Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks

Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, *Member, IEEE*

***Abstract*—This study presents a healthcare monitoring architecture coupled with wearable sensor systems and an environmental sensor network for monitoring elderly or chronic patients in their residence. The wearable sensor system, built into a fabric belt, consists of various medical sensors that collect a timely set of physiological health indicators transmitted via low energy wireless communication to mobile computing devices. Three application scenarios are implemented using the proposed network architecture. The group-based data collection and data transmission using the ad hoc mode promote outpatient healthcare services for only one medical staff member assigned to a set of patients. Adaptive security issues for data transmission are performed based on different wireless capabilities. This study also presents a monitoring application prototype for capturing sensor data from wireless sensor nodes. The implemented schemes were verified as performing efficiently and rapidly in the proposed network architecture.**

***Index Terms*—Healthcare monitoring, wearable sensor, security, ad hoc, WSN, ECG.**

I. Introduction

MOBILE, wireless, pervasive computing and communication environments are changing the way medical staffs interact with their patients and the elderly. By deploying self-organized wireless physiological-monitoring hardware/software systems, continual patient monitoring in certain types of patient postures becomes convenient to assuring timely intervention by a healthcare practitioner or a physician. For example, cardiac patients wearing electrocardiogram (ECG) sensor systems can be monitored remotely without leaving their residence. Healthcare sensor systems are required to be connected directly or indirectly to the Internet at all times, which allows medical staff to timely acquire arrhythmia events and abnormal ECG signals for correcting medical procedures. Moreover, physiological records are collected over a long period of time so that physicians can provide accurate diagnoses and correct treatment. However, developing a pervasive sensor network for healthcare has numerous challenges, including wireless healthcare sensor systems conforming to the human body, the integration of different wireless networks with various transmission techniques, and the development of healthcare applications over these types of networks.

Typically, to catch the vital signs from an individual requires a stand-alone monitoring device with a number of medical sensors connected to the patient through wired connections. This limits patient flexibility and mobility. Mainly due to the rapid progress in sensing techniques, sensors have been adapted in all shapes and sizes, accommodating human body parts with various degrees of functionality. Various kinds of wireless communication motes have been integrated with medical sensors to support healthcare and medical supervision by UC-Berkeley Research, Intel Research, and ETH Zurich [14]. Wearable sensor devices are designed for physical contact with the substance or object being measured to record physiology such as blood pressure, heart rate, ECG, weight, body temperature, etc. For example, the CodeBlue project [3] developed a range of small and wearable wireless vital sign sensors based on the Mica2, MicaZ, and Telos commonly-used sensor platforms [5]-[8]. The developed devices include a wireless pulse oximeter, wireless two-lead EKG, and some specialized sensor motes. Many network-level and system-level mechanisms have been investigated to achieve wireless pervasive communication for healthcare monitoring architectures. The AlarmNET [4] network, integrated with existing medical practices and technology, provides long-term healthcare monitoring for elderly and chronic patients. Other remote sensor systems for healthcare (such as MobiHealth, Lifeguard, Smart Medical Home, AID-N, and SMART) organize smart healthcare processes for timely, continuous, and vitals monitoring plus analysis, etc. However, a monitored individual should feel comfortable and easily move around while wearing a system integrated with biomedical sensors. Therefore, wearable biomedical textile clothing is needed for easy-wearing, comfortable feeling and convenient movement. Moreover, a wearable sensor system situated into clothing is unsuitable as a router for helping other nodes forward data.

Remote healthcare monitoring has the advantages of reduced medical costs, increased medical quality, continuous and timely patient monitoring, complete patient physical data collection, and timely presenting the correct adaptive remedy. The hierarchical architecture is used in wireless sensor network technology development for healthcare monitoring [4], [13], [15], [22], [25], [26]. Each layer in the hierarchy is formed using fixed or mobile nodes and saturated

Manuscript received 23 July 2008.

Y.M. Huang is with the Dept. of Engineering Science at National Cheng Kung University, Taiwan (e-mail: huang@mail.ncku.edu.tw).

M.Y. Hsieh is with the Dept. of Computer Science and Information Engineering at Providence University, Taiwan (e-mail: mengyen@pu.edu.tw).

H.C. Chao is with the Institute of Computer Science & Information Engineering and the Dept. of Electronic Engineering at National Ilan University, Taiwan (email: hcc@niu.edu.tw).

S.H. Hung is with the Dept. of Engineering Science at National Cheng Kung University, Taiwan (e-mail: bonitahung@nchc.org.tw).

J.H. Pa is with the Dept. of Computer Science and Engineering at Kyungnam University, Korea (e-mail: parkjonghyuk1@hotmail.com).

Digital Object Identifier 10.1109/JSAC.2009.090505.

with different computing and communication capabilities. The lower layer is usually designed with low-cost computing, communication capabilities for sensing objectives over a long period of time because only one or two dry batteries and micro-sensing chips are needed. On the other hand, the higher layer is organized with more complicated computing and long-distance communication devices and stations. Hierarchical networks are easily separated into different types of tasks, such as the communication and control transmission paths with reconfigurable mapping and pipeline applications for efficiently reducing power consumption.

