PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UNA RED DE SENSORES PARA EL SISTEMA DE DETECCIÓN DE ROGUE APS EN LA RED WIFI DEL CAMPUS PUCP

Tesis para optar el Título de Ingeniero de las Telecomunicaciones, que presenta el bachiller:

ENZO ENRIQUE SALDARRIAGA RHOR

ASESOR: PhD. César Augusto Santiváñez

Lima, Diciembre del 2015

Resumen

El trabajo desarrollado en la presente tesis consiste el diseño de una red de sensores para el sistema de detección de Rogue APs en la red WiFi del campus PUCP para las bandas de 2.4GHz y 5GHz.

El primer capítulo presenta una descripción del marco problemático actual sobre la importancia de la seguridad en las redes inalámbricas. Luego, se señala la importancia del sistema de detección planteado al inicio de la tesis. Posteriormente, se definen los sistemas teóricos que permiten la detección y localización de los Rogue AP. Finalmente, se muestra el estado del arte de dispositivos que permiten la detección y métodos de mitigación de Rogue APs.

En el segundo capítulo se exponen la problemática de la tesis y se plantea los requerimientos y razones por la cual se utiliza la teoría de NP-Complete para el diseño de la red. Luego, se discute sobre el problema general que representa el diseño de una red de sensores con triple cobertura posible.

El tercer capítulo consiste en el diseño de modelos de optimización y heurísticas para la red de sensores. Primero, se expone el proceso con el cual se maneja la información para el desarrollo de los algoritmos. Segundo, se muestran la estructura de los modelos de programación y lógica del algoritmo con los cuales se puede diseñar una red de sensores para combatir la presencia de un Rogue AP.

El cuarto capítulo comienza explicando el escenario y parámetros sobre los cuales se basaron los algoritmos generados para el diseño de la red de sensores. Luego, se muestran los resultados finales obtenidos y una discusión sobre el grado de cobertura obtenido.

Por último, se presentan las conclusiones y recomendaciones a las que se llegó después de terminar la presente tesis.

FACULTAD DE
CIENCIAS E INGENIERÍA

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE TELECOMUNICACIONES

Título	:	Diseño de una red de sensores para el sistema de detección de Rogue APs en la red WiFi del campus PUCP.
Área	:	Telecomunicaciones ✓ 309
Asesor	:	César A. Santiváñez, Ph D.
Alumno	:	Enzo Enrique Saldarriaga Rhor
Código	:	20092358
Fecha	:	13/09/2015

PONTIFICIA UNIVERSIDAD CAT
Facultad de Ciencias
16 DIC
MIGUEL MEJIA
DECANO

Descripción y Objetivos

El *Rogue AP* es un Punto de Acceso (AP, por sus siglas en inglés) inalámbrico que ha sido conectado sin autorización a la red fija, o un AP que suplanta la identidad (BSSID) de un AP válido dentro de la red WiFi Empresarial, como la red WiFiPUCP. Un *Rogue AP* representa una amenaza para la seguridad de la red, debido a que provee al atacante una puerta trasera de acceso, evitando medidas convencionales de seguridad en redes fijas, como los *firewalls*. Así mismo, un *Rogue AP* puede capturar y robar información privada y valiosa, como credenciales de acceso, de cualquier usuario inadvertido en su rango de cobertura (*HoneyComb Attack*).

Los sistemas de prevención de intrusos inalámbricos (WIPS) son un tipo de sistema de seguridad que permite el monitoreo de una red inalámbrica por medio del espectro radioeléctrico en búsqueda de *Rogue APs* u otras amenazas. Los WIPS son capaces de detectar, bloquear, generar alarmas e incluso localizar la posición de un *Rogue AP*, para lo cual se requiere la instalación de sensores inalámbricos especializados encargados del monitoreo del espectro; o en su defecto dedicar tiempo de operación de los AP existentes para fines de monitoreo, lo que impacta negativamente en la experiencia de usuario de los usuarios móviles. Una de los sensores compatibles con los Puntos de Acceso (AP) de la red *WiFiPUCP* son los módulos de seguridad inalámbrica e inteligencia espectral (WSSI) de Cisco. El módulo WSSI se instala de forma adjunta a un AP Cisco Aironet de la serie 3600 o 3700 (instalados en la red WiFiPUCP), reusando las antenas y circuitos de recepción sin alterar el normal funcionamiento del AP.

El objetivo de la presente tesis es el diseño de una red de sensores WSSI (número y ubicación) dentro del campus de la PUCP que permita la ubicación de *Rogue APs*. El diseño de la red es elaborada usando una combinación de modelos predictivos en base a planos de los edificios de la PUCP (dimensiones y obstáculos), las posiciones candidatas para los sensores, y los valores del mapa de atenuación de RF.

El diseño de la red de sensores WSSI implica la medición y recolección de la relación señal/ruido para los diversos pabellones dentro del campus, el procesamiento de la información obtenida para determinar la cobertura de señal inalámbrica de los puntos de detección, la formulación del problema de localización de sensores como un problema de optimización combinatoria buscando minimizar el número de sensores sujeto a la condición de poder triangular la posición de los Rogue APs, la implementación de un algoritmo (heurística) con la finalidad de encontrar una solución en tiempo razonable a la instancia representada por la topología de la red WiFiPUCP, y finalmente la evaluación de la red de sensores propuesta vía simulaciones.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Especialidad de Ingeniería de las Telecomunicaciones
Ing. GUMERCINDO BARTRA GARDINI
Coordinador

FACULTAD DE
CIENCIAS E INGENIERÍA

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE TELECOMUNICACIONES

Título : Diseño de una red de sensores para el sistema de detección de Rogue APs en la red WiFi del campus PUCP.

Índice

Máximo: 100 páginas

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Especialidad de Ingeniería de las Telecomunicaciones
Ing. GUMERCINDO BARTRA GARDINI
Coordinador

Dedicatoria

Dedico esta Tesis a Dios, a mis padres, familiares, amigos y a todos aquellos que me apoyaron para poder lograrlo, pues es a ellos a quien les debo haberme permitido llegar a este punto

Agradecimiento

A Dios por haberme dado una vida para vivir en este mundo.

A mis padres, por todo el sacrificio, entrega y amor que demuestran en mí desde niño, y por enseñarme a siempre dar todo mi esfuerzo y seguir mejorando.

A mi hermana, por siempre estar conmigo y apoyarme.

A mis tíos y abuelos, por ayudarme en momentos cruciales y siempre apoyarme aun cuando se encontraban lejos.

A mis amigos, por darme su apoyo y motivarme a mejorar.

Al Dr. Cesar Augusto Santivañez, por orientarme y aconsejarme durante el desarrollo de la presente tesis. Asimismo, por recordarme siempre a hacer el mejor trabajo y a trazarse metas en lo que uno se propone.

ÍNDICE

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

En los sistemas de comunicación actuales, un Rogue AP es un Punto de Acceso (AP, por sus siglas en inglés) inalámbrico que ha sido conectado sin autorización a la red fija, o un AP que suplanta la identidad (BSSID) de un AP válido dentro de una red Wi-Fi Empresarial, como la red de la universidad "redpucp". Un Rogue AP representa una amenaza para la seguridad de la red, debido a que provee al atacante una puerta trasera de acceso, evitando medidas convencionales de seguridad en redes fijas, como los firewalls. Asimismo, un Rogue AP puede ser utilizado para capturar y robar información privada y valiosa, como credenciales de acceso, de cualquier usuario inadvertido en su rango de cobertura (HoneyComb Attack).

Para lograr combatir este tipo de amenazas es que surgen los sistemas de prevención de intrusos inalámbricos (WIPS), los cuales permite el monitoreo de una red inalámbrica por medio del espectro radioeléctrico en búsqueda de Rogue APs u otras amenazas. Los WIPS son capaces de detectar, bloquear, generar alarmas e incluso localizar la posición de un Rogue AP, para lo cual se requiere la instalación de sensores inalámbricos especializados encargados del monitoreo del espectro; o en su defecto dedicar tiempo de operación de los AP existentes para fines de monitoreo, lo que impacta negativamente en la experiencia de usuario de los usuarios móviles.

Una de los sensores compatibles con los Puntos de Acceso (AP) de la red "redpucp" son los módulos de seguridad inalámbrica e inteligencia espectral (WSSI) de Cisco. Dicho módulo se instala de forma adjunta a un AP Cisco Aironet de la serie 3600 o 3700, los cuales forman parte de la infraestructura para la red inalámbrica "redpucp", y funcionan reusando las antenas y circuitos de recepción sin alterar el normal funcionamiento del AP.

El objetivo de la presente tesis es el diseño de una red de sensores WSSI, número y ubicación de módulos, dentro del campus de la PUCP que permita la ubicación de Rogue APs. Esto se lograra mediante una combinación de

modelos predictivos en base a planos de los edificios de la PUCP (dimensiones y obstáculos), posiciones candidatas para los sensores y los valores del mapa de atenuación de RF; los cuales serán obtenidos mediante la medición y recolección de la relación señal/ruido para los diversos pabellones dentro del campus, el procesamiento de la información obtenida para determinar la cobertura de señal inalámbrica de los puntos de detección y la formulación del problema de localización de sensores como un problema de optimización combinatoria buscando minimizar el número de sensores sujeto a la condición de poder triangular la posición de los Rogue APs

Capítulo 1

Lidiando con Ataques Inalámbricos

Originalmente lo que se inició con la experimentación que permita comunicar dos computadores ha llevado al nacimiento, descubrimiento y desarrollo del mundo de las telecomunicaciones entre ordenadores. En este aspecto, durante los años 70 se produjo un acontecimiento histórico en el mundo de las telecomunicaciones, el cual fue los primeros diseños que redes de computadoras conocidos como ARPANET y ALOHAnet, tal que ARPANET utiliza las líneas telefónicas arrendadas y ALOHAnet utilizaba las ondas de radio. Posteriormente, ARPANET se fusiono con otras entidades, dando origen al protocolo TCP/IP y al termino conocido como internet. De esta forma empezó el desarrollo de la redes de computadoras, que el día de hoy han alcanzado una presencia tan alta que los usuarios esperan acceso permanente, sin importar su ubicación. Es por esto que en la actualidad existe una gran inclinación hacia el uso de la tecnología inalámbrica, con su correspondiente ubicuidad.

La tecnología WLAN basada en el protocolo 802.11 es una de las tecnologías de acceso inalámbrico más populares y que ha sido ampliamente implementada por diversas empresas, operadoras, e incluso gobiernos. Pese a la existencia de tecnologías móviles como 3G, HSPA, LTE, entre otras, la tecnología WLAN es una de las soluciones más populares de comunicaciones debido a su relativa facilidad de implementación, menores costos, movilidad y flexibilidad. Por tal motivo, existe una creciente tendencia de implementación de redes WLAN en lugares públicos como aeropuertos, cafés, centros comerciales, campus universitarios y plazas públicas. [8,11]

El creciente uso del Internet ha causado una creciente producción de equipos que soporten el estándar para Wi-Fi como celulares de nueva generación, laptops, PDA's. Así mismo, este fenómeno ha ocasionado nuevas tendencias que afectan el modo en el cual se implementaban las redes, desarrollando la tendencia denominada como Bring Your Own Device ("Trae tu propio dispositivo", o BYOD, por sus siglas en ingles) y creación de diversas aplicaciones críticas como el procesamiento de información, gestión de inventario, telefonía VoIP las cuales son soportadas por una red WLAN. No obstante, este crecimiento conlleva a su vez un alto costo en el desarrollo de nuevos tipos de hardware y software que permitan salvaguardar datos críticos de forma eficiente, pero sobretodo que sean capaz de prevenir los ataques cibernéticos sin desagradar la calidad de experiencia de los usuarios. [6,12]

En el presente capitulo se describen tecnologías inalámbricas populares basadas en TCP/IP, así como una serie de herramientas que actualmente se utilizan para mejorar la seguridad de las redes Wi-Fi y algunos de los ataques más comunes que sufren las redes, haciendo enfoque en la suplantación de identidad de Access Points de una red inalámbrica, conocido como “Rogue AP”. En los capítulos siguientes se diseñará una red de sensores WSSI que permita detectar y neutralizar estos ataques.

1.1. Redes Inalámbricas

Las redes inalámbricas, en ingles Wireless Networks, son aquellas redes que se comunican por un medio de transmisión no guiado, sin cables, mediante ondas electromagnéticas. De forma que han existido diversos intentos de desarrollos de redes inalámbricas con diferente vertientes de tecnologías. Una de ellas es denominada y basada en la tecnología infrarroja, que ha sido utilizada exitosamente para las comunicaciones de dispositivos entre sí y no para el acceso a redes; debido principalmente al alcance limitado que tienen las ondas infrarrojas puesto que no son capaces de atravesar objetos opacos. Otra tecnología inalámbrica es la basada en propagación de ondas acústicas, usada en comunicaciones bajo el agua, donde no es factible la propagación de ondas electromagnéticas. Sin embargo, tanto la velocidad de propagación como la de transmisión son demasiado bajas para la mayoría de aplicaciones.

En este trabajo, se realizara un enfoque en las redes inalámbricas basadas en Radio Frequency (RF), que gracias a su combinación de costo, alcance y velocidad, han logrado la máxima aceptación y adopción.

En la actualidad existen diversas formas de implementar redes inalámbricas, así como diversos estándares de implementación, por los cuales existen organizaciones internacionales que formalizan los estándares para el uso correctos de redes inalámbricas. Las principales entidades son la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), la UIT (Unión Internacional de Telecomunicaciones) y la IETF (Internet Engineering Task Force), que se encargan de dictar las normas llamadas RFC, en donde se rige el tráfico de internet para redes de largo y corto alcance.

1.1.1. Clasificación de las redes inalámbricas según su cobertura

Las redes inalámbricas se pueden clasificar teniendo en cuenta como parámetro principal su rango de cobertura. En la siguiente figura se muestra la clasificación de

las principales tecnologías usadas en la actualidad en función de su rango de cobertura.

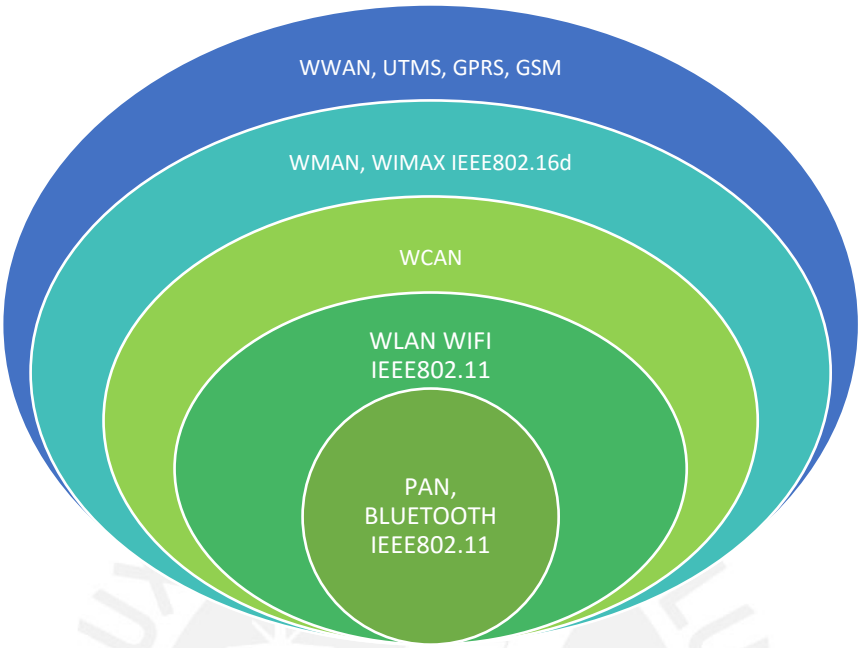


Figura 1-1: Clasificación de las tecnologías inalámbricas.
Fuente: [7]

Redes Inalámbricas de área personal (WPAN)

Las WPAN son redes inalámbricas de corto alcance que abarcan un área máxima de algunos pocos metros. Este tipo de red es usada generalmente para conectar dispositivos periféricos o dispositivo de salida o entrada de datos como son las impresoras, mouses e incluso algunos electrodomésticos. Así mismo, esta red también puede ser utilizada para conectar de forma inalámbrica dos computadoras cercanas u otros dispositivos inalámbricos como los celulares inteligentes o PDAs.

Actualmente, existen soluciones, como Bluetooth, que operan en frecuencias no licenciadas o libreas para instrumentación, ciencia y medicina en la banda de 2.4GHz, banda de 5GHz e incluso mayores a estas. WPAN es un concepto de red dinámico que debe emplearse en conjunto con soluciones de técnicas apropiadas a la arquitectura, protocolos, administración y seguridad.

Redes inalámbricas de área local (WLAN)

Las redes de área local inalámbrica, Wireless Local Area Network (WLAN) son redes inalámbricas de área local que abarcan un área máxima de algunas decenas de metros, equivalente a uno o más ambientes. Una WLAN es un sistema de

comunicación de datos inalámbricos flexibles, el cual es altamente utilizado como una alternativa a las redes cableadas o como una extensión de las mismas. Las WLAN utilizan ondas electromagnéticas para enlazas los equipos conectados a la red, en lugar de utilizar los cables coaxiales o fibra ópticas que se utilizan convencionalmente en las redes locales cableadas.

El objetivo fundamental de las redes WLAN es el de proporcionar la facilidad de desplazamiento sin perder conectividad que no es disponible en los sistemas cableados con la finalidad de formar una red total donde coexistan ambos tipos de sistemas. Por otra parte, el principal atractivo de las WLAN es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

Sin embargo, no se espera que las redes inalámbricas lleguen a reemplazar totalmente a las redes cableadas. Debido a que las redes cableadas son capaces de ofrecer mayores velocidades de transmisión que las redes inalámbricas. Por tal motivo, se suele plantear una solución que utiliza el sistema inalámbrico como medio de acceso a la red y el medio alámbrico como la parte principal de la red. [3]

Redes inalámbricas de área de Campus (WCAN)

Las redes inalámbricas de campus (WCAN) son redes inalámbricas que abarcan el área de un edificio, como por ejemplo una empresa, hospital o un hotel, o un campus, como un conjunto de edificios como la sede principal de una corporación, o el campus de una universidad. Una red WCAN puede ser formada como la combinación de varias WLAN bajo un mismo dominio de control. Por ejemplo, una Enterprise WiFi es formada por varias WLANs con el mismo BSSID, servidor de autenticación, y capacidad de movilidad entre ellas. Las WCAN son diseñadas para soportar los requerimientos de aplicaciones y distribuir un alto nivel de experiencia de usuarios.

Estas redes fueron diseñadas para cumplir con los requerimientos cliente/servidor de aplicaciones y servicios compartidos usando laptops. Actualmente, el rango de aplicaciones y protocolos se ha expandido mientras que los usuarios finales se han vuelto más dependientes del uso de WCAN para soportar la movilidad y consistencia de la conectividad. Cada vez más, se ve una integración de la red WCAN y la red fija del campus, donde el usuario espera el mismo nivel de servicio y privilegios sin importar el medio de conexión, ya sea fijo o inalámbrico. Es decir, las redes inalámbricas se están convirtiendo en ciudadanos propios del mundo digital y no una simple capa.

Redes inalámbricas de área metropolitana (WMAN)

Las WMAN o también conocidas como WLL, del inglés Wireless Local Loop, se basan en el estándar IEEE 802.16.d. Las WMAN son redes diseñadas para tener un rango de cobertura de decenas de kilómetros. Se caracteriza debido al hecho de que existen redes de área metropolitana basadas en WiMAX (Worldwire Interoperability for Microwave Access), el cual es un protocolo de comunicaciones inalámbrico basado en la norma IEEE 802.16. WiMAX es un protocolo similar a Wi-Fi, pero con una mayor área de cobertura y ancho de banda. Por otro lado, también es posible encontrar otros sistemas de comunicaciones como LMDS (Local Multipoint Distribution Service)

Redes inalámbricas de área extensa (WWAN)

Las WWAN, Wireless Wide Area Network, son las redes inalámbricas que tienen el alcance geográfico más grande. Así mismo, una WWAN difiera de otras tecnologías inalámbricas debido a que utiliza principalmente tecnologías de la red celular de comunicaciones móviles como es WiMAX, UMTS, GMS, GPRS, EDGE, HSPA y 3G para transferir datos.

1.2. Retos en redes inalámbricas

Desde los primeros esquemas del estándar 802.11 para las redes inalámbricas publicados por la IEEE, se han realizado una vasta cantidad de modificaciones que han permitido mejorar la calidad del servicio, lo cual ha permitido brindar una mayor cantidad de ventajas a los usuarios de esta tecnología. No obstante, aun con todas sus ventajas, las redes inalámbricas presentan una serie de retos. Por un lado, la movilidad de sus usuarios y el dinamismo de las condiciones del canal presenta un reto para la implementación de radios que soporten al mismo tiempo largo alcance, alta velocidad de usuarios, y alta tasa de transmisión. Por otro lado, el cambiante estado de la red (espectro compartido, localización de usuarios y tráfico, entre otros) presenta retos para la gestión de la red. En este trabajo nos enfocaremos en la gestión de la red, y no en la capa física.

En esta sección, discutiremos brevemente los tres principales retos a la gestión de la red: la movilidad de los usuarios, el espectro compartido, y las vulnerabilidades a la seguridad que presenta el acceso compartido.

1.2.1. Gestión de Movilidad

Conforme la cobertura de la red se expande y los dispositivos móviles aumentan, las redes empresariales y de campus, las WMAN, y las WWAN deben ser capaces de brindar una total capacidad de acceso de aplicaciones directamente a sus usuarios móviles. En este sentido, Los usuarios cursan por medio de múltiples puntos de acceso (p.ej., WLAN), usando múltiples tipos de conexiones y se topan con distintas áreas de coberturas, no obstante, el usuario espera obtener el mismo nivel de confiabilidad y disponibilidad continua de los recursos de la red.

La gestión de movilidad emerge como uno de los más importantes y desafiantes problemas para las redes inalámbricas en ambientes empresariales y campus. La gestión de movilidad permite que las redes sean capaces de localizar a un usuario móvil que se encuentra conectado a un determinado punto para la transmisión de los paquetes de data, y mantener la conexión de dicho mientras se mantiene un cambio del punto de acceso.

El desafío de este proceso no se encuentra focalizado respecto al punto de acceso en sí mismo, sino durante el proceso de transferencia (HandOff). Este proceso de transferencia se da a cabo cuando un dispositivo cliente se encuentra asociándose con el siguiente punto de acceso que posee la señal más fuerte. Este proceso de transferencia debe realizar sin que el usuario pierda su proceso de descarga o llamada.

Principalmente, existen tres procesos de transferencia. El primer proceso, escaneo, se realiza cuando un dispositivo se traslada lejos del punto de acceso al que se encuentra conectado, por lo que el dispositivo envía paquetes de prueba para identificar que otros puntos de acceso se encuentran disponibles para conectarse. Entonces, en el caso del descubrimiento de un punto de acceso accesible, el dispositivo selecciona el siguiente punto de acceso en base a un criterio definido por el mismo. El segundo proceso, autenticación, se realiza cuando se envía una solicitud de autenticación hacia un nuevo punto de acceso por medio de un dispositivo cliente, el cual aguarda por la respuesta del primero. El tercer proceso, re-asociación, se realiza luego de la aprobación de un nuevo punto de acceso, entonces el dispositivo cliente envía una petición de re-asociación. Una vez que la re-asociación es completada, el punto de acceso envía un paquete de disociación para poder actualizar las tablas de enrutamiento.

El proceso de transferencia tarde típicamente menos de medio segundo, siendo la etapa de escaneo la que contribuye principalmente al retardo. Finalmente, cabe recalcar que el cliente es quien incita al cambio.

1.2.2. Espectro Compartido

La calidad de una red inalámbrica es influenciada por eventos de interferencia internos (*co-channel interference*) y externos (*ruido*). Co-channel interference o interferencia co-canal ocurre cuando dispositivos bajo el mismo dominio de control y dentro del rango de interferencia de cada uno, operan en el mismo canal. La interferencia co-canal puede ser mitigada mediante cuidadosa planificación en la asignación de canales, mediante el uso de técnicas de detección multiusuario (MUD) o mediante complejas técnicas de sincronización a nivel MAC. El Ruido es el producto de emisiones de dispositivos que no pertenecen al dominio de control, del ruido atmosférico, y el ruido térmico de los dispositivos electrónicos en los circuitos de recepción. Dado que por lo general no se conocen las formas de onda/timing de estas señales (MUD no es posible) las únicas posibilidades para mitigar el ruido son elevar la potencia de transmisión (elevar el SNR), sensar el nivel de potencia del espectro antes de transmitir (CSMA), o elegir otro canal.

Para el caso de redes WCAN Enterprise WiFi, compartir el espectro en la frecuencia de 2.4Ghz, por una diversidad de equipos que pertenecen y que no pertenecen al estándar 802.11, es otro de los principales obstáculos en su diseño y funcionamiento. De esta forma, un paquete que viaja en el espacio puede ser corrompido por dichas señales u opacado en el receptor. Por otro lado, el transmisor puede detectar la presencia de otros paquetes en dicho canal, ocasionando un retraso en la transmisión para evitar colisión de paquetes.

Una pequeña cantidad de energía no WiFi puede tener un mayor efecto en el desempeño del canal de radio que cualquier señal que pertenezca al estándar 802.11[34]. A mayor carga en un canal, la influencia del ruido externo crece logarítmicamente en el desempeño del mismo. Por tal motivo, la interferencia en ambientes debe ser minimizada para asegurar un nivel de calidad óptimo para los usuarios.

Por otra parte, es conocido que teóricamente múltiples transmisiones bajo el estándar 802.11 en proximidad física pueden coexistir sin interferir destructivamente entre dichas. Esto ocurre al utilizar canales vecinos separados con una distancia de 25MHz (frequency planning). Sin embargo, se ha demostrado en práctica que la interferencia

co-canal puede existir en canales no coincidentes. Este fenómeno ocurre cuando el origen de la interferencia se encuentra en cercanía con el receptor. La interferencia entre banda no coincidentes tiene un efecto menor a mayores distancia. Este tipo de interferencia posee un gran efecto en el diseño de redes WiFi de malla con múltiples bandas simultáneas. [34]

1.2.3. Seguridad

Actualmente, muchas organizaciones utilizan las redes inalámbricas para proveer un medio de acceso hacia el Internet o Intranet, lo cual permite un método de trabajo flexible. Los usuarios son capaces de trasladar sus computadoras de una locación a otra, y al realizar esta materia, la comunicación y acceso se mantiene de forma constante; convirtiéndose una capacidad que ha mostrado claramente que puede mejorar la productividad que cualquier entidad que la utiliza. De esta forma, existen diversos usuarios cuya computadora principal de trabajo solo dispone de interface de red inalámbrica, como algunos dispositivos de la marca Apple, o utilizan únicamente esta interfaz como medio de acceso. No obstante, la seguridad inalámbrica siempre ha sido uno de los principales retos, debido a que la información es transmitida por el aire, y cualquiera dentro de su rango de transmisión es capaz de capturar dicha información.

