Universidad Autónoma de Querétaro
Facultad de Informática
Maestría en Sistemas Computacionales

Sistema para reconocimiento de actividad humana mediante el análisis de señales WiFi

Tesis

Que como parte de los requisitos para obtener el Grado de
Maestría en Sistemas Computacionales

Presenta:
Alejandro Velázquez Luna

Dirigido por:
MCC. Alberto Lamadrid Álvarez

M.C.C. Alberto Lamadrid Álvarez Presidente	Firma
M.C.C. Ricardo Chaparro Sánchez Secretario	Firma
Dra. Ma. Teresa García Ramírez Vocal	Firma
M.C.C. José Arturo Gaona Cuadra Suplente	Firma
M.A. Jesús Desantiago Durán Suplente	Firma

M.I.S.D Juan Salvador
Hernández Valerio
Director de la Facultad

Dra. Ma. Guadalupe Flavia
Loarca Piña
Director de Investigación y Posgrado

Centro Universitario
Querétaro, Qro.
Noviembre, 2018
México

Resumen

Hoy en día en México es común encontrar sitios en los cuales se dispone de conexión a internet mediante alguna red inalámbrica a la cual se conectan dispositivos de todo tipo como teléfonos inteligentes, tabletas, computadoras, etc. En los últimos años el uso de redes LAN inalámbricas se ha incrementado de manera exponencial al tiempo que se han vuelto cada vez más complejas permitiendo una velocidad de intercambio de datos cada vez mayor. Aunque este tipo de redes no precisan de cables para conectarse a ellas, los datos requieren un medio físico para transmitirse, en el caso de las redes LAN tradicionales el medio de transmisión son cables, mientras que en las redes inalámbricas puede ser luz infrarroja u ondas de radio. La creación de redes LAN inalámbricas para el intercambio de datos se remonta décadas atrás sin embargo aquellas primeras redes eran diseñadas para conectar algunas estaciones predeterminadas y no tenían las prestaciones de interoperabilidad que conocemos hoy en día. Para hacer posible la convivencia de distintos tipos de dispositivos de diferentes marcas en una misma LAN inalámbrica fue necesario llegar a una estandarización. En 1997 el IEEE liberó la primera versión del estándar IEEE 802.11 que dio la posibilidad de implementar las redes WiFi que conocemos hoy en día. Actualmente las redes IEEE 802.11 tienen una robustez tal que es posible intercambiar secuencias de datos complejas tales como audio y video a muy alta velocidad entre dispositivos muy variados. Los estándares y la electrónica han avanzado lo suficiente para lidiar con las afectaciones que sufren las ondas de radio en su viaje de un dispositivo a otro sin embargo esto no quiere decir que estas afectaciones hayan dejado de existir. Una de estas afectaciones es la atenuación entre el trasmisor y receptor debida a diferentes factores como los obstáculos y la distancia. Si se considera que la atenuación es debida entre otras cosas a los obstáculos, entonces puede usarse para la detección de personas en un área determinada. Este trabajo trata del uso del receptor WiFi de una Raspberry Pi 3B para capturar las variaciones en la potencia de la señal proveniente de algún punto de acceso y mediante el procesamiento adecuado de esas variaciones determinar si existe presencia de personas en un área determinada.

Summary

Nowadays in Mexico is a common thing to find places with internet access connection by wireless networks to which is possible to connect different kind of devices like smartphones, tables or computers. In recent years the use of wireless LAN networks has increased exponentially as the have become increasingly complex allowing an increasing speed of data exchange. Although this kind of networks do not need cables to connect them, data still requires a physical medium to be transmitted through, in the case of traditional LANs the medium was cables, while in wireless networks it can be infrared light or radio waves. The creation of wireless LANs goes back decades, however, the first networks were designed to connect some predetermined stations and did not have the advantages of interoperability we know today. To make possible the coexistence of several types of devices of different vendors in the same LAN it was necessary to reach a standardization. In 1997 the IEEE released the first version of IEEE 802.11 standard by which was possible to implement the WiFi networks we know today. At present time the IEEE 802.11 networks have such a robustness that it is possible to exchange complex data sequences such as audio and video at a very high speed between very varied devices. The standards and the electronics had advanced enough to deal with affectations suffered by radio waves when it goes from one device to another, however, it does not mean these effects do not exist anymore. One of these affectations is the attenuation between the transmitter and the receiver due to factors such as distance and obstacles. Signal attenuation is due to among other things to obstacles, then it can be used for people detection in a certain area. This work deals with the use of Raspberry Pi 3B WiFi receiver to capture the variations in the signal power coming from an access point and through the appropriate processing of these variations determine if there is presence of people in a certain area.

Dedicatoria

A mis familiares, seres queridos y amigos.

Agradecimientos

A DIOS por permitirme seguir en este camino.

Muchas veces durante la realización de este trabajo fue necesario sacrificar tiempo que estaba destinado a familiares, seres queridos y amigos. Agradezco a ellos su compresión, paciencia, tiempo, consejos y conocimientos para cursar el posgrado y para la realización de este trabajo.

A mis compañeros de posgrado que estuvieron compartiendo este proceso conmigo apoyándome con los datos e información necesaria en el momento justo.

A mis profesores que me apoyaron en los momentos de mayor exigencia en el trabajo y el posgrado, gracias a todo el grupo de doctores que tuvieron siempre la paciencia para ayudar en lo que hacía falta, en especial a mi asesor el MCC. Alberto Lamadrid Álvarez por el apoyo que me brindó. Agradezco también al MCC. Ricardo Chaparro Sánchez por su compartirme sus conocimientos que fueron fundamentales para la realización de este trabajo. De igual manera agradezco el apoyo de la Dra. Teresa García Ramírez por el apoyo y comprensión para la revisión de este documento.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) por la beca recibida para llevar a cabo mis estudios de posgrado.

Índice

Índice de tablas

Índice de figuras

1. Introducción

La detección de las diferentes variables en la naturaleza con una capacidad mayor a la de los sentidos humanos ha sido una necesidad constante que se acentúo desde la revolución industrial. Ésa época trajo consigo la creciente automatización de procesos industriales para lo cual fue necesario contar con artefactos que pudieran hacer mediciones de diferentes variables como temperatura, presión, fuerza, movimiento, pH, etc. Fue así como surgieron los primeros sistemas de sensado, que convertían una magnitud física en otra, por ejemplo, presión en desplazamiento o temperatura en fuerza.

En la actualidad el concepto de sensor está en su mayoría ligado artefactos que convierten alguna magnitud física en otra de tipo eléctrico como corriente, tensión o resistencia. Esto es así porque representa un problema sencillo acondicionar las magnitudes eléctricas para que posteriormente sean procesadas por algún tipo de computadora de acuerdo con Fraden, (2010) .

En este trabajo la magnitud de interés es el movimiento. Específicamente interesa la detección de movimiento humano, para éste propósito existen desde hace décadas diferentes dispositivos basados en distintas tecnologías, las más comunes son: sensores piroeléctricos, de ultrasonidos, microondas y fotoeléctricos. Fraden, (2010).

Los sensores basados en el efecto piroeléctrico detectan fuentes de calor tales como el cuerpo humano o animales. Realizan la detección comparando las diferencias de temperatura entre los elementos biológicos y el ambiente que los rodea.

Los sensores basados en microondas hacen uso del Efecto Doppler para detectar presencias. Básicamente lo que hacen es emitir ondas de radio que rebotan en los objetos y regresan a la fuente emisora, entonces se mide la diferencia entre la onda emitida y la onda reflejada para conocer la ubicación del objeto. Pallás-Areny y Webster, (2001).

Los sensores basados en ultrasonidos en cierta forma son parecidos a los basados en microondas, la diferencia es que las ondas no son electromagnéticas sino acústicas. Se aprovechan también del efecto Doppler para detectar presencias. Fraden, (2010).

Las cámaras digitales son una de las aplicaciones más populares de los sensores fotoeléctricos. Actualmente se pueden encontrar en gran parte de dispositivos de comunicación y de info-entretenimiento como teléfonos inteligentes, tabletas, etc. La detección de movimiento en este caso se hace procesando las imágenes generadas por las cámaras digitales mediante algoritmos de Procesamiento Digital de Imágenes.

Este trabajo de investigación trata de la detección y clasificación de actividad humana mediante el procesamiento de las variaciones en las ondas de radiofrecuencia emitidas por los módems inalámbricos WiFi de uso doméstico.

1.1 Estado del arte

El análisis de las variaciones en la potencia de las señales de radio entre un emisor y un receptor para detección de presencia ya ha sido propuesto por Puccinelli et al., (2011) para realizar conteos de personas en espacios abiertos. En otro caso Lee et al., (2009) explora la factibilidad de usar el mismo principio aprovechando las ondas de radio en Redes de Sensores Inalámbricos para detectar intrusión de personas logrando caracterizar las variaciones en la potencia de la señal y traducirlas en información suficiente que corresponde con actividad humana. En otra investigación similar Lin et al., (2011) han logrado confirmar experimentalmente que las variaciones significativas en la intensidad de una señal de radio debidas a movimiento humano pueden ser usadas para implementar conteos de personas en espacios cerrados. Mediante el procesamiento de muestras de variaciones en la potencia de la señal de varios nodos distribuidos en entornos cerrados Kaltiokallio et al., (2010) demostraron que es posible detectar personas e incluso realizar la localización y seguimiento de las mismas. En años recientes investigadores como Pu et al., (2013) han ido más allá logrando hacer un reconocimiento gestual.

Para llevar a cabo investigaciones sobre este tema, el primer reto a resolver es realizar la captura de muestras de variaciones en intensidad de la señal WiFi. En este aspecto los investigadores han optado por diferentes enfoques, Pu et al., (2013) utilizan hardware muy especializado para realizar mediciones del Efecto Doppler de la señal percibida por el receptor detectando de esta manera no sólo variaciones en la intensidad sino también la reflexión. Otros investigadores como Wei et al., (2015) analizan la propiedad RSSI de la señal WiFi la cual es en

sí misma un indicativo de la potencia de la señal percibida por el receptor. Sin embargo, Lin y Yue, (2015) recomiendan usar la propiedad CSI de las señales WiFi debido a que el análisis de solamente las variaciones en la potencia/intensidad de la señal podrían no aportar suficientes detalles como para lograr hacer una detección y clasificación de movimientos finos sino solamente detección de movimientos burdos. Otro enfoque más recientemente usado por Tan y Yang, (2016) y Wu y Huang, (1999) consiste en analizar la propiedad CSI medir variables adicionales como por ejemplo, dispersión, atenuación y disipación de la potencia con la distancia siendo posible detectar movimientos finos, Zhang et al., (2016) ha logrado incluso hacer una identificación personal basada en los perfiles de movimiento únicos en cada persona. Sin embargo, para hacer la captura de las variables adicionales mencionadas es necesario hardware y software especializados.

1.2 Definición del proyecto de investigación

El aprovechamiento de las ondas de radiofrecuencia generadas por los módems WiFi para detección de presencias es un tema muy investigado en años recientes. La naturaleza de la señal WiFi posee diferentes propiedades que se pueden medir para detectar presencia, algunas de estas propiedades como el RSSI aportan poca información en comparación otras como el CSI, sin embargo, medir esta última requiere de hardware y software especializado no disponible para esta investigación. En este trabajo hace un análisis las variaciones en el RSSI debidas a la interferencia provocada por algún tipo de actividad dentro de un espacio controlado, el procesamiento requerido para hacer una detección y clasificación de actividad humana se llevará a cabo en un sistema embebido Raspberry Pi 3.

1.3 Justificación

En el mundo actual se producen movimientos sociales todos los días a nivel de países provocando cambios en el estilo de vida de muchas personas. Uno de los efectos de estos cambios sociales es la inseguridad pública López, (2013), esto ha llevado a que la población busque soluciones que protejan sus espacios personales propiciando con esto el desarrollo de tecnologías para la vigilancia de dichos espacios.

Desde hace décadas están disponibles de manera comercial diferentes dispositivos capaces de detectar indicios de actividad mediante el uso de ondas de radiofrecuencia. Sin embargo, la gran mayoría de estos dispositivos funcionan a base de un emisor de ondas y un receptor que detecta y procesa las afectaciones en dichas ondas para detectar actividad. Por otro lado, es importante hacer notar que hoy en día existen en muchos lugares de reunión módems inalámbricos para acceso a internet mediante WiFi, los cuales en sí mismos son una fuente emisora de ondas de radiofrecuencia. En este trabajo se aprovecha la existencia de estas ondas para detectar las variaciones en las mismas y determinar indicios de actividad humana en un espacio controlado.

1.4 Objetivos

1.4.1 Objetivo general

- Este trabajo tiene como objeto crear un sistema que haga posible la detección de actividad humana mediante el análisis de la propiedad RSSI de la señal WiFi.

1.4.2 Objetivos específicos.

- Desarrollar hardware y/o software para capturar las variaciones potencia de la señal WiFi.
- Desarrollar algoritmos necesarios que permitan filtrar los datos obtenidos de las variaciones de potencia.
- Proponer un algoritmo clasificador que recibirá como entrada los datos filtrados de variaciones de potencia y dará como resultado una detección de la actividad realizada por una presencia humana.

2. El Estándar IEEE 802.11

WiFi es una tecnología que hace posible la conexión e intercambio de datos entre dispositivos de manera inalámbrica mediante ondas de radio. La WiFi Alliance define como dispositivos WiFi todos aquellos "productos de Red de Área Local (WLAN) que estén basados en los estándares 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)" Wi-Fi Alliance, (2016).

2.1 Versiones del estándar IEEE 802.11

Las actividades de estandarización del IEEE están organizadas por *proyectos* a los cuales se les asigna un número. El proyecto de redes de comunicación más conocido es el IEEE 802 que se encarga del desarrollo de estándares para redes de área local (LAN). Dentro de un proyecto existen además *grupos de trabajo* individuales que desarrollan estándares para resolver aspectos particulares de un problema. A estos grupos de trabajo también se les asigna un número el cual es escrito después del punto decimal del correspondiente proyecto. Así, por ejemplo, Ethernet que es el proyecto de tecnologías LAN más ampliamente conocido fue estandarizado por el tercer grupo de trabajo y por lo tanto el estándar recibió el número 802.3. Por su parte, las redes LAN inalámbricas fueron estandarizadas por el onceavo grupo de trabajo y por lo tanto recibieron el número 802.11. IEEE, (2010).

