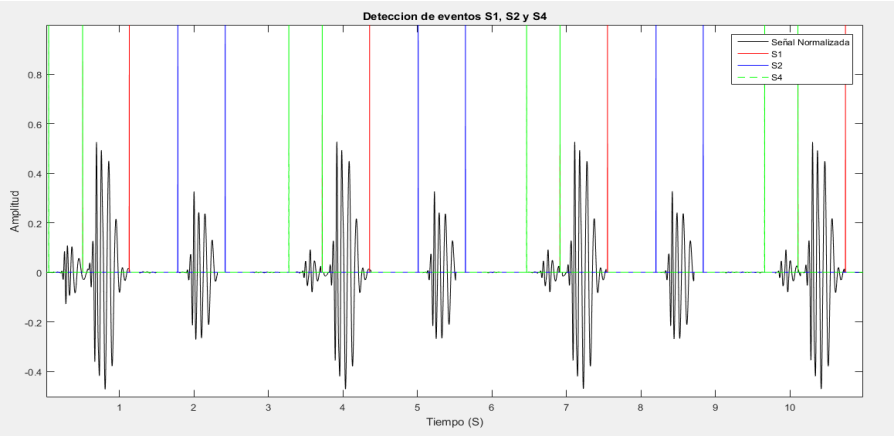


Fig. 3. Detección de eventos S1, S2 y S4 en señal Hs.

Tabla 2. Eficiencia de clasificación con VAD aplicando detección automática en señales HS con S1, S2 y S3.

# Estados	# Gaussianas	Vectores Acústicos	Eficiencia de clasificación
3	3	Cuartiles	90.4762
3	3	MFCC	95.3968
2	3	Cuartiles	85.0794
2	3	MFCC	96.9841

Tabla 3. Eficiencia de clasificación con VAD aplicando detección automática en señales HS con S1, S2 y S4.

# Estados	# Gaussianas	Vectores acústicos	Eficiencia de clasificación
3	3	Cuartiles	90.2143
3	3	MFCC	96.1111
2	3	Cuartiles	91.3456
2	3	MFCC	97.2222

Para evaluar la eficiencia en este proceso, se experimentó con varias configuraciones de arquitectura en los modelos HMM, así como 2 tipos de vectores acústicos (cuartiles y MFCC). Donde los mejores resultados de la eficiencia de clasificación se muestran en la **Tabla** , siendo para una arquitectura compuesta por 2 estados y 3 Gaussianas obteniendo hasta un 96.98% de eficiencia de clasificación.

Para el segundo experimento se utilizó el mismo conjunto de señales que en el experimento anterior (esta vez para S4), obteniendo mejores resultados de clasificación con una composición de 2 estados y 3 Gaussianas como se muestra en la **Tabla** .

Primero se obtuvo un corpus con segmentación manual de los eventos, este nuevo corpus fue de utilidad para calcular modelos GMM que fueron la base del método propuesto de VAD. La segmentación automática se logró aplicando el método de VAD propuesto, mientras que para evaluar la eficiencia se calcularon modelos HMM empleando el corpus obtenido con el VAD propuesto. Aunque aquí no se muestran resultados con segmentación manual, los resultados obtenidos con segmentación automática indican que puede sustituir la segmentación manual realizada por una persona. Además, este proceso resulta más objetivo y menos dependiente de las capacidades auditivas y visuales del profesional de la salud.

5. Conclusión

Para el mejoramiento de la detección automática de eventos en señales HS se propuso la detección aplicando transformada de Hilbert combinada con modelos GMM constituyendo una técnica de VAD.

Por medio de detección automática se obtuvo un corpus de 20 señales (para cada uno de los eventos), de S1, S2, S3 y S1, S2 y S4. Se efectuó la clasificación de señales aplicando dos corpus, uno obtenido mediante recortes manuales, y otro mediante la detección automática. La detección automática supero los resultados en clasificación con respecto al corpus obtenido por detección (recortes), manuales. Se llevó a cabo la clasificación por medio de HMM obteniendo hasta un 96.9% de eficiencia para los sonidos de S3 y un 97% para S4.

El diagnóstico mediante detección automática promete ser un método más eficaz y seguro que métodos tradicionales, los cuales quedan limitados por la capacidad auditiva de un médico. Resulta interesante y necesario extender estas metodologías para sonidos del pulmón (LS), y hacer diagnósticos cardiopulmonares.

Referencias

1. Azarbarzin, A., Moussavi, Z. M. K.: Automatic and Unsupervised Snore Sound Extraction From Respiratory Sound Signals. IEEE Transactions on Biomedical Engineering, 58, pp. 1156−1162 (2011)
2. Earis, J.: Lung sounds. Thorax, 47, pp. 671−672 (1992)
3. NOM-016-SSA3-2012: Características mínimas de infraestructura y equipamiento de hospitales y consultorios de atención médica especializada. Diario Oficial (2013)
4. Forgacs, P.: Lung sounds. Br J Dis Chest, 63, pp. 1–12 (1969)
5. Lozano, M., Fiz, J. A., Jan, R.: Automatic Differentiation of Normal and Continuous Adventitious Respiratory Sounds Using Ensemble Empirical Mode Decomposition and Instantaneous Frequency. IEEE Journal of Biomedical and Health Informatics, 20, pp. 486−497 (2016)
6. Kosasih, K., Abeyratne, U. R., Swarnkar, V., Triasih, R.: Wavelet Augmented Cough Analysis for Rapid Childhood Pneumonia Diagnosis. IEEE Transactions on Biomedical Engineering, 62, pp. 1185−1194 (2015)

7. Herzig, J., Bickel, A., Eitan, A., Intrator, N.: Monitoring Cardiac Stress Using Features Extracted From S1 Heart Sounds. IEEE Transactions on Biomedical Engineering, 62, pp. 1169−1178 (2015)
8. Emmanouilidou, D., McCollum, E. D., Park, D. E., Elhilali, M.: Adaptive Noise Suppression of Pediatric Lung Auscultations With Real Applications to Noisy Clinical Settings in Developing Countries. IEEE Transactions on Biomedical Engineering, 62, pp. 2279−2288 (2015)
9. Chen, Jie., Hou, Hai-Liang., Luo, Liang-Cai., Yun, C.: Automatic Identification Method for the First and Second Heart Sound Based on Double-threshold. Journal Computer Engineering, 38, pp. 174−177 (2012)
10. Bajelani, K., Navidbakhsh, M., Behnam, H., Doyle, J. D., Hassani, K.: Detection and identification of first and second heart sounds using empirical mode decomposition. Journal of Engineering in Medicine, 227, pp. 976−987 (2013)
11. Dong, M. S., Hangsik, S.: A Localization Method for First and Second Heart Sounds Based on Energy Detection and Interval Regulation. Journal of Electrical Engineering and Technology, 10, pp. 2126−2134 (2015)
12. Sun, S., Jiang, Z., Wang, H., Fang, Y.: Automatic moment segmentation and peak detection analysis of heart sound pattern via short-time modified Hilbert transform. Computing Methods Prog. Biomed, 114, pp. 219−230 (2014)
13. Abushakra, A., Faezipour, M.: Acoustic Signal Classification of Breathing Movements to Virtually Aid Breath Regulation. IEEE Journal of Biomedical and Health Informatics, 17(2), pp. 493–500, DOI:10.1109/JBHI.2013.2244901 (2013)
14. Devangan, H., Jain, N.: A Review on Classification of Adventitious Lung Sounds. International Journal of Engineering Research & Technology, 4 (2015)
15. Ashok, M., Parthasarathi, B., Goutam, S.: An automated tool for localization of heart sound components S1, S2, S3 and S4 in pulmonary sounds using Hilbert transform and Heron's formula. Department of Electronics and Electrical Communication Engineering, IndianInstitute of Technology, Kharagpur, Kharagpur, 721, pp. 302, DOI:10.1186/2193-1801-2-512 (2013)
16. Istrate, D. M.: Detection et Reconnaissance des Sons pour la Surveillance Médicale. These pour obtenir le grade de docteur de l'INPG: spécialité Signal, Image, Parole, Télécoms docteur Institut National Polytechnique de Grenoble (2003)
17. Mayorga, P., Druzgalski, C., Vidales, J.: Quantitative Models for Assessment of Respiratory Diseases. Pan American Health Care Exchange (PAHCE), pp. 25−30 (2010)
18. Boston Children's Hospital: http://www.childrenshospital.org/
19. Pearce, D.: Developing the ETSI Aurora advanced distributed speech recognition front-end and what next?. Automatic Speech Recognition and Understanding, (ASRU'01), IEEE Workshop, pp. 131−134 (2001)
20. Mayorga, P., Besacier, L., Lamy, R., Serignat, J. F.: Audio packet loss over IP and speech recognition. IEEE Workshop on Automatic Speech Recognition and Understanding, pp. 607−612 (2003)
21. Yoon, Jae Sam, Gil Ho Lee, Hong Kook Kim: A MFCC-Based CELP Speech Coder for Server-Based Speech Recognition in Network Environments. IEICE Trans. Fundam. Electron. Commun. Comput. Sci, E90-A, pp. 626−632 (2007)

22. Mayorga, P., Druzgalski, C., González, O. H., Lopez, O. H.: Modified classification of normal Lung Sounds applying Quantile Vectors. Engineering in Medicine and Biology Society (EMBC), Annual International Conference of the IEEE, pp. 4262–4265 (2012)
23. Martinez, W. L.: Computational Statistics Handbook with Matlab. Second ed. (2008)
24. Wendy, L., Martinez, A., Martinez, R., Solka, J. L.: Exploratory Data Analysis with MATLAB. Second Edition, (2011)
25. Mayorga-Ortiz, P., Druzgalski, C., Criollo-Arellano, M. A., González-Arriaga, O. H.: GMM y LDA aplicado a la detección de enfermedades pulmonares. Revista mexicana de ingeniería biomédica, 34, pp. 131−144 (2013)
26. Bimbot, F., Bonastre, J.-F., Fredouille, C., Gravier, G., Magrin-Chagnolleau, I., Meignier, S., et al.: A Tutorial on Text-Independent Speaker Verification. EURASIP Journal on Advances in Signal Processing, pp. 1–22 (2004)
27. Kannadaguli, P., Bhat, V.: A comparison of Gaussian Mixture Modeling (GMM) and Hidden Markov Modeling (HMM) based approaches for Automatic Phoneme Recognition in Kannada. Signal Processing and Communication (ICSC), International Conference on, pp. 257–260 (2005)
28. Rabiner, L. R., Juang, B. H.: Fundamentals of speech recognition. Englewood Cliffs, N.J., PTR Prentice Hall, (1993)
29. Mondal, A., Kumar, A. K., Bhattacharya, P. S., Saha, G.: Boundary estimation of cardiac events S1 and S2 based on Hilbert transform and adaptive thresholding approach. Medical Informatics and Telemedicine (ICMIT), Indian Conference on, pp. 43–47 (2013)
30. Jongseo-Sohn, N. S. K., Wonyong, S.: A Statistical Model-Based Voice Activity Detection. IEEE Signal Processing Letters, 6 (1999)

ISSN 1870-4069

Máquinas de soporte vectorial para inferir el punto de atención de automovilistas vistiendo lentes inteligentes

José M. Ramírez, Marcela D. Rodríguez, Ángel G. Andrade, Antonio Ordorica

Universidad Autónoma de Baja California, Facultad de Ingeniería, Mexicali, B.C., México

{jramirez53, marcerod, aandrade, aordorica}@uabc.edu.mx

Resumen. La mayoría de los métodos para inferir la distracción durante la conducción, se basan en características visuales de la postura de la cabeza, ya que es un fuerte indicador de la distracción durante la conducción. En este trabajo, se propone el uso de sensores inerciales empotrados en lentes inteligentes. Para ello, recopilamos datos de cinco participantes y realizamos experimentos para evaluar la viabilidad del uso de máquinas de soporte vectorial (SVM) para generar modelos de los conductores para inferir el punto de atención. Los resultados muestran un desempeño aceptable de la SVM para identificar las posiciones particulares de la cabina del automóvil donde los conductores centran su atención. Hasta el momento hemos obtenido una exactitud promedio de 83,42%.

Palabras clave: distracción, conducción; máquinas de soporte vectorial; lentes inteligentes, sensores inerciales.

Support Vector Machines to Infer the Point of Attention of Motorists Wearing Smart Glasses

Abstract. Most of the methods for inferring distraction while driving are based on visual characteristics of head posture, since it is a strong indicator of distraction while driving. This paper proposes the use of mounted inertial sensors on intelligent lenses. Hence, data was collected from five participants and experiments were conducted to evaluate the feasibility of using support vector machines (SVM) to generate models of drivers to infer the point of attention. Results show an acceptable performance of the SVM to identify specific positions of the car cabin on which drivers focus their attention. Until now, an average accuracy of 83.42% has been achieved.

Keywords: distraction, driving, support vector machines; intelligent lenses, inertial sensors.

1. Introducción

La distracción del conductor durante la conducción o la inatención se refiere a la falta de atención a las tareas de conducción debido a la participación en otras tareas durante la conducción. Estas otras tareas pueden ser cualquier distracción de la atención como distracciones cognitivas, físicas o visuales que conducen a la degradación del rendimiento [1]. Se estima que las distracciones causan el 23% de los accidentes o casi accidentes [2], y que podría reducirse un 10-20% mediante sistemas de monitoreo y predicción de los comportamientos de la conducción [3,4]. Evitar la distracción durante la conducción ha sido de particular interés al utilizar artefactos de navegación [5]. También se han explorado métodos para detectar la distracción del conductor y la somnolencia, que se basan principalmente en el análisis de las características abstraídas de imágenes y videos de las expresiones faciales, posición de la cabeza [4], y el comportamiento de la mirada [6].

En particular, la posición de la cabeza (o la orientación de la cabeza) es un fuerte indicador del campo de visión del conductor y el centro de atención actual [7, 8]; por lo tanto, se ha considerado como un proceso integral para monitorear el nivel de alerta del conductor [8]. Sin embargo, los métodos basados en el procesamiento de imágenes requieren que la cabina del vehículo sea equipada con cámaras [7, 8, 9]. Por ejemplo, faceLAB utiliza dos cámaras para determinar la posición de la cabeza y la dirección de la mirada del ojo [9]. Por otro lado, los lentes inteligentes han surgido como una interesante plataforma de investigación y de productos para una amplia gama de sistemas de apoyo portátiles debido a sus capacidades de detección. La seguridad en relación con el uso de los lentes inteligentes durante la conducción ha sido cuestionada, ya que permiten a los usuarios enviar mensajes de texto o acceder sus redes sociales a través de comandos de voz. Sin embargo, las investigaciones han demostrado que podrían mejorar la seguridad de los conductores que corren el riesgo de sufrir fatiga (por ejemplo, los conductores de camiones); y que quienes usan teléfonos inteligentes se distraen más y con más frecuencia que quienes utilizan Google Glass [10]. En este artículo, proponemos el uso de sensores inerciales incorporados en los lentes inteligentes para obtener características de la postura de la cabeza para inferir el foco de atención actual de los conductores. Para alcanzar este objetivo, se utilizaron los datos recolectados del acelerómetro, magnetómetro y giroscopio de un Google Glass. Estos datos fueron utilizados para generar modelos de la Máquina de Soporte Vectorial (SVM). Esta es una técnica de aprendizaje supervisado que busca un hiperplano óptimo para separar los datos entre clases definidas [11, 12]. El objetivo general de este proyecto es conocer cuál es el desempeño de la SVM y bajo qué condiciones, para determinar el foco de atención del conductor.

En la siguiente sección, se explican los métodos utilizados para recolectar datos y procesarlos para experimentar con la SVM. La sección 4 presenta el diseño del experimento, el cuál consistió de 3 ensayos en los que probamos diferentes condiciones relacionadas a las técnicas de entrenamiento y a los sensores utilizados. La sección 4 muestra los resultados obtenidos, y la sección 5 concluye y presenta las posibles direcciones futuras de este trabajo.

2. Recolección y procesamiento de datos

Se recolectaron datos de 5 sujetos (media de edad M=32; DS= 11.2 años), mediante un experimento controlado en condiciones naturalistas. Cada sujeto participó en una sesión en la que realizó un conjunto de tareas (ver Tabla 1), en un automóvil mientras usaba los Google Glass, y conduciendo en un estacionamiento privado. Los datos recogidos consistieron de vectores de 9 tuplas, correspondiente a los valores x, y z del acelerómetro, giroscopios y magnetómetro.

Tabla 1. Tareas realizadas por los sujetos asociadas a la distracción causantes de riesgos [13].

Tarea Secundaria	**Tareas realizadas durante el experimento**
Uso del teléfono celular	Marcar (teclas rápidas), hablar / escuchar, enviar mensajes de texto
Interacción con un objeto	Mirar el objeto, mover un objeto, alcanzar un objeto
Bebiendo	Quitar tapadera al recipiente
Uso de la consola de confort e información	Encender / Apagar el clima, ajustar la temperatura, insertar / retirar CD, ajuste de radio

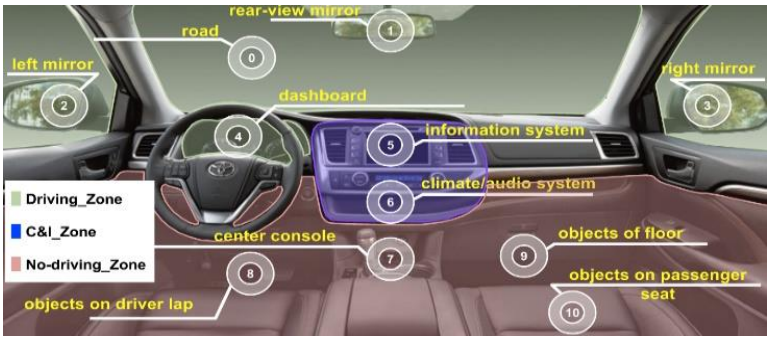


Fig. 1. Posiciones de la cabina usadas como clases (Posición 0-10).

Tabla 2. Instancias capturadas por cada posición de todos los sujetos.

S	**Muestra**		**Posiciones**										
	D	D E	0	1	2	3	4	5	6	7	8	9	10
S1	3,443	1,877	~~1,064~~	122	434	17	16	89	20	8	97	7	3
S2	3,138	1,203	~~466~~	281	238	87	7	51	49	8	6	5	5
S3	2768	1351	~~933~~	2	256	26	56	30	24	13	0	4	7
S4	2000	898	~~463~~	14	308	23	33	15	17	7	8	3	7
S5	2042	1074	~~489~~	37	384	38	0	36	21	18	23	9	19
TOTAL	**13,391**	**6,403**	**3,415**	**456**	**1,620**	**191**	**112**	**221**	**131**	**54**	**134**	**28**	**41**

La frecuencia de muestreo del acelerómetro se estableció en 15.5 Hz, la más rápida a través de la API de Android, lo que nos permitió obtener un promedio de 15.5 lecturas por segundo. Todas las sesiones fueron grabadas en video para posteriormente etiquetar los datos para poder utilizar técnicas de aprendizaje supervisado como la SVM [11, 12]. Etiquetamos los datos usando diez clases de posiciones relacionadas con las ubicaciones de la cabina del vehículo donde los participantes centraron su atención conforme realizaban las tareas solicitadas. Como se muestra en la Figura 1, estas clases corresponden a diferentes posiciones de la cabina del vehículo. Por ejemplo, un conductor podría centrar su atención en el punto 5 cuando cambia la estación de radio. Por lo tanto, se evaluó la viabilidad de identificar puntos particulares donde los conductores enfocaron su atención, lo que ayudaría a identificar si está llevando a cabo una tarea secundaria.

3. Descripción del experimento

La plataforma utilizada para generar un modelo SVM fue WEKA (Waikato Environment for Knowledge Analysis), ya que ofrece una colección de algoritmos de aprendizaje automático para tareas de minería de datos. WEKA contiene herramientas para pre procesamiento de datos, clasificación, regresión, clustering, reglas de asociación y visualización. [14] Adicionalmente se utilizó la funcionalidad de WEKA para normalizar los datos.

Este experimento consistió de 3 ensayos para identificar bajo qué condiciones la SVM logra un mejor desempeño de clasificación.

Para cada ensayo se reportan la Exactitud (*Accuracy*), la Precisión (*Precision*) y el Recuerdo (*Recall*) como las métricas del desempeño de la clasificación [11,12]. Precisión es la proporción de elementos clasificados como positivos que son realmente verdaderos positivos [16]:

$$Precisión = \frac{vp}{vp+fp}, \tag{1}$$

donde vp son los verdaderos positivos y fp los falsos positivos.

Recuerdo (*Recall*) es la proporción de elementos verdaderos positivos que son correctamente clasificados como positivos [16]:

$$Recuerdo = \frac{vp}{vp+fn}, \tag{2}$$

donde fn son los falsos negativos.

Exactitud (*Accuracy*): que es una medida de eficiencia generalizada para evaluar el desempeño de un clasificador, y se refiere a las instancias correctamente clasificadas [16]:

$$Exactitud = \frac{vp+vn}{vp+vn+fp+fn}, \tag{3}$$

donde vn son los verdaderos negativos.

Cabe mencionar que se generó un modelo de clasificación para cada sujeto, ya que en experimentos previos se identificó que este logra mayor precisión en comparación con utilizar un modelo generalizado, obtenido con datos de todos los sujetos [15].

3.1. Ensayo 1

El objetivo fue determinar el desempeño de la SVM generando modelos entrenados con las técnicas "Split-Percent" y "Cross-Validation" las cuáles son las más utilizadas. Pare el entrenamiento "Split Percent" se utilizó un 66% de datos para aprender y el 33% restante para clasificar. Para el entrenamiento "Cross Validation", el cual consiste en dividir los datos suministrados a la SVM en *n* particiones y por cada una de ellas, construir el clasificador con las *n-1* partes restantes, e ir probando con cada una de las particiones, donde el valor de *n* de este primer ensayo fue 10. Dado que por defecto WEKA utiliza el Polikernel, decidimos utilizarlo para el primer experimento.

3.2. Ensayo 2

El objetivo de este ensayo fue identificar con cuál de los kernels comúnmente utilizados (Polinomial, Normalized, RBFKernel y PUK) se logra un mejor desempeño de clasificación.

3.3. Ensayo 3

Utilizar Google Glass para inferir inatención del conductor, representa un reto en cuanto al buen uso de la batería, de manera similar que en otros dispositivos vestibles. Similar a otros trabajos [17,18], esto lleva a preguntarnos ¿cuál es el desempeño de la SVM si se limita la cantidad de sensores? Es por esto que el objetivo de este ensayo fue determinar cuál sensor o combinación de sensores entre los disponibles en Google Glass, mejora el desempeño de la SVM para identificar el punto de atención del conductor. En este ensayo se realizaron pruebas de clasificación con datos de un sensor, parejas de sensores y la combinación de todos ellos.

4. Resultados

Dado que el objetivo de realizar estos tres ensayos fue conocer cuáles condiciones permiten obtener una mejor clasificación de los datos; se decidió que las condiciones del modelo que ofreciera un mejor desempeño serían las que se utilizarían en el posterior ensayo. Es decir, la condición del ensayo 1 que arrojó el mejor desempeño, se usó para el ensayo 2, y así sucesivamente.

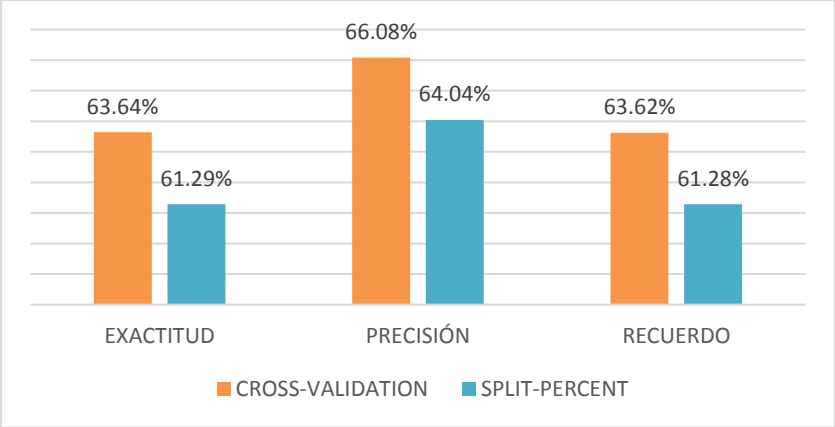


Fig. 2. Comparación del desempeño de la SVM utilizando dos técnicas de entrenamiento.

Tabla 3. Matriz de confusión del sujeto 5 correspondiente al ensayo 1 con la técnica Cross-Validation.

