Republic of Yemen
Ministry of Higher Education and Scientific Research
University of Science and Technology
Deanship of Postgraduate Studies and Scientific Research

Hybrid Machine Learning Algorithm to Detect DDoS Attacks in Software Defined Networks

A Thesis Submitted by

Ahmed Mohammed Ahmed Saad Al-Bakali

To

The Council of Postgraduate Studies and Scientific Research, in Partial Fulfillment of the Requirements for the Master Degree of Computing in Computer Networks

Supervisor

Prof. Dr. Abdullatif Saleh Nasser Ghallab

Associate Professor of Computer Science

University of Science and Technology

December, 2024AD **Sana'a** **Jumada II, 1446AH**

Republic of Yemen
Ministry of Higher Education and Scientific Research
University of Science and Technology
Deanship of Postgraduate Studies and Scientific Research

Hybrid Machine Learning Algorithm to Detect DDoS Attacks in Software Defined Networks

Abstract

The distributed denial of service (DDoS) attack can be considered one of the most dangerous and costly digital threats on computer networks. The network is monitored by software-defined networking (SDN) and emerging technology that provides a network architecture to separate the control plane from the data plane. This research presents a proposed solution aimed at addressing this type of attack by effectively monitoring and detecting the targeted traffic. The detection of DDoS attacks is performed by hybridizing two machine learning algorithms, support vector machine, and K-nearest neighbors call (HKSVM). This research was applied on InSDN and SDN datasets with 18 features. The experiments showed that the average accuracy rate (ACC) of the HKSVM is approximately 99% with a small amount of total flux. The results show that the HKSVM was an effective method for detecting DDoS in SDN as performed the best.

Keywords: Hybrid Algorithms, Machine Learning, DDoS Attacks, SDN, Detection Method.

Candidate

Ahmed Mohammed Ahmed Saad Albakali

Supervisor

Prof. Dr. Abdullatif Saleh Nasser Ghallab
Associate Professor of Computer Science
University of Science and Technology

December, 2024AD **Sana'a** **Jumada II, 1446AH**

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

خوارزمية التعلم الآلي الهجينة لاكتشاف هجمات رفض الخدمة الموزعة في الشبكات المعرفة بالبرمجيات

المُلخص

يمكن اعتبار هجوم رفض الخدمة الموزع (DDoS) أحد أخطر التهديدات الرقمية وأكثرها تكلفة على شبكات الكمبيوتر. حيث تتم مراقبة الشبكة عن طريق الشبكات المعرفة بالبرمجيات (SDN) وهي التكنولوجيا الناشئة التي توفر بنية شبكة لفصل مستوى التحكم عن مستوى البيانات. اقترح هذا البحث حلاً للتغلب على هذا النوع من الهجوم لرصد واكتشاف حركة المرور التي تتعرض للهجوم. يتم إجراء تحليل الشبكة عن طريق تهجين خوارزميتين للتعلم الآلي، وهي خوارزمية الـ (SVM) وخوارزمية أقرب جيران (KNN) تسمى (HKSVM). تم تطبيق هذا البحث على مجموعات بيانات (InSDN) و(SDN) مع 18 عددًا من الخصائص. أظهرت التجارب أن متوسط معدل الدقة (ACC) للطريقة المقترحة هو 99٪ مع قدر ضئيل من التدفق الكلي. أثبتت النتائج أن (HKSVM) كانت طريقة فعالة لاكتشاف DDoS في بيئة الـ SDN حيث كان الأداء الأفضل.

الطالب

أحمد محمد أحمد سعد البكالى

المشرف

أ.د. عبد اللطيف صالح ناصر غلاب

أستاذ علوم الحاسوب المشارك

جامعة العلوم والتكنولوجيا

ديسمبر، 2023م **صنعاء** **جمادي الثاني ، 1446هـ**

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

خوارزمية التعلم الآلي الهجينة لاكتشاف هجمات رفض الخدمة الموزعة في الشبكات المعرفة بالبرمجيات

رسالة مقدمة من الطالب

أحمد محمد أحمد سعد البكالي

إلى

مجلس الدراسات العليا والبحث العلمي، وهي جزء من متطلبات الحصول

على درجة الماجستير في الحوسبة – شبكات الحاسوب

المشرف

أ.د. عبد اللطيف صالح ناصر غلاب
أستاذ علوم الحاسوب المشارك
جامعة العلوم والتكنولوجيا

ديسمبر، 2024م صنعاء جمادي الثاني، 1446هـ