De esta forma, el gran número de dispositivos clientes dentro de un campus o empresa represente un desafío a la seguridad presente. Una red es tan débil como su eslabón más débil, por lo que un grande y disperso campus debe ser provisionado con mecanismo de seguridad que permitan eliminar las vulnerabilidades a ataques u acceso inadvertidos. Para lo cual, se cuentan con diversas herramientas como listas de control de acceso (ACLs), autenticación, encriptación y otros métodos seguros de restricción de acceso que permitan solo a usuarios y dispositivos autorizados y detengan cualquier intento de penetrar la red dentro del campus.

Existen una serie de protocolos y servicios que soportan la seguridad de extremo a extremo dentro del campus. Puesto que el verdadero desafío es el balance entre una red segura que permita el acceso a información sensitiva a los usuarios y visitantes de la red; mientras que se soporta una velocidad de acceso necesaria en un entorno de acceso Wi-Fi con total disponibilidad.

Tradicionalmente, organizaciones utilizan firewalls para poder proteger los recursos internos, sin embargo, en un mundo inalámbrico, los ataques no viajan por medio de los cables y, por esta razón, pueden ser burlados. La mayoría de las redes

empresariales o de campus son dependientes de firewalls en términos de filtrado de tráfico externo y control físico. Sin embargo, este enfoque tradicional no es capaz de restringir la señal inalámbrica que ingresa a la red vía un punto interno, sin pasar por el firewall.

1.3. Arquitectura de redes Enterprise Wi-Fi

Las redes empresariales o de campus son diseñadas para soportar los requerimientos necesarios para distribuir un nivel alto de calidad de usuarios. Esta red debe tener un diseño modular que le permita un control complejo de los recursos mientras se soporta un amplio rango de escalabilidad y opciones de desempeño. De esta forma, la arquitectura de estas redes debe ser capaces de soportar una diversidad de criterios.

Las redes empresariales se encuentran continuamente soportando comunicaciones unificadas e incluso entornos virtuales con requerimientos constantemente crecientes de desempeño y escalabilidad. Además, conforme el tráfico se incrementa, se debe mantener una confiabilidad y disponibilidad de recursos que permitan soportar y mantener un estándar de calidad de usuario.

Una arquitectura o topología clásica de las redes empresariales cuenta con partes distinguidas, el acceso, distribución y centro. La capa de acceso representa una de las jerarquías más complejas del diseño. En este sentido, diseñar una capa de acceso proactiva y escalable a las aplicaciones necesarias es de vital importancia. Asimismo, debido a que la alta disponibilidad, desempeño y requisitos de seguridad varían según áreas o departamento, esta capa debe ser capaz de soportar múltiples velocidades de acceso, capacidad de conmutación de errores, VPN y otros protocolos de seguridad requeridos [35]

1.3.1. 802.11 en modo Infraestructura

Cualquier computadora, móvil, portable o fijo, puede ser referido como una estación en 802.11, en ingles Mobile Station (MS), siempre y cuando cuente con una interfaz inalámbrica habilitada. La principal diferencia entre una estación móvil y portable es el hecho de que la estación móvil tiene la capacidad de trasladarse de una ubicación a otra, pero es utilizada en una ubicación establecida. Mientras que las estaciones móviles acceden a la red mientras se encuentran en movimiento.

El propio funcionamiento de las redes inalámbricas requiere de diversos elementos, los cuales varían según los requerimientos de la red. Existen dos tipos de redes las cuales son referidas como BSS, conjunto básico de servicio, e IBSS, conjunto independiente básico de servicio. Una red BSS consiste un grupo de puntos de acceso o router inalámbricos, así como una determinada cantidad de clientes. Mientras que una red IBSS o Ad-hoc consiste de un grupo de clientes conectados entre ellos como se puede apreciar en la siguiente figura:

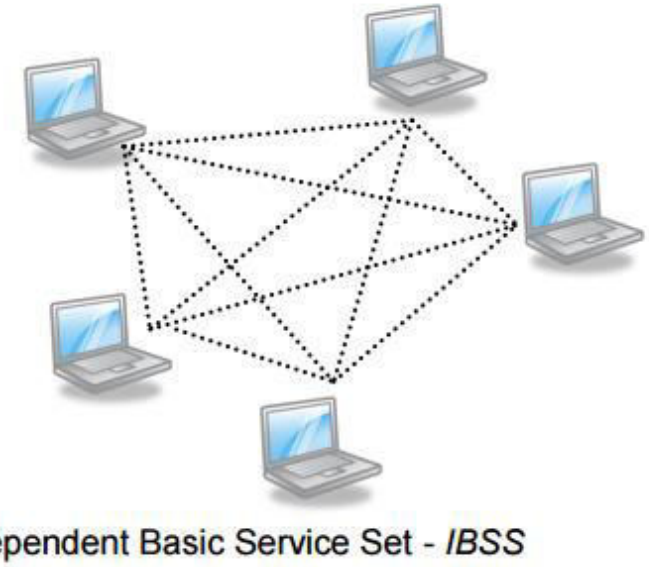


Figura 1-2: Modo Ad-Hoc o IBSS.
Fuente: [36]

Cuando los BSSs se encuentran interconectados por una red, entonces se convierten en lo que se conoce como un modo infraestructura del WiFi. De esta forma, dos o más BSSs se interconectan utilizando un sistema de distribución (DS), el cual incrementa el concepto de cobertura de la red. La infraestructura de la capa de acceso de las redes empresariales inalámbricas consiste principalmente de los dispositivos llamados Access Points (APs), o puntos de acceso, los cuales son dispositivos que transformación la señal de las tramas alámbricas Ethernet en señales inalámbricas de radio frecuencia que viajan por el aire. Estos tienen la función de brindar el medio por el cual las MS acceden a la red fija.

Todas las redes cuenta con una SSID, la cual es una etiqueta que permite diferencias las redes. La SSID permite asegurar que el tráfico entre radios, ya sea un AP o un dispositivo cliente, pueda ser direccionado correctamente. Por default, esta etiqueta es distribuida automáticamente por los APs mediante el uso de la trama beacon y esta puede ser capturada por cualquier cliente o herramienta de monitorio.

La creación de una red grande y compleja mediante la utilización de BSSs y DSs sirve como referencia al siguiente nivel de jerarquía, los conjunto de servicio extendido o ESS, por sus siglas en ingles. La principal cualidad de los ESS es que permite que la red se vea como una único BSS independiente para la capa de control lógico (LLC). De esta forma, una estación dentro de una ESS puede comunicarse e incluso trasladar entre los BSSs de forma transparente para la capa de control.

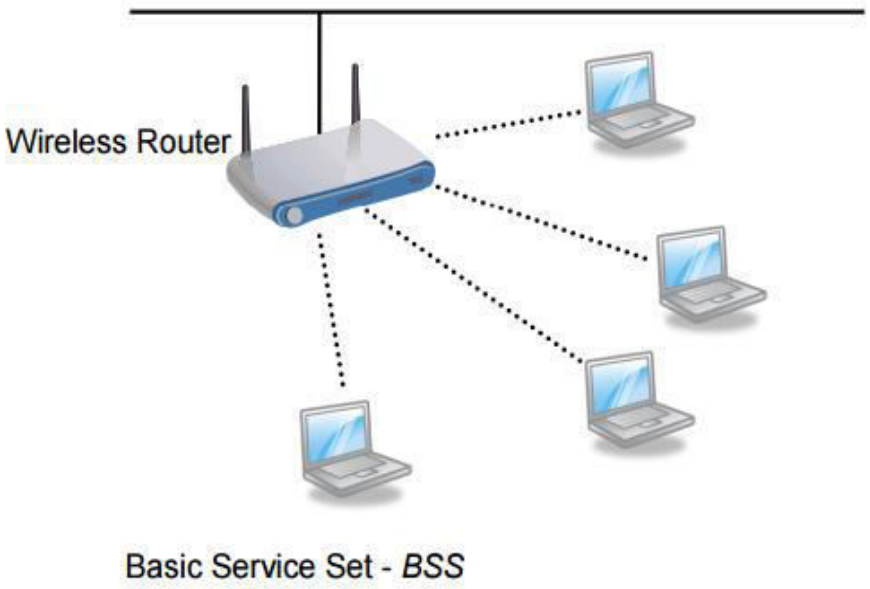


Figura 1-3: Modo Infraestructura.
Fuente: [36]

1.3.2. Gestión de tramas en 802.11

Antes de que un cliente inalámbrico puede intercambiar información con un AP, este debe pasar por un procedimiento conocido como “apretón de mano”, del inglés handshaking, en el cual se intercambian tramas en la capa MAC. La siguiente tabla enlista las principales tramas de gestión en 802.11:

Valor de subtipo	Descripción de subtipo
0000	Petición de asociación
0001	Respuesta de asociación
0010	Petición de re-asociación
0011	Respuesta de re-asociación
0100	Petición de prueba
0101	Respuesta de prueba
1000	Beacon
1001	Mensaje indicador de anuncio de tráfico(ATIM)
1010	Disociación
1011	Autenticación
1100	Des-autenticación
Otros valores	Reservada

Tabla 1-1: Trama de gestión en 802.11

Fuente: [17]

Cada valor de subtipo identifica una función específica de la trama. Las tramas de autenticación son utilizadas para autenticar la identidad de una estación de comunicación. Las tramas de petición y respuesta de asociación, así como, las tramas de petición y respuesta de re-asociación son utilizadas para establecer una comunicación lógica con un AP. Las tramas de des-autenticación son utilizadas para destruir la identidad que ha sido previamente autentificada. Las tramas disociación son utilizadas para destruir una conexión previamente utilizada entre una estación y un AP. Las tramas beacon son enviadas por un AP para anunciar su existencia a las estaciones cercanas. Las tramas de petición y respuesta de prueba son utilizadas por una estación para escanear activamente la existencia de un AP en el área cercana. Las tramas ATIM son utilizadas por otro tipo de conjunto de BSS denominado modo ac-hoc. [17]

1.3.3. Two-tier enterprise Wi-Fi architecture

Existen diversas formas en las cuales los APs, parte clave de la red de acceso, son configurados. La configuración autónoma de APs es una configuración en donde los APs son completamente autosuficiente y son distribuidos como dispositivos independientes que conectan múltiples clientes a una red alámbrica. Tal que, cada configuración de un AP es configurada independientemente. Este enfoque es el más básico dentro de los modelos de distribución, siendo utilizado principalmente debido a que los dispositivos son de bajo costo y fácilmente obtenibles en el mercado por una variedad de vendedores. Sin embargo, esta configuración no puede responder efectivamente a la movilidad de usuarios (HandOff) ni a cambios en el estado del espectro electromagnético, funciones que por su naturaleza se benefician de una coordinación global.

Estos problemas son resueltos con la arquitectura de dos niveles (Two Tiers) donde los APs se encuentran gestionados por medio de un controlador central, ubicado localmente en el campus o en la nube, como se aprecia en la figura 1-4. Este controlador cuenta con diversas funciones que permite ejecutar políticas de configuración (asignación de canales, asignación de potencia de transmisión), seguridad, calidad, entre otras; gestión de software y permitir autenticación de clientes. Este enfoque es el más utilizado y sugerido por las redes empresariales debido a su mayor escalabilidad, gestión y disponibilidad de funciones, no obstante, la principal desventaja de este enfoque es que – al ser el protocolo entre los APs y el controlador propietario – una vez adquirido un controlador de un vendedor, el usuario se encuentra cautivo a el mismo para subsecuentes compras de APs.

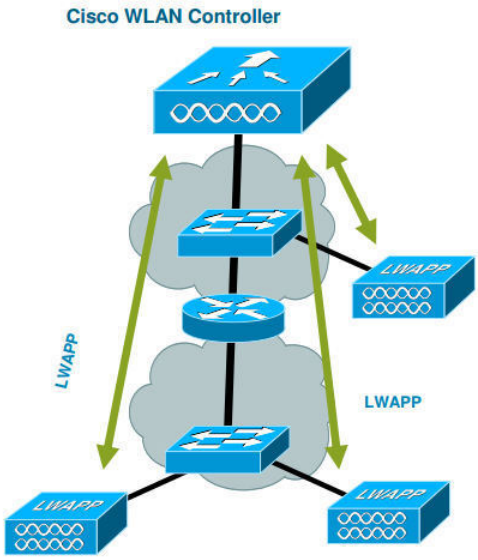


Figura 1-4: Esquema de la arquitectura de dos niveles.

Fuente: [37]

1.3.4. Autenticación

La seguridad inalámbrica ha evolucionado para utilizar métodos adicionales y más robustos. Los APs pueden utilizar una variedad de métodos de autenticaciones que hacen uso de una variedad de servidores y base de datos de autenticación y autorización. El protocolo de autenticación extensible, EAP en inglés, es un método que forma parte de muchos sistemas de seguridad inalámbricas, asimismo, las diversas variantes de este protocolo como PEAP y LEAP.

Este protocolo es utilizado una variedad de ambientes seguridad debido a su versatilidad. Además, EAP cuenta con precedentes con protocolo punto a punto, PPP, en comunicaciones y no solo autenticaciones inalámbricas.

1.4. Amenazas de seguridad en redes Enterprise WiFi

En esta sección se realiza una descripción de los ataques más frecuentes en las redes Enterprise WiFi. Mientras que en la sección siguiente se describen las técnicas para mitigarlos.

1.4.1. Intercepción y monitoreo no autorizado del trafico

Esta amenaza consiste en la utilización de una serie de software y herramientas que me permitan capturar y monitorear los paquetes de una red inalámbrica por parte de

una tercera parte no autorizada. Los principales métodos usados son el uso de un software rastreador, capaz de ver y capturar la data, y de un punto de acceso con identificación falsa (HoneyComb attack) que recolecta las claves de acceso y encriptación de los usuarios. Este último es posible debido a que generalmente los equipos inalámbricos están configurados para conectarse automáticamente a APs con BSSIDs conocidos.

1.4.2. Encriptación

Los ataques de encriptación se basa en la intercepción de los paquetes y luego mediante el uso de una serie de herramientas y algoritmos busca obtener la clave con la cual se ha encriptado la comunicación. Este tipo de ataque explota una de las vulnerabilidades más antiguas que se tiene al utilizar WLAN, el tener un medio compartido y no contar un algoritmo de encriptación robusto.

1.4.3. Bloqueo

En este tipo de ataques podemos encontrar una diversidad de subtipos enfocadas a explotar una determinada vulnerabilidad del sistema, pero que tiene como fin el negar o evitar que los usuarios tengan acceso a los recursos de la red inalámbrica. Entre los principales ataques de bloqueo tenemos el de radio interferencia, desautenticación y disociación, falso SSID. El ataque de radio interferencia o también conocido como jamming fue originalmente desarrollado para propósitos militares. Este ataque consiste en el envío de una señal de radio potencia que deje la señal del Access Point inutilizada. El segundo ataque consiste en aprovechar la vulnerabilidad de los protocolos del estándar 802.11 ante el envío de paquetes no autorizados de gestión, tal que se fuerza al cliente o AP a desconectarse de la red. El último consiste en el envío de beacon con SSID falsos que agoten los recursos de procesamiento en los APs.

1.4.4. Inserción

Este tipo de ataque involucra cualquier intento de utilizar los recursos de la red inalámbrica cuando no se cuentan con los permisos necesarios. Un caso especial de este ataque es la inserción de un punto de acceso (AP) no autorizado a algún puerto de un switch de la red fija. Un AP atacante que se encuentra conectado de esta forma se le denomina Rogue AP.

1.4.5. Cliente-Cliente

Este tipo de ataque tiende a ser efectivos e ignorados por los WIDS, sistemas de detección inalámbricos, debido a que solo se enfoca en la protección de los sistemas internos, pero no se toma en cuenta la enorme cantidad de información de carácter sensible que puede poseer un usuario. [11]

1.5. Técnicas de seguridad de Enterprise WiFi

Las redes inalámbricas son vulnerables a los diferentes tipos de ataques descritos en la sección anterior debido a que el aire es un medio de acceso compartido para cualquier persona que se encuentre dentro de la cobertura del punto de acceso a la red, Access Point (AP). No obstante, existen diversas técnicas con el objetivo de evitar la intercepción ilegal de la información, las que serán discutidas en esta sección.

1.5.1. Protocolos de Encriptación

Los protocolos de encriptación ha pasado por un proceso evolutivo que inicia en el protocolo WEP, hasta el protocolo actual WPA2 que pertenecen al estándar IEEE 802.11i

1.5.1.1. WEP (Wired Equivalent Privacy)

WEP es el protocolo de encriptación original del estándar IEEE 80211 que emplea un algoritmo cíclico de redundancia (CRC) para verificar la integridad y una clave secrete de 40 o 104 bits y un vector de inicialización de 24 bits. Sin embargo, el envío de la clave es en texto plano, lo cual lo hace vulnerable a ataques de decodificadores de código WEP y sniffers.

1.5.1.2. WPA (Wi-Fi Protected Access)

WAP es un algoritmo de encriptación que requiere una clave secreta de 104 a 128 bits, un vector de inicialización de 24 a 48 bits y la implementación del protocolo de llaves dinámicas TKIP, lo cual evita que se vea afectado por ataques WEP. Además, WPA implementa un código de integridad de mensaje (MIC) mediante una llave hash o un cálculo complejo que solo pueda ser generado en una dirección, el cual es necesario para evitar que la información sea alterada sin conocer la clave.

1.5.1.3. WPA2 (Wi-Fi Protected Access 2)

WPA2 es un algoritmo compatible con WPA y WEP, pero que utiliza un algoritmo de cifrado diferente conocido como CCMP (Counter Mode With Cipher Block Chaining Message Authentication Code Protocol) basado en AES. Así mismo, se diferencia porque existen dos tipos de protocolos WPA2 conocidos como Personal y Enterprise.

WPA2-Personal es una versión de este protocolo de encriptación que fue diseñado para uso doméstico o en pequeñas empresas, tal que encripta los datos con AES y cuenta con una clave única o una lista de claves estáticas para establecer el acceso a la red. Este algoritmo es evitado en las redes de compañías debido a que vulnerabilidades y herramientas de descifrado han sido publicadas. Siendo una de sus principales vulnerabilidades el hecho de que el intercambio inicial individual es sin encriptación, por lo tanto, es posible descifrar y descubrir la clave dinámica de la sesión.

Por otra parte, WPA2-Enterprise cifra los datos con AES y verifica la identidad de los usuarios de la red utilizando el protocolo de autenticación EAP o un servidor. Usualmente, se utiliza un servidor RADIUS, un directorio activo o una base de datos LDAP para almacenar a los usuarios y sus credenciales. Esto elimina la debilidad de la clave en WPA. Para lo cual, se requiere de tres elementos en este proceso, un cliente, el dispositivo usuario; un autenticador, el Access Point; y un servidor de autenticación, como el servidor RADIUS. [36]

Actualmente, la PUCP utiliza WPA2-Personal con una clave única para el acceso de todos los usuarios. No obstante, se encuentra en proceso de migración a WPA2-Empresarial. Debido a este motivo, robar la clave de un usuario privilegiado puede llegar a ser muy atractivo para un atacante.

1.5.2. Protocolos de integridad y confidencialidad de datos

La principal diferencia entre los protocolos de integridad y de encriptación es que el protocolo de encriptación tiene como finalidad que la información no pueda llegar a ser leída por ninguna tercera parte; mientras que el protocolo de integridad evita que la información sea corrompida durante el trayecto por el cual viaja hasta su receptor final. Por otra parte, los protocolos de confidencialidad tienen como finalidad impedir la divulgación de información a personas o sistemas. En otras palabras, aseguran que el acceso a la información sea únicamente a dichas personas que cuenta con la debida autorización. Es en este contexto que los protocolos de integridad y

confidencialidad de datos han pasado por un proceso evolutivo que inicio en el protocolo TKIP, el cual se incorporó en la encriptación WAP, hasta el protocolo CCMP, el cual ha sido incorporado en el protocolo de encriptación WAP2.

1.5.2.1. TKIP (Temporal Key Integrity Protocol)

TKIP es un protocolo de integridad de clave temporal que surgió para reforzar la seguridad de los sistemas WEP. Este protocolo ofrece la ventaja de migrar del protocolo WEP a sistemas del estándar 802.11i. Este protocolo se basa en el algoritmo de encriptación RC4, lo que implica ciertas limitaciones en seguridad, debido a que este algoritmo es vulnerable a una diversidad de ataques y se ha comprobado que es posible recuperar la clave compartida en cuestión de horas.

1.5.2.2. WRAP (Wireless Robust Authenticated Protocol)

WRAP está basado en el algoritmo de encriptación AES-Offset Code Book (OCB), y fue el primer protocolo elegido para el estándar IEEE 802.11i; sin embargo, fue abandonado por motivos de propiedad intelectual.

1.5.2.3. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

Este protocolo cuenta con un nuevo diseño basado en el algoritmo de encriptación de bloques AES, a diferencia de TKIP que se originó para ser acomodado a la estructura establecida por WEP. Este protocolo cuenta con una clave única, pero con diferentes vectores de inicialización.

Además las técnicas antes mencionadas, existen los sistemas conocidos como WIDS, los cuales se discutirán posteriormente, y que son sistema que brinda un nivel de protección y reacción ante una diversidad de ataques inalámbricos dentro de las redes empresariales. En las siguientes secciones se realizara un enfoque sobre los peligros que representa la presencia de los Rogue APs dentro de la red inalámbrica y la utilización de los WIPS para poder mitigarlos.

1.6. Rogue AP

Una de las principales amenazas que corresponden un problema de seguridad para las WLAN es la denominada Rogue AP. Esta amenaza es definida como un punto de acceso ilegal que no es implementado por el administrador de la red. Por otro lado,

un Rogue AP también puede definir como un AP que suplanta la identidad (BSSID) de una AP valido dentro de la red inalámbrica y que tiene intenciones maliciosas para comprometer el sistema de información de una organización. En este aspecto, los Rogue APs pueden ser implementados de dos formas con diferentes equipos. La primera forma es mediante una conexión directa de un punto de acceso inalámbrico con la red cableada. Mientras que, la segunda forma mediante el uso de una laptop con dos tarjetas de red inalámbricas, tal que una de las tarjetas está conectada a un AP verdadero y la otra está configurada como un AP para proveer acceso a Internet a otros puntos inalámbricos.

Por otra parte, un Rogue AP puede trabajar de forma pasiva, es decir, espera a que un usuario se conecte a él por sí mismo; o de forma activa, mediante el envío constante de tramas falsas de disociación para forzar que los usuarios cambien su conexión hasta que se logren conectar con el Access Point.

La amenaza del Rogue AP yace en el hecho de que puede manipular y monitorear todo el tráfico entrante y saliente del usuario, e incluso puede realizar otros tipos de ataques. Por ejemplo, el administrador del Rogue AP puede analizar los paquetes enviados y redireccionar la página pedida por el cliente por una página falsa en donde se puede robar toda la información sensible de este como su número de cuenta o contraseña. Además, otra amenaza de este tipo de ataques es que no puede ser detectado por los medios de seguridad comunes como son los firewalls o antivirus, por tal motivo se desarrollaron sistemas especiales que permiten la detección de este tipo de amenazas conocidos como WIDS. [5,24]

1.6.1. Clasificación de los Rogue AP

Según el ambiente empresarial, existen cuatro clasificaciones de Rogue APs que caen baja esta definición:

A) Rogue AP de usuario: un usuario dentro de una entidad es el responsable de la compra e instalación de un Access Point sin autorización dentro de la red LAN dicha entidad para sus propios intereses. Esto permite que usuarios no autorizados o atacantes externos accedan a la red de la entidad. Este tipo es muy común en organizaciones que no cuentan con políticas de seguridad inalámbrica y de empleados sin entrenamiento en dicho campo.

B) Rogue AP de atacante externo: el punto de acceso es colocado afuera de la organización y no se encuentra conectado dentro de la compañía. De esta

forma, el atacante toma ventaja de la alta potencia de la señal con un SSID falso con la finalidad de que todo el tráfico de los usuarios sea redirigido por medio del Rogue AP, lo que le permite analizarlo.

C) Rogue AP de atacante interno: el punto de acceso es colocado dentro de la organización y se encuentra conectado directamente a la red cableada. Este tipo es menos probable, debido a que implica que el atacante supere todas las seguridades y consiga acceso a la red LAN, no obstante, si se presenta constituye una seria brecha de seguridad. En esta forma, el atacante suele desactivar la diseminación del SSID con la finalidad de ocultarlo y poder posteriormente acceder la red fija vía el Rogue AP.

