The Need for Rules of Engagement Applied to Wireless Body Area Networks

Steve Warren[1] 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

Abstract—**Wireless body area networks (WBANs) and their supporting information infrastructures offer unprecedented opportunities to monitor state of health without constraining wearer activities. 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 addresses the functional needs of future point-of-care environments that will employ ad-hoc WBANs for patient monitoring and treatment. It then summarizes the use cases and constraints that will help to formulate rules of engagement for smart, interoperable components that operate within a distributed medical monitoring environment populated by WBANs and other local sensors.**

Keywords—**components, encryption, Health Level 7, ISO/IEEE 11073, plug-and-play interoperability, point of care, security, telemedicine, telemonitoring, wearable, wireless**

I. Background and Motivation

A. Future Health Monitoring Environments

Recent efforts have attempted to forecast medical technology progression and characterize the information infrastructures required to accommodate emerging technologies [1-8]. Recurring themes in these publications center around telemedicine, predictive diagnostics, electronic patient records, security, human factors, policy changes, and the increased role of the patient. While some of these publications focus on nearer-term technology, others engage in far-forward thinking, where systems of today are replaced by technology that provides a completely new care model. Consistent with the latter, we put forward the idea that wearable telemonitoring systems offer opportunities to move beyond 'telemedicine,' which purports to replicate the traditional face-to-face, patient-physician consultation using technology. Some roadmapping efforts assume that these systems will be provided by medical technology companies, and users will have little or no role in their construction. However, the convergence of Internet technology, electronic patient records (EPRs), wearable sensors, portable consumer electronics, and intelligent agents can provide a more patient-centric environment, 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 the patient needs [9-12]. In some cases, these systems may be permitted to make care decisions on behalf of the patient, creating a closed-loop system where the monitor/assess/treat process is automated. Not only will the frequency of care delivery increase for a given patient, but a typical care provider will be able to manage a greater number of patients.

Because of the broad range of possible point-of-care scenarios, these systems will benefit from the availability of smart components that, when assembled, form a robust ad-hoc network and exhibit a collective awareness regarding the patient's state of health. Strict rules of engagement must govern ad-hoc interactions, and these rule sets must rely on interoperability standards and security mechanisms, which together will drive down costs through vendor competition and increase technology acceptance by patients that use the systems [1, 2, 5, 11, 12]. Products that were previously 'stovepipe' systems (one vendor creates all) will then become hybrid systems created by combining off-the-shelf, commodity components manufactured by different vendors.

These distributed, plug-and-play systems will generate important regulatory issues not traditionally encountered in medical monitoring and treatment systems. The U.S. Food and Drug administration (FDA) continues to investigate emerging medical technologies in an effort to anticipate these system and device trends [3, 4, 10, 13-15].

B. Hospital Versus Point-of-Care Infrastructures

EPRs, interoperability standards, and security will form the backbone of future medical systems. Guided by both near-term needs and far-forward technology forecasting efforts, hospital-to-hospital information exchange technology has incorporated a growing number of EPR middleware tools [16], information exchange standards [17-20], nomenclature standards [21-24], and security mechanisms [25, 26]. Further security guidelines for clinical environments have been published by HIPAA [27], the National Research Council [28], and the Markle Foundation [6].

Unfortunately, the evolution of EPRs, interoperability standards, and security technology geared toward wearable systems (e.g., for home care or telerehabilitation) has been slow. Recent projects have merged hospital-owned EPRs into regional databases in an effort to share access to medical information, but the clients that have access to these repositories do not typically include homes and individuals. In addition, these repositories have been designed as read-only archives that are not intended to store data streams generated by home monitoring equipment, where data corruption is a primary concern. A small number of efforts have looked at HL7 to upload data from store-and-forward, desktop telemedicine systems [29, 30], but information ex-

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.

change and nomenclature standards have not been well integrated into ambulatory point-of-care environments.