Instancias Correctamente Clasificadas 52.1701 %, Instancias Incorrectamente Clasificadas 47.8299 %, Precisión 0.526, Recuerdo 0.522									
a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**<-- classified as**
224	43	19	0	46	39	0	13	0	a=Pos2
85	136	21	0	43	39	20	40	0	b=Pos5
18	22	120	10	44	84	20	66	0	c=Pos3
0	0	20	240	0	0	80	0	44	d=Pos10
31	11	7	0	288	36	11	0	0	e=Pos1
36	75	36	0	0	179	4	54	0	f=Pos6
0	0	42	118	0	0	213	0	11	g=Pos9
15	73	17	0	0	161	0	118	0	h=Pos8
0	0	0	78	0	6	15	0	285	i=Pos7

4.1. Ensayo 1

Los datos que se muestran en la figura 2 corresponden a los promedios de los resultados de los 5 modelos SVM, correspondientes a los 5 sujetos. Se observa que *Cross-Validation* permitió obtener el mejor desempeño de clasificación (Accuracy=63.64%) comparado con *Split-Percent* (*Accuracy*=61.29%), En consecuencia, para los ensayos posteriores se utilizó esta técnica de entrenamiento.

A manera de ejemplo se muestra la matriz de confusión del sujeto 5 (tabla 3), donde se aprecia que la SVM confundió las posiciones 5 que tiene a confundirla con la posición 6 y la 9 que tiene a confundirla con la posición 10, esto se debe a que la posición 5 y 6 se encuentran muy cerca al igual que las posiciones 9 y 10 (ver figura 1).

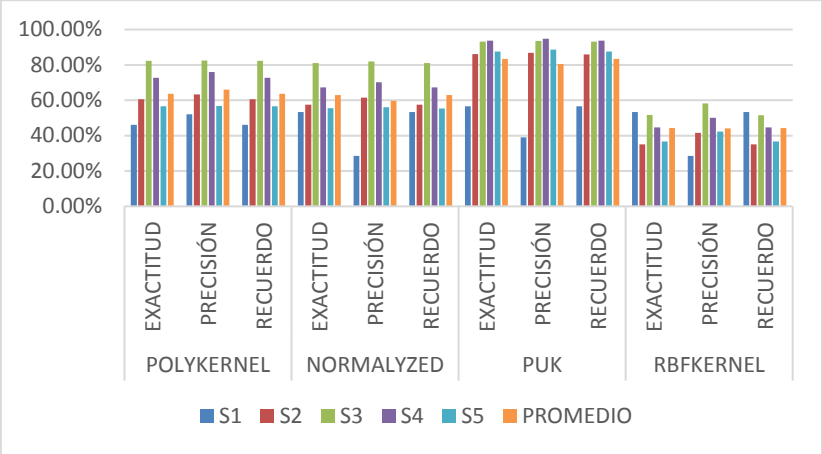


Fig. 3. Comparación de los 4 kernels más comunes.

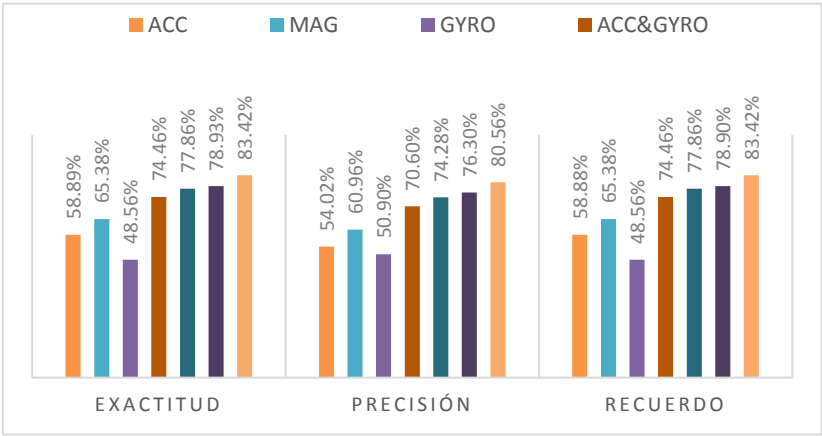


Fig. 4. Desempeño de la SVM usando datos de cada sensor y sus combinaciones.

4.2. Ensayo 2

De la comparación entre los cuatro kernels comúnmente utilizados, obtenemos los siguientes resultados, como podemos ver en la figura 3 el kernel que proporciona una mejor clasificación fue el PUK con un promedio en la exactitud de 83.42%

4.3. Ensayo 3

Los resultados que se muestran a continuación se obtuvieron de la técnica de clasificación Cross-Validation, y el kernel PUK. Como se observa en la figura 4, la mejor

Tabla 4. Matriz de confusión del sujeto 5 correspondiente al ensayo 3 utilizando todos los sensores.

Instancias Correctamente Clasificadas 87.5579 %, Instancias Incorrectamente Clasificadas 12.4421 % , Precisión 0.887 Recuerdo 0.876									
a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**<-clasificado como**
234	30	26	1	35	28	0	30	0	a=Pos2
16	284	9	0	11	32	0	32	0	b=Pos5
4	20	280	0	0	40	0	40	0	c=Pos3
0	0	0	384	0	0	0	0	0	d=Pos10
0	0	0	0	384	0	0	0	0	e=Pos1
0	0	0	0	0	367	0	17	0	f=Pos6
0	0	0	0	0	0	384	0	0	g=Pos9
0	5	0	0	0	33	0	346	0	h=Pos8
0	0	0	0	0	21	0	0	363	i=Pos7

Tabla 5. Comparación con el trabajo más similar al nuestro.

	Nuestro trabajo	**[21]**
Zonas de la cabina	10 clases	6 clases
Técnicas de predicción	SVM	Random Forest
Entrenamiento	10 folds, cross-validation	10 folds, cross-validation
Sujetos	5	7
Desempeño de clasificación	Exactitud=71.1132 %,	Exactitud= 79.4%

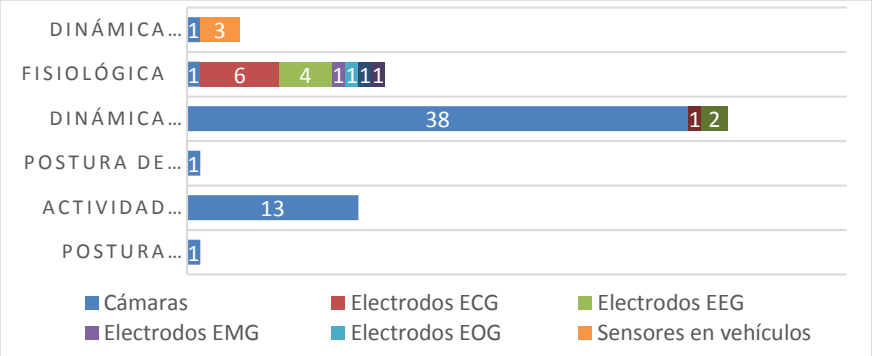


Fig. 5. Tipos de sensores y Enfoque utilizados en los trabajos similares al nuestro.

clasificación se obtiene al utilizar la combinación de los 3 sensores, con una Exactitud promedio de 83.42%. Sin embargo, utilizar solamente los datos del giroscopio y magnetómetro, el porcentaje de instancias correctamente clasificadas es de 78.93%, lo cual sugiere que es una combinación de sensores que podría ser apropiado a utilizar.

Adicionalmente podemos observar en la tabla 4 que se disminuye la confusión de las posiciones 5 con 6 y 9 con 10 en comparación con la tabla 3

5. Comparación con trabajos relacionados

Con el propósito de identificar trabajos similares a nuestro enfoque, recientemente realizamos un mapeo de literatura a partir de la cual obtuvimos 75 trabajos que están enfocados en la predicción de la postura de la cabeza durante la conducción, la figura 5 muestra la cantidad de artículos y los diferentes enfoques que se utilizan para esta predicción. Como se observa en la tabla, son 41 de un total de 75, los trabajos que detectan la postura de la cabeza. De estos 41, solamente se identificaron 2 que exploran el uso de sensores inerciales. El primero presenta resultados preliminares del desempeño del HMM para determinar solamente 7 posturas de la cabeza, con base a la guiñada (yaw), cabeceo (pitch) y alabeo(roll) que no están asociadas a zonas de enfoque particulares de la cabina [19]. El segundo, se limita a proponer detectar los ángulos asociados al giro de la cabeza utilizando solamente un sensor inercial (giroscopio) [20]. Sin embargo, de los 38 artículos que exploran el uso de cámaras para detectar la postura de la cabeza, solo uno propone detectar la orientación de la cabeza con base a las zonas de la cabina [21]. Dada la similitud en cuanto a las variables que se proponen inferir (orientación de la cabeza hacia zonas de la cabina), a continuación, presentamos una comparación de nuestros resultados con respecto a este.

Para poder compararnos realizamos un entrenamiento generalizado, esto es, generar un modelo con base a los datos de todos los usuarios, similar al realizado en [21]. Se puede observar en la tabla que nuestra exactitud es ligeramente menor que la reportada en [21]. Esto podría deberse a que es una menor cantidad de clases y a la poca variabilidad de nuestros datos debido al desbalanceo obtenido durante la recolección.

5.1. Conclusiones

Nuestros resultados muestran que inferir la distracción durante la conducción, basándonos en datos recolectados de sensores inerciales de lentes inteligentes es una solución viable.

Similar a otros trabajos [18], podemos observar que no existe compromiso entre la precisión y el recuerdo al variar las diferentes condiciones de los ensayos. Esto sugiere que en nuestro caso la disposición fija de los sensores (montados en la cabeza), además del movimiento del vehículo no influye en la tendencia de las tres métricas de desempeño.

Los resultados demuestran que el uso de datos crudos (vectores de 9-tuplas) es una opción adecuada para evitar realizar un procesamiento adicional en el Google Glass que detrimente el uso de la batería.

Adicionalmente observamos que el uso de la combinación de dos sensores (gyro y mag), podría ser una opción viable a explorar en futuros experimentos

Se planea realizar experimentos adicionales para obtener una recolección de datos balanceada, para lo cual estamos considerando diseñar un experimento semi-controlado en lugar de realizarlo en condiciones naturalistas.

Agradecimientos. Se agradece a Luis Castro y Jessica Beltrán por su retroalimentación para conducir estos experimentos. Y a los voluntarios que participaron en el estudio.

Referencias

1. Sajan, S., Ray, G. G.: Human Factors in Safe Driving - A Review of Literature on Systems Perspective. Distractions and Errors, Proceedings IEEE Global Humanitarian Technology Conference, pp. 83–88 (2012)
2. Klauer, S. G., Dingus, T. A., Neale, V. L., Sudweeks, J. D., Ramsey, D. J.: The impact of driver inattention on near-crash/crash risk: An analysis using the 100-car naturalistic driving study data. National Highway Traffic Safety Administration, USDOT (2006)
3. Bayly, M., Fildes, B., Regan, M., Young, K.: Review of crash effectiveness of intelligent transport system. Traffic Accident Causation in Europe (TRACE) (2007)
4. Kang, H. B.: Various Approaches for Driver and Driving Behavior Monitoring: A Review. Proceedings IEEE International Conference on Computer Vision Workshops (ICCVW '13), IEEE Computer Society, pp. 616–623 (2013)
5. Tarqui, G., Castro, L. A., Favela, J.: Reducing Drivers' Distractions in Phone-Based Navigation Assistants Using Landmarks. Ubiquitous Computing and Ambient Intelligence, (UCAMI LNCS) 8276, Springer, pp. 342–349 (2013)
6. Chamberlin, J.: Smart glasses: Driver distraction or safety tool?. 45(3), pp. 12, Note available at: http://www.apa.org/monitor/2014/03/smart-glasses.aspx (2014)
7. Zhang, L., Liu, F., Tang, J.: Real-Time System for Driver Fatigue Detection by RGB-D Camera. (ACM), Trans. Intell. Syst. Technol., 6(2), pp. 22 (2015)
8. Murphy-Chutorian, E., Manubhai, M.: Head Pose Estimation and Augmented Reality Tracking: An Integrated System and Evaluation for Monitoring Driver Awareness. IEEE Translate on Intelligent Transportation Systems, 11(2), pp. 300–311(2010)
9. Seeing machines Driver State Sensor: https://www.seeingmachines.com/solutions/
10. Zhang, Y. F., Gao, X. Y., Zhu, J. Y., Zheng, W. L., Lu, B. L.: A novel approach to driving fatigue detection using forehead EOG. Neural Engineering (NER), 7th International IEEE/EMBS Conference, pp. 707–710 (2015)
11. Mohri, M., Rostamizadeh, A., Talwalkar, A.: Foundations of Machine Learning. The MIT Press (2012)
12. Mitchell, T. M.: Machine Learning, 1st. Edition, Mc Graw Hill Higher Education (1997)
13. NHTSA: National Motor Vehicle Crash Causation Study Report to Congress. DOT HS 811 059, National Highway Traffic Safety Administration (2008)
14. WEKA: http://www.cs.waikato.ac.nz/ml/weka/index.html
15. Ordorica, A., Rodríguez, M. D., Castro, L. A., Beltran, J.: Support Vector Machines for Inferring Distracted Behavior of Drivers Wearing Smart Glasses. To be in the Springer Proceedings of Ubiquitous Computing and Ambient Intelligence, (UCAMI) (2016)
16. Michie, D., Spiegelhalter, D. J., Taylor, C. C.: Machine learning, neural and statistical classification (1994)

17. Bulling, A., Blanke, U., Schiele, B.: A tutorial on human activity recognition using body-worn inertial sensors. (ACM) Comput. Surv., 46(3), art. 33, pp. 1–33, DOI:10.1145/2499621 33 (2014)
18. Ozlem-Durmaz, I.: Analysis of movement, orientation and rotation-based sensing for phone placement recognition. Sensors 15(10), pp. 25474–25506, DOI:10.3390/s151025474 (2015)
19. Chuang, C. F., Yang, C. H., Lin, Y. H.: HMM-based driving behavior recognition for in-car control service. IEEE International Conference on Consumer Electronics - Taiwan, pp. 258–259, DOI:10.1109/ICCE-TW.2015.7216886 (2015)
20. Wei-Yao, C., Chung-Hsien, Y., Hsiao-Chien, T., Yi-Chun, L., Chun-Fu, C., Kao-Hung C.: Driver distraction recognition based on dual compass motion sensoring. 17th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp. 1375–1380. DOI: 10.1109/ITSC.2014.6957879 (2014)
21. Tawari, A., Trivedi, M. M.: Robust and continuous estimation of driver gaze zone by dynamic analysis of multiple face videos. IEEE Intelligent Vehicles Symposium Proceedings, Dearborn, pp. 344–349. DOI:10.1109/IVS.2014.6856607 (2014)

ISSN 1870-4069

Estudio de cobertura en anillo para redes de tasa alta

Ashley Meléndez Cano[1], Sergio Alberto Juárez Cazares[1], Edgar Allende Chavez[2], Amit Kumar[1], José Cruz Núñez Pérez[1], Andrés Calvillo Téllez[1]

[1] Instituto Politécnico Nacional, CITEDI, Baja California, México

[2] Instituto Tecnológico de Tijuana, Baja California, México

nunez@citedi.mx, calvillo@citedi.mx, edgar.allende@tectijuana.edu.mx

Resumen. Se presenta el estudio de cobertura de redes de tasa alta donde lo irregular de la topografía del terreno no permite la viabilidad de conexión por fibra óptica y las condiciones climáticas agreden la calidad de radioenlaces de tasa alta. Además, se establecieron 7 radioenlaces maestro-esclavo en arquitectura de anillo en la región de Tijuana, Baja California para la zona este de la ciudad, estimando mediante simulación de radioenlaces por medio del software sugerido airFiberHD24 con frecuencia de operación en banda libre a 24GHz. Se realizó el cálculo de las pérdidas de propagación en el espacio libre, se obtiene la orientación de las antenas, considerando altura de la antena sobre el nivel del mar, margen de desvanecimiento, y el cálculo de su zona de Fresnel, con lo que se garantiza que la señal se encuentre en el rango debido. Finalmente, se propuso el tipo de antena en base a las especificaciones del fabricante.

Palabras clave: cobertura, conectividad inalámbrica, redes de tasa alta.

Study of Ring Coverage for High Rate Networks

Abstract. The study of coverage of high-rate networks is presented where irregular terrain topography does not allow the viability of a fiber optic connection and climatic conditions vanished the quality of high-rate radio links. In addition, seven master-slave radio links were established in a ring topology at Tijuana city, Baja California for the eastern zone of the city, we estimated the simulation of radio links using the suggested software airFiberHD24 with the frequency of operation in a free band at 24GHz. We obtained the estimation of the points of view of the elevation of the antennas, the height over the sea level, the fading margin and the calculation of its Fresnel zone, thereby ensuring that the signal is in the proper range. Finally, the type of antenna was proposed based on the manufacturer specifications.

Keywords: coverage, high rate networks, wireless connectivity.

1. Introducción

1.1. Antecedentes

Con la incorporación de tecnología inalámbrica en casi todos los ámbitos de la vida cotidiana, cada individuo requiere de una demanda de conectividad. Sin embargo, hay zonas alejadas de los logares donde se centraliza el servicio, y en algunos casos no es posible brindar el servicio donde la topografía del terreno lo impide. Debido al incremento en el tráfico de los canales de comunicación por el uso de internet en las redes móviles, y a que el número de consumidores ha aumentado drásticamente en los últimos años; el servicio de los proveedores tiende por obligación a modernizar sus tecnologías para brindar un mejor producto al que presenta la competencia, esto es un incremento en la tasa de usuario, se traduce a mayor velocidad, menor costo e incremento en el alcance y la cobertura. Este es el motivo de utilizar la tecnología que está en el mercado brindando un menor índice de error en la caída de sus señales; disminuir el costo de recursos tecnológicos para competir y otorgar una garantía en los enlaces punto a punto. Este esquema crea mayores ingresos en los prestadores de servicio de interconectividad del servicio y cambia el costo al uso del mismo. Por ello el avance tecnológico requiere de una infraestructura que conecte los sistemas de la ciudad en una misma red para sistemas inalámbricos [1-5].

Este costo radica en todos los insumos que forman parte de la infraestructura que se debe instalar para prestar el servicio a tasas semejantes a las que puede brindar la fibra óptica. El costo se puede estimar en ciudades donde la topografía de ciudades es más o menos plana y se instalan los postes y el tendido de cables. Sin embargo, en ciudades donde la topografía es rugosa, montañosa donde físicamente no es posible el tendido de la fibra, la conectividad inalámbrica a tasas altas es viable, por ello el presente estudio así lo muestra [6-8].

Lo anterior requiere estudios de factibilidad para obtener resultados científicos. Las oportunidades y el potencial en la construcción de infraestructuras de Internet de banda ancha en las zonas. Utilizando tecnología alternativa como Broadband Wireless que utilizan la tecnología de radiofrecuencia. Haciendo observación en las topologías de los diferentes diseños para los enlaces punto a punto, el fabricante hace hincapié que la tecnología airFiber fue diseñada para crear enlaces de alto rendimiento. Este tipo de enlaces debe ser por medio de transporte aéreo por el medio de la fibra y es soportado por diferentes técnicas de duplexado como lo son FDD (Duplexado por división de Frecuencia), TDD (Duplexado por división de tiempo) y HDD (Duplexado por División Hibrido). El fabricante muestra cómo alcanzar la mejor velocidad y la menor latencia dependiendo de las condiciones climáticas, topográficas y rango de alcance del radioenlace [9-16]. La topología que sugiere Ubiquiti Network es la de anillo, por su sencillez para un enlace punto a punto y la redundancia entre enlaces, ya que, si uno de los enlaces se cae, el sistema debe tener la capacidad de encontrar la ruta necesaria para otorgar el servicio.

Esta topología configura un punto como maestro y el otro como esclavo, así genera series de maestros y esclavos para cerrar el círculo del anillo. La Figura 1 muestra la topología de una red anillo.

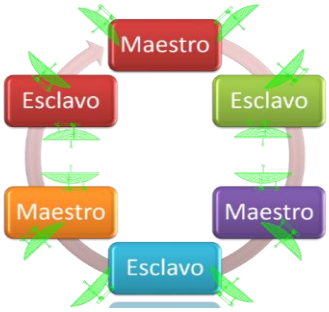


Fig. 1. Topología de anillo redundante.

Fig. 2. Escenario anillo de los enlaces conectados.

Tabla 1. Locación de los enlaces en latitud y longitud.

Headin	**Latitudes**	**Longitudes**
Punto 1	32°28'29.85"	116°53'57.23"
Punto 2	32°29'40.11"	116°56'11"
Punto 3	32°32'4.4"	116°56'50.71"
Punto 4	32°32'56.19"	116°55'4.39"
Punto 5	32°31'52.73"	116°52'19.72"
Punto 6	32°30'16.32"	116°50'1.68"
Punto 7	32°28'11.06"	116°51'21.44"

Este artículo está organizado de la siguiente manera, en la Sección 2 se presenta el desarrollo de cada uno de los siete enlaces del anillo, en la Sección 3 se presenta el perfil de la trayectoria con libramiento y el nivel del margen de desvanecimiento de los radioenlaces.

Tabla 2. Especificaciones de la Antena airFiber.

Parámetros	**Valores**
Fuente de Alimentación	24.05-24.25GHz
Frecuencia de Operación	50V-1.2ª
Dimensiones Radio Box	593 x 768 x 370 mm (23.35 x 30.24 x 14.57") 796 x 696 x 49.5 mm (31.34 x 27.40 x 1.95")
Temperatura de Operación	-40 a 55°C
Rango	20+ Km
Banda ancha del Canal	100 Mhz
Ganancia de Tx	33dBi
Ganancia de Rx	38dBi
Polaridad	Polarización Dual

Tabla 3. Parámetros de los enlaces.

Enlace	1-2	2-3	3-4	4-5	5-6	6-7	7-1
A	4.14	4.57	3.19	3.19	11.19	4.39	4.11
B	-63.89	-64.75	-61.64	-61.64	-72.53	-64.40	-63.83
C	24	24	24	24	24	24	24
D	38	38	38	38	38	38	38
E	100	100	100	100	100	100	100
F	154.03	153.84	154.49	153.79	153.81	153.91	154.03
G	-58.09	-13.06	59.97	65.43	50.36	-28.24	81.86
H	211.90	256.93	329.97	335.43	320.36	241.75	188.13
I	132.29	133.23	130.12	133.49	133.41	132.88	132.28
J	6.95	8.36	3.69	8.75	8.62	7.82	6.93
K	-72.29	-73.23	-70.12	-73.49	-73.41	-72.88	-72.28
L	-59.29	-60.23	-57.12	-60.49	-60.41	-59.88	-59.28
M	1.4755	1.4755	1.4755	1.4755	1.4755	1.4755	1.4755
N	5.8159	5.5085	6.5894	5.4264	6.5894	5.6224	5.8183

2. Desarrollo

En un mapa mostrado en la figura 2, se localizan las coordenadas de aquellos lugares que presenten línea de vista entre sus enlaces, y liberen al menos el 60% la primera zona de Fresnel de tal forma que se cubra la mayor área posible garantizando que se mantendrá la comunicación a tasa alta.

Una vez localizados los sitios potenciales ver tabla 1 se vaciarán los datos del equipo de comunicaciones para obtener un margen aceptable del radioenlace.

Se alimentará al programa con los datos del equipo en especial de la antena AirFiberHD24 haciendo la comparación de ciertos parámetros en el software AirLink con los presupuestos de enlace, tomando las características que otorgan los fabricantes de la antena. Para realizar el presupuesto de enlaces para un escenario de anillo se tomaron en cuenta las latitudes y longitudes de cada una de las locaciones en la región de Tijuana, que se muestran en la Tabla 2 [17].

3. Resultados

A. Distancia entre puntos (Km),
B. Potencia del enlace (dBm),
C. Frecuencia (Ghz),
D. Ganancia de la antena, estación y acceso (dBi),
E. Banda del canal (Mhz),
F. Altura de la antena desde nivel del mar (m),
G. Azimuth punto 1 (°),
H. Azimuth punto 2 (°),
I. Perdidas por espacio (dB),
J. Margen de desvanecimiento (dBm),
K. Nivel de señal recibida Europea (dBm),
L. Nivel de señal recibida Americana (dBm),
M. BW (°),
N. Zona de Fresnel.

Cada enlace presento condiciones especiales debido a que las alturas de los lugares para transmitir superaron el libramiento de obstrucciones de la primera zona de Fresnel, así lo demuestra cada uno de los siete enlaces. Los puntos de transmisión presentaron condiciones de rugosidad en el terreno, finalmente se concretaron cada uno de los radioenlaces, manejando márgenes de desvanecimiento por encima de los 14dB, lo que permite manejar toda la potencia del enlace y superar las inclemencias del tiempo para sostener la tasa alta de la transmisión.

4. Conclusiones

La topografía de la ciudad de Tijuana es del tipo rugosa, serrana, y con cañones, valles y mesetas, que impiden brindar calidad de servicios de telecomunicaciones a altas tasas a la población que los habita, por los altos costos que representan brindar el servicio, o la imposibilidad física del tendido e instalación de infraestructura apropiada.

El software empleado, permitió seleccionar de entre varios puntos aquellos que terminaron definiendo los siete lugares marcados, para conformar el arreglo de anillo. Cada punto del anillo logro la línea de vista sin obstrucción, con la zona despejada, libre de matorrales y construcciones futuras, que impidan el enlace en un futuro.

