Suhas Bettapalli Nagaraj

EE 597 IoT Review 13

08 November 2020

MoLe: Motion Leaks through Smartwatch Sensors

The main objective of this paper is to find out if it is possible to use a watch based motion sensor to infer input words?

In order to understand all the possibilities, we need to understand how a human types. The authors place a smartphone camera on top of the keyboard and try to understand the range of moments and keystrokes which happen on the keyboard through image processing techniques.

The authors found that there is a strong correlation between words typed and the positions where the hand reaches for typing a particular keystroke but at the same time, there are a few challenges that need to be addressed.

The authors list three design challenges:

1. Noisy sensor data - The authors use keystroke time and z-acceleration to infer keystroke time.

For watch displacement, the authors used an Android linear acceleration to estimate watch displacement.

To take care of this, the authors use MoLe architecture which takes into account both the time and the location for the keystroke detector.

2. Watch location does not imply the keystroke - the authors found that the ground truth location of some of the keystrokes don't imply the same displacement in the X and Y directions on the graph. Some of the points were very close to one another, forming clusters rather than independent points, which made identifying keystrokes hard. Along with this, the data is unlabeled which makes classification tougher. Thus, the authors propose using an unlabeled point cloud which makes us something called point cloud fitting to make sure that the key strokes are identified.

3. Information from the other hand is missing - the data from your right hand keystrokes are missing which makes it tough to identify the words which are being typed. To record this data from the right hand the

authors propose using a Bayesian inference which makes use of a dictionary and from here, computes the likelihood of a word and provides the rank of the word.

To explain the keystroke detector in the MoLe architecture, the autos make use of a 3D smartwatch motion which comprises of an accelerometer and a gyroscope. They use a peak detection method which generates errors. By trying to understand the data more carefully they also understood that the x-axis displacement is also important. To solve this problem the authors use a machine learning approach where they use a low threshold peak detection to generate candidates. They then apply a bagged decision tree to classify keystrokes. Most of the true positive results range from about 89% all the way till 98% for the keystrokes from the left hand. Whenever there is a false positive for the keys, the authors assign it to the right hand and that range from 2.6% to 6.2%.

Now, in order to identify the displacement of the smartwatch, the authors use an Android API which used linear acceleration however after using double integral they were able to remove the mean which made it more significant and reduced noise. MoLe makes use of a gyroscope to estimate and remove gravity with the Kalman filter. The displacement error for the median is less than 1.5 mm but for Android the median error was less than 2.5 mm.

The second module uses point cloud fitting. As mentioned earlier, the authors use Bayesian inference.

Thus, the authors have three observations :- number of keystrokes, location of keystrokes, time interval between keystrokes. These have been taken care of by the methods mentioned above.

For evaluation, the authors make use of a Samsung Galaxy gear live with Android Wear, which has a sampling rate of acceleration and gyroscope values of 200 Hertz. Next, the analysis is done offline using MATLAB.

8 participants were recruited for the study, which included five native speakers and three non-native speakers. A total of 300 words were used for each subject for a total of 2400 words. The words were randomly selected from the 5,000 most frequently used words.From here, to the labeled point clouds for training data were used which consisted of two people collecting offline data with the top 500 longest words.

The evaluation metrics consisted of three main points.

1. How will MoLe guess each word? - The key to improving the accuracy is by improving the key press detection which is possible using MoLe.
2. Observation improvements - by adding keystrokes along with displacement and time, there was a significant improvement in the median rank.
3. Recovery via human observation - Can use Natural Language Processing to guess the words.

In a nutshell,

MoLe : motion leaks through smartwatch sensors. It identifies leaks when using watch motion sensors to infer input words. for a word with a length greater than 6, MoLe can shortlist 10 words on average that includes the word.

However, there were a few points that needed more clarity :

Questions :

1. The proposed method is unable to detect spacekey and works only for single words. How do the authors plan to improve upon this?

2. Since the system is based on English, there was no mention of identifying numerical/special character keystrokes.

3. The authors assume that the person typing is using a standard typing method and map the keystrokes to a particular hand which may not be the case for a person who does not know a standard typing method.

More details about the paper

Wang, H., Lai, T. T. T., & Roy Choudhury, R. (2015, September). Mole: Motion leaks through smartwatch sensors. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (pp. 155-166).