Artif Life Robotics (2018) 23:87–93
https://doi.org/10.1007/s10015-017-0404-z

ORIGINAL ARTICLE

# On applying support vector machines to a user authentication method using surface electromyogram signals

Hisaaki Yamaba[1] · Tokiyoshi Kurogi[1] · Kentaro Aburada[1] · Shin-Ichiro Kubota[2] · Tetsuro Katayama[1] · Mirang Park[3] · Naonobu Okazaki[1]

Received: 10 April 2017 / Accepted: 20 September 2017 / Published online: 1 November 2017

**Abstract** At present, mobile devices such as tablet-type PCs and smart phones have widely penetrated into our daily lives. Therefore, an authentication method that prevents shoulder surfing is needed. We are investigating a new user authentication method for mobile devices that uses surface electromyogram (s-EMG) signals, not screen touching. The s-EMG signals, which are detected over the skin surface, are generated by the electrical activity of muscle fibers during contraction. Muscle movement can be differentiated by analyzing the s-EMG. Taking advantage of the characteristics, we proposed a method that uses a list of gestures as a password in the previous study. In this paper, we introduced support vector machines (SVM) for improvement of the method of identifying gestures. A series of experiments was carried out to evaluate the performance of the SVM based method as a gesture classifier and we also discussed its security.

**Keywords** Mobile device · User authentication · Shoulder surfing · s-EMG · SVM

## 1 Introduction

This paper presents an introduction of support vector machine (SVM) to the user authentication method for mobile devices using surface electromyogram (s-EMG) signals, not screen touching.

At the present time, mobile devices such as tablet type PCs and smartphones have widely penetrated into our daily lives. Consequently, an authentication method that prevents shoulder surfing, which is the direct observation of a users personal information such as passwords, comes to be important.

In general, authentication operations on mobile devices are performed in many public places, so we have to ensure that no one can view our passwords. However, it is easy for people who stand near such a mobile device user to see login operations and obtain the users authentication information.

And additionally, it is not easy to hide mobile devices from attackers during login operations because users have to see the touch screen of their mobile device, which do not have keyboards, to input authentication information. On using a touchscreen, users of a mobile device input their authentication information through simple or multi-touch gestures. These gestures include, for example, designating his/her passcode from displayed numbers, selecting registered pictures or icons from a set of pictures, or tracing a registered one-stroke sketch on the screen. The user has to see the touch screen during his/her login operation; strangers around them also can see the screen.

To prevent this kind of attack, biometrics authentication methods, which use metrics related to human characteristics, are expected. In this study, we investigated application of surface electromyogram (s-EMG) signals for user authentication.

This work was presented in part at the 22nd International Symposium on Artificial Life and Robotics, Beppu, Oita, January 19–21, 2017.

✉ Hisaaki Yamaba
yamaba@cs.miyazaki-u.ac.jp

[1] University of Miyazaki, 1-1, Gakuen Kibanadai-nishi, Miyazaki, Japan

[2] Kumamoto Universiry, 1030, Shimo-ogino, Kumamoto, Japan

[3] Kanagawa Institute of Technology, 1030, Shimo-ogino, Atsugi, Kanagawa, Japan

S-EMG signals, which are detected over the skin surface, are generated by the electrical activity of muscle fibers during contraction. These s-EMGs have been used to control various devices, including artificial limbs and electrical wheelchairs. Muscle movement can be differentiated by analyzing the s-EMG [1]. Feature extraction is carried out through the analysis of the s-EMGs. For example, fast Fourier transform (FFT) can be adopted for the analysis. The extracted features are used to differentiate the muscle movement, including hand gestures.

In the previous researches [2–4], we investigate the prospect of realizing an authentication method using s-EMGs through a series of experiments. First, several gestures of the wrist were introduced, and the s-EMG signals generated for each of the motion patterns were measured [2]. We compared the s-EMG signal patterns generated by each subject with the patterns generated by other subjects. As a result, it was found that the patterns of each individual subject are similar but they differ from those of other subjects. Thus, s-EMGs can confirm ones identification for authenticating passwords on touchscreen devices. Next, a method that uses a list of gestures as a password was proposed [3, 4]. And also, experiments that were carried out to investigate the performance of the method extracting feature values from s-EMG signals (using the Fourier transform) adopted in this research. The results showed that the Fourier transform has certain ability to extract feature values from s-EMG signals, but further accuracy was desired

In this paper, a support vector machine (SVM) was introduced to identify gestures from s-EMG signals. Some feature values were selected and a gesture classifier was trained using measured s-EMG signals. A set of other s-EMG signals that were used as test data was given to the classifier and the false rejection rate and the false acceptance rate of this method were evaluated from the results of the experiments. We also discussed the security evaluation of the proposed method.