Dentro de un grupo de trabajo se conforman *grupos de tarea* con el objetivo de revisar aspectos muy específicos de un estándar. A los grupos de tarea se les asigna una letra que se une al número de grupo de trabajo. Algunas letras que se pueden prestar con confusión no son usadas, por ejemplo, la letra "l" puede confundirse con el número "1" y por lo tanto no se usa en los nombres de estos estándares. En las redes inalámbricas, el primer grupo de tarea que ganó notoriedad y reconocimiento fue el "b" que produjo la especificación IEEE 802.11b. IEEE, (2010).

2.1.1 IEEE 802.11-1997

La versión original del estándar IEEE 802.11 fue liberada en 1997 pero es obsoleta actualmente. Esta versión especificaba velocidades de transmisión de 1 o 2 Mbit/s. Especificaba 3 tipos de tecnologías para la capa física:

- Luz infrarroja (IR) a 1 Mbit/s
- Espectro Expandido por Salto de Frecuencia (FH o FHSS) a 1Mbit/s o 2 Mbit/s
- Espectro Expandido por Secuencia Directa (DS o DSSS) a 1Mbit/s o 2 Mbit/s

De las tres mencionadas, las últimas dos tecnologías usan ondas de radio para trasmitir en la banda de frecuencia ISM a los 2.4 GHz. Aunque la tecnología de luz infrarroja continúa siendo parte del estándar IEEE 802.11 actualmente sus implementaciones prácticas son muy escasas. Esta primera versión del estándar podría considerarse más como una versión “beta” que como una especificación real. Una de las debilidades de esta versión es que era demasiado abierta provocando que muchos fabricantes de dispositivos WiFi flexibilizaran tanto el estándar que al final había dispositivos no compatibles entre diferentes redes WiFi. J.Berg, (2011).

2.1.2 IEEE 802.11b

La versión IEEE 802.11b tiene como máximo una velocidad de transmisión de 11 Mbit/s. Alrededor del año 2000 aparecieron los primeros productos comerciales bajo el estándar 802.11b los cuales presentaban un incremento significativo en el desempeño comparados con el estándar original (IEEE 802.11-1997) además de una reducción substancial en el precio, esto condujo a la rápida aceptación del estándar 802.11b como la opción definitiva para el comienzo de la tecnología LAN inalámbrica. J.Berg, (2011).

2.1.3 IEEE 802.11a

La versión 802.11a fue liberada en el año 1999 y usa el mismo protocolo que el estándar original y fue la primera en operar en la banda de los 5 GHz. Además de las tres tecnologías existentes para la capa física (FH, DS, IR) agregaba la Multiplexación de frecuencias ortogonales

(OFDM) con la cual típicamente alcazaba velocidades de hasta 20 Mbit/s. Esta versión no es compatible con la versión 802.11b debido a que operan en diferentes frecuencias. Sin embargo, los APs actuales tienen capacidad multibanda.

El uso de la banda 5 GHz tiene la ventaja de evitar los posibles conflictos con otro tipo de tecnologías y dispositivos que transmiten en la banda ISM de 2.4 GHz. Sin embargo, la frecuencia de 5 GHz tiene la desventaja de que las señales no pueden penetrar tan lejos como en los 2.4 GHz porque son absorbidas más fácilmente por paredes u objetos sólidos y además porque de acuerdo con ciertos principios físicos la perdida de la potencia de señal es proporcional al cuadrado de la frecuencia de la misma.

La confusión entre la precedencia de los estándares 802.11a y 802.11b es algo común. Los productos comerciales de la versión 802.11a tuvieron un cierto retraso en salir al mercado debido a que los componentes de 5 GHz eran más difíciles de fabricar. Adicionalmente el desempeño de la primera generación de estos productos era deficiente y con muchos problemas. Mientras esto pasaba, los productos comerciales de la versión 802.11b ya estaban disponibles. Para cuando la segunda generación de productos 802.11a comenzó a aparecer, la versión 802.11b ya había sido ampliamente adoptada. Sin embargo, tiempo después la versión 802.11a tuvo una gran aceptación en el ámbito empresarial y de negocios debido a que ofrecía un incremento en la capacidad y confiabilidad en comparación con 802.11b. J.Berg, (2011).

2.1.4 IEEE 802.11g

El estándar 802.11g fue adoptado ampliamente por los fabricantes de dispositivos WiFi a inicios de 2003 debido a la demanda de los consumidores por una mayor velocidad y reducciones en los costos de manufactura. En el verano de 2003 aparecieron dispositivos compatibles con 802.11a/b/g. La versión 802.11g trabaja en los 2.4 GHz al igual que 802.11b, pero usando la tecnología OFDM de 802.11a. Si bien el hardware 802.11g es completamente compatible con 802.11b, en una red 802.11g la presencia de un dispositivo 802.11b reduce significativamente la velocidad de toda la red 802.11g. A pesar de que 802.11g tuvo una gran aceptación, tiene el inconveniente de la gran interferencia que existe en la banda de los 2.4 GHz debida no únicamente a la tecnología WiFi. Para prevenir en la medida de lo posible la interferencia, en los E.U.A y otros

países con regulaciones similares existen solamente tres canales en la banda 2.4 GHz que no se sobreponen estos son 1, 6 y 11 con 25 MHz de separación. En Europa los canales que no se sobreponen son 1, 5, 9 y 13 con 20 MHz de separación. Incluso con tal separación, existe interferencia aunque es considerablemente menor. Ho et al., (2016).

2.1.5 IEEE 802.11n

La versión 802.11n incluye modificaciones que mejoran el rango, confiabilidad y tiempos de respuesta de las LAN inalámbricas. En la capa física (PHY), se agregaron técnicas avanzadas de procesamiento de señales y modulación para aprovechar las múltiples antenas de los dispositivos que salieron al mercado a partir de esta versión. Todo esto dio como resultado que se alcanzaran velocidades de hasta 600 Mbit/s con la posibilidad de operar en las bandas de 2.4 GHz y 5 GHz, aunque el soporte para 5 GHz es opcional. Perahia, (2008).

En esta versión se introduce la tecnología de Múltiple Entrada Múltiple Salida (MIMO) gracias a la cual se hizo posible transmitir y recibir simultáneamente a través de múltiples antenas. Las configuraciones de antenas de los sistemas MIMO con frecuencia son descritos en términos de “M X N” donde M y N son números enteros usados para referirse al número de antenas tanto el transmisor como del receptor. 802.11n define muchas configuraciones de “M X N” antenas que van desde “1 X 1” hasta “4 X 4”. MIMO usa múltiples antenas intercambiar más datos de lo que sería posible con una sola antena. La manera se lleva a cabo esto es mediante Multiplicación por División de Espacio, gracias a esta técnica es posible trasmitir diferentes tramas de datos al mismo tiempo, una por cada antena. De esta manera se incrementa notablemente la velocidad de transmisión. Hampton, (2013).

El número de tramas de datos que se pueden enviar simultáneamente está limitado por el mínimo número de antenas usadas en ambos lados de la conexión. Sin embargo, es común que los dispositivos estén limitados también en la cantidad de tramas diferentes que se pueden enviar a través de las múltiples antenas. La notación “M X N : Z” permite además identificar la capacidad de un sistema MIMO. El número Z es el máximo número de tramas de datos diferentes que se pueden enviar. Por ejemplo, un sistema MIMO que pude transmitir por dos antenas y recibir por

tres y que solo puede enviar o recibir dos tramas de datos diferentes sería un sistema 2 X 3 : 2. Hampton, (2013).

2.1.6 IEEE 802.11ac

Los primeros estándares IEEE 802.11 fueron diseñados principalmente para conectar computadores tipo laptop en casas y oficinas. La amplia aceptación y éxito que tuvieron las LAN inalámbricas propició la aparición de dispositivos de otro tipo y que demandaban mayores velocidades de intercambio de datos. Algunos ejemplos de estos dispositivos son:

- Televisores inteligentes
- Televisores de alta resolución
- Teléfonos inteligentes
- Tabletas
- Equipos industriales de automatización

IEEE 802.11ac alcanza velocidades de alrededor de 1.3 Gb/s y trabaja en la banda de los 5 GHz garantizando pero retrocompatibilidad con los estándares previos. Entre otras ventajas, el hardware usado en los dispositivos de esta versión consume menos energía, lo que es bueno para dispositivos que funcionan con baterías. Además es capaz de transmitir datos idénticos al mismo tiempo y a múltiples destinatarios, por ejemplo, un vídeo mediante una única corriente de datos. Por otra parte, es capaz de utilizar canales de 40 MHz, 80 MHz e incluso 160 MHz. Gast, (2013).

2.2 Componentes principales de una red 802.11

De acuerdo con la publicación de Gast, (2005), los componentes principales de una red inalámbrica bajo el estándar 802.11 son: estaciones, punto de acceso, medio inalámbrico de transmisión y sistema de distribución. A continuación, se una breve descripción de cada uno.

- Estaciones. Se pude considerar estación a cualquier dispositivo provisto de algún sistema computacional con interface de red, algunos ejemplos podrían ser los teléfonos inteligentes, tabletas, laptops, etc.

- Punto de acceso. Son dispositivos que hacen posible la interconexión entre las estaciones de una red inalámbrica.
- Medio inalámbrico de transmisión. Si en una red cableada el medio de transmisión son los cables de red, el equivalente en una red inalámbrica serían las ondas de radio en el aire. Se tiende a pensar que el único medio son las ondas de radio y esto no del todo cierto pues como se describirá más adelante también existe una implementación en luz infrarroja.
- Sistema de distribución. Es el componente usado para conectar varios puntos de acceso cuando se necesita que la red inalámbrica cubra un área extensa. En estas situaciones es común que medida que una estación se mueve quede fuera del alcance de un punto de acceso pero cerca de otro, por lo tanto, se requiere de una unión entre los diferentes puntos de acceso. El estándar 802.11 no especifica alguna tecnología en especial para este componente de tal manera que pude utilizarse incluso una red cableada clásica.

2.3 Modelo OSI.

"El estándar OSI es un modelo de referencia abierto para la interconexión de sistemas" Li et al., (2011). El modelo OSI suele dividirse en 7 niveles o capas (Figura 2.1) donde cada una se dedica a resolver una parte del problema de comunicación. Cada capa superior utiliza los servicios de las capas inferiores: cada capa se comunica con su similar en otro sistema, pero debe hacerlo enviando mensajes a través de los niveles inferiores. Con la finalidad de tener un marco de referencia para esta investigación, a continuación se describen de manera breve cada una las capas del modelo OSI.

- Capa física. Define las características físicas del medio (por ej. cables) de comunicación para la transferencia de información mediante especificaciones eléctricas, mecánicas y funcionales. Igualmente define especificaciones eléctricas, mecánicas y funcionales. Además, define la técnica de transmisión, tipo de transmisión, codificación, velocidad y modo de operación de la línea de datos. Esta capa será de particular interés en esta

investigación puesto se trata básicamente del análisis de la potencia de las ondas de radiofruencia que constituyen el medio de transmisión en las redes inalámbricas.

- Capa de Enlace. Proporciona facilidades para organizar los bits (1's y 0's) de la capa física en formatos o grupos lógicos de información. Actúa como capa intermedia entre la capa de red y la capa física, codificando las tramas recibidas desde la capa de red para su transmisión desde la capa física, controlando el acceso al medio y los posibles errores en la transmisión.
- Capa de red. Provee el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse a la capa siguiente (Transporte) o bien la capa 2 (Enlace). Nótese que la capa de red pude ser referida como la dirección lógica.
- Capa de transporte. Esta capa se encarga de hacer la unión entre las tres capas bajas encargadas de las comunicaciones y las tres capas altas encargadas el procesamiento de la información. Entre otras tareas, la capa de transporte garantiza la entrega confiable la información al nivel de sesión, define el direccionamiento de localidad física de los dispositivos en la red, define la manera de habilitar y deshabilitar las conexiones entre nodos y determina el protocolo que garantiza el envío del mensaje.
- Capa sesión: Proporciona los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos. Establece el inicio y término de la sesión. Permite referenciar a los dispositivos de la red por nombre y no por dirección lo que permite entre otras cosas escribir programas que corran en cualquier instalación de la red.
- Capa de presentación. Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red. Determina la forma de presentación de los datos sin preocuparse de su significado o semántica. Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
- Capa de aplicación. Proporciona aspectos de comunicaciones para aplicaciones específicas entre los usuarios de la rede tales como: manejo de la red, protocolos de transferencias de archivos (FTP), etc.

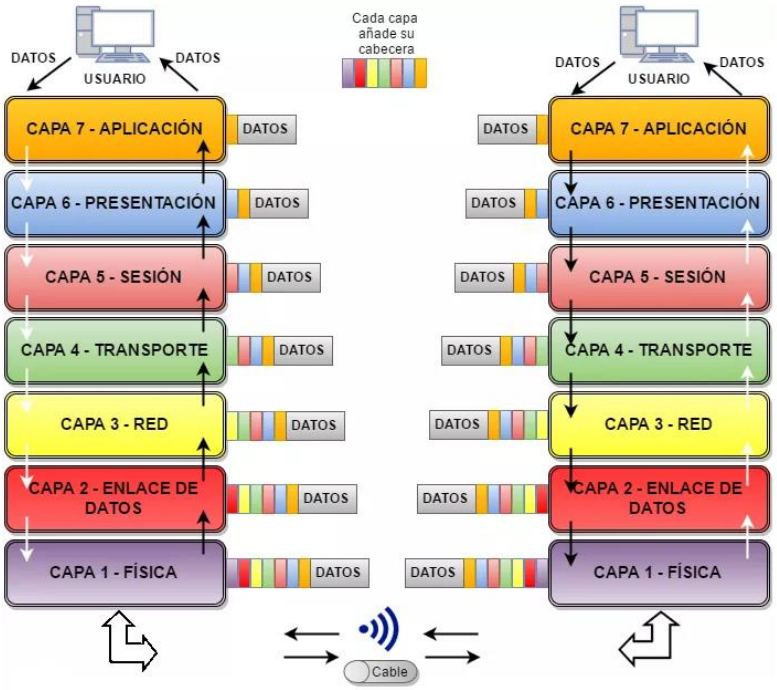

Figura 2.1. Modelo OSI. Adaptado de Rico, (2016)

2.4 Capa física (PHY) del estándar IEEE 802.11

En línea con los objetivos de esta investigación, la capa física (PHY) del estándar 802.11 adquiere mayor importancia. En apartado se tratan de manera general algunos temas de Radiofrecuencia y técnicas relacionadas con la capa física. Se describen también el valor RSSI, su significado, inconvenientes y su posible uso para detección de personas en interiores.

