Poster: Leveraging Breathing for Continuous User Authentication

Conference Paper · October 2018

DOI: 10.1145/3241539.3267743

5 authors, including:

Jian Liu
Stevens Institute of Technology
35 PUBLICATIONS **561** CITATIONS

SEE PROFILE

Yudi Dong
Stevens Institute of Technology
3 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Yingying Chen
Stevens Institute of Technology
207 PUBLICATIONS **3,741** CITATIONS

SEE PROFILE

Yan Wang
Binghamton University
34 PUBLICATIONS **1,188** CITATIONS

SEE PROFILE

Poster: Leveraging Breathing for Continuous User Authentication

Jian Liu[†], Yudi Dong[§], Yingying Chen[†], Yan Wang[*], Tianming Zhao[*]
(The first two authors are co-primary student authors with equal contributions)

[†]WINLAB, Rutgers University, North Brunswick, NJ 08902, USA
[§]Stevens Institute of Technology, Hoboken, NJ 07030, USA
[*]Binghamton University, Binghamton, NY 13902, USA
jianliu@winlab.rutgers.edu,ydong6@stevens.edu,yingying.chen@rutgers.edu,yanwang@binghamton.edu,
tzhao7@binghamton.edu

ABSTRACT

This work proposes a continuous user verification system based on unique human respiratory-biometric characteristics extracted from the off-the-shelf WiFi signals. Our system innovatively re-uses widely available WiFi signals to capture the unique physiological characteristics rooted in respiratory motions for continuous authentication. Different from existing continuous authentication approaches having limited applicable scenarios due to their dependence on restricted user behaviors (e.g., keystrokes and gaits) or dedicated sensing infrastructures, our approach can be easily integrated into any existing WiFi infrastructure to provide non-invasive continuous authentication independent of user behaviors. Specifically, we extract representative features leveraging waveform morphology analysis and fuzzy wavelet transformation of respiration signals derived from the readily available channel state information (CSI) of WiFi. A respiration-based user authentication scheme is developed to accurately identify users and reject spoofers. Extensive experiments involving 20 subjects demonstrate that the proposed system can achieve a high authentication success rate of over 93% and robustly defend against various types of attacks.

CCS CONCEPTS

• **Security and privacy** → **Biometrics**; **Multi-factor authentication**; • **Human-centered computing** → *Ubiquitous and mobile computing design and evaluation methods*;

MobiCom '18, October 29-November 2, 2018, New Delhi, India

ACM ISBN 978-1-4503-5903-0/18/10.
https://doi.org/10.1145/3241539.3267743

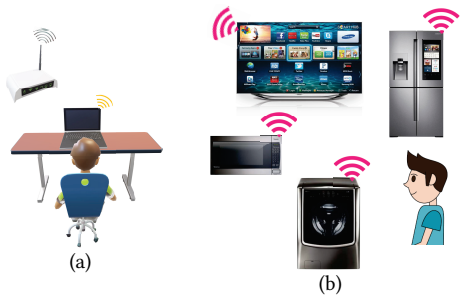


Figure 1: Potential applications that utilize respiratory motions extracted from WiFi to conduct continuous user authentication: (a) accessing mobile devices such as computers; (b) accessing electronic devices and appliances in smart homes

KEYWORDS

Continuous Authentication, Breathing, WiFi

ACM Reference Format:
Jian Liu, Yudi Dong, Yingying Chen, Yan Wang, Tianming Zhao. 2018. Poster: Leveraging Breathing for Contin-uous User Authentication. In *The 24th Annual International Confer-ence on Mobile Computing and Networking (MobiCom '18), October 29-November 2, 2018, New Delhi, India.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3241539.3267743

1 INTRODUCTION

Reliable and convenient user authentication has become increasingly critical in recent years due to the rapidly increasing use of mobile devices (e.g., smartphones, smartwatches, smart appliances, and laptops). Current mobile devices usually request user authentication in an on-demand manner. For example, unlocking smartphone and mobile computing devices, logging in email accounts, processing mobile payment, applying parent control, etc. And most of them involve only one-time identity verification, which requires users to re-verify themselves every time use the particular services.