## 2 Characteristics of authentication method for mobile devices

It is considered that user authentication of mobile devices has two characteristics [2].

One is that an authentication operation is performed when a user wants to start using their mobile devices. The authentication often takes place around strangers. Therefore, the strangers around the user can possibly see the users unlock actions. Some of these strangers may scheme to steal information for authentication such as passwords.

The other characteristic is that user authentication of mobile devices is almost always performed on a touchscreen. Since many of current mobile devices do not have hardware keyboards, it is not easy to input long character based passwords into such mobile devices. When users want to unlock mobile touchscreen devices, they input passwords or personal identification numbers (PINs) by tapping numbers or characters displayed on the touchscreen. Naturally, users have to look at their touchscreens while unlocking their devices, strangers around them also can easily see the unlock actions. Besides, the user moves only one finger in many cases. So, it becomes very easy for thieves to steal passwords or PINs.

To prevent shoulder-surfing attacks, many studies have been conducted. The secret tap method [5] introduces a shift value to avoid revealing pass-icons. The user may tap other icons in the shift position on the touchscreen, as indicated by a shift value, to unlock the device. By keeping the shift value secret, people around the user cannot know the pass-icons, although they can still watch the tapping operation. The rhythm authentication method [6] relieves the user from looking at the touchscreen when unlocking the device. In this method, the user taps the rhythm of his or her favorite music on the touchscreen. The pattern of tapping is used as the password. In this situation, the users can unlock their devices while keeping them in their pockets or bags, and the people around them cannot see the tap operations that contain the authentication information.

## 3 Surface electromyogram signals

The s-EMG signals (Fig. 1) are generated by the electrical activity of muscle fibers during contraction and are detected over the skin surface (Fig. 2) [2]. Muscle movement can be differentiated by analyzing the s-EMG.

However, since measured s-EMG signals vary by subject, the extracted features do not show enough performance to correctly differentiate the muscle movement in multiple subjects. Therefore, researchers have explored other methods to improve the performance of feature extraction. Since some methods demonstrate good performance for some subjects but other methods show better performance for other

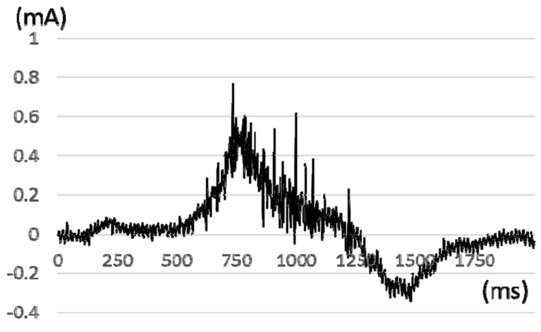


**Fig. 1** A sample of an s-EMG signal

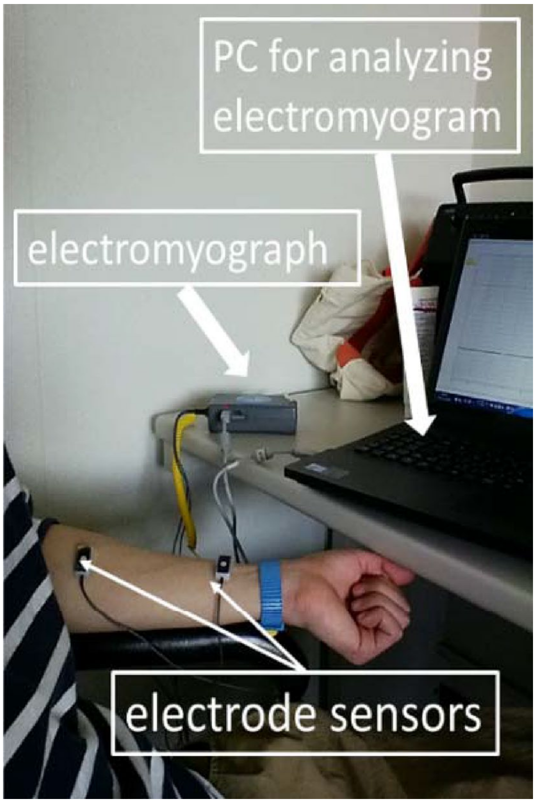


**Fig. 2** Measuring an s-EMG signal

subjects, a feature that can be used to distinguish gestures for everyone is desired. For example, a method that uses the maximum value and the minimum value of raw s-EMG signals was proposed [7].