2.4.1 Componentes básicos de un sistema de transmisión por RF

El trabajo con redes inalámbricas 802.11 eventualmente requiere de por lo menos conocimientos básicos de radiofrecuencia, antenas, electromagnetismo, etc. Tan solo para cubrir conceptos introductorios a la ingeniería de radiofrecuencia podría tomar varios libros completos. El objetivo de este apartado no es adentrarse en este tipo de temas sino solamente explicar a grandes rasgos los componentes básicos de un sistema RF y su propósito.

Los componentes de un sistema de radiofrecuencia pueden variar bastante dependiendo de las frecuencias a las que opera y las distancias que debe cubrir, sin embargo fundamentalmente todos los sistemas comparten algunos componentes comunes. En el caso de las redes 802.11 y particularmente para los objetivos que se persiguen en esta investigación hay dos componentes de interés: las antenas y los amplificadores.

Las antenas son las encargadas de convertir señales eléctricas en ondas de radio y viceversa. En diagramas y manuales es común encontrar el símbolo de la Figura 2.2 para representar una antena.

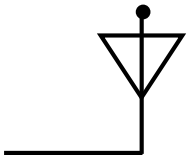

Figura 2.2. Símbolo antena. Elaboración propia.

Las antenas están hechas de un material conductor de manera que el impacto de las ondas radio causa un flujo de electrones creando una corriente eléctrica. A la inversa, cuando se aplica una corriente eléctrica a una se crea un campo eléctrico alrededor de la misa. Los cambios en la corriente eléctrica aplicada a la antena causarán cambios en el campo eléctrico, ese "campo eléctrico cambiante" pasa a ser un campo magnético y entonces la onda radio sale al aire. Tse y Viswanath, (2005).

El tamaño de la antena dependerá de la frecuencia, a mayor frecuencia se necesita una antena más pequeña. Teóricamente la antena más pequeña posible para una frecuencia dada es ½ de la longitud de onda en dicha frecuencia. En la práctica existen técnicas para reducir el tamaño de las antenas más allá del límite teórico. Como ejemplo, una antena para la banda 2.4 GHz debería medir 12.5 centímetros y sin embargo los teléfonos inteligentes tienen antenas de escasos milímetros. En las computadoras tipo laptop es común que parte de la antena para la red 802.11 esté oculta alrededor del monitor. Otro aspecto importante a mencionar acerca de las antenas es que son de dos tipos las más usadas en 802.11, las omnidireccionales que irradian en todas

direcciones y las unidireccionales que tienen la capacidad de dirigir las ondas una radio en una dirección específica. Molisch, (2010).

Los amplificadores por su parte tienen la función de incrementar la amplitud de la señal en un determinado factor de ganancia medido en decibeles (dB). En la literatura acerca de las redes 802.11 se mencionan comúnmente dos tipos de amplificadores: los de bajo ruido y los de alta potencia. Los amplificadores de bajo ruido pueden amplificar la señal que reciben de la antena pero dejando el ruido a un nivel muy bajo. Los amplificadores de alta potencia son usados para amplificar la señal que se enviará al aire mediante la antena.

2.4.2 Propagación de ondas RF

En las redes cableadas las señales están confinadas a los cables y por lo tanto los ingenieros de redes no necesitan saber mucho de propagación de las señales. Para esto, en temas de Física solo es necesario conocer algunas fórmulas para calcular la longitud de los cables y poco más. Las redes inalámbricas en cambio son un caso muy diferente.

En los tiempos actuales, el ambiente que nos rodea está plagado de ondas electromagnéticas. A medida que la recepción de una señal se degrada, la amplitud de la señal se hace cada vez más pequeña llegando a parecer sólo ruido. El desempeño en la recepción de una señal está determinado por la *relación señal a ruido (SNR)* que se define como la razón de la potencia de la señal con respecto a la potencia del ruido. Molisch, (2010).

$$SNR = \frac{P_{signal}}{P_{ruido}}$$

Una buena relación señal a ruido es importante que porque de esa manera es fácil distinguir entre ruido y señal. En algunas ocasiones cuando la SNR no es buena se puede aumentar la potencia de la señal sin embargo debido a regulaciones legales esto no es una opción cuando se trabaja en las bandas de 2.4 GHz y 5 GHz.

La capacidad de un canal de comunicaciones ya sea cableado o inalámbrico está determinado por el teorema de Shannon-Hartley el cual expresa el límite teórico de la capacidad en bits por segundo C como una función del ancho de banda y la relación señal a ruido.

$$C = Blog2(1 + SNR)\ bps$$

En ocasiones, el teorema de Shannon-Hartley se usa para saber la mínima SNR que debe existir para transmitir a una velocidad de transmisión dada. Como ejemplo, un típico canal telefónico de voz tiene una razón de señal a ruido de 30 dB y un ancho de banda de 3 kHz, esto da como resultado que la capacidad máxima del canal es aproximadamente 30,000 bps. En resumen, el teorema dicta que es posible transmitir información libre de ruido siempre y cuando la tasa de información no exceda la Capacidad del Canal. De esta manera, si el nivel de SNR es menor, o sea la calidad de la señal es más cercana al ruido, la capacidad del canal disminuirá.

En el estándar 802.11, la velocidad de la red depende además del alcance o rango de la señal. A medida que una señal es transmitida y viaja por el aire también se degrada. En una red 802.11 la SNR se mantiene relativamente constante en las cercanías del punto de acceso pero a medida que una estación se aleja la potencia de la señal cae y sin embargo el ruido se mantiene constante dando como resultado una degradación de la SNR. Conforme la distancia al punto de acceso se incrementa, la señal tiende a parecerse cada vez más al ruido. Cuando la SNR se hace demasiado pequeña como para soportar una alta cantidad de datos (teorema Shannon-Hartley), entonces la estación operara a una velocidad de transmisión más baja que requiere una más baja SNR.

En lugares abiertos donde no hay obstáculos que obstruyan la señal de radio, la degradación puede calcularse de la siguiente manera:

$$Atenuación\ de\ ruta\ (dB) = 32.5 + \log F + \log d$$

Donde la frecuencia F es expresada en Hz y la distancia *d* es expresada en metros. De acuerdo con Molisch, (2010) las pérdidas de la señal en un espacio abierto se denominan comúnmente como *atenuación de ruta* que es la pérdida mínima que se podría esperar a lo largo de toda la ruta de la señal. La atenuación de ruta depende de la distancia y de la frecuencia de la onda de radio. A mayores distancias y mayores frecuencias la atenuación de ruta es mayor. Esta

podría ser una de las razones por las cuales 802.11a tenía un rango más corto que 802.11b ya que como se recordará 802.11a operaba a 5 GHz.

La atenuación de ruta no es el único factor para determinar el rango de alcance de una señal. Los obstáculos como paredes y ventanas también atenúan la señal aunque a menudo se usan antenas y/o amplificadores para mejorar la señal los cuales compensas las perdidas en la transmisión. Muchos autores incluyen un *factor de compensación* en la fórmula para calcular el rango. Según Gast, (2005) la fórmula es la siguiente:

$$TL = P_{TX} + AG_{RX} + AG_{RX} - (PL + OL + FC)$$

Donde:

TL= Atenuación total

P_{TX}=Potencia TX

AG_{RX}= Ganancia de la antena RX

PL= Atenuación de ruta

OL= Atenuación debida a los obstáculos

FC= Factor de compensación

2.4.3 Desvanecimiento por multitrayecto

La fórmula para calcular la atenuación total es muy simple y por lo mismo debe aclararse que sólo proporciona una estimación aproximada para predecir la propagación de las ondas de radio en una red 802.11. En la realidad existen más fenómenos que afectan la recepción de la señal, uno de estos es lo que se conoce como *desvanecimiento por multitrayecto.* Las ondas de radio se

suman y/o restan entre sí cuando viajan por el aire de tal manera que cuando múltiples ondas convergen en un punto determinado, la onda percibida en ese punto es la suma total de dichas ondas. Molisch, (2010).

En la práctica, el desvanecimiento por multitrayecto es muy común debido a que la mayoría de los dispositivos usan antenas omnidireccionales y entonces las ondas son irradiadas en todas direcciones y son reflejadas en superficies en las chocan. Por lo tanto, la onda percibida por el receptor es la suma total de la onda original y las reflejadas. En el caso de que la suma total tenga una amplitud demasiado baja el receptor no entenderá la transmisión o en el peor caso no detectará transmisión alguna. Una simple solución para disminuir el desvanecimiento por multitrayecto podría ser simplemente cambiar la orientación y/o posición del receptor.

De acuerdo con la información de Molisch, (2010) un factor importante a considerar del desvanecimiento por multitrayecto es el retardo entre las diferentes reflexiones de la misma onda. Es decir, la onda que no se reflejó en ningún momento sino que llegó directamente al receptor llegará primero que la onda reflejada que tomó un camino más largo, este retardo es llamado *delay spread*. Ente más grande sea el retardo se requiere más procesamiento en el receptor para decodificar la señal, las redes 802.11 pueden manejar retardos de hasta 500 ns pero a estos niveles el desempeño de la red disminuirá notablemente. Algunos fabricantes de dispositivos WiFi revelan en las hojas de datos el máximo retardo que pueden soportar sus dispositivos. Estos datos se pueden encontrar en las hojas de datos correspondientes. En la Tabla 2.1 se muestran algunos ejemplos:

Tabla 2.1.Ejemplos de tolerancia el Delay Spread

Fabricante	***Modelo***	***11 Mpbs***	***5.5 Mbps***
Broadcom	Cisco 350	140 ns	300 ns
Cisco	BCM94306	250 ns	300 ns

Adaptado de Gast, (2013).

2.4.4 Asignación de canales en las bandas 2.4 GHz y 5 GHz

Las versiones 802.11b/g/n operan en la banda de 2.4 - 2.5 GHz mientras que las versiones 802.11a/n/ac lo hacen en la banda de 4.915 – 5.825 GHz. Por simplicidad estas dos bandas son

comúnmente llamadas 2.4 GHz y 5 GHz respectivamente. Cada una de estas bandas se subdivide en canales con una frecuencia central y un ancho de banda de manera similar a como ocurre con otros espectros comerciales como los de televisión o telefonía móvil. La banda 2.4 GHz está divida en 14 canales espaciados 5 MHz cada uno, el primer canal está centrado en 2.412 GHz como se muestra en Figura 2.3. La numeración de los canales la banda 5 GHz no es simple debido a que cambia de país a país a causa de las diferencias de las regulaciones en distintos países. Flickenger, (2006).

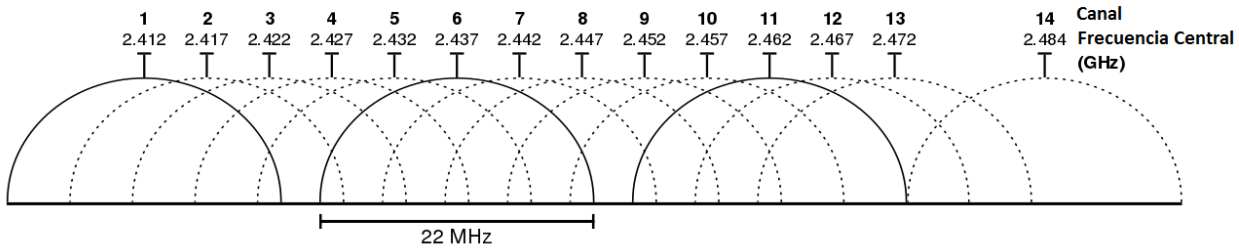

Figura 2.3.Representación gráfica de los canales en la banda 2.4 GHz. Adaptado de Flickenger, (2006).

Los primeros dispositivos 802.11 usaban canales que tenían un acho de aproximadamente 20 MHz. En Norteamérica, los radios 802.11b/g usan una de las once frecuencias de 20 MHz (hay tres canales que no se sobreponen, 1,6,11) dentro de los 2.4 GHz. Cuando se introdujo la tecnología OFDM, el ancho de banda de cada canal era de 20 MHz, pero posteriormente se agregó soporte para anchos de banda de 5 y 10 MHz. Los dispositivos 802.11a operan en uno de doce canales de 20 MHz de la banda de 5 GHz mientras que los de versión 802.11n pueden operar con canales de 20 o 40 MHz. Aruba, (2014).

2.4.5 Regulaciones legales del espectro radioeléctrico

Todos dispositivos inalámbricos comerciales tienen ciertas limitaciones para solo operar dentro de ciertas bandas de frecuencia autorizadas. Existen diversas bandas de frecuencia para diferentes propósitos, por ejemplo, para televisión, telefonía, radio civil, etc. El uso del espectro radio eléctrico está rigurosamente controlado por las autoridades de cada país mediante procesos

de licenciamiento. En México, el Instituto Federal de Telecomunicaciones a través de su Comité Técnico en materia de Espectro Radioeléctrico es el encargado de elaborar las regulaciones, en los estados unidos es la *Federal Communications Comission* (FCC) y en Europa la *European Radiocommunications Office* (ERO). Existe además la Internacional *Telecommunications Union* (ITU) que se encarga de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. IFT, (2013).

