اختيار تقنية التصنيف في كشف التسلل

صالح بن عامر الشهري

المشرف

د. إفتخار أحمد

المستخلص

أصبحت أجهزة الكمبيوتر في هذا العصر عناصر أساسية للاستخدام اليومي، وعلى الرغم من سهولة الوصول واستخدام المعلومات لا تزال عرضة للمتطفلين داخل وخارج المنظمات الذين يسيئون استخدام تفويضهم لتحقيق الأهداف الشخصية، وهذا الاستخدام غير النظامي يسبب كوارث في الشبكات وللمستخدمين. لذلك يجب على قطاعات الحكومة والمنظمات التغلب على هذه المشاكل من خلال حماية أنظمتها، أحد أهم الطرق لحماية النظم هو نظام كشف التسلل. يقوم نظام كشف التسلل بمراقبة وتحديد واكتشاف أي سلوك ضار يقصد منه انتهاك السياسات الأمنية لاتخاذ التدابير اللازمة للحفاظ على سلامة الأنظمة. هناك العديد من الطرق في كشف التسلل ولكن المشكلة الرئيسية تكمن في أدائها. يعتمد الأداء على معدل الكشف والإنذارات الكاذبة الذي يمكن تعزيزه من خلال زيادة معدل الكشف والتقليل من الإنذارات الكاذبة وذلك يعتمد اعتمادا كبيرا على المصنف. لذلك اختيار المصنف المناسب هو مطلب ضروري، لذلك في هذا العمل سيتم دراسة مصنفات مختلفة مبنية على الشبكات العصبية وتنفيذها وسيتم تقييم نتائجها ومقارنتها. هذا العمل سوف يحسن أداء أنظمة كشف التسلل ويكون مساعداً وموجهاً لمنفذي السياسات الأمنية والباحثين.

Towards The Selection of Classification Technique in Intrusion Detection

Saleh Amer Al-Shehri

Supervised By
Dr. Iftikhar Ahmad

ABSTRACT

Intrusion detection systems are essential in computer and network systems because they provide the main defense line to shield the systems from inside and outside intrusions. Different intrusion detection methods are available but the main problem is their performance which depends on accuracy. The accuracy can be improved by increasing the detection rate and reducing false alarms which can be accomplished in one way to select a suitable classifier for the intrusion detection system. For this purpose, three different neural networks; Generalized feed forward (GFF) networks, Radial basis function (RBF) and Time-Lagged Recurrent Networks are applied on the standard dataset NSL-KDD which is a benchmarked in the evaluation of intrusion detection mechanism. Principal component analysis (PCA) is used for feature transformation and pre-processing. The results demonstrate that GFF outperforms the other two classifiers in intrusion detection.