A SYSTEM FOR CELL PHONE ANTI-THEFT THROUGH GAIT RECOGNITION

A Thesis

presented to

the Faculty of California Polytechnic State University,

San Luis Obispo

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Computer Science

by

Cameron Stearns

May 2014

COMMITTEE MEMBERSHIP

TITLE:	A System For Cell Phone Anti-theft Through Gait Recognition
AUTHOR:	Cameron Stearns
DATE SUBMITTED:	May 2014
COMMITTEE CHAIR:	Phillip Nico, Ph.D Associate Professor of Computer Science
COMMITTEE MEMBER:	Franz Kurfess, Ph.D Professor of Computer Science
COMMITTEE MEMBER:	Zachary Peterson, Ph.D Assistant Professor of Computer Science

ABSTRACT

A System For Cell Phone Anti-theft Through Gait Recognition

Cameron Stearns

Studies show that smartphone thefts are a significant problem in the United States. [30] With many upcoming proposals to decrease the theft-rate of such devices, investigating new techniques for preventing smartphone theft is an important area of research. The prevalence of new biometric identification techniques for smartphones has led some researchers to propose biometric anti-theft measures for such devices, similar to the current fingerprint authentication system for iOS. Gait identification, a relatively recent field of study, seems to be a good fit for anti-theft because of the non-intrusive nature of passive pattern recognition in walking. In this paper, we reproduce and extend a modern gait recognition technique proposed in *Cell Phone-Based Biometrics* by testing the technique outside of the laboratory on real users under everyday conditions. We propose how this technique can be applied to create an anti-theft system, and we discuss future developments that will be necessary before such research is ready to be implemented in a release-quality product. Because previous studies have also centered around the ability to differentiate between individual users from a group, we will examine the accuracy of identifying whether or not a specific user is currently using a system. The system proposed in this paper shows results as high as 91% for cross-fold accuracy for some users; however, the predictive accuracy for a single day's results ranged from 0.8% accuracy to 92.9% accuracy, showing an unreliability that makes such a system unlikely to be useful under the pressure of real-world conditions.

Keywords: Computer Security, Mobile computing, Biometrics

ACKNOWLEDGMENTS

Special thanks to Eric Buckthal for early development work and research towards a class project that eventually became this thesis.

Thank you to Dr. Phillip Nico for advising me both officially and unofficially throughout the course of the project.

Thanks to Nick Leighton and Kevin Sale, undergraduate students at UC Irvine who pointed me towards issues using cell-phone accelerometers for detecting the phone's orientation.

TABLE OF CONTENTS

Page

Chapter

LIST OF FIGURES

Chapter 1. Introduction

Reproducibility is key to the scientific process. One would expect that in computer science, where the majority of our technical tools can be shared cheaply across the internet, reproducibility would be a simple process; however, studies show that computer science researchers are frequently unwilling to allow others to test their results. [23] Because of this, the main goal of our paper is to reproduce the technique for gait recognition proposed in *Cell Phone-Based Biometric Identification*, to test this technique on users in real-world scenarios, and to propose an extension of this technique to address smartphone theft.

Smartphone theft is a swiftly growing concern in the United States. According to the California Legislature, "...smartphone thefts now account for 30 to 40 percent of robberies in many major cities across the country." [25] According to a survey projection by Consumer Reports, 1.6 million Americans were victims of smartphone theft in 2012. [30] As of June 13, 2013, New York Attorney General Eric Schneiderman has announced the Secure our Smartphone Initiative, a group dedicated to reducing smartphone robberies. [5] In order to address the growing concerns surrounding smartphone theft, some lawmakers have proposed the addition of kill switches to phones, which would allow users to remotely disable smartphones. This allows a user, or company, to remotely disable a phone and to prevent the device from being used after a theft or other illegitimate use. Apple has announced plans to release such a feature for iOS 7, but many other manufacturers remain reluctant to do so. [12] Such a feature can easily be implemented to remove functionality remotely from these phones, but the problem of when to apply such a feature remains open.

Reproducing the work of *Cell Phone-Based Biometric Identification*, this paper considers the application of this work to build a theft detection system. This would allow smartphone users to detect thefts earlier, and could help to deter theft by remotely killing or GPS tracking the device. Specifically, gait analysis is investigated, because it is a current area of research which has found relatively few practical applications. By taking samples of typical user behaviors over time, using machine learning to analyze this behavior, and using the resulting neural network to analyze samples of walking behavior as they are produced, the system can provide a prediction of whether the authorized user is using the device. If the system detects an unauthorized user, it can be used to inform users, and (perhaps) the police of the GPS coordinates of the phone. This work is focused around addressing technical hurdles to such a system, but there are also legal and other administrative issues to address with such a system.

Provided that legislation pushes for these new kill switches, there is a clear use for such a system. Using notifications from our system, a user can be informed that a “loss” of such a device is actual theft, and can choose to activate such a kill switch. However, kill switches are currently opposed by some cell-phone carriers. [5] The carriers cite this is because kill switches could “allow a hacker to disable someone's phone.”[5] While this is certainly a potential issue, proponents of the kill switch solution point out that, “Replacement of lost and stolen mobile communications devices was an estimated thirty-billion-dollar ($30,000,000,000) business in 2012 according to studies conducted by mobile communications security experts.” [25] Both of these issues disincentivize smartphone manufacturers from providing kill switch behaviors, but other potentially useful notification systems are discussed in later sections.

Chapter 2. Background

In the field of gait-based biometric identification, there are generally two core steps to the algorithm. The first part is to pick attributes on which to differentiate. For example, some techniques use the time between steps as part of the algorithm. [29] The second part is evaluation of the known properties to make a best estimate at which user produced the properties. We will discuss more classification techniques in our related work section; however, neural networks are one example of such an evaluator.

2.1. Neural Networks

Bear in mind that it is sufficient for the reader to understand that neural networks are trainable evaluators, which can take in a "training set" of data (example: time between steps mapped to users), and then make predictions about similar data in the future, such as predicting which user generated a specific time between steps. Therefore, the following description is included only to describe the data-mining techniques used in this paper, and may assist in an understanding of the results of our research.

Neural networks are an artificial intelligence technique that mimic the structure of the human brain, by providing a network of interconnected neurons. [21] The first layer of neurons, the input layer, generates outputs based on weighting of the inputs from an initial set of data. In this case, the inputs would be values such as time between steps, as discussed above. Eventually, after passing through "hidden layers" of interconnected neurons, the system sends the outputs of previous neurons to the "output layer" which has one or more exit points. [10] Each neuron has an "activation function," a calculation based on its inputs and their weights that determines whether it outputs a signal. Because the nodes are interconnected and networks tend to contain many neurons, neural networks exhibit emergent, difficult to predict behaviors. This means that looking at any particular element of the network alone tends not to help in analyzing what the system as a whole is doing. The actual implementation of these networks and the methods for training varies from system to system; however, the neural network tools used by this work are those provided by the Weka Data Mining Toolkit. [20] This neural network tool trains using backpropogation, a technique for learning appropriate connection weights by starting with randomly weighted connections, and reducing the system's error by adjusting the connections leading to correct solutions. [10]

2.2. Cross-Validation

Cross-validation is a technique for determining the accuracy of data mining evaluators, such as neural networks. In k-fold cross-validation, some dataset is split into k subsets, referred to as "folds." [16] The data mining evaluator is then trained on the complete dataset except on one fold, which is used as the test set. This is repeated k times, once for each fold. Leave-one-out cross validation is essentially k-fold cross validation, where k is equal to the size of the data set. This means that the evaluator is trained on all values of the data set, except one, then tested on only the removed data point. Cross-validation (in particular, 10 fold cross-validation) is by far the most popular method of evaluating results in the related works described here. It is important to discuss this technique, as cross-validation shows good results when a sample is representative of data that the system will be used on, but when the training data differs significantly from real-world data, it can give overly generous accuracy estimates. This is a larger issue and will be discussed in our experimental results sections.

