Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science and
Mathematics
Department of Computer Science

Security Reinforcement of Real time SDN-IoT

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
as a Partial Fulfillment of Requirements
for the Degree of Master of Science
in
Computer Science**

by

Mahmood Mohammed M. Abdal

Supervised by

Prof.Dr.Dhuha Basheer Abdullah Albazaz

2023 A.D. **1445 A.H.**

Abstract

The Internet of Things (IoT) refers to the network of connected devices, vehicles, and physical objects with sensors, and internet access. However, IoT devices often have resource constraints such as limited processing, memory capacity, and energy supply, making it difficult to implement robust security measures. This vulnerability makes them attractive targets for cybercriminals, particularly for distributed denial of service (DDoS) attacks. A DDoS attack is an effort to interrupt regular service by flooding servers, services, or networks with excessive traffic to disrupt regular service. These attacks can occur sporadically or irregularly and without any pattern.

To address these challenges, a Software Defined Network (SDN) model is proposed. This model leverages SDN techniques to enhance real-time security in IoT environments. It identifies and mitigates DDoS attacks by monitoring network traffic and analyzing packets in real time. By extracting the source IP and MAC addresses and storing them in a dictionary. IP-MAC address mapping serves to identify potential security threats within the network. When more than one IP address are detected using the same MAC address, it raises concerns about malicious activities like spoofing or concealing the true source of attack traffic. The proposed system consists of a controller, computers, and switches connected simultaneously. The controller is programmed to dynamically reconfigure network policies and routing rules to drop malicious packets. The Python language is used for the implementation, with Mininet used for network emulation and the RYU controller managing and controlling the network devices.

This SDN model offers advantages over traditional solutions such as centralized control, programmability, automation, scalability, and traffic optimization. To evaluate its effectiveness, extensive emulation is conducted under various attack scenarios, such as TCP_SYN flooding, which needs 3 seconds to frustrate it. A UDP flooding attack needs 4 seconds to frustrate the attack. The results show that the model significantly reduces the impact of DDoS attacks on IoT. It can identify and mitigate DDoS attacks in real-time within a few seconds, ensuring stable bandwidth for legitimate users even during such malicious activities and ensuring stable CPU consumption during attacks (19% under the TCP_SYN attack and 18.9% under the UDP attack). The model drops a large number of flooding packets through switch-based rules, about 6709204 packets were dropped through the UDP attack, and 6487795 packets were dropped through the TCP_SYN attack.

وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

تعزيز الأمن في الزمن الحقيقي للشبكات المعرفة برمجيا مع انترنت الأشياء

رسالة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة ماجستير علوم في
علوم الحاسوب
من قبل

محمود محمد محمود عبدال

بإشراف
الاستاذ الدكتور ضحى بشيرعبدالله البزاز

١٤٤٥هـ ٢٠٢٣م

الملخص

يتم استخدام عبارة "إنترنت الأشياء" للإشارة إلى شبكة من الأجهزة والمركبات والأشياء المادية الأخرى التي تحتوي على أجهزة استشعار وبرامج ووصول إلى الإنترنت. تنشأ قيود الموارد في أجهزة إنترنت الأشياء من المعالجة المحدودة، وسعة الذاكرة، وإمدادات الطاقة. هذه القيود تجعل من الصعب تنفيذ تدابير أمنية قوية على هذه الأجهزة. ونتيجة لذلك، تصبح أهدافًا ضعيفة لمجرمي الإنترنت الذين يتطلعون إلى استغلال نقاط الضعف. يعد هجوم حجب الخدمة الموزع محاولة لمقاطعة الخدمة العادية عن طريق إغراق خادم أو خدمة أو شبكة بكمية زائدة من حركة المرور. يمكن تصنيف هجوم DDoS على أنه مهمة متقطعة تحدث بشكل غير منتظم، دون أي انتظام أو نمط معين.

ولمواجهة هذه التحديات، تم اقتراح نموذج الشبكة المعرفة برمجيا (SDN). يستفيد هذا النموذج من تقنيات SDN لتعزيز الأمان في الزمن الحقيقي في بيئات إنترنت الأشياء. فهو يحدد ويخفف من هجمات DDoS من خلال مراقبة حركة مرور الشبكة وتحليل الحزم في الزمن الحقيقي. عن طريق استخراج عنوان IP وMAC للمصدر وتخزينها في القاموس. يخدم تعيين عنوان IP-MAC على تحديد التهديدات الأمنية المحتملة داخل الشبكة. عندما يتم اكتشاف أكثر من عنوان IP واحد يستخدم نفس عنوان MAC، فإن ذلك يثير مخاوف بشأن الأنشطة الضارة مثل الانتحال أو محاولات إخفاء المصدر الحقيقي لحركة مرور الهجوم. يتكون النظام المقترح من المتحكم، أجهزة كمبيوتر واجهزة توجيه متصلة ببعضها البعض في آن واحد. تمت برمجة المتحكم لإعادة تكوين سياسات الشبكة وقواعد التوجيه ديناميكيًا لإسقاط الحزم الضارة. تم استخدام لغة Python للتنفيذ، مع استخدام Mininet لمحاكاة الشبكة، والمتحكم RYU لإدارة أجهزة الشبكة والتحكم فيها.

يوفر نموذج SDN مزايا متعددة مقارنة بالحلول التقليدية مثل التحكم المركزي وقابلية البرمجة والأتمتة وقابلية التوسع وتحسين حركة المرور. ولتقييم فعاليته، تم إجراء محاكاة في ظل سيناريوهات هجوم مختلفة، مثل هجوم TCP_SYN flooding، احتاج النموذج المقترح إلى 3 ثوان لإحباطه. وهجوم UDP flooding، احتاج 4 ثوان لإحباط الهجوم. تظهر النتائج أن هذا النموذج يقلل بشكل كبير من تأثير هجمات DDoS على إنترنت الأشياء، ويكتشف ويخفف هجوم DDoS في الزمن الحقيقي بعد بضع ثوانٍ، ويظل النطاق الترددي متاحًا ومستقرًا للمستخدمين الشرعيين حتى أثناء مثل هذه الأنشطة الضارة، ويضمن النموذج المقترح استهلاكًا مستقرًا لوحدة المعالجة المركزية أثناء الهجوم 19٪ تحت هجوم TCP_SYN و18.9٪ تحت هجوم UDP. ويتم إسقاط معظم حزم الإغراق من خلال استخدام القواعد المضافة في اجهزة التوجيه، تم اسقاط حوالي 6709204 حزمة خلال هجوم UDP و6487795 حزمة خلال هجوم TCP_SYN.