En la Tabla 2.2 se muestran algunas bandas de frecuencia usadas en México, se resaltan las bandas de operación 802.11.

Tabla 2.2. Algunas bandas de frecuencia licenciadas en México

Rango de Frecuencias	***Uso***
535 – 1705 kHz	Se emplea para la provisión del servicio de radiodifusión sonora en Amplitud Modulada (AM).
54-60 MHz	Televisión digital terrestre canal 2
60-66 MHz	Televisión digital terrestre canal 3
66-72 MHz	Televisión digital terrestre canal 4
76-82 MHz	Televisión digital terrestre canal 5
82-88 MHz	Televisión digital terrestre canal 6
88 – 108 MHz	Se emplea para la provisión del servicio de radiodifusión sonora en Frecuencia Modulada (FM)
151.6125 - 151.6375 MHz	Espectro libre
153.0125 - 153.2375 MHz	
154.5875 - 154.6125 MHz	
159.0125 - 159.2000 MHz	
163.0125 - 163.2375 MHz	
174-180 MHz	Televisión digital terrestre canal 7
180-186 MHz	Televisión digital terrestre canal 8
186-182 MHz	Televisión digital terrestre canal 9
192-198 MHz	Televisión digital terrestre canal 10
198-204 MHz	Televisión digital terrestre canal 11
204-210 MHz	Televisión digital terrestre canal 12
210-216 MHz	Televisión digital terrestre canal 13
700 MHz	Designadas para las Telecomunicaciones Móviles Internacionales (IMT por sus siglas en inglés).
814-824/859-869 MHz	
824-849/869-894 MHz	
902 a 928 MHz	Espectro libre
1525 – 1559 MHz	

1626.5 – 1660.5 MHz	Sistema Satelital del Gobierno Federal para proporcionar servicio móvil por satélite
1710-1780/2110-2180 MHz	Designada para las Telecomunicaciones Móviles Internacionales (IMT por sus siglas en inglés).
1850-1910/1930-1990 MHz	
1920 – 1930 MHz	
2400 – 2483.5 MHz	**Espectro libre**
3.400 – 3.700 GHz	Empleadas por el Sistema Satelital del Gobierno Federal para la para la provisión del servicio fijo por satélite.
6.425 – 6.725 GHz	
5.15 – 5.35 GHz	**Espectro libre**
5.47 – 5.6 GHz y 5.65 – 5.85 GHz	Espectro libre
10.7 – 10.95 GHz	Sistema Satelital del gobierno federal para proporcionar servicio fijo por satélite
11.2 – 11.45 GHz	
12.75 – 13.25 GHz	
13.25 – 13.4 GHz	Radionavegación aeronáutica, investigación espacial, exploración de la tierra por satélite.
13.4 GHz – 13.75	Radiolocalización, investigación espacial, fijo por satélite, frecuencias patrón y señales horaria por satélite.
14.47 GHz – 14.g GHz	Para uso de investigaciones en radioastronomía, fijo por satélite.

Adaptado de IFT, (2017)

Las bandas de frecuencia ISM (*Industrial, Scientific and Medical*) están reservadas internacionalmente para uso en áreas industrial, científica y médica. Estas bandas de frecuencia son:

- UHF ISM 902-928 MHz
- S-Band ISM 2.4-2.5 GHz
- C-Band ISM 5.725-5.875 GHz

De inmediato se puede apreciar que el estándar 802.11 opera precisamente en las bandas ISM. Quizás de manera insospechada, uno de los dispositivos más comunes que opera en la banda ISM 2.4 GHz es el horno de microondas, esto es debido a que la radiación electromagnética a esa frecuencia es particularmente efectiva para calentar agua. Las bandas ISM fueron definidas por la ITU en el artículo 5 de las Regulaciones Radio. El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia, respetando las regulaciones que limitan los niveles de potencia transmitida. El licenciamiento de una banda en particular garantiza el acceso exclusivo a

la misma. Cuando una banda bajo licencia es interferida, el licenciatario puede demandar ante la autoridad reguladora. La interferencia de frecuencias no permitidas está sujeta a sanciones penales y civiles.

Si bien la anda 2.4 GHz pertenece al espectro libre, esto no significa que los fabricantes de equipos 802.11 pueden vender equipos sin control alguno. En la mayoría de los países los organismos reguladores del espectro radioeléctrico exigen un número de identificación único para cada dispositivo vendido.

2.4.6 Arquitectura de la Capa Física (PHY) 802.11

La capa física está dividida en dos subcapas (Figura 3.5) que son: PLCP (*Physical Layer Convergence Procedure*) y PMD (*Physical Medium Dependent*). El PLCP hace posible la unión de la capa física y la capa de enlace, es decir, la unión entre las tramas de datos provenientes de la MAC y los mecanismos que hacen posible transmitir esas tramas en el aire. Al hacer esto, el PLCP agrega información al encabezado del mensaje. El PMD por su parte es la parte responsable de transmitir en el aire mediante una antena los bits lógicos que todavía recibe del PLCP. Carpenter y Badman, (2016).

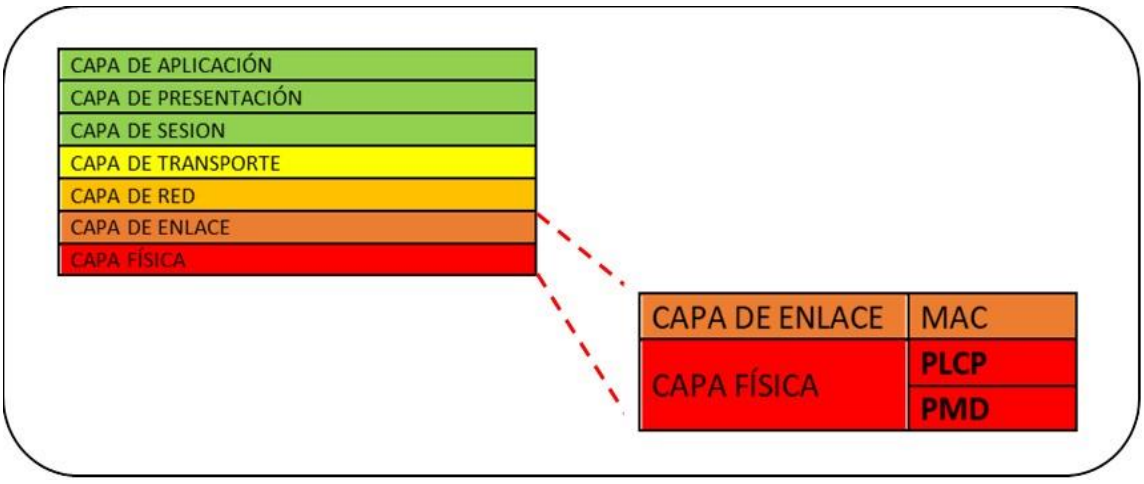

Figura 2.4. Arquitectura de la capa física IEEE 802.11. Elaboración propia.

2.4.7 Proceso de operación de una red 802.11

En una red 802.11 todas las estaciones comparten un mismo canal de frecuencia de radio. Las transmisiones en este canal son recibidas por todas las estaciones dentro del rango del alcance del punto de acceso. La cobertura de punto de acceso puede ser extendida de un área pequeña como un par de habitaciones hasta varios kilómetros sobreponiendo el alcance de varios puntos de acceso. También la sensibilidad del receptor es importante pues determina que el máximo rango del punto de acceso sea efectivo. Para este propósito se lleva a cabo una prueba de RSSI durante una breve secuencia de inicialización.

Al encender un dispositivo 802.11 el software de las capas superiores a la capa física entra en acción para tratar de establecer contacto, esto se realiza mediante escaneos en modo pasivo o activo. El estándar permite flexibilidad para implementar ese proceso de diferentes maneras y por lo tanto puede variar de un dispositivo a otro. El proceso de escaneo de usan tramas de datos llamadas *Beacons* y *Probe Requests*. Carpenter y Badman, (2016).

- Modo Pasivo. En este modo, después de seleccionar un canal el dispositivo permanece escuchando *Beacons* o *Probe Request*. Los *beacons* son transmitidos desde el punto de acceso y contienen información acerca del mismo además de una referencia de tiempo. Al igual que con cualquier otro dato la transmisión del *beacon* depende de si el canal está libre y en caso de que no sea así entonces la transmisión se retrasa. El dispositivo busca una red solamente escuchando los *beacons* hasta que encuentra una que sea factible para conectarse.
- Modo Activo. El dispositivo intenta localizar un punto de acceso transmitiendo tramas *Probe Requests* y espera una respuesta. La trama *probe request* puede ser abierta o para un punto de acceso en específico. La respuesta que se obtiene del punto de acceso es parecida a un *beacon*, a continuación, la respuesta es evaluada por el dispositivo para determinar si es factible conectarse. El escaneo en modo activo permite una manera más rápida de establecer un primer contacto, pero consume más energía.

En este punto la estación ya ha establecido un primer contacto y ha identificado un punto de acceso factible para conectarse a la red. Posteriormente la estación necesita autentificarse ante el punto de acceso para poder acceder a la red. En una red abierta, los dispositivos envían

peticiones de autentificación y obtienen una respuesta del punto de acceso sin restricción. En una red segura existe un proceso de autentificación más complejo, este proceso involucra tres partes: el punto de acceso, la estación o dispositivo y el servidor de autentificación. En el caso de los puntos de acceso domésticos de hoy en día el servidor de autentificación es simplemente un programa más corriendo en el mismo hardware del punto de acceso. El dispositivo o estación (también llamado *supplicant*) no es admitido en la red a través del punto de acceso hasta que el servidor de autentificación valida las credenciales. Carpenter y Badman, (2016)

La asociación es el siguiente paso después de la autentificación y permite la transferencia entre el dispositivo y el punto de acceso. El dispositivo envía una petición de asociación al punto de acceso el cual responde habilitando o deshabilitando la asociación. Una vez que la asociación es satisfactoria, el punto de acceso emite un Identificador de asociación para el dispositivo y lo agrega a su base de datos de dispositivos conectados.

La transferencia de datos es permitida solamente después de la autentificación y la asociación. Si un dispositivo intenta enviar datos al punto de acceso sin haberse autenticado y asociado correctamente ocasiona que el punto de acceso le retire la autentificación. Las tramas de datos siempre son seguidas de una señal de *acknowledge*, esto significa que cuando un dispositivo envía una trama de datos al punto de acceso éste responderá enviando una señal de *acknowledge* y viceversa.Carpenter y Badman, (2016)

2.4.8 Indicador de Fuerza de la Señal Recibida (RSSI)

En IEEE, (2014) el estándar 802.11 define un mecanismo por medio del cual la energía de las ondas RF es medida por la electrónica de la interface de red. Este mecanismo da como resultado un valor numérico entero de 0 a 255 llamado Indicador de Fuerza de Señal Recibida (RSSI). En realidad, los fabricantes no proporcionan una representación de 0 a 255 valores diferentes, sino que cada fabricante establece su propio valor máximo RSSI (de 0 a 255). El valor RSSI es un valor entero definido en el estándar 802.11 para ser usado por el driver del dispositivo WiFi con diferentes propósitos. Por ejemplo, antes de que un dispositivo intente transmitir un paquete de datos debe ser capaz de detectar si el canal está libre, es decir que nadie está transmitiendo y esto

se hace midiendo la potencia de la señal de RF. Otro uso es calcular la ganancia del amplificador dependiendo del valor RSSI, para un valor bajo se necesitará mayor amplificación.

"El Indicador de Fuerza de Señal Recibida (RSSI) es un parámetro opcional que tiene un valor de 0 hasta RSSI_MAX. Este parámetro es una medida mediante la subcapa PHY de la energía observada en la antena usada al recibir el PPDU. RSSI debe ser medido entre el comienzo del delimitador de inicio de trama SFD y el final del encabezado PLCP HEC. El RSSI está destinado para ser usado de manera relativa. La exactitud absoluta de la lectura RSSI no está especificada" IEEE, (2014). Nótese que el parámetro RSSI está especificado como opcional, aunque todos los fabricantes de interface 802.11 parecen implementarlo cada uno a su manera. Una de las partes más significativas de la definición anterior es cuando se especifica que el RSSI está destinado para un uso relativo y que su exactitud absoluta no está especificada. Esto significa que en los casos en los que el driver proporcione el RSSI como un simple valor de 0 a 255 sin unidades no hay nada en el estándar 802.11 que estipule una relación entre dicho valor y algún nivel de energía en particular medido en mW o dBm. Cada fabricante por su lado escoge proporcionar su propio nivel de exactitud, resolución, rango y unidades para la potencia real de la señal en la antena. Esto causa algunos inconvenientes cuando se trata hacer algún mapeo de espectro para determinar la mejor ubicación para un punto de acceso dentro espacios cerrados. Quizás esto haya motivado que en las interfaces 802.11 más recientes los drivers ya proporcionan el RSSI en dBm en la mayoría de los casos.

En la Figura 2.5 se muestra que la medición de RSSI abarca desde el inicio de la trama hasta el final del PLCP como lo indicar el estándar. No se abordarán cuestiones de estructura de tramas y contenidos de las mismas debido a que no es tema relevante para esta investigación.

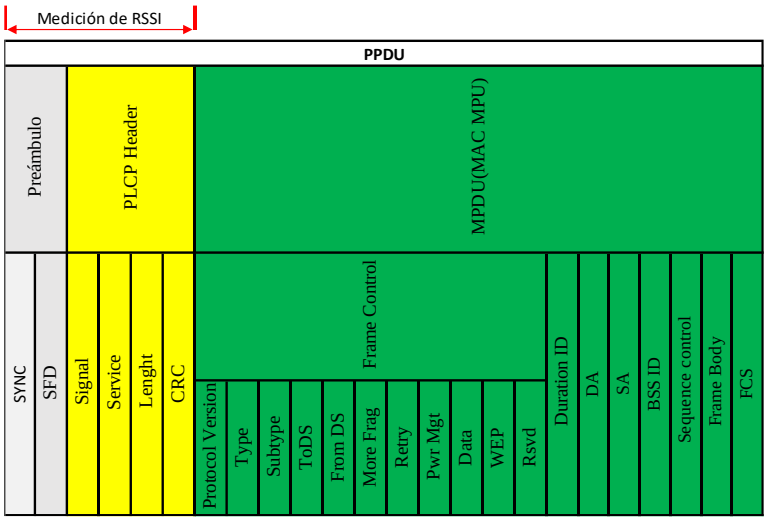

Figura 2.5. Medición RSSI en una trama Management Frame. Elaboración propia.

