Project Summary

TWC: Small: Authenticating Smart Wearable Devices Using Unique Human Body Movement Patterns

Zhang, Rutgers University

This is the summary.

1 Introduction

We live in a world that has seen a generation of technological revolutions; from wired to wireless communications, immovable to mobile machines, large sized to hand-held devices. Today, we are witnessing what can be deemed as the next phase of mobile revolution through *wearable computers*. Research in wearable computers can be dated back to as early as 1980s when Steve Mann developed a prototype heads-up-display goggles [19]. Thanks to the advances in hardware miniaturization technology, cheap sensors/processor chips, and low-power sensing/computing, today, wearables are available off-the-shelf and have almost become an integral part of human lives [2, 4, 1].

With the onset of proliferation of wearable devices, preserving security and privacy of these devices and the data on the devices, is becoming critically important – most of the data is highly personal to the user. A solution for safeguarding the security and privacy of user's data on the wearable device, however, is only effective as long as the device itself is authenticated to the right user/owner.

Authentication on most commercially available wearable devices today [1, 4] relies on an indirect mechanism, where users can login to their wearables through their phones. This requires the wearable device to be registered and paired to the user's mobile device, which makes it inconvenient as the user has to carry both the devices. The security of this approach is also in question as it increases the chance of hacking into both the devices if either of the devices are lost or stolen. Some devices including Google Glass [2] and FitBit's health tracker [1], pair the device to the users email account instead of the phone for user's convenience; however, it does not add any security benefit. Though wearable devices today almost contain the same suite of sensors as a smartphone, the computing capacity and battery lifetime of wearables are far less comparable. This implies that, translating the same authentication solution from a phone to the wearable device, to enable direct authentication, is not only undesirable but also impractical. *Thus, the need for the day is a simple, low-power, and accurate direct authentication solution.*

Broadly speaking, there are two direct authentication methods that are commonly adopted: password based authentication and biometric based authentication. We argue that neither method is suitable for wearable devices. **** Collecting and recognizing these biometrics is subject to the availability of the sensing hardware and the computing capability on the wearable units, hence unrealistic in most cases.

In addition to password-based authentication and biometric-based authentication, there is another class of authentication method that relies upon the uniqueness of human behavior characteristics such as human walking gait, arm swings, typing patterns, body pulse beats, eye-blinks, etc. This way of authenticating users is called *behavioral* biometrics, which has been studied in the context of authenticating smart phones and tablets [28, 10, 30, 24, 22, 15, 7, 11]. In this proposal, we propose to authenticate wearable devices to users based on one type of behavioral biometric characteristics – our unique body movement patterns. We believe body movement patterns are well suited for authenticating wearable devices because ***.

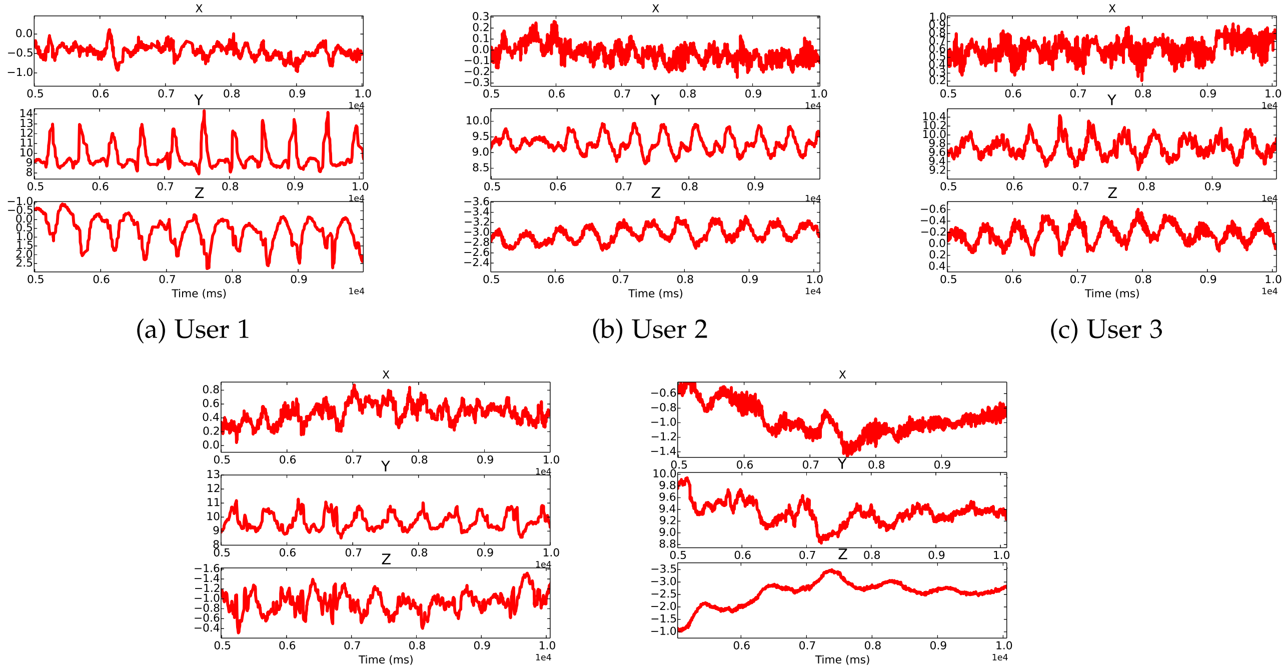
***Challenges ***

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 Authenticating Wearable Devices

