Proceedings of the 2005 IEEE
Engineering in Medicine and Biology 27th Annual Conference
Shanghai, China, September 1-4, 2005

Interoperability and Security in Wireless Body Area Network Infrastructures

Steve Warren[1], Jeffrey Lebak[1], Jianchu Yao[3], Jonathan Creekmore[2], Aleksandar Milenkovic[2], and Emil Jovanov[2]

[1]Department of Electrical & Computer Engineering, Kansas State University, Manhattan, KS, USA
[2]Department of Electrical & Computer Engineering, The University of Alabama in Huntsville, Huntsville, AL, USA
[3]Department of Technology Systems, East Carolina University, Greenville, NC, USA

Abstract—**Wireless body area networks (WBANs) and their supporting information infrastructures offer unprecedented opportunities to monitor state of health without constraining the activities of a wearer. These mobile point-of-care systems are now realizable due to the convergence of technologies such as low-power wireless communication standards, plug-and-play device buses, off-the-shelf development kits for low-power microcontrollers, handheld computers, electronic medical records, and the Internet. To increase acceptance of personal monitoring technology while lowering equipment cost, advances must be made in interoperability (at both the system and device levels) and security.**

This paper presents an overview of WBAN infrastructure work in these areas currently underway in the *Medical Component Design Laboratory* at Kansas State University (KSU) and at the University of Alabama in Huntsville (UAH). KSU efforts include the development of wearable health status monitoring systems that utilize ISO/IEEE 11073, Bluetooth, Health Level 7, and OpenEMed. WBAN efforts at UAH include the development of wearable activity and health monitors that incorporate ZigBee-compliant wireless sensor platforms with hardware-level encryption and the TinyOS development environment. WBAN infrastructures are complex, requiring many functional support elements. To realize these infrastructures through collaborative efforts, organizations such as KSU and UAH must define and utilize standard interfaces, nomenclature, and security approaches.

Keywords—**Bluetooth, CORBA, components, encryption, Health Level 7, ISO/IEEE 11073, MySQL, OpenEMed, plug-and-play interoperability, point of care, telemedicine, telemonitoring, TinyOS, wearable, wireless, ZigBee**

I. Introduction and Motivation

A. Technology Trends and Wearable Devices

Recurring themes in technology forecasting efforts center around telemedicine, predictive diagnostics, electronic medical records, security, human factors, policy changes, and the increased role of the patient in future care scenarios [1-7]. While some of these exercises focus on nearer-term technology, others engage in far-forward thinking, where systems of today are replaced by technology that supports a new care model. Consistent with the latter, we put forward the idea that wearable telemonitoring systems implemented as Wireless Body Area Networks (WBANs) offer opportunities to move **beyond 'telemedicine**,' which purports to replicate the traditional face-to-face patient/physician consultation using technology. The convergence of low-power wireless communication standards, plug-and-play device buses, off-the-shelf development kits for low-power microcontrollers, handheld computers, electronic medical records, and the Internet can provide a more patient-centric care model, where ad-hoc collections of devices could be assembled on-the-fly by a physician, care provider, and/or patient to create monitoring systems matched to patient needs [8, 9].

The number of groups investigating wearable sensors has increased, as evidenced by their representation at recent conferences. Much of this work focuses on the repackaging of traditional parameter measurement sensors (e.g., electrocardiographs, pulse oximeters) for wearability and the signal processing necessary to recover motion-artifact-corrupted data. However, there has also been a movement toward the development of WBANs that incorporate 'invisible' devices, wireless inter-device communication, and PDAs or data loggers as device managers [10-15].

B. Areas Requiring Continued Emphasis

While progress has been made in the areas of wearable sensors and WBANs, more work is needed in (a) **information infrastructures** that facilitate remote storage and viewing of patient data as well as access to external processing and analysis tools via the Internet, (b) the development and use of **interoperability standards** that promote information exchange, plug-and-play device interactions, ease of use, and reconfigurability, and (c) **system-** and **device-level security** functionality that will ensure data integrity and limit access to patient-identifiable information. ***This combination of interoperability and security will help to increase acceptance of ambulatory monitoring technology while at the same time lowering the cost of these systems through vendor competition*** [1, 2, 5, 9].

