Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 8793025, 14 pages
http://dx.doi.org/10.1155/2016/8793025

Research Article

Privacy Leakage in Mobile Sensing: Your Unlock Passwords Can Be Leaked through Wireless Hotspot Functionality

Jie Zhang,[1] Xiaolong Zheng,[2] Zhanyong Tang,[1] Tianzhang Xing,[1] Xiaojiang Chen,[1] Dingyi Fang,[1] Rong Li,[1] Xiaoqing Gong,[1] and Feng Chen[1]

[1] *School of Information Science and Technology, Northwest University, Xi'an 710127, China*
[2] *School of Software and TNLIST, Tsinghua University, Beijing 100084, China*

Correspondence should be addressed to Zhanyong Tang; zytang@nwu.edu.cn

Received 11 December 2015; Accepted 6 March 2016

Academic Editor: Tingting Chen

Mobile sensing has become a new style of applications and most of the smart devices are equipped with varieties of sensors or functionalities to enhance sensing capabilities. Current sensing systems concentrate on how to enhance sensing capabilities; however, the sensors or functionalities may lead to the leakage of users' privacy. In this paper, we present WiPass, a way to leverage the wireless hotspot functionality on the smart devices to snoop the unlock passwords/patterns without the support of additional hardware. The attacker can "see" your unlock passwords/patterns even one meter away. WiPass leverages the impacts of finger motions on the wireless signals during the unlocking period to analyze the passwords/patterns. To practically implement WiPass, we are facing the difficult feature extraction and complex unlock passwords matching, making the analysis of the finger motions challenging. To conquer the challenges, we use DCASW to extract feature and hierarchical DTW to do unlock passwords matching. Besides, the combination of amplitude and phase information is used to accurately recognize the passwords/patterns. We implement a prototype of WiPass and evaluate its performance under various environments. The experimental results show that WiPass achieves the detection accuracy of 85.6% and 74.7% for passwords/patterns detection in LOS and in NLOS scenarios, respectively.

1. Introduction

With the boom of mobile smart devices, mobile sensing on smart devices has become a new style of applications and more and more people rely on the smart devices since the rich functionalities and enhanced computing power conveniently provide intelligent service for peoples' daily lives. Most of the smart devices are equipped with a variety of sensors and kinds of functionalities to enhance sensing capabilities, such as detecting the vehicle steering maneuvers using gyroscope and accelerometer [1]. However, current researches have paid much attention on how to process the sensing data 4Vs (Volume, Velocity, Variety, Veracity) to enhance sensing capabilities; the security of mobile smart devices themselves has not received much attention. The sensors or functionalities on the smart devices may leak the users' privacy, since the smart devices are carrying much sensitive personal information, such as personal photos, credit card numbers, and passwords. Once the smart devices are attacked, the sensitive personal information is prone to leak, bringing the privacy leakage and even financial loss.

Previous studies have shown that the accelerometer and gyroscope can track users [2], and the accelerometers on the devices can recognize the unlock passwords of touch-enabled screen devices [3]. However, previous sensor attacks against unlock passwords [3–5] just aim at digital unlock passwords and successfully decode the digital unlock passwords; for graphical unlock passwords, as shown in Figure 1, it has not been mentioned. Besides, it is known that the sensors on the smart devices may lead to the leakage of users' privacy; however, can the functionalities of the smart devices leak the users' privacy?

In this paper, we present WiPass, a snooping method that does not require attacker close to the target or have control of the device. Only the wireless hotspot functionality is used in WiPass to recognize the graphical unlock passwords. WiPass

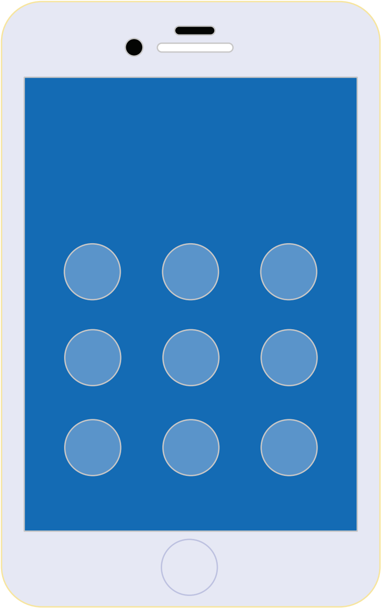


Figure 1: Graphical unlock passwords in the screen of current smart mobile devices.

can "see" your passwords/patterns through the impacts of finger motions on wireless signals even in NLOS (Nonline of Sight) scenarios.

Many existing works have already demonstrated the feasibility of leveraging the impacts of body motions on wireless signals to do localization [6], gesture recognition [7, 8], and even keystroke detection [9, 10]. However, most of existing methods are not suitable to recognize the unlock passwords/patterns. Most existing recognition methods are used in control systems. The user in a control system tends to comply and performs predefined gestures near the devices. However, in WiPass, the attacker cannot access the target devices. The impacts of finger motions on wireless signals from the devices not close to the target are not easy to extract since the impacts are easily overwhelmed by the significant noise.

The differences between attack and control systems bring new challenges. First, it is nontrivial to extract the influenced signal traces among the sampled sequence with intrinsic noise. Second, recognizing the finger motions under the serious noisy environment is challenging. Existing methods usually leverage the amplitude information which is suspected to be corrupted under the noisy environments, decreasing the detection accuracy significantly. Third, the similarity of many unlock patterns significantly increases the difficulty of accurate recognition.

To cope with those challenges, WiPass constructs *finger motion profiles* for the influenced signal traces of different unlock passwords. First, a common method to extract the influenced signal traces is a sliding window. However, in general, a threshold is needed for a sliding window and the threshold is obtained through abundant experiments; it will be time-consuming. Besides, there are lots of different unlock passwords, different unlock passwords correspond to different influenced signal traces, and different influenced signal traces correspond to different amplitude information of wireless signals; thus, different thresholds need to be set for different unlock passwords. Thus, a new efficient method needs to be considered to extract the influenced signal traces. In this paper, DCASW (the difference of cumulative amplitude of the sliding window) is used to extract the influenced signal traces and the max value of the difference can be seen as the beginning of the unlock passwords (where the user starts to unlock the device).

Inspired by time-series data matching method, a well-established technique—Dynamic Time Warping (DTW)—is used to recognize the unlock passwords. However, there are lots of unlock passwords; the matching will be time-consuming and cost large computational overhead; thus, a hierarchical approach is used to reduce time and computational overhead. Given that there are many similar graphical unlock passwords and amplitude information is suspected to be corrupted, phase information can be used with amplitude information together to recognize the unlock passwords and improve the recognition accuracy.

We implement a prototype of WiPass on commercial wireless devices and evaluate its performance under various environments. The experimental results show that, for those unlock passwords with great difference, the recognition accuracy can achieve 70% when using amplitude only. But for those similar unlock passwords, the recognition accuracy can only achieve 37%. The results also show that combining the amplitude information and phase information together can effectively improve the recognition accuracy of similar unlock passwords to 58%. Besides, in LOS scenario, the recognition accuracy of 25 tested graphical unlock passwords can achieve 85.6% within three attempts and 74.7% in NLOS scenario.

Contributions. This paper makes the following contributions:

(i) WiPass is an unlock passwords recognition system, in which a mobile smart phone with wireless hotspot functionality is used as a transmitter to transmit wireless signals, and it exposes a serious threat for mobile device users.

(ii) WiPass exploits the impacts of finger motions on wireless signals to achieve unlock passwords recognition. As a result, the design delivers 74.7% accuracy even in NLOS scenario.

(iii) WiPass uses DCASW to extract the influenced traces and the basic idea can be extended to other systems when different thresholds are needed according to different conditions.

(iv) WiPass also demonstrates the capability of dynamic time warping to recognize the unlock passwords, and a hierarchical approach is used to reduce the time and computational overhead.

The rest of this paper is organized as follows. Section 2 presents the related work about attack against unlock passwords/patterns. Section 3 introduces the overview of the system, followed by designs in Section 4. Hierarchical approach for unlock passwords recognition is presented in Section 5. Implementation and microbenchmark are introduced in Section 6 and evaluation of the recognition accuracy is presented in Section 7. Section 8 discusses the defense strategies; Section 9 introduces discussions and limitations. Then conclusion is introduced in Section 10.

2. Related Work

Currently, attackers try to attack the unlock passwords to obtain the users' privacy, and there are four main ways that the attackers usually use.

(1) Shoulder Surfing Attack. Mobile devices are often used in public places where shoulder surfing attacks [11, 12] often happen and the unlock passwords are easy to be obtained. It is the most simple way to snoop the unlock passwords and does not need any support of additional hardware. However, shoulder surfing attack only can be done when the attacker and the user are very close and the attacker looks unsuspected. If the users are careful enough during unlocking period, the shoulder surfing attack will not succeed.

(2) Finger Print Attack [13]/Smudge Attack [14]. In fingerprint attack, fingerprint powder is needed to dust the touch screen to reveal fingerprints left from tapping fingers and then the fingerprints are sharpened to obtain the unlock passwords [13]. In smudge attack, the attack is done under a variety of lighting and camera conditions [14]. So, fingerprint attack/smudge attack needs the support of additional hardware (e.g., fingerprint powder/camera). Zhang et al. [13] also suggest that a randomized software keyboard is a feasible solution to prevent the unlock passwords from being obtained.