Chapter 3. Related Work

3.1. Other Motion Identification Systems

Motion-based biometrics are not a new concept. Typing pattern analysis can be used to differentiate users of traditional keyboard systems. [9,11,18] Keystroke dynamics and typing analysis have been studied as a tool for user identification since the late 1970's. In fact, the motions used in typewriting have been studied for a variety of other reasons since the 1920's. [9] While these systems have not garnered much popularity as a means of authentication for traditional desktops, some researchers have identified use cases where they fit well, such as applications that require extended interaction. [18]

Previous papers in the field of cell phone based biometric identification described using touch-screen pressure differences between users. [24] Unfortunately, this is more difficult on modern capacitive touch screen devices, which rely on current analysis rather than pressure detection. iPhones do not currently support pressure sensitivity, though this may change as Apple is filing a patent for a new force-sensitive touch screen. [22] While the Android OS contains tools for determining on-screen pressure, these measures are calibrated differently on different device models. [19] Additionally, the tools used to determine this pressure range from "size" analysis using the surface area of the device being touched to estimate pressure to actual hardware pressure sensors on specific devices. The end result of this is that it is difficult to get consistent pressure results across different Android devices. Because of this, modern approaches to biometric identification in smartphones have largely moved away from the pressure-based approach, despite the technique showing accuracies as high as 99%. [24]

3.2. Gait Recognition Systems

Gait recognition did not begin with smartphone devices in mind. Instead, in the 1990's and early 2000's, researchers began to use camera systems to determine spatio-temporal patterns in walking behaviors. [7] Researchers measured the positions of individual parts of the leg throughout a walking motion, the time between steps, and modeling human walking patterns as a series of steps, and measuring where in space and in time each of these steps occurred for each person in the study. For example, in a given walking window, a person will strike the ground with their heel first. By measuring the time between right heel strikes, the distance between these strikes, and the distance from the left heel strikes, a characterization of the observed subject's walking pattern can be created. These characterizations can be differentiated between with use of data mining techniques and evaluators, such as genetic algorithms and Bayesian classifiers. [1,7]

Later systems, such as that described in *Robustness of Biometric Gait Authentication Against Impersonation Attack* attempt to use accelerometer data to create a different characterization of walking patterns. Using a fixed position accelerometer at a subject's hip, a "resultant gait signal" could be calculated from the resultant acceleration across the X, Y, and Z axis of the accelerometer. [8] While this experiment is a large leap forward towards commercially available gait recognition, this system has some differences when compared with the real world. The sampling rate for the accelerometers used in this experiment was a fixed rate. This differs from that available to Android systems, in that it allows for regular polling with predictable results. Additionally, this system was only tested on indoor lab conditions.

The paper that inspired this thesis is *Cell Phone-Based Biometric Identification*. [17] *Cell Phone-Based Biometric Identification* describes a method for differentiating users by taking 10-second samples of the accelerometer data on a phone while a user walks around with the device in their pockets. When using only a single sample, the authors report 90.9% accuracy after taking 4,866 samples from 36 users. [17] This system is studied further in my paper, and will be discussed again in the implementation section. The other paper relies mainly on cross-validation as a means of accuracy measure. While cross-fold validation is good for determining the accuracy of an evaluator, it does require the initial sample to be representative of future samples.

Cell Phone-Based Biometric Identification was not the first attempt to perform such gait recognition. The article *Personalization and user verification in wearable systems using biometric walking patterns* produced a system with even higher accuracy. [6] However, this accuracy was acquired using rigs attached to the chest of users, rather than under the normal conditions of smartphone usage. This paper was interesting because it used a multi-stage analysis, starting with a determination of what activity the user was participating in (walking, climbing stairs, etc.) followed by a determination of which user was using the device. By splitting the data-mining portion of their technique across multiple evaluations they were able to boost their accuracy significantly when they had larger numbers of data points. One very interesting portion to this article was that while an initial round of testing was done entirely within a laboratory setting, the results were repeated using less customized rigs in a 'wild' scenario. According to the article, as the number of users are added to the system is increased, the error rates rise. Additionally, they claim "A general verification system considering just authorized users[‘] patterns is not feasible, since FAR [False Acceptance Rate] will undoubtedly increase due to the fact that there is more feature space considered as authorized.” [6] Similarly to *Cell Phone-Based Biometric Identification,* this research also used cross-validation techniques for estimating the accuracy of their evaluator function.

Chapter 4. Contributions

This thesis expands on previous work in the field by reproducing and extending a modern biometric identification technique by testing it under real-world conditions. Additionally, a discussion of anti-theft as a practical application of this technique is addressed.

This work contributes by testing an existing evaluation method under real-world conditions, rather than lab conditions. The case studies associated with this work were done over several days for a small set of users, allowing us to observe patterns of accuracy over time and in different environments. Because of this, we can see how day-to-day differences in phone orientation, footwear, and activities can make a major difference in results. Additionally, we observe users acting out a normal routine, rather than simply walking a track under observation. Some previous works did do outdoor studies; however, these studies often used cross-validation to evaluate their systems, which does not take into account issues that may arise when having a training set under different conditions than a test set.

This paper also adjusts a known evaluator to address what is known as the masquerading problem. The masquerading problem centers on whether or not a user is who they claim to be. This differs from the identification problem in which the difficulty lies in determining which user the sample belongs to. Using the evaluator to determine whether or not a data-point belongs to a specific user, rather than testing which user provided the data point affords review of data over multiple days. The researcher can get a good idea of how the system varies from user to user, and get a better idea of the challenges involved with applying the evaluator under non-laboratory conditions

While both this work and previous efforts have used biometrics to identify users, previous works have generally only suggested using the identification system to gate whether a user may access a device, similarly to how pin-based authentication currently works on these devices. While these techniques can prevent access to a user's data, they do little to protect the device itself if stolen. This paper seeks to address this weakness by proposing "notification systems" for device recovery and theft-deterrence.

Chapter 5. System Design

When describing the system design, it is important to consider the use case. High interaction systems are less likely to be used, as people do not generally want to spend excessive amounts of time focusing on the security of their devices. The ideal system by our design would be a system that automatically retrieves a stolen device. While that is not possible, deterring theft, notifying users of stolen devices, and improving the ability of local authorities to take appropriate action for thieves are all useful to reduce smartphone theft.

5.1. Use Case

In order to meet this use-case, we need several components: an application to run on the physical device, providing for user interaction and other inherent needs, an evaluator to determine whether or not an authorized user is using the device, and a notification system to take appropriate action to notify the user and to deter theft.

