نظام اكتشاف الدخلاء في الشبكة المحلية اللاسلكية

المستخلص

مع التطور السريع وتزايد الاهتمام في استخدام تطبيقات الشبكة اللاسلكية ، أصبحت الحماية احد أهم ما يواجهه هذا النوع من الشبكات هذه الأيام. بينما نجد أن الجدار الناري اثبت قدرته كخط دفاع أول في الشبكات السلكية نرى أن الحالة تختلف في الشبكات اللا سلكية ، حيث إن تراسل البيانات فيها هو هدف مباشر لعمليات الاستراق أو الاعتراض والتشويش . فالاستخدام السيئ لطبقة التواصل مع وسط الإرسال (MAC Layer) للشبكات في معيار (IEEE ٨٠٢.١١) يمكن أن يؤدي إلى سوء التوزيع لنطاق التراسل . هذا التوزيع السيئ من الممكن أن يؤدي إلى مشاكل خطيرة في منافذ الدخول اللاسلكية للانترنت الواسعة الانتشار ، حيث إن المستخدم يقوم بدفع قيمة الاشتراك نتيجة استفادته منها. لذلك ربما يحاول المستخدم نتيجة لطمعه أن يزيد من نطاق التراسل الخاص به على حساب بقية المستخدمين المشتركين معه في هذه الخدمة من خلال إجراء بعض التعديلات البسيطة على تعريف الكرت الخاص بالشبكة اللاسلكية. هذه بعض أهم المشاكل الأمنية الخاصة بالشبكات اللاسلكية . ونظرا لتزايد الاستخدام لهذه الشبكات أصبح من الضروري إيجاد طريقة تراسل مؤمنة وفعالة لمستخدميها . نظام كشف الدخيل هو احد أهم مفاتيح الحماية ضد الدخلاء غير المرغوب بهم في الشبكة . وضعت أبحاث كثيرة في هذا المجال أنتجت لنا أنظمة كشف دخيل متعددة تختص بالشبكات السلكية. ولكن وجد أن أغلب هذه الأنظمة لم تعط النتائج المرجوة منها حين طبقت على الشبكات اللاسلكية.

تم في هذا البحث تصميم نظام اكتشاف الدخلاء في الشبكات المحلية اللاسلكية وتجربته حالات مفتعلة بشكل افتراضي وأظهرت لنا نجاحا كبيرا في اكتشاف أنواع من حالات التلاعب الممكن حدوثها في الشبكة المحلية اللاسلكية وبتطبيق هذا النظام بشكل تجاري سيتمكن مديرو الشبكات من اكتشاف وجود مثل هذه الحالات من ا لتلاعب في الشبكة اللاسلكية والذي بدوره يضعف من فعاليتها بالنسبة للمستفيدين منها مما يساعد مديري الشبكة على معالجتها ومعاقبة مرتكبيها.

المشرف على الرسالة
د/ رضا بن محمد سلامة

Intrusion Detection System for WLAN

ABSTRACT

Wireless network play a crucial role in the lives of people at work, home, and public places. Because of the widespread implementation of wireless network, providers deploy Wireless Local Area Network (WLANs) to provide broadband access to the Internet. The rapid growth rate of public wireless LANs is making the Internet available to people at areas where people tend to congregate. Users within range of a public wireless LAN hotspot, such as an airport or hotel, can access e-mail and browse the Internet either free or mostly for a fee when it is not offered freely. However, as the number of users soars, so does the risk of possible misbehaviour. Misbehaviour user can substantially increase his share of the bandwidth, at the expense of other paid users, by slightly modifying the driver of his network adapter. As the uses of such networks grow, users will demand secure yet efficient, low-latency communications. Intrusion detection is one of the key techniques behind protecting a network against intruders. Many Intrusion Detection Systems (IDSs) have been designed for wired networks. Most of these IDS systems did not produce the expected results when applied to wireless networks especially for the Media Access Control (MAC) layer problem.

Thesis Advisor
Dr. Reda Salama