The lack of technology progression in the point-of-care arena is especially true for systems which incorporate embedded devices that do not have access to the resources of an operating system, such as microcontroller-based devices designed to operate for months or years on a single battery. Some interoperability work has been done at the bedside-device level through the Medical Device Communications Industry Group (MDCIG), which has developed the IEEE 1073 (a.k.a. Medical Information Bus (MIB)) standards for plug-and-play medical devices [31, 32]. This group of standards was recently renamed the ISO/IEEE 11073 standards (a.k.a. X73) to reflect efforts to internationalize the standards. In addition, a handful of desktop telemedicine systems use USB, FireWire, and wireless technologies (e.g., Bluetooth and Wi-Fi) to enable flexible sensor configurations [33]. A related effort led by Kang Lee at the National Institute of Standards and Technology is working toward the integration of wireless standards such as Bluetooth into the IEEE 1451 Smart Sensors standard [34, 35]. With the exception of IEEE 1073, these plug-and-play technologies provide technical ad-hoc connectivity based upon the 7-layer ISO/OSI protocol stack, but they do not address the domain-level 'rules of engagement' that specify interactions and security for the target application.

An ongoing effort at Kansas State University has shown that IEEE 1073 can be migrated down to the embedded level via minor modifications to the formal standard [36-38]. This system, which utilizes MIB for device-to-device interactions and Bluetooth wireless technology for physical data transport, is being upgraded to incorporate HL7-based information exchange with an external SQL database [29, 39]. Note that the MDCIG has been involved in discussions with the HL7 working group regarding how these two standards might coexist with one another.

While interoperability technology has not made major in-roads into point of care environments, some security has been implemented at the system level, primarily by desktop telemedicine vendors interested in tapping the home care market. While most of these systems provide encryption capabilities and incorporate user name and password access (this assumes a keyboard is present), they do little to authenticate the identity of the user through other means. A small number of vendors has begun to offer device-level security options such as fingerprint biometrics, voice recognition, and iButton access. Given the amount of functionality in future systems that would no longer be under the control of the care provider, it will be more important than ever to authenticate the identity of a WBAN user and thereby maintain the integrity of their electronic medical record.

C. Contents of this Paper

The goal of this paper is to facilitate a dialogue regarding broad rules of engagement that can guide and supplement current WBAN work in interoperability and security. The following section addresses WBAN functional requirements in the areas of interoperability and security. The document then specifies use cases, guidelines, and assessment questions that will drive the development of rules of engagement applied to ad-hoc WBAN systems.

II. WBAN Functional Requirements

A. Overall Goals of Near-Term WBAN Research

High-impact WBAN efforts share two broad and complementary goals: (1) to enable data acquisition, analysis, and information sharing in real-world ambulatory monitoring environments and (2) to utilize technologies and design approaches that promote acceptance of wearable monitoring systems, whether for rehabilitative or preventive care. These broad goals are supported by five specific aims:

1. Create **distributed information infrastructures** to acquire, store, and analyze electronic patient data.
2. Design **wearable/remote sensors and devices** suited to point-of-care environments.
3. Research, develop, and assemble technology tools that promote system- and device-level **interoperability**.
4. Utilize effective **security** mechanisms in wearable device networks.
5. Define **rules of engagement** for smart, interoperable components that populate distributed monitoring and treatment systems.

These aims are critical for the realization of ambulatory monitoring environments. Additionally, Aims 3 through 5 support acceptance of this technology: interoperability technology promotes ease of use and vendor competition, allowing best-of-breed solutions to interact with one another. Security and clear rules of engagement do and will provide peace of mind to patients and providers.

B. Information System 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, limit real-time capabilities of a typical WBAN. In addition, a personal server (a.k.a. wearable data logger) must have (a) enough local storage to log hours of raw or processed 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 should be designed in such a way that they can be assembled and configured by the patients themselves, which imposes ease-of-use constraints on the user interface and implies ready access to 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.

The requirements above imply 'interoperability,' which has multiple connotations. First, interoperability implies that elements of a system can exchange information and understand one another's syntax and nomenclature. Second, interoperability implies ease of use, or plug and play, where the user can insert a device into the WBAN and assume that it will function correctly with no additional intervention on their part. Third, interoperability implies that devices from different manufacturers can be used simultaneously in the same system. This leads to reconfigurability, where one device can be swapped out for a different type of device, or a device can be added to an existing system. Standards, whether proprietary or consensus, are key to the realization of interoperability at both the system and device levels.

