عنوان الرسالة : الحد من هجمات حجب الخدمه الموزعه في الشبكات المعرفه برمجيا باستخدام تعليم الاله

اسم الطالب : فاطمه رطيان زعل العنزي

اسم المشرف: د. كمال منصور جمبي

المستخلص

الشبكات المعرفة بالبرمجيات (SDN) عرضة للعديد من التهديدات الأمنية. على سبيل المثال، يمكن ان يكون لهجوم رفض الخدمة الموزعة (DDoS) عواقب وخيمة على توافر خدمة الشبكات المعرفة بالبرمجيات. وبالتالي، فإن تطوير حل دفاع ذكي لهذه الهجمات يعد مشكلة بحثية كبيرة. الأساليب الحالية القائمة على طرق الكشف التقليدية معقدة للغاية وتوفر دقة منخفضة وتعميم ضعيف للحل. بالإضافة إلى ذلك، يمكن أن تولد الشبكات المعرفة بالبرمجيات بيانات ضخمه؛ وبالتالي، تفشل الأساليب التقليدية في توفير حلول مرنة. لمعالجة هذه المشاكل وتحسين دقة الكشف عن الهجمات، تقترح هذه الأطروحة نظام اكتشاف لهجمات رفض الخدمة الموزعة والتخفيف من حدتها للشبكات المعرفة بالبرمجيات والذي يعتمد على نموذج التعلم الجمعي العميق.

مر تصميم النظام المقترح بمرحلتين. في المرحلة الأولى، تم تقديم أربعة نماذج من التعلم الجمعي من خلال اعتماد ثلاث تقنيات للتعلم الجمعي وبنيات مختلفة من خوارزميات التعلم العميق وهي الشبكات العصبية الالتفافية، الشّبكة العصبيَّة ذات الذَّاكرة الطَّويلة قصيرة المدى، الشَّبَكَةُ العُصبيَّة ذاتُ البوَّابات وذلك لتحسين تصنيف البيانات المتدفقة المرحلة الثانية هي تصميم النظام المقترح، والذي يتكون من ثلاث وحدات، أي الكشف والتخفيف والمراقبة. تتبنى وحدة الكشف تقنية التصويت للتعلم الجمعي والشبكات العصبية التلافيفية (CNN) والتي تم ترشيحهم من المرحلة الأولى.

تم تقييم نموذج التعلم الجمعي العميق المقترح على مجموعات البيانات المعيارية والتي تسمى (CICDDoS2019) و (CICIDS2017) و بيانات فعليه من (SDN). بالإضافة إلى ذلك، قمنا بتقييم النظام المقترح في محاكاة للشبكة المعرفة برمجيا في الوقت الفعلي. تم مقارنة النهج المقترح بأحدث الأساليب الأخرى من أدبيات امن الشبكات. توضح النتائج التجريبية أن نموذج التعلم الجمعي المقترح يمكنه تحديد هجمة رفض الخدمة الموزعة بدقة عالية ومعدل منخفض من الإنذارات الكاذبة. استنادًا إلى النتائج التي توصلنا إليها، نستنتج أن النظام المقترح لديه إمكانات كبيرة لبناء حلول دفاعية لهجوم رفض الخدمة الموزعة في بيئات الشبكات المعرفة بالبرمجيات.

Thesis title: DISTRIBUTED DENIAL OF SERVICE ATTACK MITIGATION USING MACHINE LEARNING IN SOFTEWARE DEFINED NETWORKS

Students name: Fatmah Rtian Alanazi

Supervisor Name: Prof. Kamal Jambi

Abstract

Software-defined networks (SDN) are susceptible to several security threats. For example, distributed denial of service (DDoS) can have devastating consequences in terms of SDN availability. Thus, developing an intelligent DDoS defense solution is a significant research problem. Existing approaches based on traditional detection methods are highly complex and provide low accuracy and poor solution generalization. In addition, SDNs can generate large-scale data; thus, traditional approaches fail to provide flexible solutions. To address these problems and improve attack detection accuracy, this thesis proposes a DDoS detection and mitigation system for SDNs that is based on a deep ensemble learning model.

The proposed system design went through two phases. In the first phase, four ensemble models are presented by adopting three ensemble techniques and different DL architectures, namely convolutional neural network, long short-term memory, and gated recurrent unit, to improve the SDN traffic classification. The second phase is the proposed system design, which comprises three modules, i.e., detection, mitigation, and monitoring. The detection module adopts the voting ensemble technique and convolutional neural networks (CNN) which were selected from phase one.

The proposed deep ensemble learning model was evaluated on flow-based public datasets called CICDDoS2019 and CICIDS2017 and real SDN traffic data. In addition, we evaluated the proposed system in an SDN simulation in real-time. We compared the proposed approach to other state-of-the-art approaches from the network security literature. Experimental results demonstrate that the proposed ensemble model can identify DDoS attacks with high accuracy and a low rate of false alarms. Based on our findings, we conclude that the proposed system has significant potential to build defense solutions for DDoS attack in SDN environments.