(3) Video Attack. Shukia et al. [15] introduce one kind of side-channel attacks, and the attack can successfully decode the passwords after several attempts. However, cameras are needed to obtain a video and the success rate is related to the camera configurations. Yue et al. [16] present another side-channel attack, in which webcam or a phone camera is needed instead of a camera. They also design randomized virtual keyboards to defeat the attacks.

(4) Sensors Attack. Sensors are exploited to infer touched keys of touch-enabled screen devices, including orientation sensor, accelerometer, and motion sensors [3–5]. They also point out that the defense strategy is to force every application to declare their intention when accessing the sensors and then inform users about dangerous combinations of permissions.

However, some of the defense strategies mentioned above do not protect the devices completely. For example, the randomized virtual keyboards mentioned above are only put forward to defeat the attacks against digital unlock passwords, and it cannot defeat the attacks against graphical unlock passwords. Besides, most touch-enabled devices such as smart phones have not implemented that functionality. For the defense strategy that aims at sensors attack, it has not been achieved in current touch-enabled screen devices because of the friendly interactive interfaces and many other reasons.

The attack against unlock passwords using wireless signals is always neglected by people, and the attack is similar to gesture recognition system based on wireless signals. However, the attack is different from gesture recognition system, because gesture recognition system [7, 17] can only detect more notable motions because of the limited frequency of the wireless transmission, and those tiny motions cannot be detected. Besides, previous gesture recognition studies used machine learning to recognize the gesture because of the few number of gestures in the control system. However, for unlock passwords, there are a large number of unlock passwords and the influenced signal traces are also different when different people unlock the same kind of devices with the same unlock passwords. Given that, learning-based approach is not appropriate for unlock passwords recognition. This paper introduces an attack against unlock passwords using wireless signals, which is immune to those defense strategies. The attacker can turn on the wireless hotspot functionality of their smart devices and the smart device with hotspot functionality can be used as a transmitter; once the signal reflections from the users' finger motions during the unlocking period are collected by an attacker, the users' unlock passwords will be leaked.

3. System Overview

WiPass is an unlock passwords recognition system that enables mobile smart devices with wireless hotspot functionality to "see" the unlock passwords if the influenced signal traces from finger motions during unlocking period are collected by attackers.

Following a common practice in gesture recognition system, WiPass leverages a wireless transmitter to transmit wireless signals. The difference of WiPass and gesture recognition system is that the transmitter of WiPass is a smart mobile device with wireless hotspot functionality instead of a wireless router. In WiPass, one antenna is enough for receiver to capture signal reflections, and current mobile devices with two omnidirectional antennas can be used as the receiver. Figure 2 illustrates the framework of WiPass. It consists of a transmitter and a receiver. The transmitter transmits wireless signals and the receiver extracts signal reflections from finger motions.

To recognize an unlock password, at a high level WiPass goes through the following steps:

(i) WiPass collects the signal reflection information when there exists an unlock password.

(ii) WiPass removes the noise from the collected signal reflection information using Symlet filter, and the details are introduced in Section 4.2.

(iii) WiPass extracts the influenced signal traces from the noise-removal signal reflection information using DCASW, and the details are introduced in Section 4.3.

(iv) By comparing and matching the desired unlock password's *finger motion profile* with the reference

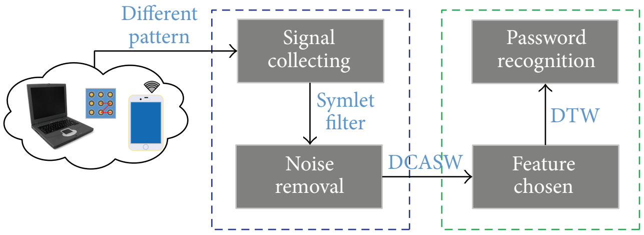


Figure 2: The overview of WiPass.

unlock passwords' *finger motion profiles*, as described in Section 4.5, WiPass identifies the desired unlock password.

In unlock passwords recognition, there are a large number of reference unlock passwords. It is difficult and time-consuming to do unlock passwords matching using DTW, as described in Section 4.5. In Section 5, we describe a hierarchical approach to recognize the desired unlock password.

The next few sections elaborate on the above steps, providing the technical details.

4. Designs

4.1. Signal Collecting. In experiments, the data starts to be collected before the user starts to unlock the device and ends being collected after the user ends unlocking the device. The purpose of such collection is that we need to make sure that the collected data contains the influenced signal traces during the unlocking period. What we have collected is a sequence of CSI data and each CSI represents the phases and amplitudes on a group of 30 OFDM subcarriers.

4.2. Noise Removal. After obtaining the signal, noise needs to be removed from obtained signal, because when the signal is collected, it is unavoidable that the noise in the environment is also collected. For example, additive white Gaussian noise is common in the environment, and the collected signal always contains such noise. In this paper, discrete wavelet decomposition is used to remove noise from obtained signals [18]. Using wavelet decomposition has the following twofold advantages:

(1) It facilitates signal analysis on both time and frequency domain. This attribute can be leveraged in WiPass for analysing the finger motions in varied frequency domains. It can also help WiPass locate the start time for finger motions when one unlock password happens.

(2) It achieves fine-grained multiscale analysis. In WiPass, the finger motions share a lot in common when the unlock passwords of touch-enabled screen devices are similar, such as the "Z" in the top left corner and the "Z" in the bottom right corner, and it makes them difficult to be distinguished. By applying discrete wavelet packet transform to the original signals y_i that contains noise, the tiny differences can be figured out among the similar unlock passwords.

The steps of noise removal using discrete wavelet decomposition are usually as follows.

4.2.1. Forward Wavelet Transform. Generally, a discrete signal $f[n]$ is approximated by the following equation [18]:

$$\begin{aligned} f[n] &= \frac{1}{\sqrt{M}} \sum_k W_\phi[j_0, k]\, \phi_{j_0,k}[n] \\ &\quad + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} \sum_k W_\psi[j,k]\, \psi_{j,k}[n], \end{aligned} \tag{1}$$

where $f[n]$ represents the original discrete signals, and it is defined in $[0, M-1]$ while there are totally M points. $\phi_{j_0,k}[n]$ and $\psi_{j,k}[n]$ are both discrete functions, which are defined in $[0, M-1]$, and they are called wavelet basis. In general, the basis sets $\phi_{j_0,k}[n]_{k\in Z}$ and $\psi_{j,k}[n]_{(j,k)\in Z^2, j\geq j_0}$ are chosen to be orthogonal to each other in order to obtain the wavelet coefficients conveniently in the decomposition process.

During the decomposition process, first the original signals are divided into approximation coefficients (i.e., $W_\phi[j_0,k]$) and detail coefficients (i.e., $W_\psi[j,k]$). Then the approximation coefficients and detail coefficients are both iteratively divided into approximation coefficients and detail coefficients, just as the strategy in the division. The division is an iterative step and the times of iteration depend on the level of decomposition, as shown in Figure 3. The approximation coefficients $W_\phi[j_0,k]$ and detail coefficients $W_\psi[j,k]$ in each level can be computed as the following equations when $j \geq j_0$:

$$\begin{aligned} W_\phi[j_0,k] &= \frac{1}{\sqrt{M}} \sum_n f[n]\, \phi_{j_0,k}[n], \\ W_\psi[j,k] &= \frac{1}{\sqrt{M}} \sum_n f[n]\, \psi_{j,k}[n]. \end{aligned} \tag{2}$$

Given the distortion of signals, we apply a two-level decomposition in this paper.

4.2.2. Threshold Quantification. The threshold plays a very important role in denosing process. A small threshold value will still retain the noisy coefficients while a large threshold value will lose the coefficients that may contain the useful information of the influenced signals. There are two types of threshold, and they are separately soft threshold and hard threshold. For hard threshold, set the smaller coefficients to zero while keeping the larger coefficients. For soft threshold, set the smaller coefficients to zero while shrinking the large coefficients towards zero. Based on that and the effectiveness and simplicity of soft threshold and its frequency of use in literature [19, 20], soft threshold is used in this paper.

4.2.3. Inverse Wavelet Transform. Through the above two steps, the original signals experience n-level decomposition, and the numbers of approximation coefficients and detail coefficients are both 2^{n-1}, so the next step is using the coefficients to reconstruct the signal to achieve noise removal.

However, the reconstruction efficiency relies on the selection of wavelet basis. There are 15 kinds of wavelet basis that

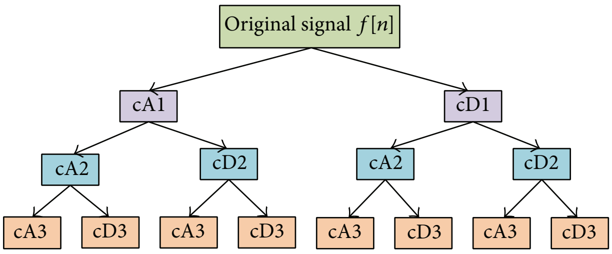


FIGURE 3: An example of 3-level discrete wavelet packet decomposition, where in the figure cA and cD separately represent the approximation coefficients and detail coefficients.

