Context-aware Access to Public Shared Devices

David Jea
Department of Electrical Engineering
University of California, Los Angeles
Los Angeles, CA USA
dcjea@ee.ucla.edu

Ian Yap
Department of Electrical Engineering
University of California, Los Angeles
Los Angeles, CA USA
ianyap@ucla.edu

Mani B. Srivastava
Department of Electrical Engineering
University of California, Los Angeles
Los Angeles, CA USA
mbs@ee.ucla.edu

ABSTRACT
To allow for an efficient usage of a device in pervasive computing environments, reliable and yet convenient user access is an important requirement. The problem becomes more complex when the accessed device is shared by the public with many different individuals. This paper first illustrates the common pitfalls and issues of establishing sessions to such devices. The paper then proposes a context-aware solution that uses different contexts to capture a usage session. The paper presents a general system design that supports a secure, selective, and identifiable user access of public shared devices with high usability. We have implemented a prototype system to demonstrate the concept.

Keywords
Body Sensor Networks, Pervasive Computing, User Access

1. INTRODUCTION
People have envisioned a pervasive computing environment where numerous ambient sensors and actuators are embedded. In recent years, Body Sensor Networks (BSN) have utilized miniaturized wearable and portable sensor systems to provide remote health-care monitoring. We imagine in the future that most ambient devices will be shared by the public and can temporarily participate in a user's BSN to provide specific services or data.

There are three main stages involved when a user is trying to access a device. The first action is to log in successfully (with authentication if necessary) to use the device. The second stage is to maintain a usage session (presence) with the device. The last action is logging out of the device, i.e. a detachment of use. The usage session with a detached device will be invalidated. We believe that it is important, when a user is trying to access multiple public devices among all other devices that can possibly be used by the public, to address all three stages from four distinct aspects: ***security, selectivity, usability,*** and ***identity***. The security of a session has been widely investigated in diverse breadth of literature. However, considering environments where multiple users are surrounded by public shared devices, the numerous existing schemes have not fully addressed the remaining three aspects reasonably.

In a recent publication [12], we have identified a common pitfall in the user access methods, which is that "**the context to gain access control of a device is not necessarily the same context to maintain a session and/or the context to release the access control. Moreover, the fact that someone is connected to a device is insufficient to describe whether the same user is using it.**"

In this paper, we present a system design for the proposed solution and an implementation that proves the concept. To explain this issue, we first review the related work in access control in section 2 and the problems of current techniques in section 3. We propose in section 4 a context-aware user access solution and describe our system design in section 5. We demonstrate an implementation of the concept in section 6 and experimental results in section 7. We summarize the paper in section 8.

2. RELATED WORK
In recent years, the academic world has started looking into more novel authentication mechanisms when pairing devices that could be less demanding on the user, and yet still maintain the security guaranteed by traditional techniques. Stajano et al. proposed the Resurrecting Duckling security model in [4] where a device will recognize as its owner the first entity that sends it a secret key (Imprinting), where the imprinting process is carried out with physical contact. In [3], Balfanz et al. extends the concept in great detail on the use of location-limited channels to be able to authenticate and use a device. This paper provides a more concrete pre-authentication details and implementation based on infrared. Another similar solution is the Zero-Interaction Authentication (ZIA) protocol from [1]. The ZIA protocol considers a user wearing a short-range, wireless authentication token to communicate with a system to determine whether to grant access.

The idea of location-limited channel has been applied in secure device pairing using various other techniques, such as visual [8] and aural [9]. The term “OOB” (Out-of-Band) channel is given to these forms of human-centric interaction. Such channel is governed by users while the attacker will find it difficult to eavesdrop to and modify the messages on the OOB channel. In general, existing work contributes to

pairing a device to a user and do not consider the actual usage session.

There is also a context-based user access which explores a new domain of authentication. These techniques rely on contextual data to authenticate the user and grant usage. Contextual data refer to information that can be gathered in a pervasive environment. Proximity-based authentication uses the location [2] of the user to determine if the user is still in the session. For instance, the context of a doctor (such as "in the surgery room") facilitates the authentication process when s/he tries to use computers near the vicinity. Gupta et al. [5] point out that proximity based access control potentially allows someone access the resource, when an authorized user is in proximity. To address the problem, they have introduced different authentication levels and the notation of proximity zone. However, defining the proximity zone for each device is also a challenging task. Lately, researches in role-based access control (RBAC) ([10], [13]) extend the role concept to improve security by incorporating access control decisions with dynamic context information.