5.2. Evaluator Needs

The needs of our evaluator are straightforward: the evaluator simply needs to detect when a user other than the authorized user is in possession of the device. Because the goal of this paper is specifically to look at the practicality of using gait recognition systems; therefore it was stipulating that the evaluator must use gait as the principle decider methodology.

Several evaluators are described in the related work presented in this thesis; however; time constraints make it difficult to re-implement and test each one. As such, one described by *Cell Phone-Based Biometric Identification* was selected for this project. This system was best documented for reproducible results, as the authors detailed their evaluation system with enough clarity to develop a new implementation of the evaluator. Additionally, the system uses easily accessible, open-source data mining tools which are readily applicable in an academic environment.

5.3. Notifications

The goal of developing a system to reduce the prevalence of cell-phone theft provided multiple possibilities for addressing the needs of a notification system.

Remote kill switches have been proposed in states such as California. [3] While the laws requiring such tools are still in their infancy, they provide an option for action taking that reduces the utility of a stolen device. Remote kill switches do not aid in device recovery, but they reduce the value of theft and could deter potential thieves.

One of the simplest methods to respond to a failed authentication is to provide a basic notification of suspicious behavior. If the device detects suspicious activity, the main user can be sent an email or other notification to alert them to the theft. The user can then determine appropriate activity. This notification system could be further supplemented by GPS data or other techniques, such as providing the option for a remote kill switch.

A slightly more complex system that could provide for more immediate response, in an area where quick response is key is the use of trust-chains. By setting up an emergency contact: a user can trust that person to quickly determine whether the appropriate user is using the device by sending them an SMS (Short Message Service) message. If the user is able to unlock the phone, respond as the user normally would, and tell them not to disable the device, they should be trusted. Otherwise, if the device is being walked with, not authenticated as the main user, and unable to respond to the selected emergency contact, severe action can be taken. This is similar to the simple notification system with options given to the user, except that it provides for more agility. It is also superior to a simple shut-down system, because it requires a human to oversee more extreme measures such as GPS reporting and kill switch flipping, as both of these actions have strong negative effects when triggered in poor circumstances.

A system could be imagined where a user is required to enter a pin or password when the biometric evaluator reports suspicious activity. Locking, killing, or remote report of GPS coordinates could then be a consequence of failed authentication. This could cause major problems if the user forgot the password, but this system could be supplemented by adding an extra layer between notifying up the trust chain and a false rejection of an authorized user. In other words, this system could decrease the negative consequence for non-device users being trusted. This may also give a false-sense of excess security, as there would now essentially be two forms of negative authentication required to perform any anti-theft behaviors.

Chapter 6. Implementation

Filling the system design requires several choices to be made. We need to choose an evaluator, we need to determine what portions of the design are necessary for testing a proof of concept, and we need to limit the scope so that we can focus the appropriate amount of resources on evaluation, rather than software engineering.

6.1. Prototype Limitations

Because the prototype implementation provided here is a mere proof of concept, it is limited in scope. This is most noticeable in the system's user-friendliness. The UI was not a focus of concern in this stage of development, and while user-interaction is an important issue for the product, it is not an area of focus for this research project..

The study is limited to a single application platform because repeated implementation on multiple types of devices would take considerable resources. The device is implemented for Android largely because of previous developer competences; however the decision was also influenced by the relative "open-source" nature of the device and easy access to accelerometer data. This was convenient as the paper *Cell Phone-Based Biometric Identification* also used Android phones for testing their system. One minor drawback of this system is that Android devices differ in size, shape, and weight, which may affect results. The studies here do not include attempts to differentiate between the same user on different Android devices; however, the suspicion that users using different Android devices may be easier to distinguish remains a possibility.

Additionally, finding the best notification system was left as a future challenge. Instead, the prototype system developed here uses a simple email system which directly emails the user whenever suspicious activity is detected. This does not provide for much actionable information; however, for the purposes of determining whether the system can send more meaningful notifications, this approach was sufficient.

6.2. Evaluator

The evaluator used for this project is based on the system proposed in *Cell Phone-Based Biometric Identification*. This system polled the output from each of the three accelerometer feeds of a modern smartphone over ten second windows. Each of the three accelerometer feeds in such a smartphone give units in m/s^2, the SI unit for acceleration. [12] These windows were then condensed down into statistical analyses, and sent to a storage system to be analyzed at a later date. The original researchers ran this system while users walked and performed other activities with smartphones in their pockets. In this test, each axis was polled 20 times per second. These 10 second samples were analyzed for 43 statistical features as follows:

- **Average:** The average value of the individual recordings for each axis. These values provide an idea of the overall orientation of a phone while a user interacts with the device. The averages here are useful for users who consistently carry a device in similar positions, but can lead to overly confident results in cross-validation because of devices remaining at similar orientations during a single travel event. In other words, a user may have placed their phone in their pocket during a trip, facing outward towards the world and with the device facing down, but when they walk again on another day they may position the device towards themselves, which would give a highly differentiated result on this data point.
- **Standard Deviation:** The standard deviation for each axis. This gives an idea of

how much movement occurs in the window. While the original paper used standard deviation without any special treatment, some of the experiments done in this work use gaiting on standard deviation to filter points where the device is sitting still. The method used for filtering points will be described in the experiment section, along with an explanation for why this is necessary.

- **Average Absolute Difference:** The average absolute difference for each axis is recorded. This is a measure of variance, which compares each value against every other value in the samples, then takes the average of these differences. This is similar to standard deviation, but because it is calculated differently, it is not used to remove non-movement points.
- **Average Resultant Acceleration:** The average resultant acceleration is calculated as follows: avg(sqrt(x^2+y^2+z^2)). X, Y, and Z are then all values of each accelerometer in the 10 second window. In practice, this means that 200 samples from the x, y, and z are pumped into this equation, with only a single resulting number. Similar to the two above measures, this gives another idea of the amount and type of movement detected by the system.
- **Time Between Peaks:** Activities such as walking tend to cause wave patterns in motion. Because of this, the time between peak values of x, y, and z accelerometer readings can each be used to calculate a wave period. This value is an average of the time between peaks for each of the three accelerometers, and gives a rough idea of the peaks perceived in the walking.
- **Binned Distribution:** On each of the three accelerometers, we divide the collected values into 10 bins. Essentially, a histogram of the data is produced;

however, the final data recorded is as a percentage of total data points in each bin, rather than the raw number of data points in each bin.

These outputs are stored on a remote server before being analyzed by the evaluator. This technique is useful on the scale of these pet projects, but a carrier-wide network would have significant tolls on both the wireless medium and server space for running these programs. However, because the evaluator uses far more resources to train on an initial dataset than to continuously address new data points, it is possible that a low power version of the system could be adapted for local use on smartphones. After collecting 4,866 10 second samples from the 36 users under lab conditions, participants were instructed to perform only one type of behavior, such as walking, the researchers generated a neural network using the WEKA data-mining tool to classify the users. While the original authors experimented with a few different data-mining techniques, the application used in the experiments presented in this work use the neural network technique. This is used to select between the list of known users in order to identify which user was responsible for each provided data point. Using 10-fold cross validation, the researchers of this original evaluator were able to correctly match 90.9% of data points to the appropriate user. Please note that all references to samples or data points in the remainder of this paper refer to the 10-second window samples, and not the raw X, Y, and Z readings at any given moment in time.

