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

Entropy-Based DDoS Detection Models in an Unequal Access Software Defined Network

A Thesis Submitted by

Arafat Alawi Saleh Al-Hawshabi

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. Belal Abdullah Rassea Al-Fuhaidi

Professor of Networking and Communication Engineering

University of Science and Technology

May, 2026AD **Sana'a** **Dhul-Qidah, 1447AH**

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



Entropy-Based DDoS Detection Models in an Unequal Access Software Defined Network

Abstract

Distributed Denial-of-Service (DDoS) attacks represent a persistent and significant threat to Software-Defined Networking (SDN), especially within unequal-access environments characterized by inherently imbalanced traffic distributions among hosts. In these scenarios, conventional entropy-based detection methods particularly those utilizing Shannon's entropy face substantial limitations due to pronounced traffic variability, undermining the reliability and consistency of detection thresholds. To effectively address these challenges, this research proposes two novel entropy-based detection models designed to enhance both detection accuracy and entropy stability: the ATHA-EM and the HAMMA-EM. Each model integrates a specialized preprocessing algorithm with Shannon entropy, forming lightweight yet robust frameworks for effective DDoS detection. The first model, ATHA-EM, employs the ATHA Algorithm to harmonize synthetic traffic flows with real traffic across network hosts, thereby producing entropy measurements that remain comparable and consistent across hosts. This harmonization significantly mitigates entropy inconsistencies caused by baseline unequal access among hosts. ATHA-EM achieves Bhattacharyya Coefficient (BC) similarity scores in the range of 0.61–0.99 compared to the equal-access baseline. However, it does not fully reduce entropy fluctuations, which may compromise detection precision. To overcome this limitation, the second model, HAMMA-EM, integrates the HAMMA Algorithm with Shannon's entropy to effectively stabilizing entropy values and mitigating fluctuations under unequal traffic conditions. The

HAMMA Algorithm is constructed by integrating AMMA through The ATHA Algorithm, The AMMA algorithm operates through three complementary mechanisms: MDRTF, which normalizes drop behavior across overall traffic, a shrinking-window mechanism that progressively suppresses dominant high-frequency effects, and a cumulative mean of means that stabilizes evolving drop-ratio behavior. Together, these mechanisms effectively mitigate residual entropy fluctuations. Empirical evaluations show that HAMMA-EM improves BC similarity to the equal-access baseline into the 0.93–0.9991 range, enabling a unified, reliable detection threshold. It also achieves Detection Rate (DR) by approximately 96%. Comprehensive evaluations across both equal and unequal access SDN scenarios validate the effectiveness of both models. While ATHA-EM significantly enhances entropy consistency, HAMMA-EM provides superior stability and detection performance, making it a scalable and resilient solution for DDoS mitigation in heterogeneous SDN environments.

Candidate
Arafat Alawi Saleh Al-Hawshabi

Supervisor
Prof. Belal Abdullah Rassea Al-Fuhaidi
Prof. of Networking and Communication Engineering
University of Science and Technology

May, 2026AD **Sana'a** **Dhul-Qidah, 1447AH**

الجمهورية اليمنية
وزارة التربية والتعليم والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

نماذج مبتكرة معتمدة على الانتروبي لاكتشاف هجوم رفض الخدمة الموزع في الشبكات المعرفة برمجيا ذات الوصول غير المتساوي

