AYUSHMAN: A Secure, Usable Pervasive Health Monitoring System

K. Venkatasubramanian, and S.K. Gupta
IMPACT Lab School of Computing and Informatics
Arizona State University
Tempe, AZ 85287
{kkv, sandeep.gupta}@asu.edu
http://impact.asu.edu

ABSTRACT

Ayushman is a pervasive health monitoring system which has the ability to collect, process, store and display health data in a *secure and easy to use* manner. Recent years have seen considerable activity in this field. Most of these systems tend to treat health monitoring as an extension to generic sensor networks. and depend on a network of wearable and implanted, medical and ambient sensors (called a body area network) for data collection and transport. We contend that this paradigm is not suitable for medical monitoring given the low reliability of the sensors, and the mission critical nature of medical monitoring. Further, the existing systems mainly focus on patient monitoring and do not consider security at all, and those that do, treat it in an isolated manner. With *Ayushman* we present a system which addresses both these issues. It integrates sensors and highly capable entities in the back-end to provide *robust* health monitoring. It also considers security as an integral part of its design. Sensors in Ayushman utilize *physiological values based security* for securing their communication. Our design approach enables Ayushman to provide health monitoring in a secure and usable manner - a property that traditional systems lack.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and Design*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*; J.3 [**Life And Medical Sciences**]: Medical information systems, Health

General Terms

Design, Usability, Security, Health Monitoring

Keywords

Pervasive Health Monitoring, Ayushman, Physiological Value based Security

1. INTRODUCTION

In this work we present a prototype of the pervasive health monitoring system we are building in the IMPACT lab at Arizona State University called **Ayushman**. Our *motivation* for developing Ayushman is to build a pervasive health monitoring system that can be used for remote and in-situ monitoring of individual or a large population of patients in an efficient manner. The current method of health management, which expects patients to detect symptoms and contact a medical professional (who then diagnose and treat the problem), is inherently slow and reactive in nature. With an automated health monitoring system, we can reduce the number of visits to caregivers or care facilities for patients thereby reducing cost. It also allows caregivers to manage a larger number of patients simultaneously, by allowing them to focus on only those patients who need attention at any given time. Health management can thus become proactive and efficient.

With Ayushman we are building a real-time patient monitoring system which is secure, robust (available, dependable) and easy to use. In this regard we are building the system based on the following **guiding principles**: 1) to provide a secure health monitoring such that security does not interfere with the health data collection and management aspects of the system; and 2) to provide a robust architecture which integrates low-capability sensors and capable (those with high computational, communication and storage capabilities) back-end entities for collecting, storing, analyzing and visualizing patient medical information. Our ultimate aim is to make health monitoring truly pervasive - a system which can not only be used for monitoring people with ailments but also aid normal people in maintaining a healthy lifestyle. For such a system to be possible, health monitoring has to attain a character where usability of the system is complimented with secure and robust data collection.

The focus of the pervasive health monitoring research in recent times has been either on developing hardware for medical monitoring [7] [12] [6] or building systems for monitoring patients for specific ailments [12] [13] [5] [1]. These systems are, for most part, designed along the lines of traditional sensor networks. Sensors are deployed on a large group of people and their environs for monitoring physiological and environmental stimuli. The collected data is routed over a multi-hop network formed by the networking-capable sensor nodes (spanning multiple patients) to a central base station. As this approach relies on the sensors to relay the data collected, it implicitly assumes that the people being monitored have limited mobility (within a building or home). This reliance on sensors for data collection, distribution and management in a mission critical domain such as health monitoring may be a problem given their low reliability. With Ayushman, the main responsibility of sensors is to collect medical data. The processing, distribution and management is taken care of by more capable back-end entities implemented on hand-held devices and workstations. The sensor network range is limited to a single patient, and forwarding of data beyond this body area network is taken care of by devices much more capable than

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
HealthNet '08, June 17, 2008, Breckenridge, CO.
Copyright 2008 ACM ISBN 978-1-60558-199-6/08/06 ...$5.00.

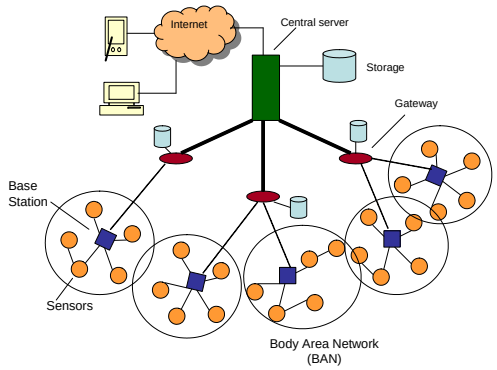

Figure 1: Ayushman Architecture

the sensors. We contend that such a hybrid system enables a more robust data collection and management than traditional systems.