C. Contents of this Paper

This paper addresses the elements of interoperability and security relevant to WBAN systems. It then presents recent WBAN infrastructure, interoperability, and security work performed at two institutions: the *Medical Component Design Laboratory* at Kansas State University (KSU) and The University of Alabama in Huntsville (UAH). The aim of this paper is to facilitate a dialogue that supports collaborative inter-institutional development, where tools created by different research groups can be more readily integrated into capable WBAN infrastructures through the utilization of interface, nomenclature, and security standards.

This material is based in part upon work supported by the National Science Foundation under grant BES–0093916. Opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

II. Background

A. WBAN Functionality and Interoperability Requirements

WBAN environments pose information challenges that are atypical in clinical monitoring environments. Performance characteristics of typical wireless sensors, such as **processing power** and **available memory**, severely limit real-time capabilities of a typical WBAN. In addition, a personal server must have (a) enough **local storage** to log hours of sensor data and (b) the ability to upload these data wirelessly to a **remote medical record** repository using the **Internet** when a hub becomes available. At this point, the data will be available for **remote access** by physicians and researchers that wish to extract physiologic parameters, apply state-of-health assessment algorithms, note trends in patient data over time, and even predict health crises.

Additionally, WBANs will be assembled and configured by the patients themselves, which imposes **ease-of-use constraints** on the user interface and implies access to a **different class of help resources**. These point-of-care systems must also utilize the same **information exchange standards** and **nomenclature rules** employed by the hospital information network if these data are to integrate seamlessly into a patient's electronic medical record. Finally, these wearable systems must be **reconfigurable** at the device level to accommodate different monitoring needs. This means that the personal server must be able to update its local device registry 'on-the-fly' and alter the lengths of its transmission packets depending on the number and type of sensors worn by the patient. Typical reconfiguration scenarios include (1) **system assembly and disassembly** (e.g., for a bath or exercise in a pool), (2) **sensor removal** (e.g., to change batteries or switch out a poorly functioning device), (3) **sensor addition** (e.g., adding a pulse oximeter to identify desaturation events during exercise or sleep), and (4) changing a sensor's **operational mode** (e.g., asking it to send raw data rather than calculated parameters).

B. WBAN Security

Because WBAN systems and their supporting infrastructure are geographically distributed, they present a greater challenge in the areas of throughput, data integrity, and data security when compared to traditional clinical systems. Besides the engineering issues of just 'making it work,' there are issues of patient protection that become important. These issues speak to '**surety**,' which addresses system viability in the areas of safety, security, reliability, fault tolerance, accuracy, repeatability, and human factors. Patient and data protection require the integration of services to (a) verify the **identity** of the WBAN wearer (i.e., authentication), (b) protect the **confidentiality** of the wearer, (c) establish and maintain **secure links** between the wearer and their personal WBAN as well as an individual sensor and its parent device, (d) maintain the **integrity** of sensor data from initial acquisition to final storage, and (e) **protect access** to stored data or data in transit [16]. Wireless links must therefore transfer encrypted data. These security needs create significant challenges. Fortunately, one advantage of WBAN environments is that the very short communication ranges (several meters) aid secure communication.

III. Methods

As noted in the *Introduction*, research groups at KSU and UAH have been working on efforts that address the requirements necessary to realize effective WBAN systems (see the *Background* section). KSU has recently targeted remote information storage tools based upon industry standards. UAH has recently focused on ZigBee-enabled [17] BAN elements with hardware-level encryption. These efforts will be addressed in this section of the paper.

A. KSU Efforts in System-Level Interoperability

Recent work in the *Medical Component Design Laboratory* at KSU has resulted in a wearable, plug-and-play monitoring system that consists of four component types: (1) a set of plug-and-play, wearable and nearby **sensor units (**electrocardiogram, pulse oximeter, weight scale, and ambient temperature/humidity sensor), (2) a wearable **data logger**, (3) an Internet-ready **base station**, and (4) a set of **local and remote databases** for storing patient data [12, 18]. In this scenario, the base station is the external access point for the personal network created by the data logger and sensor units. The focus of this work has been the incorporation of industry interoperability standards, which include

- Bluetooth™ [19] for wireless telemetry between the components in the point-of-care environment and
- ISO/IEEE 11073 [20] (formerly IEEE 1073 – Medical Information Bus) for plug-and-play interoperability between medical monitoring system components

ISO/IEEE 11073 utilizes the CEN TC 251 VITAL standard [21] for physiologic information representation and access as well as a suite of ISO standards [22]. Bluetooth lower layers provide the transport functionality for this embedded implementation of ISO/IEEE 11073, a standard originally developed for plug-and-play operation between bedside devices and a local hospital network.

