Activity-based Authentication by Ambient Wi-Fi Fingerprint Sensing

Nobuyuki Kasuya Takashi Miyaki Jun Rekimoto
Interfaculty in Information Studies,
The University of Tokyo
7-3-1 Hongo, Tokyo, Bunkyoku, 113-0033, Japan
qq086404@iii.u-tokyo.ac.jp
{miyaki, rekimoto}@acm.org

ABSTRACT

Preserving a good balance between security and usability is often an important issue in many ubiquitous computing applications. This paper proposes a new user interface model for security based on device's activity history by environmental Wi-Fi fingerprint sensing. If a device periodically senses and records Wi-Fi fingerprint, such record represents the device's location and activity history. This information can be used to detect whether this device is in a normal situation or in an unusual (abnormal) situation. If two devices compare these activity logs, it is also possible to determine whether these devices are moved together or not. Then the system changes its security level based on such activity information. Unlike other Wi-Fi positioning systems, geological Wi-Fi access point information is not always necessary, because only fingerprint matching is enough for authentication purpose. This feature makes our security model more scalable; it works even though a Wi-Fi access point location database is not provided. (This paper describes new user interface model for security based on this idea, and reports initial experimental results.

Keywords

activity history, authentication, Wi-Fi fingerprint sensing

INTRODUCTION

To provide better balance between usability and security is an important problem of ubiquitous computing. However, it is not always easy to balance both. If authentication is too strict, applications become difficult to use, but simply lowering the security level is not the answer.

"Smart-Its Friends"[1] uses accelerometer information to make wireless connection between two devices. When a user shakes two devices together, one device can find the other device by comparing vibration patterns. Since faking such vibration pattern is not easy, this method is also a user-friendly way to securely establish a connection between two devices. However to do this, we must carry a devices which equips acceleration sensor. Shaking is not always possible because of the device's size (e.g., laptop computers).

In this paper, we propose a new security model which use ambient Wi-Fi fingerprint sensing. As many previous researches pointed out, our urban environment is surrounded by many Wi-Fi access point signals. These signals, or often called "Wi-Fi fingerprints" are easy to be detected without making a wireless connection. Almost all the Wi-Fi equipped devices have an ability to sense such fingerprint information containing access point's ID (MAC address) and received signal strength indication (RSSI). Many systems [2,3,4,5] use this information as location recognition purpose.

Our approach is to use this Wi-Fi fingerprint logging for authentication purpose. Our models have two variations, as shown in Figure 1.

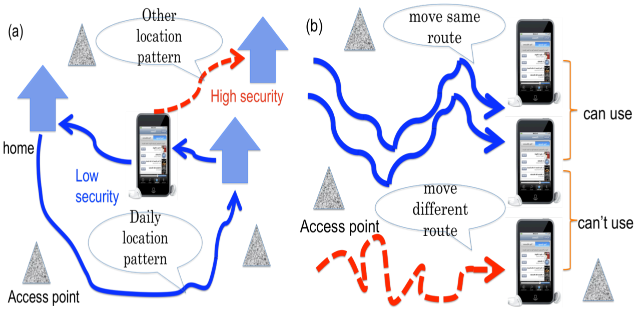

Figure1: Usage examples. (a) Pattern of a device move around in a same daily route or not, (b) Pattern of two devices move around in a same route or not.

One is for single device security (Figure 1 (a)). When a user carries a device such as a cellular phone, a digital camera, or laptop computers, their location histories become similar to the owner's. Then the device can detect whether the device is in a normal (and repetitive) activity situation or not. For example, if a user's daily morning activity is commuting from his/her home to the office, the device also detects this situation, and set the security level lower. However, when the device detects unusual activity pattern, the device detects and set security level higher. For example, if a user attends an event instead of going to the office, a user's laptop would require password to use it. Even when other users move a PC to its owner's office, normal authentication operation is still required unless the movement route to the office is not identical to its owner's.

The other model is to use fingerprint history to allow connection between devices (Figure 1 (b)). If a user always carries two devices, such as a cellular phone and a digital camera, these two devices would have similar Wi-Fi fingerprint history. In this case, the device would allow connection to the other without strict security control. However, if devices were not sharing similar activity patterns, security level would become higher. Security level can be changed by setting different time period of Wi-Fi pattern (e.g. day, week, month). Although an attacker could be able to get similar Wi-Fi fingerprints by shadowing the target, if period of Wi-Fi fingerprint for authentication is enough long, it is difficult to get similar one's.