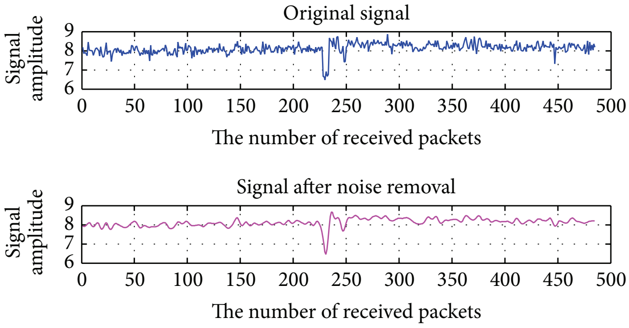


FIGURE 4: The comparison between original signals and signals after noise removal.

Matlab can support and the most commonly used are the three following families: Daubechies, Coiflets, and Symlets [20]. An ideal wavelet basis should contain the following features: orthogonality, short support, symmetry, smoothness, and high order of vanishing matrix [21]. However, Symlet is an improvement of Daubechies, and the symmetry of Coiflets is higher than that of Daubechies. So Symlets or Coiflets can be used to achieve noise removal, but which kind of wavelet basis is better? Actually, after the wavelet transform, what we have obtained are the coefficients and the coefficients reflect the main information of original signal, so when the signal that is reconstructed by coefficients is more similar to the original signal, the reconstructed signals will not lose useful information of the original signal. Compared with Symlets and Coiflets, the constructed signal of Symlets is more similar to the original signal; besides Wang et al. [18] and Chavan et al. [22] also use Symlets to achieve noise removal. Thus, in this paper, a two-level Symlets wavelet filter is applied to remove noise and the signal after noise removal is as shown in Figure 4.

4.3. Feature Extraction. Feature extraction is important for *finger motion profile* construction. In this paper, we define the influenced signal traces as *features*, and thus the *features* just reflect the unlock passwords. If the extracted *features* are too little, the extracted *features* will not fully reflect the unlock passwords, and if the extracted *features* are too many, redundant information about the signal will be stored and that will lead to a waste of the space and large computational overhead. So how can we automatically extract the *features* and the extracted *features* just reflect the unlock passwords?

Inspired by the sliding window *feature extraction* [23], the cumulative amplitude of the sliding window can be used to extract the *features*. However, for the cumulative amplitude of the sliding window, the *features* are usually extracted according to thresholds and the thresholds are generally obtained after many attempts in actual experiments, the process is time-consuming. Besides, there are many unlock passwords for touch-enabled screen devices and the impacts of finger motions on wireless signals for different unlock passwords are different; thus, for different unlock passwords, different thresholds need to be set to extract *features*. Thus, a new efficient method to extract *features* is needed to be considered.

In this paper, difference of the cumulative amplitude of the sliding window (DCASW) is used to extract the feature. DCASW needs no threshold; thus, it reduces the time overhead. The accumulated amplitude of the sliding window can be calculated by the following equation:

$$F_i = \left|\mathrm{Sum}_i - \mathrm{Sum}_{i-\tau}\right|, \tag{3}$$

where τ is the size of the sliding window and Sum_i is the cumulative amplitude of the sliding window, which can be computed as follows:

$$\begin{aligned} \mathrm{Sum}_i &= \mathrm{Sum}_{i-1} + A_i; \\ \mathrm{Sum}_0 &= 0, \\ \mathrm{Sum}_1 &= A_1, \end{aligned} \tag{4}$$

where A_i represents the amplitude of ith received packets. Then the difference of cumulative amplitude of the sliding window is computed to extract the *feature*, and the computation is as follows:

$$D_i = F_i - F_{i-1}. \tag{5}$$

The max value of the difference can be seen as the beginning of the unlock passwords (where the user starts to unlock the device). That is because when the unlock password begins, the signals begin to fluctuate while the signals keep stable when there is no unlock password, as shown in Figure 4. So the max value of the difference can be thought to be the beginning of the unlock passwords. When the unlock passwords end, the signal will return to keep stable, and the min value of the difference that occurs after the max value can be thought to be the ending of the unlock passwords. The result of the feature extraction using DCASW is shown in Figure 5.

4.4. Finger Motion Profile Construction. After removing the noise from the collected original signals and extracting *features*, what we have obtained is a sequence of cleaned CSIs. Each CSI represents the phases and amplitudes on a group of 30 OFDM subcarriers. Since the noise has been removed from the signals, there would be little dramatic fluctuation caused by interference or noise [24]. Thus, the cleaned CSIs

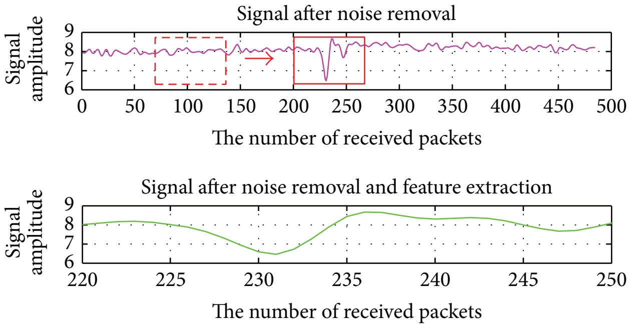


FIGURE 5: The comparison between signals after noise removal and signals after noise removal and feature extraction.

can represent the influenced signal traces caused by finger motions (*features*), and we define the cleaned CSIs as a *finger motion profile*.

4.5. Unlock Passwords Recognition. After building the *finger motion profiles*, the next work is how can we recognize the different *finger motion profiles* and further recognize the unlock passwords. Having recognized the similarity between time-series data matching and unlock passwords recognition, we borrow the technique dynamic time warping (DTW) from time-series data matching to recognize the unlock passwords.

Dynamic time warping is widely used in time-series data matching, and it is used to quantify the similarity of two time-series data sets. However, our work is quantifying the similarity of two signals; they have something in common. Besides, Rath and Manmatha [25] exploit the potentiality of dynamic time warping to match word image, Wang and Katabi [26] evaluate the similarity between the multipath profiles of the desired tag and the multipath profiles of the reference tags by using dynamic time warping, and many others [18] also leverage dynamic time warping to achieve the evaluation of similarity between two series. Thus, we can use dynamic time warping to quantify the similarity between the signals of two different unlock passwords.

The input of DTW is two signals, one is reference signal and another is desired signal, and the output of DTW is a calculated distance. When given a desired signal, what we want to know is which reference signal is the most similar to the desired signal. The only measurement index is the calculated distance, and the reference signal whose calculated distance with desired signal is the minimum can be thought to be the most similar to the desired signal [27, 28].

5. Hierarchical Approach for Unlock Passwords Recognition

After computing the distances between the desired signals and reference signals, WiPass will identify the unlock passwords. However, there exist plenty of reference signals. When the distances are computed between desired signal and all those reference signals, that will cost a lot of time and computational complexity will be high. Hence, in order to keep the cost and computational complexity low, WiPass recognizes the unlock passwords hierarchically using the protocol below.

Protocol. In stage 1, several *finger motion profiles* of each type of unlock passwords are chosen as the reference signals. Then DTW will compute the distances between the desired signal and reference signals. In the computed distances, there will exist a type of the unlock passwords whose distance is much smaller than other types, and the desired unlock password is thought to belong to that type.

In stage 2, the unlock passwords with similar shape can be thought to belong to one kind, and the different kinds of unlock passwords are chosen as the reference signals. Similar to stage 1, the unlock passwords will belong to one kind of the unlock passwords with similar shape.

In stage 3, the unlock passwords will be matched with the kind of unlock passwords and finally the desired unlock password will be recognized.

Computational Complexity. The complexity of WiPass comes from the number of the reference signals and the length of the features of desired signals and reference signals. Let N be the total number of reference signals, let L_1 be the length of the feature of desired signals, and let L_2 be the length of the feature of the reference signals. Thus, recognizing the desired unlock password has a complexity of $O(NL_1L_2)$. Using hierarchical approach can reduce the complexity to $O(nL_1L_2)$, where n is total number of reference signals that are matched with the desired signal, and $n \ll N$.

The runtime of unlock passwords matching is 37.131518 seconds when the system computes the calculated distances between one desired unlock password and 25 reference unlock passwords (the length of the unlock passwords is more than 300 packets). The runtime of unlock passwords matching is 9.668004 seconds when the system computes the calculated distances between one desired unlock password and 5 reference unlock passwords (the length of the unlock passwords is more than 300 packets). The runtime of *finger motion profile* matching is 0.243151 seconds when the system computes the calculated distances between one desired *finger motion profile* and 5 reference *finger motion profiles* (the lengths of the *finger motion profiles* are 60 packets). The experiments are done using MATLAB R2012b on a 64-bit machine with Intel Core i3-4150 Quad-Core processor and 8 G memory. The actual runtime experiments demonstrate that the complexity of WiPass is positively correlated to the number of the reference signals and the length of the features.

6. Implementation and Microbenchmark

We implement WiPass on current mobile smart devices with the wireless hotspot functionality and evaluate its performance in typical indoor scenarios.