3. PROBLEM STATEMENT

The current state-of-art user access methods can be fundamentally categorized into common wireless technologies and location-limited channels that exploit the communication medium. The first group is the use of conventional wireless protocols such as 802.11, Zigbee, and Bluetooth. The second group utilizes location-limited channels (such as infrared, RFID, etc.) that are defined in [3] and possess the property where a user can precisely control which devices s/he is interacting with. Additionally, we add a third category that involves user access with the aid of context-based information. We treat this as a separate category due to its intrinsic uniqueness of utilizing context-based information in a session.

Table 1 lists the caparison of different user access methods in the logging in, maintaining a session, and logging out phases. We discuss in detail of each user access method in the following sections to elaborate why a single solution does not fit in pervasive computing environments.

3.1 Conventional Wireless Channels

Initiating a session through conventional wireless channels has low usability in pervasive environments. The main issue here is that it is not easy to dynamically set up a connection between devices on the go without much user interaction. Imagine a user, Alice, with three Bluetooth keyboards in front of her. All three keyboards appear on her PDA to be selected for use. Now, with the conventional wireless channel protocol, Alice is confused on mapping id to the keyboard and getting her PDA to figure out which keyboard to be used. This low usability in selectivity rises when a user intends to connect to specific devices among multiple devices. It is apparent that we do not want to employ such awkward processes in future device-rich environments.

Table 1. Comparison of existing user access techniques.

	Existing Wireless Technology	**Location-limited channels**	**Context-based**
Logging In	Low Usability, especially when logging into multiple nodes	Moderate Usability, user must visit nodes one by one	No selectivity among nodes
Maintaining a session	Without explicitly logging out the nodes, a possible identity confusion problem	Either only one node can be used at a time, or the allowed proximity is rather constrained	To continuously detect the context
Logging Out	Receives a command or/and lost signal	Automatically logged out when heartbeat signal lost	Automatically logged out when the context changes

Moreover, maintaining sessions to the authenticated public shared devices through wireless channels could lead to identity issues. If the user does not explicitly log out of a device when s/he is done using it, the device needs to detect that itself explicitly. Imagine that Alice is connecting to a treadmill to receive personal training data while exercising. When Alice finishes her daily miles and steps off the treadmill, the next person, Bob, who was waiting in line, now steps up the treadmill and starts using it. Alice will keep receiving Bob's information unless she is out of the communication range. There is no way for the system to figure out who is using the device if the existing connection to Alice is maintained through mere wireless channels without any intelligent observations. This is because wireless solutions do not seek to exploit the use of "context information".

3.2 Location-Limited Channels

The location-limited channel is one extreme case of proximity-based authentication where a user can precisely control which device s/he is interacting with. Unlike initiation through conventional wireless channels, this intuitive selection process avoids confusion. A user can easily initiate a session to a device through a location-limited channel (Out-Of-Band). We consider that it has some slight usability issues because a user still has to visit the public shared devices that s/he wants to use one by one.

For a user to "precisely" select the device, these location-limited channels are either super-short-range (such as physical contact) or directional (such as infrared). Therefore, maintaining sessions through these types of channel limits the distance to or the number of connected public shared devices. Such usability issues of pervasive devices constitute an impetus to creating practically useful pervasive computing environments.

3.3 Context-Based User Access

A context is an event or a piece of information. A more complicated context captures human behavior or environment changes. In this type approach, a user will access a device if s/he is involved or within a specific context state. Proximity-based access control methods are the most popular methods to determine the context of a user and accessibility of a device. Some example contexts in these methods are "the user is inside the room" or "the user is within proximity zone of a device". The session between an authorized user and a connected device is terminated when the defined context changes (such as when the user leaves the room).

Context-based methods address a more general and flexible way in user authentication and are not limited to proximity-based access control. One example is that, in a station, if Alice faints suddenly (the context), her BSN will automatically authenticate with all nearby defibrillators to grant her access. It authenticates with the public address system to broadcast emergency messages for a doctor.

However, in a scenario of multiple users in the same context (such as they all in the same room), the unoccupied devices are randomly assigned to all users or exclusively to one user [5]. This appears to be a problem in pervasive environments. Alluding to an earlier example in 3.1, Alice only needs one treadmill, the one she selected, at a time, and neither needs nor wants the neighbor treadmills to become part of her BSN. Without special constraints, a context-based method generally *does not* select among devices for use.