Commercially, most wireless electronic devices incorporate Bluetooth technology to allow wireless connection with other Bluetooth-enable devices. Bluetooth is a good candidate for low power consumption wireless communication because the transmission rate and range are nearly 1Mbps and up to 10 or 100 meters respectively. The intention behind Bluetooth development is simultaneous communications between multiple devices to create small group networks in which one master device operates up to seven active slave devices. This is called a piconet. A Bluetooth-based sensor network [9] was presented based on the BTnode technology developed at ETH Zurich. In addition to the Bluetooth protocol, the IEEE 802.15.4 standard [1] specifies a physical layer and medium access control for low-rate wireless personal area networks. The ZigBee [2], based on the IEEE 802.15.4, is designed to perform high level communication protocols using small, low-power digital radios. A large number of research papers used the Zigbee technology to develop inexpensive robust wireless sensing networks (WSN) with a very large set of sensor motes. The typical Zigbee WSN applications contain industrial control monitoring, sensor networks, building automation and home control/automation. However, most mobile computing devices do not yet support Zigbee.

Wireless healthcare sensor network development has several challenges; reliable transmission, individual privacy and security, wearable sensor device power management, wireless node computing and communication diversity and fast and convenient sensor deployment. The schemes proposed in this paper were developed for the following reasons:

1) A wearable healthcare system should consider environmental parameters such as temperature, humidity, light and CO2 gas during monitoring.
2) Medical staff, e.g. a nurse, could be responsible for indirectly collecting real-time physical records from several patients at the same time to promote outpatient or hospitalization services.
3) Security issues [10]-[12] should be considered to assure individual safety and privacy under legal secrecy healthcare requirements.

Therefore, the key benefits of this study include a hierarchical-based architecture applied to three healthcare monitoring applications, the timely and continuously monitoring of individual physiology and environmental physical records, temporary group-based healthcare monitoring, adaptive secure transmissions corresponding to nodes in the architecture.

The remainder of this paper is organized as follows. Section 2 introduces the related works that developed pervasive or ubiquitous healthcare monitoring systems. Section 3 describes a healthcare architecture with three network tiers. The proposed healthcare architecture is applied to home network, nursing home and hospital applications for monitoring and outpatient services. Grouping and ad hoc modes are considered in the network architecture. Section 4 discusses the security mechanisms between different network tiers to achieve individual privacy protection. Section 5 describes the proposed healthcare hardware and software environment applications. Section 6 provides the security analysis and performance evaluation of a prototype monitoring application in the proposed pervasive and secure healthcare network. Conclusions and future work are drawn in Section 7.

II. Related Work

Zhou et al. [14] presented a pervasive medical supervision system in a three layer network structure. Different wearable wireless bio-sensor nodes forming the first network layer were used to sample physiological conditions. Any of those nodes could be set up using a self-organizing or manual configuration as a gateway node for routing sensing data from other nodes. Nodes in the second layer were responsible for reliable data transmission as backbone sensor nodes using mobile phones/PDA depending on two kinds of transmission modes, home mode and nomadic mode. The hospital medical data center acts as the third layer supporting personal services and aggregates patient health data from the other layers.

Kang et al. [26] proposed a wearable context aware system for ubiquitous healthcare, composing of two types of wearable sensor systems: a watch type sensor system and a chest belt type sensor system. The context aware system in distributed networks was configured around wearable sensors, wearable computers e.g. PDA, and internet-based healthcare services. The Zigbee capability is used for communication between wearable sensors and PDAs with a wireless LAN with the 802.11b (Wi-Fi) capability used for communication between PDAs and healthcare service providers on the Internet. The wearable system operates on an OSGi-based context aware framework as a java-based component service middleware.

Using the public key infrastructure (PKI), Haque et al. [15] proposed an efficient security scheme for a hospital healthcare system acting between patients and medical staff e.g. doctor or nurse. This healthcare network was built using a hierarchical model that includes three primary components: Patient (PT), Healthcare Service System (HSS), and Secure Base Station (SBS). The SBS operates as a central key generator, that either a PT or a HSS can establish a pairwise secret with it using the bilateral key handshaking method. As the SBS has prior key knowledge of any PT and HSS, the PT-to-HSS and HSS-to-PT secure communication can be achieved using a secret PT key (or the HSS) disclosed to the HSS (or the PT).