Authentication mechanisms for a wearable device can broadly be divided into two categories: (i) *Direct* authentication, where the users can directly authenticate themselves to their wearable device using the input/output interface and/or using signatures generated from the sensors available on the device, and (ii) *Indirect* authentication, where a secondary device – typically the user's smartphone – is used as a medium



(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.

for authentication. Today's commercially available wearable devices predominantly use the latter approach where users login to their wearable devices through their smartphone – using a PIN or an email account.

Unlike the indirect approaches, that require a wearable device is registered to and connected (wireless) to a smartphone, direct mechanisms can leverage the built-in interfaces and sensors on the wearable device. 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) [14, 23, 32]. 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. In addition, body shape such as body height, width, and body-part proportions can also be used as biometric cues to identify different people [9]. 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.

An other 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 [30]. Okumura et.al. [24] have shown that the human arm swing patterns can be used to create signatures to authenticate to their cell-phones. Monrose et.al. [22] 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 [15] and touchpad touching dynamics [7, 11] have also been shown to serve as 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 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 unique body-movement patterns (e.g., head movements, arm movements, and hand movements) in response to an external audio stimulus.

We can use accelerometer data to detect a person's movement context such as walking or running [17], or to identify a person's gait characteristics [20, 12]. ***YZ: this needs to be moved. ***

2.2 Body Movement as a Behavioral Biometric

According to [14], 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 body movements are *distinctive* and *repeatable*, especially when body movements are combined with external stimuli such as music. It has also been shown [33] 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 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 present our body movement based authentication 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 glass*.

Example Body Movement Patterns: Depending upon the wearable device to be authenticated, we can focus on the movements of different body parts. 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 movements.

To facilitate natural and repeatable body movements, and to further set users apart from each other (by observing how their motor system responds to external stimuli), we can play short, fast-tempo music tracks on the wearable devices, and then measure the corresponding body movements using built-in sensors such as accelerometer sensor, gyroscope sensor, infrared sensor, etc.

2.3 Overview of *Headbanger*

We refer to the proposed body-movement based authentication 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 device keeps movement features of its legitimate users. Every time when a user tries to unlock the device, she is first asked to claim her user ID from the list of legitimate users. Next, the user is asked to pick a music track from a

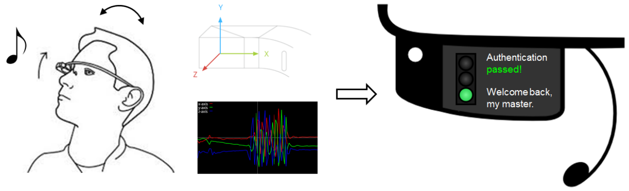


Figure 2: Illustration of Headbanger. The head-worn device authenticates the right user based on signatures generated from head-movement patterns in response to an audio snapshot played on the device.

preset music list: if her pick does not match the claimed user's pick, then the authentication process exits immediately. 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 her body along with the music. We then records the raw sensor signals (e.g., from built-in accelerometer sensor or gyroscope sensor) during the music period. We refer to the raw sensor data 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.
- *Signature generation*: In this step, we process the filtered signals to extract appropriate features and establish the user's movement signature.
- *Classification*: In this step, we classify the user's movement signatures against the signatures stored in the system to determine whether the user is who she claims. If there is a plausible match, the user is authenticated access; otherwise, she is rejected.

The illustration of *Headbanger* is shown in Figure 2.

2.4 Research Challenges

Specifically, the proposed research effort consists of the following thrusts:

- Developing signal processing and learning algorithms that can accurately identifying each user's body movement patterns.
- Developing a light-weight, low-cost authentication system that can run on wearable devices efficiently.

3 Establishing Body Movement Patterns as Behavioral Biometrics

3.1 Preliminary Results

In our preliminary study, we used Google glass to collect accelerometer data (*ACC* in short) when a user moves her head with music, and studied whether head movement patterns are distinctive and repeatable. After collecting raw *ACC* data samples, we went through the following steps to process the data:

1. *Filtering*: Since the frequency spectrum of the *ACC* samples is significantly concentrated within 5Hz, we filtered the raw samples using a low-pass digital Butterworth filter [8] by adopting a relaxed cut-off frequency of 10Hz. In this way, we removed spurious head movements and obtained smooth *ACC* data.
2. *Training Set Construction:* We constructed the training set to include m *ACC* samples from the legitimate user (which we refer to as *true* *ACC* samples), as well as m *ACC* samples each from N random users (referred to as *false* samples).