6.1. Hardware and Scenarios. A smart device with wireless hotspot functionality is used as the transmitter (IPhone 6 plus), and a desktop equipped with Intel 5300 NIC (Network Interface Controller) is used as the receiver. The transmitter operates in IEEE 802.11n. The receiver has 3 working antennas

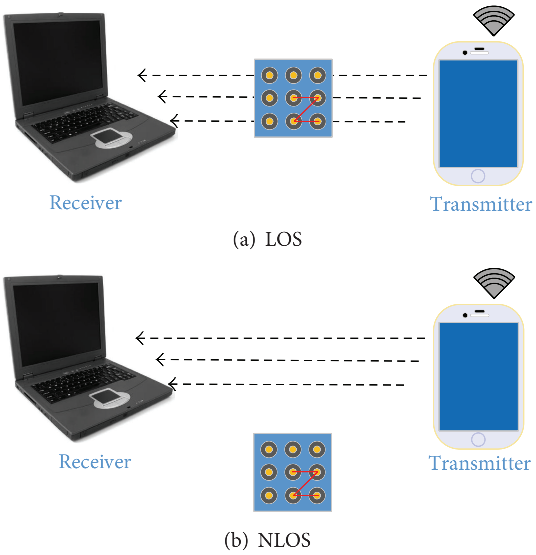


Figure 6: Experiment scenarios.

and the firmware is modified to report CSIs to upper layers. During the measurement, the receiver continuously pings packets from the smart devices at the rate of 5 packets per second. The collected CSIs are stored and processed at the receiver. The tested mobile phone is SAMSUNG Galaxy Note 3.

The experiments are conducted in a typical indoor office whose area is 3.6 m × 6.6 m. To evaluate WiPass's performance, the experiments are done in two scenarios, LOS scenario and NLOS scenario.

LOS Scenario: Line of Sight. The target person is just on the straight line between transmitter and receiver and is within the radio range of the transmitter, as shown in Figure 6(a).

NLOS Scenario: Nonline of Sight. The target person is not on the straight line between transmitter and receiver but also is within the radio range of the transmitter, as shown in Figure 6(b).

6.2. Unlock Passwords Vocabulary. The unlock passwords are divided into four types, some of each type of unlock passwords are chosen as the tested unlock passwords, and 25 unlock passwords are chosen randomly as the tested unlock passwords. All the tested graphical unlock passwords can be divided into four types, and one type of the unlock passwords is that there is no inflection points in the unlock passwords, one is one inflection point in the unlock passwords, one is two inflection points in the unlock passwords, and the last is three or more than three inflection points in the unlock passwords. As shown in Figure 7, unlock passwords pattern 1, pattern 2, and pattern 3 can be thought to be the first type of unlock passwords, and unlock passwords pattern 4 and pattern 5 can be thought to be the second type, unlock passwords pattern 10 and pattern 11 can be thought to be the third type, and unlock passwords pattern 23, pattern 24, and pattern 25 can be thought to be the last type. In the second type, there are three kinds of unlock passwords, pattern 4 to pattern 7 belong to the first kind, pattern 8 and pattern 9 belong to the second kind, and pattern 17 and pattern 18 belong to the third kind. The first three types of unlock passwords can be thought to be simple unlock passwords, and the last can be thought to be complex unlock passwords.

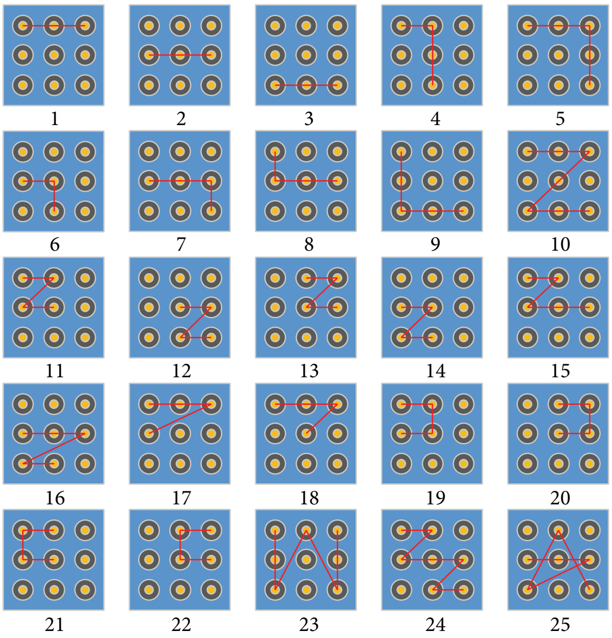
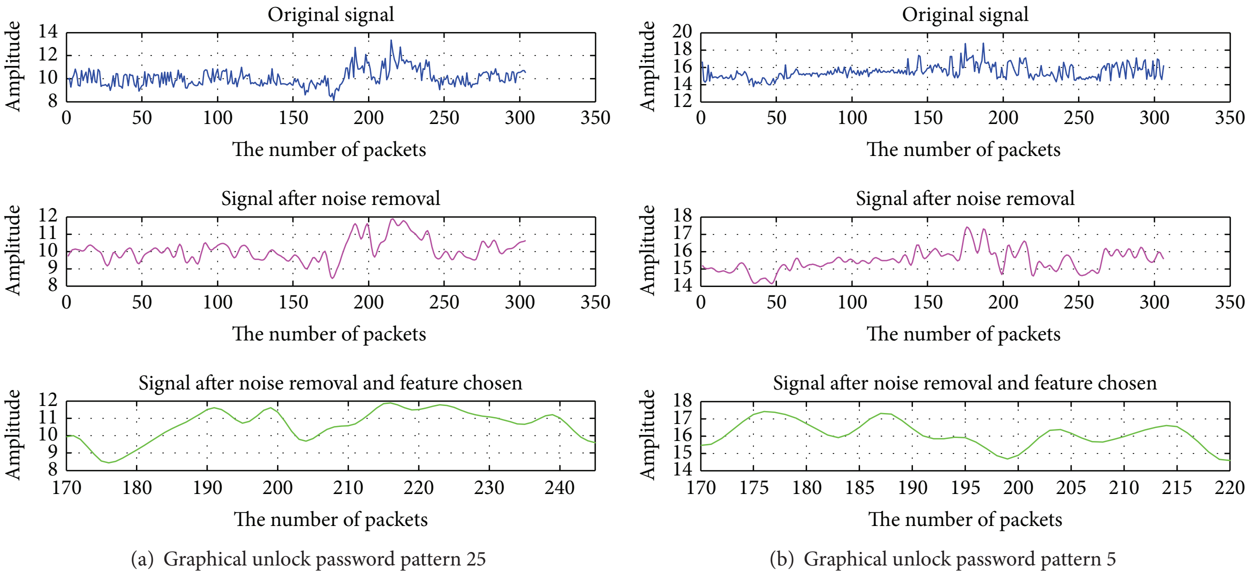


Figure 7: 25 tested unlock passwords in the experiment.

The lengths of extracted features (the number of received packets for the influenced signal traces) of different types of unlock passwords are different, since the time spent on unlocking for simple unlock passwords and complex unlock passwords is different when the same group of persons unlock the same-size touch-enabled devices. The impacts of finger motions of different kinds of unlock passwords are also different; thus, the hierarchical approach is feasible theoretically.

6.3. Microbenchmark Experiment. We start with a microbenchmark experiment to provide insights into the working of WiPass. In order to better understand how unlock passwords influence the wireless signals, we conduct a simple experiment of two different unlock passwords. The experiments are conducted in the conditions that there are no surrounding people in the environment and the user does not move while unlocking the devices.

Figure 8 shows the signals under different conditions for two different graphical unlock passwords when the transmitter is current smart mobile phone with wireless hotspot functionality. As Figure 8 shows, the impacts of finger motions of different unlock passwords on wireless signals are different. When there is no surrounding people in the environment and there exist no unlock passwords, the collected signals keep relatively stable. When the user starts to unlock the device, the collected signals will fluctuate, and



(a) Graphical unlock password pattern 25

(b) Graphical unlock password pattern 5

FIGURE 8: Microbenchmark experiments of two different unlock passwords.