4. PROPOSED SOLUTION

Our proposed solution involves defining an access-method that is characterized by three different types of context information throughout the entire usage process of a device(s). When a user plans to use a device, the device is bound to the user when s/he has established a connection through **initiation-context**[1] (for example, a location-limited channel). When s/he is successfully authenticated with a device and begins to use it, there should be two context states bound to this session, namely a **session-context** (e.g., user leaves the room) and a **govern-context** (e.g., user is on the treadmill). The session-context defines a specified context state of the connection to this session. The govern-context defines a specified state of the user to this device. A device is connected to the user only when the session-context is valid. Based on formalized and user-defined rules of how the specific context state changes, the device will determine whether the user has logged out and finished using the system. This will then lead to the system cleaning up this current session. As indicated earlier, the session-context is insufficient to describe whether the user is physically using the device currently. We thus require govern-contexts to represent this usage relation. A corollary is that a session-context will consist of none or at least one govern-context entity. A reasonable assumption is that when a user is using one device then no other people (with weaker or equal access rights) can override that relationship physically or virtually. And the system believes that all the sampled data from that device will belong to the user who is using it (exclusivity).

4.1 Initiation Context

Initiation-context binds a device to a user uniquely and securely. Therefore, the defining characteristics of this context are: selectivity, security, and trust. Location-limited channel possesses these requirements and is suitable for the initiation-context. When using a location-limited channel, a user can easily and precisely select the device s/he wants to communicate with by first approaching it intuitively. The basic assumption here is that ***at least one location limited channel*** is available between a BSN and a public ambient sensor. After selecting the device, the next step includes authenticating a trust entity and establishing a secure communication channel to protect privacy information flowed between the user and the device. Possible candidates for a location-limited channel are RFID, Infrared, Sound, Camera, Physical Contact, and LED.

4.2 Govern Context

We use the govern-context to determine if a user is physically using a device. We list the three general forms of a govern-context. The first form is the god view, where a central context server that monitors all entities and their behaviors in its controlled environment. An example is the location of a user and the public shared devices. When a user is in proximity of a device, then the system assumes that the user is using the device.

The second form is one based on local decision, where the context is determined by the BSN that a user is wearing. The BSN detects the current context of the user and the decision is based on this context. For example, if the inferred context of a user is running and a treadmill has been connected to his/her BSN, then the system considers that the user is using the device.

[1] In secure device pairing literature, this is the one phase that focuses on binding a device to another device

There is the special case where the context can rely on *context proximity* among devices as epitomized in [6]. Their work proposes a scenario where small devices are connected when two persons shake hands, the two artifacts connect with each other if both experience similar context. We extend a similar idea to search matchmaking context between a user and the devices. In our implementation, the system considers the target is using a device if similar accelerometer context results are found on both entities.

4.3 Session Context

We refer to session-context as a collection of event(s) that manage a connection's state. The most common form of session-context is an event that triggered by user. It happens when a user explicitly take actions to disconnect with a device (pressing a button, executing a command, etc). Another popular form of session-context would be the events that are generated naturally and detected by the system. For example, when the user leaves the room, the signal is lost, or the connection idles out, etc. Systems nowadays cover both forms in managing a session. However, a complicated session-context is flexible in the expressiveness of human behaviors and environmental changes. The system captures natural descriptions such as disconnecting the devices when the user finishes a set of routine exercises. The BSN then continuously monitors all session-contexts of each connected device and terminates the connection if any of its session-contexts is invalidated.