2.4.9 Conversión de unidades en el valor RSSI

En una red inalámbrica las estaciones necesitan conocer una medida de la potencia de la señal de radiofrecuencia que está recibiendo del punto de acceso para hacer ajustes en el amplificador entre otras cosas.

Existen cuatro representaciones la potencia de la señal. Estas son: miliwatt (mW), decibel-miliwatt (dBm), porcentaje o número entero (0-255) sin unidades. Estas cuatro representaciones están relacionadas unas con otras de tal manera que se pueden hacer conversiones cuando el driver tiene la capacidad de presentar dBm o mW.

Cuando la potencia de la señal es representada en miliwatts no hay mayor complicación para su interpretación pues indica directamente la potencia percibida. A primera vista la representación en miliwatts podría parecer la mejor representación de la potencia de señal y se podría pensar que todos los dispositivos WiFi la proporcionan así.

La señal WiFi es una onda electromagnética y como tal le aplican las leyes de la mecánica ondulatoria, una de estas leyes es la que se conoce como “Ley de la inversa del cuadrado”, mediante esta ley física aplicada a los propósitos de esta investigación se puede decir que a medida que la estación se aleje del punto de acceso la potencia percibida no decrecerá de manera lineal, sino que lo hará de manera exponencial e inversamente al cuadrado de la distancia. Es por esta

razón que muchas veces se opta por una representación logarítmica. La unidad dBm permite representar de manera logarítmica la potencia de la señal. Las conversiones dBm a mW y viceversa pueden realizarse usando las siguientes fórmulas.

$$P_{dBm} = 10logP_{mW} \qquad P_{mW} = 10^{\frac{P_{dBm}}{10}}$$

Como dato relevante para esta investigación se aclara que el driver del chipset WiFi del sistema Raspberry pi 3 B entrega un resultado en dBm.

2.5 Valor RSSI en diferentes WiFi Chipsets comerciales

Es sabido que el desempeño de dispositivos de diferentes fabricantes puede variar significativamente debido a factores de manufactura, calidad de materiales, tecnología, etc. Con el objetivo de dar una noción sobre esto la Tabla 2.3 muestra una lista de diferentes tarjetas de diferentes marcas. En dicha tabla se puede observar el valor mínimo y máximo de RSSI detectable, así como el rango de medición.

Tabla 2.3. Rango de medición del RSSI en algunas tarjetas de diferentes marcas

Fabricante	***Modelo***	***Versión IEEE 802.11***	***Máximo (dBm)***	***Mínimo (dBm)***	***Rango de medición (dBm)***
Lucent	Orinoco Gold	802.11b	−10	−102	92
Lucent	WaveLAN Silver	802.11b	−10	−94	84
Cisco	Aironet 350 series	802.11b	−10	−117	107
Proxim	Orinico Gold	802.11a/b/	−11	−93	82
SMC	EZ connect SMC2635W	802.11b	−14	−82	68
D-Link	AirPlus DWL−650+	802.11b	−50	−100	50
Hawking	HWC54G rev.R	802.11g	0	−75	75
3COM	3CRUSB10075	802.11b/g	10	−94	104
Intel	PRO/wireless 2200BG	802.11b/g	−10	−84	74

Adaptado de Kaemarungsi y Krishnamurthy, (2012)

2.6 Descripción del WiFi Chipset de la Raspberry Pi 3 B

El chipset WiFi de la Raspberry Pi 3B se puede encontrar bajo dos numeraciones, ya sea como BCM43438KUBG Figura 2.6 o también como CYW43438. Esto es debido a que anteriormente era fabricado Broadcom Inc., pero actualmente es fabricado por *Cypress Semiconductor Corporation*. Este chip capaz de soportar transferencias de datos desde 1 Mbps hasta 96 Mbps en modos de alto y bajo consumo, además está diseñado para proveer conectividad inalámbrica en diferentes tipos de redes operando bajo los siguientes estándares:

- Bluetooth 2.1 + EDR
- Bluetooth 3.0
- Bluetooth 4.1
- IEEE 802.11n
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11d
- IEEE 802.11h
- IEEE 802.11i

Soporta las siguientes características de seguridad:

■ Security:

- WEP
- WPA™ Personal
- WPA2™ Personal
- WMM
- WMM-PS (U-APSD)
- WMM-SA
- WAPI
- AES
- TKIP

El transceptor del BCM43438 está optimizado para trabajar en la banda 2.4 GHz, lo cual se puede confirmar al analizar la lista de estándares soportados donde no se encuentra la versión 802.11a. Es importante mencionar que pesar de que es capaz de trabajar con la versión 802.11n no soporta la recepción/transmisión multitrama de los sistemas MIMO.

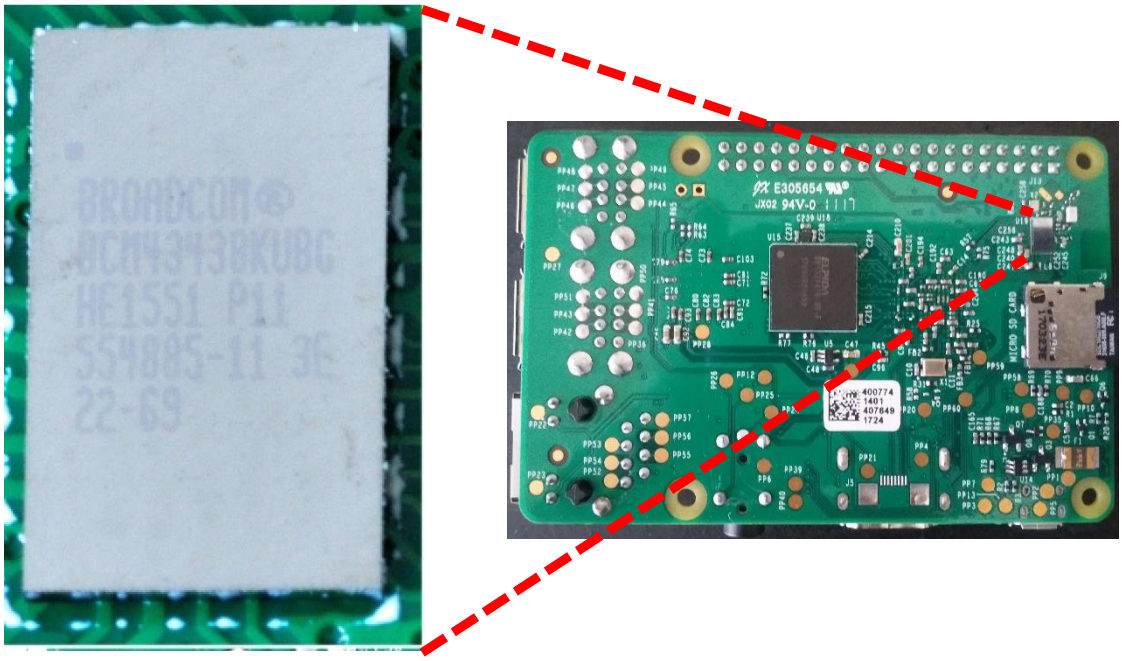

Figura 2.6. Ubicación física del WiFi Chipset. Elaboración propia.

Anteriormente se mencionó que la longitud de la antena en un sistema RF teóricamente debería ser ½ de la longitud de onda, pero mediante ingeniería de radiofrecuencia es posible reducir ese tamaño. En este caso la antena debería tener una longitud de 12.5 cm sin embargo en la realidad solo mide 5 mm. En la Figura 2.7 se puede ver la antena del BM43438 la cual se localiza en la parte posterior de la tarjeta.

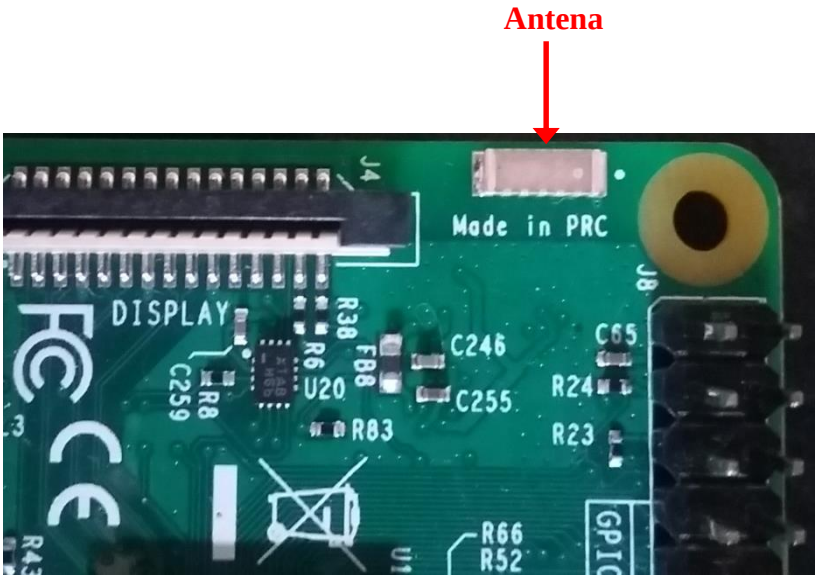

Figura 2.7. Ubicación de la antena WiFi en la Raspberry. Elaboración propia

Otro dato de interés en esta investigación es la sensibilidad del receptor del BCM43438 pues indica cual es el mínimo y máximo de potencia de señal que es capaz de registrar. El fabricante aporta los valores de la Tabla *2.4*. En la siguiente sección se reportan los datos de obtenidos al realizar una caracterización del receptor.

Tabla 2.4. Sensibilidad del BCM43438

Parameter	***Condition/Notes***	***Minimum***	***Typical***	***Maximum***	***Unit***
RX sensitivity (10% PER for 4096 octet PSDU). Defined for default parameters: Mixed mode, 800 ns GI.	6 Mbps OFDM	–91.5	–93.5	-	dBm
	9 Mbps OFDM	–90.5	–92.5	-	dBm
	12 Mbps OFDM	–87.5	–89.5	-	dBm
	18 Mbps OFDM	–85.5	–87.5	-	dBm
	24 Mbps OFDM	–82.5	–84.5	-	dBm
	36 Mbps OFDM	–80.5	–82.5	-	dBm
	48 Mbps OFDM	–76.5	–78.5	-	dBm
	54 Mbps OFDM	–75.5	–77.5	-	dBm

3. Metodología

En el presente capítulo se detalla un diseño experimental que permite hacer detección de presencia humana basándose en el procesamiento de variaciones de señal RSSI capturadas por el chipset WiFi de un sistema Raspberry Pi 3 B. Para hacer esto posible es necesario primero resolver algunos retos relacionados con la frecuencia de muestreo inherente al sistema, así como realizar una caracterización de valores RSSI puesto que no se encuentran disponibles en la documentación proporcionada por el fabricante.

3.1 Caracterización del RSSI del Chipset WiFi de la Raspberry Pi 3 B

Para implementar una detección de presencia basada en RSSI se debe considerar algunos de los factores mencionados anteriormente. Por un lado, aunque el estándar IEEE 802.11 define la medición de la potencia de la señal RF como un valor entero (RSSI_Max) que va de 0 a 255, en la práctica ningún fabricante de WiFi Chipsets opta por una representación en 256 valores de señal. Por otro lado, es importante recordar que también existen diferencias considerables en el rango de detección de los chipsets dependiendo del fabricante, es decir, la potencia mínima y máxima detectable varía entre dispositivos. Lo anterior sumado a que el fabricante no proporciona información del chipset WiFi de la Raspberry (BCM43438) motiva a que se obtenga una caracterización mediante mediciones directas.

Existen otros trabajos de investigación como Luong et al., (2016) que han demostrado que si el RSSI tuviera una mayor resolución sería posible incluso un reconocimiento gestual y movimientos finos.

El uso creciente de las redes WLAN y el aumento de las prestaciones de la mayoría de los Sistemas Operativos trajo consigo una variedad de herramientas informáticas para obtener no solo el valor RSSI sino además otros datos como el nombre del AP, dirección MAC, Relación Señal a Ruido (SNR), y número de canal al que se está conectado.

