Cyber-Physical Handshake

Fang-Jing Wu
Department of Computer
Science, National Chiao Tung
University, Hsin-Chu, Taiwan
fangjing@cs.nctu.edu.tw

Feng-I Chu
Department of Computer
Science, National Chiao Tung
University, Hsin-Chu, Taiwan
fychu@cs.nctu.edu.tw

Yu-Chee Tseng*
Department of Computer
Science, National Chiao Tung
University, Hsin-Chu, Taiwan
yctseng@cs.nctu.edu.tw

ABSTRACT

While sensor-enabled devices have greatly enriched human interactions in our daily life, discovering the essential knowledge behind sensing data is a critical issue to connect the cyber world and the physical world. This motivates us to design an innovative sensor-aided social network system, termed *cyber-physical handshake*. It allows two users to naturally exchange personal information with each other after detecting and authenticating the handshaking patterns between them. This work describes our design of detection and authentication mechanisms to achieve this purpose and our prototype system to facilitate handshake social behavior.

Categories and Subject Descriptors: C.2.1 [Network Architecture and Design]: Wireless communication

General Terms: Algorithms, Design, Experimentation

Keywords: cyber-physical system, participatory sensing, pervasive computing, social network, wireless sensor network

1. INTRODUCTION

Recently, sensor-enabled mobile phones have become essential tools in the study of cyber-physical systems (CPSs) [1]. CPSs enrich the interactions between the virtual and the physical worlds and sensor-aided social networking has been recognized as one of the main CPS applications [2, 3].

This work designs an innovative sensor-aided social network system, termed *cyber-physical handshake*, to enable natural information exchange after detecting and authenticating the handshaking patterns between two persons. In the physical world, the *handshake* behavior between two people implies that a social link will be authenticated between them before they exchange personal information (e.g., exchanges of business cards). On the other hand, in the cyber world, a handshake procedure is adopted by two nodes to authenticate each other before they start data exchanges. The work follows the concept of "handshakes" to design an authentication mechanism based on sensing patterns to facilitate automatic data exchanges between two users after they have a handshake, as shown in Fig. 1. Instead of generating and authenticating shared keys [4, 5], our system is
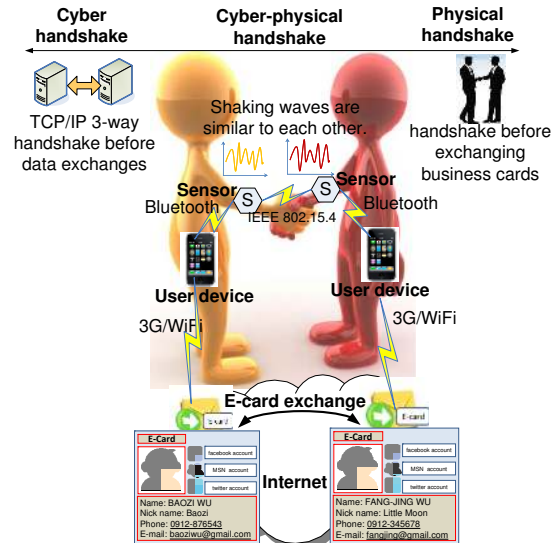
Figure 1: Architecture of our cyber-physical handshake system.

a light-weight approach which incurs less computation overhead and is more suitable for simple sensor devices (e.g., a watch).

2. SYSTEM ARCHITECTURE

The basic idea of the cyber-physical handshake system is to allow two users to exchange data if they have a handshake with each other. When two users make friends with a handshake in the physical world, the shaking waves perceived by the two users' sensor nodes will have high degree of similarity in both frequency and time domains. We then use the similarities to authenticate a handshake behavior. Fig. 1 shows our system architecture. Each user is equipped with a smart phone and wears a watch-like sensor node with an accelerometer on his/her wrists. Sensor nodes follow IEEE 802.15.4 to communicate with each other. Each sensor node is associated with its user's smart phone through bluetooth. Each sensor node is responsible for detecting and reporting handshaking samples to its user's smart phone. The smart phone will compute a value of similarity between the two users' samples. If the value of similarity is greater than a predefined threshold, it will exchange the user's E-card with the other user over the Internet.

2.1 Software Design

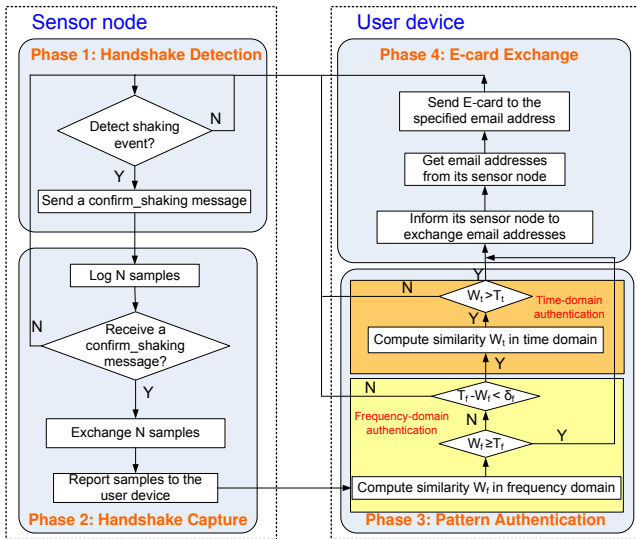Our software design is composed of four phases, as shown in Fig. 2.
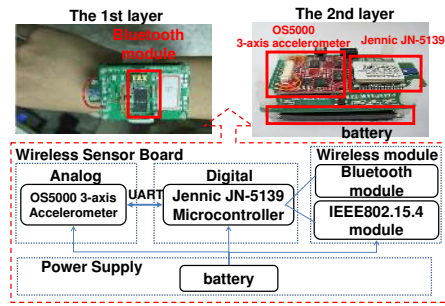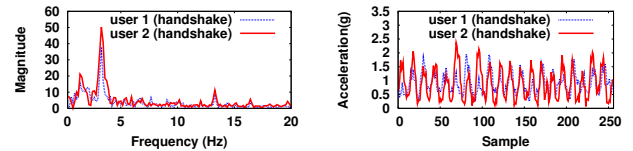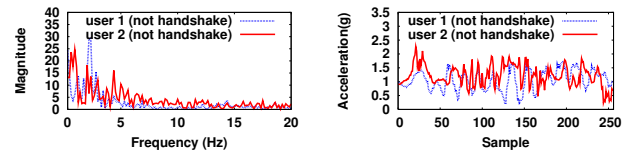
Figure 2: Software design of our system.

