Towards Supporting Contextual Privacy in Body Sensor Networks for Health Monitoring Service

Fuming Shih[1] and Mi Zhang[2]

[1] MIT CSAIL, Cambridge
Massachusetts, USA
[2] Department of Electrical Engineering
University of Southern California
Los Angeles, USA
{fuming@mit.edu, mizhang@usc.edu}

Abstract. Body Sensor Network (BSN) is a network of sensors attached to human bodies. It can facilitate observers (such as physicians) to monitor subject's (patients) current status. By continuous monitoring physiological vital signs and physical activities, healthcare professionals can obtain a much more accurate description of a patient's health condition. Moreover, patients being monitored can be free from a constrained environment to continue a regular life. However, privacy issues should be well addressed to ensure the appropriate use of the sensitive data collected from BSN. In this paper we present the findings of privacy issues of applications in BSN and a model to capture privacy concerns. The goal is to build a policy-driven, customizable networked wearable sensor system for health and wellness monitoring. The system will support dynamic configuration of sensors to reflect the privacy policy specified by the user, and disclose the user's sensing data accordingly.

1 Introduction

Traditional health care services are primarily based on scheduled evaluations at clinic visits that are intended to detect the onset of an illness. However, this methodology has two major drawbacks. First, it only provides instantaneous snapshots of the patient's health state. Second, it fails to acquire patient's health information that can only be acquired in a natural environment, such as home or workplace where important events or symptoms may manifest.

The emergence of body sensor networks (BSN) attempts to fill in this gap. Body sensor network is a network of sensors attached to the human bodies. These networked systems continuously monitor patients' physiological and physical conditions, and transmit sensed data in real time via either wired or wireless technology to a centralized location where the data can be monitored and processed by trained medical personnel. Numerous assets are provided beyond what is currently available with traditional methods by using these systems: (1) BSN enables continuous monitoring of the patients using high-fidelity sensors such that symptoms that could occur at any time can be captured precisely; (2) Instead of staying at hospital, patients with BSN equipped can be monitored in a natural environment. As a result, the quality of the sensed data is improved.

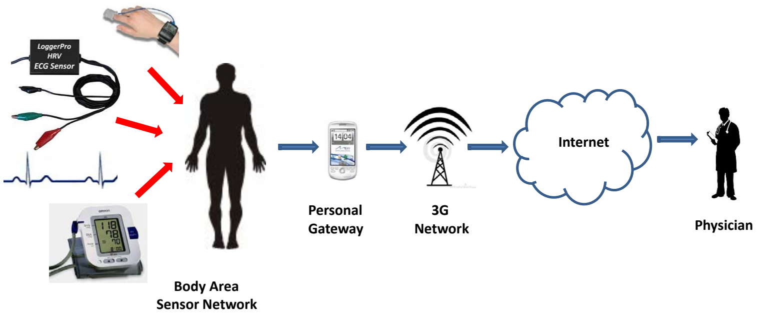

Fig. 1. Data flow in Body Sensor Network

2 Data Collection and Usage in Health Monitoring Application

One of the most popular applications of BSN in healthcare monitoring is cardiac dysrhythmia diagnosis. Normally, a electrocardiography (ECG) sensor is plugged into the BSN platform to continuously record the patient's heartbeat as he goes about his daily activities. A cardiac dysrhythmia is detected if the heartbeat is irregular, either too fast (tachycardia), too slowly (bradycardia), too early (premature contraction) or too irregularly. In order to better diagnose the causes of cardiac dysrhythmia, patients are asked to keep a diary log of their activities and symptoms. This labor-intensive task can be solved by integrating motion sensors onto the BSN platform. Motion sensors such as accelerometer and gyroscope, are widely used to recognize activities of daily living (ADLs), such as running, walking, sleeping, and etc. As a result, the ECG signal is tagged by patient's physical activities, and both of these data are transmitted to clinic physicians for diagnosis. However, the introduction of motion sensors for activity tagging comes with privacy issues and chances for data misuses. More than enough of the information about the patient's activities could be collected and transmitted, and some of these activity data may be private data that patients do not want to share with others, even clinic physicians. The disclosure of such private data could lead to unwanted privacy threats to the patients. In the following sections, we first explain the concept of privacy in context for the applications in BSN. Next, we list the requirements of the policy framework specifically integrated with the lower sensor platform to preserve privacy. Lastly, we discuss about the plan of how this approach could be evaluated for the effectiveness in privacy-preserving using utility function.

3 Privacy in Health Monitoring Application

3.1 Perception of Privacy

One privacy protecting mechanism that a system should provide is end-user controls to how the sensitive data should be collected, used and disseminated. In BSN, the applications first collect sensitive physiological data of the user and send to other parties for further analyses. This process is not transparent to the user. In [2], the authors pointed out that the control over systems in this kind of pervasive computing environment is hard to specify by general users due to the various types of contexts within in which a user resides. Because a user's perception of privacy is captured at the level of contextual information that is meaningful to them, not at the lower level where system really operates. This gap between privacy concerns of the user and the actual controls over system's operating functions poses challenges we want to present in this paper. To bridge this gap, we propose an integration of a policy framework and sensor configuration in BSN to adaptively adjust data collection and dissemination according to context information that is relevant to user's privacy concern.

