powerful classification algorithms, which will be very hard, if at all possible, to run on wearable devices. For this reason, wearable device authentication usually leverages a second device, which is much more powerful (e.g., smartphone). In this project, we take the viewpoint that authenticating users with two devices is inconvenient, and instead, we would like to implement the entire authentication process on the wearable device. To address this challenge, we propose to carefully choose the features and classifiers, and more importantly, we propose to pipeline the online authentication operations to significantly reduce the latency and power consumption. Finally, we also propose to dynamically adjust the sampling rate based upon the physical context information about the device.

3 Challenge I: Establishing Body Movement Patterns as Reliable Behavioral Biometrics

Even though body movements have been deemed unique by human brains for a long time, the need to capture the signal and quantify its uniqueness using wearable device is highly challenging. In this section, we present our proposed techniques to address this challenge.

3.1 Preliminary Results

We have conducted a preliminary study to find out whether body movements measured by wearable devices can potentially be used for robust authentication. In our preliminary study, we used Google glass to collect accelerometer data (*ACC* in short) when a user moves her head following music beats, and studied whether the measured head movement patterns are distinctive and repeatable. Our preliminary study involves the following data processing aspects:

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 [18] by adopting a relaxed cut-off frequency of 10Hz. In this way, we removed spurious head movements and obtained smooth *ACC* data.
2. *Reference Data Construction:* We constructed the reference data 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). Then we calculated the distances between these samples using the dynamic-time warping (DTW) tool [10][1]. 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. In general, we find that same-user distances are much smaller than cross-user distances.
3. *SVM Classification:* In the online authentication phase, after filtering the raw *ACC* signal, we calculated the DTW distances between the test sample and the true samples, and then feed these distance values and the reference data to the Support Vector Machine (SVM) to obtain classification results.

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 movement patterns. In this set of experiments, we employed the simplest head movement pattern: nodding. In total, we had one glass owner, who designed the nodding

[1]DTW is generally used to measure similarity between temporally varying signals. DTW compares a temporal signal with a reference signal over a certain time-window and calculates the distance between these two signals.

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 in our preliminary study. The results show that even for the simplest nodding, we can correctly authenticate 95% of the users when the samples are longer than 6 seconds.

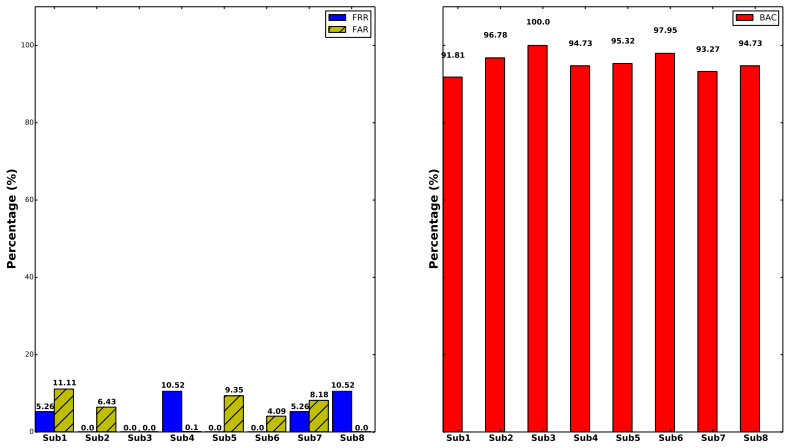

Figure 3: In this set of experiments, we studied whether a user can successfully repeat her own head-movement pattern. We had 8 subjects, each performing her own choice of head-movement patterns. We collected 38 samples for each subject. (a) shows the FRR and FAR results for each subject, and (b) shows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

pattern, and 15 imitators who imitated the pattern. 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 arises with time. We also made a great deal of effort to make sure the imitators accurately copy the owner's movement – the owner carefully explained how he nodded his head to each imitator, and sat through each data collection session for all the 15 imitators to make sure their nodding patterns look the same to the owner's eye. For each imitator, we collected 40 10-second *ACC* samples. By averaging over many different combinations of reference data and test data, we generated the average 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 help 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 pattern if each user is asked to come up with their own movement pattern. 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 simple 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 free-style body movements, we need to eliminate several important roadblocks.

3.2.1 Feature Selection and Information Entropy

Feature selection plays the most important role in determining the accuracy of an authentication system, and we will thus start our discussion from this topic. Most wearable devices have accelerometer (*ACC*) and gyroscope (*GYRO*) sensors, whose readings can be used to characterize a person's body movements. There has been a long history of studying these two types of sensor data to detect/analyze motion, and a large number of features have been discussed [69, 71, 72, 8, 104]. In this project, we will start our investigation