INVESTIGACIÓN

F – IN - 03 | PROYECTO DE SEMILLERO TERMINADO | VERSIÓN: 3.0

Información General

Facultad: CIENCIAS NATURALES E INGENIERIA			
Programa Académico: INGENIERIA DE TELECOMUNICACIONES		Grupo(s) de Investigación: GNET	
Nombre del semillero /Sigla: Semillero en sistemas de Telecomunicaciones/ SISTEL		Fecha creación: 12 febrero de 2015 Regional: Bucaramanga	
Líneas de Investigación: Comunicaciones inalámbricas - Protocolos de Transmisión y Recepción			
Áreas del saber *			
	1. Ciencias Naturales	X	2. Ingeniería y Tecnologías
	3. Ciencias Médicas y de la Salud		4. Ciencias Agrícolas
	5. Ciencias sociales		6. Humanidades

Información del Director del Proyecto

Nombre: Johan Leandro Tellez Garzon	No. de identificación:	Lugar de expedición:
Nivel de Formación Académica (Pregrado / Postgrado / Link de CvLAC): Ingeniero en Telecomunicaciones / Maestría en Ingeniería Electrónica y Telecomunicaciones / Doctorado en Ingeniería Eléctrica /		
Celular	Correo Electrónico:	

Información de los autores

Nombre	No. de Identificación y lugar de expedición		Celular	Correo Electrónico
Brayan Alberto Álvarez Fontecha				
Andrés Felipe Martínez Fragoso				

Proyecto

1. Título del Proyecto:	Modalidad del Proyecto				
	PA	PI	TG	RE	Otra. ¿ Cuál?
Prototipo de generación de interferencia Wifi usando dispositivos programables para análisis de impacto en el bloqueo de la señal en un aula de clase					

2. Resumen del trabajo:

La metodología utilizada para esta investigación es un proceso experimental y empírico con el cual se quiere llegar al diseño y la implementación de un Inhibidor de Wi-Fi en la banda de 2.4 GHz por medio de un dispositivo programable; con el fin de ayudar a evitar la copia y/o distracciones de los estudiantes que usan redes locales inalámbricas institucionales. Investigando los diversos procesos de inhibición de señales en el espectro de 2.4 GHz, validando cual tiene mayor efectividad dentro de un aula de clase teniendo en cuenta factores como ambiente de operación, distancia relativa de los bloqueadores y de los dispositivos finales.
A través de todo el proceso de investigación se lograron tener resultados fructíferos y satisfactorios evidenciados a través del programa iPerf, el cual valida la pérdida total de la conexión entre los dispositivos finales y el Access Point, teniendo una transmisión final de 0 Kbps a la hora de accionar los dispositivos bloqueadores. Estos resultados solo se han llegado a verificar en la banda de 2.4 GHz ya que, las redes que estén en la banda de 5.0 GHz manejan diferentes protocolos y frecuencias por lo que se requieren otros métodos para lograr interferirlas.
Finalmente, queda en evidencia que, si es un método factible a la hora de implementarlo en un aula de clase, ya que su efectividad es del 100% en la perdida de la conexión cuando los bloqueadores estén activos, además de que emite radiaciones seguras para los seres humanos.

3. Objetivo General y Objetivos específicos:

Diseñar e implementar un inhibidor de Wi-Fi en la banda de 2.4 GHz por medio de un dispositivo programable verificando su funcionamiento como bloqueador de señal en un aula de clase a fin de establecer una herramienta en el ámbito educativo que ayude a evitar la copia o las distracciones de los estudiantes que usan redes locales inalámbricas.

- Realizar una revisión bibliográfica para identificar métodos de inhibición de señal WIFI en ambientes de aula y para conocer el funcionamiento y programación de los dispositivos programables adecuados para el prototipo bloqueador.
- Realizar la programación de uno o varios dispositivos programables para transmitir información de manera constante sobre los canales de la banda 2.4GHz de WIFI con el fin de generar interferencia perjudicial a otros dispositivos que se encuentren en el mismo ambiente de operación.
- Validar la efectividad del dispositivo a través de una serie pruebas en una sala de aula con diferentes distribuciones de dispositivos móviles, Access Point y prototipo bloqueador para analizar los resultados en la inhibición de la señal WIFI considerando la cantidad de bloqueadores y sus distancias relativas a los demás dispositivos del ambiente de operación.

