



Published Researches الأبحاث المنشورة



Title عنوان البحث	تقييم فعالية التصنيف باستخدام نماذج التعلم ذي الإشراف في حل مشكلة هجمات الحرمان من الخدمة	تخفيف أثر هجمات الحرمان من الخدمة باستخدام طريقة تعاونية بين مزودات خدمة الانترنت
Author الناشر	م. سامر سليمان- د. وسيم السمارة - د. رافة خازم	م. سامر سليمان- د. وسيم السمارة - د. رافة خازم
Source Title اسم المجلة	مجلة جامعة دمشق للعلوم الهندسية	مجلة جامعة دمشق للعلوم الهندسية
ISSN	1999-7302	1999-7302
Q		
Link رابط البحث من موقع المجلة	https://journal.damascusuniversity.edu.sy/index.php/engj/authorDashboard/submission/10270	https://journal.damascusuniversity.edu.sy/index.php/engj/authorDashboard/submission/9330
Abstract خلاصة	<p>شاع استخدام تعلم الآلة في العديد من المجالات في أيامنا هذه. وقد أدى التطور السريع لهجمات الحرمان من الخدمة إلى إبطال وسائل الحماية التقليدية للشبكات فيما يتعلق بهجمات الحرمان من الخدمة. يقترح العديد من الباحثين أن تعلم الآلة تقنية واعدة في مجال مكافحة هجمات الحرمان من الخدمة وتحديداً بتركيزهم على استخدام طرائق التعلم ذي الإشراف لإثبات نظريتهم. من المتوقع أن ينجح استخدام التصنيف في كشف هجمات الحرمان من الخدمة وخصوصاً أنه كانت نتائجه جيدة في مرحلة التدريب والاختبار إلا أنها لم تكن كذلك في التجارب المنجزة في الحياة العملية. قمننا في هذا البحث ببناء سبعة نماذج مختلفة للتصنيف بالاعتماد على مجموعتي المعطيات CSE-2018 و NSL-KDD واختبارها ضمن بيئة المحاكاة OMNET++ نظراً لعدم إمكانية تنفيذ هذه الاختبارات ضمن شبكة حقيقية. وجدنا فجوة كبيرة بين الدقة النظرية وتلك الناتجة في عملية المحاكاة. يعزى إلى مشكلة الانزياح التبايني. من الممكن أن التصنيف التقليدي غير ملائم لحل مثل هذه المشكلة حيث تم اقتراح نماذج أخرى ليتم اختبارها في الدراسات المستقبلية.</p>	<p>تطورت وسائل التصدي لهجمات الحرمان من الخدمة خلال السنوات الماضية وقد تم الاعتماد على العديد من التقنيات الحديثة في تطوير آليات حماية محلية تساعد في التخفيف من شدة هذه الهجمات وتعزز من أمن الشبكات بشكل عام. على الرغم من أن استخدام التقنيات الحديثة ساهم في تخفيف الآثار السلبية لبعض أنواع الهجمات إلا أن هذه المحاولات الفردية قد لا تثمر حلاً فعالاً للتصدي للهجمات وإنما يجب العمل على تطوير حلول تعاونية بين عدة جهات للتخفيف من أثر هذه الهجمات. تم في هذه الدراسة استخدام بنية معطيات يتم تبادلها بين أجهزة الشبكات المختلفة والتي تتضمن معلومات خاصة بالهجمات التي يتم اكتشافها وتعميمها على جميع الأجهزة ضمن الشبكة وكأنها عملية وشاية، تحقق الطريقة المقترحة حلاً رادعاً عن طريق عزل كامل التجهيزات الشبكية التي تشارك بهجمات الحرمان من الخدمة حتى ولو لم تتعاون جميع التجهيزات في التصدي للهجمات وذلك عبر تبادل بنية معطيات DoSGoS بين التجهيزات المختلفة. أظهرت النتائج تحسناً في تخفيف أثر هجمات الحرمان من الخدمة عبر عزل المهاجمين مهما كان نوع الهجمة المستخدمة وضمن وقت مقبول انطلاقاً من بدء الهجمة.</p>