We envision that the ultimate goal of user authentication is to free users from manually entering secret information for identity verification and enable computing devices to identify the users around-the-clock automatically. In this work, we take advantage of the WiFi infrastructures that are already pervasive in our daily lives and devise an innovative user authentication system that can verify users' identities based on their respiratory biometrics continuously. Existing work [3] has demonstrated that WiFi signal can be re-used to detect human vital signs (e.g., breathing rate). Our system takes one step further to provide non-invasive continuous authentication only relying on breathing independent of user behaviors in various applications. As illustrated in Figure 1, our system could let users log in their mobile devices (e.g., the laptop in Figure 1(a)) without entering passwords and continuously use user-specific applications without additional identity verification. Furthermore, our system could be applied to WiFi-enabled devices and appliances (e.g., Amazon Echo, smart TV at home), which allow users to perform restricted operations (e.g., online purchase and parent control) without manually input authentication information, as shown in Figure 1(b). Specifically, our system leverages the CSI readily available in commodity WiFi devices to capture users' unique biometrics rooted in their always-exist respiratory motions for user authentication. The main contributions of our work are summarized as follows:

- We explore the existing WiFi's sensing capability to capture respiratory motions and show that our morphologic-based features and fuzzy-wavelet-packet-based features can well model the unique respiratory biometrics enabling automatic user authentication.
- We devise the first respiratory biometrics-based user authentication system using off-the-shelf WiFi. Our system could be easily integrated into any WiFi-enabled devices (e.g., laptops, smartphones, and smart appliances) to continuously authenticate/identify users in an unobtrusive manner.
- We develop an respiration-based user authentication method that can accurately authenticate/identify users using the distinct biometric information rooted in their respiratory motions. And our scheme can also successfully reject spoofers using the feature distance to k nearest samples in the profiles.

2 SYSTEM DESIGN

2.1 Attack Model

Random Attack. The adversary does not have any knowledge of the user's respiratory patterns. When attacking the system, the adversary will stay at the same location as the user does and breathe in an randomly chosen style in terms of the breathing rate, inhale/exhale rhythm, and deepness.

Imitation Attack. The adversary has observed how the user passes the system using breathe multiple times. The adversary will stay in the same location as the user does and try to mimic the user's breathing pattern based on the adversary's observation.

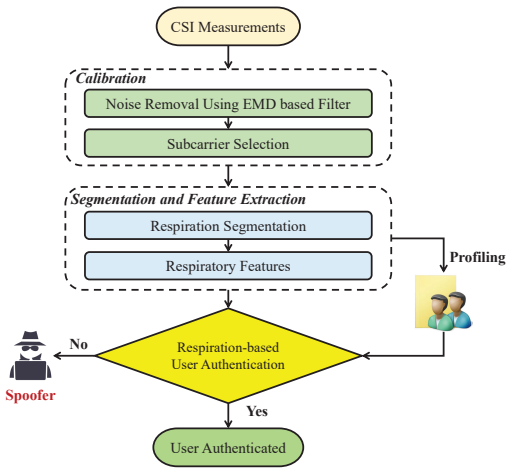
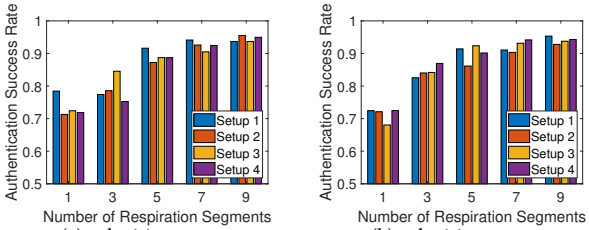


Figure 2: Overview of system flow.

2.2 System Overview

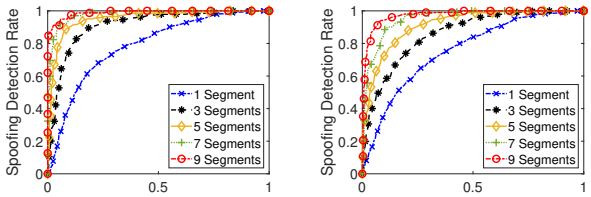
We devise a continuous user authentication system, which leverages the distinct respiration motions to differentiate users. The flow of our system is illustrated in Figure 2. Our system first continuously collects time series of CSI from off-the-shelf WiFi devices and determines whether the wireless signals contain repetitive respiratory patterns with human respiratory frequency or not. Once detects the respiratory patterns, the system applies an Empirical Mode Decomposition (EMD) based filter [1] to mitigate the effects caused by the immanent/environmental radio interference, which generates the CSI samples with more significant patterns related to respiration. Unlike conventional filters (e.g., low-pass or band-pass filters) that may mistakenly remove useful signal components due to fixed cutoff frequencies, the EMD-based filter is fully data-driven and can adaptively filter the noisy components and maximize the preservation of the signals resulted from respiratory motions. Then the filtered CSI samples are analyzed by a subcarrier selector to determine the most sensitive subcarrier that is most significantly impacted by respirator motions based on the periodicity and sensitivity. The measurements of the selected subcarrier are further processed to reconstruct the respiratory motion signals that well capture the tiny movements of the human body (e.g., belly and chest) caused by respiration.