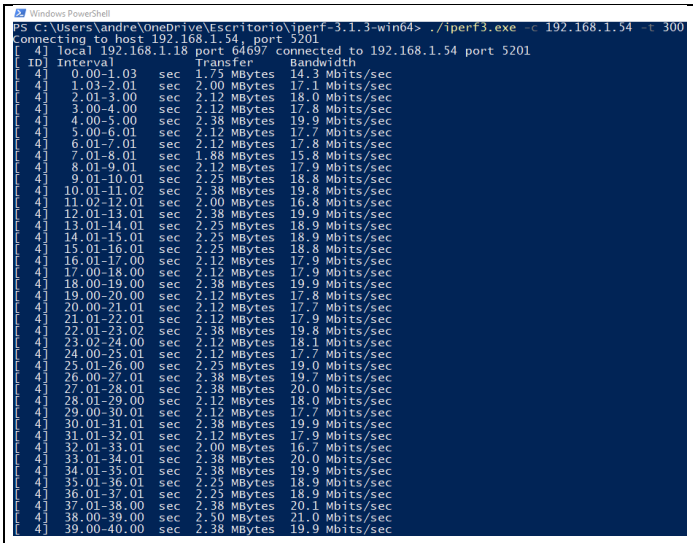
4. Análisis de resultados:

A través de las distintas pruebas que se realizaron, se pudo evidenciar que hubo una pérdida de la señal en la red, ya que los dispositivos finales no podían conectarse a la red Wi-Fi de 2.4Ghz. Sin embargo, decidimos hacer uso de la aplicación iPerf más específicamente en su versión 3.1.3, que, entre sus tantas funcionalidades, nos permite evaluar el rendimiento de la red, por medio del envió de paquetes entre dos computadores previamente configurados uno como servidor y otro como cliente y observar el funcionamiento en vivo de la red mientras se realiza el ataque, evidenciando de manera clara el momento justo donde la transmisión de paquetes es totalmente nula.

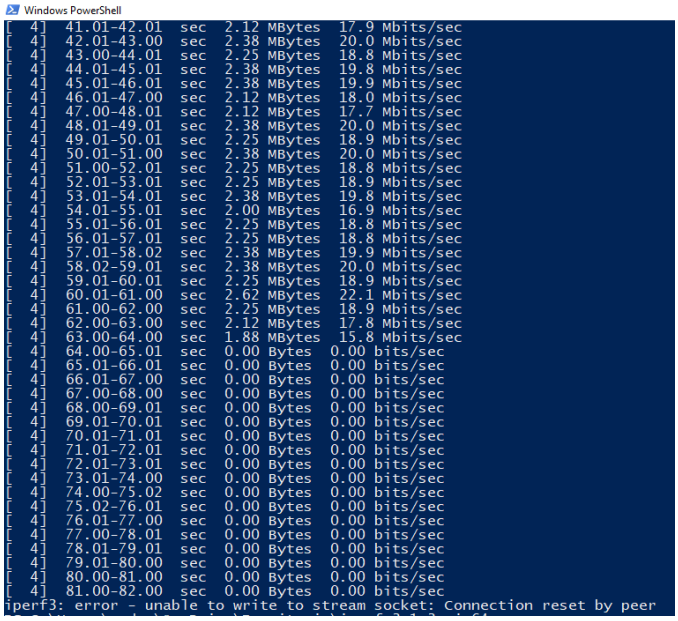
Resultados Aula de Clase Distribución 1

En la primera prueba se ubicó el dispositivo inhibidor en la mitad del Access Point y el dispositivo final, obtuvimos como resultado la inhibición total de la conexión a la red.