D) Rogue AP vecino: el punto de acceso es colocado en proximidad cercana de la organización por una tercera organización. En esta forma, el administrador de la red no cuenta con permiso para controlar o apagar punto de acceso de otra organización. No obstante, se considera una buena práctica entrenar a los empleados a estar pendientes de este tipo debido a que la conexión inadvertida puede comprometer la seguridad.[10]

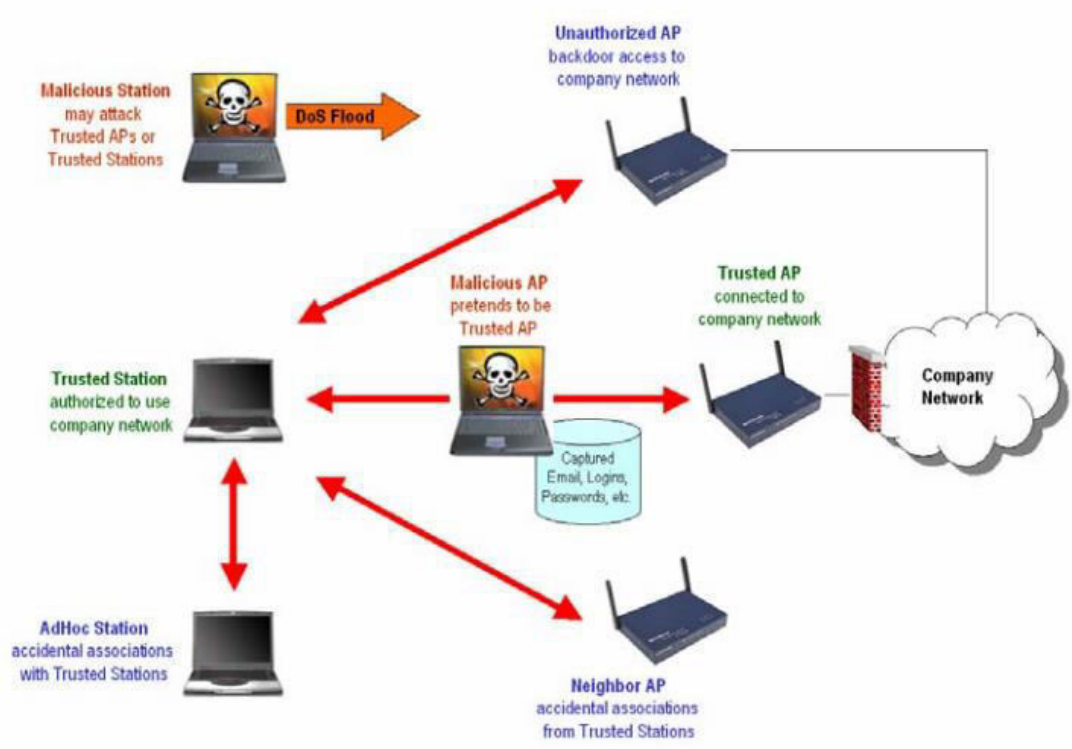


FIGURA 1-5: Clasificación de los Rogue APs.

Fuente: [38]

1.7. Detección y Prevención de Intrusos en redes Enterprise WiFi

La seguridad en los sistemas de tecnología de la información (IT) es una creciente e importante área de investigación debido al hecho de que los usuarios han aceptado que todos los sistemas que se encuentra conectados a Internet son vulnerables. Estas vulnerabilidades se originan de amenazas conocidas como ataques de día cero, malware, ataques de denegación de servicio, entre otros. Algunos de los sistemas que buscan proveer un medio de protección ante estos incluyen a los firewalls y antivirus. Cada uno de estas defensas solo puede cubrir una fracción de la seguridad de las computadoras. Por un lado, los firewalls son barreras y no informan de la actividad dentro de la red; mientras que los antivirus solo protegen a los usuarios de software malicioso. Existen diversos protocolos y amenazas a la red que ninguna de estas opciones pueden proteger. En la siguiente sección, se introducirán los sistemas conocidos WIDS y WIPS, los cuales son los principales medios de defensa en contra de las amenazas de las redes inalámbricas.

1.7.1. Detección versus Prevención

Un WIDS, Wireless Intrusion Detection System, o sistemas de detección inalámbrica de intrusos es uno de los primeros términos conocidos que se utilizó para describir un sistema partículas de hardware o software cuya funcionalidad y eficiencia era variada según el proveedor, pero que su función principal era detectar la presencia de un intruso o usuario no autorizado y de ser capaz de tomar las medidas o acciones apropiadas para contrarrestar la amenaza al bloquear su acceso o actividades. Por tal, tratar con intrusiones al sistema implica una serie de actividades relacionadas a su tratamiento como detección, identificación, prevención, reacción, entre otras.

El modelo tradicional de este sistema solo era capaz de detectar los intrusos y responder a la destrucción ocasionada al sistema por los mismos. Sin embargo, los sistemas actuales son principalmente utilizados en áreas locales inalámbricas y son capaces de determinar el tipo de invasión, detectar comportamiento ilegal o inusual en la red, monitorear y analizar las actividades de los usuarios y activar alarmas cuando detectan un flujo anormal de datos en la red.

Los WIDS se caracterizan principalmente por los siguientes componentes:

A) Arquitectura: los sistemas inalámbricos de detección son principalmente de dos formas, sistemas centralizados y descentralizados. En el primer caso, los sistemas de detección se basan en el uso de sensores externos al sistema,

los cuales se encargan de la recolección de la data y de su transmisión a la central del sistema que se encarga de procesar toda la data almacenada. En el segundo caso, los sistemas incluyen una variedad de dispositivos auxiliares los cuales se encargan del procesamiento y la creación de reportes de forma individual. En otras palabras, la principal diferencia entre estos sistemas es que en el sistema centralizado el procesamiento se realiza en un único nodo central, mientras que en el enfoque descentralizado se realiza en diversas entidades. El sistema descentralizado es más compatible para redes de pequeña escala, debido a que su gestión es sencilla y requiere un menor costo. Sin embargo, si se cuentan con una gran cantidad de sensores, esto ocasionara que la capacidad de gestión del tiempo de procesamiento y reporte de los sensores sea ineficaz comparado con el modelo centralizado.

B) Respuesta física: la localización física de los sensores es una parte vital para los sistemas de detección de intrusos, sobre todo debido a los ataques a los sistemas inalámbricos tienen la tendencia a realizarse en una locación geográficamente cercana de la red. Por lo tanto, la respuesta debe darse en el menor intervalo de tiempo posible, lo cual se lleva a cabo mediante la localización de la dirección física del intruso y la detección de las víctimas.

C) Detección de amenazas: los sistemas de detección inalámbricos no solo son capaces de detectar el comportamiento del atacante, así mismo, debe ser capaz de detectar Access Points inalámbricos solitarios e identificar flujos de datos no encriptados. Puesto que existen diversas herramientas utilizadas por los hackers que permiten la identificación de blancos potenciales; de igual formar, existen ataques que explotan estas vulnerabilidades, siendo el ataque más serio el ataque de denegación de servicio.

D) Política de ejecución: los sistemas de detección inalámbricos no solo cuentan con la capacidad de identificar un invasor o ataque, sino que de igual forma son vastamente utilizados para reforzar las políticas de seguridad de la red.[8]

De lo anterior, un WIDS es capaz de detectar actividad no autorizada crítica en la red. Sin embargo, la detección es solo una parte de la solución, puesto que la verdadera meta es poseer un sistema que sea capaz de prevenir automáticamente la ocurrencia de una actividad no autorizada. Este tipo de sistema es una creciente

tendencia en el mercado conocido como Wireless Intrusion Prevention System (WIPS) o Sistema de Prevención Inalámbrica de Intrusos.

Un WIPS es un sistema de seguridad de red que monitorea la red y el espectro electromagnético en búsqueda de actividades maliciosas o comportamiento no deseado, y cuenta con la capacidad de bloquear o prevenir dichas actividades en tiempo real. Los WIPS es una vertiente tecnológica en el área de la seguridad de red que combina las capacidades de un firewall con la capacidad de inspección profunda de un WIDS. Por lo cual, todos WIPS cuenta con las siguientes tareas básicas: la detección automática y clasificación de amenazas a la red, el reconocimiento preciso del plan de ataque de los perpetradores y la activa respuesta y prevención de un ataque que ha ocurrido, está ocurriendo o va a ocurrir. [4]

1.7.2. Técnicas de Detección

En [2] el autor diseña un auditor de seguridad inalámbrica distribuido (DWSA), basado en los sistemas Linux y Windows. Este auditor provee continuamente estimaciones de la red inalámbrica al modificar el poder disponible y el estatus de clientes inalámbricos confiables a sensores anómalos a la infraestructura de la empresa. Utilizando reportes periódicos de seguridad, servidores son capaces de detectar los Rogue APs y APs mal configurados, y subsecuentemente ubicándolos por medio de triangulación de señal y algoritmos de localización usados en sistemas como GPS. [25]

En esta forma, la mayoría de los sistemas basados en enfoques para detectar Rogue APs son rudimentarios y fácilmente evadidos por hackers. En este sentido, existen organizaciones que han equipado al personal de IT con herramientas inalámbricas para análisis de paquetes en laptops u otros dispositivos portátiles. Este enfoque fuerza al personal a realizar recorridos en el área de las instituciones o campus en búsqueda de Rogue APs. No obstante, este método es altamente inefectivo, debido a que los escaneos manual consumen grandes periodos de tiempo y son costosos, por lo cual no son realizados frecuentemente. Además, debido a que los dispositivos que funcionan en el estándar 802.11 pueden operar a distintas frecuencias, 802.11b/g/n - 2.4GHz y 802.11 ac - 5GHZ, el personal de IT debe actualizar sus equipos de detección para permitir múltiples frecuencia. Así mismo, el escaneo puede ser fácilmente eludido, debido a que los Rogue AP pueden ser fácilmente desactivados cuando se realiza el escaneo. [22,24]

Otro enfoque es iniciar un escaneo al utilizar dispositivos dedicados o APs para detectar los beacons de los (Rogue) APs cercanos, y transmitir esta información a una plataforma central que contiene políticas de la red inalámbrica para el análisis. De esta forma, se puede contar con una red de detección funcional y automatizada que permita la detección en cualquier lugar y momento de los Rogue APs. No obstante, este método es costoso, considerando que se deben posicionar sensores o AP por toda la red de la institución para monitorear el espectro. Así mismo, este enfoque es totalmente impráctica si no se cuenta con APs inalámbricos. No obstante, este es el caso a seguir si se desea conseguir un sistema de detección confiable que no impacte directamente en la experiencia de los usuarios. Por tal motivo, este método debe ser optimizado para lograr minimizar el costo de implementación. [22]

1.7.3. Técnicas de bloqueo de intrusos

Los WIPS cuentan con diversas técnicas para bloquear el acceso de usuarios no autorizados, entre dichas se encuentra el RF jamming, bloqueo de puertos del Switch y Over-The-Air (OTA) Prevention. La primera técnica es muy efectiva para evitar el acceso a un intruso, sin embargo, bloquea todo el espectro de radio frecuencia lo cual así mismo significa que bloquea el tráfico de los usuarios validos que viaja por el medio. La segunda técnica que se basa en apagar el puerto del Switch que se encuentra asociado a un equipo no autorizado, no obstante, esta técnica cuenta con la limitan de no poder bloquear el tráfico que no se encuentre asociado a un puerto, como es en el caso del ataque HoneyComb. Finalmente, la tercera técnica se basa en técnicas de dirección física (MAC), técnica por la cual se bloquea o niega lógicamente cualquier actividad proveniente de un determinado puerto físico en la red cableada, las cuales fueron originalmente creadas en contra de un ataque de negación de servicio.

En general, existen cuatro técnicas de OTA Prevention, las cuales explotan las vulnerabilidades durante el proceso de autenticación, limitantes de hardware o software de los equipos de la red y la naturaleza de un medio compartido para las comunicaciones inalámbricas. Estas técnicas son descritas a continuación.

1.7.3.1. Técnica de desautencación

Esta técnica implica la transmisión de una trama de desautenticación para poder romper la asociación o conexión entre un (Rogue) Access Point y su estación cliente. En esta forma, esta técnica puede realizarse mediante una trama unicast, para un solo cliente, o una trama broadcast, para todos los clientes. Esta técnica funciona

debido a que las tramas de autenticación no cuentan con la protección pertinente, lo cual permite el envío de tramas de la dirección física del AP a la dirección de broadcast. Este bloqueo tendrá un determinado tiempo de duración, el cual depende de la implementación del dispositivo. No obstante, este tiempo se encuentra entre el rango de milisegundo a unos pocos segundos. Por tal motivo, se requiere que los paquetes sean enviados de forma constante para mantener el bloqueo.

1.7.3.2. Técnica de asociación de flujo

Esta técnica se basa en la transmisión de una vasta cantidad de paquetes de petición de autenticación y asociación de dirección físicas aleatorias al AP no autorizado para evitar que cualquier nueva estación pueda asociarse a ella por un tiempo determinado. Esta técnica explota el hecho de que los APs inalámbrico cuenta con una cantidad limitada de memoria. De esta forma, esta técnica previene cualquier conexión futura, no obstante, cualquier conexión previa se mantiene; por tal motivo, la técnica anterior suele utilizarse previamente a esta técnica. Sin embargo, este técnicas solo tienden a utilizarse cuando los APs no utilizan técnicas de encriptamiento para la autenticación de la dirección física.

1.7.3.3. Técnica de detección de portadora virtual

Esta técnica permite un efectivo bloqueo de los dispositivos no autorizados a los canales mediante la transmisión de tramas MAC del tipo de control (RTS/CTS) con grandes valores de tiempo de vida. Según el standard IEEE 802.11, el máximo valor de duración es de 32767 microsegundos, por lo tanto, se requiere una transmisión periódica 32 milisegundos aproximadamente. En este sentido, esta técnica es más eficiente que el jamming desde el punto de vista de energía, debido a que en esta técnica se realiza una transmisión periódica, mientras que en el jamming se tiene una transmisión continua.

1.7.3.4. Técnica de confusión de beacon

La técnica de confusión de beacon está basada en el hecho de que los clientes asociados a un AP y este a su vez deben transmitir de forma automática y periódica sus tramas beacon. En esta forma, se explota esta característica al tratar de confundir un cliente inalámbrico mediante el envío de beacons falsos con campos incorrectos. Esto ocasiona que los dispositivos clientes se desconecten de sus puntos de acceso asociados y se conecten a dispositivos falsos, por lo tanto, se bloquea cualquier comunicación inalámbrica no autorizada. Por otro lado, de igual forma que con las

técnicas previamente desarrolladas, se requiere una constante transmisión de tramas para asegurar un bloqueo constante; de forma que, en este caso, se requiere que los beacons falsos tengan una tasa de transmisión mayor a la tasa de transmisión de los reales.[9]

1.7.4. WIPS en redes Cisco de última generación

Es esta sección se describe las técnicas WIPS de Cisco de última generación, por dos motivos: (i) para ilustrar de forma concreta un caso de un sistema WIPS, y (ii) porque la red inalámbrica "redpucp", objeto de este estudio, tiene equipo Cisco compatible con este sistema, por tal punto este es el más probable candidato para un sistema WIPS para la PUCP.

1.7.4.1. Componentes de WIPS

Los WIPS se encuentra conformados principalmente por cinco componentes (ver Figura 1-6), tal que uno o más componentes pueden integrarse en un mismo dispositivo e incluso utilizar la infraestructura inalámbrica existente:

- Dispositivos que capturen la información de los paquetes de datos de la WLAN (sensores)
- Servidor para la detección de intrusos, cuya labor es el procesamiento de la información recolectada de la WLAN para identificar las actividades de algún intruso. Además, cuando un intruso es detectado, este servidor se debe encargar de enviar una alerta y detalles de la amenaza al sistema de prevención.
- Sistema de prevención, el cual se encarga de realizar las acciones pertinentes de forma automática o con interacción humana para lidiar con la amenaza detectada. Este sistema se caracterizada en base a sus políticas de prevención o bloquea de intrusos.
- Base de datos de eventos, de forma que toda la información de los intrusos detectados por los dispositivos de captura de información sea almacenada para auditorias y análisis posterior.
- Consola de gestión, que provea a los usuarios con una interfaz amigable que permite al administrador acceder a información de la base de datos y configurar las WIPS de acuerdo a la WLAN. [16]

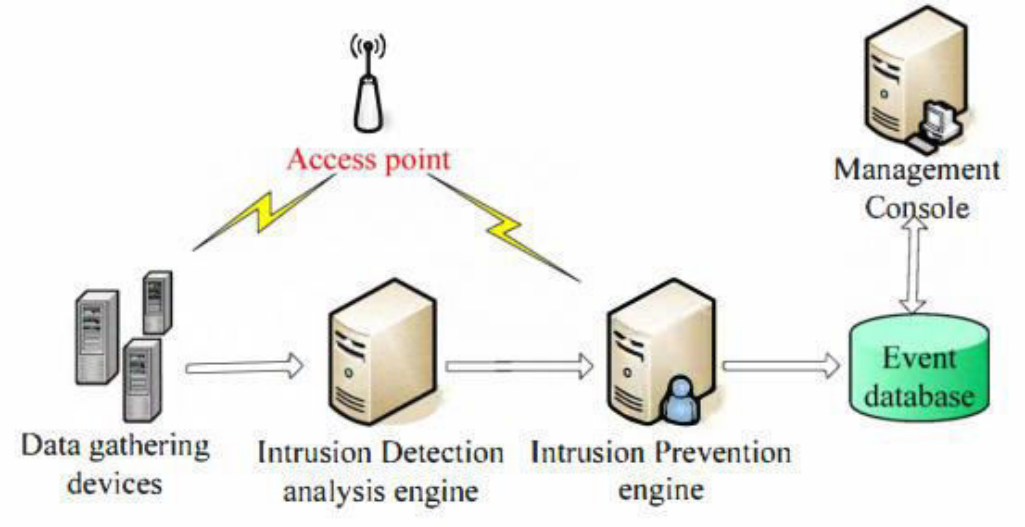


FIGURA 1-6: Componentes de WIPS.

Fuente: [16]

1.7.4.2. Modalidades de detección

Existen 3 tipos de enfoque para la detección: sensores dedicados, escaneo por los mismos APs, y un enfoque hibrido donde se utiliza una combinación de módulos dedicados de escaneo y hardware RF de los APs. [21, 23, 25]

El uso de sensores dedicados provee el mayor nivel de protección debido a que los transmisores utilizan todos sus recursos para la detección y contramedida de amenazas, pero a un costo alto

El uso de los APs para el escaneo durante intervalos libres de tráfico es costo-efectivo debido a que re-utiliza los receptores de los APs. No obstante, presentan la desventaja de que los APs no pueden detectar ni responder ante amenazas mientras este atendiendo al tráfico de los usuarios inalámbricos. Asimismo, cuando el AP se encuentra escaneando el espectro, escaneo de canales, no podrá atender tráfico de los usuarios. Esta latencia, la cual puede llegar a ser un segundo o más, es inaceptable para sesiones real-time como VoIP.

El enfoque hibrido, donde el escaneo se implementa en módulos que reúsan las antenas y la circuitería RF del AP sin interferir con las comunicaciones (solo escucha y cuenta con tuner/sintonizador de canal propio), presenta el mejor compromiso costo-beneficio.

1.7.4.3. Cisco Aironet 3600 & 3700

La red “redpucp” cuenta con varias centenas de APs modelos Aironet 3600 y 3700 de la compañía Cisco, desplegados a lo largo del campus. Como se muestra en la figura 1-7, estos APs pueden trabajar en cualquiera de los modos de escaneo para WIPS descritos en la sección anterior: ya sea como sensor dedicado (modo monitor), escaneo durante intervalos de inactividad, denominado modo “enhanced local mode”, o en combinación con un módulo adicional (WSSI) para un escaneo hibrido.

Dado que la opción hibrida, mediante la utilización de los módulos WSSI cuyo costo es una fracción del costo de los APs, presenta la mejor relación costo beneficio, este trabajo asumirá que la red de sensores a ser implementada consistirá de módulos WSSI anexados a algunos de los APs existentes en la universidad.

FIGURA 1-7: Cisco Aironet 3600.
Fuente: [39]

1.7.4.4. Módulo WSSI

La compañía Cisco cuenta con módulos WSSI, Wireless Security and Spectrum Intelligence en inglés, los cuales toman ventaja del diseño modular de la serie Aironet 3600 para el escaneo espectral. El WSSI es un módulo dedicado al monitorear el espectro electromagnético y a los servicios de seguridad desde los clientes a los servidores de data. Esto no solo permite un mejor desempeño para los clientes, sino que también reduce los costos al eliminar la necesidad de un punto de acceso dedicado al monitoreo y de la infraestructura alámbrica requerida para conectar estos dispositivos a la red. Este módulo en conjunto con un AP de la serie Aironet 3600

permite que el usuario provee con una seguridad de última tecnología y funciones de análisis espectral para todos los clientes Wi-Fi en todos los canales, tanto para las bandas 2.4 y 5GHz.

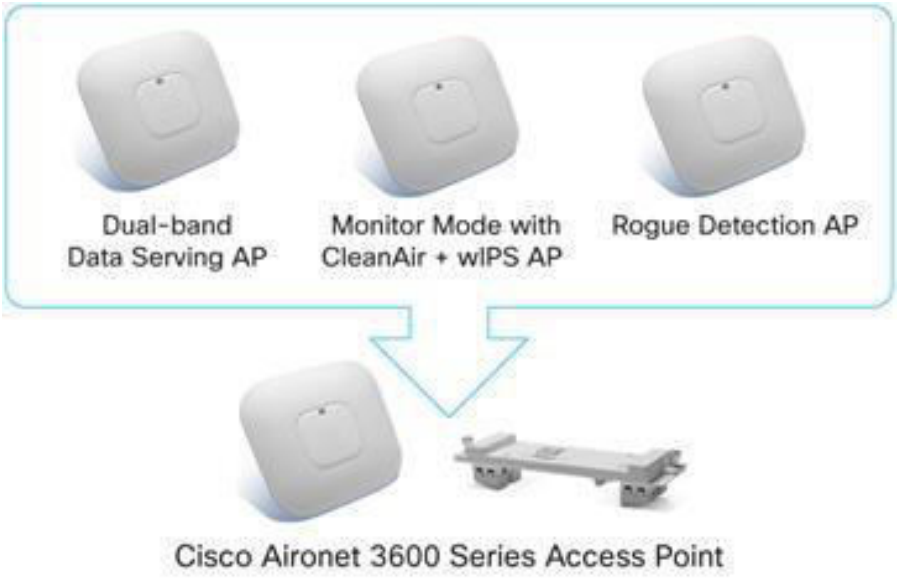


FIGURA 1-8: Cisco Aironet 3600 con módulo WSSI.

Fuente: [28]

1.8. Objetivos

El alcance de la presente tesis se definirá con el objetivo general y los objetivos específicos planteados en las secciones 2.1.1 y 2.1.2

1.8.1. Objetivo general

El objetivo general de la tesis es el diseño de una red de sensores (número y ubicación) para el sistema de detección de Rogue APs en la red WiFi del campus PUCP. Cada sensor es un módulo WSSI conectado a uno de los APs Aironet 3600/3700 existentes en la PUCP.

1.8.2. Objetivos específicos

Además, los objetivos específicos necesarios para poder lograr el objetivo general son:

- Medición y recolección de la relación señal/ruido para los diversos pabellones dentro del campus.
- Procesamiento de la información obtenida para determinar la cobertura de la señal inalámbrica para los diversos APs válidos.
- Implementación de algoritmos de optimización con la finalidad de buscar una solución que permita obtener la posición del Rogue AP en base a triangulación de la señal.

Capítulo 2

Optimización combinatoria: NP-Completeness y Minimum Cover Set

El objetivo de la presente tesis es el diseño de una red de sensores en base a la infraestructura actualmente disponible. Esta red se forma añadiendo módulos WSSI a APs Aironet 3600/3700 ya existentes. El problema a resolver (encontrar un set óptimo de APs para albergar los módulos WSSI) tiene una naturaleza combinatoria que lo hace computacionalmente demandante. Como se mostrara más adelante, este problema pertenece a la clase de problemas de decisión NP-Complete (NPC), los que han sido objeto de estudio e investigación por décadas.

Esta sección presenta un resumen de la teoría de NP-Completeness, con la intención de ayudar a entender la naturaleza del problema a resolver, y algunas herramientas existentes. Se caracterizara el problema a resolver como una instancia de la clase de problemas Minimum K-Cover Set, y se presentara una formulación optima del problema (Mixed Linear Integer Programming, o MILP, que puede requerir tiempos de ejecución muy altos), junto con dos heurísticas que proveen una solución sub-optima en un tiempo razonable.

2.1. NP-Completeness

A fin de entender la naturaleza de un problema (su dificultad inherente) y sus sub-problemas, se ha estudiado y clasificado diferentes clases de problemas en la literatura. El problema a resolver pertenece a la clase NP-C (NP-Complete) por lo que en esta sección se presenta una descripción de esta clase de problemas.

2.1.1. Problemas de decisión

Los problemas de decisiones son un tipo de problema computacional cuya respuesta es “SÍ” o “NO”. A pesar de que existen diversos tipos de problemas computacionales, la mayoría de ellos pueden ser reformulados (o transformados en tiempo polinómico) como problemas de decisión. Por ejemplo, un típico problema de optimización como encontrar el mínimo valor de Z que satisfaga una determinada condición puede ser reformulado como uno de decisión iterando sobre posibles valores de Z. Tal que para

Z=1, existe una configuración que satisfaga dicha condición; si la respuesta es negativa, incrementar el valor de Z, si la respuesta es negativa, el primer valor que dio afirmativo en el valor optimo).

De esta forma, se puede identificar un problema de decisión como aquel problema conformado por un subconjunto de entradas Q que permiten obtener una respuesta positiva. Esto permite simplificar la notación de los problemas de la manera siguiente: si una entrada x pertenece al conjunto Q, se escribe Q(x) = SÍ, y si una entrada x no pertenece a un conjunto Q, se escribe Q(x) = NO. La connotación “Sí” es una referencia a una entrada que resulta en una respuesta positiva, y la connotación “NO” es una referencia de una entrada que resulta en una respuesta negativa.

El objetivo es encontrar un algoritmo para problemas de decisiones que sea lo más eficiente en términos de los recursos computables.

2.1.2. Algoritmos

En términos generales, un algoritmo es una serie procedimientos seriales que permiten resolver problemas. De forma concreta, se puede expresar un algoritmo como un programa de computadora que se encuentra escrito en un determinado lenguaje de computadora, tal que si este algoritmo puede resolver un problema Q, el mismo algoritmo puede ser utilizado siempre para resolver cualquier instancia I del mismo problema.

En general, el diseño de un algoritmo tiene como objetivo hallar aquel algoritmo que sea el más eficiente para resolver un problema. En este sentido, la noción de eficiencia implica el uso de los diferentes recursos computacionales para la ejecución de un algoritmo, sin embargo, normalmente se considera como más eficiente al algoritmo que requiere un menor tiempo de ejecución. De modo que los requerimientos de tiempo de un algoritmo son expresados en términos del tamaño de una instancia de un problema, lo cual refleja la cantidad de información necesaria para describir una instancia. Por lo cual se denomina una función de complejidad en el tiempo como el máximo periodo de tiempo que se requiere para resolver cualquier instancia de un problema para cada una de las posibles entradas.

Por consiguiente, diferentes algoritmos poseen diferentes funciones de complejidad en el tiempo, y por consecuencia denominación sobre cuales son considerados eficiente o ineficientes. No obstante, se reconoce una distinción entre dos tipos de algoritmos. En primer lugar, se tiene a los algoritmos de tiempos polinómico, los

cuales se definen como aquellos cuya función de complejidad en el tiempo es la de forma O(p(n)) para una función polinómica p y una entrada de longitud n. En segundo lugar, se denomina a los algoritmos de tiempo exponencial como aquellas cuya función de complejidad no puede ser delimitada por ninguna función polinómica.