## 4 Proposed method

### 4.1 User authentication system using s-EMG

In the previous research, the method of user authentication using s-EMGs, which do not require looking at a touchscreen, was proposed [3, 4]. Figure 3 shows the sketch of the authentication system using s-EMG signals. First, wearable devices such as a smart watch measures s-EMG signals and send the signals to mobile devices such as smartphones using Bluetooth. Next, the feature values of the measured raw signals are extracted. Then, the mobile device estimates gestures made by a user of a mobile device from the extracted features. Small devices such as *Myo*$^{TM}$ [8] and Deus Ex Aria [9] are now available to measure s-EMG signals and communicate with other devices using wireless Bluetooth. *Myo*$^{TM}$ is a gesture control armband, which can control PCs without touching its screen (Fig. 4). Deus ex Aria is a clip type device that is attached to a wristband of a watch (Fig. 5). It is expected that the authentication system using s-EMG will be realized using such kind of devices.

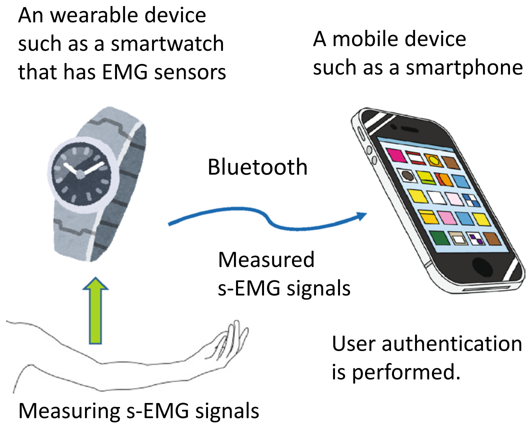

An wearable device such as a smartwatch that has EMG sensors
A mobile device such as a smartphone
Bluetooth
Measured s-EMG signals
User authentication is performed.
Measuring s-EMG signals

**Fig. 3** A sketch of user authentication using s-EMG

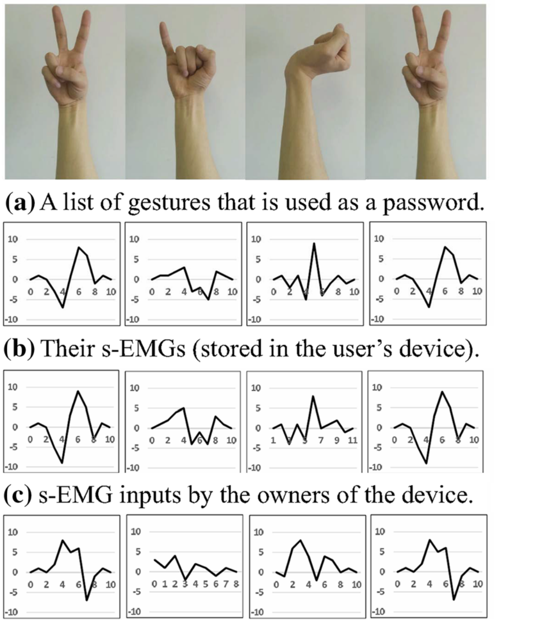
**Fig. 4** *Myo*$^{TM}$: Gesture control armband (quoted from http://store.myo.com/)

**Fig. 5** Deus ex Aria: clip type gesture controller (quoted from http://www.techtimes.com/articles/62999/20150623/control-android-wear-smartwatches-finger-gestures-using-deus-ex-aria.htm)

### 4.2 User authentication method using s-EMG

In this study, combinations of the gestures are converted into a code for authentication. These combinations are inputted into the mobile device and used as a password for user authentication.

