Cifrado en Access Point

Guillermo Venegas Ceciliano[1], Geovanny Cordero Valverde[2]
Escuela de Ciencias de la Computación e Informática
Universidad de Costa Rica, San José, Costa Rica.
{[1]guillermo.venegasceciliano, [2]geovanny.corderovalverde}@ucr.ac.cr

***Resumen*— Se realiza un análisis de rendimiento al enviar paquetes cifrados a través de un punto de acceso determinado de un computador a otro. Lo anterior utilizando el firmware Advanced Tomato. Se presentan los resultados y se dan recomendaciones según estos.**

I. Introducción

Hoy en día la seguridad informática se ha convertido en un tema del que muchas personas discuten, independientemente de su conocimiento sobre temas informáticos. También, casi en todos los lugares donde habitan personas (apartamentos, casas, e incluso cuartos), se utilizan puntos de acceso para proveer una conexión a internet o a la intercomunicación de distintos dispositivos. En esta investigación buscara distinguir el rendimiento (tiempo) que en la que dos dispositivos intercambia información en una red local generada por punto de acceso. La motivación principal es apreciar las diferencias en los costos a la hora de utilizar algoritmos empleados por el Linksys N600 E2500 para la encripcion de datos. es obtener una aproximación de el tiempo asociado con los métodos de cifrado al momento de transmitir información a través de una red wireless. Los experimentos se realizarán utilizando distintos métodos de cifrado para establecer las comparaciones entre los mismos. Además, se utilizará un firmware diferente al que trae por defecto el enrutador utilizado. Todo esto para la realización de diferentes experimentos y se genera un análisis sobre los resultados obtenidos.

II. Marco Teórico

II-A. Experimento

Se mide la rapidez en la que un punto de acceso inalámbrico (WAP) transmite información entre dos nodos distintos (computadoras personales) en una red local. Esta medición de la velocidad se realizará con 3 modalidades diferentes: una en una red insegura (sin encripción) contra dos de red segura (usando métodos de encripción WPA (AES) y WPA2(AES)). La completitud de cada experimento se da (se prueba) cuando se recibe completamente un archivo. Esto se verifica mediante el commando *diff* en la terminal de Unix.

C++: Se utiliza C++, que es un lenguaje de propósito general, que nació como una extensión de C. Provee programación orientada a objetos (modo usado para la investigación), imperativa y genérica.

Sockets: Se utilizan Sockets para el envío de paquetes por medio del llamado de sistema socket, el cual crea un endpoint para la comunicación y devuelve un descriptor (entero) que hace referencia a ese endpoint.

Virtualización: No se utilizan virtualizadores, ya que se trabaja en el sistema operativo que poseen dos maquinas físicas distintas.

II-B. Probabilidad y Estadística

Distribución Normal: Conocida a menudo como distribución gaussiana, es la distribución de probabilidad continua más importante. Su gráfica tiene forma de campana, la cuál se denomina curva normal. Sus desviaciones estándar establecen valores de referencia para estimar el porcentaje de observaciones de los datos [1]

Prueba de Anderson-Darling: Permite determinar si una muestra de datos se extrae de una distribución de probabilidad normal o no.

Prueba de Shapiro–Wilk: Se utiliza para contrastar la normalidad de una población. La prueba devuelve un valor, si es pequeño dice que la distrubución no es normal.

Prueba T de Welch: También se le conoce como Prueba T de varianzas desigules. Es una variación de la prueba T de *Student*. Se utiliza para probar la hipótesis de que dos poblaciones tienen medias iguales y se inicia asumiendo que estas dos poblaciones tienen distribuciones normales e igual varianza.

III. Objetivos

III-A. Objetivo General

Describir el rendimiento del envío de paquetes cifrados y no cifrados con el firmware Advanced Tomato en el enrutador Linksys N600

III-B. Objetivos Específicos

1. Contrastar el rendimiento de envío de paquetes cifrados y no cifrados en en el enrutador Linksys N600.
2. Identificar rendimiento al enviar archivos de diferentes tamaños y formatos usando el firmware Advanced Tomatoe.
3. Sugerir buenas prácticas al usar cifrado en puntos de acceso para lograr buenos resultados.