We focus on Wi-Fi information because it can be used in both indoor and outdoor environments. In contrast to "Smart-its Friends", we need not put a new sensor, because almost all mobile devices have Wi-Fi function. Moreover, the above scenarios do not require device's location information. This feature makes this security model more scalable, because it only assumes reasonable numbers of Wi-Fi access points surround us, and no Wi-Fi location database is necessary.

EXPERIMENTS

Our method focuses on using recorded activity histories for authentication. In a possible usage example, discriminant capability between given multiple time series of Wi-Fi fingerprints is strongly needed. The system should be able to detect difference of movements only by observing fingerprints from two Wi-Fi equipped devices. In order to confirm feasibilities of proposed method, following two experiments are carried out. A pair of Apple iPod touch was used as Wi-Fi devices for these two experiments.

Experiment 1: To confirm a correlation of Wi-Fi fingerprints from two devices, activity histories are captured when these are carried by two people walking together.

Experiment 2: To clarify the differences of Wi-Fi fingerprints, activity histories are captured when two devices are carried by two people walking on different route in urban environment.

Correlation ratio of Wi-Fi fingerprints between two devices is shown in Figure 2. Axis of ordinate is correlation rate of matched Wi-Fi fingerprints (%). Axis of abscissas is time (second). Correlation rate is calculated by a number of matched MAC addresses from both devices in range of 15 seconds divided by total number of captured MAC addresses. During overall period shown in Figure 2, two people are walking together in period A and C (Experiment 1) and walking on different route in period B (Experiment 2). Each period also corresponds with route A, B and C in map shown in Figure 3.

RESULTS

In period A and C, average correlation ratio is 73.7%. In these periods, precision rate is 75.8% when discriminal threshold is 50%. Decreasing correlation rate is caused by scan failure of Wi-Fi fingerprints. On the other hand, average correlation of period B is 14.8% and precision is 92.5%. It is confirmed that correlation rate is highly depends on distance between two devices in daily environment.

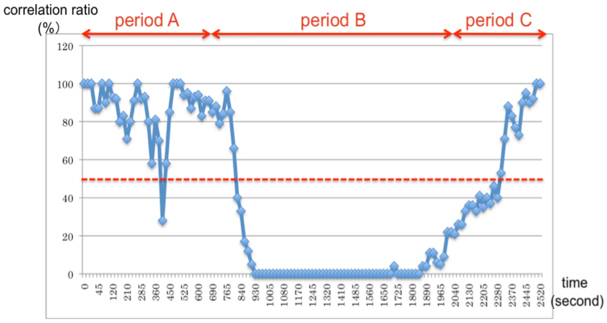

Figure2: correlation ratio of Wi-Fi fingerprints.

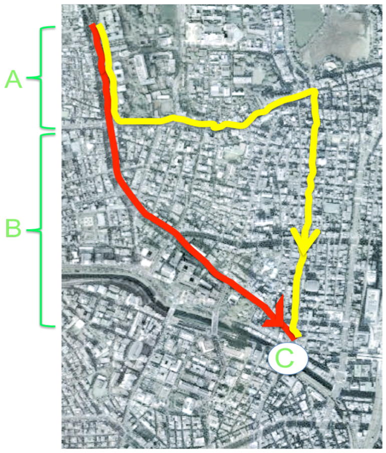

Figure3: a route mapping of walking for this experiment.

CONCLUSION

We proposed to use the changing ambient Wi-Fi signals for authentication. The result of experiment showed that activity history of persons or objects can be used for authentication. We are also looking at incorporating RSSI information for more accurate distance measurement.

REFERENCES

1. Holmquist, L. E., Mattern, F., Schiele, B., Alahuhta, P., Beigl, M, Gellersen, H. W., Smart-Its Friends: A Technique for Users to Easily, Establish Connections between Smart Artifacts, Proc. Ubicomp 2001, pp.273-291, 2001.

2. Anthony, L. et al., Place lab: Device Positioning Using Radio Beacons in the Wild, In proc. of Pervasive 2005, pp.166-133, 2005.

3. Rekimoto, J., Miyaki, T., and Ishizawa, T. LifeTag: WiFi-based Continuous Location Logging for Life Pattern Analysis, Int. Symp. on LOCA2007 ,pp.35-49, 2007.

4. SKYHOOK Wireless, http://www.skyhookwireless.com/

5. PlaceEngine, http://www.placeengine.com