3. *Signature Generation*: Next, we generated signatures from the filtered *ACC* samples using the dynamic-time warping (DTW) tool [**?**]. DTW is generally used as a similarity matching tool for time-domain analysis of temporally varying signals. DTW compares a temporal signal with a reference signal over a certain time-window and yields a distance measure as the score. A low score (distance) implies that the test signal is in close match with the reference.

   Using DTW, we calculated the distances between true *ACC* samples and the distances between true samples and false samples, and refer to these two types of signatures as same-user distance signatures as well as across-user distance signatures.

4. *SVM Classification:* In the classification phase, we first calculated the DTW distances between the test sample and the true samples, and then feed these values and the signatures to a Support Vector Machine (SVM) for classification. SVM returns ′1′ to denote that the test user is legitimate and ′0′ to denote otherwise.

Distinctiveness: We designed the first set of experiments to show that even the simplest head movements are distinctive – i.e., it is hard to imitate other’s head movements. In this set of experiments, we employed simplest head movement patterns: nodding. We have one owner for the Google glass who designed the nodding pattern and 15 imitators who imitated the movement. We collected 100 10-second *ACC* samples from the owner, during the course of 60 days (from 10/1/2014 to 11/30/2014), ensuring the owner’s sensor data includes sufficient variation that naturally occurs with time. We also made a great deal of effort to make sure the imitators accurately imitate the owner’s movement – the owner carefully explained his movement pattern to each imitator, and sat through each data collection session for all the 15 imitators to make sure their movement pattern looks the same to the owner’s eye. For each imitator, we collected 40 10-second *ACC* samples. Using different combinations of training data and test data, we generated the classification results and summarized the mean FAR (false acceptance rate), FRR (false rejection rate), and BAC (balanced accuracy) in Table 1. The results show that *even simple nodding is not easy to imitate: nodding for 6 seconds can classify 95% of the users.*

Repeatability: We designed the second set of experiments to show that a user can successfully repeat her own head movement if each user is asked to come up with their own movement patterns. In this set of experiments, we had 8 subjects, and for each subject, we collected 38 *ACC* samples with sample duration of 10 seconds. Each subject performed different head-movement patterns of their choice. We report the average FAR, FRR, and BAC values in Figure 3, where Figure 3(a) shows the FRR and FAR values, while Figure 3(b) shows the BAC values. The results show that *head-movements are highly repeatable.* Among the 8 subjects that we studied, the highest BAC value is 100%, and the lowest is 91.81%, with the average BAC value of 95.57%.

3.2 Proposed Research

Our preliminary results show that head movement patterns have the potential to be used as a reliable biometric characteristic for wearable user authentication. However, in order to develop a full-fledged authentication system using unique body movements, we need to address several important challenges.

3.2.1 Feature Selection and Information Entropy

We usually characterize a person’s body movements using accelerometer (ACC) signals and gyroscope (GYRO) signals that are a few seconds long. In this project, we will investigate the following statistical

Sample duration (s)	2			3			6			10		
	FRR (%)	FAR (%)	BAC (%)	FRR (%)	FAR (%)	BAC (%)	FRR (%)	FAR (%)	BAC (%)	FRR (%)	FAR (%)	BAC (%)
SVM	25.0	16.74	79.12	15.0	14.05	85.47	3.33	6.66	95.0	0.0	9.62	95.18

Table 1: Average FAR, FRR, and BAC for SVM-based classification when we choose different 4 imitators in the training set (from the total 15 imitators). We have the results for different sample durations. In these results, we use the earliest 40 owner samples in the training set.

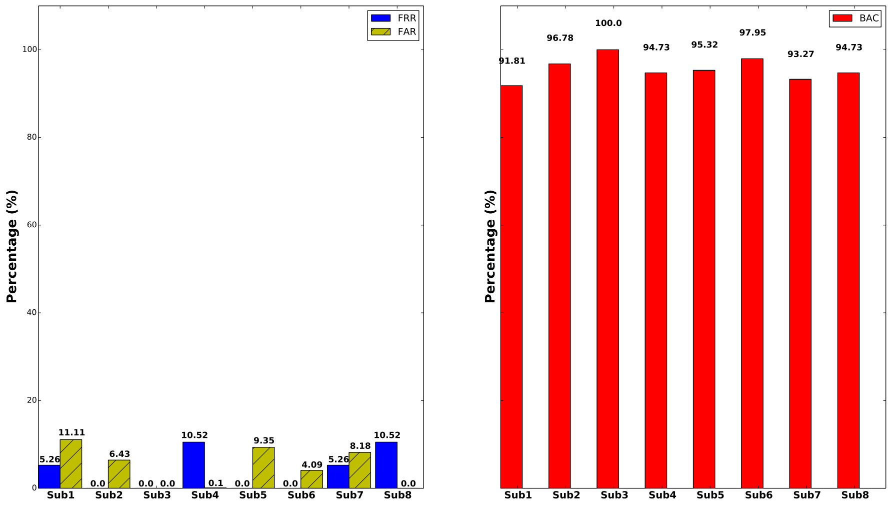


Figure 3: In this set of experiments, we studied whether a user can successfully repeat her own head-movement pattern. We had 8 subjects, each performing her own choice of head-movement patterns. We collected 38 samples for each subject. (a) shows the FRR and FAR results for each subject, and (b) shows the BAC results. Thresholding-based classification with top 3 voting was used to generate these results.