El margen de desvanecimiento logrado por la potencia de transmisión, las ganancias de las antenas y la sensibilidad del receptor, garantiza que la calidad de la señal no decaiga y se presenten perdidas en el enlace a tasa alta.

Este tipo de enlaces tomo poco tiempo implementarlos, con respecto a los que deben realizar tendido de cables, y la problemática que representa cuando se rompe la fibra.

Referencias

1. Freeman, R. L.: Telecommunication system engineering. John Wiley & Sons (2015)
2. Seybold, J.: Introduction to RF Propagation. John Wiley & Sons (2005)
3. Longley, A. G., Rice, P. L.: Prediction of Tropospheric Radio Transmission Loss Over Irregular Terrain. ESSA Technical Report ERL 79–ITS 67 (1968)
4. Nautel: RF Toolkit Technical Resources (2012)
5. Hata, M.: Empirical Formula for Propagation Loss in Land Mobile Radio Services. IEEE Transactions on Vehicular Technolgy, 29(3), pp. 317–325 (1980)
6. UIT-R: P1238 Recomendación Datos de propagación y métodos de predicción para la planificación de sistemas de radiocomunicaciones en interiores y redes de radiocomunicaciones de área local en la gama de frecuencias de 900 MHz a 100 GHz (2017)
7. COST Telecommunications: Digital Mobile Radio Towards Future Generation Systems-COST 231 Final Report (1999)
8. Walfisch, J., Bertoni, H. L.: A Theoretical Model of UHF Propagation in Urban Environments. IEEE Transactions on Antennas and Propagation, 36(12), pp. 1788–1796 (1988)
9. Recommendation ITU-R P.1406-1: Propagation Effects Relating to Terrestrial Land Mobile and Broadcasting services in the VHF and UHF Bands (2007)
10. Ikegami, F., Yoshida, S., Takeuchi, T., Umehira, M.: Propagation factors controlling mean field strength on urban streets. Antennas and Propagation, IEEE Transactions, 32(8), pp. 822–829 (1984)
11. Sarkar, T. K., Zhong, J., Kyungjung, K., Medouri, A., Salazar-Palma, M.: A survey of various propagation models for mobile communication. Antennas and Propagation Magazine, IEEE, 45(3), pp. 51–82 (2003)
12. Walfisch, J., Bertoni, H. L.: A theoretical model of UHF propagation in urban environments. Antennas and Propagation, IEEE Transactions, 36(12), pp. 1788–1796 (1988)
13. Kozono, S., Watanabe, K.: Influence of Environmental Buildings on UHF Land Mobile Radio Propagation Communications. IEEE Transactions, 25(10), pp. 1133–1143 (1977)
14. Seidel, S.Y., Rappaport, T.S.: 914 MHz path loss prediction models for indoor wireless communications in multifloored buildings. Antennas and Propagation, IEEE Transactions, 40(2), pp. 207–217 (1992)
15. Schantz, H. G., Siwiak, K., Win, M. Z.: A Comprehensive Standardized Model for Ultrawideband Propagation Channels. Antennas and Propagation, IEEE Transactions, 54(11), pp. 3151–3166 (2006)
16. Cichon, D. J., Kürner, T.: COST 231 group final repport: Capítulo 4 Propagation Prediction Models.
17. Data sheets: The airFiber®24 is ideal for outdoor, PtP bridging and carrier-class network backhauls. https://dl.ubnt.com/datasheets/airfiber/airFiber_DS.pdf (2012)

ISSN 1870-4069

Estimación del alcance de radiotransmisores Xbee

José Cruz Núñez Pérez[1], Aldo Bonilla Rodriguez[2], Andrés Calvillo Téllez[1]

[1] Instituto Politécnico Nacional, CITEDI, Baja California, México

[2] Instituto Politécnico Nacional, IPN-UPIITA, Ciudad de México, México

nunez@citedi.mx, calvillo@citedi.mx, aldo.bonilla.r@gmail.com

Resumen. Este artículo trata dos aspectos importantes de la comunicación de redes inalámbricas, el primero estima el máximo alcance del enlace para operar dentro del estándar XBee, en la frecuencia de 2.4 GHz que fija la Potencia Isotrópica Radiada Equivalente a 20 dBm, y el segundo, estima el alcance máximo que se puede obtener. Considerando los parámetros de calidad del enlace como potencia radiada, ganancia de antenas, atenuación por propagación en espacio libre, margen de desvanecimiento y nivel de recepción de la señal. Los resultados obtenidos muestran en la simulación en Matlab la gráfica referente a: la relación que existe entre la suma de Ganancias Vs distancia de propagación y el rango permisible antes de que el nivel de RSSI alcance su valor mínimo de -100dB.

Palabras clave: conectividad inalámbrica, redes de sensores inalámbricos, RSSI.

Estimation of Range of Xbee Radio Transmitters

Abstract. This article treats two important aspects of the communication of wireless networks, the first one estimates the maximum scope of the link to operate inside the standard XBee, in the frequency of 2.4 GHz that fixes the Equivalent Isotropic Radiated Power at 20 dBm, and the second one estimates the maximum scope that can be obtained. Considering the quality parameters of the radiolink to be removed, power, profit of antennas, attenuation for a spread in free space and the margin of faint and level of receipt of the signal. The obtained results show in the simulation in Matlab the graph relating to the relation that exists between the sum of Earnings Vs distances of spread and the maximum range before RSSI's level reaches his minimal value of-100dB.

Keywords: RSSI, wireless connectivity, wireless sensor networks.

1. Introducción

1.1. Antecedentes

Existen un número creciente de servicios y aplicaciones de redes inalámbricas que requieren del uso del espectro electromagnético reservado para las áreas industrial, científica y médica (ISBN, por sus siglas en inglés), que utilizan la banda de frecuencias comprendida entre 2,4 GHz y 2,5 GHz. Los radios XBee hacen uso de esta banda y proporcionan conectividad inalámbrica de punto a punto o multipunto para aplicaciones de redes de malla. Utilizan el protocolo de red IEEE 802.15.4 para dispositivos de corto alcance, están diseñados para aplicaciones de alto rendimiento que requieren baja latencia y tiempo de comunicación predecible. Estos dispositivos, cuentan con dos tipos de radiocomunicación, para enlaces punto a punto o bien enlaces de redes malla; la serie 1, emplea un microchip de Freescale ampliamente usado en radiocomunicación punto a punto y la serie 2 de Ember Networks basadas en la creación de redes de malla bajo el protocolo Zig Bee. Ambos radiotransmisores poseen una gama de potencias de transmisión que depende de la máxima distancia que logre la cobertura. Sin embargo, estos dispositivos, presentan limitaciones en cuanto a que hay pocas opciones de modificación de los parámetros de potencia de transmisión, sensibilidad de recepción, ganancia de transmisión y recepción, por lo que hay que trabajar con estas restricciones.

Con el PIRE fijo a máxima potencia de 20 dBm y ganancias comunes en las antenas de transmisión y recepción de 1.5 dB, estos valores influyen en la restricción de la máxima distancia a la cual pueden comunicarse sin que presente perdidas en los datos. El canal de radio inalámbrico es susceptible a interferencias lo que lo hace un medio de comunicación presente fluctuaciones en la potencia de la señal recibida, que disminuye su fiabilidad en la medida en que se incrementa la distancia y aumenta la taza de transmisión [1-3]. Estas perturbaciones modifican su intensidad durante el día, provocada por los mecanismos de propagación y los fenómenos físicos que afectan a las ondas electromagnéticas, a través de la absorción, reflexión, dispersión y difracción.

Para determinar el alcance de comunicaciones fiables, es necesario interpretar el parámetro de indicador de fuerza de la señal recibida (RSSI, por sus siglas en inglés). La escala que presenta emplea como el valor del alcance (d), referido a una distancia de un metro (d0) y una radiación de un mW, para medir el nivel de potencia recibida por un dispositivo inalámbrico a una distancia (d) expresada en metros. La escala inicia en cero, como punto de radiación de la potencia isotrópica efectivamente radiada centro; representa 0 RSSI, o 0 dBm. Aunque teóricamente puede darse el caso de medirse valores positivos, generalmente la escala se expresa dentro de valores negativos; cuanto más negativo, mayor pérdida de señal [4-8]. La fig.1 se muestra a la señal RSSI como la potencia útil de las ondas de radio, expresado en decibelios donde 0 dB representa la señal PIRE en su máxima intensidad y -120 dB representa la señal cercana al umbral de recepción o el piso de ruido del módulo receptor. Los valores menos negativos representan una señal más limpia o poco corrompida por los mecanismos que imponen los fenómenos físicos de atenuación. Para las comunicaciones inalámbricas de datos, rango normal es de -45 dB a -87 dB. Cualquier

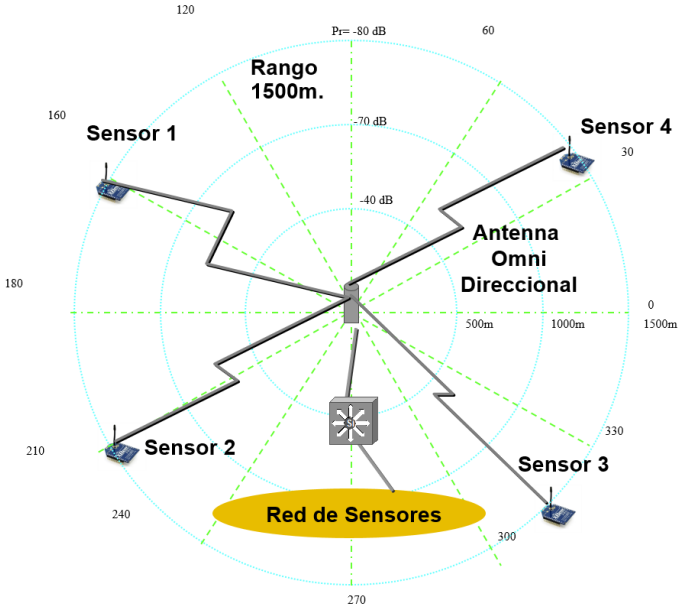


Fig. 1. Rango de la señal, y atenuación respecto al nodo.

Tabla 1. Valores recomendados de RSSI.

Rango de RSSI	**Calidad de la Señal**
Mejor a -40 dB	Excepcional
-40 dB a -55 dB	Muy Bueno
-55 dB a -70 dB	Bueno
-70 dB a -80 dB	Marginal
menores a -80 dB	Intermitente o no operacional

cosa por debajo de -85 dB es generalmente inutilizable, y más de 50 dB puede ser considerado perfecto ver la tabla 1.

2. Desarrollo

Para estimar la distancia de alcance desde que la señal viaja del trasmisor hasta que arriba al receptor. Se analiza la variación de potencia de la señal recibida con respecto a la distancia debido a la disminución de intensidad provocada por los fenómenos físicos que se producen dentro de la trayectoria, causado disipación de la potencia

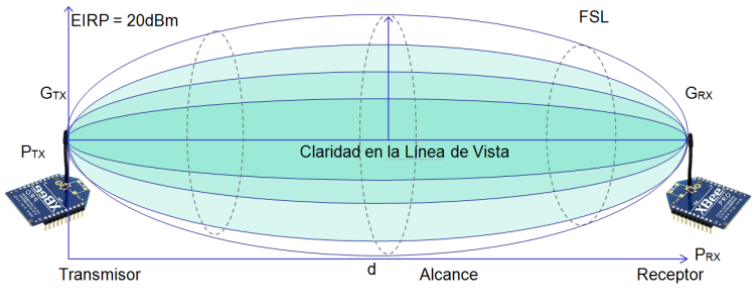


Fig. 2. Parámetros del modelo de Friis.

radiada por el transmisor. En este cálculo se involucran los parámetros que se observan en la figura 2 y cuyo modelo parte de la ecuación de Friis [9-12].

Las ecuaciones de la uno a la ocho relacionan los parámetros de: potencia del transmisor P_{TX} [dBmW], potencia que arriba al receptor P_{RX} [dBmW], después de recorrer la distancia d [m], atenuada por las pérdidas de propagación en el espacio libre PPE [dB], y las ganancias de la antena transmisora G_{TX} [dB] y receptora G_{RX} [dB].

La estimación de la distancia entre los nodos se obtiene a partir de la intensidad de la potencia de la señal recibida que arriba a la antena del módulo receptor:

$$PPE = 10\log\left(\frac{4\pi\times10^{12}}{3\times10^{8}}\right) + 20\log d_{km} + 20\log f_{GHz}. \quad (1)$$

PPE_{dB} = Perdidas por Propagación en el Espacio en dB.

d_{km} = Distancia del enlace en *km*.

f_{GHz} = Frecuencia de operación en *GHz*.

$$PIRE = P_{Tx} - L_{LT} + G_{Tx}. \quad (2)$$

$PIRE_{dB}$ = Potencia Isotrópica Radiada Equivalente en dB.

P_{Tx} = Potencia de transmisión en dB,

G_{Rx} = Ganancia de la antena de recepción,

L_{LT} = Perdida por conector y por línea de transmisión en dB.

$$NRS = PIRE - PPE + G_{Rx} - L_{LR}. \quad (3)$$

NRS = Nivel de Recepción de la Señal en dB,

G_{Rx} = Ganancia de la antena receptora,

L_{LR} = Perdida por conector y por línea de receptor en dB.

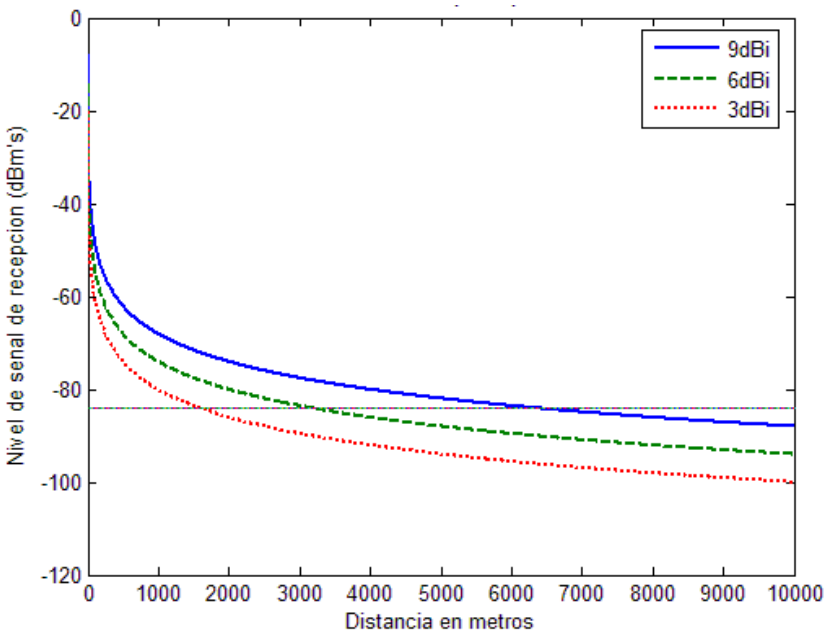


Fig. 3. Relación Distancia vs. Nivel de recepción para frecuencia de 2.4 GHz.

$$M = S - NRS\,. \tag{4}$$

M = Margen de desvanecimiento de la Señal,
S = Ganancia de la antena receptora.

$$RSSI = 10log\left(\frac{NRS}{P_{Ref}}\right). \tag{5}$$

NRS = Nivel de Recepción de la Señal en mW,
P_{Ref} = 1 mW.

$$RSSI = NRS - 10\log(1mW). \tag{6}$$

NRS = Nivel de Recepción de la Señal en dB:

$$P_{Rx} = RSSI + MDP_{Rx_{Superior}} \quad si\ RSSI > 0. \tag{7}$$

MDP_{Rx} = Margen Dorado de la potencia de Recepción:

$$P_{Rx} = RSSI + MDP_{Rx_{Inferior}} \quad si\ RSSI < 0. \tag{8}$$

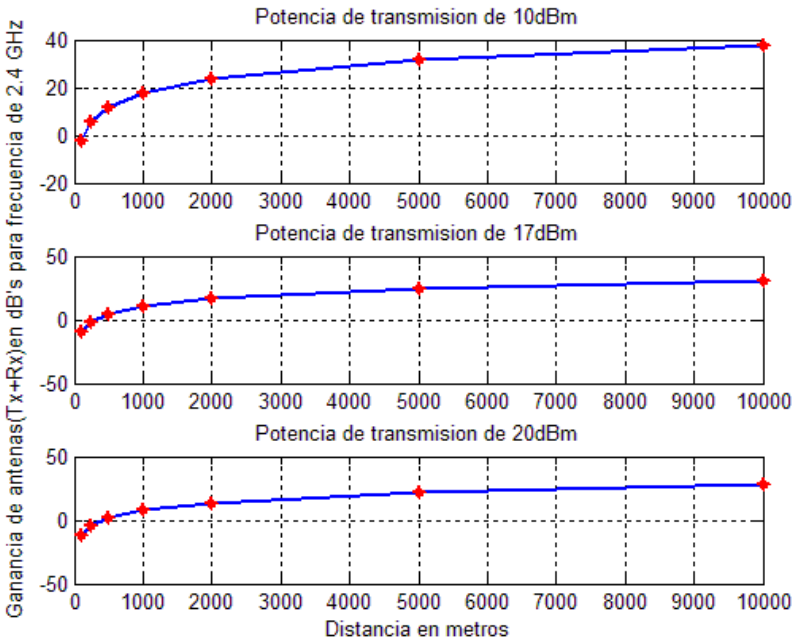


Fig. 4. Relación Distancia vs. Nivel de recepción para frecuencia de 2.4 GHz.

Tabla 2. Valores Medidos de RSSI.

Latitud	Longitud	Descripción	Paquetes 0K	RSSI
32^0 32" 47'	117^0 05" 4'	30m	99%	-42 dBm
32^0 32" 47'	117^0 05" 2'	100m	99%	-64 dBm
32^0 32" 47'	117^0 04" 55'	300m	99%	-80 dBm
32^0 32" 47'	117^0 04" 49'	500m	98%	-94 dBm
32^0 32" 47'	117^0 04" 39'	800m	0%	-
32^0 32" 47'	117^0 04" 33'	1000m	0%	-
32^0 32" 47'	117^0 04" 27'	1200m	0%	-
32^0 32" 47'	117^0 04" 17'	1500m	0%	-

$$MDP_{Rx_{Inferior}} < P_{Rx} + MDP_{Rx_{Superior}} \quad si\ RSSI = 0. \tag{9}$$

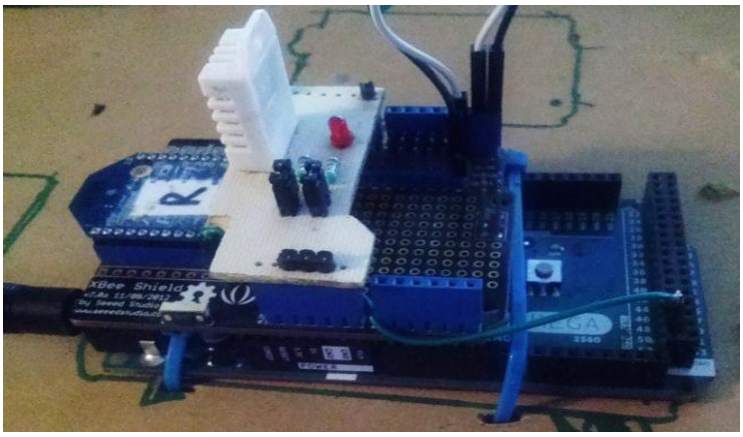


Fig. 5. Módulo de la red de sensores inalámbrica.

3. Resultados

Los resultados obtenidos del rango que puede lograr un módulo Xbee en la frecuencia libre de 2.4 GHz, empleando la potencia de radiación presente en la antena se fijó a PIRE = 20 dBm. A partir del EIRP los alcances máximos se logran con dos elementos el primero lo define el arreglo de antenas para transmitir y recibir [13]; el segundo mediante el análisis de las simulaciones presentadas en las gráficas de las fig. 3 y fig. 4, las cuales muestran las curvas de máximo alcance. Por lo que el elemento de mayor importancia es el umbral de recepción. En la fig. 3 la línea puntuada nos muestra la sensibilidad del receptor XBee, y las demás líneas muestran que teóricamente con una antena de 3dB se alcanzaría un rango cercano a los 100 metros, siempre y cuando esté libre de obstáculos, así una antena de 6 dB teóricamente alcanzaría los 3000 metros, y una de 9 dB, puede alcanzar los 6000 metros.

En la fig. 4 se puede observar que para una potencia de transmisión de 10dBm el rango máximo depende del factor G_{Tx} y G_{Rx} para un par de antenas con ganancia de 1 dB, la primera marca distancia máxima de separación entre antenas de es de 10m la segunda marca indica 10m a 1.3dB la de 100m, requiere de antenas de 9dB, y para la marca de 5000m se requiere de una ganancia conjunta cercana a los 36dB; si las antenas son semejantes para este enlace se tiene que las ganancias de dichas antenas son de $G_{Tx}=G_{Rx}=$ 18 dB. Y para esta marca de 5000m la potencia de transmisión de 17 dBm y 20 dBm se requiere de antenas de 15 dB y 12 dB [14-17].

4. Conclusiones

Para mantener la comunicación de los nodos en un nivel sin pérdidas de datos, la señal de recepción debe alcanzar valores que no decaigan más allá de los -70dBm.

En la medida que se incremente la distancia, la señal recibida disminuye. Si se mejora el sistema de ganancia permitirá mejorar el margen de seguridad del radioenlace. La imagen 3 presenta las máximas distancias que se pueden obtener mediante la ganancia conjunta de las antenas de transmisión y recepción. Es necesario considerar esta ganancia debido a que no siempre se puede obtener el máximo alcance, cuando no se considera esta ganancia es probable que se entre en la violación de la norma pues si consideramos una ganancia superior a 20dBm, ya se está rebasando la recomendación de la norma y se estarán infringiendo las regulaciones de enlaces inalámbricos en banda libre.

Las mediciones permitieron corroborar cómo el RSSI cambia a lo largo de la distancia, las lecturas de la potencia de recepción estuvieron dentro de margen dorado de la potencia de recepción hasta -50 dBm, sin embargo, los valores cercanos al margen dorado de la potencia de recepción inferior, hacían al enlace inestable y con pérdida de datos y por el contrario las lecturas cercanas al margen dorado de la potencia de recepción superior presentaban un enlace robusto.

Referencias

1. Freeman, R. L.: Telecommunication system engineering. John Wiley & Sons (2015)
2. Callaway, E. H.: Wireless Sensor Networks. Segunda ed., USA, Prentice Hall (2013)
3. Dorottya, V., Zoltán, V., Rolland, V., Attila, V.: Energy Efficiency in Wireless Sensor Networks Using Mobile Base Station. IFIP International Federation for Information Processing, 196, pp. 173–186 (2006)
4. XBee: XBee-PRO OEM RF Module Antenna Considerations. Application Note XST-AN019, http://ftp1.digi.com/support/images/XST-AN019a_XBeeAntennas.pdf (2015)
5. Freeman, R. L.: Radio System Design for Telecommunications, Wiley & Sons, (2006)
6. Parson, J. D.: The Mobile Radio Propagation Channel, Wiley & Sons (1992)
7. Doble, J.: Introduction to Radio Propagation for Fixed and Mobile. Artech House (1996)
8. Bertoni, H. L., et al.: UHF Propagation Prediction for Wireless Personal Communications. Proceedings of the IEEE, 82(9), pp. 1333–1359 (1994)
9. Andersen, J. B., Rappaport, T. S., Yoshida, S.: Propagation Measurements and Models for Wireless Communications Channels. IEEE Communications Magazine, pp. 42–49 (1995)
10. Lee, W. C. Y.: Mobile Communications Design Fundamentals. Second Edition, Wiley & Sons (1993)
11. CCIR (now ITU-R): Propagation data and prediction methods for the terrestrial land mobile service using the frequency range 30 MHz to 3 GHz. Report 567–4, International Telecommunication Union (1990)
12. Gschwender, A.: ZigBee Wireless Sensor and Control Network. Prentice Hall (2009)
13. Figueroa, T. C., Medina, M. J. L., Chávez, P. R. A., Calvillo, T. A.: Circular monopole antenna with defected ground plane for UWB applications. Research in Computing Science, 64, pp. 207–214 (2014)
14. Agrawal, S., Singh, S.: Indoor Localization based on Bluetooth Technology: A Brief Review. International Journal of Computer Applications, ISO 690, 97(8), pp. 31–33 (2014)
15. Gharghan, S. K., Nordin, R., Ismail, M.: Energy-efficient ZigBee-based wireless sensor network for track bicycle performance monitoring. Sensors, ISO 690, 14(8), pp. 15573–15592 (2014)

ISSN 1870-4069

Diseño de un sistema de comunicaciones en tiempo real en la web y su escalabilidad en la nube para consultas y seguimiento médico

José Vargas-Huamán, Kevin Quispe-Huaman, Eduardo Sutta-Gonzales, Amarilis Tipo-Parillo, Pedro Yanque-Churo, José Sulla-Torres

Escuela Profesional de Ingeniería de Sistemas,
Universidad Nacional de San Agustín, Arequipa,
Perú

{josemvargh, kevinxpt27, laloeasg, amarilis.sussan, yanque.sis}@gmail.com,
jsulla@unsa.edu.pe

Resumen. En este artículo, se elabora un sistema de comunicaciones en tiempo real en la web con infraestructura en PubNub para las consultas y seguimiento médico por videoconferencias. El modelo se compone de dos etapas, la primera de ella es la generación de la comunicación por WebRTC y la segunda consiste en la configuración de la IaaS (Infrastructure as a Service) de PubNub y su puesta en marcha. Para evaluar el rendimiento de la aplicación se realizaron pruebas sobre usuarios en entornos de atención, obteniendo como resultado una confiabilidad del 80% sobre cinco sesiones de dos participantes cada uno. Los resultados muestran que la posibilidad de comunicarse entre los usuarios paciente-doctor fortalecen y facilitan el seguimiento de un tratamiento.