Esta distinción entre ambos tipos de algoritmo tiene una principal importancia cuando se consideran problemas con grandes instancias, debido a que, como se aprecia en la figura, la tasa de crecimiento de las funciones exponenciales es mucho mayor que la polinómica.

Función de complejidad en el tiempo	Tamaño de n					
	10	20	30	40	50	60
n	.00001''	.00002''	.00003''	.00004''	.00005''	.00006''
n^2	.0001''	.0004''	.0009''	.0016''	.0025''	.0036''
n^3	.001''	.008''	.027''	.064''	.0125''	.0216''
n^5	.1''	3.2''	24.3''	1.7'	5.2'	13.0'
2^n	.001''	1.0'	17.9'	12.7 días	35.7 años	366 siglos
3^n	.059''	58'	6.5 años	3855 siglos	2*10^8 siglos	1.3*10^13 siglos

Tabla 2.1: Comparación entre diversas funciones de complejidad en el tiempo para algoritmos polinómicos y exponenciales.

Fuente: [29]

La tabla anterior indica una de las principales razones por la cuales los algoritmos de tiempo polinómico son considerados sobre los algoritmos de tiempo exponencial y permite introducir un noción central a la teoría de NP-Completeness. Por lo tanto, dado una constante "k" y un tamaño de variable que ingresan "n", se determina un tiempo polinómico (tiempo "p") $O(n^k)$, tal que todos los problemas que puedan ser solucionados en un tiempo "p" son considerados tratables.

2.1.2.1. Problemas P

Un problema P, por su sigla en inglés Polynomial-Time, es una clase de problemas de decisión que pueden ser resueltos eficientemente, es decir, problemas que cuenta con algoritmos de tiempo polinómico. Más específicamente, son problemas que pueden ser resueltos en un tiempo $O(n^k)$, dadas una constante k, donde n es el tamaño de la entrada del problema. De manera formal, se dice que un problema de decisión Q es P si existe un algoritmo eficiente A tal que para todas las entradas x:

- Si Q(x) = "SÍ", entonces A(x) = "SÍ".
- Si Q(x) = "NO", entonces A(x) = "NO".

2.1.2.2. Problemas NP

Por otra parte, existen casos en los cuales no existe ninguna forma conocida para hallar en tiempo polinómico la solución a un problema de decisión, pero que si un tercero entrega la solución y una prueba, es posible verificar en tiempo polinómico si la solución es correcta o no. Debe notarse que la prueba debe tener un tamaño polinómico para que su tiempo de lectura, además de su tiempo de ejecución, deben ser polinómico.

Los problemas NP, por sus siglas en inglés Non-deterministic Polynomial-Time, son una clase de problemas de decisión los cuales tiene eficientes verificadores, es decir, existe un algoritmo de tiempo polinómico que puede verificar si una solución dada es la correcta. De manera formal, decimos que un problema de decisión Q es NP si existe un algoritmo V de tiempo polinómico tal que para todas las entradas x se cumple que:

- Si Q(x) = "SÍ", entonces existe una prueba "y" tal que V(x, y) = "SÍ".
- Si Q(x) = "NO", entonces para todas las pruebas "y", V(x, y) = "NO".

Por claridad, se presenta una definición alternativa de los problemas NP, basados en una propiedad fundamental con respecto a las máquinas de Turing determinísticas, como todas las computadoras existentes en la actualidad. La definición original de los problemas NP es que son aquellos problemas que pueden ser resueltos en tiempo polinómico por una máquina de Turín No-Determinística, de allí su nombre NP (Non-Deterministic Polynomial, por sus siglas en ingles

La principal ventaja de este tipo de problemas es que existen una variedad de problemas naturales en los cuales se puede verificar eficientemente su solución, dada una prueba corta, a pesar de que no se conoce una forma eficiente de hallar una solución.

2.1.2.3. Relación entre los P y NP

La relación entre las clases P y NP es fundamental para la teoría de NP-Completeness y, así mismo, es uno de los mayores paradigmas en teoría de la computación sin resolver. De forma informal, este paradigma cuestiona la posibilidad de que todo problema cuya solución puede ser verificada fácilmente, en tiempo polinómico, por una computadora también puede ser resuelto rápidamente por una computadora.

Una primera observación es que obviamente $P \subseteq NP$, ya que si existe un algoritmo A polinómico que puede resolver un problema Q, entonces este mismo algoritmo puede ser usado como verificador V.

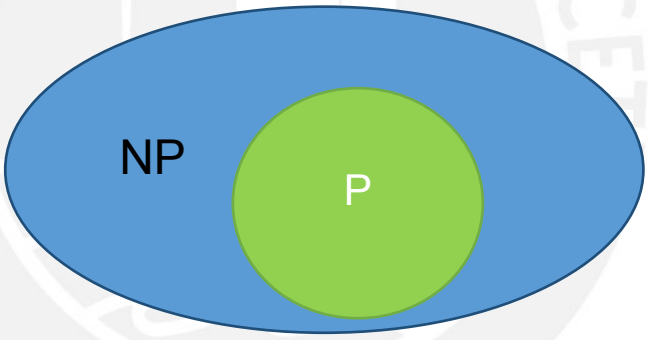


FIGURA 2-1: Visión tentativa de la relación entre P y NP.
FUENTE: [29]

Por otra parte, si P es diferente de NP, entonces la distinción entre P y NP es significativa e importante. Debido a que significa que todos los problemas P pueden ser resueltos por algoritmos de tiempo polinómico, mientras que todos los problemas en (NP – P) no cuentan con solución. Por lo tanto, para comprobar lo antes mencionado, se utiliza el concepto de reducción.

El concepto de reducción nace como un caso especial de la transformación polinómica, en donde se considera la existencia de un determinado algoritmo capaz de resolver un determinado problema, tal que una subrutina de este puede utilizarse para resolver otro problema. Formalmente, dado dos problemas de decisión A y B, ver Figura 2-2, tal que existe un algoritmo β capaz de resolver B en tiempo

polinómico. Además, se tiene que B es una instancia del problema A. Finalmente, se supone la existencia de un procedimiento que transforme cualquier instancia de α de A, algoritmo que resuelve A en tiempo polinómico, a cualquier instancia de β de B tal que la transformación se realice en tiempo polinómico y las respuestas son las misma. Esto último implica que la respuesta es α es "Sí", si y solo si la respuesta de β también es "Sí".

A partir de esta operación de reducción, nace una clase dentro los problemas de decisión conocida como NP-Hard definida informalmente como aquellos problemas que son al menos tan difíciles como los problemas NP. Mas formalmente, un problema es NP-Hard si y solo si todos los problemas en NP pueden ser reducidos en tiempo polinómico a este. Como consecuencia, si existe un algoritmo en tiempo polinómico que resuelva cualquier NP-Hard, entonces este puede utilizarse para encontrar algoritmos polinómico para todos los problemas NP.

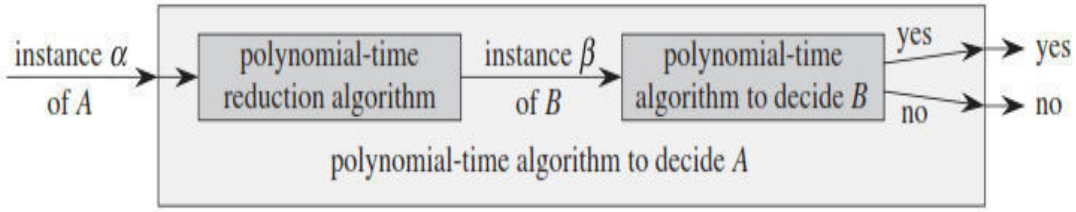


FIGURA 2-2: Proceso de reducción algorítmica.

FUENTE: [29]

2.1.2.4. Problema NP-Complete

Los problemas NP-Complete son aquellos problemas que son considerados como los más difíciles dentro de los problemas NP, este sentido de dificultad es referencia a la cantidad de tiempo necesario para verificar su solución respecto a otros problemas NP. Por lo tanto, si se puede solucionar un problema NP-Complete eficientemente, todos los problemas NP pueden ser resueltos. De manera formal, se denomina a un problema de decisión A como NP-Complete si A es un problema NP y es a la vez NP-Hard (es decir, si todos los problemas NP puede ser reducidos a "A" en tiempo polinómico).

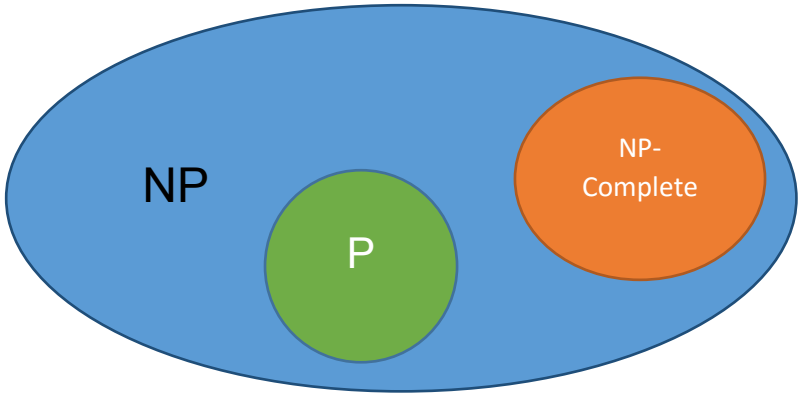


FIGURA 2-3: Nueva perspectiva del mundo de NP.

FUENTE: [29]

Se debe recalcar que si "A" es NP-Complete, se puede resolver cualquier problema NP utilizando el algoritmo de A. Además, si cualquier problema NP-Complete pudiera ser resulto en tiempo polinómico entonces P=NP [29]. En la actualidad, si P = NP es una de las preguntas sin responder más importantes de las Ciencias de la Computación. Luego de décadas, no se ha encontrado ningún algoritmo de tiempo polinómico para los problemas NP-Complete. De encontrarse uno, por ejemplo, todos los sistemas de encriptación actuales pudieran ser descifrados en tiempo polinómico.

Los problemas NP-Complete se encuentran en diversos dominios: booleanos, lógicos, gráficos, aritméticos, diseño de redes, conjuntos y particiones, almacenaje y entrega, programación matemática, algebra y teoría de números, juegos y laberintos, biología, química, física y muchos otros campos. En la presente tesis, se enfocara a un determinado tipo de problema conocido como mínimo conjunto de cobertura (Minimum Cover Set, o MCS), el cual es un problema de diseño de redes y es un problema NP-Complete.

2.2. Minimum Cover Set

El problema de set de cobertura, en ingles set-covering problem, es un problema de optimización que modela diversos problemas cuyo objetivo es la distribución de recursos que requieren ser asignados. Su problema de decisión correspondiente generaliza el problema NP-Complete de vértice de cobertura, y por lo tanto es también NP-Hard.

Una instancia del problema de set de cobertura consiste de un finito conjunto X y una familia F de subconjuntos (S) de X, de forma que cada elemento de X pertenece al menor a un elemento S de F.

$$X = \bigcup_{S \in F} S$$

El problema del mínimo conjunto de cobertura, Minimum Cover Set (MCS) en inglés, es uno de los principales problemas dentro de la categoría de NP-Complete. Para el cual, se establece un grupo o colección “F”, el cual es un conjunto de subconjunto de un conjunto finito X, y un integral positivo “K”. Este problema de decisión busca determinar la existencia de un subconjunto de F denominado FK con una cardinalidad menor o igual a K, tal que cada elemento de X pertenece al menos una vez a un miembro de FK.

$$X = \bigcup_{\in F^K} S$$

2.2.1. Triple Cobertura versus Cobertura

En esta tesis, se trabaja una variante de este problema en relación al posicionamiento y distribución necesaria de sensores para la detección de Rogue AP. Este se debe a que una de los principales problemas de las redes de sensores inalámbricos es el problema de cobertura. En general, este problema refleja que tan bien un área es monitoreada o rastreada por un grupo de sensores.

En esta forma, se considera una forma más general del problema de cobertura, en el cual se tiene un conjunto de sensores distribuidos dentro de un área objetivo y se busca determina si dicha área puede ser suficientemente cubierta. Cada sensor cubre un área (o grupos de posiciones objetivos) S, y el set de tosas las áreas de cobertura de todos los sensores es F. En esta sentido, se busca determinar si cada punto dentro del área objetivo X es cubierto por al menos una cantidad de sensores k, donde k es el parámetro otorgado. De esta forma, existen diversas variantes del mismo problema en base a diversos objetivos de cobertura y otros requerimientos.

Dado el caso en el que k es igual a 1, este es un caso muy especial en el área de cobertura, siendo una de sus principales variantes de este el problema conocido como el problema de Ubicación para Máxima Cobertura.

Por otra parte, existen diversas aplicaciones en los cuales se requiere un parámetro k mayor a 1, en los cuales se requiere una alta capacidad de monitoreo. Así mismo, este caso ocurre cuando se utilizan protocolos de posicionamiento basado en triangulación, en donde se requiere un k mayor o igual a 3.

2.2.2. Optimal Problem formulation

La programación lineal puede ser aplicada a los problemas de cobertura, como el problema de localización de máxima cobertura, y obtener soluciones óptimas globales. Para lo cual se requiere restringir las variables que condicionan lógicamente las posiciones de los nodos para que sean valores no negativos en vez de valores booleanos como se han definido en la sección anterior.

En la optimización lineal de este problema, la variable x_j , la cual es una dependencia lógica de las ubicaciones de los nodos que forman parte de la solución, nunca será mayor que uno, salvo que se logra la cobertura total. En este sentido, si existe algún valor de x_j mayor de uno en una optimización, este puede ser reducido a uno sin invalidar ninguna restricción anterior. Además, esta reducción puede ser aplicada con la finalidad de aumentar otro x_j , mediante la restricción del número máximo de elementos en la solución, “P”.

En esta forma, el objetivo del programa trata que $\overline{y_i}$ sea tan pequeña como sea posible, y debido a que nunca es necesario que $\overline{y_i}$ sea mayor a uno para satisfacer las condiciones del sistema, $\overline{y_i}$ nunca tendrá un valor mayor de uno en una solución de programación lineal óptima. Por lo tanto, dado que x_j nunca será mayor que dado a menos de que se logre una cobertura total, el programa lineal terminara con una solución óptima en donde se tiene que $0 \leq x_j \leq 1$ para todo $j \in J$ y $0 \leq \overline{y_i} \leq 1$ para todo $i \in I$.

2.2.3. Función objetivo

El objetivo de la programación es minimizar la cantidad de nodos requeridos para que el sistema pueda propiciar a un número de puntos o personas que son cubiertas dentro de una determinada distancia efectivamente un servicio. Una primera restricción del sistema permite que la variable y_i sea igual a uno si y solo si una o más facilidades, puntos a ser cubiertos, son establecidas como sitios en el conjunto N_i.

2.2.4. Heurística

Los problemas de conjunto de cobertura son NP-Complete, y por lo tanto el tiempo de cómputo de una solución óptima – usando los algoritmos conocidos a la actualidad – se hace prohibitivamente largo a medida que se aumenta el tamaño de la instancia. Por lo tanto, para una red del tamaño de la red bajo estudio, “redpucp”, y dependiendo de la estructura de la instancia, es probable que una solución óptima no pueda ser hallada en tiempo razonable, por lo que sería necesario recurrir a heurísticas que provean soluciones aproximadas en tiempos más cortos.

En esta sección presentamos una heurística basada en el algoritmo Greedy, que explota la sub-modularidad existente en el set de nodos cubiertos por un grupo de sensores.

2.2.4.1. Submodularidad

Muchas funciones en optimización combinatoria satisfacen la siguiente propiedad $F(A \cup X) - F(A) \geq F(A' \cup X) - F(A')$. Esta propiedad expresa que la adicción de un elemento a un conjunto pequeño brinda una mayor ganancia o ayuda que cuando se añade a un conjunto de mayor tamaño, este tipo de función recibe la denominación de submodular. En este sentido, se espera que el comportamiento de la heurística al momento de seleccionar las posiciones para los módulos de la solución, tenga un comportamiento submodular al considerar un elemento nuevo como parte de su solución.

2.2.4.2. Algoritmo Greedy

El algoritmo de aproximación de codicia, o c, funciona al seleccionar en cada etapa un conjunto de S que cubra la mayor cantidad de los elementos que no han sido cubiertos en un determinado momento.

$GREEDY - SET - COVER(\mathrm{X}, \mathcal{F})$

$1\ U = X$

$2\ \mathfrak{e} = 0$

$3\ WHILE\ U\ \neq 0$

$4 \qquad selecciona\ un\ S\ \in\ \mathcal{F}\ que\ maximiza\ |S\ \cap U|$

$5 \qquad U = U - S$

$6 \qquad \mathfrak{e} = \mathfrak{e}\ \cup \{S\}$

$7 return\ \mathfrak{e}$

El algoritmo funciona de la siguiente forma, el conjunto U contiene en cada etapa un conjunto de todas aquellas ubicaciones que aún no han sido cubiertas. El conjunto ɐ contiene la cobertura que está siendo construida. En la línea cuatro es donde se realiza el paso de decisión al escoger un subconjunto de S que permita cubrir la mayor cantidad de elementos no cubiertos. De esta forma, se utiliza la propiedad de submodularidad para asegurar que haya la mayor ganancia posible al agregar dicho elemento cuando la solución aun es nula. Posteriormente a la selección de S, en la línea cinco se remueven sus elementos de U y en la línea seis, S es agregada como pate de la solución. Finalmente, cuando el algoritmo terminada, el conjunto ɐ contiene un subconjunto de $\mathcal{F}$ que cubre X.

2.3. Maximal Covering Location Problem

Este problema tiene como objetivo maximizar la población que puede ser servida dentro del rango de una distancia de servicio fijada o un tiempo para una cantidad limitada de recursos o instalaciones. Dada una red definida de nodos, se puede realizar la siguiente formulación matemática de este problema.

- Se cuenta con un conjunto de puntos que deben ser cubiertos, denotados por el conjunto “I”
- Se cuenta con un conjunto de nodos o recursos para cubrir los puntos demandados, denotados por el conjunto “J”.
- Se tiene una distancia S, para lo cual cualquier punto demandado es considerado como no cubierto.
- Se tiene una distancia $d_{i,j}$, la distancia más corta desde el nodo i al nodo j.

- Se tiene la variable x_j que es igual a 1 si el nodo se colocado en la posición j, y 0 en cualquier otro caso.
- Se define la población que puede ser servido en un punto de demanda como a_i,
- Se tiene el conjunto N_i, denominado como el conjunto de puntos elegibles para ser cubiertos.
- Se tiene el parámetro "P", que define la cantidad de nodos a ser colocados.
- Se tiene la restricción y_i, la cual permite que este valor sea igual a 1 cuando uno o más nodos son establecidos dentro de posiciones en el conjunto N_i, es decir, uno o más nodos son colocados a una distancia menor a S de un punto de demanda; y sea igual 0 en cualquier otro caso.

Dado las variables anteriores, se define este problema y sus condiciones de la siguiente forma:

- Maximizar $z = \sum_{i \in N_i} a_i * y_i$, para todos los $i \in I$. Esta expresión busca maximizar la cantidad de puntos demandados que si pueden cubiertos por algún nodo.
- Sujeto a que $z = \sum_{i \in N_i} x_j \geq y_i$, para todos los $i \in I$. Esta expresión restringe que todos los puntos que pueden ser cubiertos sean cubiertos al menos por un nodo.
- Sujeto a que $\sum_{j \in J} x_j = P$. Esta restricción limita la cantidad máxima de nodos que pueden ser colocados.[13,20]

Capítulo 3

Diseño del algoritmo de optimización

3.1. Metodología general del diseño

Para el diseño de los algoritmos de optimización necesarios para diseñar la red de sensores para la detección de Rogue AP se utilizaron dos herramientas de software:

- Matlab: es una herramienta de software matemático que ofrece un entorno de desarrollo integrado con un lenguaje de programación propio, el lenguaje m. Posee un lenguaje, herramientas y funciones internas matemáticas que permiten explorar múltiples enfoques y obtener una solución más rápida en comparación con lenguaje tradicionales de programación como C/C++ o Java. Posee diversas herramientas que permiten una diversidad de aplicaciones, incluyendo el procesamiento de señales y comunicaciones, procesamiento de imágenes y video, sistemas de control, prueba y medición, finanzas computacionales y biología computacional.
- IBM ILOG CPLEX Optimization Studio: software de la compañía IBM de programación que permite resolver problemas matemáticos utilizando algoritmos para producir precisas y lógicas decisiones para mejorar la eficiencia, reducir costos e incrementar las ganancias. Provee con solucionadores matemáticos programables y flexibles para problemas de programación linear (ILP), programación integral mixta (MILP), programación cuadrática (QILP).

Los pasos a seguir para los modelos de optimización fueron los siguientes:

1. Establecer el objetivo de los modelos de optimización, minimización o maximización, para las variables.
2. Definir todas las restricciones a las cuales se verá sujeto el sistema.
3. Usar el lenguaje de programación de Matlab para plasmar el objetivo y las restricciones de forma que pueda ser reconocido por CPLEX Optimization Studio.
4. Ejecutar el programa usando un programa CPLEX para problemas de integrales mixtas (MILP).
5. Si los resultados del programa son coherentes con los objetivos y datos, se procede a la implementación del algoritmo. De otra manera, se regresa al primer paso.

3.2. Procesamiento de la Información

El tiempo requerido de procesamiento de un algoritmo está directamente relacionado con la cantidad de información que se ingresa, así como la cantidad de parámetros con los cuales se va a trabajar. Además, gran cantidad de los algoritmos y modelos de optimización para problemas de cobertura buscan simplificar y agilizar los procesos al concretizar las restricciones de los problemas. De esta forma, un primer objetivo específico es concretizar y simplificar la información y las restricciones con la cual van a operar los algoritmos.

La información es obtenida de la tesis de Levantamiento de mapa de atenuaciones de señal electromagnética en las bandas 2.4 GHz y 5GHz para la red WiFi del campus PUCP [40]. En dicha tesis, se realizó mediciones de la señal recibida de todos los APs que pertenecen a la red inalámbrica del campus de la PUCP, "redpucp", para una específica posición.

Para el proceso de detección de Rogue AP, se requiere que los nodos de monitoreo, módulos WSSI instalados en un AP existente, sean capaces de detectar la trama Beacon de los APs que se encuentren dentro del área de cobertura de la red inalámbrica "redpucp", tal que posteriormente este información pueda ser enviada a un servidor de detección y se determine la presencia de un Rogue AP durante el escaneo. Para lo cual, se considera que un Rogue AP está configurado para transmitir a su máxima potencia posible con la finalidad de capturar la mayor cantidad de usuarios posibles dentro de un área. Debido a que al aumentar su potencia de transmisión, aumenta la probabilidad de que sus beacons sean recibidos por un usuario con una potencia mayor a los de los AP válidos, por lo tanto es más probable que el usuario se conecte al Rogue AP en vez del AP valido. Entonces, se considera que se está emitiendo al menos a 23dBm, valor pico de transmisión de los APs válidos y asimismo de dispositivos móviles categoría tres. Dado que el Rogue AP, por su naturaleza posiblemente maliciosa, puede estar transmitiendo con una potencia mayor al límite regulatorio, la opción conservadora es asumir que transmite al menor valor que tiene permitido por estándar, es decir, 23dBm ya que esto presenta el mayor reto a la red de sensores.

Para determinar la sensibilidad que permite a un sensor WSSI detectar la trama beacon, se usa la siguiente fórmula:

$$S_{dBm} = -\frac{174dBm}{Hz} + 10\log_{10} B + NF + \text{SINR}$$

En donde, -174dBm/Hz se considera como el piso de la señal existente en el éter a una temperatura ambiente, 290 grados kelvin. B es el ancho de banda de la señal, el cual corresponde a un canal de 20MHz para 802.11n, NF es la figura de ruido de los circuitos del módulo WSSI y SINR es la relación señal-interferencia-ruido necesaria para decodificar un paquete con alta probabilidad (0.9). El SINR necesario es determinado por la velocidad, modulación, y codificación del enlace, así como el diseño del receptor/decodificador (óptimo o sub-óptimo).

En 802.11n (la red bajo estudio) los beacons de los APs se transmiten usando el Modulation and Coding Scheme (MCS) index 0: un bitrate de 6.5Mbps, Modulación BPSK, coding rate ½, 1 stream espacial [39] por lo cual, para un receptor se requiere un SINR igual a 3.56dB para garantizar un Frame Error Rate (FER) menor al 10%, como se puede apreciar en la siguiente tabla.

MCS	0	1	2	3	4	5
SINR	3.56	6.55	8.93	13.03	15.73	20.44

Tabla 3-1: SINR requerido de 10%FER para 802.11n MCSs.

FUENTE: [41]

Asumiendo una figura de ruido NF = 0 dB para un receptor ideal, se obtiene una sensibilidad ideal de -97.43dBm para un ancho de banda de 20MHz. Sin embargo, los sensores WSSI a usar no son ideales, y su sensibilidad bajo modulación MCS 0 es provista por el fabricante Cisco: S_{dBm} = -90dBm a 2.4GHz, y S_{dBm} = -91 dBm a 5GHz [28]. Entonces, como se cuenta con una sensibilidad de receptor conocida, es posible determinar la máxima perdida por camino permitida (MAPL), con la siguiente fórmula:

$$P_{tx} + G_{tx} + G_{rx} - MAPL = S_{dBm}$$

En donde, P_{tx} y G_{tx} son la potencia y ganancia del transmisor, en esta situación el Rogue AP, y G_{rx}es la ganancia del receptor, el módulo WSSI, igual a 2.5dBi y 5.5 dBi para las bandas de 2.4GHz y 5GHz, respectivamente. Asumiendo G_{tx} = 0dBi, con la finalidad de mantener los valores dentro de parámetros conservadores, es posible determinar el MAPL a partir de la ecuación anterior, obteniendo un valor de 115.5 dB para la banda de 2.4GHz, y 119.5 dB para la banda de 5GHz.

Finalmente, a partir de la comparación entre los valores de pérdidas por camino encontrados, pathloss, y el valor del MAPL obtenido previamente, se determina si un punto objetivo puede ser cubierto por un determinado sensor WSSI instalado en un AP, este arreglo de puntos objetivos y APs recibe la notación de Matriz de Cobertura o detección , a_{ij}, la cual será de gran importancia para la implementación de los modelos de optimización y los algoritmos. Notar que a los valores medidos de pathloss en [40] se les agrega un margen por desvanecimiento de 6 dB, tres veces el valor de la desviación estándar promedio, 2dB, del pathloss medido.

