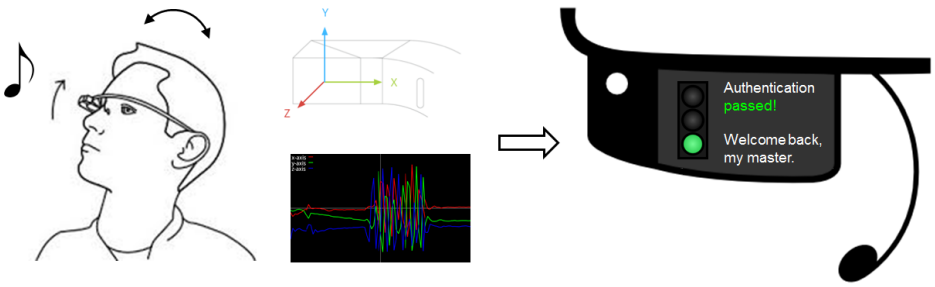

Figure 2: Illustration of Headbanger. The head-worn device authenticates the right user based on signatures generated from head-movement patterns in response to an audio snapshot played on the device.

movements or hand movements when listening to a fast beat audio track. When combined with external rhythmic stimuli, we believe body movements become more distinctive – not only a person's movement pattern is unique, but her response to rhythmic stimuli is also unique. In this way, the resulting authentication system will be more dependable.

Before we go ahead and design our system, we first conducted a preliminary analysis of the accelerometer signals from five Google glass users' head movements, and show the raw signals in Figure 1 (a)-(e). A quick glance at the raw signals reveals that these users *repeatedly* showed unique and *distinctive* head-movement patterns, when listening to the same music beats on the head-worn device. Motivated by this observation we hypothesize that *body movements can be a good behavioral biometric characteristic to authenticate users to their smart wearable device*.

Example Body Movement Patterns: Depending upon the wearable device to be authenticated, we can focus on the movements of different body positions. For example, head-mounted devices such as smart glasses can easily capture a user's head movement or eye lid movements; wrist-mounted devices such as smart watches can easily capture a user's arm/hand movements; shoe-based smart devices can easily capture a user's gait; smart rings can easily capture a user's finger/palm movements.

To facilitate natural and repeatable body movements, we can play short, fast-tempo music tracks on the wearable devices, and measure the resulting body movements using built-in sensors such as accelerometer sensor, gyroscope sensor, infrared sensor, etc.

Earlier Work on Body Movement Based Activity Detection and Authentication: There have been a few point solutions that used body gesture/movements (captured by sensors such as accelerometers and gyroscope) for activity detection or authentication purposes. For example, Harwin et al. [37] used head gestures (e.g., combining pointing and movements) for human computer interaction. Eye blinking pattern was looked at in [87] as a unique feature for authentication. Ishimaru et al. [46] proposed to combine the eye blinking frequency from the infrared proximity sensor and head motions from accelerometer sensor on Google Glass to recognize activities (e.g., reading, talking, watching TV, math problem solving, etc). Accelerometers have also been used for other parts of body movements for gait analysis, motion detection or user identification, such as waist [6], pocket [33], arm [68, 34], leg [32, 51, 59, 24] and ankle [31]. Hand gesture is often used to authenticate users on devices with touch screens. A number of features, including touch location, swipe/zoom length, swipe/zoom curvature, time, and duration, have been exploited to authenticate smartphone or tablet users [76, 30, 17, 29, 56, 78].

How *Headbanger* Is Different: Compared to earlier point solutions that used simple/limited body movements or body gesture to authenticate users for smart phones or tablets, the unique constraints of wearable devices, combined with free-style natural body movements, open up a completely new line of investigation in capturing body movement patterns, extracting unique user movement signature, and authenticating the user accordingly. Given the unique challenges of *Headbanger*, we will focus our investigation on the following two important questions: (1) Can we establish body movements as a biometric characteristic, and can sensors on wearable devices accurately capture the uniqueness of one's body movements? and (2) Can we run the body movement based classification algorithms on wearable devices without relying upon a second device?

2.3 Overview of *Headbanger*

We refer to the proposed body-movement based authentication system as *Headbanger*. We envision that *Headbanger* will be used as an authentication interface on the wearable device, which will run upon device power-up, similar to the screen-lock in smartphones or the head-nod interface on Google Glass [2].

The authentication process has two parts: offline training and online authentication. In the offline training phase, the system collects the real user's body movement data and establish the features, which are referred to as *reference* data. In the online authentication phase, we first ask the user to claim her ID from a list of user IDs (this can be done through simple gesture or voice). Next, we ask the user to pick a music track from a list of music tracks: if her pick does not match the claimed user's pick, then the authentication process exits immediately and returns FALSE. Otherwise, *Headbanger* continues to go through the following steps:

- *Test sample collection*: In this step, we play the chosen music track for a few seconds (usually for up to 10 seconds), and ask the user to move along with the music. It is up to the user to decide which part of the body she will move(e.g., a combination of head, eye, arm, hand, leg, etc) and she will move. The advantages of using music as external stimuli are two-fold: (1) humans naturally respond to music beats by moving parts of their body, and (2) each person responds to music beats in different ways, and thus more user-specific information can be encoded in the movement pattern.

  We record the raw sensor signals (e.g., from built-in accelerometer sensor or gyroscope sensor) during the music play period. We refer to the raw sensor data collected during a music track duration as a sample, e.g., an *ACC* sample is the accelerometer data collected during the music period, and a *GYRO* sample is the gyroscope data collected during the music period. After collecting the raw samples, we filter the samples to remove records of spurious motion so that the resulting sample will be much smoother and ready for subsequent processing.

- *Classification*: In this step, we extract features from the filtered signal and run the classification algorithm against the reference data that was collected during the offline training phase. We will study a large set of features and classification algorithms and choose those that are suitable for wearable devices. If there is a plausible match, the user is accepted; otherwise, she is rejected.

Figure 2 illustrates the working of *Headbanger*. In this example, we try to authenticate Google glass users by monitoring their head movement patterns with music as external stimuli.

2.4 Research Challenges

Even though body movements have been used as biometric characteristics in other systems, it is completely unknown whether this method can be applied to wearable devices due to their unique constraints: (1) first, wearable devices are limited in battery/processing power and the types of sensors available to them, and (2) wearable devices should be able to deal with a much larger variety of body movements. Towards building a robust authentication system that solely runs on wearable devices, we strive to address two significant challenges in this project.

The first challenge is *how we can establish body movement patterns as reliable biometric characteristics for authentication purposes.* In real life, it is common for us humans to recognize a person who is still far away by watching how she walks, i.e., her walking gait. To our brain, gait is unique, so are many other body movements. For example, by looking at how a person dances, we surely can recognize whether she is one of our friends. However, whether the device we have, and/or the sensors available to the device, can capture, present, and quantify the uniqueness of these body movements, remains a challenge. The challenge is even more severe for seriously resource-constrained wearable devices and free-style natura movements. In this project, we will explore ways to address this challenge. Towards this goal, we will find ways to pack as much as information in the sensor data, we will also try to authenticate users no matter they are stationary or walking, we will combine multiple movements that can be captured by a single wearable device, we will exploit multiple sensors to increase the authentication accuracy. For those users who desire a more secure authentication, we also exploit the fact that wearable devices can give out stimuli that only the wearer can feel to design body movement passwords which can greatly improve the authentication performance.

The second challenge is *how we can minimize the resource consumption and processing delay of* Headbanger . In order to achieve accurate classification results, it is often unavoidable to rely upon complex features and