features that have been proposed for ACC/GYRO signals in the literature [25, 26, 27, 6, 34]: (1) mean, standard deviation, median, 25%, and 75% of frequency (in the frequency domain), (2) mean low and mean rectified high pass filtered signals (in the frequency space), (3) centroid frequency (in the frequency domain), (4) frequency dispersion (in the frequency domain), (5) power spectrum of entropy in acceleration/rotation and average energy in acceleration/rotation (in the frequency domain), (6) magnitude of first five components of FFT analysis (in the frequency domain), (6) jerk index that indicates the smoothness of the signal (in the time domain), (7) mean crossing (in the time domain), (8) maximum difference acceleration (in the time domain), (9) correlations between axes (in the time domain).

Boosting Information Entropy: It is important to encode as much information as possible into the measured sensor signals, i.e., boosting information entropy. One way of achieving this goal is to have the user make movements following the external music stimuli – different people translate music stimuli to motor movements in different ways. As a result, in addition to the above basic *ACC*/*GYRO* features, we will also consider features concerned with the temporal relationship between music beats and corresponding body movements, such as mean and standard deviation of the interval values (between a music beat and the subsequent body movement), the top interval values, etc. These features show a person's motor response levels to external music stimuli.

In order to further boost the information entropy, we can even change the music track between a data collection session, so that we cannot only measure the user's response to music stimuli in a steady state, but we can also measure how fast the user adapts to the change of rhythm in the music. Therefore, given the same total sample duration, this method can pack more information to the resulting signals.

3.2.2 Robust Authentication in Mobile Settings

Our preliminary results show that head movements are rather distinctive and repeatable in very controlled settings – all the data were collected when the participant was in a stationary setting, e.g., sitting on a chair. However, in reality, the behavior of body movement signatures over chaotic settings will be a key factor to decide on the effectiveness of this approach.

Authenticating Walking Users: In particular, we need to solve the challenge when the user is in a mobile context such as walking. In such a case, we can't rely on the original training data that is collected when the user was sitting or standing still any more; performing head/hand movements while walking will definitely lead to different movement signatures.

We can collect sensor readings in three different scenarios (we only focus on ACC data in this part for the sake of simplicity): ACC_{M+W}, denoting the sensor readings when the user is performing body movements while walking; ACC_M, denoting the sensor readings when the user is performing body movements while sitting or standing still; and ACC_W, denoting the sensor readings when the user is walking, without any special body movements. To address the challenge of authenticating walking users (whose test data is ACC^{tst}_{M+W}), a naive method is to use an external accelerometer (such as the one the smartphone) to record the accelerometer data while walking (ACC^{tst}_W). We can then extract the accelerometer reading caused by body movements as

$$ACC^{tst}_M = ACC^{tst}_{M+W} - ACC^{tst}_W.$$

Finally we can compare ACC^{tst}_W with the reference data ACC^{ref}_W to classify the user. Though simple and effective, this method does require another device, which is less convenient and less secure, as we have argued before. As a result, we will not adopt this method in the project.

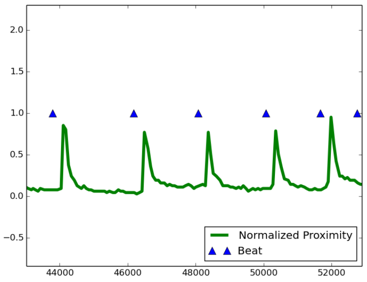
If we only use the accelerometer on the device, authenticating a walking user becomes much harder, mainly because a person's walking pattern is much less repeatable – factors such as trajectory, speed, terrain will have a bearing on the walking pattern – and the interaction between walking and designed body movements are very complex and hard to predict. Due to the complexity of this problem, we will investigate a learning-based authentication approach. In the learning phase, the system will ask the user to perform the designed body movements while she is in different walking contexts. The system will then run clustering algorithms on the collected accelerometer data, and cluster them into a small number of groups, representing the data sets in her typical walking contexts. For each group, we maintain a certain number of reference data.

In the testing phase, we adopt a two-level classifier. At the top level, we determine whether the user is stationary or mobile. This is rather easy because walking in general has much more energy than designed body movements as shown in Figure **??**. At the bottom level, if the user is walking, we then classify the test data against the user's reference data group by group. If none of the groups return TRUE classification results, we reject the user.