3.3. Modelo de Optimización

Los modelos de optimización son formulaciones matemáticas que intentan dar respuesta a un tipo general de problemas en donde se desea elegir el mejor entre un conjunto de elementos. Los problemas de cobertura, así como diversas variantes del mismo, pertenecen al grupo de problemas que pueden ser expresados mediante formulaciones matemáticas. El siguiente modelo se enfoca en las diversas necesidades que se requieren para la utilización de diversas aplicaciones para la detección, mitigación y localización de los Rogue APs.

3.3.1. Cobertura K

Existen diversas formas que como neutralizar la amenaza conocida como Rogue AP, como la técnica de desautenticación o de confusión de beacon. No obstante, la principal desventaja del uso de esta técnica es que utiliza recursos del sistema y que puede ocasionar una interrupción de los servicios innecesariamente. Por tal motivo, una de las principales funcionalidades con las cuales son configurados los WIPS es con un sistema de localización que permita detectar la localización de las amenazas y poder afrontar el problema sin el uso de recursos directos de la red. El objetivo de este modelo es permitir la utilización de aplicaciones de localización las cuales requiere una precisión mayor de la que puede proveer la cobertura simple (1-coverage). Este modelo ha sido desarrollado para mitigar la falta de precisión del modelo de máxima cobertura. De esta forma, una posición en un área es considerada como cubierta si y solo si este posición se encuentra dentro del rango de un numero K de sensores. Entonces, se dice que una región A es K-cubierta si cada punto en A es cubierto por K sensores. Para este modelo se formulan los siguientes parámetros [6]:

- Se cuenta con un conjunto de N sensores $v_1, v_2, v_3, \dots, v_n$, los cuales se encuentra distribuidos dentro de una región.

- Se tiene un conjunto de T de objetivos $I_1, I_2, I_3, \dots, I_t$ a monitorear.
- Además, cada nodo v_i cuenta con un área de monitoreo $S(v_i)$. De forma que cada objetivo dentro de esta área es monitoreada por v_i. El conjunto de objetivos cubiertos por vi se denota Tv_i.

Para localizar un Rogue AP en un área plana (2D) se requiere K = 3. En el caso de 3 dimensiones, para localizar eficientemente un punto en el espacio se requiere K=4, mientras que con K=3 en teoría se consigue determinar 2 posiciones candidatas, en una de las cuales se encuentra el Rogue AP. Sin embargo, como no todos los puntos del espacio pertenecen a la red, como por ejemplo en el subsuelo o en el aire sobre los pabellones, por lo general, basta un factor K=3 para identificar la localización del Rogue AP. Por esta razón, en este trabajo asumimos que K=3. Para los casos donde se obtengan dos localizaciones candidatas para la ubicación de un Rogue AP, se tomaran medidas correctivas en ambas.

3.3.1.1. Formulación de programación entera

Se formula el problema de K-cobertura de la siguiente forma:

a) Valores dados: son aquellos valores dados por las características del sistema.
   - n: número total de nodos de escaneo o sensores.
   - t: número total de objetivos, puntos del área de cobertura.
   - j: Indicador para los nodos de escaneo, $\forall j \in [1, n]$.
   - i: Indicador para los objetivos, $\forall i \in [1, t]$.
   - a_{ij}: indicador que determina si un objetivo i puede ser escaneado por un nodo j. Tal que este indicador es igual a 1 si puede ser escaneado y 0 en cualquier otro caso. En particular, este indicador será igual a 1 si y solo si el pathloss medido en [Ref. Tesis de Emerson] es menor o igual al MAPL – fade_margin.

b) Variable: parámetro que será optimizado por el programa.

$$x_j = \begin{cases} 1 \ , si\ el\ sensor\ j\ es\ selecionado\ para\ K-cobertura \\ 0 \ , cualquier\ otro\ caso \end{cases}$$

Posteriormente, el problema puede ser formulado en programación MILP como 0-1 de la siguiente forma:

- Objetivo: $z = Min \sum_{j=1}^{n} x_j$

- Sujeto a que: $\sum_{j=1}^{n} a_{ij} * x_j \geq K, \ \forall\, i \in [1,t]$
- Sujeto a que $x_j = \{0,1\}, \forall\, j \in [1,n]$

La primera línea expresa el objetivo del modelo lineal, el cual busca que la solución tenga la menor cantidad de sensores posible para lograr que el área objetivo sea cubierto por K.

La segunda línea es la principal restricción que limita la solución. En este sentido, el propósito de esta línea es forzar que la solución considere que todos los puntos t dentro de la región debe ser cubiertos por al menos K sensores. A partir de esta restricción, es posible realizar un enfoque en el factor K=3 establecido previamente.

Finalmente, la última restricción permite que el programa pueda ser formulado entorno a una variable binaria. [6,14]

3.4. Algoritmo de Greedy

A fin de obtener soluciones casi óptimas en un periodo razonable de tiempo, esta heurística fue desarrollada. Este algoritmo empieza con una solución vacía para posteriormente agregar de forma interactiva posible candidatos a la actual solución que maximicen una cierta función beneficio. Esta función mide el beneficio logrado cuando se agrega un nodo candidato a una solución actual parcial. La función beneficio es procesada adaptativamente para cada sitio candidato que no ha sido incluido en la solución actual. Para lo cual, se define el conjunto de puntos TP, el cuales representa a todos los puntos objetivos o posiciones que deben ser escaneadas. Además, se define el conjunto CS como el conjunto de todos los nodos o APs candidatos para poder cubrir todos los TPs. [18].

3.4.1. Submodularidad de Greedy

El problema de cobertura no es un problema sub-modular, sin embargo la función beneficio en la cual se basa el algoritmo de greedy es sub-modular. Esta función beneficio representa la ganancia de cobertura de los TPs que se obtiene dado un incremento en el conjunto de nodos candidatos CS. Dicha función tiene una propiedad sub-modular, en donde, se puede hallar similares propiedades en cuanto a la cardinalidad de los elementos que conforman la cobertura de un AP o nodo de detección. En este sentido, se presenta el siguiente sistema que representa dos conjuntos que conforman una solución al problema.

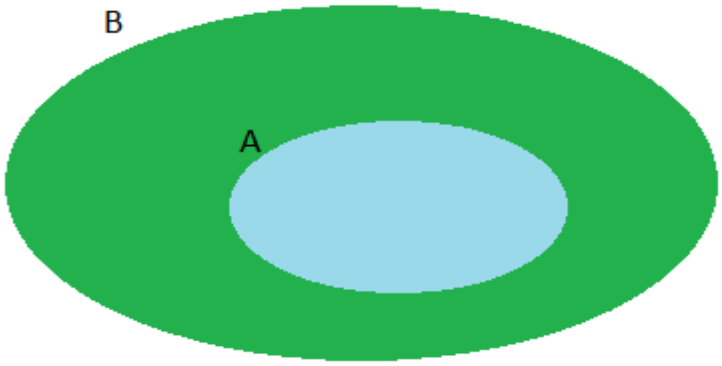


FIGURA 3-1: Visión tentativa de la solución.
Fuente: Elaboración Propia

Entonces, se va a contar con dos conjunto, A y B, tal que el conjunto $A \subseteq B \subseteq V$, los cuales representan el área de cobertura y por lo tanto la cantidad de nodos que pueden ser detectados; mientras que V representa el universo. La función beneficio va a ser dada por la adición de un nuevo nodo S al conjunto solución, en otras palabras, un aumento en el grado de cobertura de la solución. Por lo tanto, el sistema se representa de la siguiente forma:

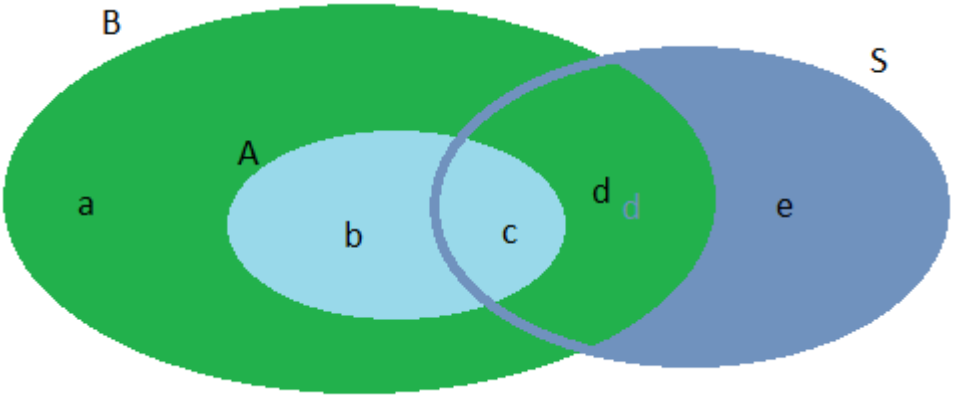


FIGURA 3-2: Visión tentativa del funcionamiento en la heurística con submodularidad.
Fuente: Elaboración Propia

Por lo tanto, en términos de cardinalidad, la propiedad submodularidad queda expresada en términos de cardinalidad de la siguiente manera:

$$f(A \cup S) - f(A) \geq f(B \cup S) - f(B)$$

$$n(A \cup S) - n(A) \geq n(B \cup S) - n(B)$$

$$n(A) + n(S) - n(A \cap S) - n(A) \geq n(B) + n(S) - n(B \cap S) - n(B)$$

$$n(S) - n(A \cap S) \geq n(S) - n(B \cap S)$$

$$c + d + e - c \geq c + d + e - c - d$$

$$d + e \geq e$$

Para lo cual, se tiene que sí $S \in V \backslash B$, entonces se comprueba que $d \geq 0$, por lo tanto se comprueba que este conjunto de funciones representa un conjunto convexo. Además, se puede decir que f es no decreciente si $f(A) \leq f(B)$, para todo $A \subseteq B \subseteq V$. Esto significa que dado un conjunto finito V, siempre existe al menos un elemento que brinda una función beneficio positiva, siempre que $n(B) \neq n(V)$. Entonces, como se ha demostrado la función beneficio exhibe un comportamiento propio de una función sub-modular, por lo tanto se espera que los algoritmos greedy tengan un buen desempeño. En el siguiente algoritmo, se utilizara la propiedad demostrada, en el cual se busca agregar primero aquellos elementos que brindan una mayor utilidad a la solución.

3.4.2. Estructura lógica de la heurística

La estructura general de la heurística es la siguiente:

$PROCEDURE \;\; Heuristic(A, k)$

$S = 0;$

$BuildUpSolution(A, S, k);$

$return\ S$

$END\ Heuristic$

En donde S es el conjunto de sitio candidatos en donde los nodos de monitoreo espectral son instalado, A es la matriz de cobertura antes definida y k es el factor de cobertura por posición objetivo. La función BuildUpSolution se encarga de implementar la fase greedy de la heurística, la cual converge interactivamente para una solución posible. Además, esta función se encarga de determinar el primer nodo que forma parte de la solución antes de la fase de greedy.

3.4.3. Fase de Greedy

La fase Greedy de la heurística propuesta empieza a partir de una solución nula o vacía (S=0) y agrega interactivamente un sitio candidato a la vez. Este procedimiento finaliza cuando todos los puntos objetivos son cubiertos por un factor de cobertura k, en esta situación igual a 3, por los nodos candidatos del conjunto S. Luego de cada interacción, el nodo que maximice la función beneficio es incluido a la solución. Un seudocódigo del proceso de implementación es de la siguiente forma:

$PROCEDURE\ BuildUpSolution(A, S, k)$

$Best\_CS = PickBestCS(A);$
$S = S\ \cup\ Best\_CS;$
$Covered\_TPs = Covered\_TPs \cup I\_Best\_CS$
$\quad WHILE\ Covered\_TPs\ != ALL\_TPs$
$\quad\quad GreedyStep(A, Covered\_TPs, S);$
$END\ BuildUpSolution(A, S)$

La función $PickBestCS$ escoge el primer nodo candidato para ser agregado a la solución. La idea de esta función es coger el AP cuya área de cobertura tenga el menor traslape con las demás áreas de cobertura del resto de los candidatos.

La función $GreddyStep$ representa el núcleo de la fase Greedy y retorna el siguiente nodo que debe ser agregado a la solución. El seudocódigo de esta función es el siguiente:

$PROCEDURE\ GreedyStep(A, Covered\_TPs, S)$
$MaxFunction = 0;$
$DO\ FOR\ j\ \notin S$
$\quad IF\ Benefit\_function\_j > MaxFunction;$
$\quad\quad CS\_ToAdd = j;$
$\quad\quad MaxFunction = Benefit\_function\_j;$
$\quad END$
END
$S = S \cup CS\_ToAdd;$
$Covered\_TPs\ = Covered\_TPs\ \cup I\_CS\_ToAdd;$
$END\ GreedyStep$

En donde, I_CS_ToAdd es el conjunto de puntos objetivos que son cubiertos por el nodo candidatos j. Los nodos que son agregados a la solución, son aquellos con la mayor función beneficio. Para lo cual se define una función F, la cual representa el número de nodos cubiertos. Así como, la función F_k que representa el número de nodos que son cubiertos 3 veces. Además, se define la variable x, la cual tiene un

valor igual a 1 cuando existe algún nodo que es cubierto al menos 3 veces. Por lo cual la función beneficio es calculada de la siguiente forma:

$$Benefit\_function\_j = \begin{cases} F(S \cup j) - F(S), x < 1 \\ F_k(S \cup j) - F_k(S), x \geq 1 \end{cases}$$

$$x = \begin{cases} 0, F_k(S) < 1 \\ 1, F_k(S) \geq 1 \end{cases}$$

De esta forma, se presenta una función beneficio la cual es definida por medio de dos instancias en la solución. En una primera instancia, se tiene que la función beneficio está definida como la ganancia en cobertura que se obtiene al agregar un nuevo sitio candidato respecto a la cobertura actual, esta instancia corresponde al estado inicial de la solución. Mientras que en la segunda instancia, la función beneficio está dado por la ganancia en cobertura de aquellos sitios candidatos que brinden un incremento en el número de sitios objetivos que son cubiertos por tres nodos.

Por otra parte, debido a que durante cada iteración se agrega un nodo, el cual puede cubrir al menos un punto objetivo, el procedimiento BuildUpSolution requiere de n*m pasos como máximo, en donde n y m son el total de puntos objetivos y de nodos candidatos respectivamente. [27]

No obstante, bajo el estado actual del algoritmo, este se encuentra diseñado para poder solucionar el problema de máxima de cobertura, pero no el de triple cobertura. Por tal motivo, se ha realizado modificaciones en la función beneficio tal que permita solucionar el anterior problema. Por lo tanto, en una primera instancia de la solución, la función beneficio se mantendrá igual hasta que ocurra una singularidad $(x = 1)$. Esta singularidad corresponde al momento en el cual existen puntos objetivos cubiertos por 3 sensores, a partir de la cual la función objetivo será definida por aquella que brinde más puntos cubiertos por 3 sensores. No obstante, existe la posibilidad de que esta singularidad no ocurra, ocasionando que el programa falle y no sea posible que los puntos objetivos sean cubiertos por 3 sensores.

3.4.4. Fase de Búsqueda Local

La fase Local Search [27], búsqueda local, es la parte final en la lógica del algoritmo Greedy de la heurística propuesta. Esta fase toma la solución S encontrada anteriormente durante la fase Greedy y trata de mejorarla. En este sentido, se utiliza la vecindad de la solución S para explorar la presencia de una mejor versión. De esta forma, a partir de la solución S, se empieza a remover la presencia de un miembro,

y luego dos miembros de la solución que la conforman para luego posteriormente aplicar una solución modificada Sp de la lógica utilizada en BuildUpSolution descrita en la sección anterior. El seudocódigo de la función es la siguiente

$PROCEDURE\ LocalSearch(A, S)$
$MaxOf = ComputeOf(A, S);$
Do
$Enhaced = FALSE;$
$DO\ FOR\ j \in S$
    $S = S\{j\};$
    $Covereded\_TPs = Covered\_TPs \setminus \{I\_j\}$
    $BuildUpSolution(A, Covered_{TPs}, S);$
    $NewOf = ComputerOf(A, S);$
    $IF\ NewOf > MaxOf$
        $MaxSOL = S;$
        $MaxOf = NewOf$
        $Enhanced = TRUE;$
    FI
    $DO\ FOREACH\ i\ IN\ s\ and\ i > j$
        $S = S \setminus i, j;$
        $Covered\_TPs = Covered\_TPs\ \setminus \{I\_i, I\_j\}$
        $BuildUpSolution(A, Covered\_TPs, S);$
        $NewOf = ComputeOf(A, S);$
        $IF\ NewOf > MaxOf$
            $MaxSOL = S;$
            $MaxOf = NewOf;$
            $Enhaced = TRUE;$
        FI
    OD
OD
$IF\ Enhaced$
    $S = Enhaced;$
FI
$WHILE\ Enhaced;$
$END\ LocalSearch;$

3.4.5. Fase de Búsqueda Local Guiada

La fase “Steered Local Search” o búsqueda local guiada es una heurística propuesta en la presente tesis para reemplazar la presencia del local search antes propuesto en el punto anterior. Esta fase se encuentra basado en el algoritmo “randomized greedy” [42], no obstante es diferente en funcionamiento y no ha ido utilizado en este algoritmo. En este sentido, este algoritmo busca todas las diversas soluciones posibles que se pueden hallar al utilizar la lógica de la fase de BuildUpSolution

cuando se permuta todos los posibles $Best\_CS$ que podrían elegirse inicialmente durante este proceso. Sin embargo, en este caso este algoritmo reduce el tiempo de procesamiento al reducir el grupo total de los candidatos iniciales que podría escoger ($Best\_CS$). Dicha reducción se logra al utilizar únicamente los APs o sitios candidatos que fueron encontrados durante la solución obtenida previamente. A partir de estos candidatos, se inicia el proceso de permutación con los distintos APs o módulos como $Best\_CS$ y luego ejecutando el resto de la lógica de BuildUpSolution.

$PROCEDURE\ LocalSearchSteered(A, S)$
$MaxOf = ComputeOf(A, S);$
$DO\ FOR\ j \in S$
$Best\_CS = j;$
$S\_rand = S\_rand \cup Best\_CS;$
$Best\_CS = j;$
$Covered\_TPs = Covered\_TPs \cup I\_Best\_CS$
    $WHILE\ Covered\_TPs\ != ALL\_TPs$
        $GreedyStep(A, Covered\_TPs, S);$
END_WHILE
    $NewOf = ComputerOf(A, S);$
    $IF\ NewOf > MaxOf$
        $MaxSOL = S;$
        $MaxOf = NewOf$
        $Enhanced = TRUE;$
    FI
DO
$IF\ Enhaced$
    $S = Enhaced;$
FI
$END\ LocalSearchSteered;$

Capítulo 4

Resultados

En el presente trabajo, se diseñan redes de sensores para 4 Pabellones de la PUCP seleccionados por DIRINFO como de alta prioridad, pues concentraban gran parte del tráfico. Para determinar las restricciones del problema, matriz a_{ij} en Sección 3.3.1.1, se usaron las mediciones de atenuación en estos Pabellones obtenidas en [40].

En este capítulo presentamos los resultados del diseño de nuestras redes de sensores, una por pabellón. La razón por la que tenemos 5 redes independientes es que los Pabellones se encuentran particionados, es decir, ningún AP dentro de un Pabellón ilumina un punto ubicado en otro Pabellón. Esto permite dividir el problema principal en 5 instancias independientes. Además, este problema se dividirá por bandas, la banda de 2.4GHz y 5GHz, que representan su respectiva cobertura, y una banda dual, la cual representa la cobertura de un punto objetivo en ambas bandas.

Los resultados obtenidos en los 5 Pabellones son muy parecidos. Por eso, por brevedad, empezaremos describiendo en detalle los resultados para el Pabellón H ("Letras y Ciencias Humanas"). Luego, culminaremos la sección mostrando un resumen de los resultados para toda la red.

4.1. Parámetros del Pabellón H

El pabellón H cuenta con cuatro pisos operacionales cuyos salones se encuentran equipados para brindar las diversas comodidades necesarias con la finalidad de mejorar el nivel de conocimiento del alumnado.

En esta tesis, se dividió este complejo en dos secciones, A y B, tal que la secciones A abarca todas las aulas que corresponde a la enumeración desde 01 hasta 06 de los cuatros pisos, como las aulas 101, 205, entre otras. Mientras que la sección B corresponde a todas las aulas que tiene una enumeración superior, tal como las aulas 312,413, entre otras. No obstante, en la presente tesis solo se consideran los salones de clases como parte de la muestra, a excepción de las aulas del cuarto piso que pertenecen a la sección B, como el aula 412, que son aulas equipadas con equipo informático. Estas áreas informáticas (al igual que áreas administrativas) fueron

excluidas al no contar con mediciones de atenuaciones en [40], debido a restricciones de acceso para toma de mediciones.

El total salones con mediciones para la presente muestra es de 31, a lo cual se adiciona la información recopilada de los corredores adyacentes a los salones por cada sección, lo cual brinda un total de 39 ambientes. En este ambiente se cuenta con ambientes de diversos tamaños, los cuales van desde las 40 muestras por salón hasta más de 80 muestras, como se puede observar en la distribución de muestras por salón de la tabla 4-1.

Piso	Distribución de ambientes	Cantidad de Puntos
Piso 1	Ocho aulas y dos corredores	518
Piso 2	Diez aulas y dos corredores	526
Piso 3	Ocho aulas y dos corredores	541
Piso 4	Cuatro aulas y dos corredores	301

Tabla 4-1: Cantidad de ambientes cubiertos por piso del Pabellón H.
Fuente: Elaboración Propia

De esta forma, se tiene un total de 1886 muestras tomadas para este pabellón. No obstante, no todos los ambientes cuentan con un AP funcional disponible para encontrar nuestra solución. En la Tabla 4-2 se muestra los APs funcionales durante el proceso de recopilación de información y que representa al conjunto finito de alternativas para el diseño de la red de detección de Rogue APs.

Nombre del AP	Potencia 802.11b/g(dBm)	Potencia 802.11ac/n(dBm)
AP_H_101-1	2	17
AP_H_102-1	2	17
AP_H_103-1	2	20
AP_H_104-1	2	12
aulpabh104	2	11
aulpabh112	2	14
AP_H_111-1	2	15
AP_H_112-1	2	15
AP_H_113-1	2	14
AP_H_114-1	2	20
AP_H_201-1	5	15
AP_H_202-1	2	17
AP_H_203-1	2	12
AP_H_204-1	2	14
AP_H_205-1	2	20
AP_H_206-1	2	15
AP_H_211-1	2	15

AP_H_212-1	2	20
AP_H_213-1	2	20
AP_H_214-1	2	15
AP_H_301-1	2	15
AP_H_302-1	2	17
AP_H_303-1	2	15
AP_H_304-1	2	15
AP_H_311-1	2	20
AP_H_312-1	2	17
AP_H_313-1	2	15
AP_H_401-1	5	17
AP_H_402-1	2	15
AP_H_403-1	2	14
AP_H_404-1	5	15
aulpabh411	4	11
aulpabh412	5	17

Tabla 4-2: Potencia 802.11 de los puntos de acceso inalámbricos del Pabellón H.
Fuente: Elaboración Propia

4.2. Resultados para instancias pequeñas del Pabellón H

Se crearon instancias pequeñas del problema las cuales solo contienen la información de los pisos de cada pabellón, tal que la matriz de cobertura solo cuenta con los puntos y lugares candidatos correspondientes al mismo piso.

Además, es preciso mencionar que este código se ejecuta como un primer modelamiento en el cual solo se considera un panorama 2D del problema. Debido a que una primera instancia del planteamiento se consideró que la herramienta de gestión de redes Cisco PRIME disponible en la PUCP para el modelamiento de la señal solo contaba con una capacidad 2D de la capacidad de cobertura.

A continuación se mostraran los resultados de la solución óptima y heurística para instancias pequeñas del problema, estos resultados corresponden a los pisos del Pabellón H, en este sentido, el procedimiento y análisis es similar para los demás pabellones. Asimismo, cabe recalcar que para la solución heurística se utilizara la lógica de la fase de greedy desarrollada en el punto 3.4.3 en conjunto con al algoritmo de búsqueda local guiada.

4.2.1. Calculo de la solución óptima en instancias pequeñas

A continuación se muestran los resultados obtenidos de la solución para cada piso del pabellón H en ambas bandas de frecuencias. De esta forma, se indica la cantidad de puntos a cubrir, la cantidad de puntos candidatos para los módulos y el resultado para lograr triple cobertura.

Pabellón H	Modelo	Puntos	Lugares Candidatos	Resultado 2.4	Resultado 5
Piso 1	Optimo	518	10	5	6
Piso 2	Optimo	526	10	8	9
Piso 3	Optimo	541	7	6	6
Piso 4	Optimo	301	7	3	3

Tabla 4-3: Resultados de la solución óptima para instancias pequeñas del Pabellón H.

Fuente: Elaboración Propia

Observando la cantidad de módulos necesarios por lugares candidatos, podemos ver que en la mayoría de los casos se requiere de más de 50% de los lugares candidatos para poder obtener triple cobertura. En la banda de 2.4GHz, se requiere de un 50% en el primer piso, 80% en el segundo, 85,71% en el tercer piso y 42.86% en el cuarto. Mientras que para 5GHz, se tiene un 60% en el primer piso, 90% en el segundo, 85,71% en el tercero y 42.86% en el cuarto.

4.2.2. Calculo de la solución mediante heurística para instancias pequeñas

A continuación se muestran los resultados de la heurística para cada piso del pabellón H. Para esta solución a pequeña instancia se utilizó la heurística de la búsqueda guiada, sin embargo cabe recalcar que se obtuvo el mismo resultado con las demás heurística. En la siguiente tabla se indica la cantidad de puntos a cubrir, la cantidad de lugares candidatos (módulos), y el resultado de los módulos necesarios para triple cobertura.