Palabras clave: WebRTC, IaaS, WebSocket, videoconferencia, PubNub.

Design of a Real-Time Communication System on the Web and its Scalability in the Cloud for Consultations and Medical Follow-Up

Abstract. In this paper, a real-time web communications system with PubNub infrastructure for consultation and medical follow-up by videoconferencing is developed. The model consists of two stages, the first of which is the generation of communication by WebRTC and the second consists of the configuration of the IaaS (Infrastructure as a Service), of PubNub and its implementation. To evaluate application performance, users were tested in care settings, resulting in 80% reliability over five sessions of two participants each. The results show that

the possibility of communicating between patient-doctor users strengthens and facilitates the follow-up of a treatment.

Keywords: WebRTC, IaaS, WebSocket, videoconference, PubNub.

1. Introducción

En los países en vía de desarrollo existe el problema relacionados con el cumplimiento o seguimiento por parte de los pacientes al tratamiento médico asignado [1]. El sistema habitual de los servicios de atención médica es a través de una interconsulta médica [2], que es cerca de 65,9 millones de atenciones por el seguro integral de salud de Perú [3]. La adecuada y oportuna atención del paciente es un factor determinante para su desarrollo [4], por lo que es sumamente importante su seguimiento y monitorización [5].

Una alternativa son los sistemas de videoconferencia, pero estos a menudo son demasiados costosos de comprar y mantener [6]. La evolución de la web nos presenta innovaciones sorprendentes y nuevas creaciones, cosa que ni siquiera imaginábamos o de plano no pensamos iban a existir. [7] La Comunicación en tiempo real para la web o WebRTC es una nueva tecnología que abre más posibilidades en nuestras aplicaciones. El desarrollo tecnológico se va incorporando a diversas situaciones, como el de un doctor y su paciente en las que las personas no disponen de tiempo, movilidad, o tienen problemas crónicos que les impide el acercamiento a una consulta, permitiendo una nueva generación de aplicaciones de Tele-salud [8]. De esta manera, tanto las plataformas online como la videoconferencia hacen posible el control, el establecimiento de diagnóstico y sus pautas terapéuticas. Al acoplar las capacidades de comunicación en tiempo real de WebRTC y las ventajas que aporta la Web of Things (WoT), se introduce el diseño de una nueva arquitectura sanitaria flexible, con el fin de proponer diversos servicios de e-salud [9], como una plataforma *web responsive* de telemedicina con videoconferencia para el seguimiento de pacientes [10], así como para módulos de videoconferencia a través de WebRTC para una plataforma de telemedicina [11].

La llamada WebRTC [12], permite utilizar HTML5 y APIs de JavaScript para crear aplicaciones que nos permitan comunicarnos vía Audio o Video, la idea es que no se necesite instalar *plugins*, para poder utilizar la tecnología. WebRTC proporciona acceso mediante programación a un vídeo en directo desde la webcam del usuario. También permite realizar conexiones punto a punto para audio y video de manera eficiente, sin embargo, para la conexión se hará uso de una infraestructura como servicio o IaaS (Infrastructure as a Service) [13].

PubNub es una red global de transmisión de dato [14]. El producto principal de PubNub es una API de mensajería publicar/suscribir en tiempo real construida sobre su red de flujo de datos global, que está compuesta por una red replicada de al menos 14 centros de datos ubicados en América del Norte, América del Sur, Europa y Asia.

La red actualmente sirve a más de 300 millones de dispositivos y transmite más de 750 mil millones de mensajes por mes, por lo que resultaría una buena opción en la implementación de la herramienta.

Como objetivo de este artículo, se ha planteado un modelo de sistema que utiliza técnicas modernas para la comunicación en tiempo real como son WebRTC y PubNub, diseñado bajo una arquitectura orientada al Cloud que provee escalabilidad para las consultas y seguimiento médico, de esta manera podrá ser una alternativa más económica y adecuada para el seguimiento médico de pacientes.

El modelo consta de dos etapas diferenciadas la primera de ellas es la generación de la comunicación por WebRTC y la segunda consiste en la configuración de la IaaS y su puesta en marcha.

A continuación, se da a conocer el estado del arte de sistemas de comunicación en tiempo real y otros trabajos tomados en cuenta en la realización de este artículo. En segundo lugar, se detalla la metodología, así como las técnicas y herramientas utilizadas para la realización de la aplicación y su evaluación. Finalmente se muestran los resultados, las conclusiones a las que se llegaron y los trabajos futuros de la investigación.

2. Trabajos relacionados

Se presenta algunos trabajos en la misma rama que anteceden este artículo.

2.1. Servicio de videoconferencia basado en WebRTC para telesalud

Este articulo desarrollado por Jang-Jaccard [6], realiza un estudio sobre los sistemas de videoconferencia existentes que se utilizan a menudo en los servicios de telesalud donde se han criticado por varias razones: (a) a menudo son demasiado costosos de comprar y mantener, (b) usan tecnologías propietarias que son incompatibles entre sí, y (c) requieren personal de TI bastante capacitado para mantener el sistema. Por lo que existe la necesidad de un sistema de videoconferencia menos costoso, compatible y fácil de usar. La comunicación web en tiempo real (WebRTC), promete ofrecer una solución al permitir navegadores web con capacidades de comunicación en tiempo real a través de API de JavaScript simples. Utilizando WebRTC, los usuarios pueden realizar llamadas de audio y video para compartir los datos a través de navegadores web sin tener que comprar o descargar software adicional.

Aunque es prometedora la perspectiva de WebRTC, no ha habido muchos casos de aplicaciones de la vida real (en particular en telesalud), que utiliza WebRTC. Jang-Jaccard presenta una experiencia práctica en el diseño y la implementación de un sistema de videoconferencia para telesalud basado en WebRTC. El sistema de videoconferencia es parte de un gran proyecto de monitoreo a distancia que se lleva a cabo en seis ubicaciones en cinco estados diferentes de Australia.

Uno de los objetivos del proyecto es evaluar si los servicios de telesalud habilitados con un alto ancho de banda, que se brindan a través de la monitorización a distancia del hogar, pueden ser rentables y mejorar los resultados en la atención de salud. Sin embargo, en este documento se centra en el sistema de videoconferencia basado en WebRTC que permite reuniones en línea entre coordinadores de atención remotamente ubicados y los pacientes en su hogar.

2.2. Solución innovadora de WebRTC para servicios de e-Health

En el trabajo de Paola Pierloni [15], presenta un estudio sobre las soluciones y servicios para e-Health y la telemedicina en el área de la salud gracias a las últimas innovaciones en electrónica, informática y telecomunicaciones. Este trabajo propone un servicio innovador para la e-Health orientada a la máxima facilidad de uso y al intercambio de signos vitales. La propuesta consiste en un servicio de teleconferencia basado en la tecnología WebRTC que permite a cualquier persona que reside de forma remota del personal médico o del hospital interactuar directamente con ellos. La solución proporciona todas las funciones comunes de WebRTC, como secuencias de video y audio en tiempo real, mensajería instantánea y uso compartido de archivos con el único requisito de un navegador web tradicional.

Más allá de eso, se implementa la transmisión y visualización en tiempo real de signos vitales y parámetros adquiridos por sensores biomédicos conectados al dispositivo personal del paciente a través del RTCDataChannel. Actualmente, la solución implica la instalación de una extensión de navegador, pero esta operación es muy simple y puede evitarse cuando las API y navegadores WebRTC admitan secuencias de medios provenientes de sensores de la misma manera que las transmisiones de audio y video. La solución demuestra cómo las tecnologías web se pueden aplicar en el sector de la salud, proporcionando servicios muy eficaces a pacientes y usuarios que por diversas razones tienen dificultades para viajar a los hospitales con el fin de recibir asistencia médica.

2.3. WebRTC: entrega de telesalud en el navegador

Arin Sime [8], explica como WebRTC está habilitando una nueva generación de aplicaciones de Telesalud y será una parte importante del futuro de Telesalud. WebRTC permite que las aplicaciones web controlen el micrófono y la cámara de video del usuario desde el navegador. En este punto de vista, el autor presenta los pros y los contras de WebRTC para aplicaciones de telesalud.

La telesalud es una parte del cuidado de la salud en rápida expansión a nivel mundial, con el potencial de ahorrar costos y servir mejor a los pacientes con atención especializada, sin importar dónde viven.

Un desafío final a tener en cuenta con WebRTC es que puede ser difícil establecer una llamada con éxito detrás de algunas redes de hospitales. Si su hospital tiene una política de seguridad de red muy restrictiva, puede ser difícil que dos navegadores web que usan WebRTC establezcan la conexión P2P necesaria para realizar una llamada.

2.4. Telemedicina para la gestión de emergencias mediante WebRTC.

Con el rápido avance y desarrollo en el campo de las comunicaciones en tiempo real, la telemedicina ha alcanzado grandes alturas y ha ayudado a salvar millones de vidas durante situaciones de emergencia. [16] El uso de la telemedicina es de larga data, pero

su aplicación en la gestión de atención de emergencia está todavía en su etapa de desarrollo.

En la actualidad hay varios sistemas de telemedicina de emergencia disponibles en el mercado que utiliza la electrónica del vehículo hasta la fecha, la última tecnología de telecomunicaciones y software especializado. Sin embargo, estos sistemas son altamente sofisticados, voluminosos y caros y son empleados por muy pocos centros de salud. Por lo tanto, estos servicios salvavidas no están disponibles para gran parte de la población, especialmente los que viven en las zonas rurales. El objetivo de este trabajo es presentar una nueva idea en la que estos servicios *Tele Emergency* puedan ser implementados de una manera mucho más eficiente, económica y menos sofisticada, para que estos servicios puedan ser ampliamente proporcionados. Aquí proponemos una nueva aplicación de Telemedicina de emergencia para la gestión de atención de emergencia que utiliza WebRTC para la comunicación en tiempo real. Este sistema sólo requiere un dispositivo móvil con conexión a Internet con Chrome o Mozilla instalado en él. El dispositivo se transporta dentro de la ambulancia para llevar a cabo una evaluación inicial del paciente y luego se lleva al centro de salud más cercano donde se lleva a cabo el tratamiento adicional con la ayuda de especialistas cuya telepresencia es proporcionada por dispositivos habilitados para WebRTC.

2.5. Arquitectura de cuidado de la salud inteligente usando WebRTC y WoT

Saad El Jaouhari [9], presenta el diseño de una nueva arquitectura de salud flexible, para proponer diversos servicios de salud electrónica al unir las capacidades de comunicación en tiempo real de WebRTC y las ventajas traídas por la *Web of Things* (WoT), En este trabajo se centran principalmente en los servicios relacionados con la atención médica remota de pacientes y personas mayores. Presenta la arquitectura a través del análisis de tres casos de uso principales: un monitoreo remoto y continuo de personas mayores y un examen médico remoto de pacientes e intervención de emergencia en caso de un accidente.

2.6. Revisión a la aplicación de cloud computing en p2p video streaming

La computación en nube se ha introducido como una solución a varios problemas del tradicional sistema de e-learning basado en la web, tales como un almacenamiento limitado, un elevado coste de mantenimiento de la infraestructura y una baja interoperabilidad entre el componente de aprendizaje electrónico basado en un sistema web. Sin embargo, el rendimiento del sistema de computación en nube puede deteriorarse con el aumento del número de usuarios y empeorar cuando muchos usuarios acceden a la trasmisión de video desde el sistema en la nube. Esto se debe a la arquitectura centralizada de la nube que puede generar congestión de tráfico de red y cuello de botella en los servidores de la nube.

Se ha propuesto la arquitectura *peer to peer* para superar este problema. Utilizando P2P todos los nodos del sistema de nube pueden actuar tanto como servidores como clientes al mismo tiempo para reducir la congestión y el cuello de botella del sistema.

En la actualidad, hay pocas revisiones en *streaming* de vídeo P2P, aunque se han realizado estudios intensivos sobre el desarrollo del sistema.

Con esta condición, la identificación y la comprensión del desarrollo de la transmisión de vídeo P2P será costosa, requiere mucho tiempo y físicamente agotador.

El objetivo de este documento es revisar el último desarrollo de *streaming* de vídeo P2P basado en *cloud computing*. Un método de revisión narrativa se ha utilizado como la metodología para investigar los artículos de *streaming* de vídeo P2P de 2009 a 2014. Los resultados de esta investigación muestran que el 90% de *e-learning* basado en la nube se integran con P2P cuando se trata de *streaming* de vídeo.

3. Metodología

3.1. Técnicas y herramientas

WebRTC. WebRTC [17] es un estándar en desarrollo por el Internet Engineering Task Force (IETF) y el World Wide Web Consortium (W3C) que pretende definir un framework, protocolos e interfaces de programación que proveerán comunicaciones interactivas y en tiempo real de audio, video y datos a las aplicaciones en los navegadores web.

Los APIs de los que consta el protocolo son los siguientes:

- *GetUserMedia*: se utiliza para acceder a los recursos multimedia del usuario como su cámara o su micrófono. El resultado será un *MediaStream*.
- *MediaStream*: es un conjunto de pistas de flujos de audio o vídeo con los recursos multimedia del usuario.
- *RTCPeerConnection*: representa un canal de conexión con otro cliente. Un cliente añade a un *RTCPeerConnection* uno o más *MediaStreams* para compartirlos con el otro cliente.

Cloud computing. Es un modelo para proveer acceso bajo demanda a recursos de computación como redes, servidores, almacenamiento, aplicaciones y servicios de forma configurable y a través de la red [18].

Las características del modelo de Cloud Computing son las siguientes:

- *On-demand self-service:* Los usuarios pueden disponer de capacidades de computación (CPU, ancho de banda, almacenamiento, etc.) según lo necesiten.
- *Broad network access:* Estas capacidades están disponibles en la red en diferentes posiciones y son servidas a través de mecanismos estándar.
- *Resource pooling:* El Cloud sigue un modelo *multi-tenant* por el cual pueden asignarse recursos a diferentes usuarios.

PubNub. Es una red global de transmisión de datos (DSN) y una compañía de infraestructura en tiempo real (IaaS), el producto principal de PubNub es una API de mensajería para publicar y/o suscribir en tiempo real, construida sobre su red de flujo de datos global.

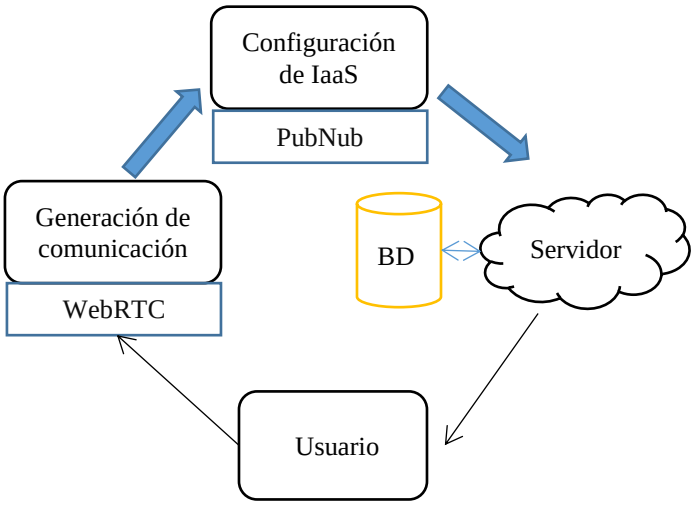


Fig. 1. Diseño propuesto de comunicación en tiempo real.

La mensajería proporciona *streaming* de datos en tiempo real y señalización de dispositivos, e incluye cifrado AES incorporado y cifrado TLS / SSL opcional.

Los componentes atómicos que componen un flujo de datos son Claves API, Mensajes y Canales.

WebSocket (BackEnd PubNub). La parte del desarrollo e implementación del WebSocket es una parte fundamental del proyecto para que los usuarios puedan comunicarse entre ellos y enviar y recibir información de forma transparente.

PubNub le ofrece el soporte completo de RFC 6455 para HTML5 WebSocket Client Specification. PubNub WebSockets permite que cualquier navegador (moderno o no) soporte las API estándar de HTML5 WebSocket.

3.2. Análisis del sistema

El sistema se ha desarrollado con la tecnología WebRTC ya que ofrece las herramientas necesarias y un API en lenguaje JavaScript fácil de utilizar y programar para este propósito. Las tecnologías utilizadas en la Sala Principal donde los usuarios se conectan y realizan llamadas entre ellos, se ha optado por utilizar en el servidor un *servlet* y un *websocket*, y en el lado del cliente JavaScript, HTML5 y CSS para renderizar la interfaz y enviar/recibir datos.

Los lenguajes de programación y tecnologías que utiliza esta aplicación son:

- En el lado del cliente (FrontEnd): HTML5, JavaScript (WebSocket), CSS, WebRTC.
- En el lado del servidor (BackEnd): Java, WebSocket, NodeJS, PubNub.
- En la base de datos: mongoDB.

3.3. Diseño del software

Modelo cliente-servidor. El sistema está basado en una arquitectura cliente-servidor, (véase la figura 1).

Los aspectos novedosos e importantes del diseño propuesto son la integración de las diferentes tecnologías que permitan la monitorización y consultas en los pacientes para una atención médica y que no existe en la mayoría de los servicios de salud en el Perú.

3.4. Implementación del proyecto

El desarrollo de la aplicación se ha realizado en MongoDb, ExpressJS, AngularJS, NodeJS. También es conocido como Stack MEAN, que nos permite el desarrollo de aplicaciones, y páginas web dinámicas, que están basadas cada una de estas en JavaScript. A esto se agregó las librerías WebRTC y PubNub, que también están desarrollas en JavaScript. Gracias a esta característica, la integración de estas librerías y *frameworks*, el sistema resulto exitosamente auto-suficiente.

En la figura 1, se muestra el diagrama de funcionamiento del sistema. Que se compone de Usuario, servidor y base de datos. En la Base de datos se almacena información de suscripción del usuario, en la que se encripta los datos confidenciales del usuario, en este caso solo contraseña. El servicio de alojamiento de base de datos en la nube que hemos utilizado es MongoLab, que una vez creada la base de datos nos provee una cadena de conexión con nuestra base de datos.

En el Servidor que se muestra en la figura 1, se desarrolló la autentificación de usuarios. El Cliente (Navegador web) envía información de validación de usuario al servidor, este obtiene la información de la base de datos y envía 3 cadenas de caracteres separados por un punto, conocido como Json Web Token (JWT). Es por medio de esto que se realiza la seguridad en cliente/servidor. El servicio de alojamiento en la nube que hemos utilizado es Heroku, ya que nos provee de servicio de seguridad SSL para la ejecución de las librerías WebRTC y PubNub, además provee seguridad en la conexión con la base de datos, a través de la configuración de variables de entorno.

En el lado de Cliente (navegador), *AngularJS* se complementa perfectamente con WebRTC y PunNub, para realizar la conexión y comunicación peer-to-peer entre dos usuarios. Para Ello las librerías nos especifica crear una variable PHONE (teléfono), en la que pondremos: un número, que se será *username* de usuario; una clave pública y una clave de suscripción, que no provee PubNub; y por último se activa el certificado de seguridad SSL, sin esto no funciona la aplicación. Posteriormente se implementa las funciones de *phone.dial, phone.receive, session.connected*, entre otras.

De esta forma explicamos, de forma general, el funcionamiento del sistema. Hay muchas cosas más que se necesitan explicar sobre lo que realiza por dentro, en su código, PubNub y WebRTC, pero hay que entender una solo una cosa, que estas librerías nos ofrecen una abstracción para realizar una comunicación peer-to-peer. Que muy en el fondo estas librerías están haciendo uso de *websockets* para crear una red de comunicación punto a punto entre dos usuarios como se muestra en la figura 2.

Tabla 1. Parámetros configuración WebRTC

Componente	Parámetros	Descripción
HTML5	<video>	Para reproducir y capturar vídeo de la cámara y mostrarlo en pantalla.
	<canvas>	Para crear imágenes o renderizaciones dinámicas.
JavaScript	XMLHttpRequest	Para obtener información de una URL sin tener que recargar la página completa.
	JSON	Para intercambio de datos.
WebSocket PubNub	onopen()	Método que se ejecuta cuando el websocket se abre por un cliente.
	send()	Método que envía un mensaje por el websocket.
	onmessage()	Método que se ejecuta cuando se recibe un mensaje
	onclose()	Método que se ejecuta cuando se cierra el websocket.
	onerror()	Método que se ejecuta cuando se produce un error en el websocket.
	Publish / .Subscribe	PubNub proporciona una manera fácil de publicar datos en tiempo real, ya sea dispositivos individuales o grupos grandes de ellos.
	Presence	Da visibilidad en tiempo real de quién está suscrito en un "canal"
	Storage / Playback	Registra flujos de datos y proporciona acceso instantáneo y consultas en datos que se publicaron en el pasado
	Analytics	Obtiene opiniones en tiempo real y en tiempo real sobre el tráfico y el uso en tiempo real
	Security	Agrega cifrado AES a tiempo real, así como un marco de concesión / revocación completa para garantizar que sólo los usuarios autorizados puedan suscribirse

3.5. Configuración WebRTC y Pubnub

Al ejecutar los diferentes módulos que hacen falta para el funcionamiento de un servicio basado en WebRTC y PubNub y que se han explicado en la arquitectura son necesarios algunos parámetros de configuración. Estos parámetros son utilizados por los diferentes módulos para establecer algunas configuraciones en sus componentes.

En la Tabla 1, pueden observarse estos parámetros junto con una pequeña descripción de su funcionalidad.

4. Resultados y pruebas

A continuación, se explica un ejemplo de las pruebas del sistema realizado en el marco de esta investigación y utilizando la unidad de control en una máquina con características similares a la *t2 medium*, del proveedor Amazon EC2 (Procesador de 4 núcleos y 4gb de *RAM*). Se han diseñado tres escenarios que son los más comunes en

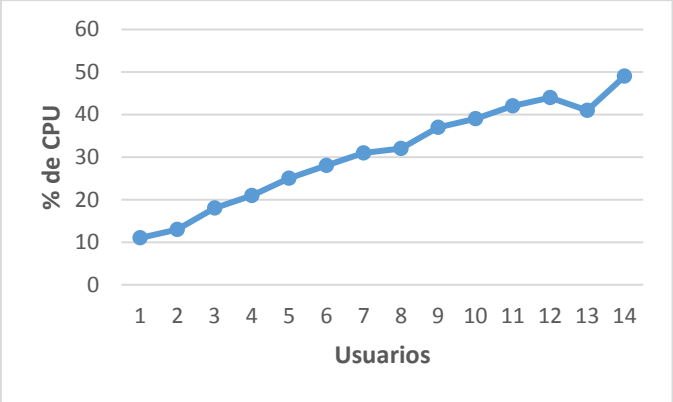


Fig. 2. Uso de CPU en Streaming.

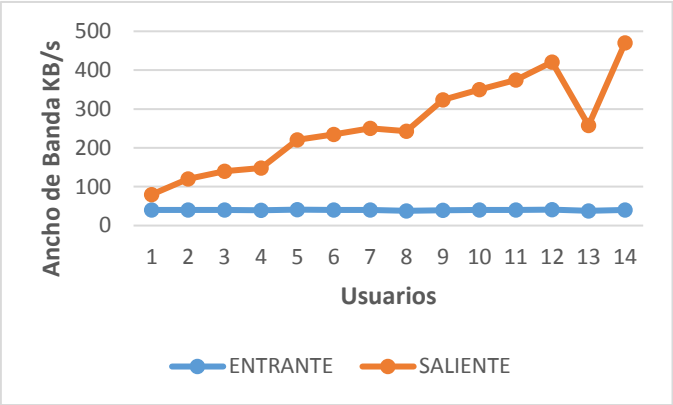


Fig. 3. Uso de ancho de banda en Streaming.

sistemas de videoconferencias: un *streaming* de vídeo en tiempo real, una videoconferencia multiusuario y múltiples sesiones de dos participantes cada uno (paciente-doctor). En los tres sistemas se ha realizado una monitorización del consumo de memoria y ancho de banda, así como del uso de ancho de banda entrante y saliente.

