نظام كشف التسلل لإنترنت الأشياء باستخدام جهاز المناعة الاصطناعي والتعلم العميق

سحر أحمد الظاهري
استاذ دكتور: دانيال الغزاوي

المستخلص

نظرًا لأن إنترنت الأشياء (IoT) يحظى بشعبية كبيرة مؤخرًا، فإن هذه التقنية الواعدة تؤدي إلى مجموعة متنوعة من التحديات الأمنية. لا تتناسب الحلول التقليدية مع التحديات الجديدة التي يطرحها نظام إنترنت الأشياء. بالمقابل ، فإن أنظمة المناعة الاصطناعية (AIS) التي تحاكي نظام المناعة البيولوجي تمتاز بأنها أنظمة ذكية ،قابلة للتكيف وتمتلك خصائص مثالية مما يوفر الفرصة لتحسين الأمن السيبراني لإنترنت الأشياء.

في هذه الرسالة ، نقوم بتطوير خوارزمية هجينة من التعلم العميق وخوارزمية الخلايا الجذعية (DeepDCA) في سياق نظام كشف التسلل (IDS). الهدف من هذا البحث هو كشف السلوكيات الخبيثة في شبكة إنترنت الأشياء وتقليل توليد الإنذارات الخاطئة. أيضا ، أتمتة مرحلة استخراج الإشارة لخوارزمية الخلايا الجذعية في مما يحسن أداء التصنيف. تم تطبيق جهاز كشف التسلل المقترح IDS على مجموعة البيانات IoT-Bot . تظهر نتائج التجربة أن DeepDCA كان أداؤه جيدًا في الكشف عن هجمات إنترنت الأشياء بمعدل اكتشاف عالي أظهر مدى دقة أعلى بنسبة ٩٨,٧٣٪ . أيضا ، قادرة على أداء مهمة التصنيف بشكل أفضل من SVM، NB والأداء المماثل مع ANN . في المستقبل نخطط لإجراء مزيد من التجارب للتحقق من الإطار باستخدام مجموعة بيانات أكثر تحديا وإجراء المزيد من المقارنات مع أساليب استخراج الإشارات الأخرى. أيضا ، اكتشاف الهجمات في الوقت الحقيقي.

DeepDCA: Intrusion Detection over IoT Based on Artificial Immune System and Deep Learning

Sahar Ahmed Aldhaheri

Supervised By
Prof. Daniyal Alghazzawi

ABSTRACT

As the Internet of Things (IoT) recently attains tremendous popularity, this promising technology leads to a variety of security challenges. The traditional solutions do not fit the new challenges brought by the IoT ecosystem. Conversely, Artificial Immune Systems (AIS) is intelligent and adaptive systems mimic the human immune system which holds desirable properties for such a dynamic environment and provide an opportunity to improve IoT security. In this thesis, we develop a novel hybrid Deep Learning and Dendritic Cell Algorithm (DeepDCA) in the context of an Intrusion Detection System (IDS). The framework adopts DCA and Self Normalizing Neural Network. The aim of this research is to classify IoT intrusion and minimize the false alarm generation. Also, automate and smooth the signal extraction phase which improves the classification performance. The proposed IDS select the convenient set of features from the IoT-Bot dataset and to perform their signal categorization using the SNN then use the DCA for

classification. The experimentation results show that DeepDCA performed well in detecting the IoT attacks with a high detection rate demonstrating over 98.73% accuracy and low false-positive rate. Also, it capable of performing better classification tasks than SVM, NB and similar performance with ANN classifier. We plan to carry out further experiments to verify the framework using a more challenging dataset and make further comparisons with other signal extraction approaches. Also, involve in real-time (online) attack detection.