Hassle Free Fitness Monitoring

David Jea[1], Jason Liu[1], Thomas Schmid[1], Mani Srivastava[12]
UCLA Electrical Engineering Department[1]
UCLA Computer Science Department[2]
{dcjea, schmid, mbs}@ee.ucla.edu; jasonliu0907@ucla.edu

ABSTRACT
Fitness monitoring is a fundamental service in pervasive healthcare, but finding a balance between usability and privacy is a hard challenge. To lessen users' anxieties in privacy concerns, we propose a new way of identification by only utilizing imprecise biometrics and existing information. Our solution is "hassle free" because it maintains the devices' original user interface without adding additional sensors and sacrificing user privacy. We demonstrate this idea with a fitness monitoring system for the healthy individuals in a workplace. The system uses collected physiological information (weight, blood pressure and heart rate) and context information (computer network activity) to identify a user. Our experiments show that we can achieve a correct user identification of up to 87%. We believe that our solution can serve as an easy addition to the simple interfaces of current technology by enhancing them with smart algorithms.

1. INTRODUCTION
Fitness monitoring is probably one of the most fundamental functionalities of pervasive healthcare systems. Proactively recording vital signs, such as weight and blood pressure changes over time, enables a caregiver to deliver qualified medical services. We are interested in the fitness monitoring of healthy individuals in workplaces or homes. Since this population has no serious health threats, they lack strong motivation in participation. Usability becomes one of the main factors that provoke (or diminish) users' interests in using a device. The interface should be simple and non intrusive. Typing a name into a computer can already be too much hassle in order to just record a weight. In addition, workplaces are semi-public, where *privacy* seems to be another concern for many users. Balancing usability and privacy is one important issue in pervasive healthcare [6].

1.1 Privacy
Studies in [3] describe that people worry about the tracking and abusing of the system. In [1], 89.2 percent of the sampled people reported medium or high concerns about privacy. This year (2008), in New York, workers are protesting over using palm print scanners to automate employee tracking. "*The palm print thing really grabs people as a step too far.*" said Ed Ott, executive director of the New York City Central Labor Council of the AFL-CIO [2].

HealthNet'08, June 17, 2008, Breckenridge, CO

1.2 Design Guidelines
To lessen users' anxieties in privacy while maintaining high usability, we propose a device should identify a user with the following design guidelines:

1. *Any data that the system records cannot be used as hard evidence (in court) to pinpoint exactly who the user is. (privacy).*
2. *The system is allowed to use existing information. (feasibility).*
3. *The original interface is maintained such that people of all age groups naturally know how to use it. (usability).*

2. THE PROPOSED DESIGN
In fitness monitoring applications, the physiological information of weight, blood pressure and heart rate are the most popular information that people would like to record. Such physiological information has high variances and is not suitable for an exact biometric identification. However, we can ask the question what level of accuracy such a system can achieve in mapping the collected data to a user. Since this is a non-critical application, if the accuracy is sufficiently high, we can then loosen the required sensitive inputs from users.

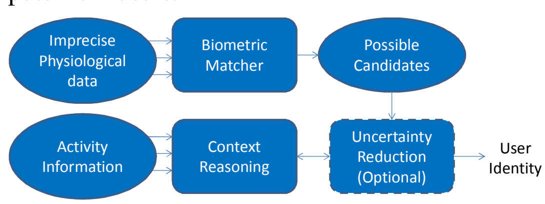

Figure 1. The components of the identity inference engine.

The identity inference engine consists of two main components as illustrated in Figure 1. The Biometric matcher takes physiological data input and generates a pool of possible candidates. Context reasoning takes user activity information gathered by other systems to infer a user's physical presence. The result is then passed through the optional uncertainty reduction component to adjust the possibility of each possible candidate based on their context information.

3. IMPLEMENTATION

We present a prototype system that performs fitness monitoring (weight, blood pressure, heart rate) for healthy individuals in workplaces. To test the feasibility of the proposed idea, we designed and deployed a system in our lab. The system consists of a weight scale (A&D Medical UC-321PL) and a blood pressure monitor (A&D Medical UA-767PC). Both devices communicate with a laptop via their RS-232C ports. A data collection program written in C++ runs on the laptop to continuously record and timestamp the weight and blood pressure readings. There are text input and speech recognition interfaces for a user to input the name. This step is required to establish ground truth for the experiment. The network activity information is used to infer the presence context of a user. The firewall server runs a monitoring program that continuously logs networking traffic from each computer. We specifically take traffic information of port 80 (the HTTP port). The assumption is that most graduate students browse the internet (access email, etc.) occasionally when they are at work. We use this assumption to infer their presence in the lab.

