نموذج الشبكة العصبية ذو التصنيف المتعدد للاكتشاف السريع لهجمات بوت نت إنترنت الأشياء

هيفاء محمد الزهراني

إشراف:
د. ميسون أبوالخير
د. انتصار الكيال

المستخلص

إن العدد الهائل من أجهزة إنترنت الأشياء (IoT) واستخدامنا لها على نطاق واسع جعل حياتنا أكثر قابلية للإدارة. إلا أن قابلية هذه الأجهزة للانتهاك الأمني يعني أن وجودنا اليومي محاط بالفعل بأجهزة خطرة؛ إذ أنها تسهل على مجرمي الإنترنت شن هجمات مختلفة بواسطة شبكات الروبوت واسعة النطاق (Botnet) من خلال إنترنت الأشياء. تتفاقم هذه المشكلة بسبب قيود إنترنت الأشياء على التقنيات الأمنية بسبب محدودية مواردها بما في ذلك وحدات المعالجة المركزية (CPU) والذاكرة واستهلاك الطاقة. بالنظر إلى هذه الإشكاليات، نقترح نموذجًا خفيف الوزن يعتمد على الشبكة العصبية لاكتشاف هجمات بوت نت إنترنت الأشياء بسرعة.

تم تطوير النموذج باستخدام خوارزمية FastGRNN وهي نسخة خفيفة الوزن وسريعة من الشبكة العصبية المتكررة. بالإضافة إلى ذلك، فإن النموذج مستقل ولا يتطلب معدات أو أدوات خارجية لجلب الميزات المطلوبة لعمليات التعلم والكشف. حيث أنه يعتمد فقط على بيانات حزم الشبكة لإكمال عمليتي التعلم والكشف. علاوة على ذلك، يوفر النموذج تصنيفًا متعددًا، وهو أمر ضروري لفهم الهجمات واتخاذ الإجراءات المضادة المناسبة لوقفها.

وفقًا للتجارب التي تم إجراؤها، فإن النموذج المقترح دقيق وحقق ٩٩,٩٩٪ و ٩٩,٠٤٪ كدرجة F1 لمجموعتي البيانات المعيارية MedBIoT و Mirai-RGU، بالإضافة إلى استيفاء قيود إنترنت الأشياء فيما يتعلق بالتعقيد والسرعة. حيث يُعد أقل تعقيدًا من حيث العمليات الحسابية المطلوبة للتعلم والاكتشاف، كما يوفر اكتشافًا سريعًا متفوقًا على أحدث التقنيات، إذ بلغت سرعة الاكتشاف ١: ٥ ونسبة ١: ٨ للمجموعتين السابقة.

A Multi-Class Neural Network Model for Rapid Detection of IoT Botnet Attacks

Haifaa Mohamad Alzahrani

Supervised By

Dr. Maysoon Abulkhair

Dr. Entisar Alkayal

ABSTRACT

The tremendous number of Internet of Things (IoT) devices and their widespread use have made our lives considerably more manageable. At the same time, however, , the vulnerability of these innovations means that our day-to-day existence is surrounded by insecure devices, thereby facilitating ways for cybercriminals to launch various attacks by large-scale robot networks (botnets) through IoT. This problem is further heightened by the constraints of the IoT on security techniques due to limited resources including central processing units (CPUs), memory, and power consumption. In consideration of these issues, we propose a lightweight neural network-based model to rapidly detect IoT botnet attacks.

The model was developed using FastGRNN algorithm which is a lightweight and fast version of the recurrent neural network. In addition, it is independent and does not require any specific equipment or software to fetch the required features for learning and detection processes. Therefore, only packet headers are required to complete learning and detection. Furthermore, the model provides multi-classification, which is necessary for taking appropriate countermeasures to understand and stop the attacks.

According to the conducted experiments, the proposed model is accurate and achieves 99.99%, 99.04% as F1 score for MedBIoT and Mirai-RGU datasets in addition, to fulfilling IoT constraints regarding complexity and speed. It is less complicated in terms of computations, and it provides real-time detection that outperformed the state-of-the-art, achieving a detection time ratio of 1:5 for MedBIoT dataset and a ratio of 1:8 for Mirai-RGU dataset.