Para iniciar realizamos una prueba la cual consistía en medir el rendimiento inicial de la red, sin el dispositivo inhibidor funcionando para demostrar que la red transmite sin problemas, obteniendo los siguientes resultados en Mbps, en un lapso de 300 segundos que equivalen a 5 minutos.



Una vez realizada la prueba de red, se procedió a realizar un segundo envío de paquetes por el mismo lapso de tiempo, es decir, 300 segundos, pero esta vez en el segundo 63 se procedió a activar el dispositivo inhibidor, obteniendo los siguientes resultados



Como se puede apreciar, el funcionamiento de la red era totalmente normal hasta llegar exactamente al segundo 64 en el que se registró una transferencia de 0 Bytes y un ancho de banda de 0 bits/sec hasta que los dispositivos finales pierden conexión entre ellos, debido a que la red deja de funcionar gracias al dispositivo inhibidor.
Entonces el resultado de esta primera prueba tiene una efectividad inmediata y 100% eficaz. Ya que los dispositivos finales no pueden conectarse a la red mientras el dispositivo esté en funcionamiento

5. Conclusiones:

A través de este trabajo de investigación, se realizó un paso a paso del diseño de un dispositivo inhibidor de Wi-Fi en la banda de 2.4 GHz el cual es totalmente funcional y aplicable en un aula de clase dentro de la institución educativa. El cual es efectivo a la hora de impedir la conexión de los dispositivos finales tales como computadores portátiles o teléfonos inteligentes con un Access Point que trabaje en la banda de 2.4GHz.

Esto es algo positivo ya que abre una puerta más a la legalidad de los exámenes y/o pruebas dentro de las instalaciones de las Unidades Tecnológicas de Santander, así mismo es una apertura de investigación de como los Deauthers los cuales cuentan con paquetes de desautentificación que impiden la conexión a las redes Wi-Fi en la banda de 2.4 GHz y como esto puede ayudar ya sea a la seguridad de redes dentro de la institución o como bien el enfoque de este proyecto evitar la copia al utilizar dispositivos que puedan conectarse a este tipo de redes Wi-Fi.

También, gracias a la investigación hecha a partir de las ventajas y usos del dispositivo programable ESP 8266 se ve que no es la única aplicación que tiene en este ámbito, también podría ser programado como un Jammer en caso de querer hacer un dispositivo de inhibición de más tipos de redes, tales como las redes de telefonía celular, Wi-fi, hasta satelitales si se quisiese. Por otra parte, se

logró profundizar mucho más en el concepto de inhibición de señales, y los distintos métodos que existen y como estos pueden ayudar en distintas aplicaciones dependiendo las circunstancias.

Gracias al programa iPerf 3.1.3 se logra comprobar la efectividad del prototipo inhibidor realizado en esta investigación en el cual, se evidencia como al ser activado tal dispositivo la perdida de paquetes es instantánea en caso de estar muy cerca al Access Point a inhibir o bien, empieza a hacer tan pesado el manejo dentro de la red si se encuentra a una distancia lejana del Access Point, hasta el punto en el cual la señal se interviene totalmente. La efectividad de la inhibición de este prototipo va a variar en que tan potente reciba la señal a interferir, si la señal es muy fuerte, la inhibición será prácticamente instantánea, mientras que si detecta la señal Wi-Fi de manera tenue o muy débil le será más costoso cumplir con su objetivo. A lo que se llega es que la distancia entre el Access Point y el dispositivo Inhibidor es el factor más decisivo en estas pruebas, y no tanto la distancia de los dispositivos finales.

Como nota final, mientras que este prototipo de inhibidor o dispositivo inhibidor este dentro del rango de la red Wi-Fi en la banda de 2.4 GHz, tendrá una efectividad de inhibición del 100% aunque su tiempo dependerá de la distancia a la que se encuentre del Access Point en cuestión.