C. Surety

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 [28]. Wireless links, whether on the body or otherwise, must therefore transfer encrypted data. These security needs create significant challenges. One fortunate advantage of WBAN environments is that very short communication ranges (several meters) aid secure communication.

III. Rules of Engagement for WBAN Systems

As noted earlier, emerging technologies offer the potential for ad-hoc collections of devices to be assembled on-the-fly to create monitoring systems matched to patient needs. However, configuring collections of components in an uncontrolled setting can lead to surety issues that are different than those encountered in a hospital or clinic. While transport standards such as USB and Bluetooth map to the 7 layers of functionality in the ISO/OSI reference model, their designs only address the technical ability of a device to interact with similar devices. Domain rules regarding (a) the environments within which these devices can function, (b) which devices are allowed to interact (and which are not), (c) how device information can be used, etc. are not specified. WBAN implementations targeted at real point-of-care environments must adhere to predefined rule sets (i.e., rules of engagement) that dictate device association and security protocols.

A. Broad Guidelines

An overarching need is to draft the early rules of engagement that can be used to guide standards work. These formalized component association guidelines can then be merged with domain standards under development for bedside device interoperability and hospital-to-hospital information exchange. Two relevant standards development groups are (1) the Medical Device Communications Industry Group, which oversees the development of the IEEE 11073 (a.k.a. X73) standards for medical device interoperability and (2) the Healthcare Domain Task Force (a.k.a. CORBAmed) within the Object Management Group [19].

We assert that smart components (a.k.a. objects) can be defined with standard, vendor-independent parameters (a.k.a. attributes) and interfaces (a.k.a. methods) to support component-level interoperability and security. This implies that, once a component is inserted into a system, it can negotiate information exchange, security, and the terms of its use, minimizing the need for user interaction or custom domain-level limitations. This is true ad-hoc connectivity: once the request for association is initiated, the remainder of the process is negotiated without the assistance of the user. This demands component self-awareness, where each component should know about itself (what it can do; how to interpret its data; how to assess its own condition, etc.) and about its context (who may use it and how, etc.).

Note that these rules of engagement deal with more than just the order of operations. They also address message syntax, data precision, sample rate/interval, device descriptions, nomenclature, session information, and other bookkeeping parameters that allow one device to interpret the information from another device. Simply stated, the rules of engagement provide application, or domain-level, conventions for operation order and security, whereas lower-level standards provide behavior that supports technical interoperability as specified in the ISO/OSI reference model.

B. Use Cases

Rules of engagement for a WBAN, including which devices will be allowed to link with one another, can be stored on any (or all) of the devices in the network. Local device registries will change as new sensors are added to or removed from the local network. Reconfiguration is a required element of this design, as multiple scenarios can require that a personal server intermittently update its device registry and subsequently the size and frequency of its message packets. Reconfiguration scenarios include

- system assembly/disassembly,
- sensor removal,

- sensor addition, and
- changing a sensor's operational mode.

In other words, the list of devices that communicate with another wearable device is not fixed and should therefore not be 'hard coded' into these network components. When a hardware or software change is made to the system, the event should be recorded. The system should also record the identification number of each sensor from which data are obtained. Additional use cases include the following:

- local rather than remote data storage,
- data uploads to an external database,
- failure of an existing sensor,
- inability of a device to upload or store data,
- user authentication,
- device-to-personal-server association via contact,
- inclusion of a nearby non-WBAN sensor, and
- existence of another WBAN within the range of the current wearer.

Anticipating and addressing scenarios like these simply amounts to asking questions like "What do we want to happen?", "What can we expect to happen?", and "What can go wrong?" These questions are important in environments that must employ high assurance devices. Even with simple use cases, the rules of engagement can change depending upon whether the sensor, personal server, or either is allowed to request a connection [36, 38].

C. Example Scenario

The following is a contrived scenario where the availability of ad-hoc component connectivity would be helpful. Consider a situation where an ECG sensor on a patient has begun to fail at a time when recent trend data have indicated the need for continuous rather than periodic heart rate monitoring. The ECG notifies the personal server (PS) that a hardware failure no longer permits reliable heart rate calculations. Realizing that the problem cannot be addressed by the user, the PS sends out a wireless query to see if alternative devices exist nearby. It then receives a response from a nearby device (D), which initiates a dialogue:

[D] "I am uncommitted pulse oximeter. Can I help?"