En el primer escenario, *streaming* en vivo, uno de los usuarios está publicando su flujo de audio y vídeo en la sesión y los clientes que se suscriben a él, van añadiéndose de forma gradual. En la Figura 2 podemos observar como el uso de CPU aumenta de forma lineal con el incremento de usuarios que se suscriben al *streaming*.

Esto ocurre porque el estándar WebRTC, como ya se ha explicado, utiliza SRTP para la transmisión de paquetes y por lo tanto se tiene que desproteger y volver a proteger los paquetes para realizar la transmisión desde el usuario que publica hacia los que se suscriben.

También podemos observar en la Figura 3 como el ancho de banda entrante es constante durante toda la sesión y el saliente aumenta también de forma lineal debido a

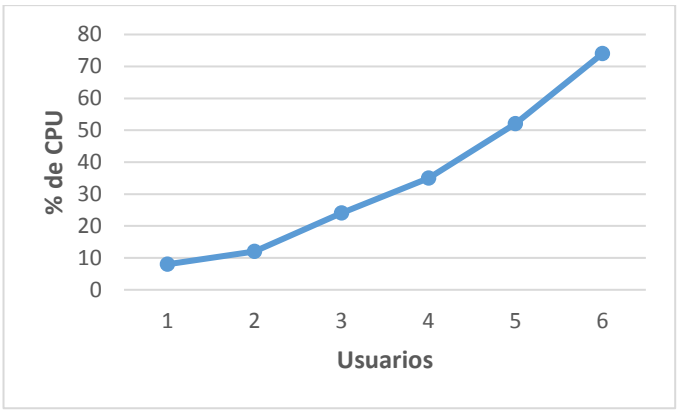


Fig. 4. Uso de CPU en Videoconferencia.

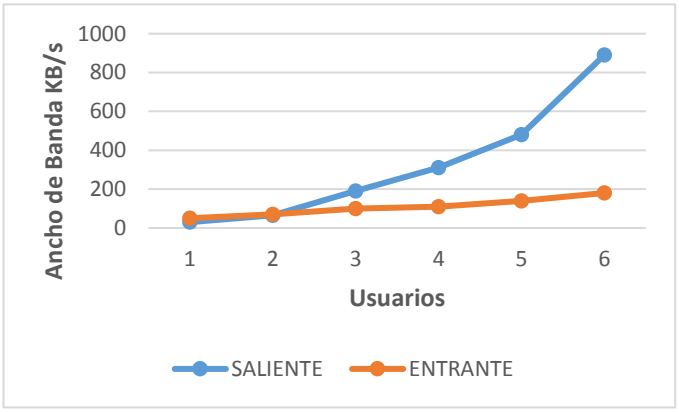


Fig. 5. Uso de ancho de banda en Videoconferencias.

que cada nuevo cliente conectado implica un nuevo flujo de salida. Acerca de la memoria utilizada aumenta también de forma lineal, pero con una variación mínima durante la sesión (de unos 10 MB). Finalmente pueden observarse pequeñas anomalías cuando se conectan más de 6 usuarios, pero probablemente sea debido a un error en el rendimiento del cliente que publica los datos.

En el segundo escenario, la videoconferencia multiusuario, cada usuario que se conecta a la sesión pública su flujo de audio y vídeo y además se suscribe al resto de usuarios que estaban conectados previamente. Se ha establecido un límite de seis usuarios ya que es el número que comúnmente se utiliza en este tipo de sesiones.

En la Figura 4 y la Figura 5 podemos observar como el consumo de ancho de banda entrante aumenta linealmente con el incremento de usuarios en la sesión debido al hecho de que cada nuevo usuario publica su flujo en el sistema. Sin embargo, el ancho de banda saliente y el consumo de CPU se incrementan de forma exponencial debido a

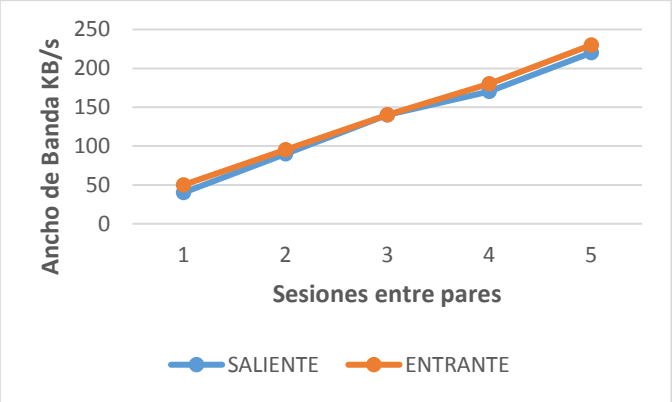


Fig. 6. Uso de ancho de banda en sesiones de pares (2 participantes).

que por cada nuevo usuario la unidad de control debe redirigir el nuevo flujo al resto de usuarios. Por lo tanto, el número de flujos de salida aumentará siguiendo la Ec. (1):

$$N = n(n-1), \tag{1}$$

donde n es el número de usuarios en la sala. El uso de memoria en este escenario también aumenta de forma exponencial, pero de nuevo con una variación insignificante para este estudio.

En la Figura 6 podemos observar como el consumo de ancho de banda tanto entrante como saliente aumenta linealmente con el incremento de sesiones de pares de usuarios debido al hecho de que cada nueva sesión pública su flujo en el sistema.

Considerando los tres escenarios, del total de pruebas realizadas se obtienen resultados razonablemente precisos y aceptables que corresponden al 80% de las pruebas hechas en desfase y duración sin cortes para redes de confiabilidad medio-baja (inferior a los 300 KB/s). El orden de complejidad del sistema de control es lineal con respecto a la cantidad de componentes (usuarios), de la red. Para redes muy confiables (cliente estable en 500 KB/s aprox.), deben realizarse gran cantidad de sesiones sin presentar alteraciones, conservando resultados aceptables, por lo que el tiempo de ejecución aumenta en función de la confiabilidad de la red.

5. Conclusiones

En el trabajo Se ha diseñado una arquitectura del sistema orientada al *Cloud* que permite proveer servicios avanzados de comunicaciones en tiempo real en los navegadores web tales como videoconferencia entre muchos usuarios. Con el particular caso que incorporaba a dos participantes paciente-médico en el seguimiento de un tratamiento.

Para el caso del streaming, el resultado del uso de cpu y el ancho de banda utilizado han sido aceptables en la comunicación paciente-médico. Para el ancho de banda

entrante se mantiene lineal, mientras que la salida tiene unos picos de crecimiento aceptable.

Para el caso de la videoconferencia, el resultado del uso de cpu y el ancho de banda saliente tiene un crecimiento exponencial en la comunicación paciente-médico, debido al hecho de que cada nuevo usuario publica su flujo en el sistema.

Para una sesión de pares, el resultado del uso de cpu y el ancho de banda tiene incrementos lineales aceptables.

En base a los tres escenarios se ha obtenido un 80% de aceptabilidad por lo que resulta confiable en una comunicación paciente-médico.

Para futuros estudios, se deben tomar en consideración, para escenarios similares, el límite de número de usuarios soportados por el sistema, así como, que se debe de hacer para incrementar ese límite.

Referencias

1. Martín-Alfonso, L.: Repercusiones para la salud pública de la adherencia terapéutica deficiente. Revista Cubana de Salud Pública. 32(3) (2006)
2. Montero-Ruiz, E., López-Álvarez, J.: La interconsulta médica: problemas y soluciones. Medicina Clínica, 136, pp. 488–490 (2011)
3. Velásquez, A., Suarez, D., Nepo-Linares, E.: Health sector reform in Peru: Law, governance, universal coverage, and responses to health risks. Revista peruana de medicina experimental y salud publica, 33(3), pp. 546–555 (2016)
4. O' Shea-Cuevas, G., Rizzoli-Córdoba, A., Aceves-Villagrán, D., Villagrán-Muñoz, V., Carrasco-Mendoza, J., Halley-Castillo, E., Delgado-Ginebra, I., Pizarro-Castellanos, M., Vargas-López, G., Antillón-Ocampo, F., Villasís-Keever, M., Muñoz-Hernández, O.: Sistema de Protección Social en Salud para la detección y atención oportuna de problemas del desarrollo infantil en México. Boletín Médico del Hospital Infantil de México, 72, pp. 429–437 (2015)
5. Fernández-Lozano, I.; Toquero-Ramos, J., Castro-Urda, V., Marín, Alonso-Pulpón, L.: Monitorización remota: una visión crítica. Cuadernos de Estimulación Cardiaca, 4, pp. 37–42 (2011)
6. Jang-Jaccard, J., Nepal, S., Celler, B., Yan, B.: WebRTC-based video conferencing service for telehealth. Computing, 98, pp. 169–193 (2016)
7. González, A.: Diseño de un sistema de comunicaciones. Tesis Master, 73, (2015)
8. Sime, A.W.: WebRTC: delivering telehealth in the browser. mHealth, 98, pp. 169–193 (2016)
9. El-Jaouhari, S., Bouabdallah, A., Bonnin, J.M., Lemlouma, T.: Toward a Smart Health-care Architecture Using WebRTC and WoT. World Conference on Information Systems and Technologies, Springer, pp. 531–540 (2017)
10. Cáceres-Taladriz, C., Pérez-Silva, J., Chausa, P., León, A., García-Alcaide, F., Gómez-Aguilera, E.J.: Auditoría y mejoras en la seguridad de la aplicación Hospital VIHrtual: plataforma web responsive de telemedicina para el seguimiento de pacientes con VIH. Libro de actas, 109 (2015)
11. Malla, C., Patricio, D.: Desarrollo e implementación de un módulo de videoconferencia a través de webrtc para una plataforma de telemedicina rural. Universidad Politécnica de Madrid, Madrid, (2014)
12. Johnston, A., Burnett, D.: WebRTC. Digital Codex LLC, St. Louis, MO (2014)

13. Sotomayor, B., Montero, R., Llorente, I., Foster, I.: Virtual Infrastructure Management in Private and Hybrid Clouds. IEEE Internet Computing, 13, pp. 14–22 (2009)
14. Burnett, D.: WebRTC: Handling Media on the Web. Multimodal Interaction with W3C Standards, Springer Link, pp. 155–169 (2017)
15. Pierleoni, P., Pernini, L., Palma, L., Belli, A., Valenti, S., Maurizi, L., Sabbatini, L., Marroni, A.: An innovative webRTC solution for e-health services. e-Health Networking, Applications and Services (Healthcom), IEEE 18th International Conference, pp. 1–6 (2016)
16. Vidul, A., Hari, S., Pranave, K., Vysakh, K., Archana, K.: Telemedicine for emergency care management using WebRTC. Advances in Computing, Communications and Informatics (ICACCI), International Conference, pp. 1741–1745 (2015)
17. Bergkvist, A., Burnett, D.C., Jennings, C., Narayanan, A.: Webrtc 1.0: Real-time communication between browsers. Working draft, W3C. 91, (2012)
18. Mell, P., Grance. T.: The NIST definition of cloud computing. Computer Security Division. Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg (2011)

ISSN 1870-4069

Energy Consumption of an Internal CRC Module in a Microcontroller

Mario Alberto Camarillo-Ramos[1], Roberto López-Avitia[1], Miguel Bravo-Zanoguera[2], Verónica Quintero-Rosas[1], Apolonio Castro-Corral Reyes[1], Andrea Magaly Alvarado-Álvarez [1]

[1] Tecnológico Nacional de México, ITMexicali, Mexico

[2] Universidad Autónoma de Baja California (UABC), Mexico

{mario.camarillo, avitia.roberto, veronicaquintero, reyes, a11490776}@itmexicali.edu.mx, mbravo@uabc.edu.mx

Abstract. In the current scenario with the Internet of Things looming on every aspect and activity of daily life, the need for the interconnection with information grids is inevitable. Information from one device to another, to others, is always happening and thus, are prone to transmission errors. To mitigate these errors, CRC can be used. The added error checking feat is also an issue since the device will need to code and decode the checksum. This research presents the energy consumption of a microcontroller with an internal Cyclic Redundancy Check module. Such microcontroller is the PIC24FV32KA302 from Microchip. An energy profile was used to determine the behavior of microcontroller using a CRC-16 configuration.

Keywords: energy consumption, microcontroller, CRC, cyclic redundancy check.

1 Introduction

With the raise of the Internet of Things the number of devices that communicate with each other over wireless mediums have increased. It is not limited to the Internet, it is also true for Bluetooth, Zigbee, and other communication schemes of wireless data transmission where different applications can be realized. Those applications have a wide spectrum of uses, ranging from parking spaces managers [1], which uses sensors to provide accurate information to users to select an empty parking slot, to aid in healthcare training for future surgeons [2].

In [3], an overview of how connected devices can achieve meaningful intelligent information is presented; it shows how different architectures and algorithms to implement this information exchange between such devices can be realized.

Whether the device is used for any application or if the information is intelligent, it must guarantee the integrity of such transmitted information. One technique used for this purpose is Cyclic Redundancy Check or CRC. In [4], this technique is used in the Internet of Things and in [5], such error correction technique is used in Bluetooth.

Another advantage of applying CRC to the transmitted information, is that by minimizing the errors in the receiver, the need for retransmission lessens, thus lowering the energy needed by the transmitter. But implementing CRC also generates a burden in energy consumption in the device, due to the information codification. This paper analyzes the energy consumption of an internal CRC module in a microcontroller using a 16 bit encoded message using CRC-16.

2 Background and Related Work

In data communications, where devices continuously exchange information in the form of bits, ones and zeros, errors are prone to happen. Whether those errors are caused by electrical distortion or signal attenuation, one way to reduce these errors is to use a checksum. This technique is used to detect errors in a data transmission and was first explored in [6], as a polynomial equation. The theory of operation is similar to that of a checksum but instead of using addition for the bits, division is used.

In [7], the algorithm is described as a number with the appended checksum divided by another fixed number. The division uses polynomial arithmetic which is simplified by applying the Boolean operation of Exclusive OR (XOR).

For instance, let C be the code checked with the algorithm, M the message (information), G the generator or the divisor (polynom), Q the quotient and R the reminder of the operation. One more characteristic is to append n zeros (X^n), shifted to the left or to the right to complete the CRC operations [8]. If a transmission is issued:

$$MX^n = [QG] + R, \tag{1}$$

$$C = MX^n + R. \tag{2}$$

Eq. 2 can be rearranged in the form of:

$$C = MX^n - R. \tag{3}$$

The receiver can be described as follows:

$$C = QG. \tag{4}$$

Combining Eq. 3 and 4:

$$MX^n = (QG) + R. \tag{5}$$

Using another combination of Eq. 3, 4 and 5:

$$(MX^n - R)/(G) = (QG)/G = Q. \quad (6)$$

Eq. 6 describes what happens if the message integrity is not compromised, there should be no remainder, the CRC value should be zero.

Although the added benefit for the information integrity is that it will be intact when it is received, there is extra computation within the application to achieve this feat, whether the CRC is done in software or hardware. In [9], a data transmission of 16 bits and 8 bits is used to demonstrate the computation requirements in clock cycles for hardware and software using four bytes of data with two CRC bytes. The implementation in software yields 6400 clock cycles; in hardware the required clock cycles are 800. This represents a 700% in time reduction from software to hardware and in terms of energy consumption, it should also require less.

Research have shown that dealing with CRC implementation in IOT applications can result in retransmission issues regarding energy consumption. They try to reduce the error correction by implementing novel approaches for Bluetooth Low Energy CRC-24 [10]. By doing this, the transmitter will send less corrupted information thus reducing the required energy for its transmission. In [11], classification methods are used to improve the efficiency of electronic devices in standby mode by analyzing the time they are doing their activity and the time they are in sleep mode. It is an interesting scheme to predict when those devices will not be used so they can be turned off.

The approaches to efficient energy consumption in IOT devices stated earlier focus on the act of predicting the errors within the transmission or the use of the devices already in communication. We present another layer of analysis but at a lower level of abstraction, in the device itself. By measuring the energy consumed in the act of generating the CRC within the device, the energy will be determined at the clock cycles level. The latter will be accomplished by measuring the current drawn by the device.

3 Methodology

Energy measurement is described in [12], [13] and [14]. This paper uses the approach of [15]. Current is measured by a shunt resistor in a low side configuration. After the current of a period is measured, an integration of the period is required to calculate the energy consumed.

3.1 Algorithm

In the algorithm department, activity is initiated in the device regarding the CRC module initialization and codification. Fig.1 provides a block diagram of the algorithm, as such, a message is issued and it is comprised of an array of sixteen unsigned integer elements, each 16 bits wide; these elements are used to apply the CRC codification. This operation is generated with the internal CRC module of the microcontroller. It does so by applying a pre-defined polynomial for CRC-16 calculation for the 16 bit message. The value for the operation is calculated by the module and it is 0x8005. The Checksum value is also generated for the data sequence been sent.

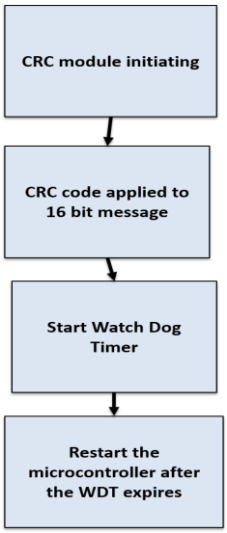


Fig. 1. Block diagram of the algorithm.

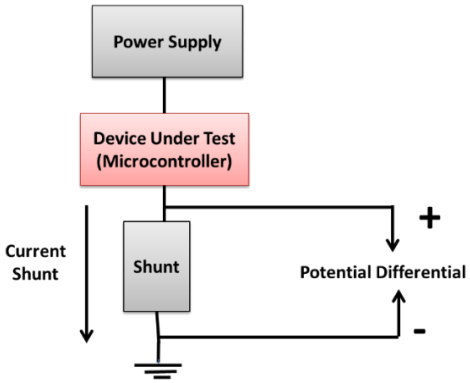


Fig. 2 Measurement setup.

Such data starts with 0x0000 and culminates with 0x000F, which comprise the array of sixteen elements; the checksum value is 0x1A0C. The algorithm is written in C and uses the free license for the XC16 compiler from Microchip in conjunction with the Microchip´s Code Configurator plugin. All the necessary functions required for the initialization and codification in hardware for the CRC-16 of the message are provided by the compiler.

3.2 Energy Measurement

Fig. 2 provides the measurement configuration by which the signal is acquired for its processing. A 10Ω@1% resistor is used as the shunt to provide the necessary voltage drop for the current to be calculated.

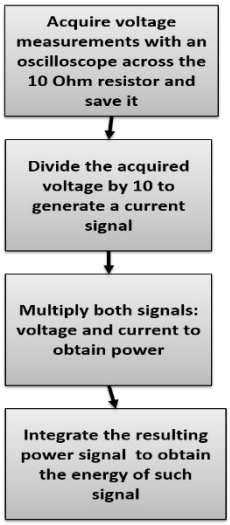


Fig. 3. Block diagram for the measurement and processing of the energy signal.

After the last element of the message is coded, the watchdog timer initiates operation; when such timer ends, it resets the device. The watchdog timer is configured to trigger every 1 ms. Since the device resets itself, no loops are required.

Fig. 3 illustrates a block diagram with the steps by which the signal is taken and then processed. A voltage reading is taken with a 10 Ohm resistor and is then saved for further analysis. The signal is then divided by 10 to generate the current passing through the shunt resistor. A power signal is then produced by multiplying the initial voltage signal with the new calculated current one. Once the power signal is known, an integration over one period is needed to calculate the energy consumption every time the device enters and exists the main program.

4 Results

Fig. 4, shows the energy profile [16], of the device. The red graph displays the voltage dropped across the 10 Ohm resistor with an oscilloscope.

A distinction should be made regarding the energy profile: it is not the actual energy consumed, it is the voltage. The energy of a device is described as the integral of the power over a certain time as stated in [17]. The latter is the reason why it is necessary to process the initial voltage signal through the energy measurements steps. Fig. 5, represents the power dissipated by the shunt resistor; this is the signal of interest for the integration in order to derive the energy consumption.

By integrating the power signal over a certain amount of time (period), we obtain the cumulative energy during the code execution. The operation of the initial configuration and the CRC calculation are 1238 cycles, plus 4 more for the sleep mode at 1 MHz or 1 microsecond for each instruction cycle.

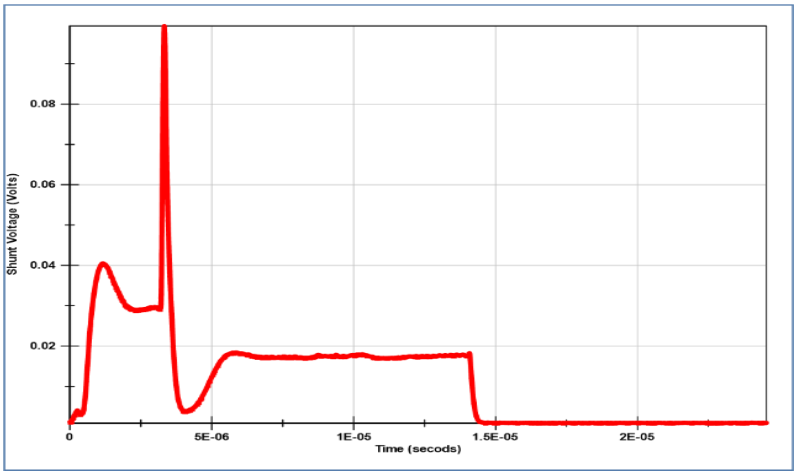


Fig. 4. Voltage across the shunt resistor.

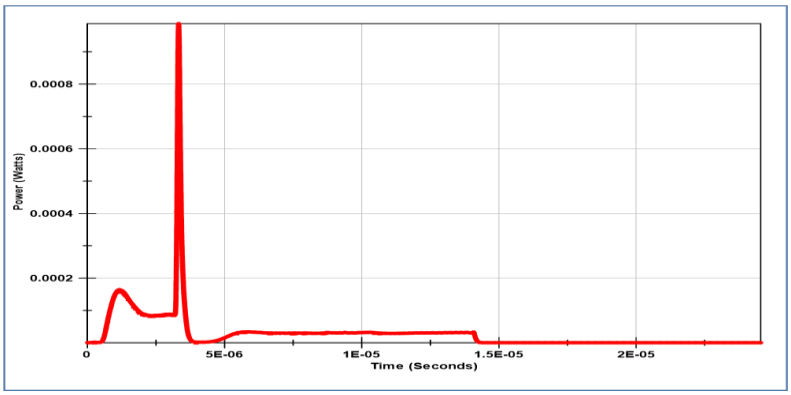


Fig. 5. Power dissipated in a period of the signal.

These clock cycles added determine the time the device is executing a task. The result is 1242 clock cycles, which translate to 1.242 seconds. The watchdog timer is configured to reset the device every 1mS after the last instruction has executed. Since the clock used for the watchdog timer is the internal RC module, it has a maximum value of 1.5 ms [18]. The actual time it takes to reset it is 1.238 ms, well within the specifications.

Fig. 6 displays the energy consumed by the device over one period. The cumulative energy consumption is 0.7203 nano Joules.

5 Conclusions

The energy consumption of a microcontroller with an internal CRC module is evaluated executing its operations at a clock cycle rate of 1 microsecond. The internal oscillator

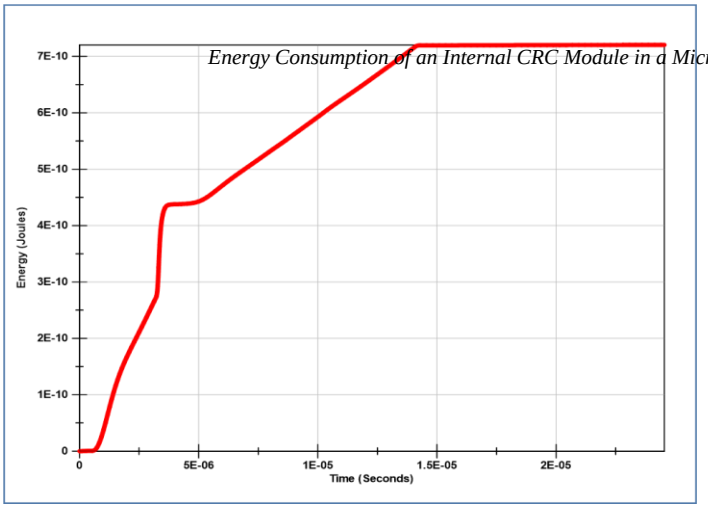


Fig. 6. Energy consumption over a period.

runs at 2MHz but the frequency of the instruction cycle runs at half that frequency. The computational power required for doing a CRC-16 with 16 bit, width data over an array of 16 unsigned integer variables is 1242 clock cycles with an energy consumption of 0.7203 nano Joules. The majority of the energy is drawn by the initial setup, which include the microcontroller wake up from reset. The initialization code form the XC16 compiler with no optimizations shows a steady power consumption up until the CRC module execution, as shown in Fig. 2 and 3. There is an increase in energy demand by way of an overshoot of current after the initial setup. This demand is most likely generated by the CRC module preparing to do the codification for the message.