الملخص

تُعدّ هجمات رفض الخدمة الموزعة (DDos) من التهديدات المستمرة والخطيرة على الشبكات المعرفة برمجيًا (SDN)، ولا سيما في البيئات غير المتكافئة من حيث الوصول، والتي تتسم بتوزيع غير متوازن لحركة المرور الخاصة بالمضيفات المتصلة عبر المتحكم (SDN Controller) في مثل هذه البيئات. وتواجه أساليب الكشف المعتمدة على الانتروبي قيودًا كبيرة نتيجة التغيرات الملحوظة في حركة المرور، مما يؤثر على موثوقية قيمة الكشف (Threshold). ولمواجهة هذه التحديات بفاعلية، تقترح هذه الدراسة نموذجين جديدين للكشف المعتمد على الانتروبي، يهدفان إلى تعزيز دقة الكشف واستقرار قيم الانتروبي. يتمثل هذان النموذجان في نموذج الانتروبي لخوارزمية التوافق التكيفي لحركة المرور (ATHA-EM)، ونموذج الانتروبي لمتوسط التوافق التكيفي لحركة المرور (HAMMA)؛ حيث يدمج كل منهما خوارزمية معالجة مسبقة مع شانون انتروبي لتشكيل أطر عمل خفيفة الوزن وفعّالة في اكتشاف الهجمات. ويستخدم النموذج الأول (ATHA-EM) خوارزمية (ATHA) لتنسيق ومواءمة تدفق البيانات الوهمية مع نسب الوصول الحقيقية بين مضيفات الشبكة، مما ينتج عنه قياسات انتروبي أكثر دقة وإمكانية للمقارنة بين المضيفات. ويسهم هذا التوافق في تقليل التباين الناتج عن عدم المساواة في قدرات الوصول بين المضيفات، حيث حقق النموذج الأول معامل تشابه باتشاريا (BC) 0.81-0.99 مقارنة ببيئة الوصول المتساوية. ومع ذلك، لا يُلغي هذا النموذج التقلبات القصيرة في قيم الانتروبي، الأمر الذي يؤثر على دقة الكشف. ولمعالجة هذا القصور، دمج النموذج الثاني (HAMMA) خوارزمية (AMMA) مع خوارزمية (ATHA) لتشكيل خوارزمية (HAMMA)، والتي تستخدم استراتيجية النوافذ المتناقصة (Sliding Windows) لإعادة حساب معدلات الانخفاض بشكل تكيفي، مما يؤدي إلى استقرار قيم الانتروبي وتقليل التقلبات الناتجة عن عدم توازن حركة المرور، وبالتالي ضمان سلوك متسق للانتروبي. وقد أظهرت التقييمات التجريبية أن نموذج الهاما (HAMMA-EM) حسّن معامل تشابه باتشاريا بين المضيفات المتصلة بالمتحكم مع بعضها البعض حيث حقق معامل تشابه باتشاريا 0.93-0.98 ، مما أتاح قيمة كشف (Threshold) موحدة وموثوقة ، كما حقق معدل كشف إيجابي بلغ (96%). وتؤكد هذه النتائج فعالية النموذجين المقترحين في بيئات الوصول المتساوية وغير المتساوية؛ فبينما يعزز النموذج الأول (ATHA-EM) اتساق الانتروبي بشكل ملحوظ، يوفر النموذج الثاني استقرارًا وأداءً أعلى في الكشف، مما يجعله حلًا قابلًا للتوسع وفعّالًا في لكشف هجمات رفض الخدمة الموزعة (DDoS) في بيئات الوصول غير المتساوية.

الطالب

عرفات علوي صالح الحوشبي

المشرف

أ.د. بلال عبدالله راصع الفهيدي

أستاذ هندسة الاتصالات والشبكات
جامعة العلوم والتكنولوجيا

مايو، 2026م **صنعاء** **ذو القعدة، 1447هـ**

الجمهورية اليمنية
وزارة التربية والتعليم والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

نماذج مبتكرة معتمدة على الانتروبي لاكتشاف هجوم رفض الخدمة الموزع في الشبكات المعرفة برمجيا ذات الوصول غير المتساوي

رسالة مقدمة من الطالب

عرفات علوي صالح الحوشبي

إلى

مجلس الدراسات العليا والبحث العلمي وهي جزء من متطلبات الحصول على درجة الماجستير في الحوسبة ـ شبكات الحاسوب

المشرف

أ.د. بلال عبدالله راصع الفهيدي

أستاذ هندسة الاتصالات والشبكات
جامعة العلوم والتكنولوجيا

مايو، 2026م **صنعاء** **ذو القعدة، 1447هـ**