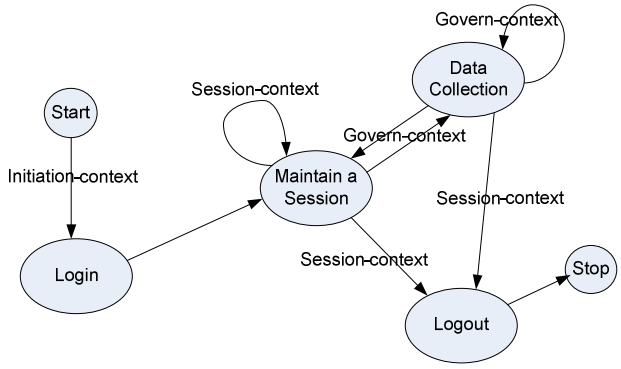

Figure 1. State Diagram of a General System Design

5. SYSTEM DESIGN

Figure 1 shows the state diagram of the user access method. Besides the login, session maintenance, logout states, we have added a data collection state to reflect the physical usage relationship between the user and the device. The BSN enters the login state once it detects the initiation-context. In the login state, the BSN authenticates with the device bounded by initiation-context and establishes a secure channel based on a generated shared session key using techniques such as the EKE protocol [7]. The authenticated device becomes a member of BSN and the system then determines the necessary session-context and govern-context involved between the user and the authenticated device. The BSN continuously maintains the session to the device while it detects a valid session-context. When the govern-context is true, this means that a user is using the device. Otherwise, the device is detached from the user. And the user's BSN only accepts the data of a connected device when the user is actually using the device, and terminates the connection when the session-context is invalidated.

A complete system incorporates various components to realize the proposed solution. In our design, we use one class (BSN_INFO) to maintain BSN information such as topology, connected ambient sensors, etc. A node can be set to either "BSN" or "Ambient" type, and provides any combination of "Authentication", "Data Source", and "Context" services. Node with "Authentication" service binds to initiation-context. In MATCHER class, "Context" nodes associate with each other to evaluate session-context or govern-context. The "Data Source" nodes provide data when the associate contexts match. One class (MONITOR) detects heartbeats of nodes and manages nodes' statuses accordingly. When the govern-context is true, the system takes in data and shows on screen (or stores into database) by the DISPLAYER class. Figure 2 shows the block diagram of the system.

Other components related to context description and context establishment have been left without addressing. Describing a context is a challenging task due to the complexity of pervasive computing. Context establishment is the phase where the user needs to establish some form of connection based on the state of using the device to determine proper statuses of session-contexts and govern-contexts. With the increasing size of a connected BSN and a variety of ambient sensors, the scalability will become a core issue that requires further studies.

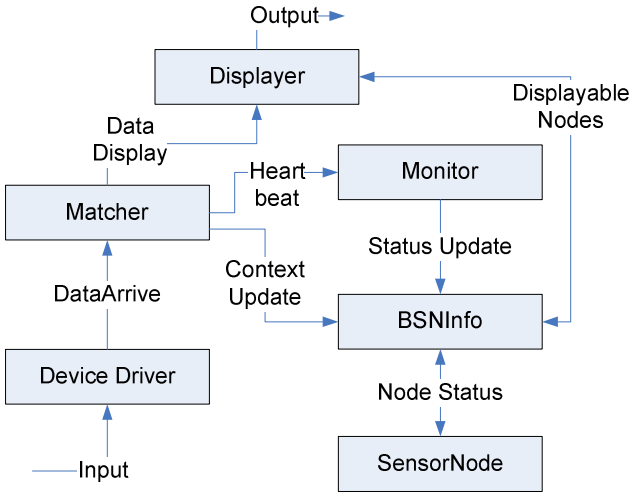

Figure 2. Block Diagram of the System

6. IMPLEMENTATION

As shown in Table 1, there is no single technique that addresses all the problems of selectivity, usability and identity. Thus, a better design incorporates the strength of these techniques. We present the design of a prototype system to demonstrate the solution described earlier. The user relies on a location-limited LED channel to precisely select a device while minimizing user interaction. We use a scenario where a user is exercising in gym that has public sensing devices installed on the fitness equipments. A device joins a body sensor network through the authentication process, but provides sensing information only when the user is indeed physically using the device. To solve the identity confusion problems and determine govern-context, we attach one accelerometer to the user and one accelerometer to the bike trainer. The ambient sensor connects to the user's BSN but only delivers data to the base station when two accelerometers experience similar phenomenon that have close dominant frequencies (context matching). When a different user hops on the same bike, the connected BSN (to the first user) stops receiving data. The purpose of this design is to demonstrate an intelligent context-based system that can identify if the same user is using the connected device. The resultant prototype system demonstrates our solution to a context-aware user-centric access system.

We implement the body sensor nodes and ambient sensors using Crossbow MicaZ platform [11], and the BSN base station on a laptop. There are three nodes in the BSN and each has a distinct functionality: gateway, authentication, and data source. The gateway node is the bridge between personal mobile devices and body sensor networks. It equips a Bluetooth module and relays all received BSN packets to the base station through a Bluetooth connection. The authentication node is responsible for building the initiation-context and has the ability to select the ambient sensors and initiate secure connections through a location-limited LED channel. The data source node equips an accelerometer board and provides ambulatory information of the user.

