République algérienne démocratique et populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Ecole Supérieure en Informatique de Sidi Bel Abbès (ESI-SBA)

Mémoire

En vue de l'obtention du diplôme de **Master**

Filière : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques (ISI)**

Network Traffic Classification

Réalisé par:
Lahouazi Chamel Djamel Eddine
Aissat Abdellah

supervisé par:
Dr. Alaa Eddine Belfedhal

Année Universitaire
2019/2020

Abstract

Network traffic classification has been studied for two decades and extended across a wide variety of systems from QoS and ISPs classification systems to firewalls and intrusion detection. In the past, Port-based and packet inspection methods were commonly used, however due to substantial changes in internet traffic, especially the increased encryption of data, they were declined due to their lack of precision. Researchers recently tested new techniques for traffic classification and recorded a high degree of accuracy via the application of Machine Learning Techniques including Deep Learning. Our goal is to do a State-of-the-art survey to explain these different methods, their advantages, and what results they have reached.

Résumé

La classification du trafic réseau a été étudiée pendant deux décennies et étendue à une grande variété de systèmes, des systèmes de classification QoS et FAI aux pare-feu et à la détection des intrusions. Dans le passé, les méthodes d'inspection basées sur les ports et les paquets étaient couramment utilisées, mais en raison de changements importants dans le trafic Internet, en particulier du cryptage accru des données, elles ont été refusées en raison de leur précision. Les chercheurs ont récemment testé de nouvelles techniques de classification du trafic et enregistré un haut degré de précision via l'application des techniques d'apprentissage automatique et d'apprentissage profond. Notre objectif est de réaliser un état de l'art pour expliquer ces différentes méthodes et leurs avantages, et ce qu'elles ont montré dans ce domaine.

ملخص

تمت دراسة تصنيف حزم بيانات الشبكات لمدة عقدين وتم توسيعه عبر مجموعة متنوعة من الأنظمة بدءًا من أنظمة تصنيف جودة الخدمة ومقدمي خدمات الإنترنت إلى جدران الحماية وكشف التسلل. في الماضي، كانت طرق فحص حزم الانترنت عن طريق البورت شائعة

الاستخدام، و لكن نظرًا للتغيرات الكبيرة التي حدثت على مستوى الانترنت، وخاصة زيادة تشفير البيانات، فقد تم رفضها بسبب عدم دقتها. اختبر الباحثون مؤخرًا تقنيات جديدة لتصنيف هذه البيانات وسجلوا درجة عالية من الدقة من خلال تطبيق تقنيات التعلم الآلي والتعلم العميق. هدفنا هو إجراء بحث على أحدث التقنيات و شرح هذه الأساليب المختلفة و ذكر مزاياها، وما أظهروه في هذا المجال.