ENHANCED SECURITY OF WIRELESS SENSOR NETWORKS USING HYBRID SECURE RANDOM KEY PRE-DISTRIBUTION SCHEME AND A MODIFIED NK CRYPTOSYSTEM

by

Tamer Mohamed Abd El-RahmanMohamed Barakat

A Thesis Submitted to the
Faculty of Engineering at CairoUniversity
In Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY
in
ELECTRONICS AND COMMUNICATIONS ENGINEERING

Under the Supervision of

Prof. Dr. Amin Mohamed Nassar **Dr. Amr Mohamed Gody**

Professor Assistant Professor
Electronics and Communications Eng. Dept. Electrical Engineering Dept.
Faculty of Engineering Faculty of Engineering
CairoUniversityFayoumUniversity

FACULTY OF ENGINEERING, CAIROUNIVERSITY
GIZA, EGYPT
JANUARY 2008

Abstract

Rapid technological advances in the areas of micro electro-mechanical systems have spurred the development of a new kind of network. This network is composed of small, inexpensive sensors capable of intelligent sensing. A significant amount of research has been done in the area of connecting large numbers of these sensors to create robust and scalable wireless sensor Networks (WSNs). Wireless sensor networks currently used in many applications including real-time traffic monitoring, building safety monitoring, military sensing and tracking, distributed measurement of seismic activity, etc.

When sensor networks are deployed in a hostile environment, security becomes extremely important. Wireless Sensor Networks used key management scheme to setup secret keys between communication nodes. This scheme has two main problems; the resilience against node capture is low and the connectivity of this scheme is weak due to the power constraint for wireless sensor networks.

On the other hand, WSNs used the RSA cryptosystem during the authentication process between each node and its base station. This cryptosystem has two huge problems; it is insecure due to several attacks such as Adaptive chosen-ciphertext attack, Adaptive chosen-message attack, common modulus attack, and low exponent attack. Another problem is that the decryption time is very slow. Recently, NK cryptosystem was proposed to solve the slowness in the decryption time but it still suffers from the previous mentioned attack.

In this thesis, a new random key pre-distribution scheme will be proposed. Security analysis of the proposed scheme will be presented to prove that our scheme has the highest resiliency and the best connectivity.

To achieve maximum authentication, the modified NK (MNK) cryptosystem is presented. Security analysis of the MNK cryptosystem will be presented which prove that the MNK cryptosystem is secure against all attacks that already applied on both RSA and the original NK cryptosystem.

Before using the MNK cryptosystem in the WSNs, it must be ensure that the energy consumed by this cryptosystem is reasonable to meet the energy constraint. Therefore, the energy analysis of the MNK cryptosystem will be evaluated to show the energy consumption due to the MNK cryptosystem is lower than that before.

Keywords

Wireless Sensor Networks; Key Management Protocol; Random Key Pre-distribution Scheme; RSA cryptosystem; NK cryptosystem; MNK cryptosystem; Handshake Protocol.

تحسين السرية في شبكات الاستشعارات اللاسلكية باستخدام نظام المفتاح العشوائي المهجن و الآمن قبل التوزيع و نظام التشفير NK المعدل

إعداد

تامر محمد عبد الرحمن محمد بركات

رسالة مقدمة إلى كلية الهندسة ، جامعة القاهرة
كجزء من متطلبات الحصول على درجة الدكتوراه
في هندسة الإلكترونيات و الاتصالات الكهربية

تحسين السرية في شبكات الاستشعارات اللاسلكية باستخدام نظام المفتاح العشوائي المهجن و الآمن قبل التوزيع و نظام التشفير NK المعدل

إعداد

تامر محمد عبد الرحمن محمد بركات

رسالة مقدمة إلى كلية الهندسة ، جامعة القاهرة
كجزء من متطلبات الحصول على درجة الدكتوراه
في هندسة الإلكترونيات و الاتصالات الكهربية

تحت إشراف

أ.د. أمين محمد نصار أستاذ بقسم هندسة الإلكترونيات و الاتصالات
كلية الهندسة ، جامعة القاهرة

د. عمرو محمد جودي مدرس بقسم الهندسة الكهربية
كلية الهندسة ، جامعة الفيوم

ملخص الرسالة

إن الأبحاث العلمية الحديثة في مجال تكنولوجيا الكمبيوتر و الاتصالات قد فتحت الطريق أمام الباحثين في هذا المجال لتطوير شبكات الاستشعارات اللاسلكية.و تتكونشبكات الاستشعارات عادة من عدد كبير جدا من أجهزة صغيرة الحجم ، كل جهاز يسمي نقطة استشعار.

وكل نقطة استشعار تعمل ببطارية و تستهلك طاقة محدودة، ثم تقوم نقطة الاستشعار باستخدام موجات الراديو القصيرة لإرسال بياناتها من مكان لأخر.

وتدخل شبكات الاستشعارات اللاسلكية في كثير من التطبيقات مثل مراقبة حركات المرور ، مراقبة حالات تلوث البيئة ، متابعة حالات المرضى ، وأيضا في معظم التطبيقات العسكرية و التي تتطلب مراقبة حركة العدو خاصا عند توزيع هذه الشبكات في منطقة العدو لغرض الاستكشافات، ولذلك لابد من استخدام نظام آمن لتأمين البيانات التي يتم إرسالها من و إلى المحطة الرئيسية.

