جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
هندسة الحواسيب والأتمتة

كشف وتخفيف هجمات رفض الخدمة الموزعة في الشبكات المعرفة برمجياً باستخدام خوارزميات التعلم الآلي

Detection And Mitigation Of DDOS Attack in SDN Using Machine Learning Algorithms

سميرة محمد علي نظام

الدكتور المشرف مفيد الياس حداد

الملخص

تناول البحث 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 للتخفيف من آثار هجمات رفض الخدمة الموزعة **DDOS** 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 من نمط **support vector machine** للتنبؤ بهجمات رفض الخدمة الموزعة في الشبكة واكتشاف حركة مرور الشذوذ مبكرًا وتخفيفها عن طريق حظر المصدر وذلك بإغلاق المنفذ.

تم اختبار هذه الطريقة باستخدام وحدة تحكم **RYU**, وبرنامج محاكي للشبكات المعرفة برمجيا **mininet** مع بروتوكول **Open flow**، حققت خوارزمية التعلم الآلي **SVM**المطبقة دقة **98.72%** ومعدل كشف يبلغ **93%**في اكتشاف هجمات **DDOS** والتخفيف من حدتها ضمن بنية الشبكات المعرفة برمجيا".

القسم العملي

تستخدم الطريقة المقدمة كلاً من أساليب التعلم الإحصائي والآلي لاكتشاف والتخفيف من هجمات DDOS في الشبكات المعرفة برمجياً. تتطلب الطريقة التي تم تنفيذها تدريب خوارزمية SVM ML لاكتشاف الهجوم في الشبكة.

يجب أن تقوم وحدة جمع البيانات بجمع بيانات كل من حركة المرور العادية وحركة الهجوم وتخزين البيانات في ملف CSV.

في البداية، يجب جمع بيانات حركة المرور العادية ثم بيانات حركة المرور الهجومية، يوصى بجمع حركة المرور العادية البيانات مرة أخرى بعد بيانات حركة المرور للهجوم من أجل دقة أفضل. يتم جمع البيانات مع الأخذ في الاعتبار جميع المعلمات الإحصائية الأربعة لاستخراج الميزات المحددة في المنهجية وهي سرعة IP المصدر وسرعة إدخالات التدفق ونسبة إدخالات أزواج التدفق وأعداد التدفق. يحدث الاكتشاف والتخفيف بعد جمع البيانات وتعيين وحدة التحكم على حالة الكشف، ثم عند إنشاء حركة المرور العادية، يتم إجراء خوارزمية SVM

يتنبأ بها كحركة مرور عادية وعندما يتم إنشاء حركة مرور الهجوم فإنها تكتشف على الفور حركة المرور على أنها حركة مرور هجوم DDOS، وتحظر المنفذ الذي تأتي منه حركة المرور.

بمجرد حظر المنفذ يتم ضبط وحدة التحكم على 120 ثانية، وبعد ذلك يفتح المنفذ.

ولكن إذا كان الهجوم لا يزال نشطًا، فإنه يكتشف ويمنع المنفذ مرة أخرى لمدة 120 ثانية أخرى. بعد حظر حركة المرور العادية، يُسمح بتدفق حركة المرور في الشبكة من المنافذ الأخرى.

تستمر هذه العملية طالما استمر الهجوم.

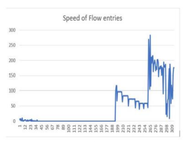
القسم العملي

تحتوي مجموعات البيانات التي تم إنشاؤها أولاً على 600+ عينة من بيانات حركة المرور العادية و300 + عينة من بيانات حركة المرور الهجومية مخزنة لخوارزمية SVM للتدريب والتحليلات للتنبؤ بالهجوم.

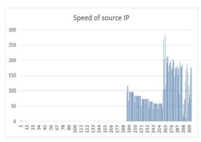
يتم إجراء الاختبارات لمدة 300 ثانية مع فاصل زمني لمدة ثانيتين لتجميع حركة المرور، ويتنبأ SVM بحركة المرور كل ثانيتين.

في هذه التجربة، يتم إرسال حركة المرور العادية من جميع المنافذ ويتم إرسال الهجوم من المنفذ / المضيف 1 في الشبكة مع التقاط حركة المرور الواردة كل 3 ثوانٍ.

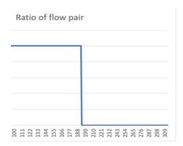
يتم إنشاء هيكل الشبكة باستخدام mininet الذي يحتوي على مفتاح تدفق مفتوح واحد مع 10 مضيفين في الشبكة.