Something*:** In addition to a person's mobile setting, other factors such as a person's mood/energy level may also have an impact on her head movement signature; for example, a fresh and energetic user may provide significant head movements as compared to a sick or tired user whose signatures may not even be repeatable. Inconsistencies in the accelerometer sensor such as drift and temporal bias can significantly affect the nature of inferred head-movement signature. Head-movements, on the other hand, may also evolve over time for a person which call for periodic calibration of the system and/or the training data.

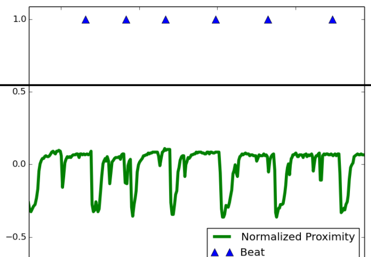
3.2.3 Multi-Modality Authentication

Smart-glass devices typically contain an array of motion sensors such as accelerometer, gyroscope, and inertial measurement unit (IMU). It is only a matter of time that motion sensor chips will be integrated into wearable devices. This opens up opportunities for multi-modal motion sensing. For example, accelerometer data can be combined with gyroscope measurements to provide multi-dimensional head-movement features that can improve the quality of the inferred signatures. Head movements can also be combined with other body movements to generate valuable, reliable signatures for authentication. In this project, we plan to explore these opportunities.



(a)

Combining Multiple Movement Signatures: In our preliminary study, we only looked at monitoring head movements for authenticating Google Glass. In reality,



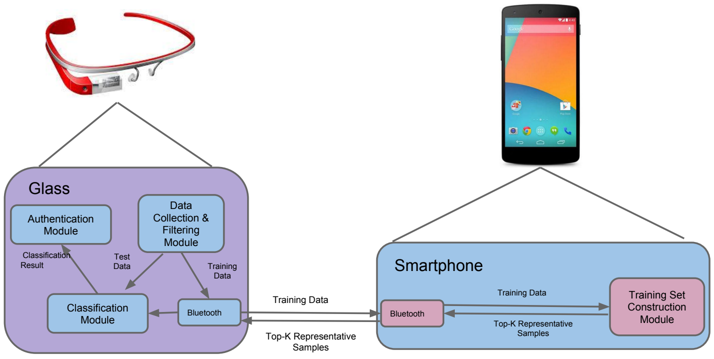


Figure 5: The software modules for the Headbanger authentication app we implemented in the preliminary study. Note that the Training Set Construction Module is executed on the bluetooth-paired smartphone because it is the most computing intensive module.

there are other types of movements that can be captured by Google Glass for authentication purposes. For example, through a simple test experiment using the Google Glass infra-red light sensor we observed that the blinking and winking patterns of users in response to the can be combined with head-movements for better results. *** YZ: Sugang, please include the blinking/winking picture here *** Recent studies have shown that heart beat or pulse can be read by Google Glass [13]. In this project, we will also look at whether the pulse information captured by the device can be combined with head movements for more accurate authentication.

The main challenge in combining multiple movement signatures stems from the fact that it is hard to separate their impacts on motion sensor readings (e.g, the fact that a user winks may change the way she moves her head). Hence, it may lead to less accurate authentication results. In this project, we will find ways of handing this challenge, similar to how we propose to authenticate walking users.

Combining Accelerometer and Gyroscope: Many previous studies have looked at combined accelerometer and gyroscope readings in detecting motion contexts such as walking, standing or fall [21, 16, 18, 35, 31, 29]. In our preliminary study, however, we find that gyroscope data from Goolge Glass fare very poorly in discriminating users' head movements. The reason is ***

4 Building an Efficient Body Movement Based Authentication System

4.1 Preliminary Work

Wearable devices have severe resource limitations in many aspects; to name a few, energy, computing, networking and storage. Building an efficient authentication system that can smoothly run on such devices, therefore, becomes a significant challenge. In order to investigate whether such a goal is attainable, we have implemented a *Headbanger* app on the Google Glass. Figure 5 shows the software modules the app consists of. In the implementation,

sample duration (s)	processing delay (s)
2	1.29
3	2.74
6	9.04
10	20.48

Figure 6: Measured processing latencies on Google Glass with different sample durations.

we established the training set and reference features on the smartphone since this step is offline and doesn't need to run on the device. The online authentication process is implemented on the device. In the implementation, we adopted a much simplified classification method. First, instead of having a set of reference samples, we only use one reference sample for each user. After computing the DTW distance between the test sample and the reference sample, we simply compare the distance to a pre-set threshold value to determine the classification result. In this implementation, we kept the algorithm to the bare minimum to test the processing capability and battery consumption of the Google Glass and did not worry about the classification accuracy.