Scenarios in the application of health monitoring present different privacy characteristics for the users [2]. Moreover, these scenarios involved different types of contexts including social contexts, sensor contexts, and application contexts that will lead to different levels of expectation of privacy. To protect privacy, the system should provide awareness to react on changes of context information [3]. In [1], the authors presented a formal framework to express privacy expectations and practices in terms of "contextual integrity". Privacy considering contextual integrity includes contexts, roles and types of information transmitted in the system. An action is permissible within the system if the communication of the information by roles under certain contexts do not violate the norm of user's privacy. For example, a norm in BSN could be "disclose least amount of data from additional type of sensors (acclerometers) to a physician if the data from default type of sensors (ECG) gives low precision output".

3.2 Privacy in Context

To capture privacy concerns of the users, we define a term called"sensitive situation" that represents a subspace or a trajectory of multiple subspaces in the "contextual space" described in [4]. A context space is a multi-dimensional space in which each dimension represent a type of context, and subspaces consisting regions of values that indicate situations of interest. In our case, it's a situation within which a user resides or a transition of situations that causes privacy concerns. So the system will provide privacy protection in the level of users perceived situation, not just on the information of individual sensed data. We believe that contextual privacy is a more appropriate tool to describe privacy issues in pervasive environment and bring awareness to the users in under different situations. Moreover, with the convergence of growth of available public data from social networks, web services, and other sources, adversary could easily put together these information to jeopardise users privacy. To give a user control over how his or her sensed data should be collected, we envision a policy framework to provide BSN the adaptability to other user's context information that could possibly lead to a "sensitive situation". Also, a privacy engine is needed to recognize the "situation" from current user's available contexts from different sources.

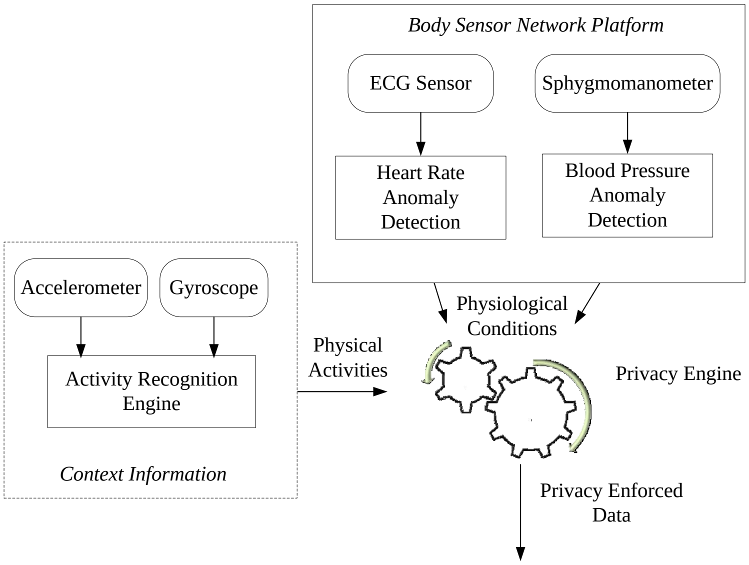

Fig. 2. Privacy Engine for Data Usage in BSN

4 Conclusion

In order to fully support privacy in the pervasive healthcare environment as described previously, several requirements need to be met. First of all, privacy concerns of a user needed to be captured with the model at the same level of how human perceive privacy. Then using this model, user's preference could be expressed in some policy language that is readable to the user and give them controls to the system. Moreover, the system should adaptively adjust its configuration of sensors according to user's policy and context information at realtime. We observe that current privacy language such as P3P/APPEL need to be extended for context information generating from BSN applications. The future specification of P3P or APPEL is expected to add more references to the characteristic of data stream, people-centric contexts and social contexts that all together could be used to identify a situation that has privacy issues. Ultimately, a context-based quantification of privacy should be designed to support measurement of privacy concerns, and to further study privacy-utility tradeoff [5] as an optimization problem in BSN.

References

1. A. Barth, A. Datta, J. Mitchell, and H. Nissenbaum. Privacy and contextual integrity: framework and applications. pages 15 pp. –198, may. 2006.
2. T. Darrell, , M. Ackerman, T. Darrell, and D. J. Weitzner. Privacy in context mark ackerman. *Human Comput.Interaction*, 16 (2-4):167–176, 2001.
3. A. Mitseva, S. Wardana, and N. Prasad. Context-aware privacy protection for wireless sensor networks in hybrid hierarchical architecture. pages 773 –778, aug. 2008.
4. A. Padovitz, A. Zaslavski, and S. W. L. C. Bartolini. Extending the context space approach to management by business objectives, 2005.
5. L. Sankar, S. R. Rajagopalan, and H. V. Poor. Utility and privacy of data sources: Can shannon help conceal and reveal information? *CoRR*, abs/1002.1347, 2010. informal publication.