IV. Metodología

IV-A. Ambiente de Trabajo

- Se utiliza el enrutador Linksys N600, modelo E2500 V3 para la realización de las pruebas, algunas especificaciones:
  - Chipset Broadcom BCM5357 chip rev 2 pkg 8

Parámetro	Valor
Wireless Mode	Access point
Wireless Network Mode	Auto
Channel	6: 2.347GHz
Channel Width	40MHz
Control de banda lateral	Upper
Wireless (5 GHz / eth2)	Desactivado
Configuracion de servicio IPv6	No

Cuadro I
CONFIGURACIÓN APLICADA AL ENRUTADOR

  - CPU Frequency 300MHz
  - Memoria 59.80 MB
  - NVRAM 60.00 KB
- Las pruebas se realizan con la última versión del firmware Advanced Tomatoe para el router mencionado, especificmente: 1.28.0000 MIPSR2-3.5-140 K26 USB Mega-VPN.
- Las pruebas se realizan sin protocolo de eccripción, usando WPA y WPA2.
- Se utilizan máquinas de 64 bits, con sistema operativo Linux. Especificaciones:
  - Máquina que envía:
    1. Distro: Ubuntu 19.04
    2. Disco: HDD, interfaz SATA, marca TOSHIBA.
    3. Procesador: i5-5200U CPU 2.20GHz x 4
    4. RAM: 8 GB
    5. Targeta de red:
       a) Tasa de bits: 150 Mbps
       b) Frecuencia: 2.437 GHz
  - Máquina que recibe:
    1. Distro: elementary OS 5.0 Juno (64-bit), Built on Ubuntu 18.04.2 LTS
    2. Disco: SSD, interfaz SATA, marca GIGABYTE.
    3. Procesador: Intel i5-4200U CPU 1.60GHz
    4. RAM: 16 GB
    5. Targeta de red:
       a) Tasa de bits: 121.5 Mbps
       b) Frecuencia: 2.437 GHz
- Se utiliza el lenguaje de programación C++ para hacer las pruebas.
- Se utilizan sockets para el traspaso de paquetes de una máquina a otra con protocolo TCP. Este es una de las forma de interconectar las dos computadoras para lograr el envío de paquetes sin perdidas.

IV-B. Protocolos de seguridad

1. WPA: creado en el 2003, usa llaves de 256 bits. Incluye chequeo de integridad de mensajes y integración del protocolo TKIP (Temporal Key Integrity Protocol).
2. WPA2: Reemplaza a WPA aproximadamente en el 2006. Usa algoritmos AES y introduce el uso del protocolo CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol).

IV-C. Archivos de prueba

Se envían archivos de texto(txt), de imagen (png) y de video (mp4) de diferentes tamaños (1MB, 2MB, 3MB, 5MB, 10MB). Por la manera en que se realiza los envíos, únicamente su tamaño afecta el tiempo de envío (en nuestro experimento).

Para la medición del tiempo se utiliza la librería *chrono* de C++ y se inicia el conteo del tiempo antes de empezar a enviar los paquetes y se termina una vez que se recibe el último, esto al enviar un *ack* al nodo que envía. Se realizan diez repeticiones por cada experimento.

IV-D. Logro de objetivos

Tanto para el primer como para el segundo objetivo, se hacen varias pruebas con las especificaciones arriba mencionadas. Se obtienen los datos y se guardan en archivos csv, los cuales se procesan mediante la herramienta *R*. Se realizan pruebas de normalidad y una vez verificada esta, se realizan pruebas de T de Student, entre las pruebas que se desean contrastar (encriptado o no) y se realiza un análisis sobre los resultados, apoyándonos en la gráficas que se generaran en esta misma herramienta (R). Todos estos datos se generan con la finalidad de completar el último objetivo, realizar un análisis de los resultados obtenidos y realizar recomendaciones en base a estos.

