Passive Biometrics for Pervasive Wearable Devices

[Poster Abstract]

Cory Cornelius, Zachary Marois, Jacob Sorber, Ron Peterson, Shrirang Mare, David Kotz
Institute for Security, Technology, and Society
Dartmouth College, Hanover, NH
{firstname.lastname}@dartmouth.edu

1. INTRODUCTION

Wearable devices – like the FitBit, MOTOACTV, and Jawbone UP – are increasingly becoming more pervasive whether for monitoring health and fitness, personal assistance, or home automation. While pervasive wearable devices have long been researched, we are now beginning to see the fruits of this research in the form of commercial offerings. Today, many of these commercial wearable devices are closed systems that do not interoperate with other devices a person might carry. However, we believe these commercial offerings signal the coming of wireless body-area networks that will connect these pervasive wearable devices and leverage the existing devices a user already owns (e.g., a smartphone). Such wireless body-area networks will allow devices to specialize and utilize the capabilities of other devices in the network. A sensor, for example, might harness the internet connectivity of a smartphone to store its data in the cloud. Utilized in this way, devices will become cheaper because they will only require the components necessary for their speciality, and they will also become more pervasive because they can easily be shared between users.

In order for such a vision to be successful, these devices will need to seamlessly interoperate with no interaction required of the user. As difficult as it is for users to manage their wireless area networks, it will be even more difficult for a user to manage their wireless body-area network in a truly pervasive world. As such, we believe these wearable devices should form a wireless body-area network that is passive in nature. This means that these pervasive wearable devices will require no configuration, yet they will be able form a wireless body-area network by (1) discovering their peers, (2) recognizing they are attached to the same body, (3) securing their communications, and (4) identifying to whom they are attached. While we are interested in all provisions of these passive wireless body-area networks, we focus on the last requirement: identifying who is wearing a device.

2. PASSIVE BIOMETRICS

Identifying who is wearing a device is necessary for nearly all applications of wireless body-area networks. Personal assistance devices will need to know which person they are assisting, while home automation systems can adjust the home to suit the wearer's preferences. However, the most interesting application that requires such provision are mobile health (mHealth) systems. Because these mHealth systems collect medical related data, this necessitates labeling the data with the patient whose sensors in their wireless body-area network collected it. Without such a label, physicians would not be able to use the data for diagnostic purposes; or worse, they might make a correct diagnosis about the wrong person in the case of mislabeled data.

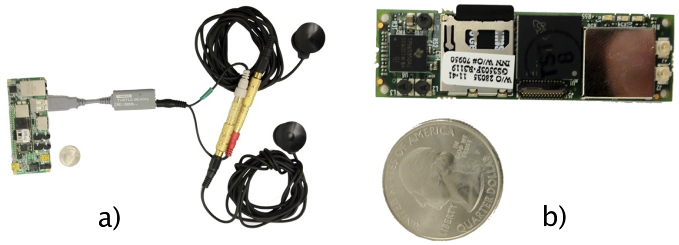

Figure 1: a) Prototype wearable device for collecting vocal resonance: Overo mounted on Gumstix Tobi expansion board, USB sound card, and two contact microphones, b) A Gumstix Overo Fire COM

Identifying who is wearing a device can be accomplished using biometrics. Typically, biometrics leverage the physiological characteristics (e.g., facial features, hand geometry, fingerprint, iris structure, and DNA) or behavioral characteristics (e.g., keyboard dynamics, vocal acoustics, locomotion and signature mechanics) of a person to identify them. Any characteristic that is *universal*, *unique*, *permanent*, and *measurable* qualifies as a biometric. We impose the additional constraints that a biometric be *unobtrusively measurable* so as to require no interaction by the user, and *difficult to circumvent* since impostors are a concern. We call such a characteristic that satisfies all these constraints a *passive biometric.*

3. VOCAL RESONANCE

We propose *vocal resonance* as a passive biometric. Vocal resonance is the voice of a user as measured through their body. We can measure this using contact microphones attached to a place on their body that can sufficiently pickup their voice through their body. By using contact microphones placed on a user's neck, we can then learn a model of that user's vocal resonance much like traditional speaker-identification methods. Like traditional speaker-identification methods, vocal resonance is unobtrusively measurable because all the user needs to do is speak. However, unlike traditional speaker-identification systems, vocal resonance is more difficult to circumvent because an adversary would need to capture a user's voice as it is heard through their body (and not just through the air).

We prototyped a wearable device utilizing vocal resonance using a Gumstix computer with contact microphones as shown in Figure 1. We also have collected vocal resonances of 25 subjects (17 males, 8 females) and describe a method inspired by traditional speaker-identification techniques to distinguish users. We then show the feasibility of vocal resonance of a passive biometric in terms of universality by measuring how well our method can distinguish users over our sample population.

Acknowledgements

This research results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation under Grant Award Number 0910842 and the Department of Health and Human Services (SHARP program) under award number 90TR0003-01. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.