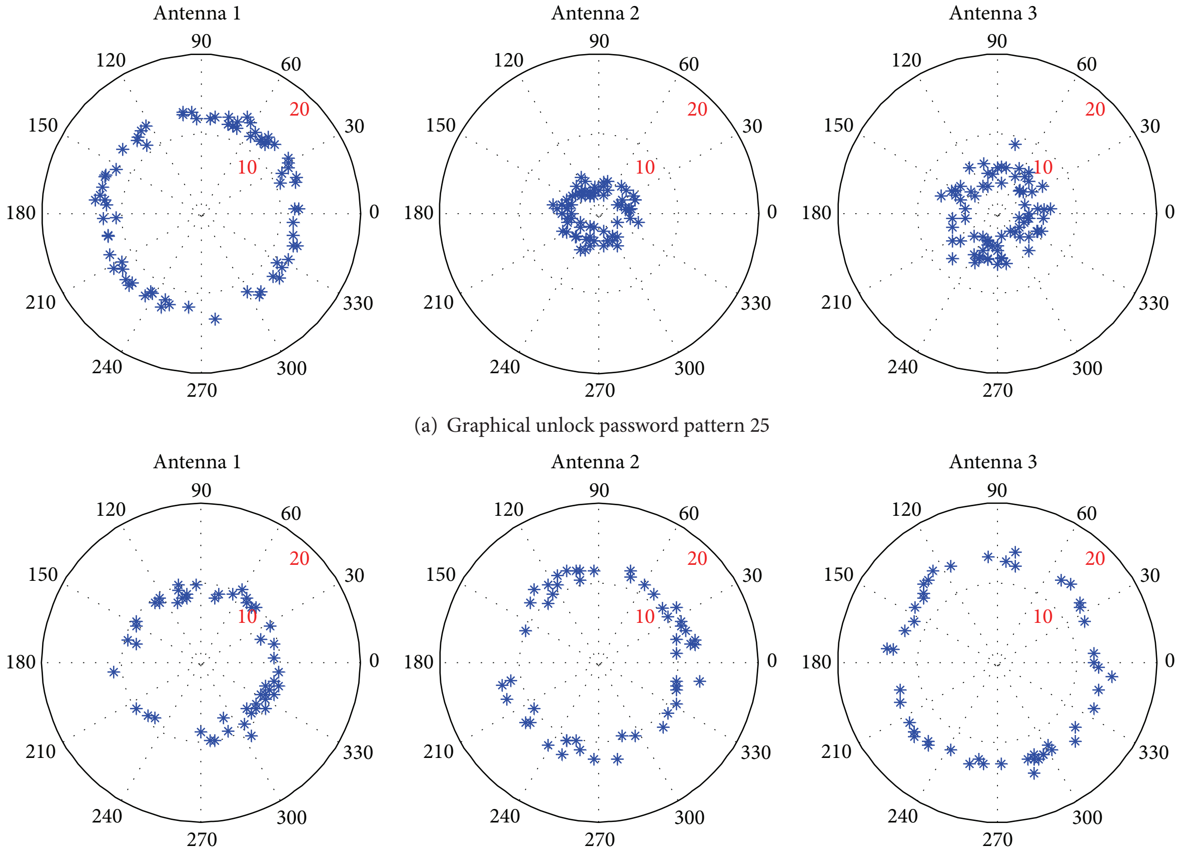
when the user ends unlocking the device, the signals will return to be relatively stable. Thus, the unlock passwords can be recognized.

6.3.1. Recognition among Unlock Passwords with Great Difference. We can see from Figure 8 that, after noise removal and feature chosen, the signals are different in amplitude. In Figure 8(a), after noise removal and feature chosen, the signal amplitude of the unlock password pattern 25 is between 8 and 12 while, in Figure 8(b), the signal amplitude of unlock password pattern 5 is between 14 and 18. Besides, when there exists great difference among the unlock passwords, the lengths of the features of unlock passwords are different. For example, in Figure 8(a), the length of the feature of unlock password pattern 25 is 75 while the length of the feature of unlock password pattern 5 is 50. That is because, for different types of unlock passwords, the spent time is usually different, and, after noise removal and feature chosen, the lengths of the features are different, as shown in Figure 8. Thus, using the signal amplitude and the length of the feature can distinguish the unlock passwords with great difference. In addition, there is another information that can be obtained from CSIs except amplitude and it is phase. Using phase can also recognize the unlock passwords with great difference successfully. Figure 9 can demonstrate it. Figures 9(a) and 9(b) separately represent the relationships between amplitude and phase of two different unlock passwords with great difference. We can see from Figure 9 that the relationships between phase and amplitude are different no matter what in terms of one antenna or in terms of three antennas. So, for those unlock passwords with great difference, the unlock passwords can be recognized using amplitude and the length of features or using amplitude, phase, and the length of features.

6.3.2. Recognition among Similar Unlock Passwords. For those graphical unlock passwords with great difference, the representations of signals are different in amplitude in time domain, as shown in Figure 8. However, for those similar unlock passwords, such as unlock passwords pattern 11, pattern 12, pattern 13, and pattern 14, the representations of signals are similar in amplitude in time domain and the lengths of the features are also the same. Besides, the relationships between amplitude and phase are also similar, as shown in Figure 10. Figures 10(a) and 10(b) represent separately the relationships between amplitude and phase of unlock passwords pattern 11 and pattern 13. We can see from Figure 10 that, for those similar unlock passwords, the relationships between amplitude and phase are also similar no matter what in view of one antenna or three antennas. So how can we recognize those similar unlock passwords? It is known that phase is another information that can be obtained from CSIs, and it can be expressed in time domain, as shown in Figure 11. We can see from Figure 11 that the phases of pattern 11 and pattern 13 are different in time domain no matter what in view of one antenna or three antennas. Thus, for those similar unlock passwords, when their signal amplitudes are similar, the lengths of features are the same, and the relationships between amplitude and phase are also similar, the phase information can be used to recognize the unlock passwords successfully. So, in this paper, amplitude and phase are used together to recognize the similar unlock passwords.

7. Evaluation

In this section, the recognition accuracy of graphical unlock passwords when using amplitude only and using amplitude and phase together is computed. This section also compared



(a) Graphical unlock password pattern 25

(b) Graphical unlock password pattern 5

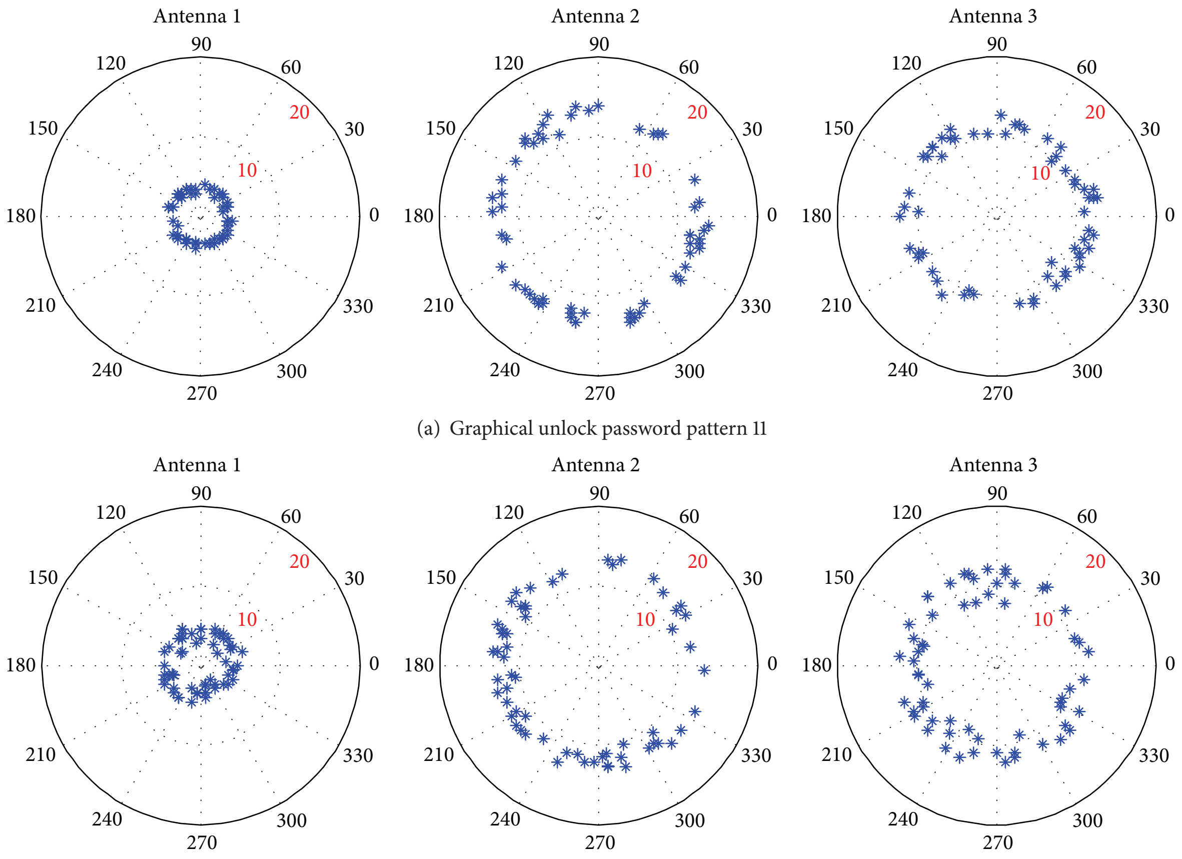
Figure 9: Comparison of the relationships between phase and amplitude of two graphical unlock passwords with great difference after noise removal and feature chosen.

the complexity of feature chosen when using AP (Access Point) as the transmitter and when using a smart mobile phone with wireless hotspot functionality as the transmitter.

7.1. Wireless Device Diversity: Router versus Smart Phones. We can see from Figure 12 that when the transmitter is TP-Link wireless router and there exist no unlock passwords, the signals after noise removal keep stable, as shown in Figure 12, when the number of received packets is between 0 and 160. However, when the transmitter is the smart phone with the wireless hotspot functionality, the signals after noise removal just keep relatively stable, as shown in Figure 8. That is because, for TP-Link wireless router, there is only one kind of antenna, and it is WiFi antenna and it is used to transmit the wireless signals while, for smart phones with the wireless hotspot functionality, there are also other antennas besides WLAN antenna, such as communication antenna, GPS antenna, Bluetooth antenna, and NFC antenna. When there exist no unlock passwords and the environment is stable, there is no other interferences that influence the signals; thus, the signals after noise removal keep stable when the transmitter is TP-Link wireless router, while when the transmitter is the smart phone with wireless hotspot functionality, there will exist other interferences coming from other antennas that influence the signals; thus, the signals after noise removal just keep relatively stable. Thus, when the transmitter is TP-Link wireless router, the feature chosen is easier than when the transmitter is a smart phone with wireless hotspot functionality. In this paper, the smart phone with wireless hotspot functionality is used as the transmitter just because, for those places where there does not exist a wireless router (e.g., in the bus), the attack against unlock passwords cannot occur; however, it should be a warning for mobile phone user that the attack can occur when the attacker has a smart mobile phone with wireless hotspot functionality regardless of the place where the attacker is.