No loops where used in the algorithm as the watchdog timer resets the microcontroller so it can repeat the operation form the power up state and not the evaluated while or for loop. Further investigation could be done using those loops to measure the current consumed by entering and exiting such loops.

The measurement was conducted for only one frequency; further analysis can be made by changing the frequencies of operation of the microcontroller.

References

1. Farhad, A. I.: Internet of Things Based Free Parking Space Management System. International Conference on Cloud Computing Research and Innovation (ICCCRI), 1(1), pp. 1–6 (2017)
2. De la Borbolla, C.T.: Applying the Internet of Things (IoT) to biomedical development for surgical research and healthcare professional training. IEEE Technology & Engineering Management Conference (TEMSCON), 1(1), pp. 335–341 (2017)
3. Bello, Z.: Intelligent Device-to-Device Communication in the Internet of Things. IEEE Systems Journal, 10(3), pp. 1172–1182 (2016)
4. Tsimbalo, F.P.: CRC Error Correction in IoT Applications, IEEE Transactions on Industrial Informatics, 13(1), pp. 361–369 (2017)
5. Tsimbalo, F.P.: Fix it, don't bin it -CRC error correction in Bluetooth Low Energy. IEEE 2nd World Forum on Internet of Things (WF-IoT), 1(1), pp. 286–290 (2015)

6. Peterson, B.: Cyclic Codes for Error Detection. (IRE), 49(1), pp. 228–235 (1961)
7. ATMEL: www.atmel.com (2017)
8. Nkom: Concise schemes for realizing 1-Wire® cyclic redundancy checks. 3rd IEEE International Conference on Adaptive Science and Technology, 1(1), pp. 70—79 (2011)
9. Microchip: www.microchip.com (2008)
10. Tsimbalo, F.P.: CRC error correction for energy-constrained transmission, IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 1(1), pp. 430–434 (2015)
11. Andrade, R.N.P.: Applying classification methods to model standby power consumption in the Internet of Things, IEEE 14th International Conference on Networking, Sensing and Control (ICNSC), 1(1) pp. 537–542 (2017)
12. Tiwari, M.W.: Power Analysis Of Embedded Software: A First Step Towards Software Power Minimization. Computer-Aided Design, IEEE/ACM International Conference, 1(1), pp. 384–390 (1994)
13. Luo, G.S.L.R.: Analysis and Optimization of Embedded Software Energy Consumption on the Source Code and Algorithm Level. Embedded and Multimedia Computing, 1(1), pp. 1–5 (2009)
14. Ortiz, S.: Impact of Source Code Optimizations on Power Consumption of Embedded Systems. Circuits and Systems and TAISA Conference, 1(1), pp. 133–136 (2008)
15. Camarillo-Ramos, L.A.B.Z.: Medición del consumo de energía en un microcontrolador de 16 bits en operación y reposo. Memoria del 1er. y 2do. seminario de investigación de la facultad de ingeniería, 1(1), pp. 20–23 (2014)
16. Renesas:http://www.techonline.com/electrical-engineers/education-trainig/webinars/4420344/Implementing-Ultra-low-Power-Design-Techniques-for-High-performance-32-bit-MCU-based applications (2013)
17. Vey: AN1416 Low Power Design Guide, Microchip. http://ww1.microchip.com/downloads/en/AppNotes/01416a.pdf. (2014)
18. Microchip:http://ww1.microchip.com/downloads/en/DeviceDoc/39995_b.pdf. (2017)

ISSN 1870-4069

Autenticación para acceso a datos distribuidos basado en Kerberos

Juan Alejandro Ibáñez Ramírez, Francisco de Asís López-Fuentes

Departamento de Tecnologías de la Información
Universidad Autónoma Metropolitana-Cuajimalpa (UAM-C), Ciudad de México, México

flopez@correo.cua.uam.mx

Resumen. Hoy en día la mayoría de datos se encuentran almacenados en sitios remotos que por lo general son sistemas distribuidos (como Dropbox, OneDrive, Google Drive, Outlook). Por lo tanto, surge la necesidad de proteger el acceso a estos datos para garantizar su privacidad e integridad ante el creciente número de ataques a la seguridad, entre ellos los virus informáticos, los troyanos, o el Ransomware [10]. Es por esto que se requieren sistemas que implementen un acceso seguro a datos distribuidos. Uno de los objetivos principales en la seguridad de la información es implementar controles de acceso, los cuales integren políticas y criterios que indiquen bajo qué circunstancias se deberá otorgar acceso a los recursos de un sistema. Este artículo presenta un sistema de autenticación entre múltiples dominios distribuidos basado en Kerberos para tener el control de acceso a datos distribuidos en una red de computadoras, haciendo uso de técnicas de cifrado de mensajes y de los datos.

Palabras claves: autenticación, seguridad, control de acceso, sistemas distribuidos.

Authentication of Access to Distributed Data Based on Kerberos

Abstract. Today most of the data is stored in remote sites that are usually distributed systems (such as Dropbox, OneDrive, Google Drive, Outlook). Therefore, there is a need to protect access to this data to ensure its privacy and integrity in the face of increasing security attacks, including computer viruses, Trojans, or Ransomware [10]. These are important reasons to require implementing secure access to distributed data. One of the main objectives in information security is to implement access controls, which integrate policies and criteria that indicate under what circumstances access to resources of a system should be granted. This article presents a Kerberos-based distributed multi-domain authentication system for controlling access to distributed data in a computer network using data encryption techniques and data.

Keywords: authentication, **s**ecurity, access control, distributed system.

1. Introducción

Las tecnologías de la información y comunicación (TICs), han permitido que las personas actualmente estén conectadas y comunicadas en todo momento sin importar el lugar en donde estén. Esta ubicuidad requiere que los sistemas de información estén distribuidos en diferentes sitios y que los datos puedan ser accedidos también desde cualquier lugar. Sin embargo, los sistemas distribuidos al funcionar dentro de un ambiente abierto de comunicación son susceptibles a diferentes ataques a la seguridad. La seguridad se refiere a las medidas de procedimiento lógicas y físicas orientadas a la prevención, detección y corrección de casos de mal uso, así como a las características que debe tener un sistema de cómputo para resistir a ataques. Los ataques más comunes a la seguridad en un sistema de cómputo son los ataques de intercepción, modificación o fabricación de mensajes. Uno de los objetivos principales en la seguridad de la información es implementar controles de acceso, los cuales integren políticas y criterios que indiquen bajo qué circunstancias se deberá otorgar acceso a los recursos de un sistema. Los mecanismos básicos de control de accesos son integridad, confidencialidad, autenticación y autorización. Las principales características de estos mecanismos son [8, 4, 6]:

- *Integridad* sirve para prevenir cambios impropios o no autorizados sobre el contenido de la información.
- *Confidencialidad* es el mecanismo que permite la ocultación de los recursos a entidades no autorizadas. El uso de la criptografía ayuda en la tarea de preservar la confidencialidad.
- *Autenticación* ofrece mecanismos que permiten una identificación correcta del origen del mensaje, asegurando que la entidad no sea falsa.
- *Autorización* es el mecanismo que determina si una entidad una vez autenticada está autorizada para obtener el acceso al recurso solicitado.

Por otro lado, las políticas de control de acceso en un sistema de seguridad deben ser implementadas para ayudar a establecer quién o quiénes tendrán acceso a los recursos del sistema, quiénes son los dueños de los recursos y qué permisos tendrán los usuarios sobre éstos. De acuerdo con los autores en [7], los actores para una política de acceso son:

- *Autoridades y regímenes:* Las autoridades son responsables de definir los medios de acceso permitidos y clasificar los recursos, determinar las autorizaciones, y especificar los niveles de confianza aplicables, mientras que los regímenes pueden ser entidades relacionadas entre sí.
- *Recursos:* Una política de seguridad debe definir los recursos a los que se aplica: éstos pueden ser elementos intangibles (datos o información), o elementos de hardware.
- *Clasificación de recursos:* Los recursos se pueden clasificar según su nivel de riesgo, costos o las consecuencias asociadas con la gestión de su acceso.
- *Contexto de acceso:* Circunstancias en las que se solicita el acceso o los medios por los cuales se proporciona el acceso, por ejemplo, la hora de la solicitud.

- *Uso permitido:* Usos posibles para un recurso (leer, modificar, crear, eliminar, etc.)
- *Partes:* Pueden ser referidas por identificador (usuario #6718), o por atributo (usuarios del grupo "Administradores").
- *Confianza en la autenticidad:* Representa las reglas de acceso dependiendo de la confianza del sistema en la autenticidad de una parte.

En este trabajo se pretende resolver problemas relacionados al control de acceso para garantizar la seguridad de datos distribuidos en diferentes sitios al integrar el modelo de control de autenticación Kerberos [1], en un ambiente distribuido. Para alcanzar esta meta nuestro modelo propuesto pretende cubrir características como: funcionar dentro de un ambiente de red inalámbrica, resistir la adivinación de contraseñas, resguardar los datos ante una petición falsa y principalmente ofrecer un servicio único de autenticación de usuarios entre varios dominios distribuidos, garantizando el cifrado de mensajes y de datos.

El resto de este artículo tiene la siguiente organización. En la sección 2 se presenta información sobre los sistemas de autenticación, principalmente de Kerberos. La sección 3 presenta el modelo propuesto. Una descripción de la implementación se describe en la sección 4. El artículo concluye en la sección 5.

2. Trabajo relacionado

Algunos de los temas a resolver por los sistemas distribuidos actuales consisten en la necesidad de garantizar un acceso efectivo y seguro a servicios ofrecidos por ciertos proveedores en la nube (infraestructura como servicio, plataforma como servicio y software como servicio). Para este tipo de escenarios, los autores en [3], proponen la utilización del modelo Kerberos. Después de revisar la propuesta anterior, se puede detectar que una posible mejora a este sistema consistiría en la utilización de un algoritmo de cifrado más actual en lugar de DES.

Por otro lado, la empresa estadounidense de desarrollo de software Vandyke [11], plantea el tema de la autenticación de usuarios para la transferencia de archivos usando el protocolo SFTP (Secure Shell File Transfer Protocol), a través de un programa desarrollado por ellos, el cual crea un túnel cifrado de comunicaciones utilizando el modelo cliente-servidor para establecer conexiones remotas. Entre las características de este programa se encuentran que la comunicación se genera mediante el protocolo SSH (Secure Shell), el sistema ofrece cifrado de comunicación SSL (Secure Sockets Layer) y no de archivos en la fuente y que es de pago.

Otro de los temas relevantes para un sistema de seguridad es el control de la autenticación de usuarios. Para lograr este objetivo en [5], los autores plantean usar el protocolo Kerberos para ofrecer un servicio de autenticación que permita acceder a un recurso hospedado en la nube. Además, presentan una modificación al modelo añadiendo un protocolo de Autenticación Distribuida llamado DSA el cual permite al sistema que, mediante una clave de sesión dinámica, realice una autenticación previa antes de que el usuario pueda acceder al servicio solicitado. Esta idea podría ser una posible aportación al presente proyecto.

En relación al tema de la transferencia de archivos usando el modelo Kerberos para el control de acceso a un servidor de descarga de archivos, Al-Ayed y Liu [2], plantean

Tabla 1. Comparativo de los diferentes sistemas de autenticación

Trabajo	Observaciones	Posible mejora
Implementation of Kerberos versión 5 in cloud computing in order to enhance the security issues [3]	- Control de acceso a servicios generales en la nube	- Uso de AES
Secure File Transfer with SSH [11]	- Arquitectura cliente-servidor. - El sistema sólo ofrece cifrado de comunicación y no de archivos en la fuente. - El sistema es de pago y no de uso libre.	- Arquitectura de autenticación distribuida. - Cifrado de archivos.
Distributed Authentication in the Cloud Computing Environment [5]	- Modificación al modelo Kerberos. - Protocolo de autenticación distribuida DSA. - Clave de sesión dinámica.	- Establecer alguna política de control de acceso a un recurso específico en la nube.
Using Kerberos Method to Secure File Transfer Sessions [2]	- Detección de intrusiones basado en el modelo de Markov. - Control de acceso a un servicio FTP.	- Control de acceso a un modelo distribuido mediante autenticación de dominios distribuidos. - Cifrado de archivos.
A lightweight authentication and authorization solution based on Kerberos [9]	- Protocolo ligero. - Resistente a ataques de replicación de mensajes y de adivinación de contraseñas.	- Mejorar las deficiencias del protocolo para hacerlo más robusto.

usar el protocolo FTP (File Transfer Protocol) y no usar SSL para cifrar las conexiones, ya que consideran que el uso de Kerberos es una solución más robusta. También sugieren usar una máquina de aprendizaje basada en el modelo de Markov para detectar intrusiones tomando como entrada la secuencia de posibles estados del modelo Kerberos.

Con el objetivo de ofrecer una versión ligera del modelo Kerberos para resolver el problema de la autenticación y autorización de derechos digitales, Zhang et al. [9], formulan un rediseño del modelo Kerberos con la intención de reducir la carga de cada nodo del sistema. Mencionan que, aunque el protocolo ligero resiste a ataques de replicación de mensajes y de adivinación de contraseñas, aún cuenta con algunas deficiencias.

Después de analizar las propuestas anteriores se puede concluir que el modelo Kerberos es muy flexible a modificaciones y puede integrarse dentro de diferentes tecnologías. Asimismo, el uso de Kerberos se justifica de forma general en todas las propuestas anteriores para responder a las necesidades actuales de autenticación. A continuación, la tabla 1 resume las principales características de cada propuesta, así como las posibles mejoras y aportaciones al presente trabajo.

3. Modelo

El modelo de autenticación propuesto toma como referencia el modelo Kerberos, el cual es un modelo creíble y funcional por las siguientes razones [7]:

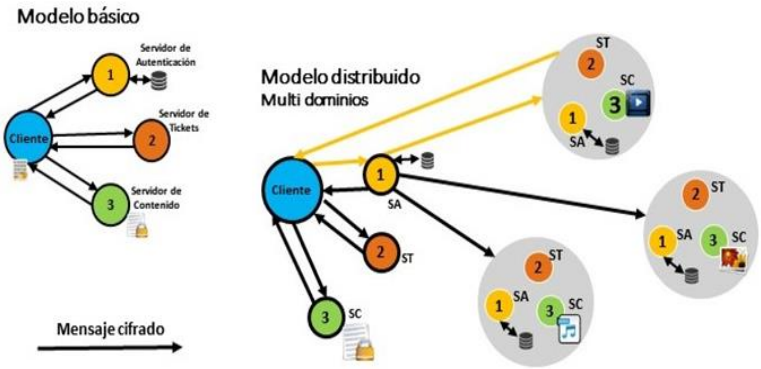


Fig. 1. Modelo básico y distribuido del sistema de autenticación.

- Ha sido ampliamente utilizado, probado, estudiado y está respaldado por una amplia comunidad de desarrolladores.
- Cumple con los requisitos de los sistemas distribuidos modernos, ya que desde el inicio fue concebido para trabajar dentro de entornos de comunicaciones abiertos.
- El modelo arquitectónico es sólido y funcional, lo cual ha permitido la evolución del modelo para una fácil integración con diferentes sistemas.
- El modelo actualmente sigue en funcionamiento e integrado dentro de varios sistemas, como Apache Hadoop, Ad-hoc Networks, Lot o SO Open Source y es una parte integral dentro de la infraestructura de la tecnología de la información actual.

El modelo consiste en tres nodos los cuales podrán estar bajo un solo dominio de red o distribuidos bajo dominios diferentes. El usuario podrá descargar de manera transparente los datos mediante un nodo cliente el cual establecerá conexión con el sistema, y éste a su vez se encargará de realizar las validaciones y enlaces para descargar el contenido distribuido.

Cada dominio tendrá una única base de datos, pero con conocimiento de otros dominios. Todas las comunicaciones o pase de mensajes entre nodos tendrán que ser procesadas mediante una función de cifrado, evitando así el envío de datos en texto claro. La figura 1 muestra de manera gráfica una descripción del modelo básico y distribuido del sistema de autenticación y las etapas de operación. En el modelo básico se muestran los tres servidores: de autenticación, tickets y de contenido, así como los intercambios de mensaje que cada servidor tiene con el cliente. Por otro lado, el modelo distribuido con multi dominios muestra como un cliente puede acceder a contenidos en otros dominios, pero debe hacerlo a través del servidor de autenticación de su propio dominio.

Cada dominio ajeno al del cliente tiene también tres servidores. Sin embargo, la autenticación entre los multi dominios se realiza por medio de los servidores de autenticación de cada dominio. En la figura 2 se puede observar la comunicación y envió de mensajes propuesta en cada etapa de comunicación. Asimismo, se indican las validaciones hechas por cada nodo del sistema.

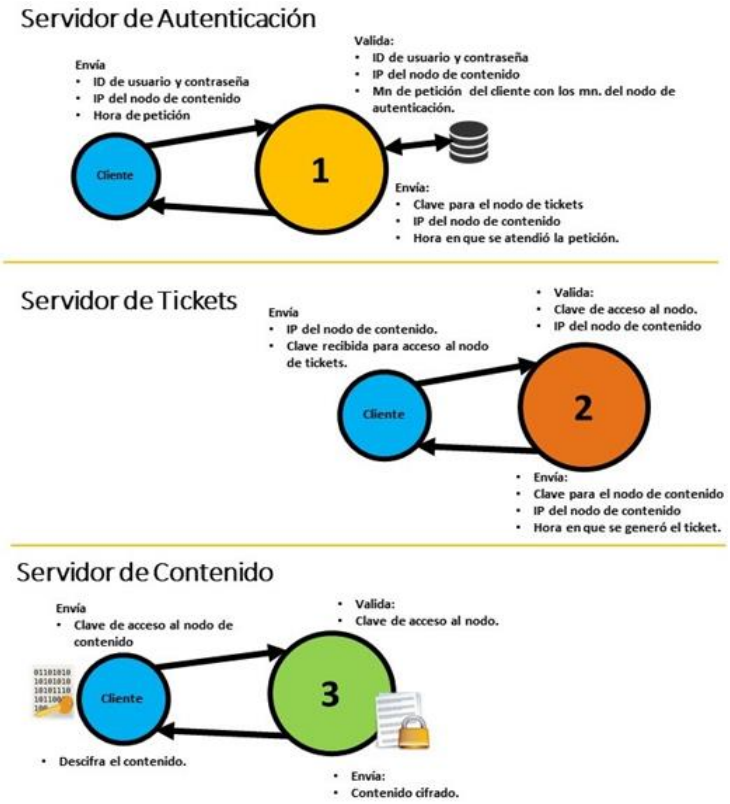


Fig. 2. Modelo de comunicación en cada nodo del sistema.

Un problema a considerar en la autenticación está asociada, con el tiempo de vida de un mensaje con el ticket de concesión, de esta manera [12]:

- Si es demasiado corta, entonces es solicitado repetidas veces por la contraseña.
- Si es demasiado larga, entonces existe una mayor oportunidad para un ataque de repetición.
- La amenaza es que un oponente se robe el ticket y lo use antes de que el tiempo expire.

En el modelo de comunicación de la figura 2, se considera este problema de tiempo de vida para cada ticket que se emite. De tal manera que se pueda determinar que quien presenta el ticket es el mismo cliente para el que se emitió dicho ticket. Una parte importante del funcionamiento de nuestra propuesta es la interoperabilidad entre dominios, ya que esta característica permite que clientes y servidores que pertenecen a diferentes organizaciones o dominios puedan ofrecer servicios entre ellos para usuarios previamente autenticados.

4. Implementación

Se ha puesto en práctica un prototipo básico del esquema de autenticación propuesto usando diferentes servidores en nuestro laboratorio. El sistema consta de 3 nodos los cuales están implementados mediante sockets para el SO Linux usando el lenguaje de programación C. Se usa TCP/IP como el protocolo de comunicación entre los servidores con el propósito de evitar pérdida de paquetes. Cada nodo del sistema es una aplicación independiente la cual puede estar bajo un solo dominio de red (IP), o distribuido bajo un diferente dominio; inclusive, cada uno de los nodos pudieran estar contenidos dentro de varios contenedores (Docker o Linux Container).

En lo que concierne al envío de mensajes entre nodos, se ha implementado una función encargada del cifrado de éstos, dicha función se explicará a detalle más adelante. En esta implementación y para fines de realizar pruebas iniciales, se asume por el momento, que todos los relojes dentro de cada entorno donde se ejecuta cada uno de los nodos están sincronizados. Por lo tanto, no se ha implementado un servicio de sincronización de relojes. Adicionalmente cada nodo fue programado para poder atender a diferentes clientes de manera paralela haciendo uso de la librería "pthread.h" para poder generar un hilo que atienda todas las peticiones de cada cliente. A continuación, se describe el funcionamiento de cada uno de los nodos.

4.1. Servidores

Servidor de autenticación

El servidor es el responsable de recibir la primera conexión del cliente junto con un mensaje compuesto por: ID, contraseña, IP del servidor de tickets y la hora de la petición. Una vez que se recibe el mensaje se validan en un arreglo estático de cadenas el ID, contraseña, IP de servidor de tickets y los minutos en que se atiende la petición. Para validar la hora se extrae como referencia la hora dentro del entorno donde se esté ejecutando el servidor de autenticación (los minutos y la hora deben ser iguales al recibido). Si las validaciones son correctas, se envía la clave para acceder al servidor de tickets y la hora en que se atiende la petición. En caso contrario se cierra la conexión, pero el servidor queda en espera de otras nuevas conexiones.

Servidor de tickets

Cuando se atiende una conexión, este servidor recibe y valida un mensaje con la clave y la dirección del servidor de contenido, si la validación es correcta, se genera un mensaje (ticket) compuesto por la hora en que se atiende la petición, la clave e IP para acceder al servidor de contenido. En caso contrario se cierra la conexión, pero el servidor queda en espera de más conexiones.

Servidor de contenido

En este servidor se encuentra el contenido al que quiere tener acceso el cliente. Cuando se recibe una conexión, el servidor valida si la clave enviada dentro del mensaje es correcta, si la validación es satisfactoria se crea un flujo de lectura de archivo y se envía el contenido bit por bit al cliente, en caso contrario la conexión se cierra y se queda en espera de nuevas peticiones.

4.2. Función de cifrado y descifrado

Para poder enviar mensajes de manera segura, se han programado dos funciones encargadas de cifrar y descifrar cada uno de los mensajes enviados en cada uno de los nodos durante cada una de las validaciones realizadas por el modelo distribuido, dicha función utiliza la librería "mcrypt.h" de uso libre, estas funciones hacen uso del algoritmo Rijndael el cual fue considerado para la especificación AES (Advanced Encryption Standard).

Cabe aclarar que la versión del algoritmo que es utilizada por el sistema es la versión que ofrece soporte para un tamaño de bloque y clave de 256 bits en el modo de cifrado de bloque CBC (Cipher Block Chaining Mode). La razón por la que se decidió utilizar esta versión y no la versión que hace uso de un bloque de 128 bits fue para darle mayor fortaleza contra posibles ataques y a su vez obtener un cifrado rápido y de bajo consumo de memoria.

Adicionalmente y con el fin de realizar pruebas rápidas al sistema, aún no se ha diseñado un servicio para el intercambio de claves. Actualmente el manejo de claves se realiza en tiempo de programación en cada nodo quedando definidas de manera estática, de forma similar, el vector de inicialización para el cifrado de bloques (IV), es establecido de manera estática en tiempo de programación. Sin embargo, no descartamos el poder integrar como una extensión al presente trabajo la integración de una función que haga uso de un algoritmo de cifrado asimétrico o de llave pública en conjunto con la implementación de un servicio de gestión de claves.

Aplicación cliente

Para poder acceder al sistema es necesario disponer de la aplicación cliente, la cual se encarga de realizar las conexiones y recibir las respuestas de las validaciones del sistema, así como del contenido. El nodo cliente está compuesto por 3 funciones principales y una auxiliar encargada de generar una conexión hacia cada nodo del sistema. Cada función es encargada de enviar datos específicos para cada uno de los nodos del sistema, esto dependiendo de la respuesta recibida en cada paso, por el sistema de autenticación. A continuación, se describen cada una de las funciones del nodo cliente.

Conecta

Esta función recibe dos parámetros: la IP para establecer una conexión y el puerto de la aplicación que atenderá la conexión, regresa una instancia de tipo conexión, la cual puede ser usada por otra función para enviar algún tipo de mensaje una vez que la conexión se ha establecido.

Autentifica

Recibe como único parámetro una instancia de una conexión a una dirección IP y puerto específico. En primer lugar, pide al cliente su ID y contraseña para concatenarlos al mensaje que será enviado al servidor de autenticación, adicionalmente a dicho mensaje se le concatena la dirección IP del servidor de tickets y la hora en que se hace la solicitud en la aplicación cliente. Una vez que se han enviado los datos en una sola cadena cifrada y dependiendo de la respuesta recibida, esta función devuelve 0 si la

respuesta de la validación fue incorrecta o 1 si fue satisfactoria, en un caso correcto se recibe una clave para acceder al servidor de tickets y se procede a realizar la conexión con el servidor de tickets, en caso contrario se cierra la conexión y la aplicación cliente.

