جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تحسين أمن الشبكات المعرفة برمجيا بالاعتماد على الانتروبية

Improving Security of SDN based on Entropy

رؤى حمدان

د. وسيم السمارة

الملخص

في ظلّ اعتمادنا المتزايد على الأنظمة الرقميّة في أغلب مجالات الحياة، أصبحت الاختراقات الأمنيّة للأنظمة المعلوماتية أكثر خطورة. في الآونة الأخيرة نجد الكثير من الأمثلة عن اختراقات كان لها نتائج مؤثّرة جداً وخاصة في مجالات السّياسة والاقتصاد. كما أتاحت التّقنيات الحديثة في بيئات العمل الفرصة للمزيد من المخاطر الأمنيّة الجديدة بالظهور، بالإضافة إلى ظهور الجيل الجديد من الشّبكات الضخمة التي فرضت نوعاً جديداً من التحدّيات والمخاطر الأمنيّة، يعتمد الحلّ المقترح على منهجيات وخوارزميات الانتروبية ونسبها الموزعة المهتمة بالسّياق وذلك لكشف هجوم منع الخدمة DDOS. حيث نقوم باستخراج معلومات وإحصائيات التدفق التراكمية والعشوائية في إطارات زمنية مختلفة.

القسم النظري

تتألف شبكة SDN من ثلاثة مستويات، مستوي المعطيات الذي يحوي التجهيزات الشبكية المسؤولة عن عمليات التمرير، ومستوي التحكم الذي يتم من خلاله برمجة التجهيزات الشبكية، ومستوي التطبيقات الذي يتم من خلاله إضافة خدمات وتطبيقات جديدة للشبكة،

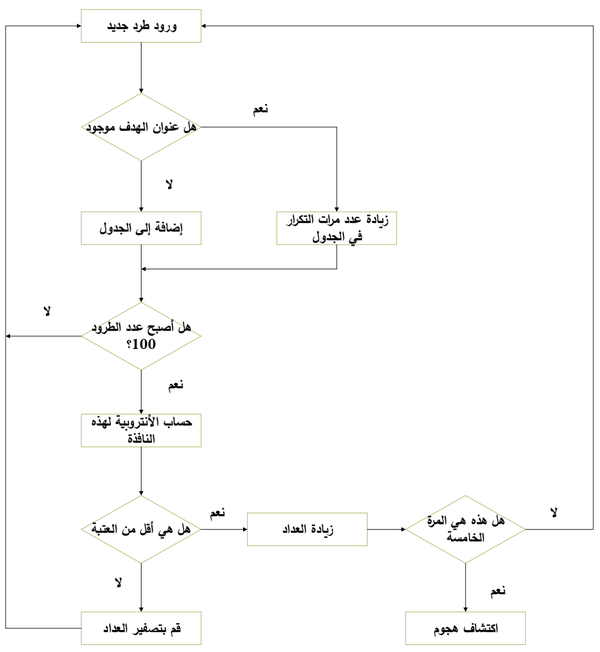
في الحل المطروح، يتم قياس عشوائية الطرود الواردة، حيث تعد الأنتروبية مقياساً جيداً للعشوائية. تقيس الأنتروبية احتمال وقوع حدث مع الأخذ بعين الاعتبار للعدد الكلي للأحداث.

القسم العملي

في شبكة مؤلفة من 64 مضيف 9gHosts مبدلات Switches، فإن جميع المضيفين ينبغي أن يكون لديهم احتمالات متقاربة لاستقبال طرود جديدة واردة، وهذا سيؤدي بشكل منطقي إلى وجود أنتروبية عالية، كما أن ورود طرد جديد، لا يوجد له تطابق مع جدول التسيير في المبدل، يعني أنه سيتم توجيهه إلى المتحكم، وفي حال بدأ مضيف أو عدة مضيفين باستقبال سلسلة متتالية من الطرود الواردة، سوف تتناقص العشوائية وبالتالي ستنخفض الأنتروبية.

$$H = -\sum_{i=1}^{n} \rho_i \, log(\rho_i)$$

القسم العملي



النتائج والمناقشة

إن أفضل اكتشاف للهجوم تم عند معدلات هجوم عالية (معدل هجوم 75%)، ويكمن السبب وراء ذلك في انخفاض قيم الأنتروبية بشكل أكبر كلما ازداد معدل الهجوم سواء كان الهجوم مطبقاً على مضيف وحيد أو كان مطبقاً على شبكة فرعية من أربعة مضيفين.

المراجع

- Allan Friedman, "Cybersecurity and Cyberwar: What Everyone Needs to Know", (2018).
- AXELSSON, S. Aspects of the modelling and performance of intrusion detection. Department of Computer Engineering, Chalmers University of Technology, (2019).
- WHITE, G.; CONKLIN, W. A.; WILLIAMS, D.; DAVIS, R.; COTHREN, C. Principles of Computer Security, CompTIA Security+ and beyond. 3rd edition, McGraw-Hill, 2012, 684.