جامعة الموصل

كلية الهندسة

حماية تدفقّات البيانات في الشبكات المعَّرفة برمجياً (SDN) باستخدام خوارزميات التعلّم الآلي

حنين رافد محمود

رسالة ماجستير علوم

في الهندسة الكهربائية/ هندسة كهربائية

بإشراف

الأستاذ المساعد الدكتور

محمد يونس ذنون

1444 هـ 2022 م

المستخلص

تعدّ الشبكات المعَّرفة برمجيا Software Defined Network (SDN) من أهم التقنيات الحديثة التي طُبِّقت في السنوات الأخيرة التي لها دور جيد في تطوير شبكات الانترنيت، الا انه ظهرت الحاجة الى تأمين هذه الشبكات بشكل أكبر من ذي قبل، وذلك بسبب المخاطر التي تتعرض لها من قبل مهاجمين محتملين مثل هجمة حجب الخدمة الموزعة Distributed DDOS Denial of Service attack وغيرها من الهجمات، وهدفت هذه الرسالة الى بناء طوبوغرافية لشبكة معرفة برمجيا حاكت واقع حدوث هجمة DDOS على إحدى الحاسبات المرتبطة التي عُدَّت حاسبة ضحية، وتم الكشف عن هجمات DDOS باستخدام خوارزمية آلة متجهات الدعم(SVM) Support Vector Machine وهي إحدى خوارزميات تعلّم الآلة واستخدمت أيضا تقنيات لتخفيف حدة هذه الهجمات، وهي الفحص الدقيق للحزم Deep Packet Inspection لمجموعة بيانات جمّعها مسبقا باحثون في المجال نفسه، فضلاً عن ربط نوعين من المسيطرات المستخدمة في هذه الشبكات، وهما: المسيطر POX، والمسيطر RYU وقورن أداء الشبكة عن طريق قياس كفاءة النقل throughput وزمن الذهاب والإياب Round Trip Timeومقارنة أداء المسيطرين، وخلصت الدراسة الى اختيار RYU بوصفه مسيطراً للدراسة، لأنه أفضل من ناحية كفاءة النقل وزمن الذهاب والإياب في حالة الحمل الهجومي، حيث بلغت كفاءة نقل البيانات قرابة 5237 بت / ثانية عند تشغيل المحاكاة لمدة 5 دقائق للحزم العادية، في حين كان زمن الذهاب والإياب 1218.442 ملي ثانية عند استخدام المسيطر RYU، بينما بلغت كفاءة النقل حوالي 2107 بت/ثانية عند تشغيل المحاكاة لمدة 5 دقائق للحزم العادية، وكان

زمن الذهاب والإياب 13175 ملي ثانية عند استخدام المسيطر POX واسُتعمِلت شفرة برمجية بلغة بايثون، لقياس الدقة ونسبة كشف الهجوم حيث بلغت قيمة الدقِّة لبيانات الاختبار 91.8% ، في حين ساوت نسبة الكشف 100% ،ونسبة الإنذار الكاذب ساوت 0%.

University of Mosul
College of Engineering
Electrical Engineering Department

Protecting Data Flows in Software Defined Networks (SDN) via Machine Learning Algorithms

Haneen Rafid Mahmood

M.Sc Thesis

Electrical Engineering/Electrical Engineering

Supervised by

Asist.prof

Dr.Mohammed Younis Thanoun

1444 A.H **2022 A.D**

Abstract

Networks technology known as software defined networks considered one of the most modern technologies that has been applied in the last years, which had a good rule in developing internet networks, but the need to secure these networks become more argent than before, due to the risks they are exposed to by potential attackers, they use attacks such as DDOS attack and other attacks. In this thesis, a programmatically defined network topography was built and the reality of a DDOS attack was simulated on one of the connected computers that was considered as a victim computer, and DDOS attacks were detected using the (support vector machine (SVM) algorithm). and it is one of Machine learning algorithms and techniques were also used to mitigate these attacks, namely, a deep packet inspection for a previously collected data set by researchers in the same field, and also attached two types of controllers used in these networks, namely the POX controller and the RYU controller, and the network performance was compared by measuring the throughput and round-trIP time and comparing the performance of the controllers. The thesis concluded that RYU was chosen as the controller for the study, as it is better in terms of throughput and round-trIP time in the case of the load attack. Round trIP 1218,442 milliseconds when using RYU Controller, While the throughput was about 2107 bits/sec when running the simulation for 5 minutes for normal load, while the round-trIP time was 13175 milliseconds when using the POX controller, and a Python code was used to measure the accuracy and the detection rate of the attack, where the accuracy value of the test data was 91.8% in While the detection rate is 100% and the false alarm rate is 0%.