La Raspberry Pi implementa por defecto el sistema operativo Raspbian el cual es una distribución del sistema operativo GNU/Linux basado en Debian Strech (Debian 9.4). La versión de Raspbian usada en esta investigación es “8 (jessie)”. Todas las muestras de RSSI se obtuvieron

consultado el proceso */proc/net/wireless* de Raspbian mediante la herramienta *iwconfig*. La Figura 3.1 muestra un ejemplo del resultado que se obtiene al usar iwconfig, además se resalta en negritas el dato RSSI. Es importante aclarar que se ha ocultado la dirección MAC.

```
wlan0     IEEE 802.11bgn  ESSID:"TP-Link_A01E"
          Mode:Managed  Frequency:2.427 GHz  Access Point: XX:XX:XX:XX:XX:XX
          Bit Rate=58.5 Mb/s   Tx-Power=1496 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=59/70  Signal level=-51 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figura 3.1. Resultado iwconfig. Elaboración propia.

La Tabla 3.1 lista la variación de RSSI del WiFi chipset (BCM43438) de la Raspberry Pi 3 B. El valor máximo fue obtenido posicionando la Raspberry inmediatamente después del AP a una distancia prácticamente nula. El valor mínimo fue obtenido posicionando la Raspberry a una distancia de 30 metros.

Tabla 3.1. Rango de medición del Chipset BCM4348KUBG

Fabricante	***Modelo***	***Estándar WLAN***	***Max (dBm)***	***Min (dBm)***	***Rango de medición***
Cypress Semiconductor	BCM43438KUBG	802.11n	-10	-102	92

La Tabla 3.1 muestra la variación del RSSI con respecto a la distancia. Las mediciones fueron tomadas en un espacio abierto desde una distancia máxima de 12 metros hasta una distancia mínima prácticamente nula. Entre la distancia máxima y la distancia mínima se hicieron corrimientos de 1 metro. En los cuatro metros más próximos los corrimientos se redujeron a 25 cm para tratar de detectar cambios más sutiles.

Tabla 3.2. Variación de potencia respecto a la distancia

Distancia (m)	***RSSI (dBm)***
12	-81
11	-78
10	-78
9	-77
8	-76
7	-76
6	-71
5	-71
4	-64
3.75	-67
3.5	-66
3.25	-63
3	-63
2.75	-66
2.5	-65
2.25	-62
2	-63
1.75	-65
1.5	-61
1.25	-61
1	-55
0.75	-53
0.5	-58
0.25	-46
0	-35

3.2 Método de detección de presencia humana

El RSSI fluctúa en diferentes ambientes con grandes o pequeñas variaciones alrededor de un valor promedio. Sin embargo, las variaciones del RSSI en un periodo de tiempo se incrementan significativamente en presencia humana. Cuando nadie está presente en una habitación, las variaciones iniciales pueden usarse para definir un intervalo de las Variaciones Iniciales de la Señal (VIS). EL VIS se establece durante la inicialización del sistema analizando el intercambio de mensajes y las muestras obtenidas del RSSI. Durante la inicialización, no hay presencia humana en la habitación y por lo tanto el RSSI se ve afectado únicamente por el ambiente circundante.

Las variaciones de RSSI analizadas durante las condiciones iniciales son usadas para definir el umbral inferior *Umi* y superior *Ums* del VIS. Los umbrales son definidos usando un conjunto de muestras RSSI tomadas dentro de un intervalo de tiempo por definir.

La variación del RSSI pude calcularse tomando en cuenta la atenuación de la señal por la distancia *Pd* y la atenuación debida a los obstáculos *Pa*. Partiendo de un razonamiento básico pude decirse que la variación de RSSI en un intervalo de tiempo determinado es igual a la resta de la medición en un tiempo *t* menos la medición en un instante *t-1*.

$$\Delta RSSI = P(t) - P(t-1) \qquad (3.1)$$

Entonces, restando la atenuación debida a la distancia *Pd* y los obstáculos *Pa* a la potencia inicial emitida *Po* se pude definir la potencia en el tiempo t de la siguiente manera:

$$P(t) = Po - Pd(t) - Pa(t) \qquad (3.2)$$

De la misma manera se puede concluir para el instante anterior *t-1*:

$$P(t-1) = Po - Pd(t-1) - Pa(t-1) \qquad (3.3)$$

Una vez que ha calculado la variación de ΔRSSI y los umbrales *Umi* y *Ums*, puede determinarse si hay presencia humana causando variaciones en la potencia de la señal:

$$\Delta RSSI = \begin{cases} presencia, Umi > \Delta RSSI > Ums \\ no\ presencia, Umi < \Delta RSSI < Ums \end{cases} \qquad (3.4)$$

Para determinar los umbrales *Umi* y *Ums* se consideran los valores máximo y mínimo de las muestras capturadas durante la etapa de inicialización del sistema. Por lo tanto, *Umi* y *Ums* representan las variaciones normales del sistema sin presencia, dichos umbrales representan un porcentaje respecto a la amplitud de la variación máxima del RSSI durante la etapa de inicialización.

$$\%Umi = \left(\frac{\|\Delta RSSI_{min} - \overline{\Delta RSSI}\|}{RSSI_{min}}\right)(100) \tag{3.5}$$

$$\%Ums = \left(\frac{\|\Delta RSSI_{max} - \overline{\Delta RSSI}\|}{RSSI_{max}}\right)(100) \tag{3.6}$$

$$Umi = \overline{RSSI}\left(1 - \frac{\%Umi}{100}\right) \tag{3.7}$$

$$Ums = \overline{RSSI}\left(1 + \frac{\%Ums}{100}\right) \tag{3.8}$$

$$\overline{RSSI} = \frac{1}{n}\sum_{i=1}^{n} RSSI_i \tag{3.9}$$

Donde los valores $\Delta RSSI_{min}$ $\Delta RSSI_{max}$ denotan los valores mínimo y máximo del conjunto de muestras durante la etapa inicial.

3.2.1 Diseño experimental e implementación

Uno de los factores que afectan la medición del RSSI en interiores es la geometría de la edificación donde se toman las muestras debido principalmente al incremento de la reflexión y el desvanecimiento por multitrayecto. El área de estudio donde se tomaron todas las mediciones necesarias para este trabajo es una casa habitación de dos plantas, sin embargo, sólo la planta baja de la edificación se usó en el experimento. La Figura 3.2 muestra la geometría del área de estudio, la ubicación del punto de acceso y el punto de medición donde se colocó el receptor (Raspberry).

Todas las mediciones reportadas en este trabajo se hicieron tomando en cuenta las siguientes consideraciones:

1. El módulo WiFi de la Raspberry Pi tiene una antena omnidireccional
2. La Raspberry Pi se mantiene estática durante las mediciones
3. El entorno al interior del área de estudio se mantiene constante

La implementación práctica del método de detección consiste en detectar la presencia de una persona al cruzar la *Línea de Vista* (LV) entre el emisor y el receptor. Como se muestra en la Figura 3.2, la línea de vista entre emisor y receptor es una distancia de 4.7 m definida por las dimensiones de la edificación.

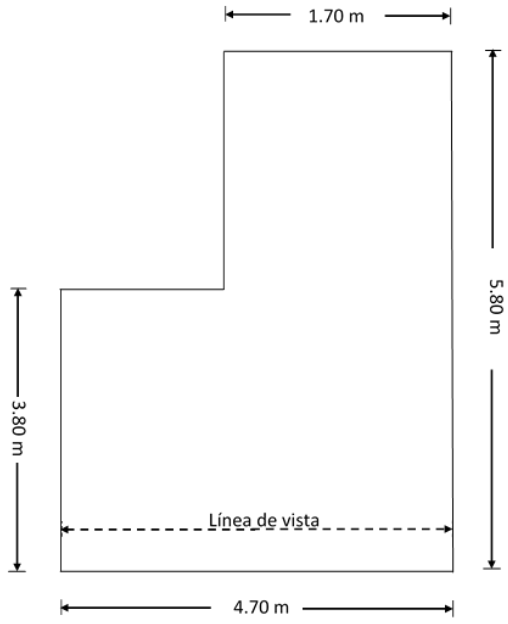

Figura 3.2. Localización del AP y punto de medición. Elaboración propia.

Para detectar el cruce de una persona por la línea de vista es necesario considerar la velocidad a la que se mueve porque de esto determinará la velocidad mínima de muestreo del RSSI. Es decir, si la velocidad de muestreo es demasiado baja entonces el sujeto podría atravesar la línea de vista antes de que el sistema capture alguna muestra. La Biomecánica y Locomoción Humana no son temas centrales de este trabajo sin embargo existen investigaciones como Snaterse et al., (2011) que profundizan en dichos temas. Con la finalidad de tener una mera referencia para este trabajo se hicieron mediciones de la velocidad al caminar de cinco sujetos. Primero se pidió a

los sujetos recorrer una distancia de 10 m caminando a una velocidad normal y después recorrer la misma distancia caminando rápidamente, con estos datos se obtuvo el promedio de cada sujeto, los resultados se muestran en la Tabla 3.3.

Tabla 3.3. Velocidad al caminar

Sujeto	***Normal (m/s)***	***Rápido (m/s)***
1	0.81	1.48
2	0.80	1.21
3	1.05	1.50
4	0.76	1.39
5	0.85	1.64

Otra variable a considerar son las dimensiones del sujeto que cruza la línea de vista. Mientras mayor sea el volumen del sujeto mayor será el cambio en RSSI y por lo tanto más fácilmente detectable.

Emisor y receptor se colocaron a 1 metro sobre el suelo con la finalidad de que la línea de vista pase a través de la región del estómago considerando que el sujeto es visible a desde una vista de perfil (Figura 3.3). En el sujeto de prueba el ancho del área del estómago se midió en 20 cm (Figura 3.4).

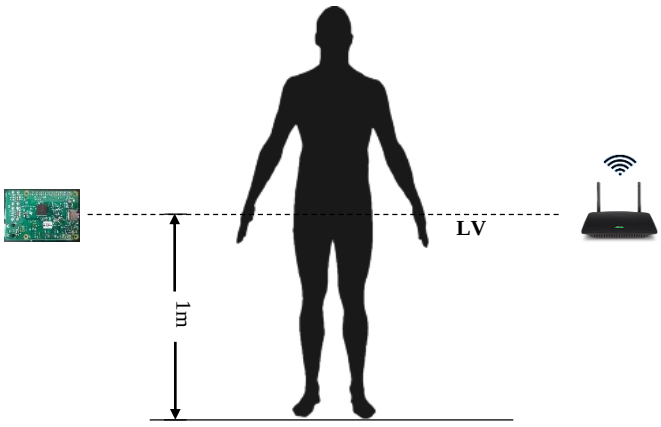

Figura 3.3. Línea de vista. Elaboración propia.

Figura 3.4. Vista lateral del sujeto. Elaboración propia

Si de la Tabla 3.1 se toma el peor caso que sería una 1.64 m/s del sujeto y se sabe que el área del sujeto que interrumpe la LV es de 20 cm. Entonces se sabe que desde el instante en que el sujeto llega a la LV hasta sale de ella transcurre un tiempo de 0.121 s. Mediante el Teorema de Nyquist se puede encontrar la frecuencia de muestreo:

$$T = 0.121s$$

$$F = \frac{1}{0.121} = 8.26\ Hz$$

$$Fs = (8.26)(2) = 16.52\ Hz$$

$$Ts = \frac{1}{16.52Hz} = 0.60s$$

Se concluye que se debe muestrear la señal RSSI con una frecuencia de 16.52 Hz como mínimo, esto equivale a un periodo de 0.60s. En la Tabla 3.4 se muestran los requerimientos de velocidad de muestreo para cada uno de los cinco sujetos de la Tabla 3.3.

Tabla 3.4. Frecuencia de muestreo requerida

Sujeto	**Normal**		**Rápido**	
	Velocidad (m/s)	***Fs requerida Hz***	***Velocidad (m/s)***	***Fs requerida Hz***
1	0.81	8.1	1.48	14.8
2	0.8	8	1.21	12.1
3	1.05	10.5	1.5	15
4	0.76	7.6	1.39	13.9
5	0.85	8.5	1.64	16.5

El sistema operativo Raspbian no es del tipo RTOS y esto trae dos inconvenientes que pueden ser determinantes para el experimento. Primero, es probable que no se pueda muestrear a 16.5 Hz que es el peor de los caso y segundo la frecuencia de muestreo es variable, es decir el espacio temporal entre muestras consecutivas no es siempre el mismo y esto dificulta la aplicación de técnicas de *Procesamiento Digital de Señales*.

Para analizar esos inconvenientes se desarrolló un programa que permite encontrar la frecuencia máxima a la cual se puede muestrear el RSSI en Raspbian. Dicho programa ejecuta consultas al proceso proc/net/wireless de Raspbian mediante la herramienta iwconfig, guarda el dato resultante y guarda también el instante de tiempo en que se capturó el dato. Se capturaron 200 muestras usando el programa. Al analizar las muestras se obtienen los resultados de la Tabla 3.5. En dicha tabla se observa que la velocidad de muestreo no es constante ya que existe un mínimo y un máximo.