In the results section, some minor modifications to the evaluator are described. These were implemented and used in later rounds of testing. In future work, more suggestions for improvements are listed, though they have not been implemented.

6.3. Application

Because the system designed for production needs to be modified to run on real-world test conditions, a few details have been changed. The data is uploaded to a remote server as normal; however, rather than performing cross-validation studies only, we can provide both a training and anti-theft stage to the application. Users run the training stage over the course of a number of days so that the system learns to identify them, after which the system can be shifted to the anti-theft stage, where each data point sent to the server receives a response saying whether the neural network appropriately identified the user as the expected user. If so, the device continues recording, and sends another point to be evaluated every 10 seconds. If not, the system can take appropriate action to notify the user of suspicious activity. In order to easily reduce the rate of false positives, the system can be adjusted to require successive negative identifications before taking action. The implementation provided used three successive failures as the cutoff for inappropriate behavior, but this number was not studied further and would need to be tuned based on the evaluator's accuracy.

Chapter 7. Experiment Set Up

To test the system, two stages of testing were used. In an initial test, we gathered 10,071 data points from 11 users. The servers for initial collection were run for just over 24 hours to give participants time to close the application appropriately and send late data points. Each user was instructed to download the Android application and collect data.

The number of participants is slightly lower than the number of participants in *Cell Phone-Based Biometric Identification*; however previous works such as *Personalization and user verification in wearable systems using biometric walking patterns* also relied on sample sizes of either 10 or 20 depending on the specific study. Increasing the user count leads to lower accuracy, and because the goal of this system is only to determine whether or not an individual is or is not a user, rather than to determine *which* user is using the system, the number of participants is less important than the overall number of data points. [6] Having more participants might help to reinforce claims regarding accuracy of the system across many users, but the findings from the studies already suggest that the accuracy is quite low when the evaluator is applied to real-world conditions.

Each data point represented a statistical analysis of a 10-second window of information on the accelerometer from an individual user. Because we are basing our identification system on that proposed by *Cell-Phone Based Biometric Identification* we have a baseline of accuracy to compare our results again when investigating using 10-fold-cross validation.

In the second test, three users were monitored across multiple days. They ran the program and sent data to the server to show the effects of different environmental factors influencing the accuracy of the evaluator system. Additionally, this provided an opportunity to test the evaluator in a non-cross-validated setting.

Note that users will not be referred to by any personal identifier, as this was a part of the agreement listed with the consent forms for the project.

Chapter 8. Results and Evaluations

8.1. Initial Findings

In the original experiment, we took the raw output for accelerometers across a one day sample for 15 users. Across these data, we received a total of 10071 data points, and applying the neural-network technique we found an overall accuracy of 79.0% when addressing the identification problem. These results were initially comparable to the results of previous works, with a slight accuracy drop. The accuracy drop can be attributed to different test conditions, as the original work had users perform a specific task, such as walking, running, or jumping while holding the device whereas this experiment was an attempt to identify a user regardless of action. Unfortunately, manual inspection of the results showed that a 78.5% of these data points were devices sitting still with no user-interaction. Devices sitting still for hours on end send us data points as normal (at least during this stage of the experiment), which means that any two points from such a period of time are interchangeable, and when used in cross-validation, make them easy for neural networks to pick out. In a non-cross-validated study, using a test-set that was different from the original training set, these points would be difficult to identify. Because of this, future experiments use a filter to remove points with no, or very low, movement by filtering points with standard deviations in the x, y, and z directions less than .1.

```
    a    b    c    d    e    f    g    h    i    j    k
 1049   11   63    7    4   66   44  109   20   11    1 |    a
    7    5    0    0    0    0    5    1    1    0    0 |    b
   42    4 1122   10    0   60   20    3   26    1   13 |    c
   20    1   15  238    0   63   21   55    1    0    5 |    d
   11    0    2    1   82   63    5    1    3    1    1 |    e
   70    4   73   48   17 3106   68  118   25   14   64 |    f
   42    3   68    9    0  123  169   97   12    3    9 |    g
   34    0    6    1    0   43   22 1112    0    4    1 |    h
   31    3   12    1    0   69   31   17  163    1    5 |    i
    5    0    0    0    0   21   11   19    0    9    0 |    j
    3    2    3    6    3   69   13    1   10    0  904 |    k
```

Figure 1. Confusion matrix for first round of evaluations as totals.

```
    a     b     c     d     e     f     g     h     i     j     k
0.757 0.008 0.045 0.005 0.003 0.048 0.032 0.079 0.014 0.008 0.001|   a
0.368 0.263 0.000 0.000 0.000 0.000 0.263 0.053 0.053 0.000 0.000|   b
0.032 0.003 0.862 0.008 0.000 0.046 0.015 0.002 0.020 0.001 0.010|   c
0.048 0.002 0.036 0.568 0.000 0.150 0.050 0.131 0.002 0.000 0.012|   d
0.065 0.000 0.012 0.006 0.482 0.371 0.029 0.006 0.018 0.006 0.006|   e
0.019 0.001 0.020 0.013 0.005 0.861 0.019 0.033 0.007 0.004 0.018|   f
0.079 0.006 0.127 0.017 0.000 0.230 0.316 0.181 0.022 0.006 0.017|   g
0.028 0.000 0.005 0.001 0.000 0.035 0.018 0.909 0.000 0.003 0.001|   h
0.093 0.009 0.036 0.003 0.000 0.207 0.093 0.051 0.489 0.003 0.015|   i
0.077 0.000 0.000 0.000 0.000 0.323 0.169 0.292 0.000 0.138 0.000|   j
0.003 0.002 0.003 0.006 0.003 0.068 0.013 0.001 0.010 0.000 0.892|   k
```

Figure 2. Confusion matrix for first round of evaluations as percentages.

The above confusion matrix shows a list of users A-K. Numbers in Figure 1 show that X number of data points for the user, shown on the far right of the row, were identified as the user shown at the top of that column. For example, 11 data points produced by User A were identified as belonging to User B. In Figure 2, the data point instances are replaced with percentages. The percentages help to give a better picture of the correct identification rates, but the absolute number of accepted samples has been included because it helps to highlight that the behavior of this system is heavily affected by the number of data points available for each user.

The matrix above reveals that some users provided only a low number of data points, even before filtering. Such users showed abysmal low true positive rates (The percentage of data points accurately identified as a given user, the inverse of the False

Rejection Rate), as low as 6.33% for user e. Users with many data points, such as f and h saw true positive values of 86.1% and 90.9% respectively. As such, further evaluation on our original data set also filtered out users below a threshold of 100 data points post filtering of the non-movement points.