7.2. Graphical Unlock Password Accuracy. In this section, the accuracy of graphical unlock passwords is tested. In order to test the accuracy of similar unlock passwords, some of the unlock passwords of each type are tested. As shown in Figure 7, 25 unlock passwords are tested and each unlock password is tested 20 times.

7.2.1. Recognition Using Amplitude Only. For those unlock passwords with great difference, the lengths of features and the amplitude of the signals are usually different; thus, using amplitude can recognize the unlock passwords successfully. In order to demonstrate it, 6 unlock passwords are chosen as the tested unlock passwords, and they are separately unlock



(a) Graphical unlock password pattern 11

(b) Graphical unlock password pattern 13

Figure 10: Comparison of the relationships between phase and amplitude of two similar graphical unlock passwords after noise removal and feature chosen.

passwords pattern 2, pattern 5, pattern 9, pattern 10, pattern 21, and pattern 23. The results are shown in Figure 13. We can see from Figure 13 that the recognition accuracy can achieve 60% at least, and the recognition accuracy is between 60% and 80%. The average recognition accuracy of the six unlock passwords is 70%; thus, for those unlock passwords with great difference, using amplitude only can recognize the unlock passwords. However, for those similar unlock passwords, using amplitude only cannot recognize the unlock passwords successfully. To further demonstrate it, three groups of similar unlock passwords are tested, and one group is unlock passwords pattern 4, pattern 5, pattern 6, and pattern 7, one group is unlock passwords pattern 10, pattern 11, pattern 12, pattern 13, and pattern 14, and the last group is unlock passwords pattern 19, pattern 20, pattern 21, and pattern 22. The results of recognition accuracy are shown in Figure 14. As shown in Figure 14, the recognition accuracy is low and most of the accuracy are between 20% and 50%, except pattern 10 and pattern 21. The average recognition accuracy of the three groups of similar unlock passwords is 37%. Thus, using amplitude only cannot recognize those similar graphical unlock passwords successfully.

7.2.2. Recognition Using Amplitude and Phase. We know from Figure 14 and the analysis of Section 6.3.2 that when amplitude cannot recognize the similar unlock passwords successfully, phase information can help to distinguish them. To demonstrate it, the amplitude information and phase information of the three groups of similar unlock passwords are leveraged together to recognize them. The results are shown in Figure 15. Comparing with Figure 14, we know that the recognition accuracy improved significantly and the average recognition accuracy can achieve 58%. Thus, amplitude information and phase information can be used together to improve the recognition accuracy of similar graphical unlock passwords.

Figure 16 shows the results of recognizing the 25 tested unlock passwords with one attempt. We can see from Figure 16 that the recognition accuracy of most unlock passwords is above 60%, and the average recognition accuracy can achieve 66%. However, because DTW computes distances between the desired unlock password and reference unlock passwords and if the computed minimum distance is not matched with the desired unlock passwords, the unlock passwords can be matched with the second minimum distance, third minimum distance. That means we can try to unlock the device with two attempts or with three attempts. After three attempts or less than three attempts, the recognition accuracy of most unlock passwords can achieve above 80%, and the average accuracy is 85.6%, as shown in Figure 17.

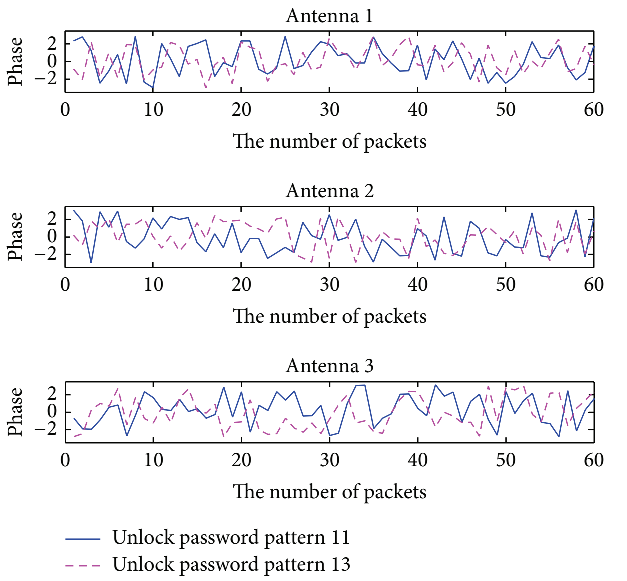


Figure 11: The comparison of phase after noise removal and feature chosen between the graphical unlock password pattern 11 and graphical unlock password pattern 13.

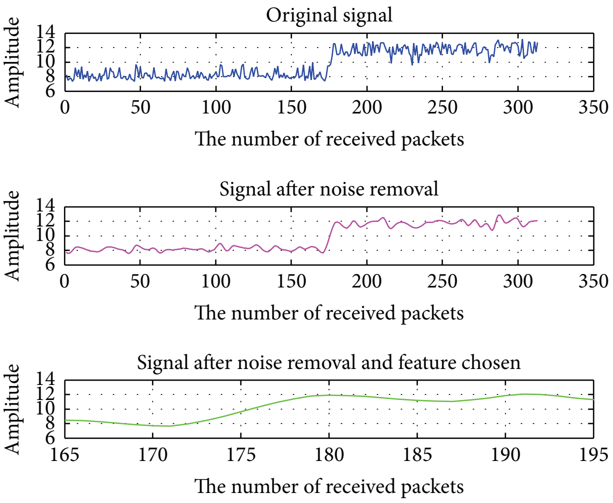


Figure 12: The signals of graphical unlock password pattern 5 when the transmitter is TL-WR740N wireless router.

In Figures 16 and 17, the successful recognition accuracy of similar unlock passwords is relatively low; for example, the successful recognition accuracy of unlock passwords pattern 11, pattern 12, and pattern 13 in Figure 16 are just separately 40%, 30%, and 40%. However, after several attempts of similar unlock passwords, the accuracy will be improved and, after enough attempts of similar unlock passwords, the desired unlock password will be recognized.

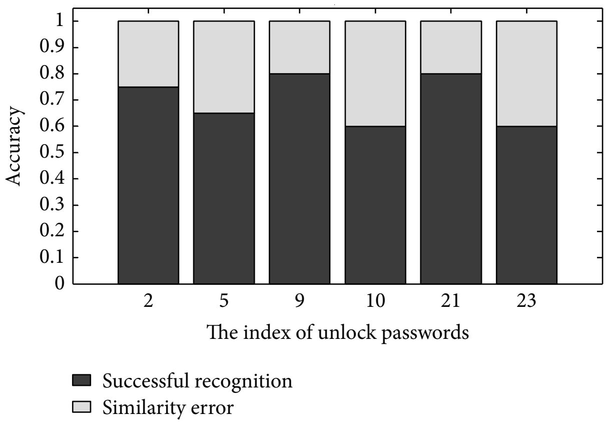


Figure 13: The accuracy of 6 tested graphical unlock passwords with great difference when amplitude is used only.

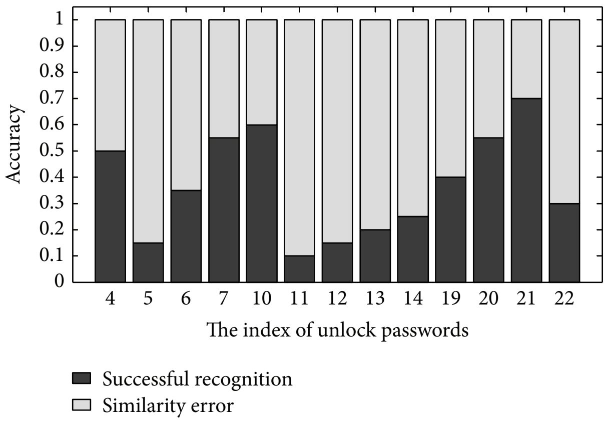


Figure 14: The accuracy of 13 tested similar graphical unlock passwords when amplitude is used only.

7.2.3. Recognition in NLOS Scenario. The above experiments are done in LOS scenario. In most cases, the attack occurs in NLOS scenario; thus, the recognition accuracy in NLOS scenario is also needed to be considered. Figure 18 shows the recognition results of 25 tested graphical unlock passwords within three attempts in NLOS scenario. We can see from Figure 18 that most of recognition accuracy of 25 tested graphical unlock passwords is between 50% and 80% and the average recognition accuracy can achieve 74.7%. Thus, in NLOS scenario, the unlock passwords can be recognized successfully within three attempts. Comparing the recognition accuracy in LOS scenario with that in NLOS scenario, the recognition accuracy in NLOS scenario is lower than that in LOS scenario. That is because, in NLOS scenario, the signal reflections from finger motions are weaker than that in LOS scenario; thus, the accuracy is lower in NLOS scenario than that in LOS scenario.

8. Defense Strategies

Unlock passwords are vulnerable to various attacks, including the attack using wireless signals. In this section, we discuss a few strategies to improve the security and protect the privacy of touch-enabled screen device users.

