نظام رقابي قائم على الشبكات المعرفة بالبرمجيات في مراكز البيانات

المستلخص

تعد الشبكات المعرفة بالبرمجيات (SDN) أحد الحلول الواعدة للمستقبل حيث تقوم بتغيير بنية الشبكة التقليدية عن طريق نقل جميع وظائف التحكم إلى موقع واحد. وهو مفضل على نطاق واسع لأنه يمكن إدارته مركزيًا وتكوينه برمجيًا. ومع ذلك ، فإن المركزية في SDN عرضة لهجمات مثل رفض الخدمة (DoS) ، ورفض الخدمة الموزعة (DDoS) ، ومسح المنفذ ، وحشد الفلاش ، وما إلى ذلك. في هذه الرسالة ، حاولنا اكتشاف هجوم DDoS باستخدام التعلم العميق و سد الفجوة بالتركيز على الجانب الشرعي لشبكة SDN لبيئات مراكز البيانات. يتكون المخطط المقترح من العقد المحمولة ، ووحدة التحكم في الرأس ، ومحرك الكشف ، ووحدة تحكم المجال ، ووحدة تحكم المصدر ، ومركز السحابة. يتم تحليل الحزم الضارة على أنها خطيرة(في هذه الحالة ، قم بتسجيل حركة المرور كأدلة إجرامية لتتبع المجرم ، وإضافة مصدر IP للحزمة إلى القائمة السوداء ، وحظر جميع الحزم من هذا المصدر)أو غير خطيرة (في هذه الحالة ، حظر جميع الحزم من العقدة المصدر لهذه الجلسة). يتم إرسال الحزم غير الضارة باستخدام البروتوكول المقترح. بشكل عام ، تم تقييم هذه الدراسة في بيئة محاكاة OMNET ++ للمقاييس مثل فقدان الحزمة ، ووقت التنفيذ ، والإنتاجية ، والتأخير من النهاية إلى النهاية ، واستهلاك الطاقة ، والدقة ، والوقت المستغرق للكشف عن الهجوم. وأخيرًا ، تشير النتائج المكتسبة إلى نجاحها مقارنة بالنهج الحالية

إسم الطالب :

زكريا محمد إبراهيم عريبي

إسم المشرف :

د.بندر أحمد الزهراني .