Pabellón H	Modelo	Puntos	Lugares Candidatos	Resultado 2.4	Resultado 5
Piso 1	Heurística	518	10	5	6
Piso 2	Heurística	526	10	8	9
Piso 3	Heurística	541	7	6	6
Piso 4	Heurística	301	7	4	4

Tabla 4-4: Resultados de la solución mediante heurística para instancias pequeñas del Pabellón H.
Fuente: Elaboración Propia

Observando la cantidad de módulos necesarios por lugares candidatos, podemos apreciar que para todos los casos se requieren de más de 50% de todos los lugares candidatos para poder obtener triple cobertura. En la banda de 2.4GHz, se requiere de un 50% en el primer piso, 80% en el segundo, 85,71% en el tercer piso y 57.14% en el cuarto. Mientras que para 5GHz, se tiene un 60% en el primer piso, 90% en el segundo, 85,71% en el tercero y 57.14% en el cuarto.

4.2.3. Comparación de la solución óptima y heurística para instancias pequeñas

Podemos observar de las tablas anteriores que los resultados, la cantidad de lugares candidatos seleccionados, son los mismos para la solución obtenida mediante la heurística como para la solución óptima, a excepción para el piso 4 en donde se requiere un nodo más para la solución en ambas. De otra forma, el posible obtener una misma solución con la misma cantidad de candidatos, salvo a excepción del caso antes mencionado.

Por otro lado, se puede ver que se requiere una mayor cantidad de APs con módulos WSSI para poder cubrir la banda de 5GHz. En este sentido, se requiere en la solución óptima de 22 módulos para 2.4GHz y de 24 módulos para 5GHz. De igual forma, se requiere mediante la solución por heurística de 23 módulos y 25 módulos para 2.4GHz y 5GHz respectivamente. Por lo tanto, podemos apreciar un aumento del 5.88% de la cantidad de módulos para 5GHz respecto a 2.4GHz.

Por lo tanto, se espera que para grandes instancias de este problema, el comportamiento presentado se mantenga constante considerando un cierto margen de error. Específicamente, la cantidad de módulos requeridos para solución obtenidos mediante los modelos óptimos y de heurística.

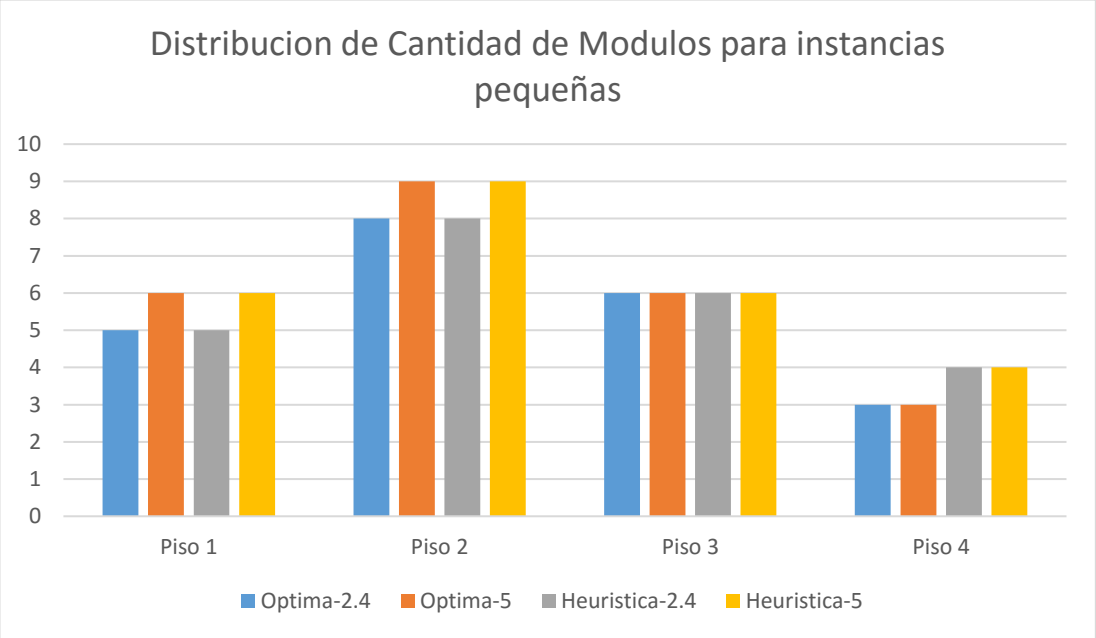


Figura 4-1: Distribución de la cantidad de módulos para instancias pequeñas según modelo de solución.
Fuente: Elaboración Propia

4.3. Resultados del modelo de optimización para el Pabellón H

4.3.1. Resultados del Modelo óptimo de Triple Cobertura

Se procedió a diseñar la red de detección de Rogue AP para grandes instancias utilizando la metodología del modelo de cobertura k-veces, o k-Coverage (k=3). Los resultados fueron procesados y graficados usando Matlab. Para lo cual se utilizaron rutinas MEX para invocar desde MATLAB rutinas del software IBM CPLEX OPTIMIZATION Studio, que fue el usado para poder obtener la solución óptima del problema MILP descrito en Sección 3.3.1. Para este caso, se utilizó el modelo de programación lineal descrito en la sección anterior conjuntamente con el nivel de sensibilidad de los equipos para ambas bandas y la potencia recibida en distintos puntos en el espacio. con la información de la distribución y potencia de transmisión de los APs.

Las siguientes graficas (Figuras 4-2 a 4-5) ilustran gráficamente la calidad de cobertura de la solución encontrada para la banda de 2.4GHz. Cada circulo representa un punto objetivo (es decir, posición que ha sido escaneada dentro de este complejo y debe ser cubierta), mientras el color representa el nivel de cobertura provista: punto rojo (cobertura de 2 o menos), punto azul (triple cobertura), punto verde (cobertura de 4 o más). Se puede concluir gráficamente que ningún punto objetivo sufre de falta de triple cobertura, y un gran porcentaje de los puntos son cubiertos 4 veces o más.

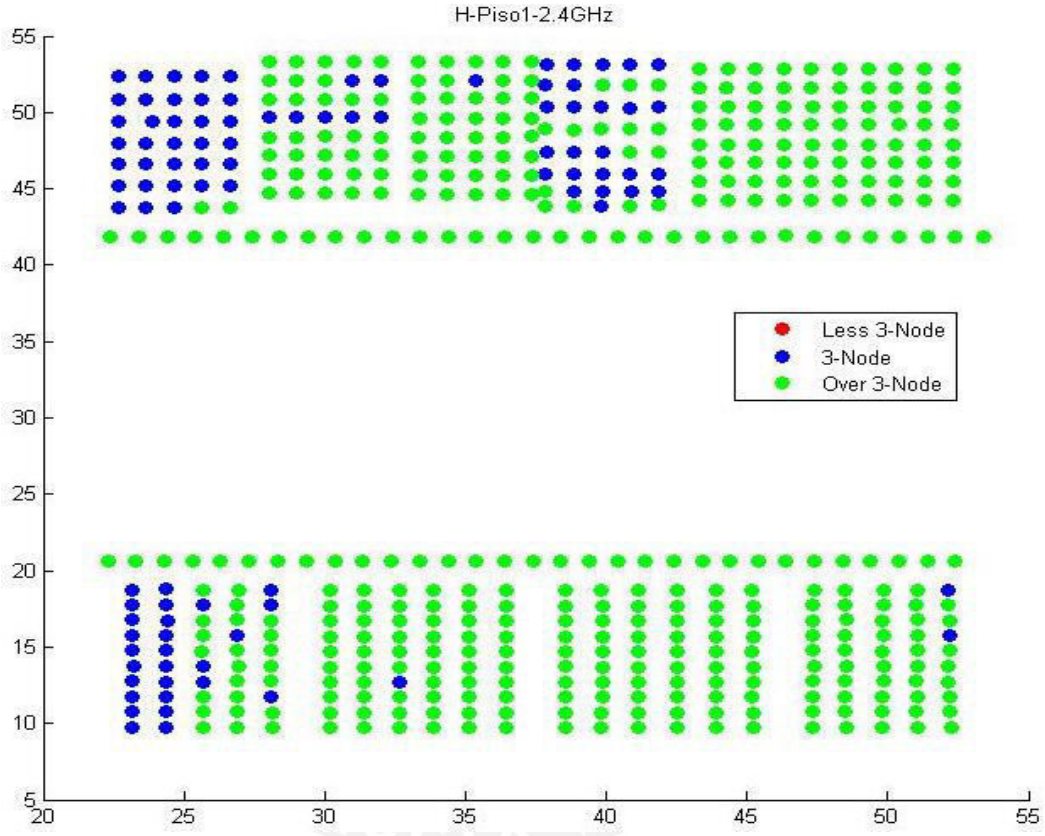


Figura 4-2: Nivel de Cobertura de puntos objetivos del primer piso (Aulas H101-102-103-104- 111-112-113-114) a 2.4GHz bajo número óptimo de módulos.
Fuente: Elaboración Propia

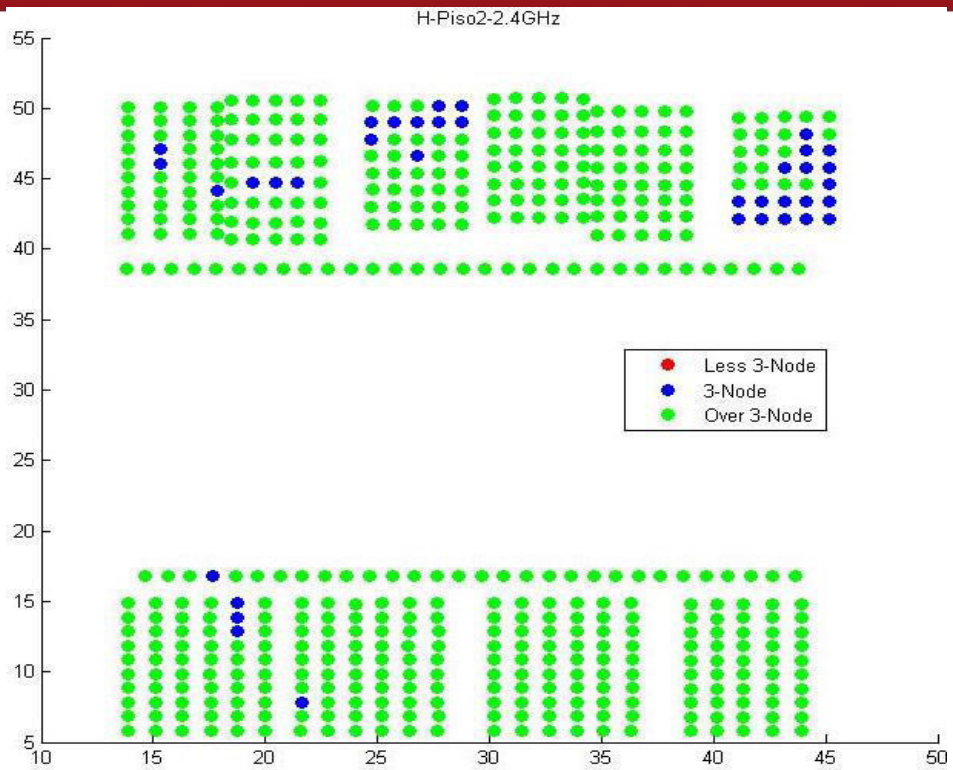


Figura 4-3: Nivel de Cobertura de puntos objetivos del segundo piso (Aulas H201-202-203-204-205-206-211-212-213-214) a 2.4GHz bajo número óptimo de módulos.
Fuente: Elaboración Propia

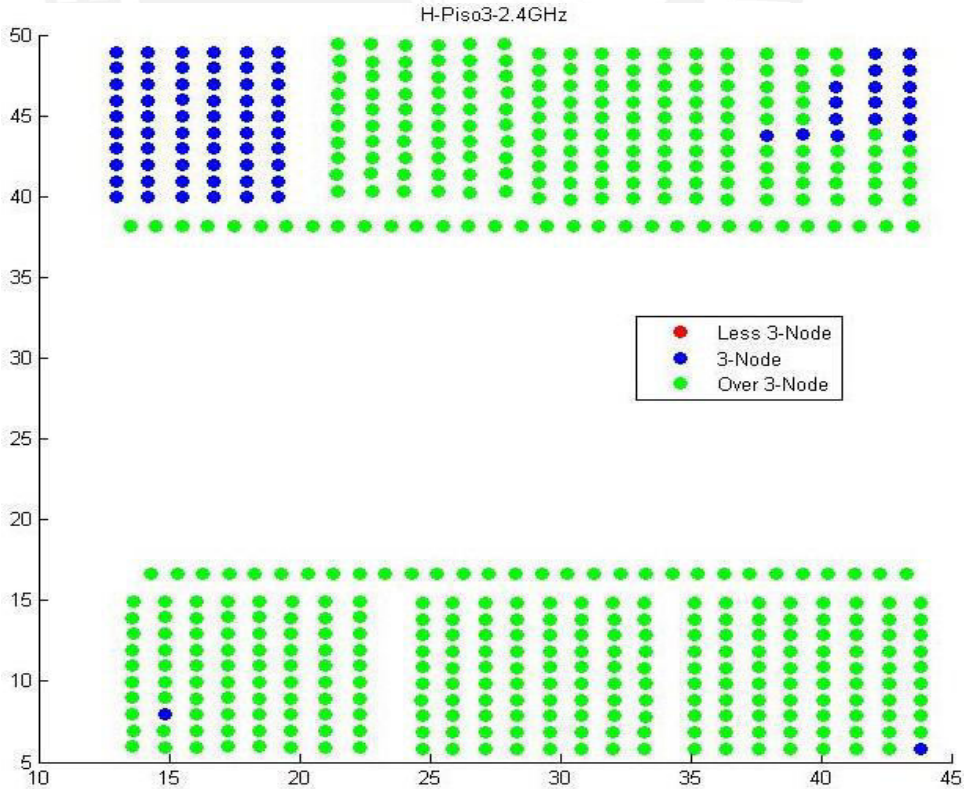


Figura 4-4: Nivel de Cobertura de puntos objetivos del tercer piso (Aulas H 301-302-303-304-311-312-313-314) a 2.4GHz bajo número óptimo de módulos.
Fuente: Elaboración Propia

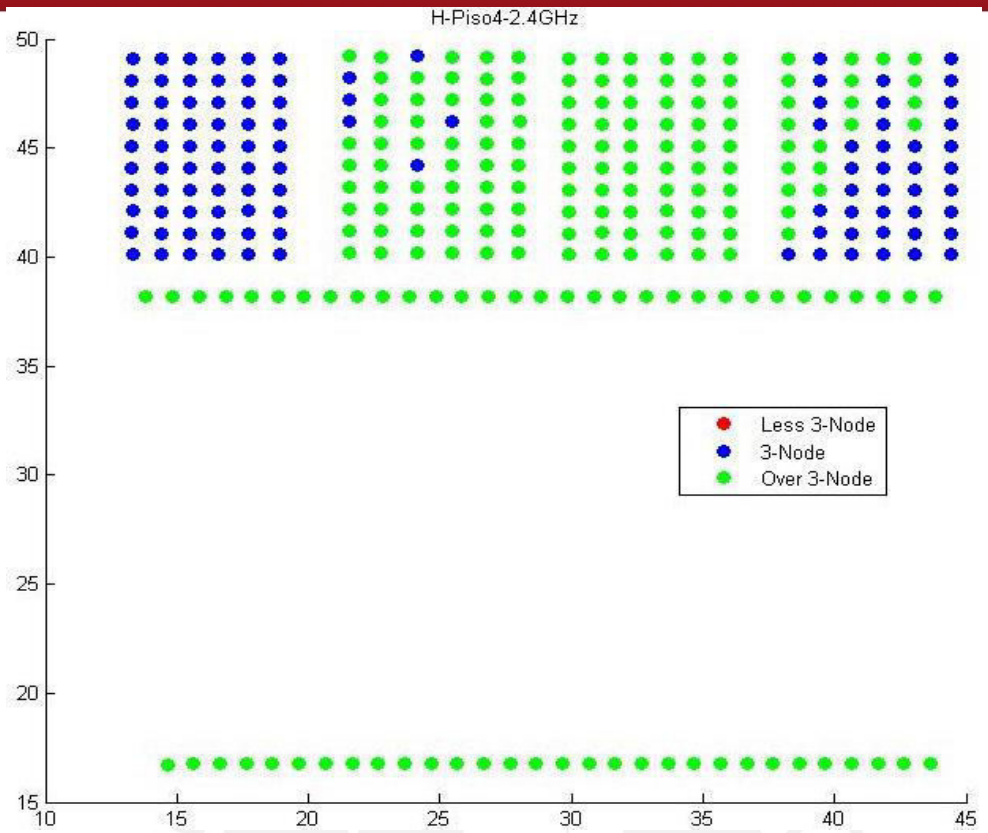


Figura 4-5: Nivel de Cobertura de puntos objetivos del cuarto piso (Aulas H 401-402-403-404) a 2.4GHz bajo número óptimo de módulos. Fuente: Elaboración Propia

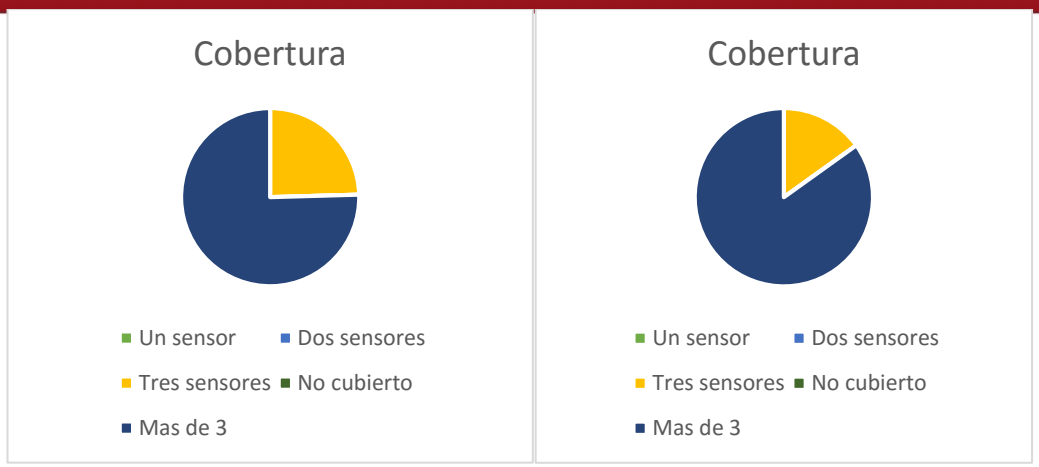
4.3.2. Distribución de los módulos para triple cobertura optima

A partir de las mediciones de la señal recibida por los APs y el modelo de triple cobertura, se comprueba que si es posible diseñar una red de sensores para la detección de Rogue APs dentro de la sección A y B del Pabellón H. Para lo cual se requirió de un total de 12 estaciones de detección para la banda de 2.4GHz y 14 estaciones para la banda de 5GHz, contra las 34 posibles instancias con las que cuenta este pabellón. Entonces, se obtiene que mediante la solución se requiere menos del 50% de los APs candidatos para cubrir una de estas dos bandas. Los módulos se encuentran distribuidos en la infraestructura del pabellón de la siguiente forma:

	2.4GHz		5GHz	
Piso	Cantidad de nodos	Ubicaciones de los nodos	Cantidad de nodos	Ubicaciones de los nodos
1	3	AP_H_104-1, aulpabh104, AP_H_113-1	4	AP_H_101-1, AP_H_102-1, AP_H_114-1, aulpabh104
2	3	AP_H_202-1, AP_H_206-1, AP_H_214-1	3	AP_H_204-1, AP_H_206-1, AP_H_214-1
3	3	AP_H_302-1, AP_H_312-1, AP_H_313-1	4	AP_H_301-1, AP_H_304-1, AP_H_311-1, AP_H_312-1
4	3	AP_H_403-1, aulpabh411, aulpabh412	3	AP_H_401-1, aulpabh411, aulpabh412

Tabla 4-5: Distribución y cantidad de sensores para el modelo óptimo de Triple Cobertura para 2.4 y 5GHz.
Fuente: Elaboración Propia

Así mismo, se puede apreciar que con este modelo no solo se logra que todos los puntos objetivos sean cubiertos por tres nodos, sino que también existe un considerable porcentaje de puntos que son cubiertos por más de tres AP. De esta forma, se obtiene que para la banda de 2.4GHz, se cuenta con un 16.81% de posiciones cubiertas por 3 sensores de detección, dejando un 83.19% del total de puntos objetivos cubiertos por más de 3 sensores. Mientras que en la banda de 5GHz, se tiene un 15.11% de posiciones que son cubiertas por 3 sensores, y un 84.89% de posiciones que son cubiertas por más de 3 puntos de detección.



(a) (b)

Figura 4-6: Porcentaje de puntos cubiertos por K-nodos en la solución óptima a a) 2.4GHz b) 5GHz.
Fuente: Elaboración Propia

4.4. Resultados de la heurística en el Pabellón H

Se utilizó el algoritmo de Greedy mencionado en los capítulos anteriores para poder alcanzar una solución al problema de decisión sobre la ubicación de los módulos de detección en tiempo polinómico. Para lo cual, el seudocódigo del algoritmo fue implementado en el software de Matlab, con la finalidad de procesar la vasta cantidad de información recolectada y lograr una solución cercana a la óptima. De igual forma que en el caso optima, se tomó en consideración la potencia y distribución de los APs para determinar la capacidad de detección que tendría cada módulo WSSI de ser instalado con dichos APs.

4.4.1. Comparación de instancias del Algoritmo de Greedy

Posteriormente a la aplicación de la heurística de greedy, se procedió a comparar ambos modelos de búsqueda local, tanto el modelo establecido como el modelo propuesto. En este sentido se obtuvo la siguiente tabla de comparación y tiempo de ejecución entre ambas lógicas respecto a la cantidad de APs obtenidos en la solución.

Modelo de Búsqueda	Banda	Resultado	Tiempo(ms)
Greedy Step	2.4GHz	15	41.6
	5 GHz	16	54.2
	Dual	17	78
Local Search	2.4GHz	14	170.0
	5 GHz	15	290.8
	Dual	16	175.6
Steered Local Search	2.4GHz	13	766.1
	5 GHz	15	587.8
	Dual	15	1383.4

Tabla 4-6: Tabla de Comparación entre los distintos métodos de optimización para la búsqueda local.

Fuente: Elaboración Propia

De la tabla anterior, se puede observar que solo la utilización de la fase de Greedy como parte de la heurística no es suficiente para poder obtener una solución razonable. En este sentido, se puede aprecia que la utilización de la búsqueda local mejora la heurística utilizada al reducir la cantidad de módulos WSSI necesarios en los APs para la solución en cualquiera de las bandas utilizadas. Debido a que podemos notar una reducción en el resultado obtenido que varía entre 1 y 2 módulos. Por lo tanto, podemos decir que la utilización de estos algoritmos permite obtener una solución más cercana a la óptima. En segundo lugar, se obtuvo que la solución obtenida mediante la búsqueda guiada (Steered Local Search) resulta más efectiva al brindar una solución que requiere de una menor cantidad de módulos. Este efecto se debe a las condiciones del sistema que requieren que cada punto sea cubierto por tres módulos, por lo cual la solución obtenida al utilizar la búsqueda normal no logra ser mejorada en un mayor grado. Por otro lado, se puede observar que utilizar el algoritmo de búsqueda requiere un mayor tiempo de solución. En esta instancia de pruebas, se obtuvo que el tiempo de ejecución del local search normal es menor que el guiado. Esto es principalmente causado debido a que este algoritmo es capaz de encontrar una solución mejorada durante una temprana instancia de ejecución. Además, este incremento en el tiempo de ejecución es ocasionado debido a que le Maltab no es suficientemente eficiente en la ejecución de bucles (for loops), lo cual podría ser revertido al implementar la heurística en código C. Finalmente, se decidió utilizar la búsqueda guiada en conjunto con la heurística de Greedy como referencia para poder obtener la solución final de la heurística, pese a que existe un incremento en el tiempo de ejecución.

4.4.2. Resultados del Algoritmo de Greedy

Las siguientes figuras, de la figura 4-7 a la 4-10, representan la relación de cantidad de módulos que tendrían la capacidad de detectar un Rogue AP en las diversas posiciones geográfica representadas por puntos en el plano.