8.2. Adjustments and Further Results

Restricting adjustments for data points with low or no movement detected, provided the results shown below in figures 3 and 4.

```
   a   b   c   d   e   f   g   h   i   j   k
 357   8  14  11   1  64  26  19  10   6   8 |
   6   9   0   0   0   1   3   0   0   0   0 |   b
  18   2  94   5   0  14   5   1   8   0   0 |   c
  21   1   2  20   0  21  10   8   2   0   1 |   d
   8   1   1   2   3  22   6   0   3   2   0 |   e
  62   1  11  16   9 412  33  18  14  17  29 |   f
  36   6   6   7   2  45 107  12   7   3  11 |   g
  16   2   2   3   0  25   3 106   0   3   1 |   h
  31   2  19   3   4  26  17   1  69   0  15 |   i
   1   0   0   0   1  24   6   1   1   5   1 |   j
   3   0   1   2   3  32   6   1   3   0  34 |   k
```

Figure 3. Confusion matrix for first round of evaluations, post-filtering data points with low movement as totals.

```
    a     b     c     d     e     f     g     h     i     j     k
0.681 0.015 0.027 0.021 0.002 0.122 0.050 0.036 0.019 0.011 0.015|
0.316 0.474 0.000 0.000 0.000 0.053 0.158 0.000 0.000 0.000 0.000|    b
0.122 0.014 0.639 0.034 0.000 0.095 0.034 0.007 0.054 0.000 0.000|    c
0.244 0.012 0.023 0.233 0.000 0.244 0.116 0.093 0.023 0.000 0.012|    d
0.167 0.021 0.021 0.042 0.063 0.458 0.125 0.000 0.063 0.042 0.000|    e
0.100 0.002 0.018 0.026 0.014 0.662 0.053 0.029 0.023 0.027 0.047|    f
0.149 0.025 0.025 0.029 0.008 0.186 0.442 0.050 0.029 0.012 0.045|    g
0.099 0.012 0.012 0.019 0.000 0.155 0.019 0.658 0.000 0.019 0.006|    h
0.166 0.011 0.102 0.016 0.021 0.139 0.091 0.005 0.369 0.000 0.080|    i
0.025 0.000 0.000 0.000 0.025 0.600 0.150 0.025 0.025 0.125 0.025|    j
0.035 0.000 0.012 0.024 0.035 0.376 0.071 0.012 0.035 0.000 0.400|    k
```

Figure 4. Confusion matrix for first round of evaluations, post-filtering data points with low movement as percentages.

Overall accuracy for the identification problem dropped to 56.3% in the example. This drop can be largely attributed to the loss of the false-accuracy given by considering the number of hours of still phones, which skews our data, as two points of a device sitting in the same position for a given period of time will be nearly identical. However, this accuracy drop has pretty rough ramifications for how useful a gait-based recognition system will be as part of an anti-theft system. As discussed above, many of these users have sharply less available data points than others. Excluding these users, we get the results shown in Figure 5.

```
   a   b   c   d   e   f
 367  17  72  30  20  18 |   a
  21  87  14  11   1  13 |   b
  71  14 452  39  22  24 |   c
  46   5  61 115   6   9 |   d
  17   3  30   4 107   0 |   e
  20  10  26  24   2 105 |   f
```

Figure 5. Confusion matrix for first round of evaluations, post-filtering users with low amounts of data and data points with low movement as totals.

```
    a     b     c     d     e     f
0.700 0.032 0.137 0.057 0.038 0.034|   a
0.143 0.592 0.095 0.075 0.007 0.088|   b
0.114 0.023 0.727 0.063 0.035 0.039|   c
0.190 0.021 0.252 0.475 0.025 0.037|   d
0.106 0.019 0.186 0.025 0.665 0.000|   e
0.107 0.053 0.139 0.128 0.011 0.561|   f
```

Figure 6. Confusion matrix for first round of evaluations, post-filtering users with low amounts of data and data points with low movement as percentages.

After applying this filter, the overall accuracy rises to 65.5%. This result is somewhat disappointing as the participant group has been reduced to a smaller number of users, which normally should increase accuracy. This unfortunately shows a strong trend of the cross-validation evaluation technique leading to skewed results when the device was at rest. For all users except User D, the true positive rate exceeds 50%, indicating that the user can be correctly identified more often than not. There is no other circumstance in which any user’s data consistently get recognized as another specific user’s, as Figure 1’s results for User B, who was identified more frequently as User A.

As indicated by the information presented in the above section, it is likely that the gulf in accuracy between this experiment and the original results presented in *Cell Phone Based Biometric Identification* describing this evaluator was a result of non-laboratory conditions. The researchers of this paper had users specifically walk, run, stand still, and perform other activities, only testing like activities against like activities, while the experiment here had users act out their normal routine, to get an idea of the accuracy of this evaluator in a real-world scenario across multiple activities. Because of this, another option for increasing accuracy: reducing the system to a one vs-all system rather than a one-vs-one-vs-etc was investigated.

8.3. One-vs-All

In order to provide higher accuracy rates, the system was modified to evaluate 1 user vs another user defined as "other" which is made up of the components of all other users. In other words, we train the neural network on the same data set used in figure 2, but replace all names with other, except those for the specific user being studied. This permutation showed interesting results, but the results differed from user to user.

When comparing the accuracies from the identification problem shown in the confusion matrix, Figure 5. above, we see the following difference for User A after switching to the one-vs-all technique. The accuracy for user a below adjusts from a True Positive rates of 66.5% and FAR of 3% to a TP rate of 62.7% and an FAR of 1.8%. The overall accuracy also increases from 55.8% to 95.6%, as determining which non-authorized user is no longer taken into account. However, as this calculation of one-vs-all includes all data points used in Figure 3, a more accurate comparison would be the user's increase change of 65.8% TP and 3.1% FAR to 62.7% TP and 1.8% FAR with overall accuracy shift of 56.3% to 95.6%. While the small change may not sound like a major factor, and the decrease in TP is concerning, the rate of FAR's being decreased is a significant boon, as in this cross-validation, the number of other data points is much higher than the number of points for our users.

Because this method of one-vs-all reveals different results from the traditional technique, rather than flat improvement or degradation of quality, we performed some case studies on individual users to get a better idea of what using the system is like in real-world use over a longer period of time.

8.4. Case Studies

Because the one-vs-all showed interesting results that were not investigated in previous papers, the decision was made to undertake further investigation. Because these studies required tuning for individual users as well as continued involvement for volunteer research participants, the studies have been acted on as case studies and will be treated on individual basis, rather than by looking at aggregate data across all users as in the previous experiments.

8.4.1. User A

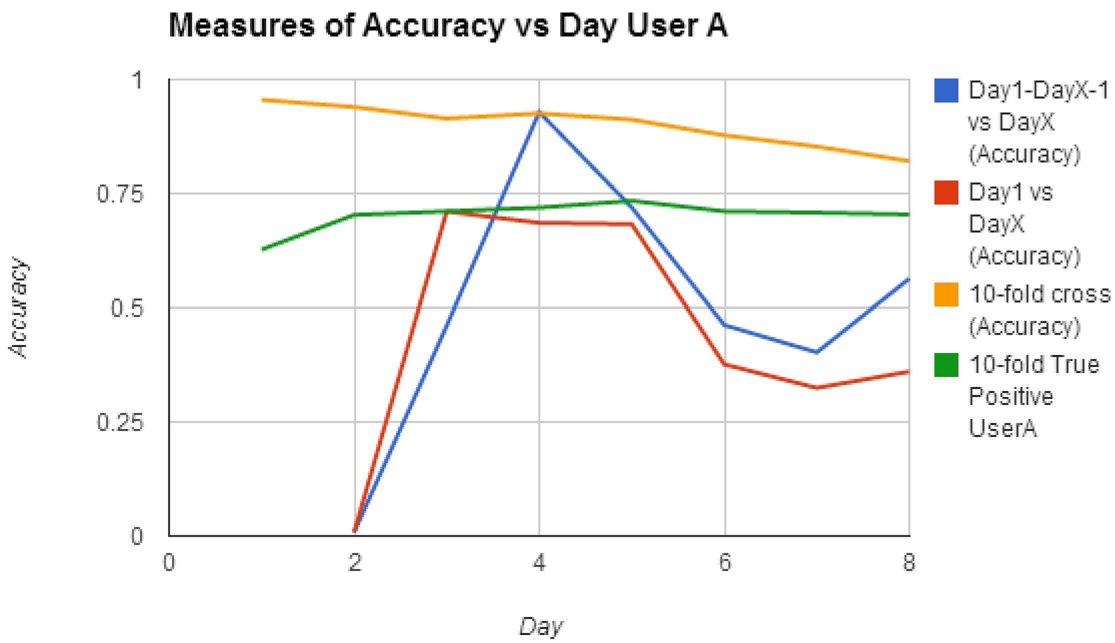

Figure 7. Measures of accuracy vs. day for User A.

