جامعـــة الموصـــــل
كليـــة الهندســـة

نظام أتمتة باستخدام شبكة متحسسات لاسلكية مُؤمنة

ندى إسماعيل نجم عبدالله المعروف

رسالة ماجستير علوم
في الهندسة الكهربائية/الكترونيك واتصالات
(شبكات الحاسبات والاتصالات)

بإشراف
الأستاذ المساعد
الدكتور قتيبة إبراهيم علي

1435 هـ 2014 م

المستخلص بلغة الرسالة

المستخلص

وجدت شبكات المتحسسات اللاسلكية طريقها إلى العديد من التطبيقات التجارية والصناعية، و العسكرية، وقد أدى هذا الانتشار الملحوظ إلى زيادة الاهتمام بتوفير الحماية الأمنية لهذه الشبكات.

وضحت هذه الرسالة أن تصميم الحلول الأمنية الخاصة بشبكات المتحسسات اللاسلكية ليس بالأمر السهل و خصوصاً في ظل الطبيعة العشوائية للشبكات، والاتصالات اللاسلكية المعروفة بثغراتها الأمنية، بالإضافة إلى محدودية الموارد. كذلك تناولت هذه الدراسة أشكال الاعتداءات التي تهدد أمان شبكات المتحسسات اللاسلكية ووسائل مواجهتها.

كان الهدف من الرسالة تصميم منظومة أمان متكاملة تعد وسيلة دفاعية تختص بتوفير الحماية من مشاكل الاعتداءات التي تتعرض لها المحطة الأساسية التي تربط شبكة المتحسسات اللاسلكية بالخدام، حيث ضمت منظومة الأمان المقترحة على اثنين من خوارزميات التشفير الكتلي وهما خوارزمية تشفير البيانات العالمية(IDEA) و خوارزمية معيار التشفير المتقدم (Rijindal - AES) وكذلك خوارزمية التشفير التدفقي الـ(Scream Cipher)، استخدمت هذه الخوارزميات من أجل تشفير البيانات وضمان خصوصيتها على طول مسارها ابتداءاً من عقد المتحسسات و انتهائاً بالخادم لغرض تحقيق اتصال مؤمن بين جميع أجزاء الشبكة، استخدمت منظومة الأمان المقترحة خوارزمية الـ(HMAC) باستخدام دالة الاختزال بدون مفتاح الـ(SHA-512) لضمان صحة ووثوقية البيانات المرسلة والمستلمة، كذلك احتوت هذه منظومة المقترحة آلية تحديث تلقائية للمفاتيح بين أجزاء الشبكة بصورة متزامنة وبدون إجراء عملية تبادل للبيانات، واخيراً الجدار الناري استخدم لمنع الوصول للشبكة من قبل الأطراف غير المخولين. فعند اعتبار النواحي الأمنية للمحطة الأساسية (مُثِّلَ طرف المحطة الأساسية من النظام المقترح باستخدام معالج الشبكة الـ(Ubicom) من نوع (IP2022)) استخدمت طرائق تحسينات على الخوارزميات المستخدمة لغرض جعلها تعمل ضمن موارد الـ(Ubicom)المحدودة دون استنزافها، وتم العمل على تحقيق التوازن بين كلفة تشغيل الآليات الأمنية و كلفة تشغيل الوظائف الأخرى للشبكة.

من طرف الخادم (أحياناً يسمى المواجهة بين الإنسان والحاسبة(Human Machine Interface)) صممت منظومة الأمان المقترحة باستخدام برنامج الـ(LabVIEW 2009).

أخيراً للتحقق من صحة منظومة الأمان المقترحة عملياً استخدمت شبكة متحسسات لاسلكية لتجميع معلومات عن درجة حرارة المنطقة المحيطة من المتحسسات إلى المحطة الأساسية، ومن ثم إرسال المعلومات المستلمة إلى الخادم الذي يعمل على إظهار حالة المتحسسات التي تم تجميع المعلومات منها،حيث اخذ بنظر الاعتبار أنواع مختلفة من معماريات الأمان في عملية الاختبار هذه.

المشرف

د. قتيبة إبراهيم علي

معاون العميد للشؤون العلمية والدراسات العليا

Abstract

Wireless Sensors Networks found their way into many commercial, industrial, and military applications this marked proliferation has led to a greater attention to protect the security of these networks.

This thesis, made clear that design security solutions for the wireless sensors networks is not easy, especially in light of the random nature of the networks, wireless communications known for its security gaps, in addition to limited resources. As well as this thesis described types of attacks that threaten the security of wireless sensors networks and defensive mechanisms against attacks.

The aim of this thesis is focused on the design and implementation challenges to localize an embedded security center into base station nodes which connects WSN to the LabVIEW based Human Machine Interface (server). The suggested base station security center consists of three ciphering methods (IDEA, AES & Scream) to provide data encryption to the whole path from the WSN nodes to the server, an HMAC function to provide message integrity and authentication between the base station and the server, a keys generation module, and a firewall. Our design takes into account the "embedded" nature of the base station (UBICOM IP2022 network processor chip in our case) and their limited resources and suggests different methods to achieve its goals.

Also, enhancements were added to the LabVIEW based Human Machine Interface (HMI) server to include all the security solutions mentioned earlier.

In order to validate the correct of the suggested secured system practically, a temperature measurement wireless sensor network was built and tested taking into consideration the diffirent security solution. the suggested secured system consists of the main parts of the proposed system; sensor, base station and (Human Machine Interface), where the sensors send their secure messages about their status to the master node. The base station collects the information from sensors and secured it and sends the information gathered to the (Human Machine Interface) that indicate the status of each node of the wireless sensor network.

University of Mosul
College of Engineering

An automation System Based on Secured Wireless Sensor Network (WSN)

Nada Ismail Najim Abdullah Almaroof

M.Sc. Thesis

Electrical Engineering /

Electronics and Communications /

(Computer Network and communication)

Supervised by
Assistant Professor
Dr. Q. I. Ali

2014 A.D. **1435 A.H.**