1. At first, pass-gesture registration is carried out. A user selects a list of gestures that is used as a pass-gesture (Fig. 6a).



**(a)** A list of gestures that is used as a password.

**(b)** Their s-EMGs (stored in the user's device).

**(c)** s-EMG inputs by the owners of the device.

**(d)** s-EMG inputs by someone who stole the device.

**Fig. 6** A list of gestures used as a password

2. The user measures s-EMG of each gesture, extracts their feature values, and register the values into his mobile device (Fig. 6b).
3. When the user tries to unlock the mobile device, the user makes his pass-gesture and measures the s-EMG.
4. The measured signals are sent to his mobile device.
5. The device analyzes the signals and extracts the feature values.
6. The values are compared with the registered values.
7. If they match, the user authentication will succeed (Fig. 6c).
8. On the other hand, an illegal user authentication will fail because a list of signals given by someone who stole the device (Fig. 6d) will not be similar with the registered one.

Adopting s-EMG signals for authentication of mobile devices has three advantages. First, the user does not have to look at his/her device. Since the user can make a gesture that is used as a password on a device inside a pocket or in a bag, it is expected that the authentication information can be concealed. No one can see what gesture is made. Next, it is expected that if another person reproduces a sequence of gestures that a user has made, the authentication will not be successful, because the extracted features from the s-EMG signals are usually not the same between two people. And then, a user can change the list of gestures in our method using an s-EMG signal. This is the advantages of our method against other biometrics based methods such as fingerprints, an iris, and so on. When authentication information, a fingerprint or an iris, come out, the user cannot use them because he/she cannot change his/her fingerprint or iris. But the user can arrange his/her gesture list again and use the new gesture list.

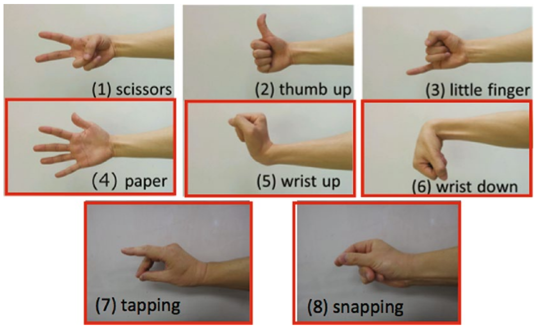


**Fig. 7** Gestures used in the experiments

### 4.3 Introduction of support vector machines

Support vector machines are one of the pattern recognition models of supervised learning. Linear SVM was proposed in 1963, and extended to non-linear classification in 1992. A support vector machine builds a classifier for sample data that belong to one of two classes. An SVM trains the separation plane that has the largest margin, and samples on the margin are called support vectors. An SVM is one of the recognition method that has the highest performance.

In this research, the programming language "R" was adopted. SVM function of the programming language R can classify data into several categories. One SVM is prepared for one user and trained by data of the user. This SVM selects one gesture for given s-EMG signals. It is expected that the trained SVM of a user can select the correct gesture from the s-EMG signals generated by this gesture. At the same time, from the s-EMG signals generated by an attacker's gesture, it is expected that this will select another gesture, not the input gesture. We used the pair of the maximum value and the minimum value of raw s-EMG signals as the feature value that was proposed in [7].

However, there may be some problems. Because of some measurement error, an incorrect gesture may be selected (false rejection). And if s-EMG signals of an attacker's gesture is similar with the true user's signal, authentication will succeed by accident (false acceptance). Additionally, user authentication may succeed by random input if a signal pattern generated by this gesture similar with this pattern. We investigated the problems in the next section.

**Table 1** The false rejection rates

| Subject | A | B | C | D |
|---|---|---|---|---|
| FR rate | 0.402 | 0.504 | 0.464 | 0.156 |
| Subject | E | F | G | H |
| FR rate | 0.272 | 0.289 | 0.416 | 0.392 |

**Table 2** The false acceptance rates

| Subject | A | B | C | D |
|---|---|---|---|---|
| FR rate | 0.262 | 0.217 | 0.249 | 0.197 |
| Subject | E | F | G | H |
| FR rate | 0.227 | 0.267 | 0.264 | 0.271 |

**Table 3** Gestures of E were given to SVM of F (good)

| | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|
| (4) | 6 | 0 | 0 | 1 | 0 |
| (5) | 0 | 1 | 49 | 0 | 13 |
| (6) | 44 | 36 | 1 | 41 | 36 |
| (7) | 0 | 0 | 0 | 1 | 0 |
| (8) | 0 | 13 | 0 | 7 | 1 |

## 5 Experiments

### 5.1 Objectives

We carried out a series of experiment to investigate next three issues.

