

**An Enhanced Gazelle Optimization Algorithm for Intrusion Detection
System in Wireless Sensor Networks**

Prepared by

Roa'a Yousof Abualigah

Supervisor By

Prof. Mohammad Otair

Abstract

As a natural progression of the widespread usage of the Internet, applications of artificial intelligence and the Internet of things have been growing in recent years, in which sensors and wireless sensor networks (WSN) have been incorporated with many important industries, such as healthcare and industrial applications defense systems. 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 WSNs in order to find any suspicious activities or behavior on the system and improve system security. Huge amounts of data are frequently transmitted over networks, this can reduce the effectiveness of IDS because it takes a long time to analyse such loads of data. Researchers have created a variety of optimization strategies to improve IDS performance in order to address this issue. In this thesis, an enhanced version of Gazelle optimization algorithm (GOA) was

implemented by merging it with the division operator of the Arithmetic Optimization Algorithm (AOA) and proposed as a method for feature selection in Intrusion Detection Systems in Wireless Sensor Networks using the SVM classifier. The performance of the suggested approach was investigated using the NSL KDD dataset, and the outcomes are compared with the original GOA, the Arithmetic optimization algorithm (AOA), the Grey wolf optimizer (GWO), the modified Grey wolf optimizer (mGWO), and Particle Swarm Optimization (PSO). The main performance measures used to assess the efficiency of the proposed algorithm are detection rate, accuracy, false alarm rate, and the number of selected features. The results showed that the proposed method is better than the compared methods, enhanced intrusion detection accuracy in the WSN system to reach (98.22%). Additionally, it has decreased false alarm rates by (0.02), 18 features chosen from the initial dataset which contains 41 features, demonstrating the effectiveness of the suggested method.

نسخة محسنة من خوارزمية الغزال لنظام كشف التسلل في شبكات الاستشعار اللاسلكية

إعداد

رؤى يوسف ابو عليقه

إشراف

الأستاذ الدكتور محمد عطير

الملخص

كتطور طبيعي للانتشار الواسع النطاق للإنترنت ، تطورت تطبيقات الذكاء الاصطناعي وإنترنت الأشياء في السنوات الأخيرة ، حيث تم دمج أجهزة الاستشعار وشبكات الاستشعار اللاسلكية (WSN) مع العديد من الصناعات المهمة ، مثل الرعاية الصحية و أنظمة الدفاع العسكري. نظراً لأهمية البيانات الموجودة في هذه المجالات وحساسيتها ، فمن المهم استخدام نظام كشف التسلل (IDS) ، والذي يطبق خوارزميات محددة لتحليل ومعالجة البيانات من WSN من أجل العثور على أية أنشطة أو سلوك مشبوه على النظام وتحسين أمن النظام. يتم إرسال كميات هائلة من البيانات بشكل متكرر عبر الشبكات ، لا سيما في التطبيقات العسكرية حيث يجب أن تتدفق البيانات باستمرار في الوقت الفعلي. هذا يمكن أن يقلل من فعالية IDS لأنه يستغرق وقتاً طويلاً لتحليل 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 بتطوير نسخة محسنة من خوارزمية الغزال (GOA) من خلال دمجها مع عامل القسمة التابع لخوارزمية التحسين الحسابي وقمنا باعتمادها كطريقة لاختيار الميزة في أنظمة كشف التسلل في شبكات الاستشعار اللاسلكية ومن ثم استخدام SVM كمصنف. تم فحص أداء النهج المقترح باستخدام

مجموعة بيانات NSL KDD ، وتمت مقارنة النتائج مع GOA الأصلي ، 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. أظهرت النتائج أن الطريقة المقترحة كانت الأفضل من الطرق المقارنة ، فوصلت دقة كشف التسلل في نظام WSN إلى نسبة 98.22%. بالإضافة إلى ذلك ، فقد حصلت على معدلات إنذار خاطئة منخفضة بنسبة (0.02) وتم اختيار 18 ميزة فقط من البيانات الأولية التي تحتوي على 41 ميزة ، مما يدل على فعالية الطريقة المقترحة.