A few strategies are available to mitigate video attack, sensors attack, and the attack using wireless signals for

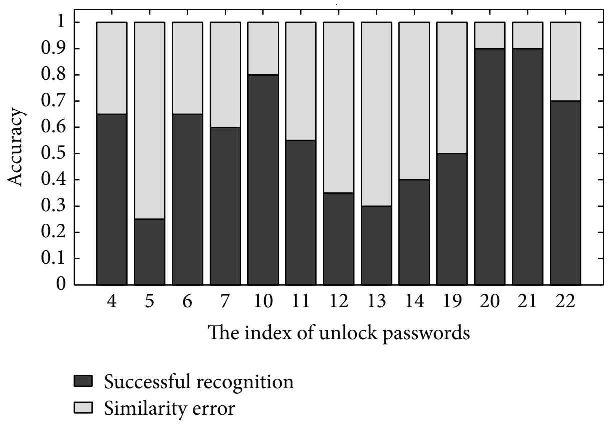


Figure 15: The accuracy of 13 tested similar graphical unlock passwords when amplitude and phase are used.

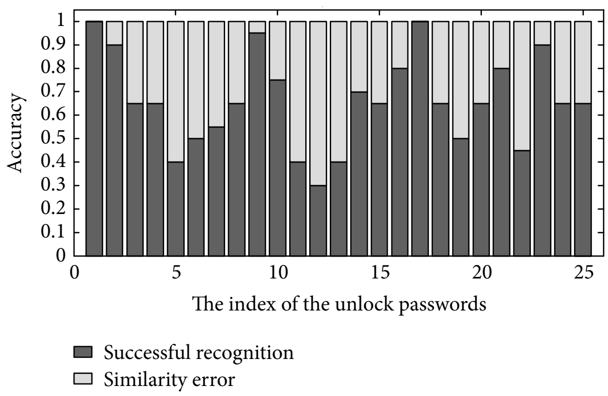


Figure 16: The accuracy of 25 tested graphical unlock passwords when amplitude and phase are used.

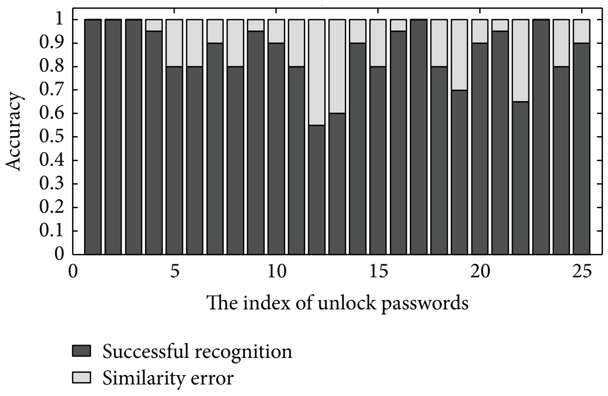


Figure 17: The accuracy of 25 tested graphical unlock passwords within three attempts when amplitude and phase are used.

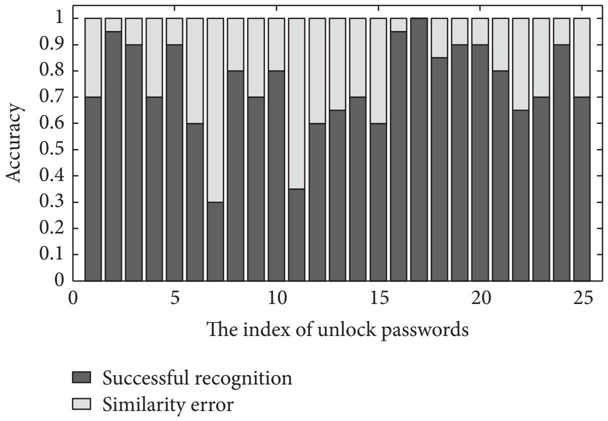


Figure 18: The accuracy of 25 tested graphical unlock passwords within three attempts in NLOS scenario.

touch-enabled screen devices without modifying the devices. The first one is setting complex passwords. Setting complex unlock passwords can defeat the attacks to some extent; however, if the complex unlock passwords are common and it can be thought of by the attacker in advance, the unlock passwords will be decoded. Besides, setting complex unlock passwords is inconvenient for users, especially for those who input passwords frequently.

Another defense strategy is that in public places, especially when there are persons near to you, we try not to unlock the devices so that the unlock passwords cannot be obtained by the attacker to the maximum possible extent. However, it is very troublesome for people, because people need to be careful when there are people near to them.

One more defense strategy is unlocking the smart devices using fingerprints, and it is the most safe unlocking. Current touch-enabled screen devices should go ahead for that fingerprints unlocking direction.

9. Discussions and Limitations

In this section, we discuss the limitations of our implementation.

(1) User Movement. In this paper, the unlock passwords can be recognized when the target person does not move. It is possible that the person unlocks the device while walking. However, the device-free localization techniques [29] can achieve real-time tracking, so combining with WiPass, we can achieve the recognition of unlock passwords when the target person moves.

(2) Impact of Surroundings. Movements of surrounding people sometimes can reflect the wireless signals more significantly than finger motions do. In this paper, we assume that there are no surrounding moving people when the target person is unlocking the devices. It is possible that there are no surrounding moving people in a silent coffee shop or library. However, there will always exist surrounding moving people in most public places, and that can be solved by MIMO technique [30]. Then MIMO beamforming will be leveraged to focus on the targets' fingers to reduce irrelevant multipath effects.

(3) Devices Diversity. There are many kinds of smart touch-enabled screen devices. For each kind of touch-enabled screen devices, the size of touch screen is different; thus, the

positions of each keypads are different. In this paper, just one kind of mobile phone is tested to demonstrate that the unlock passwords can be recognized using wireless signals and, in future work, more experiments on other kinds of smart devices will be conducted and the similar smart devices can be classified into one group (the size of touch screen and the positions of keypads are the same) to recognize the unlock passwords in order to be time-saving and labor-saving.

(4) The Diversity of Unlocking Speeds. For different people, the unlocking speeds are different. There are four user groups for smart devices, and one is teenager, one is the young, one is the middle-aged, and the last is the old. However, the young is the main user group and, in this paper, the experiments are conducted with the young people. The future work of this paper will analyse the impacts of finger motions on the signals when the unlocking speeds are different and the unlocking passwords of different speeds can be classified into different groups.

(5) The Size of Patterns. There are a great number of different unlock passwords. In this paper, only 25 patterns are considered to demonstrate that your unlock passwords can be leaked through wireless hotspot functionality. It should be a warning for current mobile device users. When the desired unlock passwords are not in the 25 patterns, the desired unlock passwords will not be recognized successfully. However, the performance can be improved by a continuously learning-based approach, where the model keeps evolving using examples collected in the end-users environments, and when a user unlocks the device using the unknown unlock passwords, the unknown unlock passwords will be put into the size of patterns. That will be a continuous process to enlarge the size of patterns and improve the recognition accuracy.

10. Conclusion

This paper presents WiPass, a novel system that enables wireless signals, which are transmitted by a smart device with wireless hotspot functionality, to "see" the unlock passwords. WiPass is easily implemented by current smart devices and does not need any support of additional hardware. To achieve the unlock passwords recognition, WiPass first removes the noise from collected signals using a two-level Symlet filter and then uses DCASW (the difference of the cumulative amplitude of the sliding window) to extract the features to build the *finger motion profiles* and then uses a hierarchical dynamic time warping (DTW) approach to recognize the unlock passwords. The experiment results demonstrate that WiPass can achieve recognition accuracy of 85.6% for graphical unlock passwords in line of sight (LOS), 74.7% in nonline of sight (NLOS). The results also demonstrate that the recognition accuracy can be improved by using amplitude information and phase information together and by adding the times of attempts. We believe that this paper exposes a serious threat for current touch-enabled screen devices users, and such attack can happen in public places where the attacker looks unsuspected.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (no. 61170218, no. 61202198, no. 61202393, no. 61272461, no. 61373177, and no. 61572402), the Key Project of Chinese Ministry of Education (no. 211181), the International Cooperation Foundation of Shaanxi Province, China (no. 2013KW01-02 and no. 2015KW-003), and the China Postdoctoral Science Foundation (Grant no. 2012M521797).

References

[1] D. Chen, K. Cho, S. Han, Z. Jin, and K. G. Shin, "Invisible sensing of vehicle steering with smartphones," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 1–13, ACM, Florence, Italy, May 2015.

[2] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "Accelprint: imperfections of accelerometers make smartphones trackable," in *Proceedings of the Network and Distributed System Security Symposium (NDSS '14)*, San Diego, Calif, USA, February 2014.

[3] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, "ACCessory: password inference using accelerometers on smartphones," in *Proceedings of the 12th Workshop on Mobile Computing Systems & Applications (HotMobile '12)*, p. 9, ACM, San Diego, Calif, USA, February 2012.

[4] L. Cai and H. Chen, "TouchLogger: inferring keystrokes on touch screen from smartphone motion," in *Proceedings of the 6th USENIX Conference on Hot Topics in Security (HotSec '11)*, p. 9, 2011.

[5] Z. Xu, K. Bai, and S. Zhu, "TapLogger: inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC '12)*, pp. 113–124, ACM, Tucson, Ariz, USA, April 2012.