V. EXPERIMENTOS Y RESULTADOS

V-A. Detalles de las pruebas realizadas

El experimento consta de enviar de 4 archivos de distintos tamaños de una computadora a otra mediante una red inalámbrica (esto usando 3 modos de transmisión: abierto, con encriptado WAP(AES) y con encriptado WAP2(AES)), para cada modo de transmisión y para cada archivo se realizo 15 repeticiones de cada para hacer la mediciones de tiempo. Al usar diferentes tipos de archivos, se intenta identificar si este parámetro afecta el tiempo de envío.

Algunos de los parámetros que pueden afectar las pruebas se listan a continuación:

1. Tamaño de archivos: A continuación se listan los tamaños de los archivos utilizados en la prueba
   - 1 MB
   - 2 MB
   - 3 MB
   - 5MB
   - 10 MB
2. Cantidad de repeticiones: el experimento consta de 12 pruebas (una por cada modo de encripción de datos más una por cada tipo diferente de archivo) que constan de 15 transferencias por cada uno de los archivos mencionado anteriormente.
3. Uso del procesador al momento de correr las pruebas: Solo se ejecutaron los procesos de recepción y envió de datos por la red (sin contar los de sistema operativo).
4. Ocupación de la red inalámbrica: El router se configura para solo las computadoras participantes en las pruebas tuvieran acceso a este.
5. Ocupación del ancho de banda utilizado por el router: Se selecciono un canal con baja interferencia, para ello se uso la información que brinda la interfaz de configuración del router sobre este parámetro.

6. Latencia en la lectura y ocupación del disco: Igualmente como solo se estaba usando el programa de envio y recepción de datos (son contar los de SO) se estima casi nulo el impacto de este parámetro.
7. Precisión de los datos obtenidos. En nuestro experimento se utiliza segundos como métrica para medir el tiempo.

V-B. Resultados obtenidos

Los resultados obtenidos se incluyen en un directorio aparte y de igual manera se puede revisar en el repositorio de Github: Access Point Encryption.

VI. Análisis de los resultados

VI-A. Normalidad de los datos

Mediante la prueba de Shapiro-Wilk, comprobamos la normalidad de los datos, al obtener un valor p mayor a 0.05 en cada conjunto de datos, por lo que se asumirá que poseen distribución normal, esto nos permite mas adelante el poder aplicar las demás pruebas correspondientes, como por ejemplo comparaciones por Student-T. Los resultados se pueden verificar en los archivos adjuntos o en el repositorio Access Point Encryption.

VI-B. Comparación por Student-T

Usando un intervalo de confianza de 95 %, si revisamos el cuadro , podemos ver que son muy pocos los valores P que están por encima del intervalo de confianza dado, lo que hace que se rechace la hipótesis de que las medias de estos son diferentes. Los resultados se pueden verificar en los archivos adjuntos o en el repositorio Access Point Encryption.

VI-C. Comprobación de la hipótesis

Comprobamos que al usar el firmware Tomato Advance, se mejora de manera considerable el rendimiento en el enrutador Linksys N600, esto mediante pruebas iniciales (que no se incluyen debido a que la investigación la enfocamos específicamente en Tomato Advance y no en la comparación de diferentes firmwares).

Luego, de manera general las pruebas mejoran al usar el cifrado WAP en contraste a las realizadas con la red abierta (hay una minoría que no lo cumple). El tiempo aumenta un poco más, en todos los casos, al utilizar cifrado WAP2.

Tal como se esperaba, al aumentar el tamaño del archivo para la realización de las pruebas, de la misma manera el tiempo incrementaba, independiente del tipo de archivo (debido a la manera en que se envían), por lo que en este caso podemos decir que el tipo de archivo no afecta la duración del envío de archivos.

Algo importante a señalar, es que con los datos mp4 no se utiliza el tamaño de 3 MB, en cambio, se utilizan de un tamaño de 2 MB,por lo que en los gráficos se ve una pequeña diferencia en la segunda prueba con los archivos de tipo mp4.

