Arabic Summary

يحتوى هذا الباب على أختبار للنظامين الاول يستخدم (back-propagation) .أما النظام الثانى يستخدم (radial basis function) على قاعدة البيانات العالمية (DARPA 98 KDD 99) وأيضا على نسختنا من القاعدة نفسها. ويركز هذا الباب على تصنيف نوعين من السجلات : فئة واحدة (طبيعية أو هجوم) ، وفئات متعددة (طبيعية ، DoS ، PRB، R2L، U2R) حيث تم الكشف عن فئات الهجوم من قبل الشبكات العصبية. وكذلك تم أختبار الأنظمة المقترحة فى الرسالة ومقارنتها ببعض الأنظمة المنشورة حديثا فى المراجع.

الباب السابع:.

يحتوى هذا الباب على ملخص للاستنتاجات وقائمة بالاعمال المستقبلية.

ينقسم هذا الباب الى قسمين .في الجزء الأول، نعرض المصطلحات الأساسية لكشف التسلل ، ونعرض أيضا الفرق بين الجداران النارية ونظام كشف التسلل ومواقع نظام الكشف تم أظهرها أيضا ، هيكل وعناصر نظام كشف التسلل تم شرحها بأختصار ، في الجزء الثاني، أوضح التصنيفات المختلفة للتسلل ، وكذلك التصنيف المختلفة لنظام كشف التسلل ومزايا وعيوب كل منها.

الباب الثالث:.

ينقسم هذا الباب الى ثلاثة أجزاء .في الجزء الأول، نقدم معنى مفهوم تعلم الآلة والفئة المختلفة من تعلم الآلة .في الجزء الثاني، نقدم شرحا للطريقة الاولى والتى تستخدم (back-propagation) .في الجزء الثالث، نقدم شرحا للطريقة الثانية والتى تستخدم (radial basis function).

الباب الرابع:.

يحتوى هذا الباب على شرح لقاعدة البيانات المستخدمة لتدريب واختبار النضام المقترح (DARPA 98 KDD 99), و كذلك تقسم وتوزيع ملفات البيانات.

الباب الخامس:.

يحتوى هذا الباب على شرح لهيكل النظام المقترح وجميع أجزائه كما يحتوى على شرح لعملية أختصار بيانات التعلم وكيفية تحويل البيانات الحرفية الى لغة تفهمها الشبكات العصبية.

الباب السادس:.

والهدف من هذا البحث هو تصنيف الهجمات على الشبكة باستخدام الشبكات العصبية (NN) مما يؤدي إلى ارتفاع معدل الكشف عن المتسللين في أقل وقت ممكن. تركز هذه الدراسة على تصنيف نوعين من السجلات : فئة واحدة (طبيعية أو هجوم) ، وفئات متعددة (طبيعية ، DoS ، PRB، R2L، U2R) حيث تم الكشف عن فئات الهجوم من قبل الشبكات العصبية .ويجري تحليل واسعة النطاق من أجل ترجمة البيانات الحرفية الى لغة تفهمها الشبكات العصبية ، تقسيم بيانات التدريب ومدى تعقيد البنية الخاصة بالشبكة العصبية. يتم اختبار النظام المقترح لكشف التسلل بأستخدام الشبكات العصيبة (BPNNIDS)في مواجهة الآلة التقليدية وغيرها من خوارزميات التعلم باستخدام مجموعة بيانات مشتركة (DARPA 98 KDD 99). وتم مقارنة بنظام معتمد على (RBF). واظهرات تلك المقارنات أن النظام المقترح حقق أعلى معدل لكشف التسلل فى اقل وقت وبدون تدخل العامل البشرى.

وتتكون الرسالة من عدد سبعة أبواب:

الباب الأول:.

يحتوى هذا الباب على خمسة أجزاء الجزء الاول يشرح التحفيز للعمل فى مجال كشف التسلل. الجزء الثانى يعرض المراجعات الادبية السابقة التى عملت فى نفس المجال. الجزء الثالث يعرض الهدف من البحث. الجزء الرابع يعرض الاسهامات. والجزء الخامس يوضح ما سوف يعرض فى باقى الابواب.

الباب الثاني:.

ملخص رسالة ماجستير بعنوان

" تقنية ذكية لكشف التسلل مبنية على تعلم الآلة"

مقدمة من

المهندس / أحمد حسن محمد فارس

ملخص البحث:

الأمن هو القضية الكبرى لجميع الشبكات في بيئتنا الحالية. الدخلاء والمتسللين قاموا بالعديد من المحاولات الناجحة لاسقاط شبكات الشركات البارزة وخدمات الشبكه العالمية. هناك طرق كثيرة وضعت لتأمين البنية الاساسية للشبكة والاتصال عبر شبكة الانترنت ، ومن بينها استخدام الجدران الناريه ، والتشفير ، والشبكات الخاصة الافتراضيه. كشف التسلل يعتبر جديد نسبيا اضافة الى هذه التقنيات. أساليب كشف التسلل بدأت تظهر في السنوات القليلة الماضية. باستخدام اساليب كشف التسلل ، يمكنك جمع واستخدام معلومات عن أنواع معروفة من الهجمات ومعرفة ما اذا كان احدهم يحاول الهجوم عليك أو على الشبكه الخاصه بك. المعلومات التي يتم جمعها بهذه الطريقة يمكن أن تستخدم لتشديد امن الشبكه الخاص بك ، وكذلك لأستخدام تلك المعلومات فى أغراض قانونيه. هناك كثير من المصادر المفتوحه و المنتجات التجارية متاحة الآن لهذا الغرض. العديد من ادوات تقييم الضعف تتوافر أيضا في السوق والتي يمكن ان تستخدم لتقييم انواع مختلفة من الثغرات الامنية الموجودة في الشبكه الخاصة بك. ولكن هدفنا هو تحسين عملية كشف التسلل.