خوارزمية الذئب الرمادي المحسنة لنظام كشف الاختراقات في شبكات الاستشعار اللاسلكية

إعداد

أسامة طلب أبراهيم

إشراف

الأستاذ الدكتور محمد عطير

الملخص

نظام كشف التسلل هو وسيلة للدفاع ضد الهجمات ، مما يجعله أحد طبقات الدفاع المهمة . وهي واحدة من أهم مجالات البحث. يحاول الباحثون إيجاد خوارزميات جديدة لفحص جميع الأنشطة الواردة والصادرة وتحديد الأنماط المشبوهة التي قد تشير إلى محاولة الهجوم على النظام. تستخدم التقنية المقترحة لاكتشاف عمليات الاقتحام خوارزمية تحسين الذئب الرمادي لحل مشكلات اختيار الميزات المهمة والتي لها علاقة من مجموعه البيانات وذلك بتهجينها مع خوارزمية تحسين سرب الطيور للاستفادة من أفضل قيمة لتحديث معلومات موقع كل ذئب. تحافظ هذه التقنية على معلومات الموقع الأفضل للفرد من خوارزمية سرب الطيور وتجنب خوارزمية الذئب الرمادي من الوقوع في المستوى المحلي الأمثل.

وتستخدم مجموعة بيانات NSL KDD للتحقق من أداء التقنية المقترحة ، ويتم التصنيف باستخدام خوارزمية k-means وخوارزمية SVM لقياس الأداء من حيث الدقة ، ومعدل الكشف ، ومعدل الإنذار الكاذب ، وعدد الميزات ، ووقت التنفيذ .وقد أظهرت النتائج أن التقنية المقترحة حققت التحسين المطلوب لخوارزمية GWO عند استخدام خوارزميات-K متوسط أو.SVM

An Enhanced Grey Wolf Optimization for Intrusion Detection System in Wireless Sensor Networks

Prepared by:

Osama Talab Ibrahim

Supervised by: Prof. Mohammed Otair

Abstract

The intrusion detection system (IDS) is a method for detection against attacks, making it one of the essential defense layers. Researchers are trying to find new algorithms to inspect all inbound and outbound activities and identify suspicious patterns that may show an attempted system attack. The proposed technique for detecting intrusions uses the Grey Wolf Optimization (GWO) to solve feature selection problems and hybridizing it with Particle Swarm Optimization (PSO) to utilize the best value to update the information of each grey wolf position. This technique preserves the individual's best position information by PSO algorithm that which prevents the GWO algorithm from falling into a local optimum. The NSL KDD dataset is used to verify the performance of the proposed

technique and the classification is done by using the k-means and SVM algorithms to measure the performance in terms of accuracy, detection rate, false alarm rate, number of features, and execution time. The results have shown that the proposed technique attained the required improvement of the GWO algorithm when using K-means or SVM algorithms.