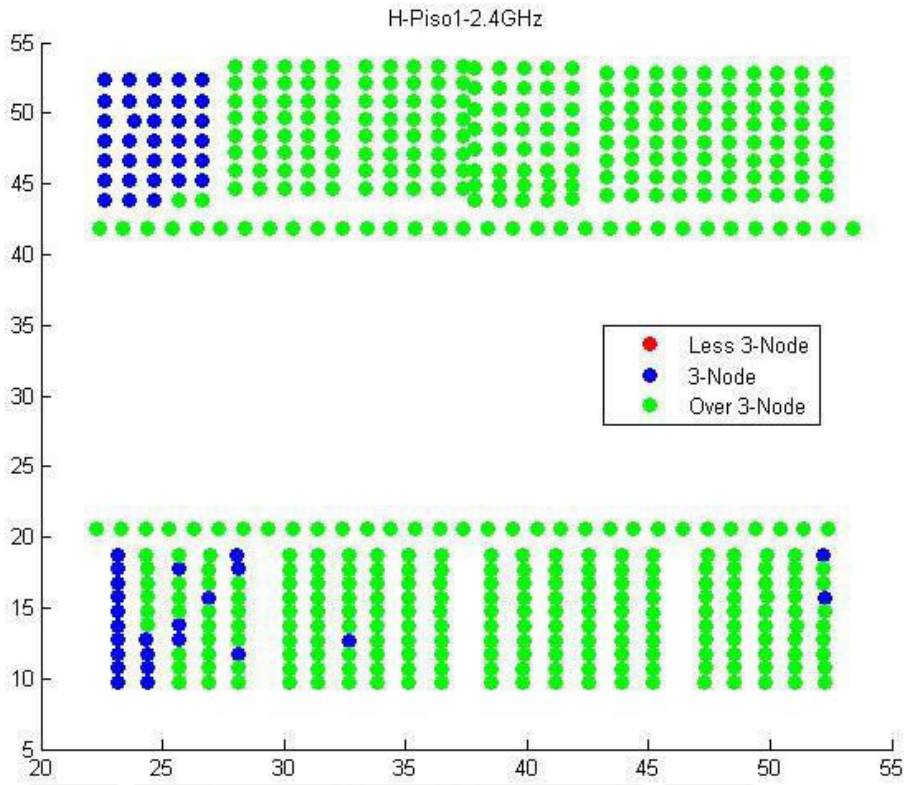


Figura 4-7: Nivel de Cobertura de puntos objetivos del primer piso (Aulas H101-102-103-104- 111-112-113-114) a 2.4GHz.
Fuente: Elaboración Propia

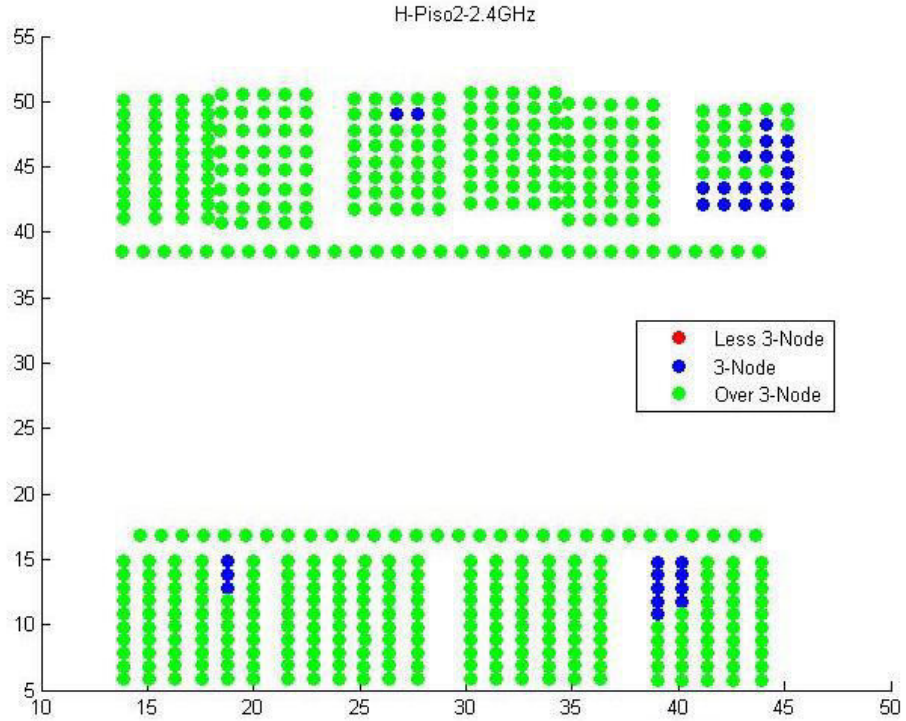


Figura 4-8: Nivel de Cobertura de puntos objetivos del segundo piso (Aulas H201-202-203-204-205-206-211-212-213-214) a 2.4GHz.
Fuente: Elaboración Propia

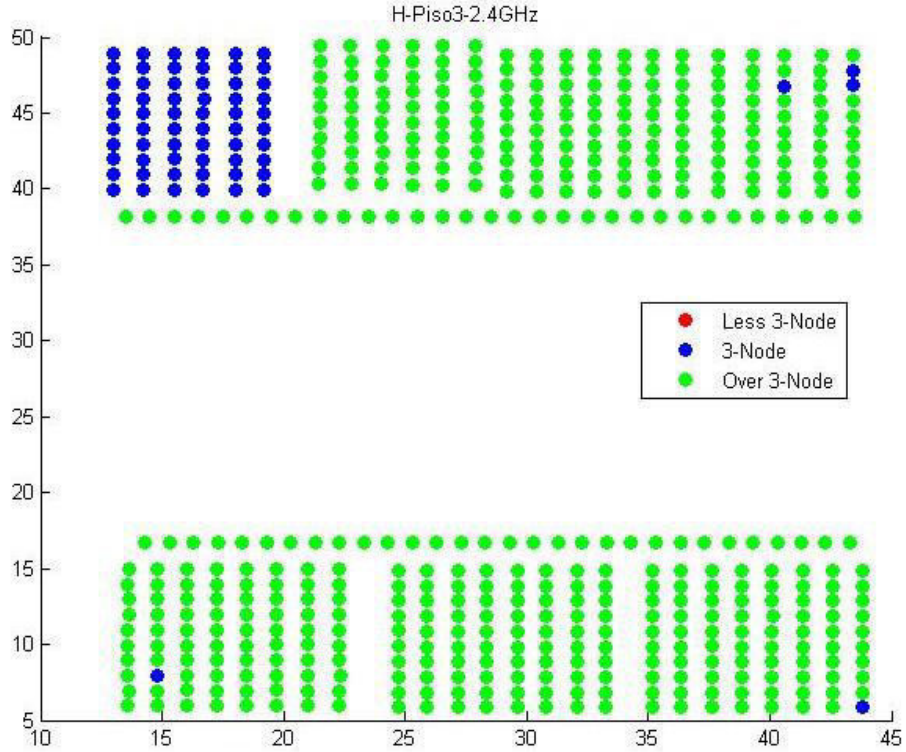


Figura 4-9: Nivel de Cobertura de puntos objetivos del tercer piso (Aulas H301-302-303-304-311-312-313-314) a 2.4GHz.
Fuente: Elaboración Propia

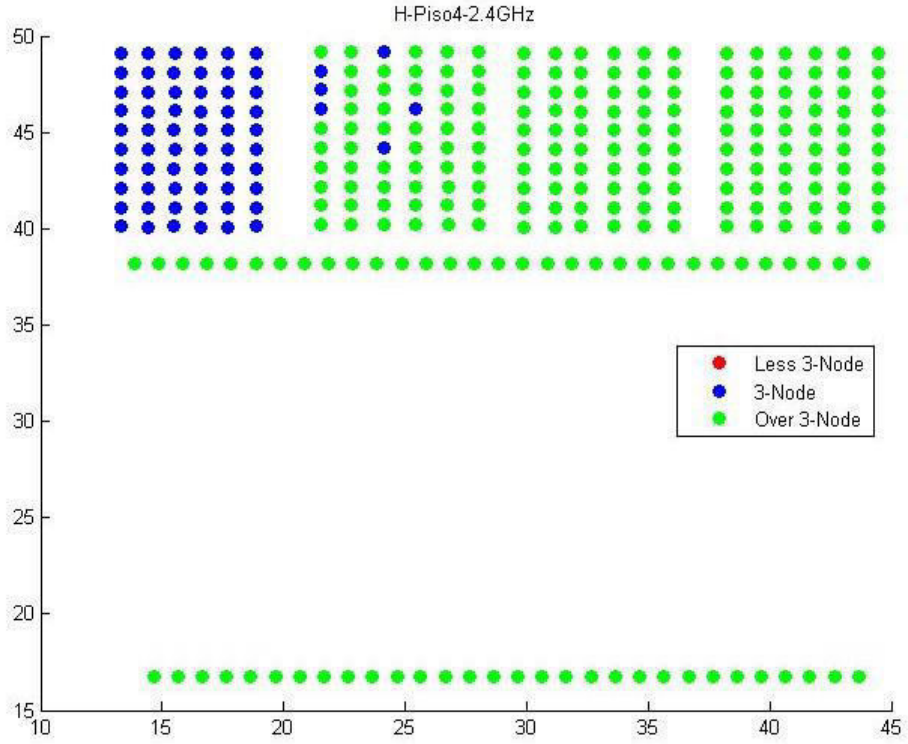


Figura 4-10: Nivel de Cobertura de puntos objetivos del cuarto piso (Aulas H401-402-403-404) a 2.4GHz.
Fuente: Elaboración Propia

4.4.3. Distribución de los módulos en el Pabellón H para triple cobertura según el algoritmo Greedy.

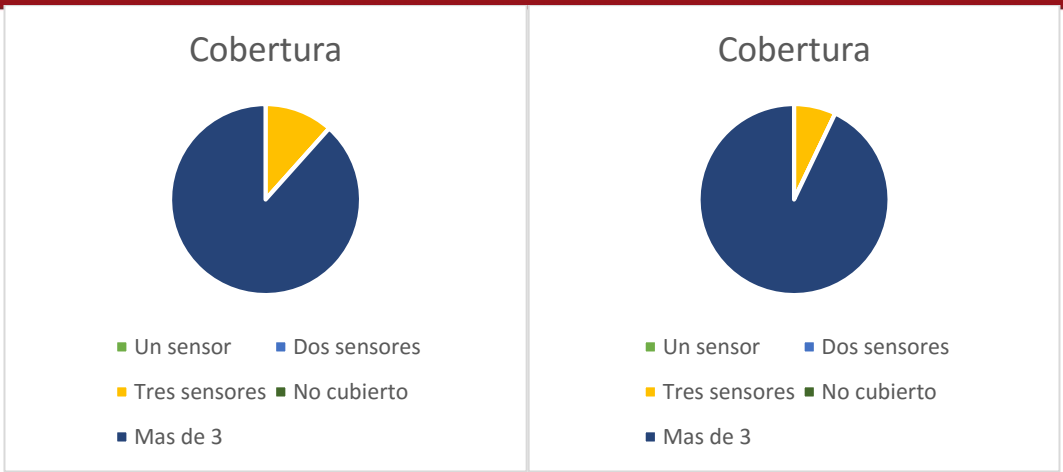
A partir de las mediciones de la señal recibida por los APs y la heurística basada en greedy, se comprueba que es posible diseñar una red de sensores para la detección de Rogue APs para los ambientes descritos del Pabellón H. En este caso, se requiere de un total de 15 módulos de detección WSSI para la banda de 2.4GHz y para la banda de 5GHz, las cuales se encuentra distribuida en la infraestructura del pabellón de la siguiente forma:

	2.4GHz		5GHz	
Piso	Cantidad de nodos	Ubicaciones de los nodos	Cantidad de nodos	Ubicaciones de los nodos
1	4	AP_H_101-1, AP_H_102-1, aulpabh104, aulpabh112	3	AP_H_102-1, aulpabh104, aulpabh112,
2	2	AP_H_204-1, AP_H_214-1	4	AP_H_201-1, AP_H_206-1, AP_H_213-1, AP_H_214-1
3	4	AP_H_303-1, AP_H_304-1, AP_H_312-1, AP_H_313-1	5	AP_H_301-1, AP_H_303-1, AP_H_304-1, AP_H_312-1, AP_H_313-1
4	3	AP_H_402-1, aulpabh411, aulpabh412	3	AP_H_403-1, aulpabh411, aulpabh412

Tabla 4-7: Distribución y cantidad de sensores para la heurística en las bandas de 2.4GHz y 5GHz

Fuente: Elaboración Propia

Igualmente, se puede apreciar que mediante el uso de la heurística no solo se logra que todos los puntos objetivos sean cubiertos por tres módulos, sino que también existe un considerable porcentaje de puntos que son cubiertos por más de un AP. Sin embargo, se requiere de una mayor cantidad de módulos con APs en comparación con los resultados anteriores. De esta forma, se obtiene que para la banda de 2.4GHz, se cuenta con un 11.61% de posiciones cubiertas por 3 sensores de detección, dejando un 88.3*% del total de puntos objetivos cubiertos por más de 3 sensores. Mientras que en la banda de 5GHz, se tiene un 7.10% de posiciones que son cubiertas por 3 sensores, y un 92.90% de posiciones que son cubiertas por más de 3 puntos de detección.



(a) (b)

Figura 4-11: Porcentaje de puntos cubiertos por K-nodos mediante la heurística a a) 2.4GHz b) 5GHz

Fuente: Elaboración Propia

4.5. Comparación entre la heurística y el modelo óptimo en el Pabellón H

Se puede observar que existe un comportamiento distinto entre la solución obtenida mediante el modelo lineal óptimo, modelado a partir del problema de máxima cobertura de la sección 2.3 como un problema MILP, y la heurística de greedy con búsqueda guiada. En una primera instancia, se puede observar que existe una discrepancia respecto a la cantidad de módulos necesarios para poder diseñar la red de detección considerando la información obtenida. Para la banda de 2.4GHz y 5GHz se tiene que mediante el modelo óptimo, se requiere una cantidad mínima de 12 y 14 nodos, mientras que en la heurística se obtiene una cantidad de 13 y 15 módulos. Por otro lado, se puede concluir que esta diferencia de módulos entre soluciones es relativamente pequeña, 1 módulo para la banda de 2.4GHz y 5GHz respectivamente. Sin embargo, sigue estando lejos del valor óptimo, debido a que estos valores representan un error del 2.94% con respecto a la cantidad total de nodos para el Pabellón H.

En las siguientes gráficas, se puede apreciar el grado de cobertura de todos los nodos conforme se incrementan la cantidad de APs, según las soluciones obtenidas para la banda de 2.4GHz y de 5GHz. De esta forma, se tiene que la línea roja corresponde al comportamiento obtenido de la solución mediante heurística, mientras que la línea de color azul corresponde a la solución óptima. El eje vertical representa

el porcentaje de los puntos objetivos que son cubiertos por al menos 3 nodos. En estas graficas se puede apreciar el comportamiento esperado de crecimiento del algoritmo basado en el algoritmo. Debido a que en esta se diseña para que seleccione con mayor prioridad aquellos APs que brindan una mayor ganancia de cobertura.

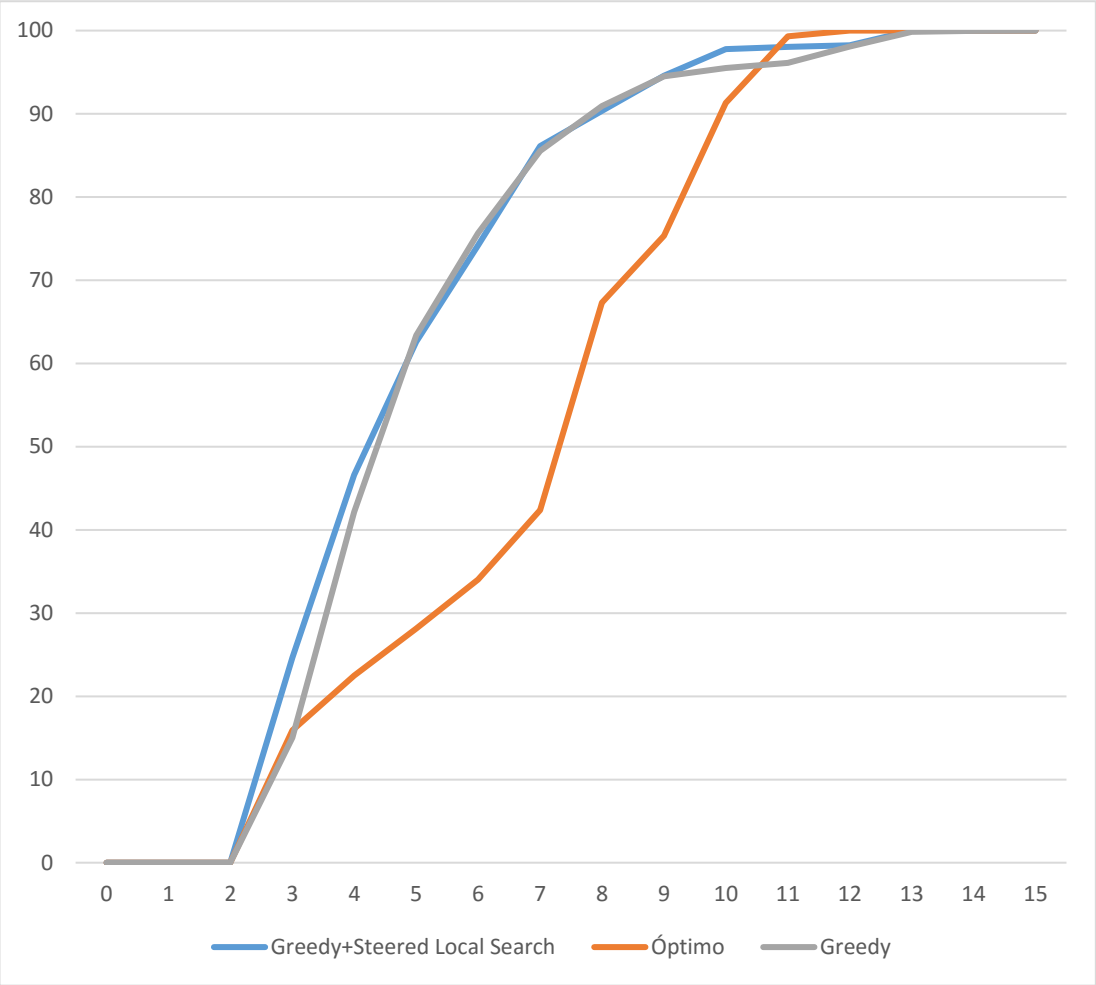


Figura 4-12: Relación de triple cobertura del Pabellón H para el modelo optima en la banda de 2.4GHz

Fuente: Elaboración Propia

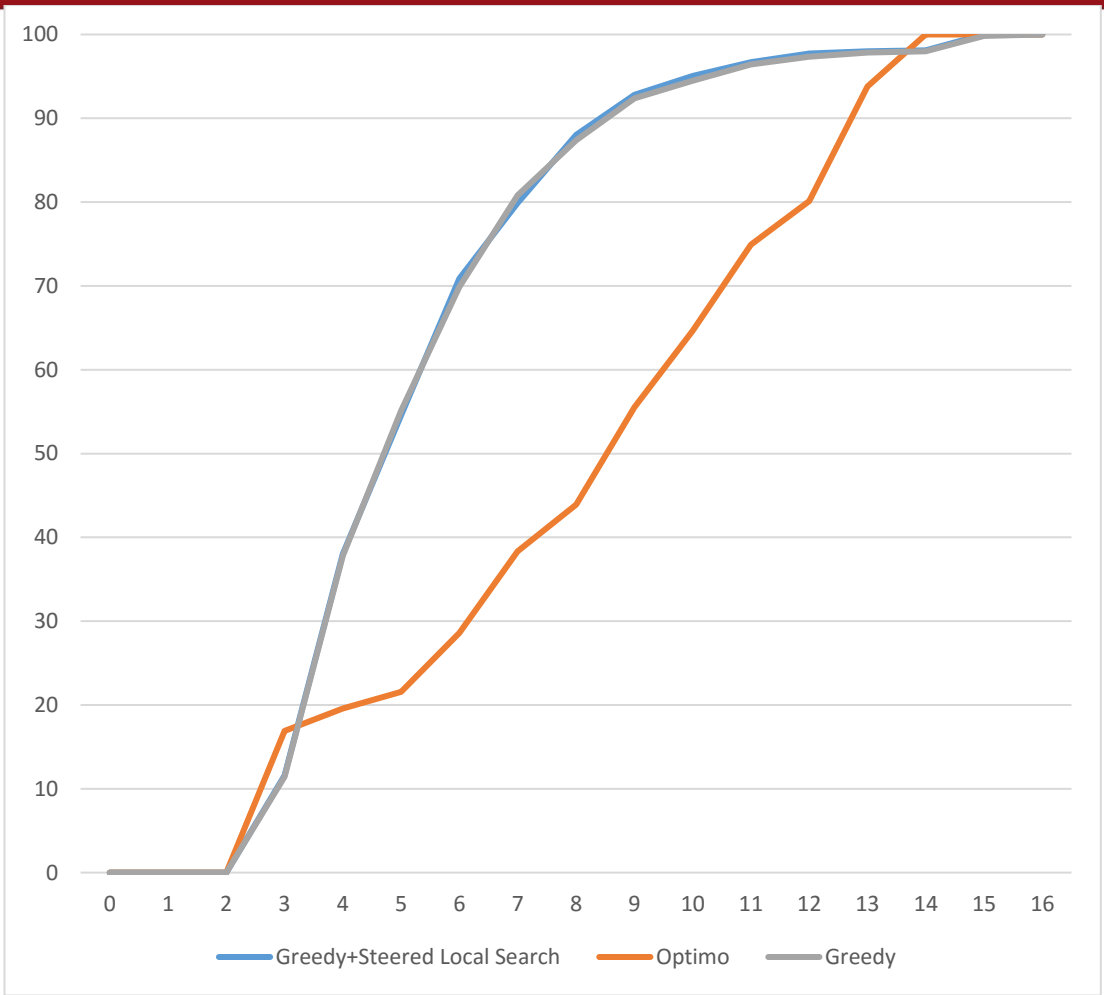


Figura 4-13: Relación de triple cobertura del Pabellón H para el modelo optimo en la banda de 5GHz
Fuente: Elaboración Propia

Por otro lado, en base a los resultados podemos que existe una diferencia en la cantidad de módulos necesarios cuando se analiza los resultados en grandes y pequeñas instancias. Para pequeñas instancias, se requiere de 22 y 24 nodos según el modelo óptimo para triple cobertura, mientras que en grandes instancias se requiere de 12 y 14 nodos para 2.4GHz y 5GHz. Es decir, se reduce en un 29.41% la cantidad de nodos respecto del total para grandes instancias. Asimismo, según la heurística, se tiene 23 y 25 módulos para instancias pequeñas contra 13 y 15 módulos en grandes instancias en sus respectivas bandas. Esto equivale a una reducción del 29.41% de la cantidad de módulos totales cuando se utilizan grandes instancias. De esta forma, se tiene que la solución en ambos casos tiene una reducción del 29.41%. No obstante, se tiene que a instancias pequeñas la cantidad de nodos obtenidos por medio de los modelos de optimización y la heurística es menor. En este caso, se tiene una diferencia de un módulo (2.94% del total de nodos

candidatos); mientras que en grandes instancias la diferencia incrementa, siendo de 2 y 3 módulos, 5.88% y 8.823% respecto del total cuando se utiliza la heurística greedy sin búsqueda local, pero se reduce a un único modulo al igual que en pequeñas instancias cuando se utiliza en conjunto con el algoritmo de búsqueda local guiada.

4.6. Resultados para el resto de Pabellones

Finalmente, en la siguiente tabla se presenta los resultados finales para el resto de los ambientes de interés para DIRINFO. En esta ocasión se muestra el resultado de los pabellones Z, Estudios Generales Ciencias, McGregor y Tinkuy. En la siguiente tabla, se muestra la cantidad de lugares candidatos y cantidad de puntos totales objetivos, en donde se tiene un total de:

Pabellón	Lugares candidatos	Puntos Objetivos
Estudios Generales Ciencias	40	4343
McGregor	36	2179
Pabellón H	34	1886
Pabellón Z	41	2882
Tinkuy	68	1478
Total	219	12768

Tabla 4-8: Cantidad de lugares candidatos y puntos objetivos por pabellón.

Fuente: Elaboración propia

Además, se muestran los resultados para la banda de 2.4GHz y 5GHz, y se agregan los resultados obtenidos al combinar las matrices de ambas banda como uno solo, banda dual. En la siguiente tabla, se muestra los resultados (cantidad de nodos) de cada pabellón utilizando ambos métodos y considerando las tres bandas y la densidad del resultado definido como el porcentaje de nodos requeridos para la solución respecto al total de candidatos en cada ambiente.

Pabellón	Banda	Algoritmo	Resultado	Densidad	Tiempo
Estudios Generales Ciencias	2.4	Optimo	16	0.4	0.2242
	5	Optimo	20	0.5	0.0991
	Dual	Optimo	20	0.5	0.1406
	2.4	Heurística	16	0.4	1.0899
	5	Heurística	20	0.525	1.6353
	Dual	Heurística	20	0.525	2.3632
McGregor	2.4	Optimo	5	0.139	0.4773
	5	Optimo	6	0.167	0.2613
	Dual	Optimo	6	0.167	0.0479
	2.4	Heurística	6	0.167	0.2077
	5	Heurística	6	0.167	0.1359
	Dual	Heurística	6	0.167	0.2295
Pabellón H	2.4	Optimo	12	0.353	0.0562
	5	Optimo	14	0.412	0.0752
	Dual	Optimo	14	0.412	0.0416
	2.4	Heurística	13	0.44	0.7661
	5	Heurística	15	0.47	0.5878
	Dual	Heurística	15	0.5	1.3834
Pabellón Z	2.4	Optimo	15	0.366	0.2554
	5	Optimo	19	0.463	0.1312
	Dual	Optimo	19	0.463	0.3511
	2.4	Heurística	16	0.439	1.5142
	5	Heurística	20	0.536	1.7519
	Dual	Heurística	20	0.536	1.5892
Tinkuy	2.4	Optimo	12	0.1765	0.027
	5	Optimo	19	0.279	0.053
	Dual	Optimo	22	0.32	0.1239
	2.4	Heurística	12	0.1765	1.6499
	5	Heurística	19	0.279	1.621
	Dual	Heurística	22	0.32	3.9038

Tabla 4-9: Resultados Finales de los ambientes de interés.

Fuente: Elaboración propia

En cuanto a los tiempos de cómputo, se puede apreciar que es posible hallar la solución óptima y la solución mediante el uso de la heurística en un tiempo computacional aceptable, del orden de los milisegundos. En otras palabras, se realiza en un tiempo razonable. Esto nos permite concluir que el código utilizado para la búsqueda de la solución óptima se ejecuta de manera rápida este tamaño de instancias. Sin embargo, se debe tener la siguiente consideración para el caso de Tinkuy, debido a que en este ambiente no se tiene una cobertura completa para la banda de 5GHz. En este sentido, se tiene que aproximadamente el 9.2% de los puntos objetivos no se encuentran cubiertos por ningún modulo. Por tal motivo, se debe tener presente que la solución encontrada en Tinkuy no incluye dichos puntos para encontrar la solución en ambas metodologías.

Por otro lado, podemos apreciar que no existe una gran diferencia en el tiempo de ejecución de la heurística y de la solución óptima. Así mismo, se puede concluir que la diferencia de nodos para la solución dual es menor en comparación cuando solo se analiza una única banda, por lo tanto, esta solución de banda dual mediante heurística tiene una mayor correlación con la solución óptima. Por lo tanto, se obtiene la siguiente cantidad de nodos del total de lugares candidatos para la triple cobertura de todos los pabellones en la tabla 4-9. A partir de esta podemos observar una densidad que abarca desde el 27% hasta 37%, por lo tanto, tomando el caso de la banda dual, podemos decir que se requiere de un 37%. No obstante, este porcentaje puede incrementarse debido a que como se mencionó anteriormente no existe una cobertura total de todos los objetivos en la banda de 5GHz en el caso de Tinkuy.

Banda	Cantidad Nodos	Densidad promedio
2.4GHz	60	0.274
5 GHz	78	0.3562
Dual	81	0.3699

Tabla 4-10: Tabla resumen de la cantidad de módulos totales por banda.