We install two ambient sensors on fitness machine (bike): cluster head and data source. The cluster head node has a light sensor and responds requests from BSN. The ambient data source node is another accelerometer mounted on the pedal. The two accelerometers (another wore by user) together determine the govern-context. Ideally, the data source sensor such as SpO2 sensor for heart rate monitoring should be used. In this implementation, we use a different axis of ambient accelerometer sensor to emulate a different ambient data source node.

We choose Python to realize the various components of the system described in section 5. For evaluation purpose, the current base station is a Linux laptop. In future, we aim to replace the laptop with a Nokia cellular phone, which also supports Python interpreter. Figure 3 illustrates this implementation setup.

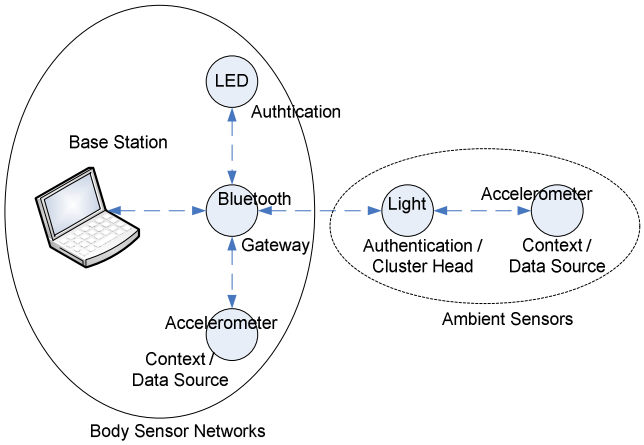

Figure 3. Experiment setups

7. EXPERIMENT RESULTS

We conducted experiments as a demonstration of the core concepts discussed in this paper. We ran the experiments in the John Wooden Center Gym at UCLA. The BSN and ambient sensors described in previous section are attached to a user and an exercise bike respectively. We show that, with ambient sensors connecting to BSN, the data sources of ambient sensors only relay data to base station when the two accelerometer contexts match. Figure 4 shows the experiment and its results.

8. CONCLUSION

In this paper, we have explored user access issues of public shared devices in pervasive computing environments, and suggested a solution that is based on the concept of an initiation-context, session-context, and govern-context.

To illustrate this idea and verify the proposed solution, we have implemented a prototype system based on the described design, and demonstrated a scenario of collecting training information for a user while maintaining usability. Future research will be devoted in developing more complex context models and protocols for all the phases, especially investigating how the session-context and govern-context are established between body sensor networks and public shared devices. We look forward to increased interests in facilitating the convenience of user access of devices in pervasive computing environments.

9. REFERENCES

[1] M. D. Corner, and B. D. Noble, "Zero-Interaction Authentication," *Proceedings of Eighth Annual International Conference on Mobile Computing and Networking (Mobicom),* 2002, pp. 23-28.

[2] J. E. Bardram, R. E. Kjær, and M. Pedersen. "Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing," *Proceedings of Fifth International Conference on Ubiquitous Computing (Ubicomp),* LNCS 2864, Springer, 2003, pp. 107-123.

[3] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks," *Proceedings of Network and Distributed System Security Symposium (NDSS),* Internet Society, 2002, pp. 23-35.

[4] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," *Proceedings of the 7th International Workshop on Security Protocols,* LNCS 1796, Springer, 1999, pp. 172-194.

[5] S. K. S. Gupta, T. Mukherjee, K. Venkatasubramanian, and T. Taylor, "Proximity Based Access Control in Smart-Emergency Departments," *Proceedings of 4th IEEE Conference on Pervasive Computing Workshops, First Workshop On Ubiquitous & Pervasive Health Care (UbiCare)*, 2006, pp. 512-516.

[6] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. W. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Artefacts," *Proceedings of Third International Conference on Ubiquitous Computing (Ubicomp),* LNCS 2201, Springer, 2001, pp.116-122.

[7] S. M. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," *Proceedings of the IEEE Symposium on Security and Privacy,* 1992, pp. 72-84.