En la figura 1 podemos ver que a medida que se aumenta el tamaño de los archivos, así aumenta el tiempo de manera casi lineal. Haría falta probar con una distribución de tamaños de archivos más regular para verificar si en efecto el tiempo

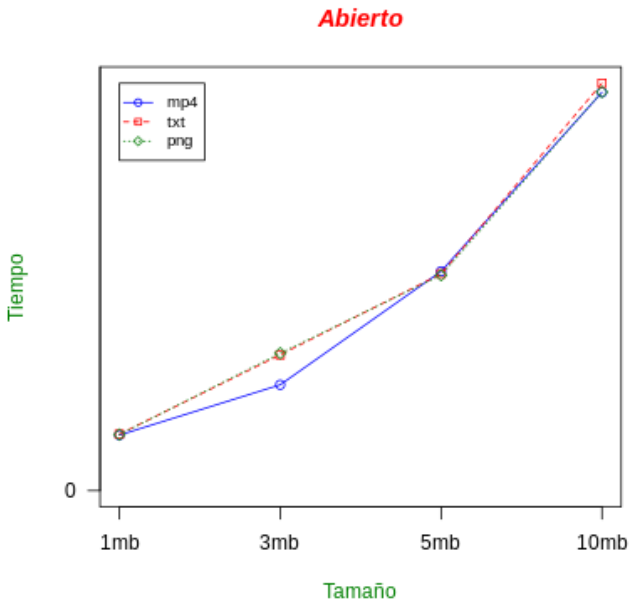

Figura 1. Medias de los tiempos del envío de datos sin encripción

de comporta de una manera muy similar a una función lineal o si se asemeja a alguna otra.

De igual forma, con encripción WPA, la forma en que se aumentan los tiempos es similar a la que se presenta al no usar ningún tipo de encripción, como se puede apreciar en la figura 2. Se ve que hay una pequeña diferencia en el segundo punto debido a que como se mencionó anteriormente se usan diferente tamaño con los archivos mp4.

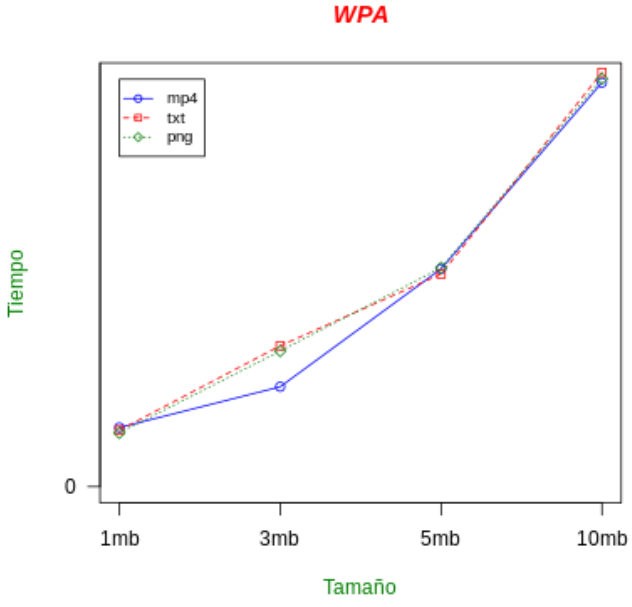

Figura 2. Medias de los tiempos del envío de datos sin encripción

En la figura 3 se puede apreciar como los datos aumentan

de manera muy similar a las anteriores. Algo interesante que surge y que se puede revisar en los tiempos obtenidos, es que en algunos casos el no usar encripción sale un poco más caro (tiempo) que el usar alguno de los dos tipos que se utilizaron para este experimento. A su vez, la diferencia obtenida de tiempos con los dos tipos de encripción son muy pocas y en ocasiones varía con cuál tarda más con un mismo archivo.