To facilitate effective feature extraction, our system examines the reconstructed CSI signals and identifies the segments containing complete respiratory cycles. We extract unique respiratory biometrics in each respiratory segment using both waveform morphology analysis and fuzzy wavelet packet transform (FWPT) [2]. The extracted morphological



(a) 1 legitimate user (b) 5 legitimate users

Figure 3: Performance of user authentication with different numbers of respiration segments.



(a) Random attacks (b) Imitation attacks

Figure 4: Performance of spoofing detection (ROC curves) under random and imitation attackers with different numbers of respiration segments.

features (e.g., inhaling/exhaling rhythm, breathing depth, duration, etc.) and the FWPT based features are mutually complementary to discriminate individuals. Finally, the derived respiratory features are used to construct legitimate users' profiles during the system enrollment. For the user authentication process, the user's incoming respirations are continuously examined by our scheme, which identifies the legitimate user and spoofer through comparing the feature distances to the k nearest samples in users' profiles.

3 PRELIMINARY EVALUATION

3.1 Experimental Methodology

We conduct experiments in an 802.11n WiFi network with two commercial laptops. Specifically, we deploy two Dell E6430 laptops to exchanges WiFi packets periodically. The packet transmission rate is set to 200 pkts/s to guarantee the high resolution of the derived respiratory motions. Our system is evaluated in a university office with the size of $17ft \times 9ft$, in which two laptops generate WiFi traffics continuously. One of the two laptops is emulated as the mobile device that the target user is operating. The target user sits with a chair in front of this laptop to breath regularly during the experiment. The distance from the participant to the accessing laptop is 0.2 meters, which is a common distance that most people would use when operating the laptop. Another laptop, emulated as the access point, is used to exchanges WiFi traffic with the accessing laptop. Two laptops are placed at on the same desk side by side.

3.2 System Performance

We examine the user authentication performance of our system by analyzing the user authentication success rate. Figure 3 illustrates the user authentication success rate when different numbers of respiration segments are available for testing. Specifically, Figure 3(a) depicts the authentication success rate when the system only contains one legitimate user. The authentication rate achieves around 90% accuracy when five or more respiration segments are used for testing. When the system has multiple registered users, it can achieve similar authentication accuracy as illustrated in Figure 3(b). In general, we find that our system can achieve over 90% accuracy when using few respiration segments.

In addition, we evaluate our system under random attacks and imitation attacks. In the random attack experiment, we consider 5 of the 20 subjects as legitimate users and the other 15 subjects act as spoofers. Figure 4(a) depicts the ROC curves with different numbers of segments for testing. We can see that our spoofing detection rate reaches over 92.14% with the false positive rate of around 5% when the system integrates the testing results of 9 respiration segments. While in the imitation attack, 1 participant acts as the legitimate user and 10 participants try to imitate the legitimate user's breathing style (e.g., breathe with similar breathing depth/duration and holding duration). We show that our system can also detect the imitation attackers with the high accuracy and low false positive rate, which are presented in Figure 4(b). Specifically, we can achieve over 89.24% detection rate with 5% false positive rate when the system combines the testing results of 9 respiration segments. All the above results validate the great robustness of the proposed system under both random and imitation attacks.

4 ACKNOWLEDGMENT

This work was partially supported by the National Science Foundation Grants CNS-1820624, CNS-1826647 and ARO Grant W911NF-18-1-0221.

REFERENCES

[1] Huang, N. E., Shen, Z., Long, S. R., Wu, M. C., Shih, H. H., Zheng, Q., Yen, N.-C., Tung, C. C., and Liu, H. H. The empirical mode decomposition and the hilbert spectrum for nonlinear and non-stationary time series analysis. In *Proceedings of the Royal Society of London A: mathematical, physical and engineering sciences* (1998), vol. 454, pp. 903–995.

[2] Khushaba, R. N., Kodagoda, S., Lal, S., and Dissanayake, G. Driver drowsiness classification using fuzzy wavelet-packet-based feature-extraction algorithm. *IEEE Transactions on Biomedical Engineering 58*, 1 (2011), 121–131.

[3] Liu, J., Wang, Y., Chen, Y., Yang, J., Chen, X., and Cheng, J. Tracking vital signs during sleep leveraging off-the-shelf wifi. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc)* (2015), pp. 267–276.