such as motion sensors, camera, microphones etc. Since the same sensors are also available on wearables, we would like to explore behavioral biometrics in this proposal. Considering that cameras and microphones, as well as vision/audio processing algorithms, are quite energy-hungry, we thus focus on those behavioral biometrics that can be easily captured by sensors that require less power consumption, such as accelerometer and gyroscope. More specifically, we propose to authenticate wearable devices to users based on one type of behavioral biometric characteristics – our unique body movement patterns, especially movement patterns when there are external stimuli such as music beats.

Body movement patterns have long been used by us humans to discriminate between people. By watching how a person walks, dances, waves her hands, we can often recognize the person from afar. This is because human body movements are *distinctive* and *repeatable*. Achieving the same through wearables, however, is not straightforward and poses significant research challenges: it is unclear whether these seriously-constrained devices are able to capture the movement patterns, process the data, and quantify the uniqueness of each user's behaviors. In this proposal, we set out to design an accurate, robust and light-weight authentication system based upon free-style human body movements. In order to make free-style body movements repeatable, we use fast-tempo music to stimulate movements. Our preliminary investigations show that under very controlled experiments, music-stimulated body movements have great potential to be used to authenticate users to their wearable devices. In order to develop a full-fledge authentication system that works in realistic settings, we propose several techniques to maximize the authentication accuracy and robustness by trying to increase the information encoded in sensor signals, exploiting multiple movements and/or multiple sensors, learning how to authenticate users in mobile settings, and designing movement pattern based "passwords", as well as minimize its power consumption and processing requirement by carefully selecting features and classifiers, pipelining authentication operations and dynamically adjusting the data sampling rate.

Our research involves a coordination of algorithm design and system evaluation, ultimately involving the construction of a realistic authentication system that can efficiently run on wearable devices. Our project also involves an important curriculum development effort. We intend to train next-generation workforces in the rapidly-growing mobile computing field, as well as recruit youth and women into research in this field.