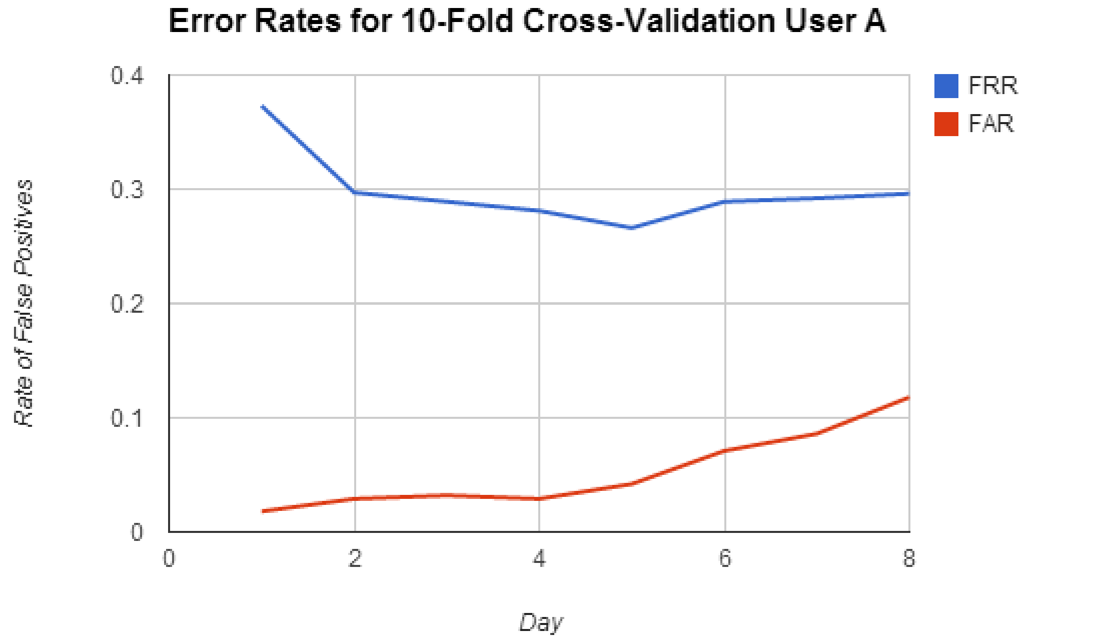

Figure 8. Error rates for 10-fold cross-validation User A.

User A uses a backpack to hold the device. The user generally walked or stood still while using the device, not driving or behaving in other non-walking forms of transportation in her normal schedule. As the graph shows, adding more points and looking at the aggregated data about the user up to a specific day shows higher accuracy than relying on the accuracy of only one day of training, however this gap does not appear to grow significantly over time, contrary to what one would expect.

Note that the accuracy for days such as day 2, day 6, and day 7 fall far short of the true positive for user A on the same date. This seems likely to be a result of cross-validation being far more accurate than doing training set on a set of data followed by a test-set in a real-world scenario. This creates some issues, as previous walking behaviors do not appear to perfectly predict the user's future walking patterns. This additionally explains the abysmal rates recorded on the second day for each user, when as compared to the cross-validation accuracies of the first day.

Additionally, the false positive authentication rates over time increase. This make intuitive sense, as more and more points are identified as valid behaviors for the user, more behaviors that other users also engage in will be included. Toward the beginning of the training process the system responds conservatively, with low false positive and true positive rates. As the system receives more points for the other user, the system becomes less particular: true positives and false positives both rise for the user. This implies that if the system was to be used in the real world, the system would want to request only a specific number of data points from the user, rather than continually learning without bound.

Finally, it is important to note that the cross-validation accuracy steadily decreases. This is in large part due to the fact that the majority of data points are not the real user, so as the system becomes less conservative, its apparent total accuracy will decrease. It accepts more points in total as belonging to User A, which means that the system's security becomes more lax as it trains on larger data sets. This produces a significant tradeoff, as the system becomes less useful as a theft-deterrent as FAR rises, but becomes less user-friendly as FRR rises.

8.4.2. User B

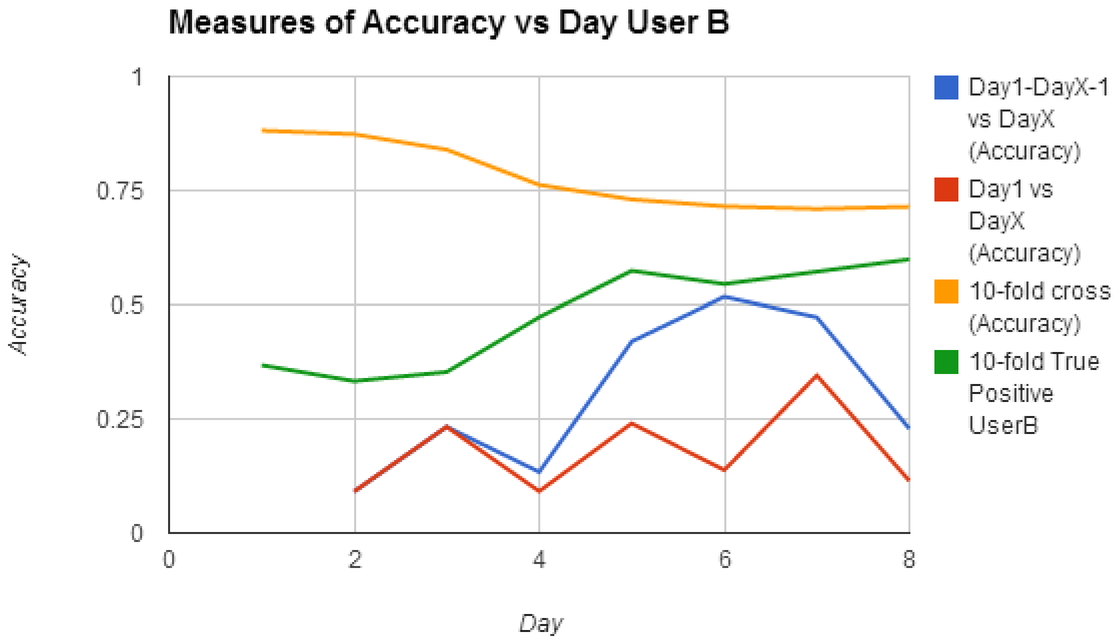

Figure 9. Measures of accuracy vs. day for User B.