[PS] "Describe yourself."

[D] "I am an Acme model P13 finger-worn unit with version 1.3a hardware and version 2.1 software drivers. I provide heart rate and blood oxygen saturation with a relative accuracy of 1% and 3%, respectively. I comply with the IEEE 11073.1.1.d interoperability specification and use VITAL v1.2b physiologic data nomenclature. I also support 128-bit public key encryption and can establish an association after physical contact. You can download my drivers at https://nonin.com/p13driv.htm. Shall I proceed?"

[PS] "Yes."

[D] "I will send you an audio clip that tells the user how and where to place me. Then I will beep for 45 seconds unless I experience a prior association event."

The PS then sends the audio message to the user through its speaker: "Your ECG device is experiencing a technical problem. Please locate the beeping sensor and touch its lighted base to the light pad on your PDA. Then open the clip and place the new sensor on the tip of your left ring finger. A service request has been filed on your behalf, and a medical technician will arrive soon."

This scenario points out the fact that much more capable monitoring systems could be constructed with smart components if standard domain rule sets existed to handle events relevant to wearable point-of-care systems.

IV. Discussion

A domain-level model for point-of-care monitoring systems would need to address use cases, stakeholders, security levels, association/disassociation protocols, roles, resources, devices, patient records, services, processing, communication, and user interfaces. The purpose of this domain model would be to provide high-surety systems [28] in an environment where care provider control is virtually unavailable.

The FDA has an interest in identifying products and technologies that have the potential to decrease surety in medical systems, since it is their obligation to develop regulations and approval procedures that protect patients from poorly designed hardware and software. Issues like the following will need to be considered during the creation of the draft domain model if monitoring systems based upon the model are to be successfully realized:

- Devices intended for other environments will be inserted into these ad-hoc systems. Should data from these devices populate electronic patient records? What limits do we place on manufacturer liability when these devices are applied improperly?
- How can component collections recover their previous state after a failure?
- If independent components can introduce themselves to other systems, can they assume inappropriate roles? How can we guarantee that they will lock themselves out of inappropriate environments? How can systems reject unapproved components?
- A virtual medical system comprised of a large number of components has an increased probability of generating false alarms and subsequent secondary alarms.
- How can we avoid run-away situations due to misinformed components?
- How can human factors testing be applied to systems assembled on-the-fly?
- How can we set up testing protocols for components that can be arranged in myriad configurations? How can we test for unintended interactions?
- At would point should a smart point-of-care system give up and call for help?
- Wireless devices may saturate home care environments with EMI interference.
- What closed-loop therapy limits should apply?
- Boundaries of highly distributed systems can be very difficult to define/control.

- Should we create FDA-approved software component repositories to which systems must link if they wish to apply remote processing algorithms and download device upgrades? Can we allow processing and decision support algorithms from other countries to contribute?

V. Conclusion

Emerging technologies offer the potential to create intelligent, closed-loop monitoring and treatment systems that support point-of-care environments matched to patient needs. To fully realize the benefit of these networked tools at low cost, interoperability and security technology must be purposefully embedded into these component environments. This speaks to the need for more formalized and widely accepted rules of engagement that specify the protocols and role-based component interaction rule sets.

References

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

[2] A. E. Sill, 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] W. A. Herman, D. E. Marlowe, and H. Rudolph. "Future Trends in Medical Device Technology: Results of an Expert Survey," Center for Devices and Radiological Health, 1998, http://www.fda.gov/cdrh/ost/trends/toc.html.

[4] J. Winters, W. A. Herman, and G. 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.

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

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

[8] "High Confidence Medical Device Software and Systems (HCMDSS) Workshop," Computer and Information Science, University of Pennsylvania, 2005, http://www.cis.upenn.edu/hcmdss/index.php3.

[9] S. Warren, et al. "A Proposed Information Architecture for Telehealth System Interoperability," Proceedings of the first joint BMES/EMBS conference Serving Humanity, Advancing Technology, Atlanta, GA, USA., 1999.