Figure 3: Hardware design of our system.

(a) The frequency distribution of a handshake event.

(b) The time-domain samples of a handshake event.

(c) The frequency distribution of a non-handshake event.

(d) The time-domain samples of a non-handshake event.

Figure 4: Experiments of a handshake and a non-handshake events.

Phase 1: handshake detection. In this phase, we use each sensor node to detect shaking events. We sample data at a rate of R_s. For each sample ν, we check if the shaking condition $|\nu - 1g| > \tau_s$ holds, where g is the gravity and τ_s is a predefined threshold. If the number of shaking samples per second detected is greater than $R_s/2$, the sensor node will broadcast a *confirm_shaking* message and enter the next phase.

Phase 2: handshake capture. In this phase, the sensor node logs the upcoming N samples and checks if it has received a *confirm_shaking* message recently. If so, it exchanges these N samples with that sensor node and then reports all these samples to its smart phone.

Phase 3: pattern authentication. In this phase, each smart phone will compute the values of similarity in both frequency and time domains to decide whether the two samples are resulted from the same handshake in the physical world. First, we compute the value of similarity in the frequency domain between two samples, say a and b, by $W_f = \frac{1}{5} \int_{f=0}^{5} C_{ab}(f)$, where $C_{ab}(f) = \frac{|P_{ab}(f)|^2}{P_{aa}(f) \times P_{bb}(f)}$ is the *magnitude squared coherence* of the two samples. Here, we only consider the coherence between $0 \sim 5\,Hz$ because the handshake frequency of a human can hardly exceed this range. If $W_f \geq T_f$, we have a handshake match and enter the next phase, where T_f is a predefined threshold. Otherwise, if $T_f - W_f < \delta_f$, where δ_f is a small value, then the value of similarity in the time domain will be computed by the Pearson's correlation coefficient $W_t = |\frac{1}{(N-1)} \frac{\Sigma_{i=1}^{N}(A_i - \overline{A}) \times (B_i - \overline{B})}{\sigma_a \times \sigma_b}|$, where σ_a and σ_b are the standard deviations of a and b, respectively. Here, A_i (resp., B_i) and $\overline{A}$ (resp., $\overline{B}$) denote the i-th reading and the mean of the a's (resp., b's) samples. Here, δ_f is a guard parameter to involve the time-domain handshake detection. If $W_t > T_t$, a handshake is detected and we enter phase 4, where T_t is a predefined threshold.

Phase 4: E-card exchange. In this phase, the user device will inform its sensor node to exchange user's email address with the other sensor. Then it sends a personal E-card to that address over the Internet for further social networking behaviors.

2.2 Demonstrations

Each sensor node is a two-layer sensor board including a bluetooth module, an OS5000 sensor [6], a Jennic JN5139 [7], and a battery, as shown in Fig. 3. Each OS5000 has a 3-axes accelerometer. We set R_s=40Hz. Jennic JN5139 has a micro-controller and a built-in 2.4GHz/IEEE802.15.4 wireless module. The user device is a smart phone (HTC Touch 2 [8]) with a bluetooth and a WiFi/3G wireless modules.

We also conduct experiments to log shaking waves of a handshake event and a non-handshake event for 7 seconds. Fig. 4 shows the experimental results, where the two users' sensing data have high degree of similarity in a handshake event in both frequency distribution and time domain samples.

3. REFERENCES

[1] F.-J. Wu, Y.-F. Kao, and Y.-C. Tseng, "From wireless sensor networks towards cyber physical systems," *Pervasive and Mobile Computing*, to appear.

[2] S. Gaonkar, J. Li, and R. R. Choudhury, "Micro-Blog: Sharing and querying content through mobile phones and social participation," in *Proc. ACM Int'l Conf. on Mobile Systems, Applications, and Services*, 2008, pp. 174–186.

[3] M.-C. Chiu, S.-P. Chang, Y.-C. Chang, H.-H. Chu, C. C.-H. Chen, F.-H. Hsiao, and J.-C. Ko, "Playful bottle: a mobile social persuasion system to motivate healthy water intake," in *Int'l Conf. Ubiquitous Computing*, 2009, pp. 185–194.

[4] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Trans. Mobile Computing*, vol. 8, no. 6, pp. 792–806, 2009.

[5] D. Bichler, G. Stromberg, M. Huemer, and M. Löw, "Key generation based on acceleration data of shaking processes," in *Int'l Conf. Ubiquitous Computing*, 2007, pp. 304–317.

[6] "Os5000," http://www.ocean-server.com.

[7] "Jennic JN5139," http://www.jennic.com.

[8] "HTC Touch 2," http://www.htc.com/tw/product/touch2/overview.html.