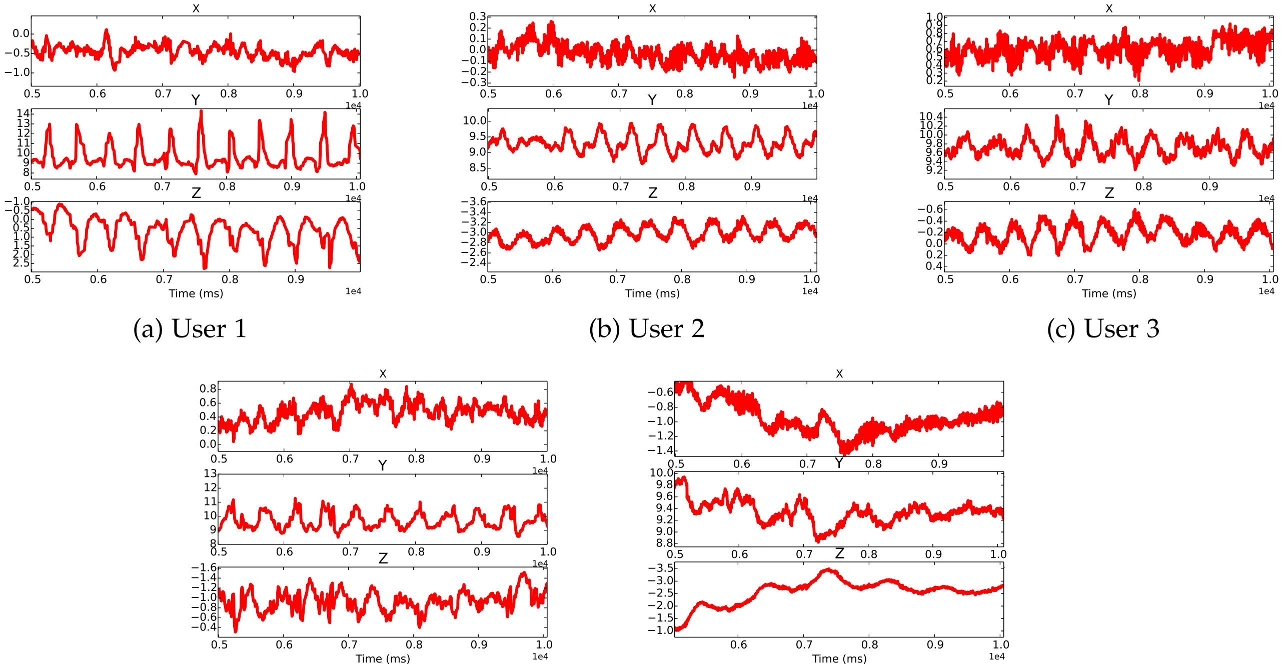
2 Background and Overview

2.1 Background on Behavioral Biometrics

Considering the fact that wearable devices relate significantly to "what we wear" on the human body, biometrics can play a key role for direct authentication to wearable devices. Biometrics allow a system to identify a user based upon "who you are" (i.e., her physiology) instead of "what you have" (i.e., ID cards) or " what you remember" (i.e., passwords) [48, 67, 97]. Physiological biometrics such as DNA, ear shape, face, fingerprint, hand/finger geometry, iris, odor, palm-print, retinal scan, and voice, have been very effective and widely used in many prototype and commercial authentication systems [90, 98, 106, 44, 88, 98, 7, 39, 60, 74, 15, 13, 79, 47]. In addition, body shape such as body height, width, and body-part proportions can also be used as biometric cues to identify different people [20]. Even "soft" characteristics such as body weight and fat percentage have been considered as secondary biometrics for authentication purposes [5].

However, biometrics are not prominently used in wearable devices commercially available today, though there have been specific point commercial designs (e.g., Nymi [3]). This can be attributed to the fact that biometrics would require the specific hardware/sensor available on the wearable device. Also the overheads for physiological biometrics in wearable devices can be high, in both, cost for hardware as well as integration and computing.

Another approach to direct authentication is using behavioral biometrics where unique signatures from human behavior (subconscious or in response to external stimulus) provide cues for differentiating and authenticating users. For example, it has been shown that gait (e.g., stride length, the amount of arm swing) when the user is walking or running is a reliable identification cue, and irrespective of the environment [81]. Okumura et.al. [68] have shown that the human arm swing patterns can be used to create signatures to authenticate to their cell-phones. Monrose et.al. [65] show that keystroke rhythms, when users type on the keyboard, that include typing dynamics such as how long is a keystroke, how far is between consecutive strokes, and how is the pressure exerted on each key, can be used as a biometric to authenticate users. Similarly, mouse usage dynamics [49] and touchpad touching dynamics [14, 23] have also been shown to serve as



(a) User 1

(b) User 2

(c) User 3

(d) User 4

(e) User 5

Figure 1: These plots show the raw accelerometer data in the time domain for five different users when they move their head in response to a music track wearing the same Google glass. The plots indicate that different users' head movement patterns appear distinctive from each other. The five users wore a Google Glass (in turns) and listened to a 10 second audio snapshot of a pop song.

potential biometrics.

In comparison to other means of authentication, behavioral biometric authentication can offer a more convenient (than physiological biometrics), and more secure (than indirect authentication) solution for wearable device authentication. With the increasing off-the-shelf availability and (almost) unlimited access to the motion sensors on the wearables, it has become possible to generate and/or infer unique behavioral signatures specific to users. We use these rationale as a motivation for our proposed design of a behavioral biometric based authentication that generates unique signatures from user's body movements. We design an authentication system, dubbed *Headbanger*, for wearable devices by monitoring user's body-movement patterns (e.g., head movements, arm movements, and hand movements) in response to an external music stimulus. Here, we do not limit body movements to pre-defined templates; rather, the user chooses *free-style* movement she feels the most natural to do.

2.2 Body Movement as a Behavioral Biometric

According to [48], a human characteristic can be considered as biometric as long as it is *universal*, *distinctive*, *repeatable*, and *collectible*. With the advancements in wearable computer designs it is becoming easier for collecting body movement patterns using the built-in sensors (e.g., accelerometer sensor, gyroscope sensor, motion sensor, etc). Such sensors are available on most wearable devices available today, thus making body movements that are both *universal* and *collectible*.

In this proposal, we will show that free-style natural body movements are *distinctive* and *repeatable*, especially when combined with external stimuli such as music. In *Headbanger*, music plays a crucial role in stimulating body movements such that the resulting movement pattern is natural to the user (more distinctive) and easier to remember (more repeatable). It has been shown [101] that most people move their body as a natural response to external rhythmic stimuli such as music; even at a very early age, infants respond to music and their movements speed up with the increasing rhythm speed. Most adults naturally perform head