Solicita_ticket

Cuando se ha pasado la validación del servidor de autenticación, se genera una conexión al servidor de tickets. Esta función recibe como único parámetro una instancia de una conexión a una dirección IP y puerto específico, las cuales corresponden al servidor de tickets. Cuando esta función es llamada se envía un mensaje cifrado el cual contiene la clave de acceso al servidor de tickets y la dirección del servidor de contenido para ser validadas. Si la respuesta es satisfactoria la función devuelve 1 y recibe un mensaje (ticket), compuesto por la hora en que se atendió la petición, la clave de acceso y la IP del servidor de contenido, y continúa con el siguiente paso para descargar el contenido, en caso contrario devuelve 0 y cierra la conexión y la aplicación.

Descarga_contenido

Esta función es ejecutada únicamente cuando las validaciones anteriores han sido satisfactorias y al igual que las anteriores recibe una instancia de una conexión con la dirección del servidor de contenido y su puerto. Una vez establecida la conexión, se envía la clave del servidor de contenido para poder tener acceso, de ser satisfactoria la validación de la clave se genera un flujo para la escritura de un archivo y se recibe bit por bit al igual que el nombre del archivo. Si por el contrario la validación es negativa, la conexión se cierra y la aplicación también.

5. Conclusiones

El rápido desarrollo y la creciente complejidad de las aplicaciones de cómputo que actualmente son desplegadas sobre redes de comunicación han generado una más exigente demanda de cuestiones de seguridad y privacidad de parte de los usuarios. Esto ha generado un gran reto tecnológico y la necesidad de construir sistemas más seguros. En este trabajo se presenta un sistema de autenticación para datos distribuidos basados en el modelo Kerberos. Se ha desarrollado un prototipo básico de nuestro modelo y actualmente se está trabajando en integrar una base de datos relacional al nodo de autenticación para garantizar la persistencia de los datos y brindar una mayor robustez a la gestión de los mismos.

5.1. Trabajo a futuro

Como trabajo a futuro se espera programar una función de cifrado y descifrado de archivos, la cual se integre dentro de los nodos de contenido y cliente, con el objetivo de garantizar la privacidad del contenido mientras viaja en la red. Adicionalmente, y como continuidad del proyecto, contemplamos integrar servicios de sincronización de relojes y de gestión de claves de cifrado para mensajes y archivos, los cuales aporten controles confiables para robustecer el funcionamiento del sistema de manera efectiva sin comprometer su seguridad. Por otro lado, consideramos que el presente trabajo

puede direccionarse hacia diferentes objetivos. Uno de éstos es el poder integrarlo a futuro en una red de internet de las cosas con el fin de poder garantizar la seguridad y privacidad de los datos generados por este tipo de redes dentro de un ambiente abierto.

Referencias

1. Neumann, B. C., Ts'o, T.: Kerberos: An Authentication Service for Computer Networks. In: IEEE Communications Magazine, 32(9), pp. 33–38 (1994)
2. Al-Ayed, F., Liu, H.: Synopsis of Security: Using Kerberos Method to Secure File Transfer Sessions. In: IEEE International Conference on Computational Science and Computational Intelligence, USA (2016)
3. Hojabri, M., Venkat, R. K.: Innovation in cloud computing: Implementation of Kerberos version 5 in cloud computing in order to enhance the security issues. In: IEEE International Conference on Information Communication and Embedded Systems (ICICES), India (2013)
4. López-Fuentes, F. A.: Sistemas Distribuidos. UAM Unidad Cuajimalpa, pp. 1–203 (2015)
5. Liu, Y., Li, Z., Sun, Y.: Distributed Authentication in the Cloud Computing Environment. In: Springer International Publishing Switzerland, LNCS, 9532 (2015)
6. MIT Kerberos Consortium: The Role of Kerberos in Modern Information Systems. pp. 1–53, (2008)
7. MIT Kerberos Consortium: Why is Kerberos a credible security solution?. pp. 1–13 (2008)
8. Bishop, M.: Introduction to Computer Security. Pearson Education, Inc., pp. 2–3 (2005)
9. Zhang, N., Wu, X., Yang, C., Shen, Y., Cheng, Y.: A lightweight authentication and authorization solution based on Kerberos. In: IEEE (2016)
10. Symantec. Informe sobre las amenazas para la seguridad en Internet de 2017. Sitio web: https://www.symantec.com/es/mx/security-center/threat-report (2017)
11. VanDyke: Software Inc. Secure File Transfer with SSH (2008)
12. Stallings, W.: Fundamentos de Seguridad en Redes Aplicaciones y Estándares. Pearson Educación, pp. 28, 31–32, 35, 106, 109 (2004)

ISSN 1870-4069

An Analysis of Dietary and Demographic Data in Oral Health, Data from the National Health and Nutrition Examination Survey: A Preliminary Study

Nubia M. Chávez-Lamas[1], Laura A. Zanella-Calzada[2], Carlos E. Galván-Tejada[2]

[1] Universidad Autónoma de Zacatecas, Unidad Académica de Odontología, Clínica Comunitaria de Tacoaleche, Zacatecas, Zacatecas, Mexico

[2] Universidad Autónoma de Zacatecas, Unidad Académica de Ingeniería Eléctrica, Zacatecas, Zacatecas, Mexico

{lzanellac, ericgalvan}@uaz.edu.mx

Abstract. Dietary and demographics features has an influence in the general health status of the population in the world. Therefore in this paper is proposed an univariate analysis of 7 dietary and demographic features to study the impact on the oral status in order recognize the different determinants that contribute to modify in a negative way the oral health status. Univariate analysis is carried on applying an multi objective linear regression and evaluated in terms of area under the curve (AUC), p-value, sensitivity and specificity. Additionally, a multivariate model is done to evaluate confounder to increase the AUC. Preliminary results shows that individually water source is an important feature that affects oral health status.

Keywords: oral health, health status, linear regression, statistical analysis, univariate model, multivariate model.

1 Introduction

The World Health Organization (WHO), defined health as a physical, mental and social healthy status, not only the absence of diseases. This definition as evolved from that conceptual concept to a serie of quantitative scales that allows be measured of the general health status, therefor in 1994, the WHO propose the concept of quality of life as an individual perception of his life position, inside the context of cultural environment and the relationship with their objectives, expectations, standards and concerns. This new aspects that comprise the definition of health implies that behavior patterns, expectations

and cultural are independent for each group, consequently, to evaluate this, three dimensions are proposed: General (lifestyle), particular (life conditions) and singular (type of life) [18,13].

Oral health is included in the general dimension, being an essential component to life quality of individuals, hence, nowadays oral health is a determining factor in individuals general health and of communities. For that reason, several studies about which characteristics of life, diet, demographic, social and others influence in the oral health are becoming an interesting niche study [18,13,7,15]. However, these studies can be influenced by several characteristics from the particular individuals, as was mentioned before, therefore, this features to evaluate oral health implies that varies depending on the condition of the country, genetic heritage, even political and public health services for each country [18].

These studies are done using a methodological scientific (survey), which is useful to prioritize, identify and solve oral health, moreover allows to generate prediction models that helps to decrease the incidence and prevalence of oral diseases. Is well-known that one of the main illness in oral health that affects 90 percent of the world population is dental caries and periodontal illness in a 80 percent [19], besides those are concentrated mainly in communities less favored by what are considered as oral health problems [15]. In last three decades, researchers develop different purpose surveys to evaluate life quality and the relationship with oral health, for instance, Social Impacts Of Dentals Disease, Geriatric Oral Health Assessment index, Dental Impact, Dental Impact on Daily Living, Oral Health Impact Profile, Oral Impacts on Daily Performances [9].

Through these instruments it is possible to recognize the different determinants that contribute to modify in a negative way the oral health status since its appearance depends on the conjugation of biological factors such as dental anatomy, diet where it is widely demonstrated the relationship between consumption and the appearance of oral diseases, both by historical evidence, observational, clinical studies and experimentation; socio-economic level, area of residence, educational level, occupation, housing characteristics, income, opportunities for general education, health, dental care as well as age and sex [17,4,14,8,19,6]

There are many risk factors and determinants of importance related to oral diseases and it is evident that the greater the degree of exposure to risk, the greater the probability of contracting or developing a condition [8], hence the importance of considering the present analysis that aims to determine some of the socioeconomic and dietary characteristics that directly influence oral health status. These may be considered as parameters that provide information on the normal or pathological state of an individual at a given time, a risk group and a specific place, in addition to helping to understand the oral health-disease process, in addition to establishing specific primary health care measures such as promotion, prevention, diagnosis, treatment and rehabilitation in a timely manner [2].

Therefore, the main contribution of this paper is to analyze as univariate models, individual demographic and dietary characteristics and the relationship

of these with a general oral health status, as well as how an interaction of these characteristics (as a multivariate model) with the general status.

The analysis is carried on using a multi objective logistic regression and evaluated using a Receiver Operating Characteristic (ROC) curve, which allows us to study the sensitivity and specificity of each characteristic, just as the model comprised by all the selected characteristics in order to explain the relationship between demographic and dietary features with the oral health status.

This paper is organized as follows, in section 2 is presented a description of the data set used for this research and methods to carry on the study. In section 3 the experimentation conditions are presented. Results from univariate and multivariate analysis are shown in section 4. Finally conclusions and future work is described in section 5.

2 Materials and Methods

In this section is described the data set of National Health and Nutrition Examination Survey (NHANES), patients selection and the methods used to carry on the univariate analysis.

2.1 Data set Description

The NHANES is a national program that design studies to perform a survey to assess the health and nutritional status of adults and children in the United States, including all ethnic groups. The survey combines interviews and physical examinations, allowing to develop studies using clinical, para-clinical and demographic characteristics (features) of individuals. NHANES is a program founded by the National Center for Health Statistics (NCHS), which is part of the Centers for Disease Control and Prevention (CDC) and has the responsibility for producing vital and health statistics for the Nation.

Content Description NHANES survey include several types of interviews, to cover a wide range of features, including demographic, socioeconomic, dietary, and health-related questions, described in detail in 1. One examination component that is critical to this study is dental care examination, which is carried on by trained medical personnel.

Table 1. NHANES data description.

Questionnaire Type	Description
Demographics	The demographics file provides individual, family, and household level information.
Examinations	Public health significance in areas of surveillance, prevention, treatment, dental care utilization, health policy, evaluation of Federal health programs.
Dietary	Total nutrient intake.
Laboratory	Laboratory tests, which includes Cholesterol, Fasting Questionnaire, Hepatitis Tests, HIV, Urinary tests.
Questionnaire	information on: Acculturation, Alcohol Use, Health Insurance, Income.
Medication	Past 30 days, used or taken medication.

Meta Data Health and Nutrition Examination Surveys are comprised by interviews applied to 27,631 persons. In Table 2 are described in detail the number of persons and the features/parameters of the groups included in the sample.

Table 2. Patient demographic information.

Characteristic	NHANES
Age of civilian	All ages from birth
Geographic areas	Unaited States
Average number of sample persons per household	2
Number of study locations	60
Domains for oversampling	Predesignated: 87 subdomains of sex-age groups for non-Hispanic black persons, non-Hispanic non-black Asian persons, and Hispanic persons. Oversampled: Hispanic persons, non-Hispanic black persons, non-Hispanic non-black.
Number of selected persons	27,631
Number of interviewed persons	20,491
Number of examined persons	19,644

2.2 Data Analysis

In this work, as mentioned before, were conducted an univariate and multivariate searches. The univariate search was conducted using the demographics and dietary features being subjected to a statistical analysis; while the multivariate search was conducted using the complete feature set, including the examinations features.

The statistical analysis consisted of submitting each of the features to a linear regression to obtain the univariate models; then, all features together developed a multivariate model trough a linear regression too.

Linear regression is an analysis which consists on a statistical technique for modeling the relationship between features. The simplest representation of a model obtained by this method is represented in Equation 1, where y is the dependent variable or the outcome feature, β_0 is the intercept, β_1 is the slope and x is the independent variable or the analyzed feature. Models can be composed by the number of terms needed. Finally, the difference between the real outcome and the outcome proposed by the model is the error of the model, ϵ; this variable

is known as a statistical error due to it's a random variable that measures the model failure for fitting the data exactly [16]:

$$y = \beta_0 + \beta_1 x + \epsilon. \tag{1}$$

The statistical validation consisted on obtaining the P-value, the odds ratio and the area under the receiver operating characteristic (ROC) curve, known as the AUC.

The P-value or the observance significance level is the smallest value obtained where the null hypothesis can be rejected [13]; while the AUC is a standard method to evaluate the accuracy of the classification model [12], finally, the odds ratio represents the ratio of the probability that an event of interest occurs against the probability that the same event doesn't occur [3].

All the data analysis were realized with the free software *R* (version 3.3.1) [20] and its packages, *pROC* (Version 1.8, 2015-06-10) [21], *epitools* (Version 0.5-7, 2012-09-30) [1], *ResourceSelection* (Version 0.2-6, 2016-02-15) [10] and *randomForest* (version 4.6-12, 2011-10-18) [11].

3 Experiments

The process realized in the univariate and multivariate models experimentation and their statistical analysis is described in this section. In Figure 1 is presented a flowchart of the followed methodology.

Firstly, the NHANES data analysis and the features selection for this research were realized by an expert dentist, according to the information obtained from the literature. Then, a new dataset with the extracted features was obtained (Figure 1 A)). Followed by a data preprocessing, where is initially described the imputation of missing data (Figure 1 B)) and then, for the univariate analysis, it was necessary removing the features that are unable to contribute meaningful information due to their contents. The univariate models development and models validation were realized in base of an statistical process (Figure 1 C)).

Finally, for the multivariate model development all features were taking into account and the model validation is also carried out (Figure 1 D)). The validation process is performed with the intention of evaluating the contributions of the results.

3.1 Dataset Preprocessing

The dataset used for this research was mostly contained by demographic and examination features, also a dietary feature was present [5] .

- Demographic features:
  - DMDMARTL: Describes the marital status,
  - INDFMIN2: Describes the annual family income,

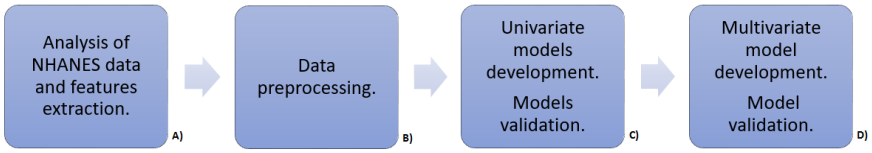


Fig. 1. Flowchart of the methodology followed. A) Dataset analysis and features extraction, B) Univariate models development and their statistical validation, C) Multivariate model development and its statistical validation.

  - RIAGENDR: Describes the gender of the participant,
  - DMDHHSIZ: Describes the total number of people in the household,
  - DMDEDUC3: Describes the education level on youths from 6 to 19 years,
  - DMDEDUC2: Describes the education level on adults from 20 years old.
- Dietary feature:
  - DR1TWS: Describes the tap water source.
- Outcome feature:
  - OHDEXSTS: Describes the overall oral health exam status (from 1 being complete to 3 being not done).

Examination features were initially removed for the univariate analysis, since they contain information about the health center where the patient was treated and each health center is represented by a different feature, therefore, each feature presents a large amount of missing data, becoming impossible to perform an univariate analysis for them.

The remaining features contained some missing values represented as Not a Number (NaN). These missing values were imputed through the $rfimpute$ function from $randomForest$ package, consisting on the substitution of NaN's for the value of the median of the column where the features are found.

3.2 Univariate Models Development and Models Validation

The development of the univariate models was realized by a linear regression process between each of the features and the outcome feature, which was related to the general status of oral health.

After the univariate models were obtained, they were subjected to an univariate statistical analysis, obtaining their P-values, odds ratios, AUC and ROC curves.

3.3 Multivariate Model Development and Model Validation

For the multivariate model development, which was realized by a linear regression between the feature set and the outcome feature, was also included the examination features that weren't used for the univariate analysis. The

information contained in the examination features was all joined in only one feature, avoiding problems in the model development because of the missing data, taking into consideration that for each patient these features only contained information in one of them, because they were related to the health center where the patients were attended and most of them were attended only in one.

Finally, for the multivariate model validation were obtained the P-value, AUC and ROC curve of the model. Odds ratio wasn't calculated for this model because this parameter is obtained for specific features and not for a set of them.

4 Results

Results obtained from the univariate statistical analysis are presented in Table 3, which is contained by every feature of the dataset and its respective P-value, odds ratio and AUC, in ascendant order according to the AUC values. For this analysis, features related with the health center where the patients were treated (examination features), weren't taken into account.

Table 3. Univariate statistical analysis.

Feature	P-value	AUC	Odds ratio	2.5%	97.5%
DMDMARTL	0.683	0.496	0.999	0.994	1.003
INDFMIN2	0.326	0.501	0.999	0.998	1.000
RIAGENDR	0.299	0.502	0.999	0.999	1.000
DMDHHSIZ	0.585	0.510	1.001	0.996	1.006
DMDEDUC3	0.744	0.521	1.005	0.997	1.003
DMDEDUC2	0.472	0.521	1.003	0.993	1.013
DR1TWS	0.101	0.540	1.000	0.999	0.101

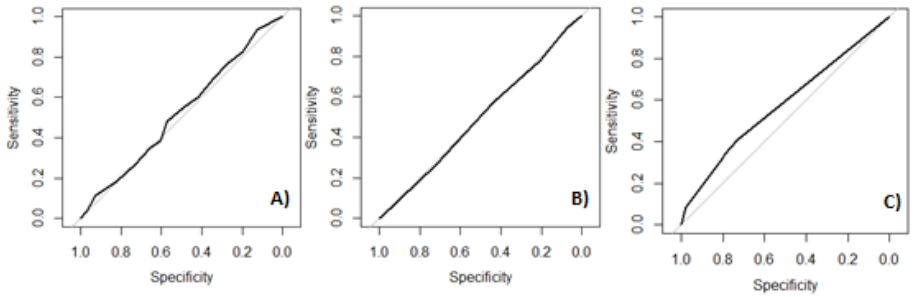


Fig. 2. ROC curves obtained from the most significant features in the univariate analysis, A) DMDEDUC3, B) DMDEDUC2, C) DR1TWS.

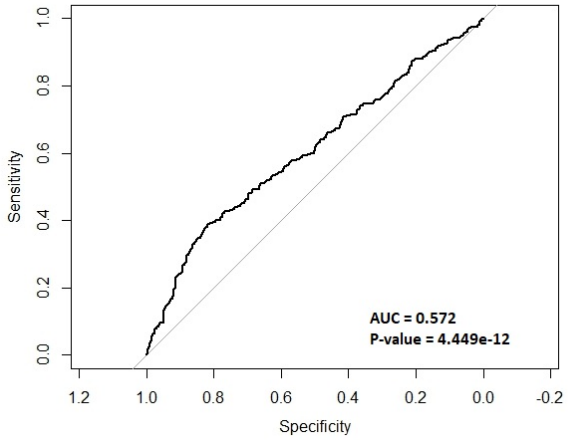


Fig. 3. ROC curve obtained from the multivariate analysis (AUC = 0.572, P-value = 4.449e-12).

From the univariate analysis results, the three most representative univariate models, according to their AUC values, present their ROC curves in Figure 2. In Figure 2 A) is shown the ROC curve of DMDEDUC3 feature, in Figure 2 B) is shown the ROC curve of DMDEDUC2 feature and in Figure 2, C) is shown the ROC curve of DR1TWS feature.

In multivariate statistical analysis, the ROC curve generated is shown in Figure 3, obtaining a P-value of 4.449e-12 and a value of AUC of 0.572. For this analysis, features related to the health center where the patients were treated (examination features) were taken into account.

5 Conclusion and Future Work

It is well known that the health problems that arouse the greatest interest are those that represent a risk of death or permanent disability, and carry with them the doubt as to the possibility of attacking a certain person.

Commonly, oral health problems do not arouse the spontaneous interest of the community, which is why identifying the determinants through such analysis in the population allows informing, educating and motivating appropriate oral health care because it depends on whether the population shows interest in receiving different treatments and thus improve oral health.

This analysis has shown that around a disease there are many factors that cause or aggravate it. When referring to the issue of socio-cultural health determinants (SHD) has become a latent concern for health professionals and oral health professionals since most of the problems derive from inequality or inequity

in health and are linked to other determinants which produce different effects in each risk group with respect to their conditions and lifestyle, generated in the short, medium or long term.

Demographic features that were used for this research showed that none of them can significantly predict the health status of the population in an univariate approach, this can be observed at the statistical analysis where all of the P-values were > 0.06, which is taken as the standard value to consider a feature to be significant; also, the AUC values and the ROC curves showed a similar result, since the higher AUC is 0.540, which means that the true positives / true negatives proportion is 54% for this specific feature, DR1TWS (dietary feature). Odds ratios didn't show a higher probability than 1 for any feature in relationship with a health condition. Although the predictive capacity of this feature is better than a blind test, its contribution isn't so statically significant.

Multivariate model showed better statistical results than univariate models. In this approach, where the examination or health centers features were also used, the P-value obtained, 4.449e-12, is statistically highly significant, which represents that the alternative hypothesis has a high probability of being true, it means that the model has an influence on the health condition. The AUC and the ROC curve presented a true positives / true negatives proportion of 57.2%, which is higher than the AUC values of the univariate models. The improvement of statistical values in the multivariate model allows to conclude that the demographic and dietary features can help to evaluate the health status in combination with the examination features. By this, it's possible to consider that social security, economic income, type of health service and other similar factors may help to determine the patient's health status, specifically the oral health, according to the data used for this work.

As future work is proposed add more dietary and medical condition features, but including a clever feature selection than can lead to a high AUC model cleaning features that can decrease specificity and sensitivity of a oral health prediction model, in addition, complex techniques of machine learning, as neural networks, elastic networks or similar can be used to tackle this problem.

References

1. Aragon, T.: EpiTools: Epidemiology Tools. R package version 0.5-7 (2016)
2. Arango, V., Sandra, S.: Biomarcadores para la evaluación de riesgo en la salud humana. Revista Facultad Nacional de Salud Pública 30(1), 75–82 (2012)
3. Bland, J.M., Altman, D.G.: The odds ratio. Bmj 320(7247), 1468 (2000)
4. Castañeda Abascal, I.E., Lok Castañeda, A., Molina, L., Manuel, J.: Prevalencia y factores pronósticos de caries dental en la población de 15 a 19 años. Revista Cubana de Estomatología 52, 21–29 (2015)
5. for Disease Control, C., Prevention, et al.: National health and nutrition examination survey, 2011-2012 (2013)
6. Escalona, T.P., Ortiz, H.R.C., Palomino, Y.P., Tamayo, M.I., Rodríguez, M.I.R.: 08-relación entre factores de riesgos y caries dental relationship between risk factors and dental caries. MULTIMED Revista Médica Granma 19(4) (2017)

7. Espinosa González, L.: Cambios del modo y estilo de vida; su influencia en el proceso salud-enfermedad. Revista Cubana de Estomatología 41(3), 0–0 (2004)
8. Gispert Abreu, E.d.l.Á., Castell-Florit Serrate, P., Herrera Nordet, M.: Salud bucal poblacional y su producción intersectorial. Revista Cubana de Estomatología 52, 62–67 (2015)
9. González, C.F., Franz, L.N., Sanzana, N.D.: Determinantes de salud oral en población de 12 años. Revista clínica de periodoncia, implantología y rehabilitación oral 4(3), 117–121 (2011)
10. Lele, S.R., Keim, J.L., Solymos, P., Solymos, M.P.: Package ResourceSelection (2017)
11. Liaw, A., Wiener, M.: The randomforest package. R News 2(3), 18–22 (2002)
12. Lobo, J.M., Jiménez-Valverde, A., Real, R.: Auc: a misleading measure of the performance of predictive distribution models. Global ecology and Biogeography 17(2), 145–151 (2008)
13. Martínez Abreu, J., Capote Femenias, J., Bermúdez Ferrer, G., Martínez García, Y.: Determinantes sociales del estado de salud oral en el contexto actual. MediSur 12(4), 562–569 (2014)
14. Martínez Abreu, J., Castell-Florit Serrate, P., Llanes Llanes, E., Morales Aguiar, D.R., Sánchez Barrera, O., et al.: Componente bucal y determinantes sociales en el análisis de la situación de salud. Revista Cubana de Estomatología 52, 53–61 (2015)
15. Medina Solís, C.E.: Políticas de salud bucal en México: disminuir las principales enfermedades. Una descripción (2006)
16. Montgomery, D.C., Peck, E.A., Vining, G.G.: Introduction to linear regression analysis. John Wiley & Sons (2015)
17. Narváez Chávez, A.M.: Asociación entre el conocimiento de los padres sobre salud bucal y uso de técnicas educativas con relación a la presencia de biofilm y caries en infantes. Master's thesis, Quito: UCE (2017)
18. Ojeda-Garcés, J.C., Oviedo-García, E., Salas, C.E.S.: Streptococcus mutans y caries dental. Odontologica 26(1) (2013)
19. Ospina, D., Herrera, Y., Betancur, J., Agudelo, H.B., López, A.P.: Higiene bucal en la población de san francisco antioquia y sus factores relacionados. Revista Nacional de Odontología 12(22), 23–30 (2016)
20. Ripley, B.D.: The R project in statistical computing. MSOR Connections. The newsletter of the LTSN Maths, Stats & OR Network 1(1), 23–25 (2001)
21. Robin, X., Turck, N., Hainard, A., Tiberti, N., Lisacek, F., Sanchez, J.C., Müller, M.: pROC: an open-source package for R and S+ to analyze and compare ROC curves. BMC bioinformatics 12(1), 77 (2011)

ISSN 1870-4069

Frequency Analysis of Honey Bee Buzz for Automatic Recognition of Health Status: A Preliminary Study

Antonio Robles-Guerrero[1], Tonatiuh Saucedo-Anaya[2], Efrén González-Ramírez[1], Carlos E. Galván-Tejada[1]

[1] Universidad Autónoma de Zacatecas, Unidad Académica de Ingeniería Eléctrica, Zacatecas, Mexico

[2] Universidad Autónoma de Zacatecas, Unidad Académica de Física, Zacatecas, Mexico

aroblesp@uaz.edu.mx, gonzalez_efren@hotmail.com, ericgalvan@uaz.edu.mx, tsaucedo@fisica.uaz.edu.mx

Abstract. The study of honey bee health has received special attention in the last years. Researchers has been monitoring physical variables to determinate the status of the colony. This is a first approach in the development of a real time monitoring system to provide useful information to beekeepers that will help them to prevent colony losses. This study presents an analysis of the sound from two colonies of bees in the Mel frequency domain. The first is a healthy colony with queen and the second one is a hive with no queen and with a reduced population. Sound samples were acquired for each colony and characterized using Mel Frequency Cepstral Coefficients (MFCC). To summarizes the information, statistical descriptors was obtained for each Mel coefficient. An exploratory analysis of samples revealed two different hive characteristics; the presence and lack of a queen bee. For honey bee buzz recognition, a Logistic Regression Model was used. The preliminary results show that it is possible to classify both characteristics obtaining high classification rates using a reduced set of features.

