الخلاصة

التقدم الحاصل في مجال الالكترونيات و الاتصالات ساهم في تطوير اجهزة تحسس رخيصة الثمن و اقتصادية في استهلاك الطاقة و متعددة الوظائف و صغيرة الحجم و ذات مدى اتصال قصير. هذه المتحسسات الصغيرة الحجم التي تتكون من وحدة معالجة البيانات و جهاز اتصال لاسلكي, ساعدت في بلورة فكرة شبكة المتحسسات اللاسلكية. تتكون هذه الشبكات من المئات من المتحسسات التي تعتمد في الاتصال فيما بينها على مبدا القفز المتعدد. ان هذا النوع من الشبكات يواجه العديد من التحديات واهمها هو محدودية مصدر الطاقة التي يعتمد عليها المتحسس. حيث انها لا تعتمد على مصدر طاقة مستمر في عملها بل على البطاريات. و لضمان اداء هذه الشبكات بشكل كفوء يجب ان يكون هناك انظمة امنية تقوم بحماية التطبيقات التي تعمل من اجلها هذه الشبكات. من اهم المتطلبات هو ضرورة تقييم احتياجات الطاقة.

قسمت هذه الدراسة الى جزئين, الجزء الاول يقوم بدراسة البروتوكول الامني (TinySec) المطبق لتوفير نظام امني للشبكات المتحسسة من خلال تطبيقه ومعرفة مدى تاثير هذا البرتوكول على استهلاك الطاقة و اثره على الذاكرة المخصصة للمتحسس, و تعديل هذا البروتوكول لتقليل هذا التاثير. البروتوكول المُعَدَّل يخفضُ 27 % من إستهلاكِ الطاقة بالنسبة TinySec-AE و50 % بالنسبة الى TinySec-Auth.

الجزء الثاني يقترح نظام لامركزي آمن و كفوء لادارة المفاتيح و يتضمن هذا النظام ثلاث مهمات فرعية وهي: Key establishment, Key update and New node addition. ان هذا النظام تمت دراسته مع اجراء مقارنة مع الانظمة السابقة و اظهرت النتائج كفاءة النظام المقترح في استهلاك الطاقة مقارنة بالانظمة السابقة.

PDF created with pdfFactory trial version www.pdffactory.com

Abstract

Recent advances in wireless communications and electronics have helped to develop sensor nodes which are low-cost, low-power, multifunctional, small in size and communicate in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks. Ad hoc sensor network is a multihop network made of hundred of sensor nodes.

Sensor nodes come with new challenges. To eliminate the constraints imposed by wires, sensor nodes come with their own limited energy sources and communicate using wireless networks. Securing data generated by sensor nodes is critical depending on the nature of the application. While securing sensor data is essential, the cost of doing so in terms of energy requirements needs to be assessed carefully.

This work is divided into two parts; the first part investigates the TinySec link layer security protocol employed for ad hoc sensor network in terms of energy consumption and memory footprint. This protocol is modified to minimize the security impact. The modified protocol based on different approaches for providing integrity and confidentiality. The modified protocol achieves 27% reduction in the energy consumption of the TinySec-AE mode and 50% reduction of the TinySec-Auth mode.

The second part presents the proposed secure and energy efficient decentralized key management protocol. The proposed protocol combines three schemes; key establishment, key update and new node addition scheme. The energy consumption of the proposed key management is analyzed and compared with those of the formal protocols. The analysis shows an advantage in term of energy consumption over the previous work.

PDF created with pdfFactory trial version www.pdffactory.com