6. Recomendaciones:

A la hora de configurar el Arduino IDE, se solicita seguir un paso a paso para agregar las librerías necesarias y que estas funcionen de manera correcta (Tutoriales, 2017), ya que, sin esto, no se podrán instalar las versiones específicas que permiten que nuestro dispositivo programable funcione como un Deauther.
Se solicita que por favor a todos los próximos estudiantes que realicen investigaciones con este tipo de interferencias hacia una red, lo hagan en un ambiente controlado/privado debido a que este tipo de dispositivos pueden hacer que cualquier persona conectada vía Wi-Fi pierdan la conexión y la idea no es usar este dispositivo para afectar a terceros, en caso de usar este dispositivo en redes ajenas puede llegar a tener consecuencias legales. Aun así, queremos invitar a todos nuestros compañeros de carrera a profundizar aún más en el tema y lograr realizar un Deauther para las redes Wi-Fi de 5Ghz, ya que las redes modernas están usando esta tecnología.

7. Bibliografía:

Arduino, A. T. (20 de Julio de 2015). *Geek Factory*. Obtenido de https://www.geekfactory.mx/tutoriales/tutoriales-arduino/driver-ch340-para-arduino-chinos-o-genericos/

Blázquez, D. R. (2015). *DOCPLAYER*. Obtenido de https://docplayer.es/8732962-En-este-capitulo-se-presenta-el-marco-teorico-sobre-las-redes-inalambricas-que-utilizan-el.html

Candy-ho. (2021). *Candy-ho*. Obtenido de https://candy-ho.com/producto/dstike-wifi-deauther-v3-esp8266-2db-escaner-wifi-control/

Cisco. (2021). *¿Qué es Wi-Fi?* Obtenido de https://www.cisco.com/c/es_mx/products/wireless/what-is-wifi.html#~preguntas-y-respuestas

Crespo, E. (2017). *Aprendiendo Arduino*. Obtenido de https://aprendiendoarduino.wordpress.com/2016/12/11/ide-arduino/

Deauther. (s.f.). *GitHub*. Obtenido de https://github.com/SpacehuhnTech/esp8266_deauther/tree/v2

Estapé, J. A. (02 de Junio de 2015). *Computer Hoy*. Obtenido de https://computerhoy.com/noticias/hardware/nuevos-trucos-tecnologicos-copiar-examenes-17399

Gonzáles, M. (18 de Abril de 2011). *Xataka Movil*. Obtenido de https://www.xatakamovil.com/conectividad/que-son-los-canales-wi-fi-y-como-escoger-el-mejor-para-nuestra-red

GSMA. (2017). *GSMA*. Obtenido de https://www.gsma.com/latinamerica/wp-content/uploads/2017/12/Reporte-Jammers-2017-Español.pdf

Guys, H. T. (10 de Febrero de 2017). *Youtube*. Obtenido de https://www.youtube.com/watch?v=N5JVQ-m5Kd0

Hernández, L. d. (2019). *Programar Fácil*. Obtenido de https://programarfacil.com/podcast/esp8266-wifi-coste-arduino/

Isaac. (2021). *Hardware Libre*. Obtenido de https://www.hwlibre.com/esp8266/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+hwlibreweb+%28Hardware+libre%29

Kremser, S. (08 de Agosto de 2017). *Udemy*. Obtenido de https://www.udemy.com/user/stefan-kremser-2/

LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES. (2011). *Crcom*. Obtenido de https://www.crcom.gov.co/resoluciones/00003066.pdf

LA DIRECTORA GENERAL DE LA AGENCIA NACIONAL DEL ESPECTRO. (18 de Noviembre de 2016). *MinTic*. Obtenido de https://normograma.mintic.gov.co/mintic/docs/resolucion_ane_0711_2016.htm

8. Anexos: Corresponde a las evidencias de realización y resultados de proyecto y a las herramientas desarrolladas y/o utilizadas en su ejecución.

***** *Organización para la Cooperación y Desarrollo Económico (OCDE)***

****** *PA: Plan de Aula, PI: Proyecto integrador, TG: Trabajo de Grado, RE:Reda***