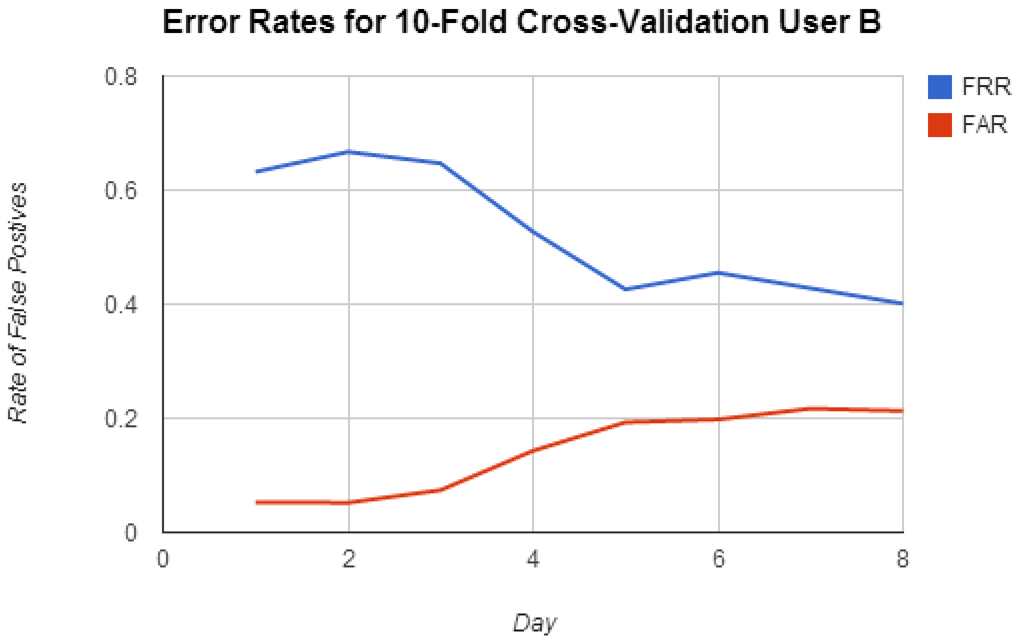

Figure 10. Error rates for 10-fold cross-validation for User B.

User B carries the device in a pocket. The user also spends time with the device both walking and driving. Overall, the results reflect sharply less accuracy than that shown for User A. Despite the lower accuracy, the overall trends as more data points are added make more sense with our initial claims. There exists a sharp inverse correlation between FAR and FRR in the second graph, which means the system becomes less and less conservative as time goes on. There is also a steadily growing difference between the analysis using only day 1 data as a training set vs using all previous days as training data. When these datasets are similar, the accuracy difference is low; however, as more data points are added, this gulf grows, until day 6. Interestingly, this is near the point where FAR and FRR cease to inversely correlate. This all said, overall cross-validation accuracy falls as time goes on, similar to the results for User A.

8.4.3. User C

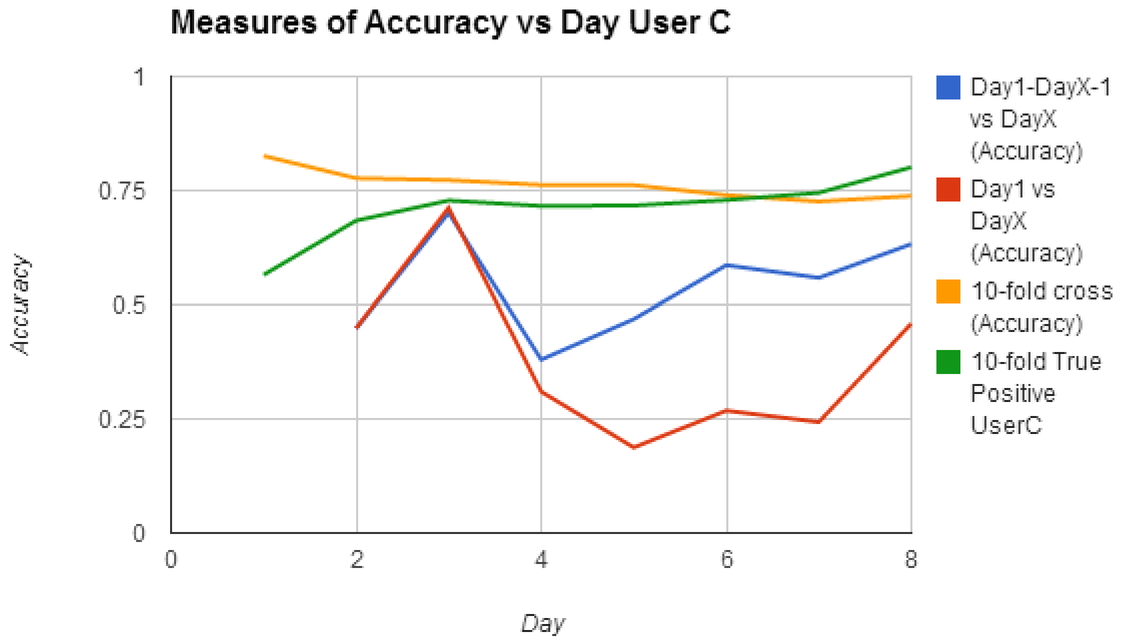

Figure 11. Measures of accuracy vs. day User C.

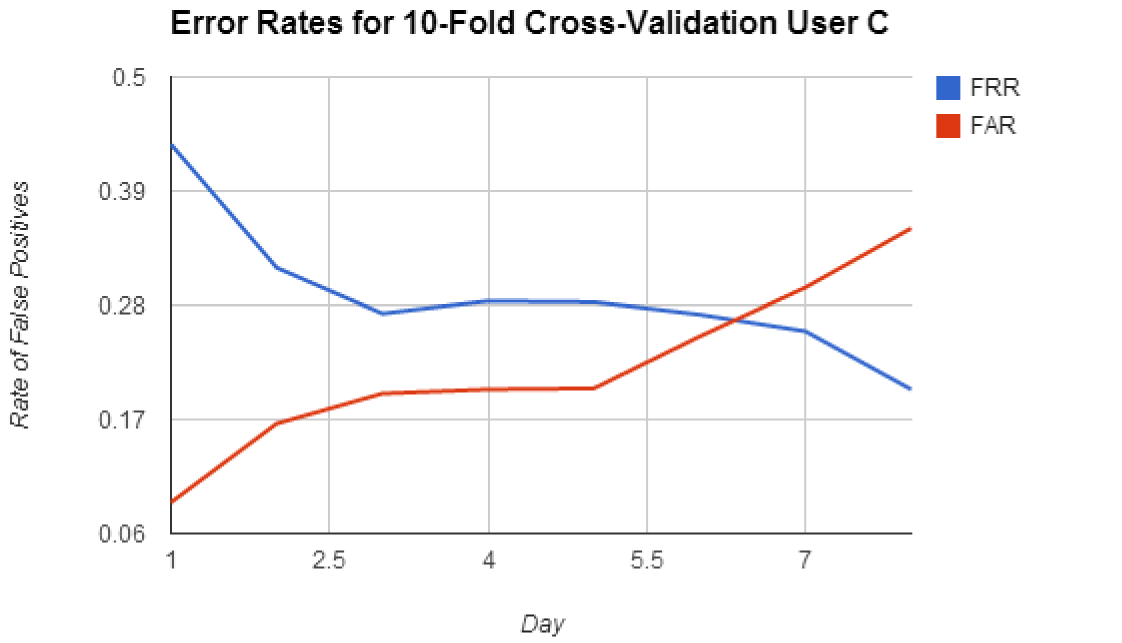

Figure 12. Error rates for 10-fold cross-validation User C.