Keywords: honey bee, remote sensing, beehive monitoring, queenless state.

1 Introduction

Pollinators are essential for diet diversity, biodiversity, and the maintenance of natural resources. The honey bee is the most important pollinator. Approximately 73% world cultivated crops depend on some variety of bees [1]. The colony health is influenced by external factors, such as, increase of pathologies,

pollution, pesticides, among others. Monitoring honey bee health is an important task for beekeepers. Early detection of health status can be crucial to ensure the survival of the colony.

A queen bee plays an important role in a colony, she controls workers by releasing pheromones and produces eggs. Lost of the queen can result in the dead of the whole colony in a few months, unless a new queen is introduced.

In the last years researchers have been looking for non invasive methods for continuous monitoring and automatic detection of honey bee health status. Special attention has received the monitoring of physical variables, such as, temperature, humidity, sound, vibrations, colony weight, and gas contents [22]. The sound in bee hives has been analyzed for detecting the swarming period. Swarming is characterized by an increase of the power spectral density before it takes place. In [14], a method for predicting the swarming period is proposed based on labeling the sounds. [12], concluded that the noise generated by bees has a high probability of correspondence to the physiological state. There are patented devices to determinate the honey bee health by comparing a captured hive sound with known acoustic fingerprints of a healthy colony [5].

Changes in sound due to Varroa mite infestation have been investigated by [19], where his prediction accuracy is claimed to be better than any random guessing, although results are not validated. The queenless state has been investigated by using spectrograms [16]. Analysis results were classified by using a Kohonen Self Organising Map and artificial neural networks. Although [16], found the frequency characteristics for each condition their results were not satisfactory.

The aim of this research work is to propose a methodology based on MFCC and Machine Learning for automatic recognition of the status of a honey bee colony based on sound recording, The proposed methodology can be implemented in dedicated devices to detect the presence or absence of the queen bee avoiding invasive inspection of the colony. Furthermore, more conditions can be analyzed by using the same estrategy.

The rest of the paper is organized as follows: in section 2 a detailed description of the data set acquisition and the methodology for feature extraction is presented. In section 3, the process for feature selection and model validation is described. The paper ends in section 4 by presenting conclusion and future work.

2 Materials and Methods

2.1 Honeybee Monitoring System

Based on previous works [10,7,11], a monitoring system was developed based on a Raspberry Pi 2 model B, figure 1. Sound samples were acquired by using omnidirectional electret microphones placed inside the hives. Microphones were protected by a metallic mesh to avoid them begin covered with wax. The main idea was keeping the system as simple as possible with only a microphone by

hive. The signal was acquired and converted to a digital signal by using a dspic microcontroller with a 12-bits resolution ADC. The system was 10000 mAh battery powered allowing an autonomy of about 24 hrs.

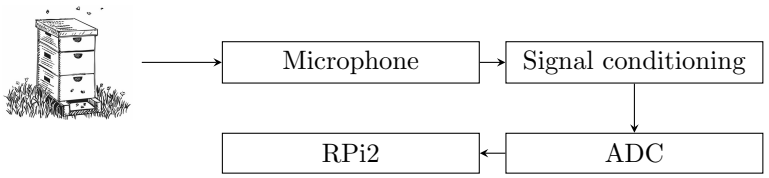


Fig. 1. System overview.

2.2 Data Set Description

Sound samples were extracted from two colonies of Carniolan honey bee (*Apis mellifera carnica*). The first colony has a queen with a large population, and the second one is a queenless colony with a reduced population. Colony population were compared only by visual examination, however a quantitative method for measuring the population is necessary. The beehives were protected with insulation material against low temperatures (low temperature is quite common in Zacatecas city).

Various researchers have reported the range of frequencies of the acoustic signals produced by a honey bee colony are in the range from 100 to 1 kHz [2,18], and that most of the sound have frequencies around 300, 410 and 510 Hz [9]. The sampling frequency for this investigation was set up to 4 kHz to get a good quality representation of the sound activity without increasing the storage requirements; this is the double of the minimum of Nyquist frequency required. [18] showed that frequency of the sound changes slowly along the day. To evaluate the evolution of the frequencies, 3 min of sound of the honey bee buzz were recorded every 15 min for 24hrs. The experiment for data acquisition was carried out during 45 days (beginning of mid-April to May).

2.3 Feature Extraction

MFCC is one of the most important technique for feature extraction in speak recognition. Although MFCC is used for human sound perception, in this work it is proposed for sound bee characterization because of its effectiveness reported in others areas (i.e. sound genre classification [21] and environmental sounds recognition [8]). The MFCC transforms the raw signal into a compact series of parameters representing the original signal. Figure 2 shows the process of feature extraction: (i) the wave form is first passed through a pre-emphasis filter, (ii) the signal is divided into frames of short duration (typically 25 ms), (iii) each frame

is multiplied by a hamming windows, (iv) the Fast Fourier transform (FFT), is calculated for each frame, (v) the power spectrum is warped according the Mel-scale, (vi) the spectrum is segmented according to a triangular filter bank, and finally (vii) the coefficients are computed by applying an Discrete Cosine Transformation (DCT), to the logarithm of the filter bank output.

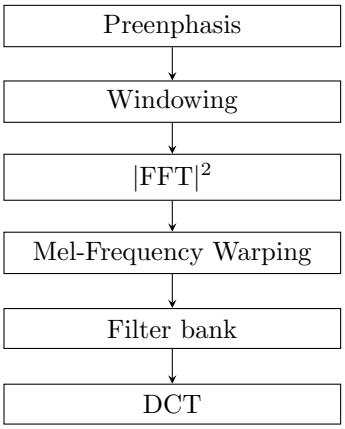


Fig. 2. MFCC feature extraction methodology.

3 Results

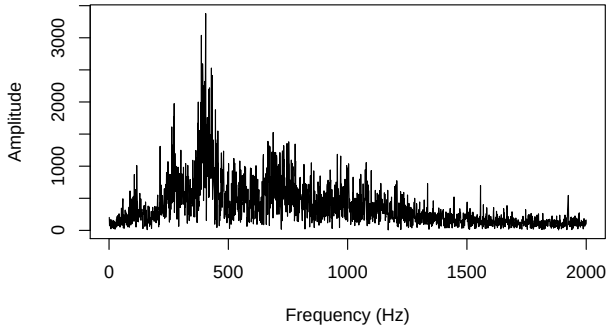
3.1 Feature Extraction and Preprocessing

The samples shown in Figure 3, correspond to sound recorded during the afternoon of a spring day in May. Figure 3(a) shows the frequency bands of the healthy colony; most of the sound activity is present around 400 Hz. On the other hand, in figure 3(b), the queenless colony present a different pattern; the emitted sound is distributed in more frequency bands.

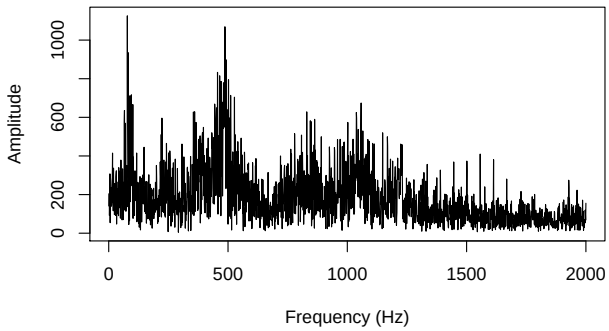
The MFCC were computed from 88 instances of sound captured from the colony with queen and 98 from the queenless colony. These data come from 24 hrs of recording. The difference between recorded instances were due to the non-equal battery life of the two recorders. The parameters of the MFCC calculation were: window size of 25 ms (in this period of time the signal is considered quasi stationary), and with 10 ms of overlapping, the pre-emphasis value was set to 0.94. Those values are typically used in speech recognition.

After the MFCC extraction were carried out, and in order to reduce the data set size and computational cost for each Mel coefficient, the following statistical descriptors were computed:

– mean,



(a) Healthy colony.



(b) Unhealthy colony.

Fig. 3. Comparison of the frequency spectrum of the healthy and unhealthy colonies.

- trimmed mean (20%),
- kurtosis,
- standard deviation,
- skewness,
- median,
- variance,
- coefficient of variation,
- quantiles (2.5, 25, 50, 75, 97.5).

The resulting data set is composed of 168 features and 186 instances. Two classes were chosen in this work: healthy and unhealthy colony.

After feature extraction standardization was performed over data; it scales data in function of the mean (μ) and the standard deviation (σ):

$$z = \frac{x - \mu}{\sigma}. \tag{1}$$

This process reduces the effects of the different distributions [6].

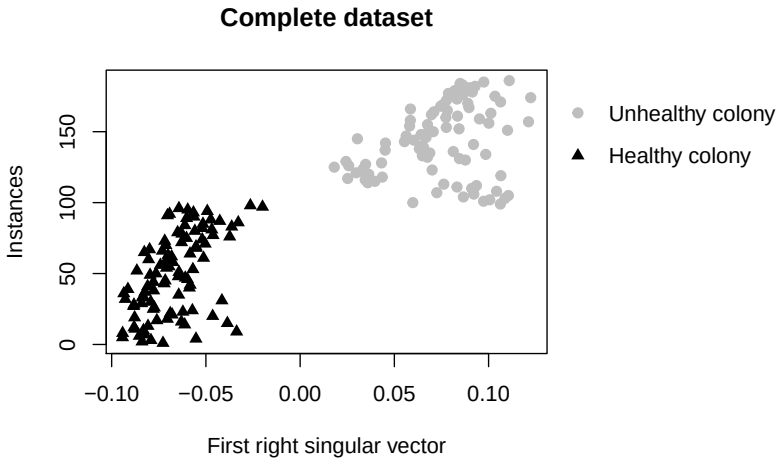


Fig. 4. SVD of the complete data set.

3.2 Feature Selection

An exploratory analysis was conducted on R Project software [20]. The first analysis carried out was a Singular Value Decomposition (SVD). SVD computes the set of eigenvalues and eigenvectors of a matrix. It is a common technique in the analysis of multivariate data that can reveal structures in the data set that may be useful for classification. The SVD analysis of the data set is shown in figure 4. The black triangle (▲) corresponds to the colony with queen and the gray circle (•) is the queenless colony. The samples are grouped forming well defined clusters, evidencing two conditions clearly distinguishable.

Not all the features are useful. In order to find features that best describe the conditions of the hives, a SVD analysis was conducted on each statistical descriptor (figure 5). Mean, trimmed mean, median, coefficient of variation and quantiles, form similar clusters. In the rest of the descriptor the cluster are mixed, and they might not be useful to make a good prediction.

By visual examination it was determined that one statistical descriptor is enough to make a good prediction; the mean values of the MFCC were selected. The free package *randomForest* (v4.6-12) [17] R Project Software was used to evaluate the importance of each feature in mean descriptor. Random Forest is a combination of tree predictors such that each of them depends on the values of a random vector sampled independently with the same distribution in the forest [4]. The result of the random forest evaluation is shown in Figure 7. The most important features are mean of Mel coefficient 4 and 10.

3.3 Validation

In order to validate the model the dataset was divided into two parts: a training set (70%), that was used to train a Logistic Regression model and a test set

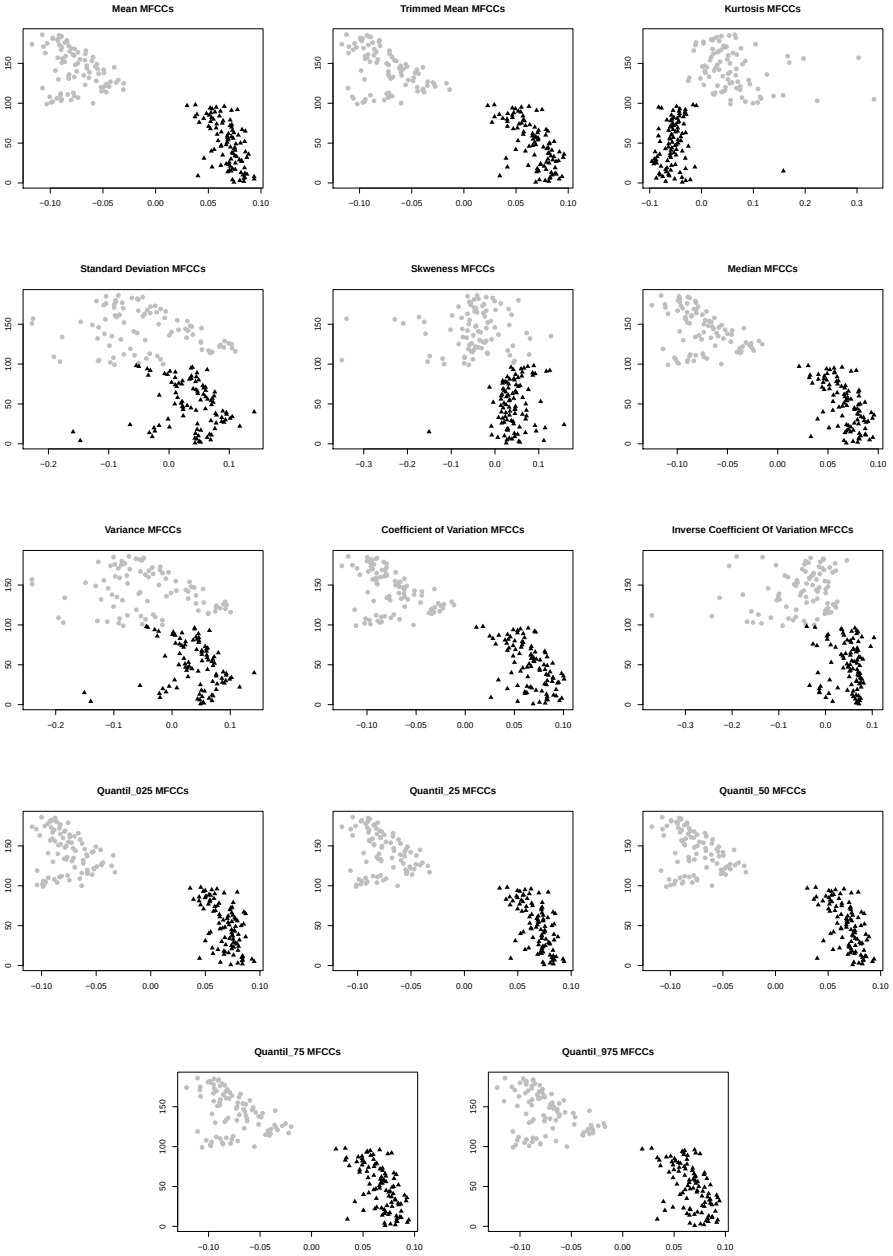


Fig. 5. Singular value decomposition of each statistical descriptor, the black triangle (▲) corresponds to healthy colony and gray circle • to unhealthy colony.

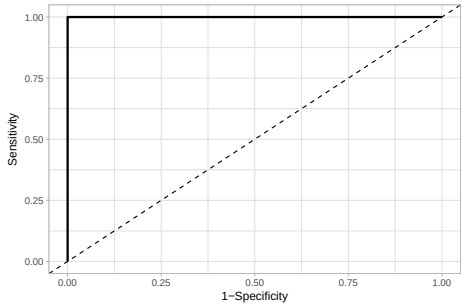


Fig. 6. ROC curve using two features.

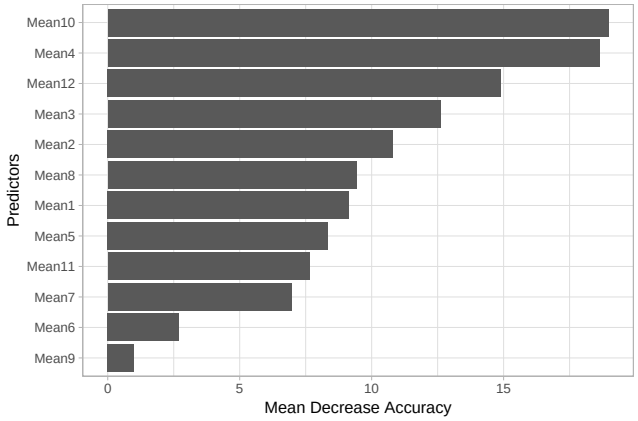


Fig. 7. Features in order of importance.

(30%), that was used to measure the model performance predictor. To evaluate the model performance a ROC curve was obtained. Receiver Operative Characteristics (ROC), analysis is a well known model performance measure for machine learning algorithms [13,15,3]. The ROC curve is a plot of true positives against false positive. The plot shows the number of correctly classified samples versus the number of incorrectly classified negative samples. A perfect classifier is reflected by a curve which lies in the upper left corner with an unitary area under the ROC curve. In figure 6, it is shown the ROC curve of the model. To achieve a perfect classification only two features were enough; mean values of Mel coefficients 4 and 10.

4 Conclusion and Future Work

The proposed methodology based on Mel Frequency Cepstral Coefficients and machine learning algorithms suggests that it can be effectively used for honey

bee status recognition by sound analysis. However, data analysis from more hives are needed in order to confirm these results.

The FFT of the sound signal from a beehive with queen shows a characteristic pattern around 400 hz that is different from that obtained from a beehive with no queen. The patter found in a queenless colony shows a different frequency distribution. Data for this research were obtained during a month and a half period.

In the model validation only two features were necessary to achieve a perfect prediction, however, more research with more beehives is needed for a better evaluation of the predictor performance

Future work will include the reduction of the number of instances and the recording time to have optimal values. This will reduce the storage space required and the computational cost on a dedicated device. It is also important, as future work, to find otjer patterns of specific health status of honey bees; such as, pre-swarming behavior, varroa mite infection, size population, among others. With this information it will be possible to create a database and a system able to identify the health status of a colony.

Acknowledgments. We thank for the partial support in the development of this project to CONACYT.

References

1. Abrol, D.P.: Pollination Biology: Biodiversity conservation and agricultural production. Springer Netherlands, Dordrecht, 1 edn. (2011), http://www.sciencedirect.com/science/article/pii/B9780125839808500193 http://link.springer.com/10.1007/978-94-007-1942-2
2. Bencsik, M., Bencsik, J., Baxter, M., Lucian, A., Romieu, J., Millet, M.: Identification of the honey bee swarming process by analysing the time course of hive vibrations. Computers and Electronics in Agriculture 76(1), 44–50 (2011), http://dx.doi.org/10.1016/j.compag.2011.01.004
3. Bradley, A.P.: The use of the area under the ROC curve in the evaluation of machine learning algorithms. Pattern Recognition 30(7), 1145–1159 (1997), http://linkinghub.elsevier.com/retrieve/pii/S0031320396001422
4. Breiman, L.: Random Forests. Mach. Learn. 45(1), 5–32 (2001), https://doi.org/10.1023/A:1010933404324
5. Bromenshenk, J.J., Henderson, C., Seccomb, R., Rice, S., Etter, R.: Honey bee acoustic recording and analysis system for monitoring hive health (2009), http://www.google.com/patents
6. Brownlee, J.: Machine Learning Mastery with R. Melbourne, Australia (2017)
7. Chen, W.S., Wang, C.H., Jiang, J.A., Yang, E.C.: Development of a monitoring system for honeybee activities. In: Proceedings of the International Conference on Sensing Technology, ICST. vol. 2016-March, pp. 745–750. Taiwan (2016)
8. Chu, S., Narayanan, S., Kuo, C.C.J.: Environmental Sound Recognition With Time-Frequency Audio Features. IEEE Transactions on Audio, Speech, and Language Processing 17(6), 1142–1158 (aug 2009), http://ieeexplore.ieee.org/document/5109766/

9. Dietlein, D.G.: A method for remote monitoring of activity of honeybee colonies by sound analysis. Journal of Apicultural Research 24(3), 176–183 (1985)
10. Edwards-Murphy, F., Magno, M., O'Leary, L., Troy, K., Whelan, P., Popovici, E.M.: Big brother for bees (3B) - Energy neutral platform for remote monitoring of beehive imagery and sound. In: Proceedings - 2015 6th IEEE International Workshop on Advances in Sensors and Interfaces, IWASI 2015. pp. 106–111 (2015)
11. Edwards-Murphy, F., Srbinovski, B., Magno, M., Popovici, E.M., Whelan, P.M.: An automatic, wireless audio recording node for analysis of beehives. 2015 26th Irish Signals and Systems Conference, ISSC 2015 pp. 1–6 (2015)
12. Eskov, E.K., Toboev, V.A.: Changes in the structure of sounds generated by bee colonies during sociotomy. Entomological Review 91(3), 347–353 (2011)
13. Fawcett, T.: An introduction to ROC analysis environments support. Pattern Recognition Letters 27(8), 861–874 (2006), http://linkinghub.elsevier.com/retrieve/pii/S016786550500303X
14. Ferrari, S., Silva, M., Guarino, M., Berckmans, D.: Monitoring of swarming sounds in bee hives for early detection of the swarming period. Computers and Electronics in Agriculture 64(1), 72–77 (2008)
15. Hand, D.J., Till, R.J.: A Simple Generalisation of the Area Under the ROC Curve for Multiple Class Classification Problems. Machine Learning 45(2), 171–186 (2001)
16. Howard, D., Duran, O., Hunter, G., Stebel, K.: Signal Processing the acoustics of honeybees (APIS MELLIFERA) to identify the "queenless" state in Hives. Proceedings of the Institute of Acoustics 35, 290–297 (2013)
17. Liaw, A., Wiener, M.: Classification and regression by randomForest. R News 2(3), 18–22 (2002), http://cran.r-project.org/doc/Rnews/
18. Pérez, N., Jesús, F., Pérez, C., Niell, S., Draper, A., Obrusnik, N., Zinemanas, P., Spina, Y.M., Letelier, L.C., Monzón, P.: Continuous monitoring of beehives' sound for environmental pollution control (2016)
19. Qandour, A., Ahmad, I., Habibi, D., Leppard, M.: Remote Beehive Monitoring Using Acoustic Signals. Acoustics Australia 42(3), 204–209 (2014)
20. R Core Team: R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria (2017), https://www.r-project.org/
21. Tzanetakis, G., Cook, P.: Musical Genre Classification of Audio Signals. IEEE Transactions on Speech and Audio Processing 10(5), 293–302 (2002)
22. Zacepins, A., Brusbardis, V., Meitalovs, J., Stalidzans, E.: Challenges in the development of Precision Beekeeping. Biosystems Engineering 130, 60–71 (2015)

Impreso en los Talleres Gráficos
de la Dirección de Publicaciones
del Instituto Politécnico Nacional
Tresguerras 27, Centro Histórico, México, D.F.
Octubre de 2017
Printing 500 / Edición 500 ejemplares