Fuente: Elaboración propia

Se observa que tiene un comportamiento esperado respecto a lo obtenido para instancias pequeñas, tal que se requiere de una mayor cantidad de nodos para poder cubrir la banda de 5GHz. De igual forma, se observa que existe un margen de error entre la solución óptima y mediante heurística, la cual en el mejor caso es cero, como

en el McGregor, pero puede llegar a diferir hasta en tres nodos. Finalmente, en el siguiente grafico se observa la relación puntos objetivos por cantidad de módulos para la solución óptima, tal que los puntos objetivos van incrementando en relación a la cantidad de puntos de los ambientes en el orden establecido de la tabla anterior. La línea azul representa al comportamiento para la banda de 2.4GHz, mientras que la línea naranja y gris representa a la banda de 5GHz y la solución dual. De esta forma, se puede observar que la solución para estos dos últimos es igual en cantidad de nodos, a excepción de cuando se obtiene la solución con Tinkuy, lo cual se apreciar ya que las líneas se superponen, y que existe una diferencia de 11 nodos entre la solución de la banda 2.4GHz y la banda de 5GHz, y una diferencia de 3 nodos entre la banda dual y la de 5GHz.

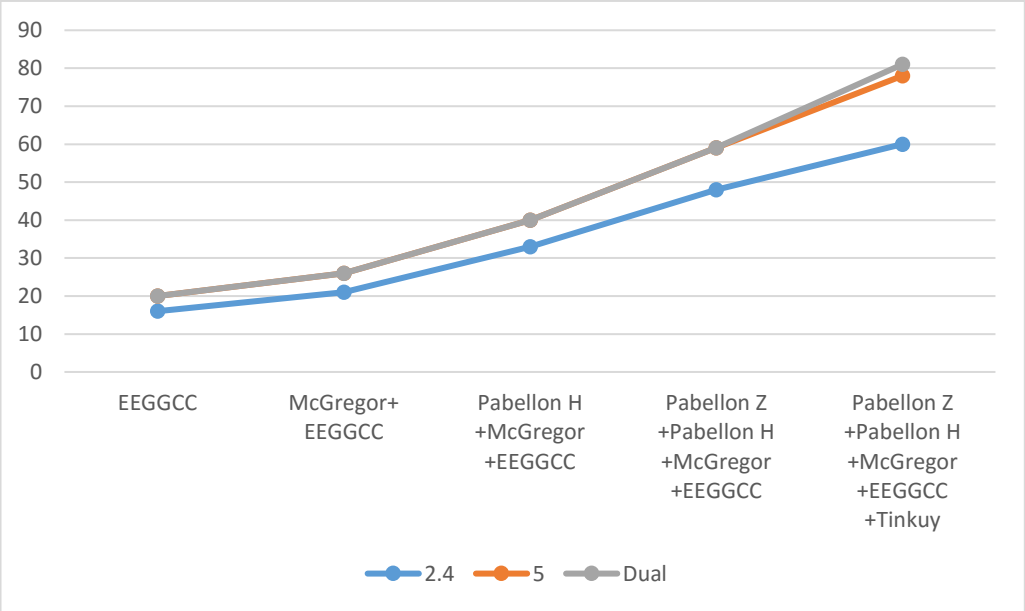


Figura 4-14: Crecimiento de módulos según cobertura de puntos objetivos.

Fuente: Elaboración propia

4.7. Comparación entre la heurística y el modelo óptimo para el resto de Pabellones

A continuación se realizara una comparación entre la solución óptima (O) y la solución obtenido por medio de las diversas heurísticas que se han implementado. En este sentido, se realizara un comparación entre la solución obtenida por media del sola de la heurística de greedy o codiciosa (G), la heurística codiciosa en conjunto con la heurística de búsqueda local (GL) y la heurística codiciosa con la búsqueda

local guiada (GSL). Esta comparación se realiza únicamente para la banda dual, ya que como se ha mencionado anteriormente la solución final considera la cobertura tanto para la banda de 2.4GHz como para la banda de 5GHz. En la siguiente tabla se muestran la cantidad de módulos WSSI requeridos por pabellón de acuerdo a cada uno de los modelos así como el tiempo de ejecución respectivo en milisegundos:

	Resultados				Tiempo			
	G	GL	GSL	O	G	GL	GSL	O
EE.GG.CC	21	20	20	20	141.6	433.5	2363.2	140.6
McGregor	6	6	6	6	504.1	298.6	229.5	47.9
Pabellon H	17	16	15	14	78	175.6	1383.4	41.6
Pabellon Z	22	20	20	19	351.1	984.6	1589.2	351.1
Tinkuy	22	22	22	22	240.9	3675.8	3903.8	123.9
Total	88	84	83	81	1314.7	5568.1	9469.1	705.1

Tabla 4-11: Tabla comparación entre la solución óptima y las heurísticas para todos los pabellones en la banda dual.
Fuente: Elaboración propia

Entonces, en la tabla 4-11 se lograr ver con mayor detalle los resultados obtenidos por medio de las distintas heurísticas implementadas en comparación con los resultados obtenidos en la solución óptima. De esta forma podemos apreciar que en la mayoría de los escenarios existe una diferencia en la cantidad de módulos y el tiempo de ejecución entre los distintos modelos heurísticos y óptimos. Tal que se obtiene que la solución heurística únicamente con la fase de greedy tiene el menor tiempo de ejecución entre las heurísticas, lo cual la coloca como el modelo con un tiempo más cercano al de la solución óptima, pese a que requiere una mayor cantidad de módulos. Por otro lado, se tiene que la solución heurística con búsqueda guiada requiere el mayor tiempo de ejecución, no obstante, esta solución requiere el menor número de módulos de todas las heurísticas y tiene el mayor parentesco con la solución optima

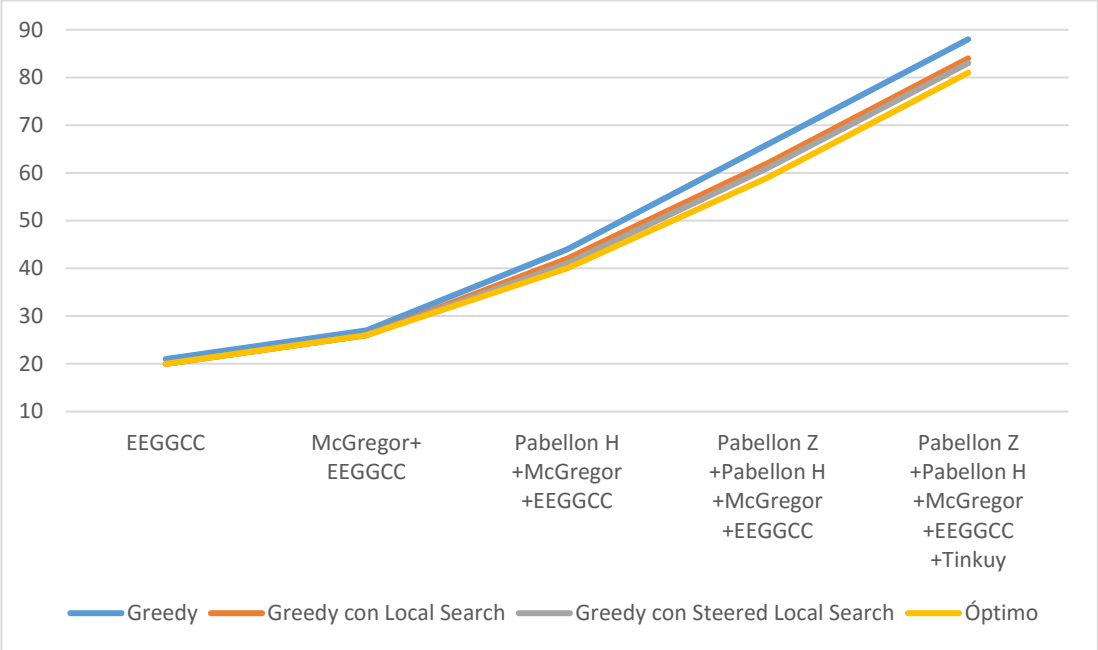


Figura 4-15: Relación del crecimiento de módulos según cobertura de puntos objetivos para las heurísticas y el modelo óptimo.
Fuente: Elaboración propia

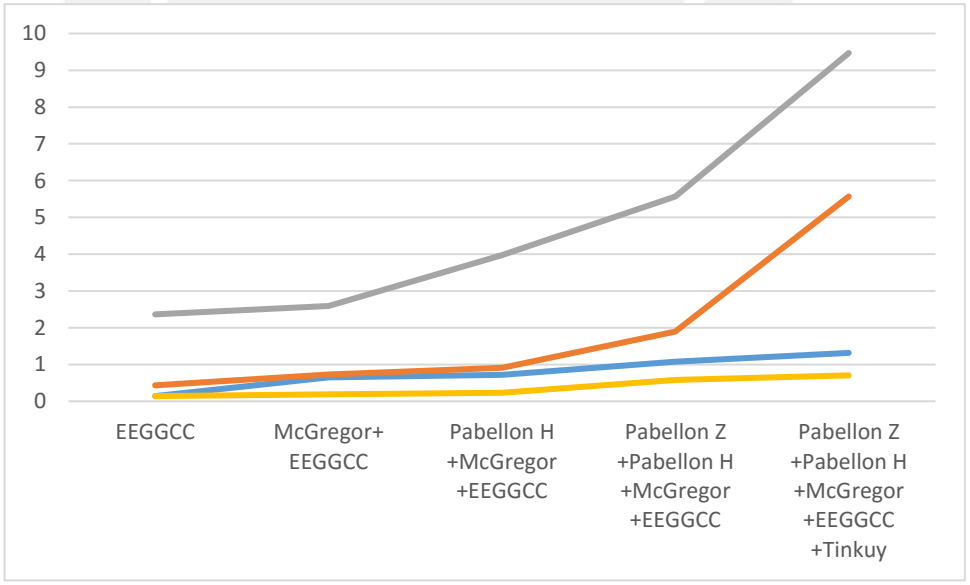


Figura 4-16: Relación del tiempo de ejecución según cobertura de puntos objetivos para las heurísticas y el modelo óptimo.
Fuente: Elaboración propia

Finalmente, podemos apreciar que la solución obtenida por medio de la fase de greedy en conjunto con la búsqueda local es la solución más cercana a la solución óptima, puesto que solo hay una diferencia de 2 módulos. No obstante, como se puede apreciar en la figura 4-16, la principal desventaja de este método es el tiempo, ya que como se observa existe una relación aproximada 1 a 10 entre los tiempos de ejecución de los mismos, lo cual puede tener un mayor efecto a instancias mayores.

4.8. Comparación entre los resultados 2D y 3D para el resto de Pabellones

En la siguiente sección, se describirá la diferencia entre los resultados obtenidos mediante el modelamiento 2D, pequeñas instancias, versus los resultados obtenidos para los modelos 3D del problema, grandes instancias. En la siguiente tabla, se muestran los resultados obtenidos en el modelo óptimo para la banda dual cuando se considera un modelamiento 2D, igual al cual se obtiene el software Cisco Prime que posee la PUCP.

Pabellón	Lugares Candidatos	Resultados	Densidad
Estudios Generales Ciencias	40	33	0.825
McGregor	36	22	0.6111
Pabellón H	34	24	0.7059
Pabellón Z	41	32	0.7825
Tinkuy	68	35	0.5147

Tabla 4-12: Tabla resumen de los resultados 2D de la solución óptima para el resto de los pabellones en la banda dual.
Fuente: Elaboración propia

En la tabla 4-12, se puede observar que para los resultados de modelos 2D se requiere una densidad que varía entre el 50% hasta el 82.5%. De esta forma, se puede apreciar que la solución con un modelo 2D no es eficiente debido a que se mencionó en secciones anteriores, la solución a grandes instancias, o modelo 3D, requiere una densidad menos al 40%. En la siguiente gráfica, se describirá la diferencia entre los resultados obtenidos mediante el modelo 2D y 3D:

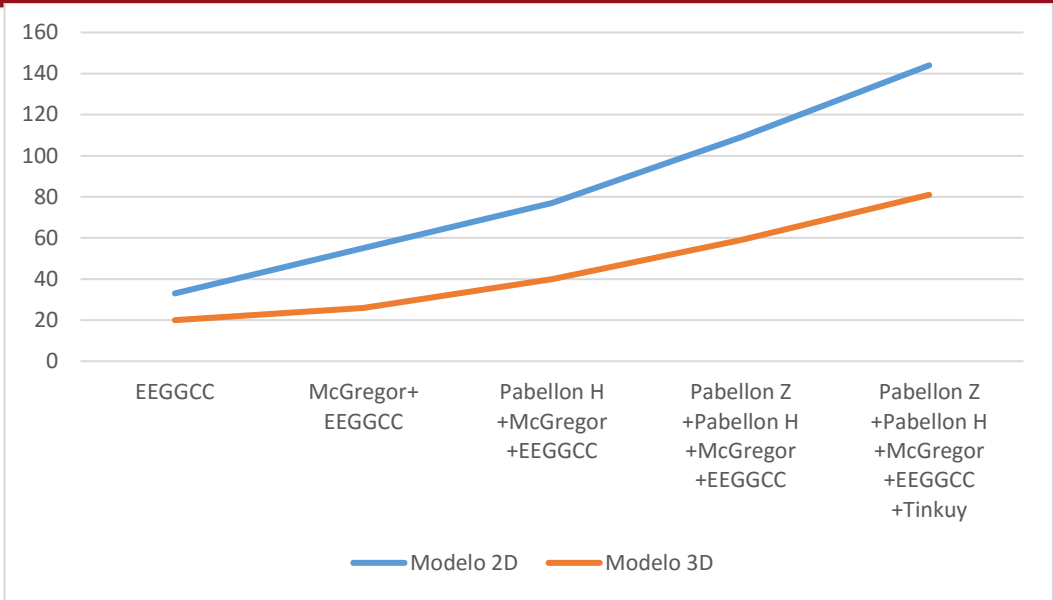


Figura 4-17: Relación del crecimiento según cobertura de puntos objetivos del modelo óptimo en 2D y 3D para la banda dual.
Fuente: Elaboración propia

Entonces, como se puede observar en la figura 4-17, se requiere un total de 146 módulos para poder brindar cobertura a los 5 pabellones mediante el modelamiento 2D, lo cual representa el 66.7% de todos los sitios candidatos. Asimismo, se logra ver que existe una diferencia de 65 módulos entre la solución 2D y 3D, lo cual quiere decir que existe un ahorro del 29.68% respecto a la cantidad de sitios candidatos cuando se utiliza el modelamiento 3D, grandes instancias, en vez del modelamiento 2D, pequeñas instancias. En este sentido, se tiene que existe un ahorro de 13, 16, 10, 13 y 13 módulos para EE.GG.CC, McGregor, Pabellón H, Pabellón Z y Tinkuy respectivamente. De otra forma, se tiene un ahorro del 32.5%, 44.4%, 29.41%, 31.7% y 19.1% respectivamente para los ambientes previamente mencionados; por lo tanto, se tiene un ahorro que va desde el rango de 19% hasta el 45%.

Conclusiones y recomendaciones

Conclusiones

- Se logró cumplir el objetivo principal de la tesis al usar la teoría de NP-Complete para diseñar un sistema de detección de Rogue AP en la red Wi-Fi del campus de la PUCP, pues, en conjunto con la mediciones de la potencia recibida, se comprobó que si es posible diseñar este sistema en base a la infraestructura actual

- El modelo de triple cobertura es apropiado para aplicaciones en donde es de vital importancia la detección de los Rogue APs a diversas horas, pero no se cuenta un gran capital de inversión para implementar sensores dedicados, ya que, se minimiza la cantidad de puntos nodos necesarios para poder cubrir ambas bandas del espectro que se emplea en Wi-Fi. Así mismo, este modelo es de gran utilidad debido a que puede utilizarse en un modelo de detección hibrida, lo cual reduce sus costo de implementación, pero afecta directamente al desempeño de la red inalámbrica.

- Se comprobó que para el Pabellón H es posible brindar un grado de cobertura mayor al objetivo lo cual es crucial si se planea implementar un servicio de localización de Rogue APS por medio de triangulación de señal en el futuro, ya que, se comprobó que todos los pisos de los ambientes puede ser totalmente cubierto por al menos tres nodos, la cual es la condición para mejorar la precisión que poseen estos tipos de sistema.

- Un criterio importante a considerar para el diseño de una red de detección de Rogue AP funcional es que los niveles de señal recibida en los nodos de detección sean lo suficientemente fuertes para detectar las tramas beacon de los Rogue AP. De esta manera, se puede obtener un mayor margen de detección de intrusos.

- Mediante el uso de modelos de optimización se buscaba diseñar una red que permita la detección y la localización en cualquier ubicación de Rogue APs. Por lo cual se comprobó que es posible diseñar una red que permita detectar y sobretodo localizar la presencia de Rogue AP para más de un 80% de posible posiciones dentro del Pabellón H con una precisión mayor a la esperada.

- Mediante el modelo de K-Cobertura con un factor de cobertura igual a 3, se logró determinar que es posible dar una cobertura de detección de Rouge APs utilizando aproximadamente el 50 por ciento de APs disponibles con módulos WSSI.

- **Recomendaciones**
  - Se recomienda la utilización de la solución óptima con banda dual para la implementación física del diseño de la red propuesta de menor CAPEX. Debido a que brinda un grado confiable de cobertura al contar con APs transmitiendo a máximo poder y debido a que la solución óptima pudo ser hallada en un tiempo aceptable de procesamiento.

  - Los modelos utilizados para determinar la red de detección en la presente tesis puede ser utilizados como base para el desarrollo de nuevos modelos de cobertura de mayor orden, para lo cual se recomienda diseñar dichos modelos con un mayor grado de restricción.

  - Los modelos utilizados puede ser utilizados no solo para el diseño de una red de sensores de amenazas inalámbricas, sino también para planeamiento y despliegue de APs dentro de una institución o campus y el despliegue de redes de sensores inalámbricos interconectadas.

Bibliografía

[1] Ali, Q.I. y S. Iazim. "Design and implementation of an embedded intrusion detection system for wireless applications". Information Security 2012, IET, volumen 6, número 3, pp.171-182.

[2] Branch, J.W.; Petroni, N.L., Jr.; van Doorn, L.; Safford, D., "Autonomic 802.11 wireless LAN security auditing," Security & Privacy, IEEE, vol.2, no.3, pp.56, 65, May-June 2004

[3] Barrenechea Zavala, Taylor Iván. “Diseño de una red LAN Inalámbrica para una empresa de Lima. Tesis para optar el Título de Ingeniero Electrónico”. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería.

[4] Chen, Guanlin, Hui Yao y Zebing Wang. "Research of wireless intrusion prevention systems based on plan recognition and honeypot," Wireless Communications & Signal Processing. WCSP 2009, pp.1, 5, 13-15.

[5] Lawton, George, "Fighting Intrusions into Wireless Networks," Computer, vol.43, no.5, pp.12, 15, May 2010.

[6] Li, Deying and Cao, Jiannong and Liu, Dongsheng and Yu, Ying and Sun, Hui. “Algorithms for the m-Coverage Problem and k-Connected m-Coverage Problem in Wireless Sensor Networks”. Network and Parallel Computing, vol.4672, pp. 250-259, 2007

[7] Neil, Reid y Ron Seide. “Manual de Redes Inalámbricas 802.11 (Wi-Fi)”. 2da Edición. México: McGraw-Hill, 2005.

[8] Peng, Xiao qiang, Cheng Zhang y Dian Gang Wang. "The Intrusion Detection System design in WLAN based on rogue AP". Computer Engineering and Technology (ICCET), 2nd International Conference, volumen 3, pp.vol.3-432, vol3-436, 16-18, 2010.

[9] Pakstas, A., S. Salekzamankhani y B. Virdee. “Fighting Intrusions in Wireless LANs: A Need for the Reference Model". Internet, 2006 2nd IEEE/IFIP International Conference in Central Asia, vol., no., pp.1, 8, 19-21, 2006.

[10] Scarfone, Karen A. y Peter M. Mell. “Guide to Intrusion Detection and Prevention Systems (IDPS). NIST 2009.

[11] Tao, Zhiqui y A.B. Ruighaver. "Wireless Intrusion Detection: Not as easy as traditional network intrusion detection". TENCON 2005 2005 IEEE Region 10, pp.1-5, 21-24.

[12] Vartak, A., S. Ahmad y K.N. Gopinath. "An Experimental Evaluation of Over-The-Air (OTA) Wireless Intrusion Prevention Techniques". Communication Systems Software and Middleware. COMSWARE 2007, pp.1, 7-12.

[13] Church, Richard and ReVelle, Charles. “The maximal covering location problem”. Papers of the Regional Science Association, vol.32, pp. 101-118, 1974.

[14] Zongheng Zhou; Das, S.; Gupta, H., "Connected K-coverage problem in sensor networks," Computer Communications and Networks, 2004. ICCCN 2004. Proceedings. 13th International Conference on, vol., no., pp.373, 378, 11-13 Oct. 2004

[15] Chi-fu Huang; Yu-Chee Tseng; Li-Chu Lo, "The coverage problem in three-dimensional wireless sensor networks," Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE, vol.5, pp.3182, 3186 Vol.5, 29 Nov.-3 Dec. 2004.

[16] Yujia Zhang; Guanlin Chen; Wenyong Weng; Zebing Wang, "An overview of wireless intrusion prevention systems," Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference on, vol.1, no., pp.147, 150, June 29 2010-July 1 2010.

[17] Yaqing Zhang; Sampalli, S., "Client-based intrusion prevention system for 802.11 wireless LANs," Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on, vol., no., pp.100, 107, 11-13 Oct. 2010.

[18] Pei Zhang; Rong-Long Wang; Chong-Guang Wu; Okazaki, K., "An Effective Algorithm for the Minimum Set Cover Problem," Machine Learning and Cybernetics, 2006 International Conference on, pp.3032, 3035, 13-16 Aug. 2006.

[19] Bosio, S.; Capone, A.; Cesana, M., "Radio Planning of Wireless Local Area Networks," Networking, IEEE/ACM Transactions on, vol.15, no.6, pp.1414, 1427, Dec. 2007

[20] Ka-Shun Hung; King-Shan Lui, "On securing perimeter coverage in wireless sensor networks," Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on, pp.384, 389, 28-30 Sept. 2009.

[21] Watkins, L.; Beyah, R.; Corbett, C., "A Passive Approach to Rogue Access Point Detection," Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, vol., no., pp.355, 360, 26-30 Nov. 2007.

[22] Vanjale, S.B.; Mane, P.B.; Patil, S.V., "Wireless LAN Intrusion Detection and Prevention system for Malicious Access Point," Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, vol., no., pp.487, 490, 11-13 March 2015.

[23] Anmulwar, S.; Srivastava, S.; Mahajan, S.P.; Gupta, A.K.; Kumar, V., "Rogue access point detection methods: A review," Information Communication and Embedded Systems (ICICES), 2014 International Conference on , vol., no., pp.1,6, 27-28 Feb. 2014.

[24] Le, T.M.; Ren Ping Liu; Hedley, M., "Rogue access point detection and localization," Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on, vol., no., pp.2489, 2493, 9-12 Sept. 2012.

[25] Liran Ma; Teymorian, A.Y.; Xiuzhen Cheng, "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks," INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 13-18 Abril 2008.

[26] Le Berre, M.; Hnaien, F.; Snoussi, H., "A multi-objective modeling of K-coverage problem under accuracy constraint," Modeling, Simulation and Applied Optimization (ICMSAO), 2013 5th International Conference on, vol., no., pp.1, 6, 28-30 April 2013.

[27] Amaldi, E.; Capone, A.; Cesana, M.; Malucelli, F.; Palazzo, F., "WLAN coverage planning: Optimization Models and Algorithms," Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th, vol.4, pp.2219, 2223 Vol.4, 17-19 May 2004.

[28] “Cisco Aironet Access Point Module for Wireless Security and Spectrum Intelligence Data Sheet”

URL:http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/data_sheet_c78-720719.html/

Fecha de consulta: 2 de noviembre de 2014

[29] Garey, Michael R. y David S. Johnson. “Computer and Intractibility: A guide to the Theory of NP-Completeness”. 1979

[30] Miranda, J.; Abrishambaf, R.; Gomes, T.; Goncalves, P.; Cabral, J.; Tavares, A.; Monteiro, J., "Path loss exponent analysis in Wireless Sensor Networks: Experimental evaluation," Industrial Informatics (INDIN), 2013 11th IEEE International Conference on, vol., no., pp.54,58, 29-31 July 2013.

[31] “802.11 Wireless LANs”

URL: http://www.inf.ed.ac.uk/teaching/courses/cn/WiFi.pdf

Fecha de consulta: 2 de febrero de 2015.

[32] “802.11 WLAN Systems – a tutorial”

URL:http://www.cacs.louisiana.edu/~perkins/csce575/papers/80211_tutorial-veriwave.pdf

Fecha de consulta: 3 de Marzo de 2015

[33] “MCS: Index”

URL: http://mcsindex.com/

[34] Gal, Z.; Balla, T.; Karsai, A.S., "On the Wi-Fi interference analysis based on sensor network measurements," in Intelligent Systems and Informatics (SISY), 2013 IEEE 11th International Symposium on , vol., no., pp.215-220, 26-28 Sept. 2013.

[35] Pan Feng, "Wireless LAN security issues and solutions," in Robotics and Applications (ISRA), 2012 IEEE Symposium on, vol., no., pp.921-924, 3-5 June 2012.

[36] Wireless Local Area Network (WLAN) Best Practices Guide

URL: https://education.alberta.ca/media/822010/wirelessbestpracticesguid.pdf

Fecha de consulta: 25 de Mayo de 2015

[37] “Enterprise WLAN Architecture”

URL: http://www.cs.uml.edu/~glchen/cs414-564/handouts/C05-WLAN_Arch.pdf

Fecha de consulta: 12 de Marzo de 2015

[38] “Best Practices for Rogue Detection and Annihilation”

URL:http://airmagnet.flukenetworks.com/assets/whitepaper/Rogue_Detection_White_Paper.pdf

Fecha de consulta: 14 de Abril de 2015

[39] “Cisco Aironet 3600 Series Access Point Data Sheet”

URL:http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/data_sheet_c78-686782.html

[40] Acuña Espilco, Emerson y Renato Herrera Ormeño, “Levantamiento del mapa de calor e atenuaciones de señal electromagnética en las bandas 2.4GHz y 5GHz para la red Wireless PUCP. Tesis para optar el Título de Ingeniero de las Telecomunicaciones”. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería.

[41] IEEE Draft 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 (PHY) Specifications--Amendment 1: Radio Resource Measurement of Wireless Lan'S," in IEEE Unapproved Draft Std P802.11k/D9.0, Sep 07 , vol., no., pp., 2007.

[42] Poloczek Matthias, “Randomized Greedy Algorithms for the Maximum Matching Problem with New Analysis”. IEEE 53rd Annual Symposium on Foundations of Computer Science. 2012.