[10] S. Warren and A. 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.

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

[12] R. L. Craft. "Toward Technical Interoperability in Telemedicine," *Telemedicine and e-Health*, vol. 11, pp. 384-404, 2005.

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

[14] S. Warren. "Beyond Telemedicine: Infrastructures for Intelligent Home Care Technology," 2003, http://www.cise.ufl.edu/~helal/preICADI.

[15] S. Warren. "Infrastructures for Intelligent Home Care Technology," Staff College of the Food and Drug Administration, Center for Devices and Radiological Health, Rockville, MD, 2003.

[16] "Status Report 2002: Electronic Health Records," Medical Records Institute, 2002.

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

[18] R. Noumeir. "DICOM Structured Report Document Type Definition," *IEEE Transactions on Information Technology in Biomedicine*, vol. 7, pp. 318-328, 2003.

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

[20] J. Ingenerf, J. Reiner, and B. Seik. "Standardized terminological services enabling semantic interoperability between distributed and heterogeneous systems," *International Journal of Medical Informatics*, vol. 64, pp. 223-240, 2001.

[21] S. Pavlopoulos and A. Anagnostaki. "Vital signs monitoring from home with open systems," *Stud Health Technol Inform.*, vol. 77, pp. 1141-1145, 2000.

[22] A. Anagnostaki, S. Pavlopoulos, and D. Koutsouris. "XML and the VITAL standard: the document-oriented approach for open telemedicine applications," *Medinfo.*, vol. 10, pp. 77-81, 2001.

[23] M. I. Lieberman, T. N. Ricciardi, F. E. Masarie, and K. A. Spackman. "The Use of SNOMED© CT Simplifies Querying of a Clinical Data Warehouse," Proc AMIA Symp, 2003.

[24] J. Bowie. "Four Options for Implementing SNOMED," *J AHIMA*, vol. 75, pp. 30-33, 2004.

[25] B. Blobel and M. Holena. "CORBA Security Services for Health Information Systems," *Int J Med Inf.*, vol. 52, pp. 29-37, 1998.

[26] H. Schull and V. Schmidt. "MedStage - Platform for Information and Communication in Healthcare," *Stud Health Technol Inform.*, vol. 77, pp. 1101-1105, 2000.

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

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

[29] J. Lebak, J. Yao, and S. Warren. "HL7-Compliant Healthcare Information System," *Telemedicine and e-Health*, vol. 11, pp. 252, 2005.

[30] H. Garsden, J. Basilakis, B. G. Celler, K. Huynh, and N. H. Lovell. "A Home Health Monitoring System Including Intelligent Reporting and Alerts," EMBC 04: Annual Conference of the Engineering in Medicine and Biology Society, San Francisco, CA, 2004.

[31] R. J. Kennelly and J. Wittenber. "New IEEE Standard Enables Data Collection for Medical Applications," Proceedings of the 18th annual symposium on Computer Applications in Medical Care, Washington, DC, 1994.

[32] R. J. Kennellly and R. M. Gardner. "Perspectives on Development of IEEE 1073: 'The Medical Information Bus'," *International of Clinical Monitoring and Computing*, vol. 14, pp. 143-149, 1997.

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

[34] K. Lee. "IEEE 1451: A standard in support of smart transducer networking," Proceedings of the 17th IEEE Instrumentation and Measurement Technology Conference, 2000.

[35] K. Lee. "Sensor networking and interface standardization," Proceedings of the 18th IEEE Instrumentation and Measurement Technology Conference, 2001.

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

[37] S. Warren, J. Yao, R. Schmitz, and J. Lebak. "Reconfigurable Point-of-Care Systems Designed with Interoperability Standards," 26th Annual Conference of the IEEE EMBS, San Francisco, CA, 2004.

[38] J. Yao, R. Schmitz, and S. Warren. "A Wearable Point-of-Care System for Home Use that Incorporates Plug-and-Play and Wireless Standards," *IEEE Transactions on Information Technology in Biomedicine*, vol. 9, pp. 363-371, 2005.

[39] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov. "Interoperability and Security in Wireless Body Area Network Infrastructures," 27th Annual Conference of the IEEE EMBS, Shanghai, China, 2005.