1. False rejection rate of the method Can a SVM of each user predict a correct gesture from s-EMG signals?
2. False acceptance rate of the method Can a SVM of each user reject s-EMG signals of the same gesture generated by another person?
3. Resistance against an accidental success Is the probability that random s-EMG inputs succeed low enough?

### 5.2 Conditions

It is assumed that an attacker does not know which his gesture generates s-EMG signals that is similar with a specific gesture of a victim user.

Eight students of University of Miyazaki participated as experimental subjects (Subject A–H). And the eight hand gestures shown in Fig. 7 were introduced. But the five red bordered gestures were selected in the experiments because their s-EMG signals were clearer than other gestures.

DL-3100 (S&M Inc.) that was an electromyograph used in the previous researches also used to measure the s-EMG of each movement pattern in this study. The measured data were stored and analyzed on a PC. Two healthy persons whose ages were in the twenties (students of University of Miyazaki) participated as experimental subjects. The subjects repeated each gesture five times and their s-EMG signals were recorded. This measurement was carried out 10 times and 50 signals were obtained for each subject and for each gesture.

### 5.3 Results

First, false rejection rates were investigated. Signals of gestures of a subject are given to a SVM trained for the subject. And we counted the number of signals that were classified into other gestures. tenfold cross validation was carried out in this experiment. We measured 50 s-EMG signals for each gesture. They were divided into ten segments. Nine segments from each of five gestures were used as training data, and rest was used as test data. Table 1 shows the false rejection rates of the eight subjects. The results of this experiment were not so good.

Next, the false acceptance rate was investigated. Signals of gestures of a subject are given to a SVM trained for another subject. And we counted the number of signals that were classified into each gesture. Table 2 shows the false

**Table 4** Gestures of G were given to SVM of F (not good)

| | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|
| (4) | 31 | 7 | 35 | 21 | 37 |
| (5) | 0 | 2 | 0 | 1 | 0 |
| (6) | 16 | 36 | 0 | 24 | 0 |
| (7) | 0 | 0 | 0 | 1 | 8 |
| (8) | 3 | 5 | 15 | 3 | 5 |

**Table 5** The worst false acceptance rate (G → A)

| | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|
| (4) | **0.38** | 0.10 | 0.30 | 0.34 | 0.36 |
| (5) | 0.00 | **0.84** | 0.00 | 0.00 | 0.00 |
| (6) | 0.34 | 0.36 | **0.12** | 0.02 | 0.00 |
| (7) | 0.08 | 0.00 | 0.00 | **0.48** | 0.32 |
| (8) | 0.20 | 0.00 | 0.24 | 0.16 | **0.12** |

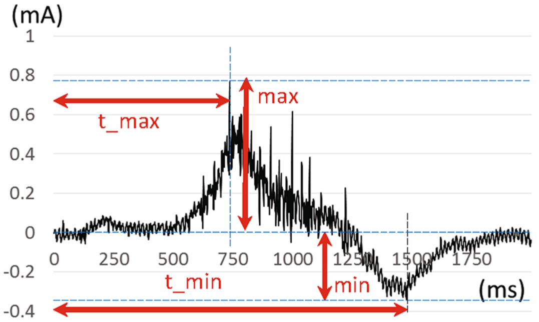


**Fig. 8** Four feature values used in the additional experiment

acceptance rates. These results are a little larger than the rate of random selection (0.200). The false acceptance rates vary according to the subject. Table 3 shows the numbers of s-EMG data of Subject E classified by the SMV of Subject F. This is a good example. False acceptance rates are low for all gesture. Table 4 shows a bad example. S-EMG data of subject G were given to the SVM of F. False acceptance rate of gesture (4) was high. And a gesture with high false acceptance rate is different according to the subject.

