Published Researches
الأبحاث المنشورة

Title عنوان البحث	**Detection And Mitigation Of DDOS Attack in SDN Using Machine Learning Algorithms** **كشف وتخفيف هجمات رفض الخدمة الموزعة في الشبكات المعرفة برمجياً باستخدام خوارزميات التعلم الآلي**
Author الناشر	Dr. Mufeed Haddad,Eng.Samera Nezam م .سميرة محمد علي نظام،د.مفيد حداد
Source Title اسم المجلة	Journal of Damascus University
ISSN	1999-7302
Q	
Link رابط البحث من موقع المجلة	
Abstract خلاصة	**The research described software defined networks, which are the future of networks, because they have the ability to provide superior management and better network security and allow us to program the network according to the use of each case, through the controller consider as an operating system for the network infrastructure based on SDN.** **However, software defined networks are still under attacks, and distributed denial-of-service attacks (DDOS) are the most dangerous and threatening attacks for the network, as they can flood the network and lead to blocking access to the server network by sending large numbers of packets and taking advantage of network resources and thus refusing to respond to further received requests.** **The method presented in this work is a combination of statistical analysis and machine learning methods. In the statistical method, 4 features are extracted from the network traffic and aggregated into a data set. This dataset is used to train a machine learning algorithm support vector machine to predict distributed denial-of-service attacks in the network, detect anomaly traffic early, and mitigate it by blocking the source by closing the port.** **This method is implemented using a RYU controller, a mininet emulator with Open flow protocol, the applied SVM machine learning algorithm achieved an accuracy of 99.26% and a detection rate of 100% in detecting and mitigating DDOS attacks within a software-defined networking architecture.** تناولت المقالة وصفاً للشبكات المعرفة برمجياً التي تعد مستقبل الشبكات، لما لديها من القدرة على توفير إدارة فائقة وأمن شبكة أفضل كما تسمح لنا ببرمجة الشبكة وحسب الاستخدام لكل حالة، من خلال وحدة التحكم التي تعد بمثابة نظام تشغيل للبنية التحتية للشبكة القائمة على **SDN**. ومع ذلك، فإن الشبكات المعرفة برمجياً عرضة للهجمات، وأن هجمات رفض الخدمة الموزعة **DDOS** هي أكثر الهجمات خطورة وتهديداً للشبكة، حيث يمكن أن تغمر الشبكة وتؤدي إلى حظر الوصول إلى شبكة الخادم وذلك بإرسال أعداد كبيرة من الحزم والاستفادة من موارد الشبكة وبالتالي رفض الاستجابة لمزيد من الطلبات الواردة. الطريقة المقدمة في هذا العمل هي الجمع بين التحليل الإحصائي وطرق التعلم الآلي. في الطريقة الإحصائية، يتم استخراج 4 ميزات من حركة مرور الشبكة وتجميعها في مجموعة بيانات. تُستخدم مجموعة البيانات هذه لتدريب خوارزمية التعلم الآلي **support vector machine** للتنبؤ بهجمات رفض الخدمة الموزعة في الشبكة واكتشاف حركة مرور الشذوذ مبكرًا وتخفيفها عن طريق حظر المصدر وذلك بإغلاق المنفذ. يتم تنفيذ هذه الطريقة باستخدام وحدة تحكم **RYU**, وبرنامج محاكي للشبكات المعرفة برمجياً **mininet** مع بروتوكول **Open flow**، حققت خوارزمية التعلم الآلي **SVM**المطبقة دقة 98.62٪ ومعدل كشف يبلغ93 ٪ في اكتشاف هجمات **DDOS** والتخفيف من حدتها ضمن بنية الشبكات المعرفة برمجيا".