المستخلص

أثرت إنترنت الأشياء على العديد من جوانب حياتنا لأنها أصبحت نوع جديد من نماذج الشبكات منتشر على نطاق واسع. في الوقت الحاضر، يتم استخدام إنترنت الأشياء في العديد من المجالات مثل المدن الذكية والمنزل الذكي والصحة الذكية وما إلى ذلك. يواجه هذا النمو السريع في استخدام إنترنت الأشياء العديد من الصعوبات المتعلقة بأمن أجهزة إنترنت الأشياء والشذوذ الشبكي يأتي في مقدمة هذه الصعوبات. لذلك أصبح استخدام نظام التخفيف من الشذوذ الشبكي ضرورة ملحة كأداة دفاع لشبكات إنترنت الأشياء من أجل حماية الأجهزة من المستخدمين الضارين. وقد قدمت الدراسات السابقة العديد من الحلول المقترحة للتخفيف من الشذوذ في شبكات إنترنت الأشياء في جانب الحوسبة السحابية. وبالرغم من ذلك فإن التخفيف من الهجمات مثل هجمات الحرمان من الخدمات الموزعه لايزال يواجه تحديات بسبب تشابه تدفق حركة مرور هجمات الحرمان من الخدمات مع تدفق حركة المرور العادي وكذلك بسبب أن نظام التخفيف في أغلب الدراسات يكون في جانب الحوسبة السحابية. وفي هذا البحث، تم وضع نظامنا المقترح على مستوى الحوسبة الضبابية لمراقبة سير المرور واكتشاف الهجوم في مرحلة مبكرة. تتمثل إحدى السمات الهامة لنظامنا في أن له القدرة على معالجة أثر إنترنت الأشياء بطريقة مختلفة لأن اهتمامنا يتركز على الهجمات الناتجة عن أجهزة إنترنت الأشياء. لرصد الهجوم واكتشافه، استخدمنا طريقة الكشف الإحصائي التي تراقب العملية بمرور الوقت وتطلق إنذار إذا تم الكشف عن سلوك غير طبيعي. ولذلك تم وضع حلنا المقترح على حافة شبكة إنترنت الأشياء(عند الحوسبة الضبابية بدلاً من الحوسبة السحابية). يعد هذا أمراً مهماً للتغلب على قيود أنظمة هجمات الحرمان من الخدمات الموزعه الموجودة والتي تقع غالباً على الجانب القائم على السحابة، وبالتالي من المحتمل أن تفشل في مواجهة هجمات الحرمان من الخدمات شديدة الكثافة. يقوم نظامنا بالتفريق بين مسار إنترنت الأشياء و المسار القياسي، ويتم مراقبة كل مسار بواسطة محرك كشف مختلف. يتمتع المحرك الذي يعالج مسار إنترنت الأشياء بحساسية كشف أعلى مقارنة بالمحرك الذي يتعامل مع المسار القياسي. يستخدم كل محرك طريقة الكشف الإحصائي للكشف عن الهجوم. تصنف محركات الاكتشاف المسار إلى مسار عادي ومشبوه ومسار هجوم مؤكد. يتم ارسال المسار العادي للإنترنت، ويتم التحقق من المسار الثاني من قبل نقطة تفتيش ثانية لتحديد ما إذا كان هجوم أم لا، ويتم إسقاط مسار الهجوم المؤكد و إدراج مصدر هذا التتبع في القائمة السوداء. في هذا البحث ، تم تطوير نظام فعال لتخفيف الشذوذ لشبكة إنترنت الأشياء من خلال تصميم وتنفيذ نظام اكتشاف هجمات الحرمان من الخدمات الموزعه الذي يستخدم طريقة إحصائية تجمع بين ثلاث خوارزميات: الجوار الأقرب، طريقة الأوساط المتحركة الموزونة و المجموع التراكمي. أدى تكامل الحوسبة الضبابيه مع إنترنت الأشياء إلى إنشاء إطار عملي لتنفيذ استراتيجية التخفيف من الشذوذ لمعالجة القضايا الأمنية مثل تهديدات الروبوتات. تم تقييم الوحدة المقترحة باستخدام مجموعة بيانات خاصة. من خلال النتائج ، نستنتج أن نموذجنا قد حقق دقة عالية (٩٩,٠٠ \%) مع معدل إيجابي خاطئ منخفض. في هذه الاطروحة قد حققنا أيضا نتائج جيدة في التمييز بين أجهزة إنترنت الأشياء والأجهزة التي لا تعتمد على إنترنت الأشياء. تساعد نتائج البحث فريق الشبكات على فهم أفضل للتمييز بين حركة مرور شبكة إنترنت الأشياء وغير المرتبطة بإنترنت الأشياء ، مما يسمح لهم بإنشاء سياسات شبكة عالية الجودة فيما يتعلق بالأمان والتوجيه وتخصيص الموارد. للدراسات المستقبلية هناك العديد من الاتجاهات المحتملة: فحص أداء خوارزميات التعلم الآلي المختلفة والتي تشمل التعلم العميق والخوارزميات الغير خاضعه للإشراف. إنشاء مجموعة بيانات باستخدام أجهزة إنترنت الأشياء الواقعية. مقارنة تأثير مقاييس الأداء مع موازنة مجموعة البيانات وبدون موازنة مجموعة البيانات. شمولية نظام التخفيف من هجمات الحرمان من الخدمات الموزعه في انترنت الأشياء على أنواع أخرى من الهجمات لحماية خدمات إنترنت الأشياء.

الكلمات المفتاحية: انترنت الأشياء, الحوسبة الضبابية, نظام كشف التسلل, رفض الخدمة الموزعة, الأمن السيبراني.

Abstract

Botnet attacks, such as DDoS, are among the most common attacks in IoT networks. A botnet is a collection of cooperated computing machines or IoT gadgets that criminal users manage remotely. Several strategies have been developed to reduce anomalies in IoT networks, such as DDoS. To increase the accuracy of the anomaly mitigation system and lower the false positive rate (FPR), some schemes use statistical or machine learning methodologies in the anomaly-based intrusion detection system (IDS) to mitigate an attack. Despite the proposed anomaly mitigation techniques, the mitigation of DDoS attacks in IoT networks remains a concern. Most anomaly mitigation methods fail because of the similarity between DDoS and normal network flows, leading to problems such as a high FPR, low accuracy, and a low detection rate. Furthermore, the limited resources in IoT devices make it difficult to implement anomaly mitigation techniques. In this thesis, an efficient anomaly mitigation system has been developed for the IoT network through the design and implementation of a DDoS attack detection system that uses a statistical method that combines three algorithms: exponentially weighted moving average (EWMA), K-nearest neighbors (KNN), and the cumulative sum algorithm (CUSUM). The integration of fog computing with the IoT has created a practical framework for implementing an anomaly mitigation strategy to address security issues such as botnet threats. The proposed module was evaluated using the Bot-IoT dataset. From the results, we conclude that our model has achieved a high accuracy (99.00\%) with a low false positive rate (FPR). We have also achieved good results in distinguishing between IoT and non-IoT devices. The research findings help the networking team better understand the distinction between IoT and non-IoT network traffic, allowing them to create higher-quality network policies regarding security, routing, and resource allocation.

Keywords: Internet of Things (IoT), Fog Computing, Intrusion Detection System (IDS), Distributed Denial-of-Service (DDoS), Cybersecurity.