نظام كشف الاختراقات في شبكات الاستشعار اللاسلكية باستخدام خوارزمية (GWO) المعدّلة و خوارزمية (SVM)

إعداد

مكرم احمد موفق صفاء الدين

إشراف

الأستاذ الدكتور محمد عطير

الملخص

تهدف الاختراقات في شبكات الاستشعار اللاسلكية إلى الحد من أو القضاء على قدرة الشبكة على أداء وظائفها المتوقعة. حيث أن شبكات الاستشعار اللاسلكية ذات موارد محدودة وغالباً ما يتم نشرها في بيئات لا يمكن التحكم فيها ويمكن للمخترق الوصول اليها بسرعة. لذا، اقترحت في هذه الدراسة تقنية للكشف عن الاختراقات باستخدام خوارزمية الذئاب الرمادية المعدلة ومن ثم تطبيق خوارزمية دعم متجه الدعم (GWOSVM-IDS) لزيادة دقة كشف التسلل ومعدل الكشف عن الاختراقات في بيئة شبكات الاستشعار اللاسلكية. بالإضافة إلى ذلك، تهدف الدراسة إلى تقليل معدلات الإنذارات الخاطئة وعدد الميزات الناتجة عن أنظمة كشف التسلل. كما يعد تقليل وقت المعالجة الذي يتطلبه نظام كشف التسلل في بيئة شبكات الاستشعار اللاسلكية هدفًا آخر في هذه الدراسة. في الحقيقة، تم استخدام مجموعة بيانات NSL KDD'99 لإظهار أداء التقنية المقترحة ومقارنتها مع التقنيات الأخرى الموجودة مثل PSO-IDS و GWOSVM-IDS باستخدام 3 ذئاب. وفيما يتعلق بالدقة، وعدد الميزات، ووقت التنفيذ، ومعدل الإنذار الخاطئ، ومعدل الكشف، فإن نظام GWOSVM-IDS المقترح مع 5 ذئاب يحسن PSO-IDS بنسبة 3 ٪ على الدقة، 40

٪ على عدد الميزات، 42 ٪ على وقت التنفيذ، 64 ٪ على معدل الانذار الخاطىء، و 3 ٪ على نسبة الكشف، أيضاً GWOSVM-IDS مع 3 ذئاب بنسبة 16 ٪ على الدقة، 50 ٪ على عدد الميزات، 13 ٪ على وقت التنفيذ، 60 ٪ على معدل الانذار الخاطىء و 14 ٪ على نسبة الكشف. إضافةً إلى ذلك، فإن الـ GWOSVM-IDS المقترحة بـ 7 ذئاب تعزز PSO-IDS على الدقة وعدد الميزات ووقت التنفيذ ومعدل الانذار الخاطىء ونسبة الكشف بنسب 7٪ و 40٪ و 46٪ و 88٪ و 15٪ على التوالي وحسّنت GWOSVM-IDS بـ 3 ذئاب بنسبة 21٪ و 50٪ و 24٪ و 87٪ و 15 ٪ على الدقة وعدد الميزات ووقت التنفيذ ومعدل الانذار الخاطىء ونسبة الكشف على التوالي. لذلك، فإن التقنية المقترحة عززت نتائج التقنيات الحالية بشكل ملحوظ من حيث الدقة، معدل الكشف، عدد الميزات، ووقت التنفيذ.

A Modified Grey Wolf Optimization and SVM Algorithm for Intrusion Detection System in Wireless Sensor Networks

Prepared by

Mukaram Ahmed Muafaq Safaldin

Supervised by

Prof. Mohammed Otair

Abstract

Intrusion in Wireless Sensor Networks aims in degrading or even eliminating the capability of these network to provide its functions. Wireless Sensor Networks (WSNs) are considered limited-resources networks and usually deployed in uncontrollable environments that attracts intruders to access them. Therefore, this study proposes an enhanced Intrusion Detection System by using a modified Grey Wolf Optimization algorithm and Support Vector Machine algorithm (GWOSVM-IDS). The proposed technique aims to increase intrusion detection accuracy and detection rate in the WSN environment. In addition, it aims to decrease false alarms rates and the number of features resulted from the intrusion detection systems in the WSN environment. Besides, decreasing the processing time required by the intrusion detection system in a WSN environment is another objective of proposing this technique. Indeed, the NSL KDD'99 dataset is used to demonstrate the performance of the proposed technique and compare it with other existing techniques including PSO-IDS (since it suffers from long execution time and low detection rate) and GWOSVM-IDS with 3 wolves (since it suffers from long execution time and low accuracy). In terms of (1) accuracy, (2) number of features, (3) execution time, (4) false alarm rate, and (5) detection rate, the proposed GWOSVM-IDS with 5 wolves enhances PSO-IDS by 3%, 40%, 42%, 64%, and 3%, and it enhances GWOSVM-IDS with 3 wolves by 16%, 50%, 13%, 60% and 14% respectively. Besides, the proposed GWOSVM-IDS with 7 wolves enhances PSO-IDS by 7%, 40%, 46%, 88%, and 15% respectively and GWOSVM-IDS with 3 wolves by 21%, 50%, 24%, 87% and 15% respectively. Therefore, the proposed

technique enhances the existing techniques noticeably in terms of accuracy, detection rate, number of features, and execution time.