Tabla 3.5. Frecuencia de muestreo RSSI en Raspbian

Frecuencia de muestreo		**Periodo de muestreo**	
Mínimo	***Máximo***	***Mínimo***	***Máximo***
11.3636364 Hz	20.8396686 Hz	0.04798541 s	0.088 s

Al contrastar la información la Tabla 3.4 y la Tabla 3.5 se concluye que la Fs que se puede alcanzar en Raspbian usando iwconfig podría no ser suficiente para hacer una detección exitosa en el peor de los casos, es decir, si el sujeto 5 camina rápidamente atravesando la línea de vista y en ese momento coincide que Raspbian bajó su velocidad de muestreo a 11.36 Hz entonces podría

no detectarse. De acuerdo con la máxima frecuencia de muestreo, si el sujeto de prueba de la figura Figura 3.4 camina a una velocidad superior a 4.16 m/s no sería detectado por el sistema. En el siguiente capítulo se detallan los resultados al probar el sistema bajo condiciones similares.

La Figura 3.5 muestra las lecturas de RSSI. El espacio temporal entre lecturas parecer ser la misma excepto entre los 0.35 y 0.43 ms ya que se observa cómo se incrementó el periodo de tiempo entre muestras y por lo tanto se redujo la *Fs*. Este tipo de situaciones se repiten de manera impredecible durante la captura de muestras.

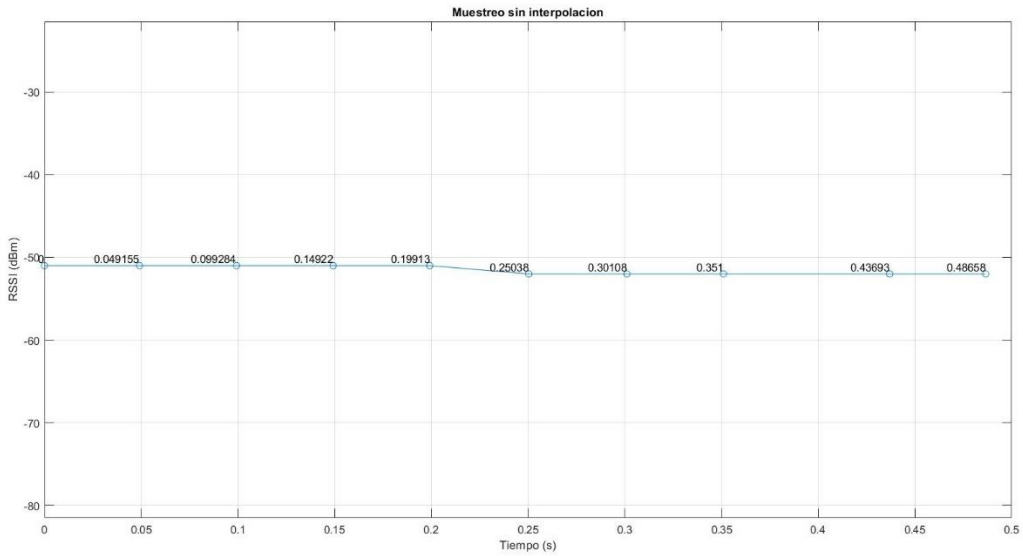

Figura 3.5. Muestreo sin interpolación. Elaboración propia.

Para resolver el problema de la variación de *Fs* se aplicó *interpolación lineal* para obtener una señal con separación uniforme entre muestras. Después de la interpolación la señal quedó como se ve en la gráfica de la Figura 3.6. Se puede ver que ahora las muestras están espaciadas uniformemente a 40 ms.

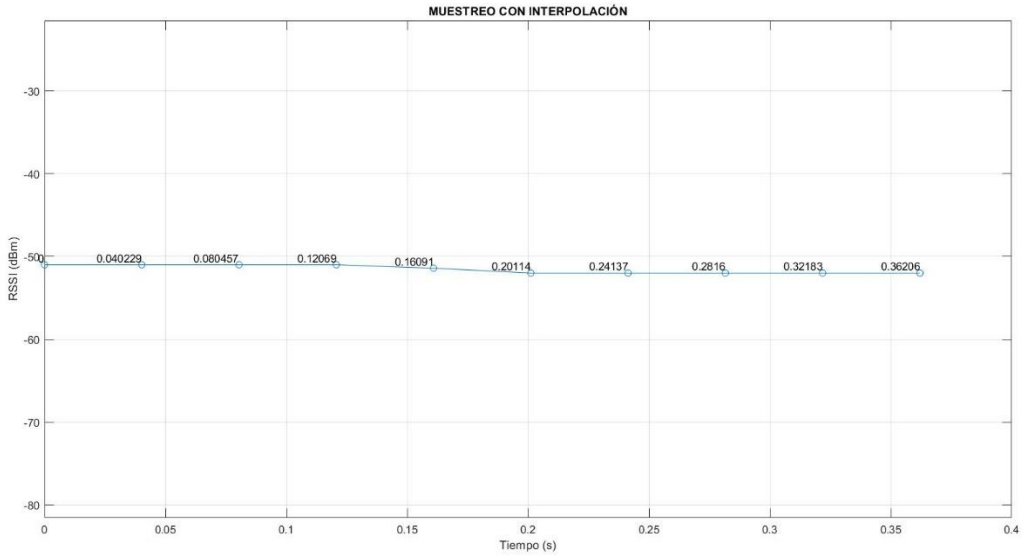

Figura 3.6. Muestreo con interpolación. Elaboración propia.

Una vez que se han determinado la *Fs* y la velocidad al caminar y se ha resuelto la inconsistencia de la *Fs* ya es posible comenzar con la implementación del Método de detección.

Primeramente, es necesario determinar un intervalo de tiempo adecuado para capturar las muestras necesarias que servirán para calcular los umbrales *Umi* y *Ums.* El intervalo se determinó obteniendo la variación máxima de un conjunto de muestras tomadas a una frecuencia 1 Hz durante un periodo de 24 horas estando el área de estudio totalmente ausente de personas. Esta observación se repitió durante los 7 días de una semana dando un total de 604800 muestras. En la Tabla 3.6 se muestran los resultados de estas observaciones. La figura Figura 3.7 muestra el comportamiento de la señal durante un periodo de 24 horas.

Tabla 3.6. Máximos y mínimos

Día	***Min (dBm)***	***Max (dBm)***	***Variación máxima (dBm)***
1	-42	-37	5
2	-41	-37	4
3	-42	-37	5
4	-42	-37	5
5	-41	-37	4
6	-42	-37	5
7	-42	-37	5

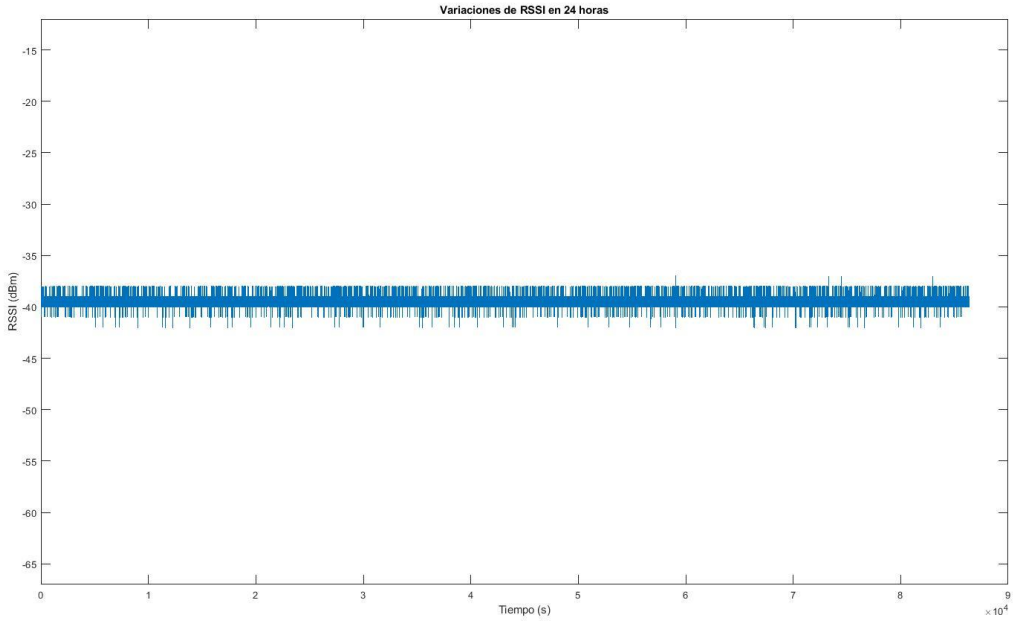

Figura 3.7. Captura de muestras durante 24 horas. Elaboración propia.

En tabla Tabla 2.1 se observa que los valores mínimo y máximo no son constantes sino que pueden variar de un día a otro sin embargo el mínimo nunca es menor a -42 dBm y el máximo nunca sobrepasa los -37 dBm. Con estos datos se calcularon la media y los umbrales *Umi* y *Ums* de acuerdo con las ecuaciones *(3.7)* y *(3.8)*. Los límites resultantes son Ums = -37.5 dB y Umi =--41.9 dB como se muestra en la figura Figura 3.8.

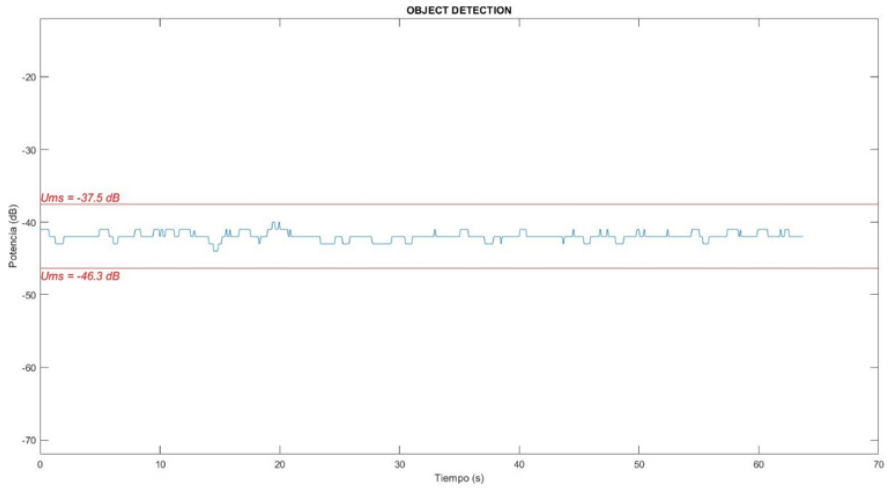

Figura 3.8. Umbrales Umi y Ums. Elaboración propia.

El siguiente paso es capturar las muestras mientras el sujeto interrumpe deliberadamente la línea de vista y hacer una comparación de dichas muestras respecto de *Ums* y *Umi*. Esperando que haya una disminución de la señal en el instante de la interrupción se aplica la ecuación *(3.4)* y entonces se detectará la presencia del sujeto. En la Figura 3.9 se muestra el resultado de realizar una prueba prelimar del sistema y como se puede observar se tiene un resultado positivo. En la Figura 3.7 se muestras los resultados con los cuales operaba el sistema al momento de realizar la prueba.

Tabla 3.7. Prueba preliminar

Variable	***Resultado (dB)***
Mínimo	-38
Máximo	-43
Ums	-37
Umi	-45.4
Detección	-51

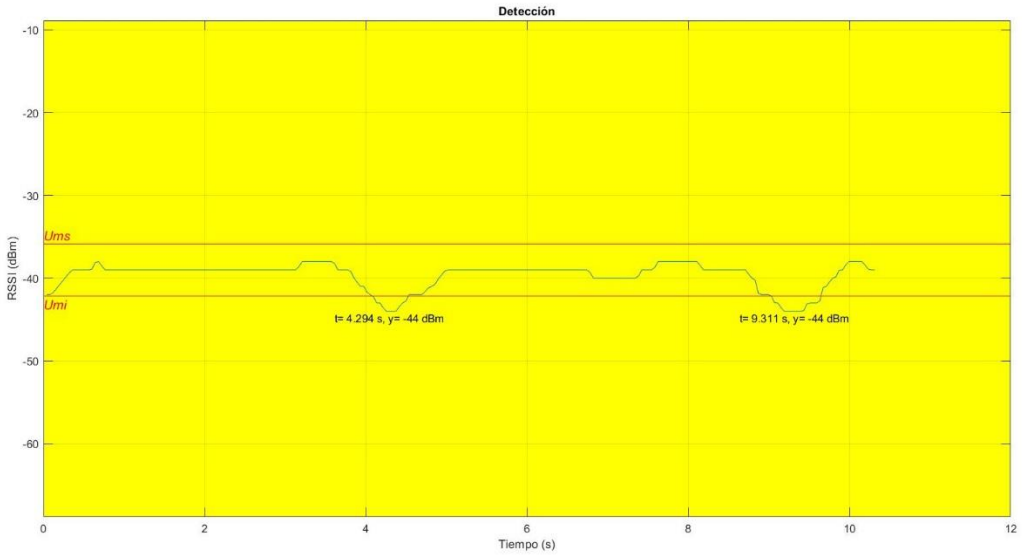

Figura 3.9. Detección. Elaboración propia

.

4. Resultados Experimentales

En el presente capítulo se muestran los resultados obtenidos al probar el sistema bajo diferentes casos de uso. Las pruebas se realizaron bajo las siguientes condiciones:

1. Se realizaron en la misma edificación usada para desarrollar el sistema
2. La ubicación del emisor y receptor dentro de la edificación fue la misma que en el desarrollo del sistema
3. El ambiente circundante (mobiliario, puertas, ventanas) se mantuvo constante.
4. La línea de vista corresponde a la puerta de acceso de la edificación

Los casos de uso son:

1. Detección de caminata a velocidad extremadamente baja
2. Detección de caminata a velocidad baja
3. Detección de caminata a velocidad normal.
4. Detección de caminata a paso veloz

Es importante aclarar que no se usó artefacto alguno que permitiera controlar la velocidad de caminata de los sujetos. Por lo tanto, *los términos velocidad extremadamente baja, velocidad baja, velocidad normal* y *paso veloz* son subjetivos, sin embargo, sí es posible tener una medición precisa de la velocidad a la cual cada uno de los sujetos cruza la línea de vista, por lo tanto, estos datos funcionan como una referencia aceptable para analizar los límites del sistema. En cada caso de prueba se presentan los siguientes análisis estadísticos:

1. Correlación Pearson de *velocidad – potencia mínima*. Mediante este análisis se pretende encontrar la relación entre la velocidad al cruzar la línea de vista y la correspondiente reducción en la potencia de la señal.
2. Correlación Pearson de *velocidad – sujeto potencia*. Mediante este análisis se pretende encontrar la alguna relación entre la complexión física del sujeto y la correspondiente reducción en la potencia de la señal.

3. Probabilidad de detección. Se calcula la probabilidad en base a los aciertos y fallos del sistema.

La Tabla 4.1 presenta datos sobre la complexión de cada uno de los sujetos. La característica “ancho” se refiere a la longitud de la zona efectiva (Figura 3.4):

Tabla 4.1. Complexión de sujetos de sujetos de prueba

Número	***Altura (m)***	***Ancho (m)***
1	1.73	.20
2	1.60	.30
3	1.45	.17
4	1.60	.20

Se pretende evaluar el desempeño del sistema en el entorno para el cual fue propuesto desde la Definición del Proyecto. En este entorno se consideraron 4 sujetos de prueba debido a que es el número de integrantes de una familia típica en México según INEGI, (2015). Para determinar el número de mediciones sobre cada sujeto se hicieron observaciones de una familia real de cuatro integrantes para encontrar el número de veces que cada sujeto interrumpiría la línea de vista durante una semana de 7 días. La Tabla 4.2 muestra el promedio de veces por día en que cada sujeto interrumpiría la línea de vista de acuerdo con las observaciones.

Tabla 4.2. Frecuencia de paso por la línea de vista

Sujeto	***Promedio (veces)***
1	5.4
2	5.7
3	7.7
4	6.2

4.1 Detección de caminata a velocidad extremadamente baja.

Con base en la información de la Tabla 2.1, el sujeto 1 cruza 38 veces la línea de vista en los 7 días una semana. La Tabla 4.3 muestra el análisis de los datos obtenidos.

Tabla 4.3. Resultados de sujeto 1 a velocidad extremadamente baja

Correlación velocidad - potencia	Probabilidad de detección
0.24	100

Con base en la información de la Tabla 4.2, el sujeto 2 cruza 40 veces la línea de vista en los 7 días una semana. La Tabla 4.4 muestra el análisis de los datos obtenidos.

Tabla 4.4. Resultados de sujeto 2 a velocidad extremadamente baja

Correlación velocidad - potencia	***Probabilidad de detección***
0.24	100

Con base en la información de la Tabla 4.2, el sujeto 3 cruza 54 veces la línea de vista en los 7 días una semana. La Tabla 4.5 muestra el análisis de los datos obtenidos.

Tabla 4.5. Resultados de sujeto 3 a velocidad extremadamente baja

Correlación velocidad - potencia	***Probabilidad de detección***
0.24	100

Con base en la información de la Tabla 4.2, el sujeto 4 cruza 43 veces la línea de vista en los 7 días una semana. La Tabla 4.6 muestra el análisis de los datos obtenidos.

Tabla 4.6. Resultados de sujeto 4 a velocidad extremadamente baja

Correlación velocidad - potencia	***Probabilidad de detección***
0.085	100

4.2 Detección de caminata a velocidad baja.

Con base en la información de la Tabla 4.2, el sujeto 1 cruza 38 veces la línea de vista en los 7 días una semana. La Tabla 4.7 muestra el análisis de los datos obtenidos.

Tabla 4.7. Resultados de sujeto 1 a velocidad baja

Correlación velocidad - potencia	***Probabilidad de detección***
0.29	100

Con base en la información de la Tabla 4.2, el sujeto 2 cruza 40 veces la línea de vista en los 7 días una semana. La Tabla 4.8 muestra el análisis de los datos obtenidos.

Tabla 4.8. Resultados de sujeto 2 a velocidad baja

Correlación velocidad-potencia	***Probabilidad de detección***
0.47	100

Con base en la información de la Tabla 4.2, el sujeto 3 cruza 54 veces la línea de vista en los 7 días una semana. La Tabla 4.9 muestra el análisis de los datos obtenidos.

Tabla 4.9. Resultados de sujeto 3 a velocidad baja

Correlación velocidad-potencia	***Probabilidad de detección***
0.32	100

Con base en la información de la Tabla 4.2, el sujeto 4 cruza 43 veces la línea de vista en los 7 días una semana. La Tabla 4.10 muestra el análisis de los datos obtenidos.

Tabla 4.10. Resultados de sujeto 4 a velocidad baja

Correlación velocidad-potencia	***Probabilidad de detección***
0.10	100

4.3 Detección de caminata a velocidad normal.

Con base en la información de la Tabla 4.2, el sujeto 1 cruza 38 veces la línea de vista en los 7 días una semana. La Tabla 4.11 muestra el análisis de los datos obtenidos.

Tabla 4.11. Resultados de sujeto 1 a velocidad normal

Correlación velocidad-potencia	***Probabilidad de detección***
0.71	100

Con base en la información de la Tabla 4.2, el sujeto 2 cruza 40 veces la línea de vista en los 7 días una semana. La Tabla 4.12 muestra el análisis de los datos obtenidos.

Tabla 4.12. Resultados de sujeto 2 a velocidad baja

