Resumo do Traballo de Fin de Grao

La clasificación del tráfico de Internet ha sido materia de estudio desde sus orígenes. El volumen de información transmitido es masivo, diverso y en constante expansión debido al carácter global de Internet, que facilita el envío de datos desde cualquier parte del mundo. La compartición de archivos entre usuarios se ha convertido en uno de los flujos primarios y, debido a sus rutas de envío irregulares, su análisis resulta problemático e intensivo para la mayoría de sistemas. Por ello, obtener estadísticas de uso exactas se convierte en una tarea compleja y laboriosa que requiere idear y producir nuevos métodos más eficaces y eficientes.

Existen múltiples enfoques o formas de afrontar la clasificación del tráfico de una red en función de los parámetros que se consideran, obteniendo así distintos grados de precisión. La técnica más expandida y utilizada en la actualidad es la inspección profunda de paquetes o deep packet inspection (DPI), que representa una evolución significativa en el área de filtrado de paquetes comparada con sus predecesores, que solo procesaban los datos de cabecera. Actúa en la capa de aplicación y se caracteriza por examinar la información de forma detallada y analizar los contenidos (payloads) de los paquetes, asegurando que se encuentren en el formato adecuado y no hayan sido alterados a raíz de una posible intrusión. Por lo tanto, no solo se encarga de comprobar y categorizar la información recibida, sino que también constituye una herramienta fundamental a la hora de mantener una red segura y robusta.

Para evaluar el funcionamiento de la técnica de inspección profunda de paquetes se encuentran disponibles tres utilidades principales de carácter open-source: L7-Filter, Statistical Protocol IDentification (SPID) y nDPI. L7-Filter está diseñado para sistemas Linux e identifica paquetes basándose en información procedente de la capa de aplicación. Emplea expresiones regulares para reconocer los protocolos a filtrar. Por otro lado, SPID es un algoritmo que se fundamenta en el análisis estadístico del flujo de una red para determinar el protocolo que se está utilizando. Por último, nDPI es una librería con un amplio repertorio de protocolos detectables y analizables.

El propósito u objetivo de este TFG es utilizar los módulos previamente mencionados para implementar la inspección profunda de paquetes y evaluar el funcionamiento, rendimiento y resultados obtenidos con cada aplicación.

Se ha seleccionado Scrum como metodología de desarrollo, que permite establecer iteraciones, denominadas sprints, durante las cuales se establecen los requisitos y objetivos a alcanzar en un período de tiempo establecido. Así, se dispondrá de flexibilidad y de la capacidad de reevaluar el progreso realizado e incorporar las modificaciones oportunas.

Para la realización del proyecto se utilizará un PC de sobremesa que dispone de Windows 10 como sistema operativo, un procesador Intel Core i5-7600k, 16GB de memoria RAM y una unidad de disco duro de 1TB.