Recent and ongoing efforts include tool development for storing patient data into a database, transferring these data to a remote database over the Internet, and presenting and analyzing data on a caregiver screen. This ongoing and future work targets the following system-level standards:

- MySQL [23] for local/remote database functionality,
- Health Level 7 [24] for information exchange, and
- CORBA [25] for physician-side data access, viewing, and analysis.

Sensor data from the monitoring system are saved to a local MySQL database using a LabVIEW virtual instrument [26], or base station (see Fig. 1), which also displays monitoring data and reports the connection and disconnection status of wearable or nearby sensors. To organize these data for transfer via HL7, a Database Inserter written in Java parses the files and stores their contents in the tables of a local MySQL database: a free, reliable data management system. HL7 messages transmit local database information to a re-

mote database. HL7 message creation, transfer, and parsing are accomplished with iNTERFACEWARE's Chameleon software [27], an HL7 messaging client and server software library with tremendous flexibility. Programmers can use Chameleon with Java, C++, and Visual Basic, among other languages. Software writers can customize messages, allowing full HL7 compliance in addition to interfacing with non-standard, in-house messages.

A Chameleon client periodically sends measurement data to a Chameleon server on the remote database. Upon receipt of an HL7 message, the Chameleon server inserts this newly received information into a database using CORBA healthcare services implemented in Java by the OpenEMed tool [28] developed at Los Alamos National Laboratories. The Patient Identification Service (PIDS) and the Clinical Observation Access Service (COAS) constitute two major CORBA healthcare services [25] implemented by OpenEMed. These services define domain-specific objects and interfaces for transferring these objects over the network. PIDS manages Patient IDs and describes patient demographic information (e.g., SSN or address). COAS applies to physiological data (e.g., samples from a pulse oximeter). OpenEMed also implements database access utilities for storing and retrieving healthcare objects. PIDS and COAS both use HL7 v2.3 nomenclature to describe their objects. OpenEMed therefore provides further standardization to an already standards-based system.

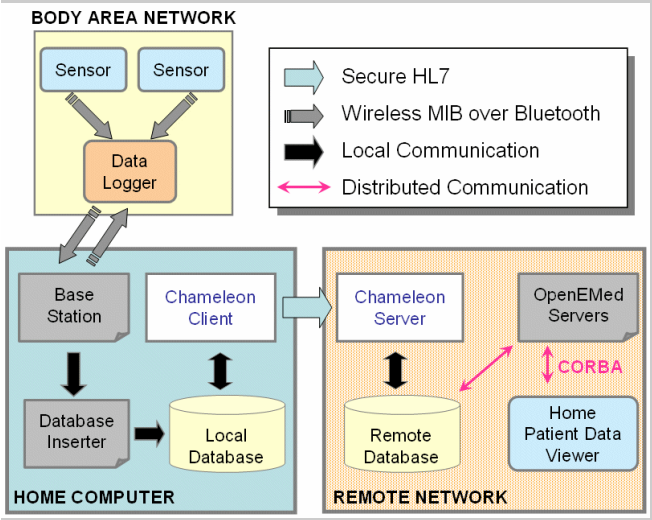

Fig. 1. System/database interaction via Health Level 7.

Once these patient data reside in an external 'hospital' database, physicians and researchers with proper access privileges will be able to retrieve these data via a CORBA-based information viewer, currently under development. This patient data viewer will incorporate the following functionality: (a) select and view archived data for a given patient, (b) zoom in or out of a sample set, (c) request the most recent data, (d) analyze and process signal data, (e) perform trend analyses, and (f) submit orders back to the patient.

When dealing with patient data, care must be taken to address privacy issues outlined by the Health Insurance Portability and Accountability Act of 1996 [29]. Secure connections between a home and a hospital must protect data during Internet transfer. OpenEMed implements a CORBA Healthcare facility called Resource Access Decision (RAD) which limits user access to patient information based on role. The Home Patient Data Viewer uses RAD to control what information is presented to a user (e.g., a researcher wanting to process waveforms would see no identifying information about a patient - only blank datasets). RAD allows a healthcare provider to see all relevant identifying information in addition to waveforms.