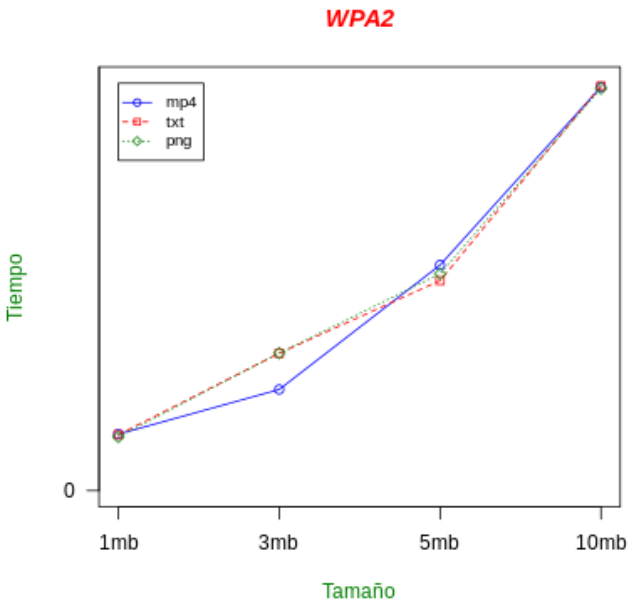

Figura 3. Medias de los tiempos del envío de datos sin encripción

De manera general, podemos decir que independiente de los archivos utilizados el tiempo aumenta de una manera similar. Aún con la variación de un Megabyte con los archivos mp4, los otros dos se comportan de una manera similar.

Tomando en cuenta todos los valores en segundos de las pruebas, para la prueba abierta la duración más alta fue de 2.5411 segundos, con WPA de 2.57292 segundos y con WPA2 de 2.486 segundos. Podemos verificar que estos resultados no son considerablemente grandes, por lo que la aplicación de encripción parece una buena práctica sin dejar de lado la eficiencia.

Dados estos resultados, instamos a que se use cifrado en los enrutadores, ya que mejorará la seguridad de manera considerable y no afecta mucho el tiempo de transmisión de datos.

VI-D. Algunas dificultades que surgieron

Se quiso realizar las pruebas para la transmisión de datos con otros otras configuraciones de encripcion como WAP o WAP2 empresariales (las cuales también se podían configurar con el punto de acceso utilizado), la configuración fue exitosa mas no se lograron completar las pruebas por un error en un computador con sistema operativo Ubuntu, el cual no se podría conectar a la red por problemas con el protocolo PEAP, se plantea a futuro buscar la solución al error mostrado para agregar las pruebas de estos.

Otro problema que surgió es que inicialmente el experimento se estaba realizando con archivos muy pesados (por ejemplo se emplearon archivos de 250 MB, 450 MB y de 2 GB) y dado a que la red inalámbrica del punto de acceso es muy lenta para el intercambio de información local estas pruebas requirieron periodos muy largos de tiempo, en los cuales podrían surgir interferencias del ancho de banda o actividades inesperadas del sistema operativo que pudieran ralentizar el proceso de intercambio, lo que impedía una correcta medición de las pruebas. En la sección de anexos se adjuntan algunos datos recolectado de estas pruebas, dichos datos serán sujetos a análisis por que no poseen una distribución normal.

VII. Conclusiones

Al usar el firmware Tomato Advance se mejora de manera considerable el rendimiento en el enrutador Linksys N600.

De manera general las pruebas mejoran al usar el cifrado WAP en contraste a las realizadas con la red abierta. El tiempo aumenta un poco más, en todos los casos, al utilizar cifrado WAP2.

El uso de archivos de diferentes formatos no aumenta o disminuye la duración.

Al aumentar el tamaño del archivo para la realización de las pruebas, el tiempo incrementaba, independiente del tipo de archivo.

Se insta a que se use cifrado en los enrutadores, ya que mejorará la seguridad y no se afecta mucho el tiempo de transmisión de datos.

Referencias

[1] R. Walpole, R. Myers, S. Myers, and K. Ye, *Probabilidad y estadística para ingeniería y ciencias - Novena Edición*, 2012.
[2] K. H. Rosen and K. H. Rosen, *Discrete Mathematics and Its Discrete and Its Applications*, 2013.
[3] W. J. Stewar, *Probability, Markov chains, queues and simulation: the mathematical basis of performance modeling*, 1st ed. Woodstock, Oxfordshire: Princeton University Press.
[4] B. Derrick and P. White, "Why Welch's test is Type I error robust," *The Quantitative Methods for Psychology*, vol. 12, no. 1, pp. 30–38, 2016.
[5] M. J. Crawley, *The R Book [2e]*, 2013, no. 1.