Finally, security evaluation was carried out for false acceptance rate and resistance against an accidental success. The false acceptance rate of the worst case is 0.0022 (the product of the bold numbers in Table 5) and the resistance against an accidental success was 0.00032 ( $= (1/5)^5$) under the conditions:

- it is assumed that an attacker knows the pass-gesture,
- the number of gestures in a pass-gesture is 5,
- all gestures are included in a pass-gesture to exploit the characteristic that the false acceptance rate of some gesture is lower.

These are larger than the security level of four-digit PIN (0.0001). This means that introduction of other gestures, longer pass-gesture, or improvement of accuracy of gesture identification.

### 5.4 Improvement of feature values

To improve the performance of this method, we newly added other feature values: *t*_max (the time of the max value) and *t*_min (the time of the min value) (Fig. 8). A SVM of each subject were trained under these four feature values (max, min, *t*_max, *t*_min) and tenfold cross validation was carried out using the same raw data and under the same conditions with 5.2. The results are shown in Tables 5 and 6. It was found that the FARs were not so improved but the FRRs were much improved (Table 7).

### 5.5 Discussion

The results of the experiments show the results of the false rejection rates were worse than those of false acceptance rates. But from the view point of security, false acceptance is more important than false rejection. The weakness about false rejection can be resolved by re-input of the pass-gesture. As for the performance of the proposed method, the additional experiment showed that selection of appropriate

**Table 6** The false rejection rates (four feature values)

| Subject | A | B | C | D |
|---|---|---|---|---|
| FR rate | 0.288 | 0.348 | 0.436 | 0.164 |
| Subject | E | F | G | H |
| FR rate | 0.236 | 0.172 | 0.252 | 0.320 |

**Table 7** The false acceptance rates (four feature values)

| Subject | A | B | C | D |
|---|---|---|---|---|
| FR rate | 0.287 | 0.201 | 0.212 | 0.163 |
| Subject | E | F | G | H |
| FR rate | 0.225 | 0.289 | 0.213 | 0.263 |

feature values is very effective to improve the false acceptance rate. It is expected that the user authentication using s-EMG can be realized by the approach used in this study. And also, it is a need to explore other gesture candidate that are more suitable to distinguish s-EMG signals, appropriate length of pass-gestures, parameter tuning in the learning of SVM.

## 6 Conclusion

We investigated a new user authentication method that can prevent shoulder-surfing attacks in mobile devices. To realize such an authentication method, we adopted an SVM to identify gestures by s-EMG signals. A series of experiments was carried out to investigate the performance of SVM. False rejection rates, false acceptance rates, and resistance against an accidental access were also investigated. The results showed that this approach involves a problem to be resolved, but the method using SVM is promising. We are planning to introduce further effective feature values, introduce other gesture candidate, explore appropriate length of pass-gesture, and so on.

**Acknowledgements** This work was partially supported by JSPS KAKENHI Grant number JP17K00186.

## References

1. Tamura H, Okumura D, Tanno K (2007) A study on motion recognition without FFT from surface-EMG (In Japanese). IEICE Part D J90–D(9):2652–2655
2. Yamaba H, Nagatomo S, Aburada K et al (2015) An authentication method for mobile devices that is independent of tap-operation on a touchscreen. J Robot Netw Artif Lifed 1:60–63
3. Yamaba, H, Kurogi, T, Kubota, S, et al (2016) An attempt to use a gesture control armband for a user authentication system using surface electromyograms. In: Proceedings of 19th international symposium on artificial life and robotics, pp 342–245
4. Yamaba H, Kurogi T, Kubota S et al (2017) Evaluation of feature values of surface electromyograms for user authentication on mobile devices. Artif Life Robot 22:108–112
5. Kita Y, Okazaki N, Nishimura H et al (2014) Implementation and evaluation of shoulder-surfing attack resistant users (in Japanese). IEICE Part D J97–D(12):1770–1784
6. Kita Y, Kamizato K, Park M et al (2014) A study of rhythm authentication and its accuracy using the self-organizing maps (in Japanese). Proc DICOMO 2014:1011–1018
7. Tamura H, Goto T, Okumura D et al (2009) A study on the s-EMG pattern recognition using neural network. IJICIC 5(12):4877–4884
8. http://www.myo.com. Accessed 30 Aug 2017
9. https://www.kickstarter.com/projects/belfio/deus-ex-aria-the-evolution-of-smartwatch-control. Accessed 30 Aug 2017