جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

# تطوير طرائق وخوارزميات لتخفيف آثار هجمات الحرمان من الخدمة باستخدام تقنيات تعلم الآلة

# Developing methods and algorithms to reduce the effects of Denial of service attacks using machine learning techniques

م. سامر ممتاز سليمان
أ. م. د. وسيم السمارة
د. رأفة خازم

## الملخص

تعد مشكلة هجمات الحرمان من الخدمة من المخاطر التي تهدد الشبكات الحاسوبية منذ زمن طويل. على الرغم من صعوبة القضاء على هجمات الحرمان من الخدمة بشكل نهائي إلا أنه من الممكن التخفيف من آثارها وقد شاع استخدام عدة طرق ومنها طرق تعلم الآلة.

تم في هذا البحث دراسة هجمات الحرمان من الخدمة رياضياً وعملياً واقتراح طرق للتخفيف من آثارها، حيث تم استخدام تقنيات تعلم الآلة في كشف الهجمة بشكل عملي ومن ثم توظيف آلية الكشف هذه بإحدى الطرق لعزل المهاجم ضمن الشبكة أما الطريقة الأخرى فقد ركزت على إبقاء الخدمة متاحة للمستخدمين في ظل هجمة الحرمان من الخدمة.

## القسم النظري

يتضمن الجزء النظري من هذا البحث دراسة هجمات الحرمان من الخدمة ونماذجها الرياضية. كما يتضمن مناقشة فكرة المسؤولية المشتركة بين المستخدمين النهائيين ومزودي خدمات الانترنت في كشف والتصدي للهجمات.يتضمن البحث دراسة مجموعة من طرائق تعلم الآلة وتوظيفها في كشف هجمات الحرمان من الخدمة كما يتطرق البحث إلى مسألة تغير قيمة معدل التعلم أثناء التدريب والتي تؤثر على عملية التدريب للشبكات العصبونية العميقة.

## القسم العملي

يتضمن البحث مايلي:

- ❖ استخدام مجموعة من نماذج التعلم الإشرافي في كشف هجمات الحرمان من الخدمة.
- ❖ استخدام التعلم العميق في كشف هجمة الحرمان من الخدمة واقتراح طريقة جديدة لضبط أحد بارامترات عملية التدريب.
- ❖ اقتراح طريقة تعاونية لعزل المهاجمين أثناء حدوث هجمة الحرمان من الخدمة
- ❖ اقتراح طريقة تستخدم التضحية بالموارد بشكل فعال للحفاظ على الخدمة للمستخدمين الحقيقيين فقط أثناء الهجمات.

## النتائج والمناقشة

1. على الرغم من قيمة الدقة العالية التي تنتج عن تدريب نماذج التعلم الإشرافي لكشف هجمات الحرمان من الخدمة باستخدام مجموعات المعطيات الشهيرة إلا أنّ هذه الدقة لم تكن فعلية في الاختبار ضمن بيئة المحاكاة.
2. أداء النماذج الناتجة عن التعلم العميق لكشف هجمات الحرمان من الخدمة أفضل من نماذج التعلم الإشرافي وذلك باستخدام مجموعات المعطيات وضمن بيئة المحاكاة.
3. أضفت الطريقة التعاونية بين مزودات خدمة الانترنت إمكانية عزل هجمة الحرمان من الخدمة خلال فترة زمنية بلغت وسطياً على شبكة مختبرة حوالي 34 ثانية إلا أنّ هذه الطريقة تعاني من مشكلة التزايد الكبير في عدد الرسائل مع نمو الشبكة.
4. أدى الاعتماد على التغيير المتكيف لقيمة معدل التعلم أثناء تدريب الشبكة العصبونية العميقة إلى الوصول إلى قيمة دقة مقبولة في الكشف وباختصار لعدد دورات التدريب بلغ 75% تقريباً من عدد دورات التدريب الإجمالي.

## المراجع


- Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. Journal of Applied Science and Education (JASE), 1-20.
- Tushar Sharma, Maria Kechagia, Stefanos Georgiou, Rohit Tiwari, Indira Vats, Hadi Moazen, Federica Sarro, A survey on machine learning techniques applied to source code, Journal of Systems a Software, Volume 209, 2024, 111934, ISSN 0164-1212 , https://doi.org/10.1016/j.jss.2023.111934.(https://www.sciencedirect.com/science/article/pii/S0164121223003291)
- Zulu, N., Plessis, D. P. D., Mathonsi, T. E., & Tshilongamulenzhe, T. M. (2023). “A User-Based Authentication and DoS Mitigation Scheme for Wearable Wireless Body Sensor Networks”. arXiv preprint arXiv:2303.14441