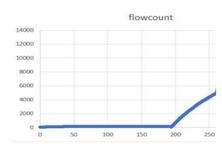
(a) SFE



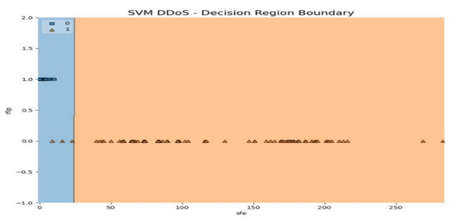
(b) SSP



(a) RFIP



(b) Flowcount



القسم النظري

الشبكات المعرفة برمجياً هي عبارة عن بنية شبكية جديدة توفر تحكم مركزي بكامل الشبكة وتقدم قابلية برمجة غير مسبوقة تتيح لمشغلي الشبكات تكوين وإدارة البنى التحتية بشكل ديناميكي. مع فصل مستويي التحكم والبيانات، يمكن التحكم في الشبكة فقط على مستوى التحكم المركزي. يعمل المتحكم كنظام تشغيل يقوم بإرسال التعليمات وتطبيق التغييرات من خلال الواجهات التخاطبية بينه وبين الأجهزة المسؤول عنها، بالرغم من أن التحكم المركزي هو عبارة عن سمة مميزة جداً في الشبكات المعرفة برمجياً إلا أنه يواجه تحديات خطيرة عديدة، وعلى جميع المستويات. يوجد اليوم العديد من الدراسات التي تهتم بمسائل حماية الشبكات المعرفة برمجياً ولعل أهم الدراسات تلك التي تعمل على تخفيف نقاط الضعف الخاصة بإمكانية حقن تطبيقات خبيثة ضمن الشبكة والقيام بمختلف الهجمات على تجهيزات الشبكة.

فكانت مشكلة البحث تتمثل بالسؤال التالي: كيف يمكن اكتشاف وتحديد صنف هجمات رفض الخدمة الموزعة DDOS ومراقبة تدفق المعطيات ضمن بنية الشبكات المعرفة برمجياً؟

تم التعريف عن هجمات رفض الخدمة الموزعة وأصناف الهجمات وتم تسليط الضوء على مشاكل الأمن في الشبكات المعرفة برمجيا ونقاط الضعف وتم استعراض الدراسات المرجعية في مجال كشف وتخفيف هجمات رفض الخدمة الموزعة في الشبكات المعرفة برمجياً.

النتائج والمناقشة

الشبكات المعرفة برمجياً توفر لنا القدرات لتصميم وتنفيذ العمليات في الشبكة عن طريق البرمجة وهو ما لا ينطبق على الشبكات التقليدية. كان استخدام SDN لاكتشاف هجمات DDOS والتخفيف من حدتها هو الهدف الرئيسي لهذا العمل

الطريقة التي تم تنفيذها هي مزيج من الميزات الإحصائية مثل مصدر IP، وسرعة إدخالات التدفق، وعدد التدفق ونسبة زوج التدفق وخوارزمية التعلم الآلي SVM لاكتشاف هجمات DDOS والتنبؤ بها في الشبكة، وتظهر النتائج المجربة أن طريقة المقدمة يمكن توفر دقة 98.72% ومعدل اكتشاف حركة المرور الضارة بنسبة 93% مع عدم وجود توقعات خاطئة عن حركة المرور (false Alarm). ومع ذلك، فإن الأمان ليس دليلاً كاملاً أبدًا ويمكن دائمًا تحطيمه بنفس الطريقة التي تم تنفيذها بها عيب، يمكن استخدام هجوم من مصادر IP الموثوقة لإرسال حركة مرور ضارة في الشبكة والتي لن يتمكن جهاز SVM من التنبؤ بها.

حاليا 4 ميزات يتم استخدامها في التحليل الإحصائي، علاوة على ذلك يمكن استخراج الميزات واستخدامها باستخدام خوارزمية ML للحصول على تنبؤ أفضل ودقيق لحركة المرور الضارة.

تم إرسال حركة مرور الهجوم من المنفذ 1 مع 10 مضيفين فقط في الشبكة، وأظهرت النتائج التي تم الحصول عليها أن خوارزمية SVM ML حققت دقة 98.72٪ وكانت نتيجة التحقق المتبادل مع بيانات التدريب 99.57% وحركة مرور الهجوم، كان معدل الكشف قريبًا من 93% مع عدم وجود إنذار خاطئ مما يعني أنه لم يتم اعتبار حركة المرور العادية كحركة مرور خبيثة malicious.

المراجع

- C. Dharmadhikari, S. Kulkarni, S .Temkar, S .Bendale" ,A Study of DDoS Attacks in Software Defined Networks" IRJET, Vol. 6 ,Dec. 2019.
- Dehkordi, A. B., Soltanaghaei, M. and Boroujeni, F. Z. (2020). The ddos attacks detection through machine learning and statistical methods in sdn, The Journal of Supercomputing pp. 1–33. JCR Impact Factor.
- Chinmay Dharmadhikari1, Salil Kulkarni2, Swarali Temkar3, Shailesh Bendale4. A Study of DDoS Attacks in Software Defined Networks. International Research Journal of Engineering and Technology (IRJET). Volume 6, Dec 2019.
- Sahoo, K. S., Iqbal, A., Maiti, P. and Sahoo, B. (2018). A machine learning approach for predicting ddos traffic in software defined networks, 2018 International Conference on Information Technology (ICIT), Bhubaneswar, India, India, pp. 199–203. CORE Ranking: C.
- L. Stancu, G. Suciu, S. Halunga and A. Vulpe, "An Overview Study of Software Defined Networking," in IE 2015 International Conference, Rome, 2015.
- K. SrikanthIntellectual History of Programmable Networks," in Newsletter ACM SIGCOMM Computer Communication Review, New York, 2014.
- K. Srikanth, K. Rajasri, S. Kingston and R. Bhaskar, "SDN and OpenFlow A Tutorial," IP Infusion Inc., Santa Clara, 2011.