[6] M. Seifeldin, A. Saeed, A. E. Kosba, A. El-Keyi, and M. Youssef, "Nuzzer: a large-scale device-free passive localization system for wireless environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, pp. 1321–1334, 2013.

[7] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, "Whole-home gesture recognition using wireless signals," in *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking (MobiCom '13)*, pp. 27–38, ACM, Miami, Fla, USA, October 2013.

[8] H. Abdelnasser, K. A. Harras, and M. Youssef, "WiGest demo: a ubiquitous WiFi-based gesture recognition system," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS '15)*, pp. 17–18, IEEE, Hong Kong, May 2015.

[9] B. Chen, V. Yenamandra, and K. Srinivasan, "Tracking keystrokes using wireless signals," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 31–44, ACM, Florence, Italy, May 2015.

[10] K. Ali, A. Liu X, W. Wang et al., "Keystroke recognition using WiFi signals," in *Proceedings of the 21st Annual International*

Conference on Mobile Computing and Networking, pp. 90–102, ACM, Paris, France, September 2015.

[11] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*, pp. 13–19, ACM, Pittsburgh, Pa, USA, July 2007.

[12] A. Habibi Lashkari, S. Farmand, O. B. Zakaria, and R. Saleh, "Shoulder Surfing attack in graphical password authentication," *International Journal of Computer Science and Information Security*, vol. 6, no. 2, pp. 145–154, 2009.

[13] Y. Zhang, P. Xia, J. Luo, Z. Ling, B. Liu, and X. Fu, "Fingerprint attack against touch-enabled devices," in *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM '12)*, pp. 57–68, Raleigh, NC, USA, October 2012.

[14] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT '10)*, pp. 1–7, USENIX Association, Washington, DC, USA, August 2010.

[15] D. Shukia, R. Kumar, V. V. Phoha, and A. Serwadda, "Beware, your hands reveal your secrets!," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp. 904–917, ACM, Scottsdale, Ariz, USA, November 2014.

[16] Q. Yue, Z. Ling, B. Liu, W. Fu, and W. Zhao, "Blind recognition of touched keys: attack andcountermeasures," http://arxiv.org/abs/1403.4829.

[17] F. Adib and D. Katabi, "See through walls with WiFi!," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 75–86, 2013.

[18] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with Wi-Fi!," in *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom '14)*, pp. 593–604, ACM, 2014.

[19] M. A. T. Figueiredo and R. D. Nowak, "An EM algorithm for wavelet-based image restoration," *IEEE Transactions on Image Processing*, vol. 12, no. 8, pp. 906–916, 2003.

[20] R. Singh, R. E. Vasquez, and R. Singh, "Comparison of daubechies, coiflet, and symlet for edge detection," in *Visual Information Processing VI*, vol. 3074 of *Proceedings of SPIE*, pp. 151–159, International Society for Optics and Photonics, July 1997.

[21] T. D. Bui and G. Chen, "Translation-invariant denoising using multiwavelets," *IEEE Transactions on Signal Processing*, vol. 46, no. 12, pp. 3414–3420, 1998.

[22] M. S. Chavan, N. Mastorakis, M. N. Chavan et al., "Implementation of SYMLET wavelets to removal of Gaussian additive noise from speech signal," in *Proceedings of the 10th International Conference on Recent Researches in Communications, Automation, Signal Processing, Nanotechnology, Astronomy and Nuclear Physics*, pp. 37–41, February 2011.

[23] D. Chendong, H. Zhengjia, and J. Hongkai, "A sliding window feature extraction method for rotating machinery based on the lifting scheme," *Journal of Sound and Vibration*, vol. 299, no. 4-5, pp. 774–785, 2007.

[24] G. Cohn, D. Morris, S. N. Patel, and D. S. Tan, "Humantenna: using the body as an antenna for real-time whole-body interaction," in *Proceedings of the 30th ACM SIGCHI Conference on Human Factors in Computing Systems*, pp. 1901–1910, ACM, May 2012.

[25] T. Rath and R. Manmatha, "Word image matching using dynamic time warping," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 2, pp. II-521–II-527, IEEE, June 2003.

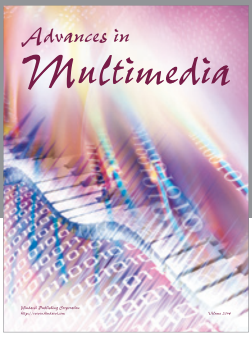
[26] J. Wang and D. Katabi, "Dude, wheres my card? RFID positioning that works with multipath and non-line of sight," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 51–62, 2013.

[27] S. Salvador and P. Chan, "FastDTW: toward accurate dynamic time warping in linear time and space," in *Proceedings of the 3rd SIGKDD Workshop on Mining Temporal and Sequential Data (KDD/TDM '04)*, Seattle, Wash, USA, December 2004.

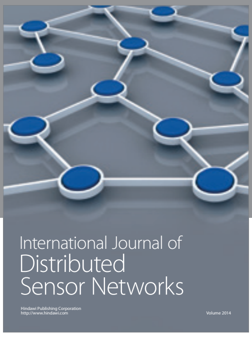
[28] M. Müller, "Dynamic time warping," in *Information Retrieval for Music and Motion*, pp. 69–84, 2007.

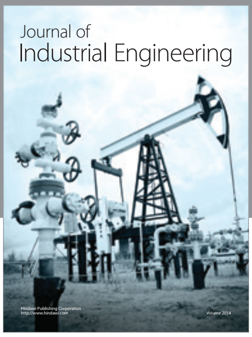
[29] J. Xiao, K. Wu, Y. Yi, L. Wang, and L. M. Ni, "Pilot: passive device-free indoor localization using channel state information," in *Proceedings of the IEEE 33rd International Conference on Distributed Computing Systems (ICDCS '13)*, pp. 236–245, IEEE, Philadelphia, Pa, USA, July 2013.

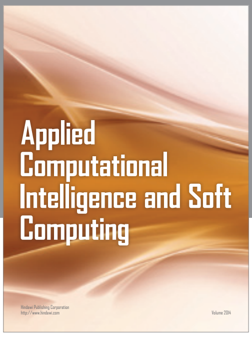
[30] A. L. Moustakas, S. H. Simon, and A. M. Sengupta, "MIMO capacity through correlated channels in the presence of correlated interferers and noise: a (not so) large N analysis," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2545–2561, 2003.

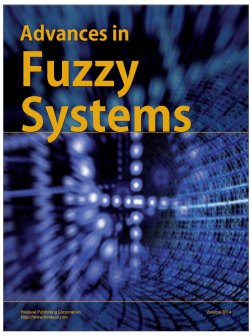

Advances in
Multimedia

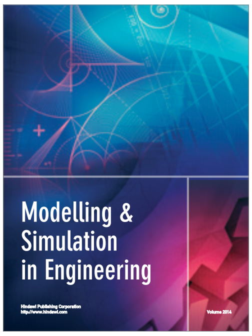
The Scientific
World Journal

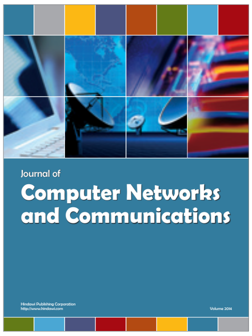

International Journal of
Distributed
Sensor Networks

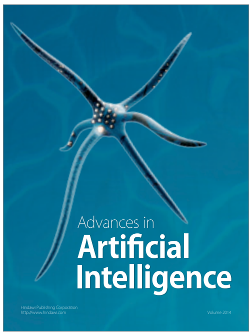

Journal of
Industrial Engineering

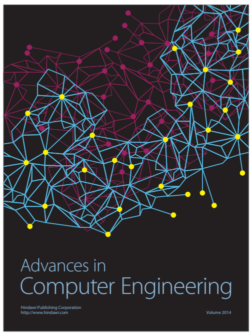

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

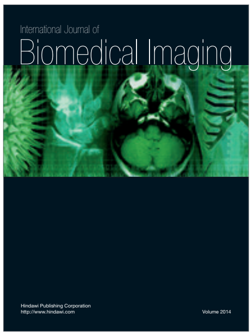

Modelling &
Simulation
in Engineering

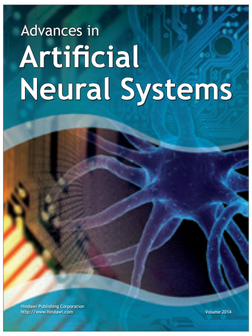

Journal of
Computer Networks
and Communications

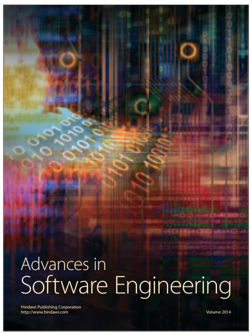

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

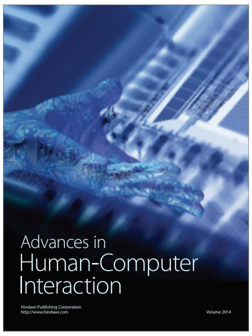
International Journal of
Computer Games
Technology

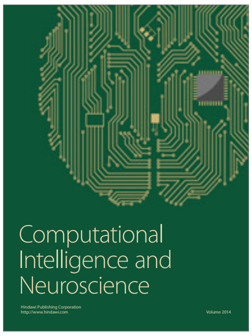

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering