البحث الرابع

أولا: الملخص باللغة العربية

تُعد عمليات الاقتحام لشبكات المعلومات سواء السلكية أو اللاسلكية تهديدا كبيراً فى السنوات الاخيرة نيجة للطلب المتزايد لشبكات المعلومات.

و قد تم إستخدام أنظمة مختلفة من أنظمة كشف التسلل (IDS) كإجراء دفاعى لشبكات المعلومات. و لكن مع وجود كمية هائلة من المعلومات التى تمر عبر شبكة المعلومات ، فإن البيانات التى تم تجميعها تحتوى على سمات غير ذى صلة و زائدة عن الحاجة التى لا تساعد فى معدل كشف التسلل و الاختراق. علاوة على ذلك ، فإن كمية هذه السمات الغير مرغوب فيها تستهلك كمية هائلة من موارد النظام و بالتالى تعمل على تباطؤ عملية التدريب و الإختيار لنظام IDS.

فى هذا البحث تم إقتراح نموذج لإختيار ميزات ذات الصلة بحيث يحدد بشكل فعال الميزات الأكثر ملاءمة لكشف التسلل.

و أعتمد هذا البحث على إستخدام مجموعة قليلة من السمات المشتركة و حذف السمات غير ذات الصلة و الذى أدى بدوره الى إسراع عملية التدريب و الإختيار لنظام IDS المقترح.

تم تطبيق هذا النظام الجديد على قاعدة البيانات KDD و المستخدمة فى إختبارات معدلات كشف التسلل ، و قد أظهرت النتائج الآتى:

١. النموذج المقترح قادرا على كشف التسلل بمعدلات عالية.
٢. عملية كشف التسلل أصبحت أسرع من ذى قبل.