An Enhanced Intrusion Detection System Using Scatter Search Algorithm with Support Vector Machine

Prepared By

Rasha Faisal Israwah

Supervisor By

Dr.Ghaith Jaradat

Abstract

As a result of the widespread use of the Internet in recent years, where sensors and wireless sensor networks have been integrated with many crucial fields, such as health care and military defense systems, the applications of artificial intelligence and the Internet of Things have been expanding. Due to the importance and sensitivity of the data in these fields, it is crucial to use an intrusion detection system (IDS), which applies specific algorithms to analyze and process the data from network in order to find any suspicious activities or behaviors on the system and improve system security. A network frequently carries enormous amounts of data, particularly in military applications where data must flow continuously. Researchers have created a variety of optimization strategies to improve IDS performance in order to address this issue. In this thesis, we make an enhanced intrusion detection system using Scattered Search (SS) algorithm, SS generates a population of random initial solutions and systematically

selects a set of diverse and elite solutions as a reference set for guiding the search. and adopt it as a feature selection method (FS), based on Support Vector Machine (SVM), (SVM) has several features, and due to simple decision boundaries, it avoids over-fit. The performance of the proposed approach was examined using NSL KDD dataset, and the results were compared with the Gazelle Optimization Algorithm (GOA), Algorithmic Optimization Algorithm (AOA), Gray Wolf Optimizer (GWO), Modified Gray Wolf Optimizer (mGWO), and Particle Swarm Optimization (PSO). The main performance metrics used to evaluate the efficiency of the proposed algorithm are accuracy, detection rate, false alarm rate, and number of features. The results indicated that the proposed method has obtained a high intrusion detection accuracy in the IDS system to 99%, it has obtained decreased false alarm rates (0.02) and just (17 features) were chosen from the initial data which contains 41 features, demonstrating the effectiveness of the suggested method.

Key Words: Intrusion Detection System, Scatter Search Algorithm, Support Vector Machine, Feature Selection, Machine Learning, Wireless Sensor Networks

نظام محسن للكشف عن التسلل باستخدام خوارزمية البحث المبعثر مع آلة دعم المتجهات

اعداد

رشا فيصل اسريوه

اشراف

د. غيث جردات

الملخص

نتيجة الاستخدام الواسع للإنترنت في السنوات الأخيرة ، حيث تم دمج أجهزة الاستشعار وشبكات الاستشعار اللاسلكية مع العديد من المجالات الحاسمة ، مثل الرعاية الصحية وأنظمة الدفاع العسكري، وتطبيقات الذكاء الاصطناعي وإنترنت الأشياء تم التوسع. نظرًا لأهمية البيانات الموجودة في هذه المجالات وحساسيتها، فمن الضروري استخدام نظام كشف التسلل (IDS)، والذي يطبق خوارزميات محددة لتحليل ومعالجة البيانات من الشبكة من أجل العثور على أي أنشطة أو سلوكيات مشبوهة على النظام وتحسين أمن النظام. غالبًا ما تحمل الشبكة كميات هائلة من البيانات، لا سيما في التطبيقات العسكرية حيث يجب أن تتدفق البيانات بشكل مستمر في الوقت الفعلي. قد يقلل هذا من كفاءة نظام كشف التسلل لأنه يستغرق وقتًا طويلاً لمعالجة مثل هذه الأحمال من البيانات. ابتكر الباحثون مجموعة متنوعة من استراتيجيات التحسين لتحسين أداء نظام كشف التسلل من أجل معالجة هذه المشكلة. في هذه الرسالة، قمنا بعمل نظام محسن للكشف عن التسلل باستخدام خوارزمية البحث المبعثر (SS) ينشئ البحث المبعثر مجموعة من الحلول الأولية العشوائية ويختار بشكل منهجي مجموعة من الحلول المتنوعة

والنخبوية كمجموعة مرجعية لتوجيه البحث. وقمنا باعتمادها كطريقة لاختيار الميزة ،بناءً على خوارزمية آلة دعم المتجهات(SVM)، وهي لديها العديد من الميزات، ونظرًا لحدود القرار البسيطة، فإنه يتجنب الإفراط في الملاءمة. وتم فحص أداء النهج المقترح باستخدام مجموعة بيانات NSL KDD، وتمت مقارنة النتائج مع خوارزمية الغزال(GOA)، وخوارزمية التحسين الحسابي (AOA)، ومحسن الذئب الرمادي (GWO)، ومحسن الذئب الرمادي المعدل (mGWO)، و تحسين حشد الجسيمات (PSO). مقاييس الأداء الرئيسية المستخدمة لتقييم كفاءة الخوارزمية المقترحة هي الدقة ومعدل الكشف ومعدل الإنذار الخاطئ وعدد الميزات. أشارت النتائج إلى أن الطريقة المقترحة قد حصلت على دقة عالية في كشف التسلل ومعدل الكشف في نظام IDSامقدارها 99٪ . وقد حصلت على معدلات إنذار خاطئة منخفضة (0.02). وتم اختيار (17 ميزة) فقط من البيانات الأولية التي تحتوي على 41 ميزة ، مما يدل على فعالية الطريقة المقترحة.

الكلمات المفتاحية: نظام كشف التسلل ، خوارزمية البحث المبعثر ، خوارزمية آلة المتجهات الداعمة، اختيار الميزات، التعلم الالي، شبكات الاستشعاراللاسلكية