Attack Detection in IoT Botnet Dataflow Using a Hybrid Deep Learning Model

Prepared by

Mohammad Tayseer Kanaan

Supervisor

Dr. Kamal Alieyan

Abstract

The advent of the Internet of Things (IoT) has been a double-edged sword, offering both seamless connectivity and a proliferation of security risks, prominently botnet attacks. These attacks not only compromise the privacy and functionality of IoT devices but also pose a substantial threat to the overarching security of internet infrastructure. This thesis propounds a cutting-edge hybrid deep learning approach, melding the spatial pattern detection of Convolutional Neural Networks (CNNs) with the sequential data interpretation capabilities of Long Short-Term Memory networks (LSTMs). The amalgamation is crucial for addressing the nuanced complexity of botnet traffic in IoT devices, making our methodology both novel and critical.

The research utilizes the extensive N-BaIoT dataset, reflecting the varied traffic data intrinsic to IoT devices, to finetune the model's capability to differentiate between benign and adversarial patterns. Our model incorporates temporal dynamics and device-specific characteristics often neglected by conventional detection systems. By leveraging Principal

Component Analysis (PCA) with 16 components, the model maintains the integrity of complex data while enhancing computational efficiency.

The CNN-LSTM model exhibits stellar performance, as evidenced by an accuracy of 98.9%, representing the proportion of true positives and true negatives among the total evaluated cases. Precision, or the reliability of the model's positive predictions, is recorded at 99%. The model's recall, measuring the correct identification of actual positives, stands at a similar mark, ensuring minimal threat omission. The F1-score, with an average of 99%, articulates the model's balanced precision-recall trade-off. These metrics are not mere abstractions but are indicative of the model's concreteness and responsiveness to the ever-evolving botnet strategies, validated against contemporaneous studies.

The thesis advances the conversation by elucidating the research's implications, acknowledging existing limitations, and charting potential future explorations. It underscores the integration of adversarial learning to counteract evolving cyber-attack strategies, the implementation of real-time detection for proactive threat mitigation, the application of transfer learning for enhanced scalability, and the pursuit of model interpretability for greater transparency. Collectively, these avenues aim to fortify the IoT environment, ensuring it is secure, resilient, and trustworthy.

Keywords: IoT Security, Botnet Detection, CNN-LSTM Hybrid Model, Machine Learning, Principal Component Analysis, Deep Learning, Network Security.

اكتشاف الهجوم في تدفق بيانات روبوتات انترنت الأشياء (بوتنت) باستخدام نموذج التعلم العميق الهجين

إعداد

محمد تيسير كنعان

إشراف

الدكتور كمال عليان

الملخص

أحدث انتشار إنترنت الأشياء (IoT) ثورة في مجال الاتصال بالشبكة، حيث قام بدمج عدد لا يحصى من الأجهزة في البنية التحتية العالمية للإنترنت. ومع ذلك، فقد أدى هذا التوسع السريع أيضاً إلى ظهور ثغرات أمنية كبيرة، لا سيما خطر هجمات الروبوتات. تقدم هذه الأطروحة نموذجاً قوياً للتعلم العميق الهجين الذي يجمع بين شبكات (CNNs) وشبكات الذاكرة طويلة المدى (LSTMs) لاكتشاف وتصنيف هجمات الروبوتات في أجهزة إنترنت الأشياء بدقة وكفاءة عالية.

باستخدام مجموعة بيانات N-BaIoT المتاحة للجمهور، والتي تشمل بيانات حركة المرور المتنوعة من أجهزة إنترنت الأشياء المختلفة، تم تدريب نموذجنا واختباره للتمييز بين أنماط حركة المرور الحميدة والخبيثة. قمنا بتنفيذ تحليل المكونات الرئيسية (PCA) مع 16 مكوناً لتقليل الأبعاد بشكل فعال، وتعزيز الكفاءة الحسابية للنموذج دون التضحية بسلامة البيانات.

وقد تفوق نموذج CNN-LSTM المقترح على النماذج الحديثة الحالية، حيث حقق دقة قدرها 98.9% ودقة قدرها 99%. وتمت مقارنة هذه النتائج بالدراسات الحديثة، مما يؤكد تفوق النموذج في كل من القوة النظرية والتطبيق العملي. لا يوضح عملنا جدوى استخدام بنيات التعلم

العميق الهجينة لأمن إنترنت الأشياء فحسب، بل يشكل أيضاً سابقة جديدة للبحث المستقبلي في هذا المجال.

وتناقش الأطروحة كذلك الآثار المترتبة على هذه النتائج، والقيود المفروضة على البحث الحالي، وتحدد عدة اتجاهات للعمل المستقبلي. ويتضمن ذلك دمج التعلم التنافسي، وأنظمة الكشف في الوقت الفعلي، ونقل التعلم، وقابلية تفسير النماذج، بهدف إنشاء بيئة إنترنت الأشياء أكثر أماناً وجديرة بالثقة.

الكلمات المفتاحية: أمن إنترنت الأشياء، الكشف عن الروبوتات، نموذج CNN-LSTM الهجين، التعلم الآلي، تحليل المكونات الرئيسية، التعلم العميق، أمن الشبكات.