Figure 6 shows the measured processing latency (the time that elapsed between when we finish collecting the test sample and when the authentication result is generated). The results show that even with a significantly reduced implementation, the processing delays are still rather substantial. For example, if the sample duration is 10 seconds, the processing delay is a little more than 20 seconds! More importantly, if there were other processes such as camera running at the same time, or if we continuously ran the *Headbanger* app for a few times, then the processing became very slow, and the glass became overheated and displayed "It is too hot. Glass needs to cool down." Then we needed to wait for 1 or 2 minutes for the glass to cool down. After the glass finally cools down, we had to start over the authentication process. We refer to this catastrophic situation as *glass overheat*.

Naturally, the second research challenge we address in this project is to optimize the system design of *Headbanger* to enable the efficient execution on severely resource-constrained wearable devices.

4.2 Proposed Research

We propose to investigate several runtime optimization techniques to make *Headbanger* suitable for wearable devices without changing the off-the-shelf hardware by minimizing the authentication latency and energy consumption. Please note that we could choose to offload computation to the device-paired smartphone to conserve cycles/energy on the wearable device, but *we will not pursue this route in this proposal*. Instead, we focus on *direct authentication* where wearable devices are not dependent upon smartphones or other more powerful devices for authentication, which we believe is more secure and convenient.

As discussed in Sec 3, a *Headbanger* authentication session consists of the following steps: (1) collecting test data, (2) extracting features from the test data, and (3) classifying the test data. Among these three steps, steps (2) and (3) usually consume more processing cycles/energy. In this project, we focus on optimizing these two steps. Before we present the proposed optimization techniques, we note that the first thing we need to is to carefully select features and classifiers in *Headbanger* from the set of features discussed in Sec **??**. We already know that using too many features may lead to noises and classification errors [**?**], but on wearable devices, this is even more catastrophic as it likely leads to quick device shutdown. As a result, we need to pay extra attention to what features we use and which classifier we adopt on the device. In the project, we will carefully measure the power consumption, processing delay, and classification accuracy of different combinations of features and classifiers, and then choose accordingly.

Pipelined Authentication: An important parameter for *Headbanger* is the sample duration T. So far, we assume that the system first collects ACC sample for T seconds, and then processes the sample (i.e., feature extraction and classification) to obtain the classification result. The value of T directly impacts the total authentication latency; larger T values lead to longer authentication latencies. From our preliminary investigation, we further take note that the processing delay increases more than linearly with sample duration – e.g., processing a 2-second sample takes 1.29 seconds, while processing a 10-second sample takes 20.48 seconds (according to Figure 6). As a result, we would like to have lowest possible T values. On the other hand, however, having a too small T value may lead

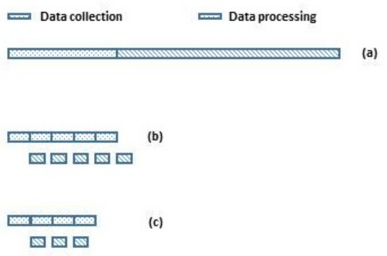


Figure 7: The benefit of pipelined authentication: (a) shows the original latency to collect and process a 10-second sample (numbers taken from Figure 6, (b) shows the much reduced latency by breaking the 10-second signal to five 2-second chunks and pipeline the collection and processing procedures, and (c) shows that the delay can be further reduced if using a portion of the signal

to inferior authentication accuracies. What further complicates the problem is that we find that it is impossible to find the uniformly optimal T value for different users. Thus optimizing this important parameter across different users becomes a serious challenge.

In this project, we propose to address this challenge by adopting the well-known pipeling technique, which is motivated by the characteristics of *Headbanger*. Suppose the original signal duration is T, and we have $T = nt$ with n being an integer and $t < 2$ seconds. Let us assume that the processing delay is less than t when the sample duration t is less than 2 seconds. Then we can explore the following pipelining method. In the first t-second window, the system collects the ACC sample for t seconds. In any subsequent t-second window, the system continues to collect the ACC sample for t seconds, and at the same time, processes the portion of the sample collected in the previous window. We refer to this method as *pipelined authentication*.

The proposed pipelined authentication can reduce the overall authentication latency in several ways. First, we overlap data collection and data processing to reduce the overall delay. Second, since processing shorter samples incurs less (than linear) latencies, by breaking a sample into smaller chunks can reduce the total latency. For example, using the numbers presented in Figure 6, we find that processing one 10-second sample takes much longer time than processing one 6-second, one 2-second, and two 1-second samples. Third, now we can conduct what we call "early classification" – maybe using a portion of the sample can already reveal the classification result – and then we don't need to collect/process the entire sample. That is, we can dynamically determine the shortest sample duration we need. Combing these two factors, we can achieve much reduced authentication latency (i.e., shorter data collection and shorter processing delays). Figure 7 illustrates the benefit of the proposed pipelined authentication scheme.

Finally, we note that in order to take the full advantage of pipelined authentication, we need to choose appropriate features whose performance is not highly dependent on the sample duration. For example, ***.

Authentication with Fewer Samples: Another optimization we will explore is authenticating users with fewer samples. We can attempt to reduce the number of samples in several ways. First, we can minimize the number of samples for the legitimate user in the training set. It is thus a tricky question to determine how many and which samples should be used. In this project, we will explore only using the "representative" samples – i.e., those that are the most similar to the rest of the user's samples. In this way, the computation/energy consumption in the authentication session can be greatly reduced.

Another optimization technique we can adopt is to dynamically adjust the sampling rate in the test phase. A lower sampling rate leads to fewer data points in a sample, thus shorter collection and processing latencies. In this project, we will explore dynamically adjusting the sampling rate based upon the temperature of the device. Namely, if we notice the device is becoming heated, then we should reduce the sampling rate. In the project, we will carefully quantify the interaction between the device temperate and the sampling rate.

5 Evaluation Plan

5.1 *Headbanger* App on Google Glass and Moto 360

In this proposal, we propose a body-movement pattern based authentication system, *Headbanger* for wearable devices. In addition to developing and evaluating the proposed algorithms, we will also conduct in-depth evaluation of the *Headbanger* system design. Even though there are many types of body movements that we can exploit for authentication purposes, in this project we will focus on the movements that can be easily captured by Google Glass (representing smart glasses) and those by Moto 360 (representing smart watches). Specifically, we will study

Figure 8: We will implement *Headbanger* on (a) Google Glass and (b) Moto 360 smart watch.

the following movement patterns:

- *Movement patterns for smart glasses:* As far as smart glasses are concerned, we will explore head movement patterns (with music), eye blinking/winking patterns (with music), and pulses measured at the temple.
- *Movement patterns for smart watches:* As far as smart watches are concerned, we will explore arm movement patterns (with music), wrist movement patterns (with music), finger movements (with music), and pulses measured at the wrist.

We will choose easy-to-follow and fast-tempo music tracks (10 seconds long) as external stimuli. The readers can download such an audio track at our web site: *http://www.winlab.rutgers.edu/ sugangli/somebody.midi*.

5.2 Data Collection

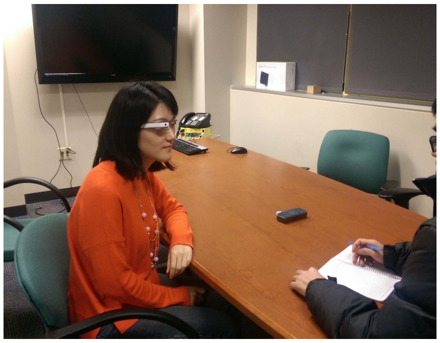


Figure 9: Our team member was collecting data with one of the participants.

The key to the success of this project is to collect data from a large and diverse set of participants, in different environments and contexts. In this three-year project, we plan to collect data from *** subjects. We will make effort to recruit participants such that we have a balanced mix of gender, age, height, and handedness. We plan to pay each subject ***.

In the data collection session, we will inform the participants of the potential risks involved in wearing Google Glass and collecting head-movement or eye blinking/winking/pulse data (e.g., feeling dizzy after head-movement for a period of time, not being able to see clearly if near-sighted, etc.), as well as the potential risks in wearing Moto 360 and collecting hand-movements/pulse data (e.g., wrist pain, ***). If they agree to participate, we will ask each subject to report their age and gender. We will help the subjects to wear the Google Glass and make head movements and eye blinking/winking while listening to the music track of their choice. We will also help the subjects to wear the Moto 360 and make wrist/hand movements while listening to the music track of their choice. Meanwhile, we will record the raw accelerometer data, raw gyroscope data, and the infra-red sensor data from the Google Glass. Each recording session will be 10 seconds long, and we (the graduate students) will sit through each session with the subject to help him/her use the system properly, as shown in Figure 9. After every 5 recording sessions, we will ask the subject to take a break to relax their muscle and regain energy. We will also split each subject's data collection session on different days, to include natural movement variability in the data sets. *Both our system design and our data collection protocol have been approved by our Institutional Review Board.*

5.3 Long Term App Evaluation

6 Work Plan

References

[1] Fitbit. `http://en.wikipedia.org/wiki/Fitbit`.

[2] Google glass. `http://en.wikipedia.org/wiki/Google\_Glass`.

[3] Nymi band. `http://www.nymi.com/`.

[4] Smart watch. `http://en.wikipedia.org/wiki/Smartwatch`.

[5] Heikki Ailisto, Elena Vildjiounaite, Mikko Lindholm, Satu-Marja Makela, and Johannes Peltola. Soft biometrics – combining body weight and fat measurements with fingerprint biometrics. *Pattern Recognition Letters*, 2006.

[6] Ling Bao and Stephen S Intille. Activity recognition from user-annotated acceleration data. In *Pervasive computing*, pages 1–17. Springer, 2004.

[7] Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. Silentsense: silent user identification via touch and movement behavioral biometrics. In *ACM MobiCom*, 2013.

[8] RE Challis and RI Kitney. The design of digital filters for biomedical signal processing part 3: The design of butterworth and chebychev filters. *Journal of biomedical engineering*, 1983.

[9] Robert T Collins, Ralph Gross, and Jianbo Shi. Silhouette-based human identification from body shape and gait. In *IEEE FGR*, 2002.

[10] Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter, and David Kotz. A wearable system that knows who wears it. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 55–67. ACM, 2014.

[11] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *ACM CHI*, 2012.

[12] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*, pages 306–311. IEEE, 2010.

[13] Javier Hernandez, Yin Li, James M Rehg, and Rosalind W Picard. Bioglass: Physiological parameter estimation using a head-mounted wearable device. In *IEEE MobiHealth*, 2014.

[14] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 2004.

[15] Zach Jorgensen and Ting Yu. On mouse dynamics as a behavioral biometric for authentication. In *ASIACCS*, 2011.

[16] Emil Jovanov, Aleksandar Milenkovic, Chris Otto, and Piet C De Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and rehabilitation*, 2(1):6, 2005.

[17] Dean M Karantonis, Michael R Narayanan, Merryn Mathie, Nigel H Lovell, and Branko G Celler. Implementation of a real-time human movement classifier using a triaxial accelerometer for ambulatory monitoring. *Information Technology in Biomedicine, IEEE Transactions on*, 10(1):156–167, 2006.

[18] Qiang Li, John A Stankovic, Mark A Hanson, Adam T Barth, John Lach, and Gang Zhou. Accurate, fast fall detection using gyroscopes and accelerometer-derived posture information. In *Wearable and Implantable Body Sensor Networks, 2009. BSN 2009. Sixth International Workshop on*, pages 138–143. IEEE, 2009.

[19] Steve Mann. Wearable computing: A first step toward personal imaging. *IEEE Computer*, 30(2):25–32, 1997.

[20] Jani Mantyjarvi, Mikko Lindholm, Elena Vildjiounaite, S-M Makela, and HA Ailisto. Identifying users of portable devices from gait pattern with accelerometers. In *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on*, volume 2, pages ii–973. IEEE, 2005.

[21] Ruth E Mayagoitia, Anand V Nene, and Peter H Veltink. Accelerometer and rate gyroscope measurement of kinematics: an inexpensive alternative to optical motion analysis systems. *Journal of biomechanics*, 35(4):537–542, 2002.

[22] Fabian Monrose and Aviel D Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation computer systems*, 2000.

[23] Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 2003.

[24] Fuminori Okumura, Akira Kubota, Yoshinori Hatori, Kenji Matsuo, Masayuki Hashimoto, and Atsushi Koike. A study on biometric authentication based on arm sweep action with acceleration sensor. In *IEEE ISPACS*, 2006.

[25] Luca Palmerini, Laura Rocchi, Sabato Mellone, Franco Valzania, and Lorenzo Chiari. Feature selection for accelerometer-based posture analysis in parkinson's disease. *Information Technology in Biomedicine, IEEE Transactions on*, 15(3):481–490, 2011.

[26] Susanna Pirttikangas, Kaori Fujinami, and Tatsuo Nakajima. Feature selection and activity recognition from wearable sensors. In *Ubiquitous Computing Systems*, pages 516–527. Springer, 2006.

[27] Stephen J Preece, John Yannis Goulermas, Laurence PJ Kenney, and David Howard. A comparison of feature extraction methods for the classification of dynamic activities from accelerometer data. *Biomedical Engineering, IEEE Transactions on*, 56(3):871–879, 2009.

[28] Tauhidur Rahman, Alexander T Adams, Mi Zhang, Erin Cherry, Bobby Zhou, Huaishu Peng, and Tanzeem Choudhury. Bodybeat: a mobile system for sensing non-speech body sounds. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 2–13. ACM, 2014.

[29] Angelo M Sabatini, Chiara Martelloni, Sergio Scapellato, and Filippo Cavallo. Assessment of walking features from foot inertial sensing. *Biomedical Engineering, IEEE Transactions on*, 52(3):486–494, 2005.

[30] Sarah V Stevenage, Mark S Nixon, and Kate Vince. Visual analysis of gait as a cue to identity. *Applied cognitive psychology*, 1999.

[31] R Williamson and BJ Andrews. Detecting absolute human knee angle and angular velocity using accelerometers and rate gyroscopes. *Medical and Biological Engineering and Computing*, 39(3):294–302, 2001.

[32] Roman V Yampolskiy. Motor-skill based biometrics. In *Annual Security Conference*, 2007.

[33] Marcel Zentner and Tuomas Eerola. Rhythmic engagement with music in infancy. *Proceedings of the National Academy of Sciences*, 2010.

[34] Mi Zhang and Alexander A Sawchuk. A feature selection-based framework for human activity recognition using wearable multimodal sensors. In *Proceedings of the 6th International Conference on Body Area Networks*, pages 92–98. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011.

[35] Rong Zhu and Zhaoying Zhou. A real-time articulated human motion tracking using tri-axis inertial/magnetic sensors package. *Neural Systems and Rehabilitation Engineering, IEEE Transactions on*, 12(2):295–302, 2004.