Further, most of the existing systems do not consider security at all. Any user (and the environment itself) is considered benign and security is mostly dispensed with. Such an approach can have serious consequences especially as the technology becomes more wide-spread. Those who do recognize the potential threats consider security in isolation resulting in solutions which require - 1) initialization and setup of keying materials [4] affecting system autonomy, 2) large storage space [4] affecting the efficiency, and 3) large computation and communication requirements [8] [15] affecting efficiency and availability of the system. This results in solutions which interfere with health monitoring and thus have limited usability - one of the main reasons why security is avoided in the design of systems in the first place. With Ayushman, we use *physiological values directly for generating cryptographic keys* in order to secure the sensed health data. This environmentally coupled way of key generation means nodes do not require any additional keying material to secure inter-sensor communication. Sensors can now be strapped on by a user and automatically ensure secure communication. No *a priori* setup is necessary [2] [11] [9]. This has the potential to make security available without affecting the primary functionality of health monitoring - health data collection and management. We are developing Ayushman using only off-the-shelf hardware technologies. Enabling these various component technologies to reliably function together in a medically dependent manner is a major challenge addressed by the Ayushman system. A preliminary version of the Ayushman architecture was presented in [10] where we mainly focused on our vision with respect to Ayushman.

2. DEMONSTRATION

We herein focus on two principal aspects of Ayushman: robust data collection and usable security.

2.1 Data Collection Infrastructure

The Ayushman system is organized as a collection of inter-networked heterogeneous components such as wireless sensors, medical devices, hand-held devices to form a health monitoring system. Figure 1 shows its organization which we now describe. The principal component of Ayushman is the **Body Area Network** (BAN). The BAN is responsible for collecting physiological and environmental data from patients. The environmental sensors provide the context for the physiological data. All the sensors on a patient send their data over a multi-hop network to a sink called the *base station*. The sink is responsible for processing the data from the sensors and is much more capable than the sensors. An important characteristic of BANs is that its constituent sensors have very limited capabilities, they may be potentially large in number, and require constant adjustments from patients to function correctly. Data collected within a BAN is forwarded regularly to the **Back-end Systems** for storage, processing visualization and remote access. The constituent entities of Ayushman back-end are highly capable unlike the BAN, and therefore can utilize complex schemes for ensuring security. The entire system is organized in the form of tiers the depth of which, is application dependent. The sensors form the lowest tier of the system.

2.1.1 Implementation

The current prototype of Ayushman is a two-tiered system with a BAN (one for each patient) and the central server (which forms the back-end) and collects data from the BAN. We have implemented the BAN using MicaZ and TelosB motes (http://www.xbow.com). Both classes of motes have a 8MHZ processor, utilize a ZigBee radio to communicate and are powered with 2AA batteries. We utilized the built-in sensors on TelosB motes to collect environmental data such as ambient temperature, and humidity. The MicaZ motes are utilized for physiological data collection by interfacing them to monitoring devices. We use MicaZ motes to collect three types of physiological data: blood pressure, blood oxygen and acceleration. We designed custom interface boards in-order to be able to connect the devices to the motes. Figure 2 shows the different components in our setup. The environmental and physiological data from the motes is sent at regular intervals to a base station. We have implemented the base station on a Dell Axim PDA running Pocket PC 2002. The reason for choosing the PDA was because of its ubiquity, light-weight, processing capability, multi-modal communication capability and screen for data visualization. As the PDA does not have the ZigBee interface, we connected a mote to the PDA both of which communicated using the serial interface. The PDA receives data from each mote in one hop, forming a star topology with the base station forming the hub. Other topologies and multi-hop networks can be easily implemented without loss of functionality. To handle the different types of sensors and medical devices, implemented a sensor abstraction layer which keeps the details of sensors' workings from the data management and visualization applications. Once the patient data has been processed, the derived physiological parameters are sent over to a central server. This is done over a Wifi connection in our setup. The central sever stores the data received in an MS Access database and connects to remote clients over the Internet. The data communication between the base station and the central server is done using XML format which allows platform independent way of communicating patient data. Remote clients connect to central server at a specific port to query patient data. The central server provides multiple ports for receiving queries from the patients, this allows remote clients to view both past and real-time data from a patient at the same time.

Some of the challenges we encountered during the development include: 1) *Platform Selection*: To successfully build a system with heterogenous components and technologies, one needs to be very careful in choosing the hardware and software platforms. Improper choices may lead to compatibility issues which slow down the development. For example during our initial setup we decided to program the PDA (executing Pocket PC 2002) using Java. We found that even though the system worked, the IBM J9 JRE we utilized for this purpose was highly unstable on a PDA running Pocket PC. Once we switched to .NET platform the problem was solved. 2) *Technological Change*: As technology keeps changing and new tools are available everyday, having a specific technology dependent infrastructure made system improvements difficult. We therefore spent some time in making the system as technology independent as possible by implementing the XML based message

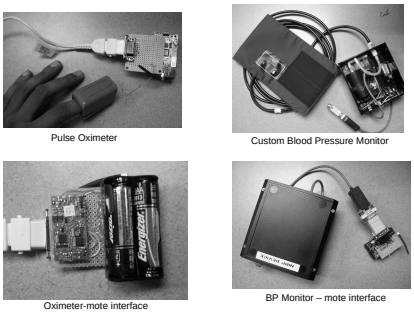

Figure 2: Ayushman Implementation

exchange and simple sensor abstraction layer.