Correlación velocidad-potencia	***Probabilidad de detección***
0.37	100

Con base en la información de la Tabla 4.2, el sujeto 3 cruza 54 veces la línea de vista en los 7 días una semana. La Tabla 4.13 muestra el análisis de los datos obtenidos.

Tabla 4.13. Resultados de sujeto 3 a velocidad baja

Correlación velocidad-potencia	***Probabilidad de detección***
0.3	100

Con base en la información de la Tabla 4.2, el sujeto 4 cruza 43 veces la línea de vista en los 7 días una semana. La Tabla 4.18 muestra el análisis de los datos obtenidos.

Tabla 4.14. Resultados de sujeto 4 a velocidad baja

Correlación velocidad-potencia	***Probabilidad de detección***
0.09	100

4.4 Detección de caminata a paso veloz.

Con base en la información de la Tabla 4.2, el sujeto 1 cruza 38 veces la línea de vista en los 7 días una semana. La Tabla 4.15 muestra el análisis de los datos obtenidos.

Tabla 4.15. Resultados de sujeto 1 a paso veloz

Correlación velocidad-potencia	*Probabilidad de detección*
0	0.13

Con base en la información de la Tabla 4.2, el sujeto 2 cruza 40 veces la línea de vista en los 7 días una semana. La Tabla 4.16 muestra el análisis de los datos obtenidos.

Tabla 4.16. Resultados de sujeto 2 a paso veloz

Correlación velocidad-potencia	*Probabilidad de detección*
0.02	0.9

Con base en la información de la Tabla 4.2, el sujeto 3 cruza 54 veces la línea de vista en los 7 días una semana. La Tabla 4.17 muestra el análisis de los datos obtenidos.

Tabla 4.17. Resultados de sujeto 3 a paso veloz

Correlación velocidad-potencia	*Probabilidad de detección*
0	0.03

Con base en la información de la Tabla 4.2, el sujeto 4 cruza 43 veces la línea de vista en los 7 días una semana. La Tabla 4.18 muestra el análisis de los datos obtenidos.

Tabla 4.18. Resultados de sujeto 4 a paso veloz

Correlación velocidad-potencia	*Probabilidad de detección*
0	0

5. Conclusiones y Trabajo Futuro

Las pruebas evidenciaron que es parcialmente posible detectar presencia humana mediante el procesamiento de las variaciones de potencia de una señal WiFi. El sistema mostró gran efectividad mientras los sujetos crucen la línea de vista a baja velocidad, sin embargo, mientras la velocidad fue incrementando gradualmente la probabilidad de detección del sistema llegó a ser cero.

El problema de la detección a altas velocidades está muy relacionado con la velocidad de muestreo la cual estuvo muy limitada por las herramientas empleadas, es decir, el programa iwconfig de un sistema Linux no RTOS. Es posible hacer mejoras en las herramientas de software desarrolladas para incrementar la velocidad de muestreo, aunque no es posible asegurar con certeza hasta qué punto debido a que Raspbian no mostró un comportamiento determinístico.

Las características observadas en las mediciones realizadas a través de toda la realización de este trabajo hacen concluir que, de momento, con un sistema como el que se propuso no es posible hacer un reconocimiento gestual debido a que los movimientos finos de una persona en la línea de vista impactan de manera casi nula en las mediciones.

Existen varias vías para continuar con este trabajo. Como primer paso se pretende usar una herramienta diferente a iwconfig que tenga mejor desempeño para obtener frecuencias de muestreo superiores y hacer posible una detección de personas cruzando la línea de vista a mayor velocidad.

Algunos routers tienen la capacidad para ser reprogramados con algunas versiones de OpenWrt. Mediante este kernel Linux es posible acceder a parámetros adicionales de la capa PHY. En una segunda etapa, como trabajo futuro se pretende sustituir la Raspberry y en su lugar usar un usar un router WiFi de última generación regrabado con OpenWrt para acceder a los parámetros y configuraciones MIMO de manera que se puedan obtener valores online de Channel State Information. Esto servirá para extender este trabajo hacia técnicas de reconocimiento gestual y movimientos tan finos como la respiración humana. Teniendo estos desarrollos la tercera etapa consistiría en crear un sistema de reconocimiento personal basado en radiofrecuencia que sirva de base para aplicaciones de domótica.

Existen sin embargo muchos otros caminos que se pueden seguir con base en lo investigado. Otro camino consistiría en usar transceptores de última generación con capacidad para proporcionar una representación de valores RSSI más allá de los 256 niveles. Con un desarrollo así se podría lograr reconocimiento gestual y movimientos finos mediante solo el valor RSSI. Por ultimo también podría explorarse la posibilidad de acceder al valor Delay Spread mediante un firmware modificado para algún chipset, esto abriría la puerta para calcular Efecto Doppler.

6. Bibliografía

Aruba, N. 2014. 802.11ac In-Depth.

Carpenter, T., y L. Badman. 2016. CWAP®Certified Wireless Analysis Professional Official Study Guide: CWAP-402. CertiTrek Publishing.

Flickenger, R. 2006. Wireless Networking in the Developing World. Limehouse Book Sprint Team.

Fraden, J. 2010. Handbook of Modern Sensors: Physics, Designs, and Applications. Springer New York.

Gast, M. 2005. 802.11 Wireless Networks: The Definitive Guide. O'Reilly Media.

Gast, M. S. 2013. 802.11ac: A Survival Guide: Wi-Fi at Gigabit and Beyond. O'Reilly Media.

Hampton, J. R. 2013. Introduction to MIMO Communications. Cambridge University Press.

Ho, Q. D., D. Tweed, y T. Le-Ngoc. 2016. Long Term Evolution in Unlicensed Bands. Springer International Publishing.

IEEE. 2014. ISO/IEC/IEEE International Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (. ISO/IEC/IEEE 8802-11:2012/Amd.3:2014(E). 1-634. doi:10.1109/IEEESTD.2014.6774849. Available from: http://dx.doi.org/10.1109/IEEESTD.2014.6774849

IEEE, I. 2010. QUICK GUIDE TO IEEE 802.11 ACTIVITIES. QUICK Guid. TO IEEE 802.11 Act. Available from: http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm

IFT. 2013. ¿Qué es el IFT? Available from: http://www.ift.org.mx/que-es-el-ift/que-es-el-ift

IFT. 2017. Cuadro Nacional de Frecuencias. Diario Oficial de la Federación, Ciudad de México.

INEGI. 2015. Encuesta Intercensal 2015.

J.Berg. 2011. The IEEE 802.11 standarization Its history, specifications, implementations, and future.

Kaemarungsi, K., y P. Krishnamurthy. 2012. Analysis of WLAN's Received Signal Strength Indication for Indoor Location Fingerprinting. Pervasive Mob. Comput. 8:292-316. doi:10.1016/j.pmcj.2011.09.003. Available from: http://dx.doi.org/10.1016/j.pmcj.2011.09.003

Kaltiokallio, O., M. Bocca, y L. M. Eriksson. 2010. Distributed RSSI Processing for Intrusion Detection in Indoor Environments. En: Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks. ACM, New York, NY, USA. p. 404-405. Available from: http://doi.acm.org/10.1145/1791212.1791276

Lee, P. W. Q., W. K. G. Seah, H. P. Tan, y Z. Yao. 2009. Wireless sensing without sensors #x2014; An experimental approach. En: 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications. p. 62-66.

Li, Y., D. Li, W. Cui, y R. Zhang. 2011. Research based on OSI model. En: 2011 IEEE 3rd International Conference on Communication Software and Networks. p. 554-557.

Lin, Q., y Y. Yue. 2015. Device-Free Passive Human Detection Using Wi-Fi Technology: Current State and Future Trend. En: 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom). p. 1717-1723.

Lin, W.-C., W. K. G. Seah, y W. Li. 2011. Exploiting radio irregularity in the Internet of Things for automated people counting. En: 2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications. p. 1015-1019.

López, C. J. 2013. Percepción de inseguridad en México. Rev. Mex. Opinión Pública. 0:13-29. Available from: http://www.revistas.unam.mx/index.php/rmop/article/view/43663

Luong, A., A. S. Abrar, T. Schmid, y N. Patwari. 2016. RSS step size: 1 dB is not enough! En:

HotWireless@MobiCom.

Molisch, A. F. 2010. Wireless Communications. Wiley.

Pallás-Areny, R., y J. G. Webster. 2001. Sensors and signal conditioning. J. Wiley.

Perahia, E. 2008. IEEE 802.11n Development: History, Process, and Technology. Commun. Mag. IEEE. 46:48-55.

Pu, Q., S. Gupta, S. Gollakota, y S. Patel. 2013. Whole-home Gesture Recognition Using Wireless Signals. En: Proceedings of the 19th Annual International Conference on Mobile Computing & Networking. ACM, New York, NY, USA. p. 27-38. Available from: http://doi.acm.org/10.1145/2500423.2500436

Puccinelli, D., A. Förster, A. Puiatti, y S. Giordano. 2011. Radio-based trail usage monitoring with low-end motes. En: 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). p. 196-201.

Rico, E. 2016. Puntos básicos del Modelo OSI – Parte 1: Aspectos generales. Available from: http://www.ermesh.com/modelo-osi-parte-1-aspectos-generales/

Snaterse, M., R. Ton, A. D Kuo, y M. Donelan. 2011. Distinct fast and slow processes contribute to the selection of preferred step frequency during human walking. J. Appl. Physiol. 110:1682-1690.

Tan, S., y J. Yang. 2016. Fine-grained gesture recognition using WiFi. En: 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). p. 257-258.

Tse, D., y P. Viswanath. 2005. Fundamentals of Wireless Communication. Cambridge University Press.

Wei, B., W. Hu, M. Yang, y C. T. Chou. 2015. Radio-based Device-free Activity Recognition with Radio Frequency Interference. En: Proceedings of the 14th International Conference on Information Processing in Sensor Networks. ACM, New York, NY, USA. p. 154-165. Available from: http://doi.acm.org/10.1145/2737095.2737117

Wi-Fi Alliance. 2016. Certification Overview: Process. Certif. Overv. Process. 7.

Wu, Y., y T. S. Huang. 1999. Vision-based gesture recognition: A review. 103-115. Available from: http://link.springer.com/content/pdf/10.1007/3-540-46616-910.pdf

Zhang, J., B. Wei, W. Hu, y S. S. Kanhere. 2016. WiFi-ID: Human Identification Using WiFi Signal. En: 2016 International Conference on Distributed Computing in Sensor Systems (DCOSS). p. 75-82.

Anexo A. Equipo Utilizado

El equipo que se utilizó para las pruebas fue:

- Un router TL-WR480N
- Un sistema Raspberry Pi 3B
- Una computadora Toshiba Satellite E-55ª
- El software utilizado para desarrollar los algoritmos es Matlab R2017B