Snake Optimization Algorithm for Intrusion Detection System in IoT Networks

Prepared by

Sahar Mohammed Al-shatti

Supervisor by

Dr. Kamal Alieyan

Abstract

The rapid spread of the Internet of Things (IoT) has led to an increase in cyber threats, which is one of the most difficult security problems, noting that traditional security mechanisms are not sufficient to detect wireless intrusions, which endangers data confidentiality, reliability and user privacy, which confirms the need for effective intrusion detection systems. In this thesis, we present a new method to improve the performance of intrusion detection system in IoT networks by impact of the power of the Support Vector Machine algorithm together with the parameter-tuning using Snake algorithm (SVM_SOA). Snake optimization algorithm, which is a heuristic method inspired by nature is applied to determine the best values for the parameters in the new method and compared with the usual methods of the SVM algorithm that adopts default or random values for the

constant and gamma parameters by three different SVM kernels - Linear, Polynomial, and Radial Basis Function (RBF) - to establish a baseline for the IDS using the NSL-KDD database. The new method achieved accuracy an astounding 99% in data classification by after apply SVM-SOA .Each method is evaluated based on key metrics such as accuracy, precision, recall, and F1-score and choosing the best values for the parameters, and comparing them with the accuracy of the genetic algorithm 98.02%, the grasshopper optimization algorithm 98.34%, and the Harris Hawks + practical swarm 97.05%, and thus the results highlight of the Snake optimization algorithm in improving the efficiency of intrusion detection systems by reducing false positive and **increasing** correct classifications (True positive and True negative) to obtain a more secure system and **reduce** false alarms that lead to the network administrator not being preoccupied with it and increasing his focus on detecting real attacks. It provides a significant contribution to the field of Internet of Things security. Future work includes extending this methodology to other machine learning algorithms and examining its potential in different application scenarios within IoT networks.

Keywords: Intrusion Detection System, Machine Learning, Support Vector Machine, Internet of Things, Optimization Algorithm, Snake Optimization Algorithm

خوارزمية الأفعى لتحسين عمل نظام كشف التسلل في شبكات أنترنت الأشياء

إعداد

سحر محمد الشطي

إشراف

الدكتور كمال عليان

الملـخص

أدى الانتشار السريع لإنترنت الأشياء (IoT) إلى زيادة في التهديدات السيبرانية وهي من أصعب المشاكل الأمنية ، علما أن آليات الأمان التقليدية ليست كافية لاكتشاف الاختراقات اللاسكلية ، ممعا يعرض سرية البيانات و الموثوقية و خصوصية المستخدم للخطر ، مما يؤكد الحاجة إلى أنظمة فعالة للكشف عن التسلل . نقدم في هذه الرسالة طريقة جديدة لتحسين أداء نظام كشف التسلل في شبكات إنترنت الأشياء ، بالاستفادة من قوة خوارزمية آلة دعم المتجهات جنبًا إلى جنب مع خوارزمية التحسين الافعى لضبط المعلمات. يتم تطبيق خوارزمية التحسين الأفعى ، وهي طريقة إرشادية مستوحاة من الطبيعة ، لتحديد افضل قيم للمعلمات في الطريقة المقترحة، وبالمقارنة مع طرق الاعتيادية لخوارزمية آلة دعم المتجهات التي تعتمد قيم افتراضية أو عشوائية لمعلمات الثابت و الجاما باستعمال قاعدة بيانات NSL-KDD،حققت الطريقة الجديدة دقة مذهلة تبلغ 99٪ في تصنيف البيانات بالبحث و اختيار افضل القيم للمعلمات ،ومقارنتها بدقة الخوارزمية الجينية98.02% و خوارزمية تحسين الجندب 98.34% و هاريس هوكس + سرب عملي 97.05% و بالتالي تسلط النتائج الضوء على فعالية خوارزمية تحسين ألافعى في تحسين كفاءة أنظمة كشف التسلل من خلال التقليل من التصنيفات الخاطئة وزيادة التصنيفات الصحيحة

للحصول على نظام أكثر أمنا وتقليل الإنذار الخاطيء الذي يؤدي لعدم انشغال مسؤول الشبكة بها و زيادة تركيزه بكشف الهجمات الحقيقة ، مما يوفر مساهمة كبيرة في مجال أمان إنترنت الأشياء. يتضمن العمل المستقبلي توسيع هذه المنهجية لتشمل خوارزميات التعلم الآلي الأخرى ودراسة إمكاناتها في سيناريوهات تطبيق مختلفة داخل شبكات إنترنت الأشياء.

الكلمات المفتاحية نظام كشف التسلل ، التعلم الآلي ، إنترنت الأشياء ، خوارزمية دعم المتجهات ، خوارزمية تحسين الافعى ، ضبط المعلمات