

Análisis de Performance y QoS en Redes de Datos – 2021

Laboratorio 2: Modelo de Tráfico

El propósito de este laboratorio es ganar experiencia con el análisis de datos, la interpretación de datos y la representación gráfica de resultados para el análisis del tráfico de red. En el camino, reforzará sus conocimientos sobre el Protocolo de control de transmisión (TCP) y las técnicas para el análisis gráfico del rendimiento del protocolo TCP. En particular, utilizará un programa C para analizar un archivo de rastreo de tráfico de red con formato especial, para evaluar y comprender el comportamiento del protocolo TCP / IP en un entorno de LAN inalámbrica.

El archivo `PDAttrace.dat` (archivo de datos ASCII de 1.3 MB) muestra un poco de tráfico de paquetes TCP / IP recolectado usando un Wireless Sniffer en una WLAN IEEE 802.11b en la Universidad de Wildstone. Esta traza contiene 13.302 paquetes TCP / IP y dura unos 35 minutos.

Durante el período rastreado, un usuario de Internet móvil inalámbrico estaba descargando páginas web de diferentes sitios web en Internet. Esta traza se utilizará para su análisis de tráfico TCP y para responder las preguntas que figuran a continuación. (Un documento IEEE WLN 2004(`WebPDA.pdf`, disponible en la plataforma del curso) proporciona más información de fondo sobre el experimento de medición WLAN, si lo necesita). Cada línea de datos en el archivo de rastreo representa un paquete TCP / IP. Hay varias columnas de datos en cada línea, separadas por espacios. Las columnas, de izquierda a derecha, representan:

- la marca de tiempo (en segundos) en que se vio el paquete
- la dirección de origen de IP en el paquete
- la dirección de destino IP en el paquete
- el tamaño del paquete IP (incluido el encabezado IP y el encabezado TCP)
- el tipo de protocolo en el paquete (siempre TCP en esta traza)
- el puerto de origen especificado en el paquete
- el puerto de destino especificado en el paquete
- el número de secuencia TCP transportado en el paquete (los valores mostrados representan el número de secuencia asociado con el primer byte de datos y el último byte de datos en el paquete, lo que indica si el paquete está transportando datos TCP. Estos dos valores están separados por un colon.)
- el número de acuse de recibo TCP transportado en el paquete
- la ventana de recepción anunciada por el receptor (¡a veces útil!)
- los flags TCP transportados en el paquete, si los hay. Estos indicadores están codificados en la traza como *S* para un paquete SYN, *F* para un paquete FIN, *P* para el bit PUSH, y *A* para indicar un número de reconocimiento válido. Estas son las únicas posibilidades en este rastro.

Un ejemplo de una línea del archivo de rastreo es:

7.974098 192.168.1.9 → 216.40.34.65 44 TCP 1104 80 533868: 533868 0 win: 32768 S

Este paquete viajó desde la dirección de origen IP 192.168.1.9 (puerto 1104) a la dirección de destino IP 216.40.34.65 (puerto 80) en el momento 7.974098 seg. Era un paquete SYN de 44 bytes de tamaño (incluidos los encabezados de protocolo TCP / IP). El número de secuencia TCP inicial propuesto era 533868. Este paquete no contenía bytes de datos TCP reales. El campo de reconocimiento no era válido y se inicializó a 0. El tamaño de la ventana de control de flujo anunciado fue de 32 KB.

El programa C `tcpconnparse.c` ha sido escrito para analizar y procesar archivos de rastreo en este formato. En particular, el programa procesa el archivo de rastreo y calcula la información de resumen sobre las conexiones TCP. Tenga en cuenta que una conexión TCP se identifica mediante una tupla de 4 (dirección de origen IP, puerto de origen, dirección de destino de IP, puerto de destino), y los paquetes pueden fluir en ambas direcciones en una conexión (es decir, de A a B y de B a A).

La información resumida calculada para cada conexión TCP incluye:

- la hora de inicio, la hora de finalización y la duración de la conexión
- el número de paquetes enviados para cada conexión (desglosado por paquetes de datos y paquetes de reconocimiento en cada dirección, así como los paquetes totales)
- el número de bytes enviados para cada conexión (desglosado por bytes en cada dirección, así como por bytes totales). Este conteo de bytes es para bytes de datos (es decir, excluyendo los encabezados de protocolo TCP e IP).

El programa escribe varias columnas adicionales de salida de depuración para verificación. Puede ignorarlos si lo desea. Cuando el programa se ejecuta con éxito, produce una salida estándar a la pantalla que resume el archivo de rastreo de paquetes TCP procesado. Esta salida se puede guardar en un archivo si lo desea. El programa también produce silenciosamente tres archivos de datos de salida:

`timeperconn.dat`: la duración del tiempo transcurrido en segundos para cada una de las conexiones TCP exitosas observadas.

`pktsperconn.dat`: la cantidad de paquetes de red enviados durante cada una de las conexiones TCP exitosas observadas.

`bytesperconn.dat`: el número de bytes intercambiados durante cada una de las conexiones TCP exitosas observadas.

Use el programa y el archivo de seguimiento, disponibles en la plataforma del curso, para responder las siguientes preguntas:

1. ¿Cuántas conexiones TCP completas se observan en la traza?

-
2. Trace un histograma de frecuencia (también denominado función de densidad de probabilidad (pdf) o un diagrama de distribución marginal) para mostrar la distribución de las duraciones de conexión TCP observadas. Indique claramente las duraciones de tiempo mínima, media y máxima para las conexiones TCP exitosas que observó.
 3. Trace un histograma de frecuencia para mostrar la distribución de paquetes por conexión TCP. Indique claramente la cantidad mínima, media y máxima de paquetes enviados en las conexiones TCP que observó.
 4. Trace un histograma de frecuencia para mostrar la distribución de bytes enviados por conexión TCP. Indique claramente la cantidad mínima, media y máxima de bytes enviados en las conexiones TCP que observó.
 5. Elija aleatoriamente cualquiera de las primeras 20 conexiones TCP observadas en la traza. Genere un diagrama de número de secuencia TCP para esta conexión para mostrar los números de secuencia de los paquetes que transportan datos enviados por el servidor y los números de secuencia de confirmación devueltos por el cliente. Anote su gráfico a mano para mostrar el tamaño total de transferencia de datos, la duración de la conexión TCP y el rendimiento promedio de la conexión.
 6. Encuentre en esta traza una conexión TCP completa que dice haber descargado unos 120 KB de bytes de datos TCP. Genere un diagrama de número de secuencia TCP para esta conexión. Identifique cualquier diferencia entre este gráfico y el anterior. Explique estas diferencias.
 7. Encuentre en esta traza la conexión TCP completa que afirma haber descargado la mayor cantidad de bytes de datos TCP. Genere un diagrama de número de secuencia TCP para esta conexión. Identifique cualquier diferencia interesante entre este gráfico y los anteriores. Explique estas diferencias.

Cuando haya terminado, suba su tarea en forma de documento pdf identificado como Laboratorio_2_xxxx(xxx su apellido) por medio de la plataforma. Asegúrese de que su nombre esté en todo lo que envíe.