Fei et al. [16] designed a practical hardware/software platform supporting a telecardiology sensor network (TSN) under a typical healthcare community with many elderly patients. The TSN network performs real-time healthcare data collection and supports medical privacy to secure ECG data transmission in wireless channels. This network adopted the Skipjack-based symmetric crypto for one-hop secure ECG

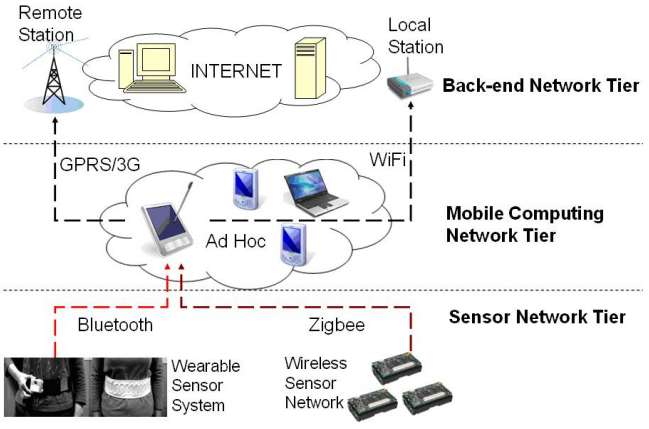

Fig. 1. Healthcare system Hierarchical Network Architecture in wireless sensor networks.

data transmission with low energy and low overhead to preserve the patients' medical privacy. For multiple patient cases, the network acted in a cluster structure to reduce the patient-to-doctor routing overhead and key management with few one-hop hash key chains. The TSN hardware of the sensor platform driven using AA batteries was equipped with RF motes built with Ember CPU-RF chips. The RF board acted as the MCU/ZigBee transceiver unit and the ECG sensor board was designed by the Harvard University CodeBlue team. For different physiological chest leads, the Model 430B, 12-lead ECG simulator in the platform provided a complete PQRST waveform at six preset rates. The TSN software architecture included wireless communication control software ad ECG feature extraction/classification software, performed on the TinyOS platform.

Anthony et al. [4] presented an assisted-living and residential monitoring network (ALARM-NET) for pervasive, adaptive healthcare, organized with a heterogeneous network, context-aware protocols, a query protocol, a hardware-accelerated secure message protocol, and a system implementation. The ALARM-NET included three node types, sensor node, body network, and back-bone nodes to monitor environmental and physiological data of individuals in their residences for analyzing and storage in a back-end database. The sensor nodes maintained connections from body networks to back-end networks for long-term data transmission and query periods. A bridge, denoted as AlarmGate, between the Alarm-NET and Internet allows user interfaces to connect, authenticate and interact with the network. The query processor designed in sensor devices parses query commands to obtain data samples. For example, pulse-rate samples were collected with 5-frequencies in one second. For wireless sensor network security a link security was developed in MICAz and Telos motes using the Chipcon CC2420 radio transceiver following the IEEE 802.15.4 standard. AES-based encryption schemes were implemented in hardware to accelerate the encapsulation of secure packets in the network link layer.

III. System Architecture and Application

This section introduces the proposed network architecture with multiple hierarchical tiers and illustrates three pervasive healthcare applications.

A. Architecture Overview

Three network tiers are applied to the proposed healthcare architecture. Figure 1 depicts the details and relationships among the tiers.

1) Sensor Network Tier: Two types of sensor systems for different sensing objectives are designed to capture the individuals' vital signals and the environmental physical parameters in their residence. Wearable sensor systems (WSS) with Bluetooth wireless transmission are integrated with biomedical sensors installed in a fabric belt. The WSS is conveniently and comfortably tailored to the individual body to capture their physiological data. Wireless sensor motes (WSM) are placed inside buildings to capture the environmental parameters transmitted through a wired or wireless network, communicating using Zigbee wireless technology. Physical records and parameters from the WSS and WSM must be transmitted securely to the upper network tier. The proposed WSS enhances the Bluetooth security authentication and encryption methods [30] by modifying the authentication procedures using AES-based encryption schemes [33]. Secure point-to-point communication between two WSM motes is developed using a polynomial-based encryption [23] scheme. Access to the devices in the upper tier is limited to legitimate WSSs or WSMs which must authenticate themselves before being allowed to connect.

2) Mobile Computing Network Tier: In the healthcare architecture, a number of mobile computing devices (MCD) such as the PDA and laptop are organized regionally using an ad hoc network to route with multiple hops or an infrastructure-based network to connect to a fixed remote or local station. One MCD with enough computation capabilities must capture and analyze physical records from the WSS or WSM because the device does not have mass data storage capability over a long period of time such as a few months or years. However, major or significant data collection storage will be required in the back-end network database through an infrastructure-based mode where one MCD can route data to a station. The ad hoc mode occurs in this tier when one medical person in motion must deliver monitored WSS or WSM data to another staff person in motion. A mobile-to-mobile text-based alarm message is required to show real-time abnormal sensing data findings. One MCD can support the short message service (SMS) using cellular or satellite networks. It can also secure the message through public key cryptosystem. In the case, the MCD must be authenticated by a third party for communication in the back-end network. Then, it obtains a secret key and public/private key pair, shared with the third party after authentication. The secure communication ad hoc mode details are introduced in Section 4. A number of MCDs without any station organized as an ad hoc mode can exchange physical data using on-demand routing protocols (AODV). Hence, secure routing protocols are required. A small temporal group is organized for outpatient healthcare services since one MCD can simultaneously communicate with several WSSs (up to seven) based on the Bluetooth piconet standard. Only a valid MCD set with the enhanced Bluetooth security and polynomial-based encryption schemes can access physical data from the WSS and WSM.