2.2 Usable Security

Collecting data is not enough, it needs to be secured as well. Lack of adequate security features may not only lead to a breach of patient's privacy but also potentially allow adversaries to modify actual data resulting in wrong diagnosis and treatment [11] [3]. Security for sensors usually relies on cryptographic keys to secure their communication. However these traditional approaches may potentially involve considerable latency during network initialization or any subsequent adjustments, due to their need for predeployment. We use physiological values as a basis for maintaining communication security. The stimuli utilized are dynamic in nature and vary unpredictably with time. Therefore each measurement of stimuli produces a different value making it difficult to guess, a very useful property in BAN which is deployed for long durations of time. Keys need not be stored at each node but generated as and when required. This property of using physiological values ensures that security is provided without affecting the autonomy, efficiency or availability of the system - making it usable.

2.2.1 Implementation

The implementation of physiological value based security has two main aspects: physiological value (PV) measurement and key generation. The first step in the whole process is to decide on the physiological values which can be used. So far we have worked with electrocardiogram (EKG) signals, which were obtained from the MIT PhysioBank database (http://www. physionet.org/physiobank/). A scheme for generating identical keys at two communicating sensors is described in [9]. The scheme is based on synchronized measurement followed by an exchange of hashed value of frequency components of the sensed signal to identify identical keys. The initial results based on EKG data of 31 patients from MIT PhysioBank database are quite promising. We are currently in the process of implementing this scheme. The main challenge we face is the availability of sensor nodes on which one can implement real domain FFTs. One option we are exploring is to integrate a low-power FFT processor with a mote [14].

3. CONCLUSIONS

In this work we presented our experiences in building Ayushman, a secure and usable pervasive health monitoring system. It integrates health monitoring sensors with highly capable entities to robustly collect patient data, and utilizes physiological values for generating keys and securing inter-sensor communication.

4. ACKNOWLEDGEMENTS

We gratefully acknowledge the contributions of Ayan Banerjee, Gianni Giorgetti and Guofeng Deng of the IMPACT Lab. This research was funded in part by National Science Foundation Grant CNS-0617671 and MediServe Information Systems.

5. REFERENCES

[1] Intel Proactive Health. http://www.intel.com/research/prohealth/.

[2] S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body. pages 432–439, October 2003. In Proc. of Wireless Security and Privacy Workshop.

[3] D. Halperin and T.S. Heydt-Benjamin and B. Ransford and S. S. Clark and B. Defend and W. Morgan and K. Fu and T. Kohno and W.H. Maisel. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. 2008. In Proc. of IEEE Symposium on Security and Privacy.

[4] L. Eschenauer and V. D. Gligor. A Key-Management Scheme for Distributed Sensor Networks. pages 41–47, November 2002. In Proc. of the 9th ACM conference on Computer and Communications Security.

[5] E. Jovanov, 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*, 2(6), March 2005.

[6] K. V. Laerhoven and H. W. Gellersen. Spine versus Porcupine: A Study in Distributed Wearable Activity Recognition. pages 142–149, Oct 2004. In Proc. of 8th Int. Symposium on Wearable Computers.

[7] P. Lukowicz, U. Anliker, J. Ward, G. Tröster, E. Hirt, and C. Neufelt. AMON: A Wearable Medical Computer for High Risk Patients. pages 133–134, October 2002. In Proc. of IEEE 6th Int. Symposium on Wearable Computers.

[8] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar. SPINS: Security Protocol for Sensor Networks. *Wireless Networks*, 8(5):521–534, September 2002.

[9] K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta. EKG-based Key Agreement in Body Sensor Networks. April 2008. In Proc. of the 2nd Workshop on Mission Critical Nets.

[10] K. Venkatasubramanian and et al. Ayushman: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed. pages 406–407, June/July 2005. In Proc. of the IEEE Int. Conf. on Dist. Comp. in Sensor Sys.

[11] K. Venkatasubramanian and S. K. S. Gupta. Security for Pervasive Health Monitoring Sensor Applications. pages 197–202, December 2006. In Proc. of the 4th Int. Conf. on Intell. Sensing and Infor. Processing (ICISIP, 2006).

[12] Victor Shnayder and Bor-rong Chen and Konrad Lorincz and Thaddeus R. F. Fulford-Jones, and Matt Welsh. Sensor Networks for Medical Care. April 2005. Harvard University Technical Report.

[13] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, and J. Stankovic. An Assisted Living Oriented Information System Based on a Residential Wireless Sensor Network. April 2006. In Proc. of the Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare.

[14] A. Wang and A.Chandrakasan. A 180-mv subthreshold FFT processor using a minimum energy design methodology. *IEEE Journal on Solid State Circuits*, 40(1):310–319, January 2005.

[15] S. Zhu, S. Setia, and S. Jajodia. LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(4):500–528, November 2006.