وتستخدم شبكات الاستشعارات اللاسلكية إدارة المفتاح قبل التوزيع و الذي يسمى إشنوير- جليجور. حيث يتم في هذا النظام تحديد و تعين مفتاح آمن بين كل نقطتين استشعاريتين متجاورتين ثم بعد ذلك يتم نقل البيانات بينهم بصورة آمنة.ولكن هذا النظام يعانى من مشكلتين رئيسيين:

المشكلة الأولى تتلخص في الاتى؛ إذا استطاع احد المهاجمين من اختراق النظام فإنه يستطيع معرفة المفتاح الآمن لعدد معين من نقط الاستشعار .و إذا وصل هذا العدد إلى حد معين(و هذا الحد محدد من قبل إشنوير- جليجور) فإن المهاجم يستطيع معرفة جميع قيم المفاتيح السرية لكل النقط الاستشعارية في جميع الشبكة.

المشكلة الثانية إن هذا النظام يستخدم مفتاح ذو ٦٤ بت في بداية النظام بين كل نقطتين استشعاريتين لإيجاد مفتاح واحد مشترك بينهم لكي يتم نقل البيانات بينهم بصورة آمنة. لذلك هذا النظام يستهلك طاقة عالية لأنه يخزن في ذاكرة كل نقطة استشعار ٦٤ بت ، مما يؤدى إلى إن تكون عملية اتصال نقطة بأخرى بطيئة نظرا لان كل نقطة تستخدم مقدار محدود من الطاقة .

من ناحية أخرى لكي يتم الاتصال بين كل نقطة استشعار و المحطة الرئيسية الخاصة بها، لابد من استخدام نظام ثقة متبادلة يتم من خلالها إثبات الهوية الذاتية كل مع الآخر. ولهذا تستخدم شبكات الاستشعارات اللاسلكية نظام التشفير RSA لذلك الغرض.ولكن هذا النظام يعانى من مشكلتين هامتين؛

المشكلة الأولى انه يعانى من عديد من عمليات الهجوم الخطيرة مثل : هجوم بسبب اختيار قيمه صغيرة لمفتاح التشفير العام ، هجوم بسبب استخدام معامل مشترك بين المستخدمين، الهجوم المعدل على النصوص المشفرة الاختيارية ، و أخيرا الهجوم المعدل على الرسائل المختارة .

المشكلة الثانية تكمن في إن وقت فك الشفرة بطئ جدا مما يجعل عملية الثقة تأخذ وقت اطول و بالتالي تسمح لاى مهاجم إن يعترض عملية الثقة و يحصل على معلومات سرية .

وقد تم التغلب على احد مشاكل نظام التشفير RSA بواسطة نظام تشفير جديد ذات المفتاح العام يسمى NK و الذي يتميز بأن وقت فك الشفرة أسرع بكثير من نظام التشفير RSA المستخدم حاليا.

وفي هذه الرسالة ، تم اقتراح نظام جديد من أنظمة إدارة المفتاح قبل التوزيع يسمى المفتاح العشوائي و الآمن قبل التوزيع و الذي يعالج مشكلة نظام إشنوير- جليجور و قد استخدم هذا النظام الجديد مفتاح ذو ١٦ بت بدلا من مفتاح ذو ٦٤ بت في بداية النظام بين كل نقطتين استشعاريتين لإيجاد مفتاح واحد مشترك بينهم لكي يتم نقل البيانات بينهم. وكذلك تم تحليل السرية لهذا النظام الجديد المقترح وقد وجد من خلال هذا التحليل الرياضي و البياني الدقيق أن سرية هذا النظام المقترح أصبحت اعلي بكثير من الأنظمة السابقة.

من ناحية أخرى ، هذه الرسالة اقترحت نظام تشفير معدل لنظام التشفير NK السابق لتحسين السرية في نظام التشفير NK السابق . وأيضا تم من خلال هذه الرسالة تحليل السرية لنظام التشفير NK المعدل و قد ثبت التحليل الرياضي لهذا النظام انه آمن ضد عمليات الهجوم التي تواجه نظام التشفير RSA و نظام NK السابق.

وكان لابد من التأكد من إن هذا النظام المعدل يستهلك طاقة اقل من ذى قبل خلال إرسال و استقبال من و إلى نقطة الاستشعارقبل استخدام نظام NK المعدل في عمليات الثقة المتبادلة بين كل من نقطة الاستشعار و المحطة الرئيسية و لذلك تم تحليل الطاقة المستهلكة باستخدام هذا النظام المعدل.

ومن ناحية أخرى تم من خلال هذه الرسالة مقارنة الطاقة المستهلكة لكل من نظام التشفير RSA و نظام التشفير NK المعدل، و قد تبين من هذه المقارنة إن نظام التشفير NK المعدل يستهلك طاقة اقل من نظام التشفير RSA.

أخيرا ، يتضح من النتائج التي تم الحصول إليها خلال هذه الرسالة انه لتحسين السرية في شبكات الاستشعارات اللاسلكية من الأفضل نظام التشفير NK المعدل لتحسين السرية أثناء عملية الثقة المتبادلة و أيضا من الأفضل استخدام هذا النظام المعدل لتقليل استهلاك الطاقة لنقاط الاستشعار خلال عمليات إرسال البيانات و استقبالها.وكذلك من الأفضل استخدام نظام المفتاح العشوائي و الآمن قبل التوزيع في تشفير البيانات بين نقاط الاستشعار و بعضها البعض للحصول على اعلي دفاع ضد هجمات التقاط المفتاح السري لهذه النقاط و الوصول لأعلى درجة اتصال ا.