B. UAH Efforts with the ZigBee Wireless Standard and Hardware-Level Encryption

The WBAN group at UAH is developing wearable health monitoring systems using off-the-shelf ZigBee wireless sensor platforms (Telos platforms from Moteiv), custom signal conditioning boards, and the TinyOS software environment [30]. TinyOS offers a security platform called TinySec, a link-layer encryption mechanism implemented in software as a security suite for ubiquitous devices. However, the TinySec platform is purely a software encryption engine; it does not utilize hardware encryption on sensor platforms that support it.

As an alternative, the UAH group utilizes hardware encryption supported by the ChipCon 2420 ZigBee complaint RF Transceiver [31] on the Telos platform. This requires a TinyOS extension that uses hardware support for secure AES communication, which is implemented on a ChipCon 2420 controller. The AES hardware encryption in the CC2420 uses a 128-bit encryption key. The goal is to use one key per session, where the personal server shares the encryption key with all of the sensors in the WBAN during the session initialization. The key is loaded to the controller and used throughout the session.

It is noteworthy that hardware encryption does not significantly increase power consumption on the sensor platform. This can be attributed to the efficient on-chip hardware support for encryption on the wireless controller and the dominant power consumption of the RF section when compared to the processing section.

IV. Results and Discussion

These recent efforts at KSU and UAH have demonstrated that it is feasible to incorporate interoperability and security functionality into a WBAN infrastructure. It should be noted that, while HL7 is the most pervasive standard for medical information exchange in the industry, it has not been widely applied to point-of-care systems: only a few HL7-compliant homecare telemedicine systems exist [32]. To the knowledge of the authors, HL7 has not yet been applied in systems that incorporate WBAN technology. Due to the complex nature of HL7, no over-the-counter software exists to "jump start" a home system. Large-scale, hospital implementations have teams dedicated to customizing soft-

ware to work with a hospital's current system, but home care providers cannot currently afford such expenditures.

It is also worth noting that ISO/IEEE 11073, Health Level 7, CORBA, Bluetooth, and ZigBee have sensible mappings to the ISO Open System Interconnect model for standardized component interactions. Health Level 7 has also begun a dialogue with the Object Management Group [25] to link the services supported by the two standards bodies [33].

On the security front, additional options exist for user authentication. First, fingerprint scanners are now available on PDAs as well as PC cards that can interface with handheld computers. Bar code, RFID tag, magnetic stripe, and smart card technologies offer alternatives. Initial physical associations between individual sensors and the personal server can be performed during session setup based upon either sensor activity or a unique device identification number (e.g., 48-bit serial silicon ID on a Tmote sky wireless sensor platform). This is the approach planned by UAH. An alternative to this 3-pin, contact-based approach (which can be considered a form of token-based authentication) would be the use of small, sensor-mounted units based upon the iButton concept from Dallas semiconductor [34].

V. Conclusion

This paper presents an overview of system- and hardware-level WBAN infrastructure work currently underway at KSU and UAH. Recent KSU efforts have targeted the development of HL7-compliant messaging tools and CORBA services for medical information retrieval and analysis. UAH efforts have focused on the development of health and activity monitors that utilize ZigBee wireless connectivity and hardware-level encryption in a WBAN. Future efforts will include the negotiation of interface, nomenclature, and interoperability standards that allow systems like these to be merged into complex WBAN infrastructures. Additional system-level efforts will focus on secure transactions between personal servers and remote electronic medical record databases, which will be accomplished according to the rules set forth in the Health Level Seven Security Services Framework [35].

References

[1] "Strategies for the Future: The Role of Technology in Reducing Health Care Costs," Sandia National Laboratories SAND 60-2469, 1996.

[2] Sill, Anthony E., S. Warren, J. D. Dillinger, and B. K. Cloer. "The Role of Technology in Reducing Health Care Costs," SAND97-1922, DOE Category UC-900, August 1997.

[3] Lewis, Carol. "Emerging Trends in Medical Device Technology: Home Is Where the Heart Monitor Is," *FDA Consumer Magazine*, May-June 2001, pp. 10-15.

