Abstract

This thesis investigated a number of security protocols, which are used in wireless networks. Security protocols like Wired Equivalent Privacy (WEP), WEP2, Wi-Fi Protected Access (WPA) and WPA2, which are protocols developed mainly to work within the IEEE 802.11 standard.

Analysis of the protocols advantages and disadvantages were introduced (vulnerabilities and problems), from the encryption and decryption point of view. A number of measures were proposed to counter most of the known vulnerabilities that face the wireless networks security today. The counter measures were introduced in the form of a proposed security protocol, which is called Multiple Slot System (MSS).

A number of tests (mathematical and computer simulations) were carried out to prove the new protocol ability to provide at least a better security capabilities than the wireless security protocols in use in the market today. The proposed measures can be used in a number of security related fields.

The new protocol implements a number of high level security measures and was developed main to secure high level public networks (like government wireless networks) that contains high level security information. Due to the nature of the new protocol a new hardware design for the network routers and gateways must be implemented.

المقدمة

هذه الرسالة تناقش و تحلل مجموعة من البروتوكولات المستخدمة فى تأمين الشبكات اللاسلكية. البروتوكولات التى تم تحليلها هى WEP, WEP2, WPA و WPA2 و هى بروتوكولات صممة لتعمل فى منظومة IEEE 802.11. لقد تم تحليل هذة البروتوكولات من وجهة نظر التشفير و نقاط الضعف و القوة بها.

مجمومة من المقترحات تم تقديمها فى هذة الرسالة لمواجهة نقاط الضعف الموجوده فى البروتوكولات السابقة. المقترحات تم تقديمها فى صورة بروتوكول جديد متخصص فى حماية الشبكات اللاسلكية تحت أسم Multiple Slot System.

لقد تم اختبار البروتوكول الجديد و تحديد قدرته على تأمين الشبكات اللاسلكية بعد اجراء مجموعة من الاختبارات (رياضية و محاكة باستخدام الحاسب الالى). سوف يتم أثبات فاعلية البروتوكول المقترح بعد مقارنته بالبروتوكولات المعاصره. البروتوكول الجديد يمكن استخدامة فى عدة تطبيقات أخرى.

بسبب صعوبة بعد أجزاء البروتوكول المقترح, يجب تغير نظم و طق عمل الاجهزة المستخدمه فى الشبكات اللاسلكية باجهزة أخرى قادرة على تنفيذ المتطلبات الجديدة.
البروتوكول الجديد قد صمم خصيصا لتأمين الشبكات ذا المحتوى عالى الاهمية مثل الشبكات الحكومية و الشبكات العامه.