3.1 Biometric Matcher

We implement a naive Bayes classifier that combines multiple sensor observations for the purpose of inferring the identity of a subject. The naïve Bayes classifier assumes that each observation is independent of every other observation, and in practice it often competes well against more sophisticated classifiers. By applying Bayes' Theorem and independence assumptions, the probabilistic classifier is described as,

$$p(I \mid O_1,\dots,O_n) = p(I)\prod_{i=1}^{n} p(O_i \mid I) \Big/ p(O_1,\dots,O_n),$$

where the class variable I is the identity of users and O is the set of sensor observations.

3.1.1 *The Model of Weight, Blood Pressure, and Heart Rate*

We establish simple Gaussian models for weight, blood pressure, and heart rate in a Bayes classifier. After the first five measurements, the mean is updated through an exponential moving average, $M_t = \alpha \cdot W_{t-1} + (1-\alpha) \cdot M_{t-1}$. We set α to 0.2 for this study, which gives more importance to recent observations. The system only updates the mean if the confidence to the user's identity is greater than 65%. We set the standard deviation of weights to 3lbs, considering the amount of food intake, difference in clothing, and typical daily weight variation. The standard deviation of the systolic blood pressure and diastolic blood pressure are set to 15 mmHg and 13mmHg respectively according to [5]. The standard deviation of the heart rate is set to 20bpm considering that this monitoring station is set in a workplace environment rather than an exercising place.

3.2 Context Reasoning

We build the context reasoning component based upon reified temporal logic. Context reasoning provides the high-level contexts about a user's state and surrounding. Reified temporal logic allows us to express *when* things are true. We adopt the two meta-predicates described in [4]. The notation HOLDS(T, *pro*) expresses that *pro* holds true over time T. Another notation HOLDS_IN(T, *pro*) asserts that *pro* holds true over some time during T. In our prototype, a user's context (such as in the lab at a specific time) is determined through these predicates of the network activity information.

$$HOLDS(T, pro) \Leftrightarrow \forall t.\, in(t,T) \Rightarrow HOLDS(t, pro)$$
$$HOLDS\_IN(T, pro) \Leftrightarrow \exists t'.\, in(t',T) \Rightarrow HOLDS(t', pro)$$

3.2.1 *The Model of Presence Context*

We use network activities to infer a user's presence in the lab. Figure 2 illustrates these rules. When a fitness monitoring measurement is taken, T_p is set to include the 20 minutes before and after the associated timestamp. The system then infers a user's presence during that period based on following rules. We describe these rules:

1. A user is present during the time period T_p if there is Internet browsing activity on the user's PCs.
   - *PRESENCE* :- HOLDS_IN(T_p, exists(*ACTIVITY*))
2. A user is browsing the Internet during T_{min}, if there is network traffic for more than $\theta_{activity}$ times.
   - *ACTIVITY* :- HOLDS(T_{min}, count(*TRAFFIC)* > $\theta_{activity}$)
3. The network has traffic during $T_{10\text{-sec}}$, if the amount of packets is more than $\theta_{traffic}$.
   - *TRAFFIC* :- HOLDS($T_{10\text{-sec}}$, count(*PACKETS)* > $\theta_{traffic}$)

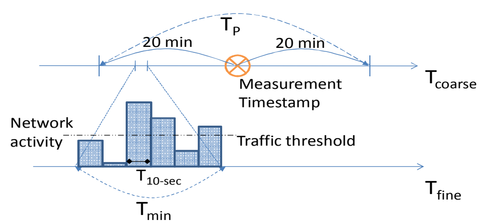

Figure 2. Context Reasoning based on Networking Traffic.

4. EXPERIMENTAL RESULTS

We have deployed the system in our lab since mid Feb, and the data points used for this paper are from Feb. 14, 2008 to Mar. 28, 2008. A total of 355 data sets were collected including 185 weight data points and 170 blood pressure /heart rate data points. The total measurement count is 222 times (most participants took measurements on both devices, but sometimes only one device was used). We have a 30-day network monitoring log spread within the period (it does not cover full span of the period due to technical issues). Users are free to take weight and/or blood pressure measurements (heartbeat rate comes with blood pressure measurement) at any time. Therefore, the user usage is in a totally casual fashion to approach reality. The operating interfaces of these devices are maintained as the original ones: one kick to start the weight scale and one button to start the blood pressure monitor. To establish ground truths, we require users to input their name before using the devices. A total of **9** users have participated, and 6 of them regularly work in lab (thus have network activities).