[8] N. Saxena J. Ekberg, K. Kostiainen, and N. Asokan, "Secure Device Pairing based on a Visual Channel," *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, 2006, pp. 306-313.

[9] M. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud and Clear: Human-verifiable Authentication Based on Audio," *Proceedings of 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06),* 2006, pp.10.

[10] MJ Moyer, M Ahamad, "Generalized Role-Based Access Control," *Proceedings of the 21st IEEE International Conference on Distributed Computing System*, 2001, pp. 391-398.

[11] Crossbow MICAz platform, http://www.xbow.com/Products/productdetails.aspx?sid=164

[12] D. Jea, I. Yap, and M. B. Srivastava, "User Access of Public Shared Devices in Pervasive Computing Environments," to be appear in *Workshop On High Confidence Medical Devices, Software, and Systems (HCMDSS),* 2007

[13] G. Zhang and M. Parashar, "Context-Aware Dynamic Access Control for Pervasive Applications," *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2004, pp. 219-225.

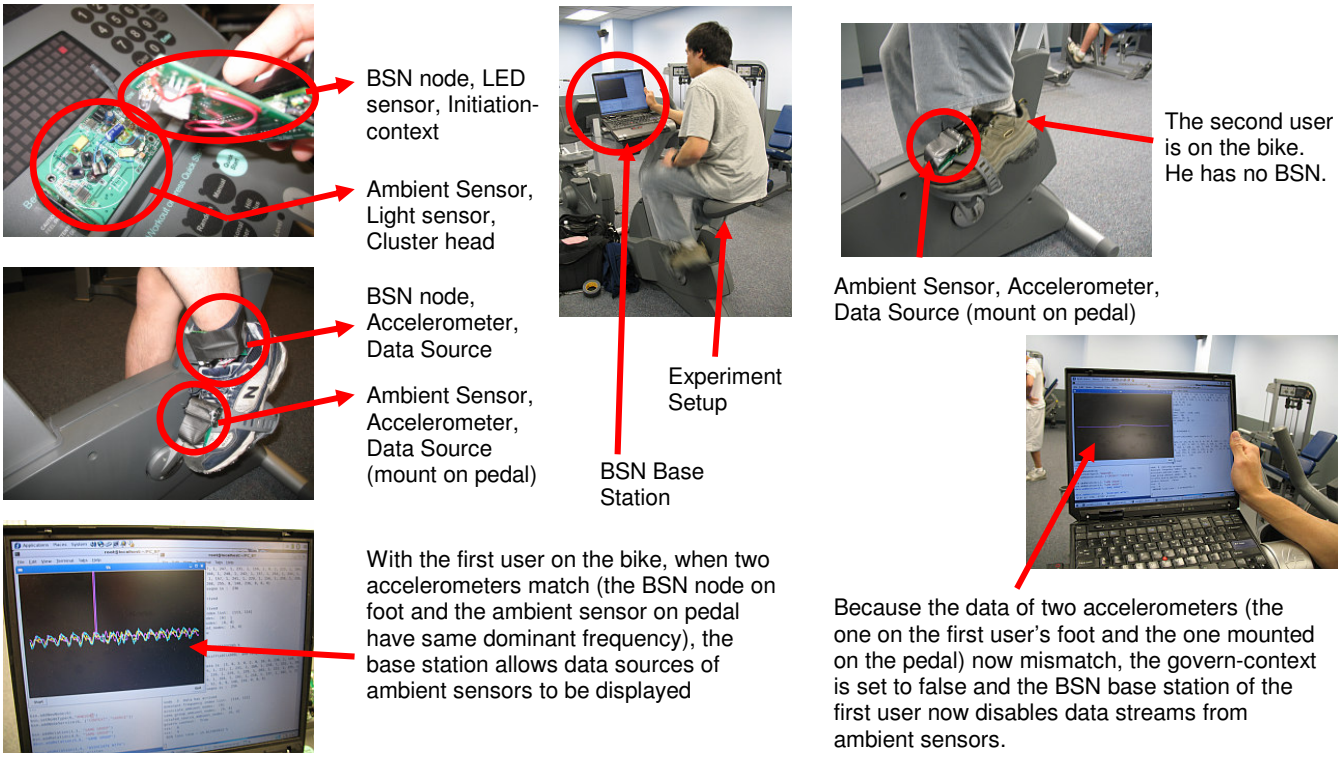

Figure 4. Experiment Results