[4] Winters, Jack, William A. Herman, and Gilbert Devey. "Workshops on Future Medical Devices: Home Care Technologies for the 21st Century," National Science Foundation, Catholic University of America, U.S. Food and Drug Administration April 7-9, 1999.

[5] "Interoperability Standards for Healthcare Systems of the Future Workshop," San Antonio, TX, 2000.

[6] Foresight. "Healthcare 2020," http://www.foresight.gov.uk/.

[7] "Connecting for Health," Markle Foundation, http://www.markle.org/markle_programs/healthcare/projects/connecting_for_health.php.

[8] Warren, Steve and Atul Dighe. "Workshop on Home Care Technologies for the 21st Century. Topic F: Smart Health Care Systems and the Home of the Future," Department of Health and Human Services April 7-9, 1999.

[9] Craft, Richard L. "Telemedicine System Interoperability Architecture: Concept Description and Architecture Overview," Telemedicine Interoperability Alliance, Sandia National Laboratories 2003.

[10] Jovanov, E., D. Raskovic, J. Price, J. Chapman, A. Moore, and A. Krishnamurthy. "Patient monitoring using personal area networks of wireless intelligent sensors," *Biomed Sci Instrum*, vol. 37, pp. 373-378.

[11] Jovanov, E., A. Milenkovic, C. Otto, and P. C. de Groen. "A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation," *Journal of NeuroEngineering and Rehabilitation*, vol. 2, March 1, 2005, pp.

[12] Warren, Steve, Jianchu Yao, Ryan Schmitz, and Jeff Lebak. "Reconfigurable Point-of-Care Systems Designed with Interoperability Standards," presented at 26th Annual Conference of the IEEE EMBS, San Francisco, CA.

[13] "A Black Box for People," Stanford University, NASA, http://science.nasa.gov/headlines/y2004/07apr_blackbox.htm.

[14] "MobiHealth uses Body Area Network concept to promote personalised mobile health services," Virtual Medical Worlds Monthly, http://www.hoise.com/vmw/02/articles/vmw/LV-VM-10-02-11.html.

[15] "Second International Workshop on Wearable and Implantable Body Sensor Networks," Department of Computing, Imperial College London, http://www.tinyos.net/scoop/story/2005/1/13/82717/5314.

[16] *For the Record: Protecting Electronic Health Information*: National Research Council, National Academy Press, 0309056977, 1997.

[17] "ZigBee Alliance," 2005, http://www.zigbee.org/.

[18] Yao, Jianchu, R. Schmitz, and S. Warren. "A Wearable Standards-Based Point-of-Care System for Home Use," presented at 3rd Joint EMBS-BMES Conference, Cancun, Mexico, 2003.

[19] Bluetooth SIG. www.bluetooth.com.

[20] IEEE 1073. http://www.ieee1073.org.

[21] CEN/TC251, European Standardization of Health Informatics. http://www.centc251.org.

[22] "ISO/OSI 7 Layer model and other models," http://www.hackerscenter.com/Knowledgearea/papers/download/ISO_OSI_7_Layer_model_and_other_models.htm.

[23] "MySQL Developer Zone," http://dev.mysql.com/.

[24] HL7. "Health Level 7," http://www.hl7.org.

[25] "Object Management Group," http://www.omg.org/.

[26] National Instruments. "LabVIEW," http://www.ni.com/labview/.

[27] "iNTERFACEWARE," 2005, http://www.interfaceware.com/.

[28] "OpenEMed," http://openemed.org/.

[29] "The Health Insurance Portability and Accountability Act of 1996 (HIPAA)," Centers for Medicare and Medicaid Services, http://www.cms.hhs.gov/hipaa/.

[30] "TinyOS," SourceForge, 2005, http://www.tinyos.net/.

[31] Chipcon. "CC2420 Product Information."

[32] "Telemedicine Information Exchange," http://tie.telemed.org/.

[33] "Health Level Seven, Object Management Group Begin Joint Healthcare Software Services Standardization Work," http://www.omg.org/news/releases/pr2005/03-08-05.htm.

[34] "iButton Overview," Dallas Semiconductor, 2003, http://www.ibutton.com/.

[35] Kratz, Mary et al. "Health Level 7 Security Services Framework," 1998, http://www.hl7.org/library/committees/secure/HL7_Sec.html.