User	Similarity in Physiological Information	Seat in Lab	Usage Habit		
			Weight Scale	BP Monitor	Both
A	Light		V	V	
B	They have similar weights. The differences in mean (of all their data points) are less than 1.9 lbs.	V		V	V
C		V			V
D		V	V		
E	Their difference in average weight is 2 lbs.	V			V
F					V
G	Their difference in average weight is 1.1 lbs.	V	V		
H		V			V
I	Heavy		V		

Table 1. Participants of the experiment.

Table **1** illustrates the challenge of identifying a user based on imprecise physiological information and their usage contexts. With just 9 people, we can easily find 3 groups that have very close weights. Additionally, the blood pressure and heart rate vary considerably depending on the circumstance of the user when taking the measurement. Table **2** shows the classifier results if it uses only one physiological information source. As shown later, combining the four sources of information (weight, systolic and diastolic blood pressure, and heart rate) can significantly enhance the accuracy in identifying a user. However, another challenge is that not all users use both devices each time. Some have a strong tendency in taking only their blood pressure or weight. This is counter to what a good classifier needs, and thus its performance degrades considerably.

Physiological Data for Classifier	Positive Match	False Match
Weights	57.23%	45.77%
Systolic Blood Pressure	22.02%	77.98%
Diastolic Blood Pressure	43.90%	56.10%
Heartbeat Rate	25%	75%

Table 2. The classifier results for one physiological information source.

The biometric matcher using the naïve Bayes classifier to combine all 4 sources of physiological information improves the identification accuracy to ~78%. As we mentioned earlier, due to users' uncertain usages, some of these inputs consist of only one data point (weight) or three data points (systolic and diastolic blood pressure, and heart rate). If the user classification is only based on complete measurements (a total of 134 measurements that have all 4 data points), the accuracy of the classifier improves to 87.3%. This result is shown in Table **3**.

Table **4** shows the context reasoning component based on network traffic. We use the fact that a user has to be in the lab to take a measurement to establish ground truths. The positive rate (a user is in the lab and the context reasoning agrees) is 89.47% and the false positive rate (a user is in the lab and the context reasoning shows the negative answer) is 10.53%. The results are analyzed based on the 114 measurement timestamps from the computers of the 6 regular lab users.

The system uses the context reasoning component when it is unsure about the results from the biometric matcher. We set the criteria to the confidence difference between the largest and the second largest of user candidates. If the difference is less than 15%, then the system triggers the context reasoning for these two users. Within the 30-day period where we have networking log (142 measurements), the performance of biometric matcher increases by 5.63% when combined with context reasoning (see Table **5**).

Biometric matcher that combines all 4 physiological sources.	Positive Match	False Match
Classification Results for partial or complete data points.	77.9%	22.1%
Classification Results for complete data points only.	87.3%	12.7%

Table 3. The classifier results based on multiple sources.

Context Reasoning Component	Positive	False Positive
The presence of a user based on network activity	89.47%	10.53%

Table 4. The accuracy of the context reasoning component.

	Biometric Matcher only	Biometric Matcher and Context Reasoning
Accuracy	78.16%	83.80%

Table 5. Combining the biometric matcher with the context reasoning.

5. CONCLUSIONS

In this paper, we proposed a hassle free design for fitness monitoring. To preserve privacy, the system identifies a user based on imprecise physiological information and existing activity context. The system maintains its original interface for users, in order to provide the same ease of usability. We believe that our design can serve as a bridging solution between present and future pervasive computing.

6. REFERENCES

[1] A. Acquisti, J. Grossklags, "Privacy and Rationality in Individual Decision Making", IEEE Security and Privacy 3, 1 (2005), 26–33.

[2] "Fingerprint Scans Replace Clocking In", The Associated Press, March 26, 2008.

[3] E. Kaasinen, User Needs for Location-aware Mobile Services. Personal and Ubiquitous Computing 2003. 7(1): p.70-79.

[4] J. Ma and B. Knight, "A Reified Temporal Logic", *The Computer Journal* 1996 39(9):800-807.

[5] B.T. Marczak, A. Paprocki, "Blood pressure variability on the basis of 24-hour ambulatory blood pressure monitoring in a group of healthy persons", Przegl Lek. 2001;58(7-8):762-6.

[6] V. Stanford, "Pervasive health care applications face tough security challenges", IEEE Pervasive Computing, April-June 2002.