Users B and C show very similar usage patterns. Both normally carry their device in pocket, drive regularly in their daily routine, and also have large periods of walking. However, there are large differences between their rates. Overall accuracy and true positive rates are much higher for User C, but the false positive rate rapidly approaches 20%. There is a similar pattern for FRR and FAR as recorded for User B, but we can see that the pattern ends for the first time around day 3. Unlike in the previous graphs, after a period of stagnation, the FRR continue to fall and the FAR continue to rise. Part of the reason for this second tier fall-off is the number of data points gathered by this user. The walking routine of this user was much higher, which actually led the number of data points for this user to exceed the number of data points for all other users towards the end of the study. As shown above, this leads to a much higher true positive rate, as more and more points overall are classified as belonging to this user. However, this leads to over 30% of data points belonging to other users being mistakenly classified as belonging to User C.

Chapter 9. Future Work

The field of gait-recognition using cell-phones is still emerging. As illustrated here, there is significant technical progress to be made, particularly in the field of evaluators. This section describes some potential areas to focus on in future studies in this field.

9.1. Implementation Improvements

While the system proposed herein has accuracy below optimum levels, there are many improvements that could be made.

9.1.1. Automation of Re-Training Process

Currently, the system requires many manual actions to train the system for a specific user. While a blanket automation of all of these stages would make for a system much more ready for the real world, some of these changes would be non-trivial. Specifically, while automating the initial training of the system would be relatively simple if it included a requirement of a few days of user input before initiating the decider portion of the program on the given data Creating a system that can adapt to changes in user gait is a bigger issue. The study in Figure 1 reveals that occasionally users will see a large burst of activity significantly different from their original activity. While the impact of this can be mitigated manually by retraining the system on the new data, it is much more difficult for an automatic system to make a decision that the system needs to retrain, rather than to report suspicious activity.

The most obvious solution to this issue includes using the phone's notification system (whether email, chain-of-trust notification, or another system) to alert the user to any suspicious activity, including cases where the system may need to be retrained. Once the user has been notified, they could then be prompted with options including system retraining, in addition to the standard ignore and report functions. An example using chain-of-trust notification: User A trains the system on himself and uses the phone normally, but breaks his leg during normal use and the system notifies his trusted contact, User B. User B then uses another method to contact User A, who can inform User B about which action to take. User A should then make a judgment call to set up the re-train function so that the device can learn to recognize his walking patterns while in a leg cast. User B as the trusted user would select the appropriate option and the system would enter retraining mode for a pre-set period of time. Other options for automating the re-training process can be imagined, and the notification system can be replaced with simple email to User A, replacing the need for communication between users; however, the base of providing an option to retrain to a trusted user remains viable. This option, like all of the notification systems, should be backed by another authentication form, such as a mundane password.

9.1.2. Multi-User Acceptance

Some smartphones will be used regularly by multiple people. While it is beyond the scope of this initial study to determine how this may affect the accuracy of our system, it is reasonable to expect that a production-quality version of the system will require a solution for this use case. There are a few possibilities for how to address this issue. One solution is to use the project system, and have data points from each of the authorized users as part of the training data as a single "user" in the system. This could work, but would require testing before any confidence is a reasonable expectation for the strategy. Another simple approach would be to train the system with multiple users, having a “User A”, “User B”, “User…X”, and an “Other” category. Any successful authentication for a non-”Other” user would be taken as a success, while repeated “Other” cases would lead to a notification. One potential issue with this solution is that notification becomes slightly more complicated, as chain-of-trust becomes a challenge, due to the need to identify someone that all users can trust. Additionally, the above solution of re-training would have to be available for each user.

9.2. Future Research Areas

9.2.1. Normalization by Device Type

Because individual Android device models have differing sizes, weights, and shapes, it is likely that they would not detect the exact same motion for the same user. Testing the same user on multiple devices, or testing whether device type difference makes it more likely to detect differences between users would help to evaluate the practicality of using these different sensors to collect the same data. If device type makes a larger impact than user, this technology will be significantly less useful, but if the effects are small, it would suggest that this research may become useful if a method for improving accuracies, such as determining activity type before differentiating between users, might be applicable in the real world.

9.2.2. Comparison of Evaluators

Testing the system I have proposed with the evaluator replaced with other modern evaluators might show different results. While the applied technique showed some promise, it does not appear to be accurate enough for reliable anti-theft. However, it’s very possible that analysis from another decider system might be more conducive to the goals of this experiment. In particular, determining activity prior to attempts to identify the user might show a marked increase in accuracy and decrease in FAR rates.

In particular, the sample size has not been thoroughly tested. 10 seconds matches the work of *Cell Phone Biometric Identification*, but even that article points out that the number is not necessarily optimal.

9.2.3. User Interaction Concerns

False negatives have a chance of being strongly negative toward a user experience. While the functional goals of the system require low false positive rates in order to quickly respond to potential thefts, false negatives have the potential to cause major issues for the user. Spending time managing false notifications, panicked attempts from emergency contacts to reach the user, and even disabling of phones are possible results in each of the notification systems proposed here. Regardless of how notifications are handled, there will be downsides to false negative interactions. Finding a rate of false negatives that is acceptable to users is something not tested here, and will require further studies as evaluators approach real-world needs in accuracy.

Another major user interaction concern is that the system has not been tested on users with disabilities. It is very likely that a system designed around analyzing gait and other behaviors with regular movement would behave wildly differently when applied to a different movement pattern, such as moving a wheelchair.

Chapter 10. Conclusion

While the concept of an anti-theft system has not been outright dismissed by this research project, the work does reveal some major technical hurdles that have not been addressed by the modern gait recognition technique applied. Using the system of user gait identification proposed by *Cell Phone-Based Biometric Identification*, we run into major hurdles when addressing test sets which differentiate from our training set. The accuracy of gait recognition techniques appears to be highly dependent on consistent human behavior, which the results of this study suggest are not necessarily accurate.

Gait recognition has been proven to be useful for certain application spaces, such as recognizing users of traditional pedometer systems from a set list of users; however, trying to identify a specific user among the population of the earth is a more difficult problem.

This study shows that tests performed under non-lab conditions show much lower accuracies than studies performed under uniform lab conditions. In particular, identification is much less accurate when we don't know what behavior a user is performing. Previous work in this field has focused heavily on proving that if the user is specifically engaged in a particular physical activity (walking, running, jumping). Users engaged in a defined activity can be differentiated between their action and another user performing the same action, and, this study shows that it is difficult to identify users without identifying what behavior they are engaged in. This may the results of tendencies of arm motions, holding patterns, or other features, and these results provide useful information for further research.

The project also shows that system accuracy is significantly improved when analysis is done as “is this the user” rather than a “which user is this” system, at least when using neural network analysis. However, the results reveal that the accuracies even in these conditions are quite unpredictable. Certain users show higher accuracies, some days for each user show higher accuracies, and while there are certainly trends of what factors improve the accuracy of the system, it is not possible from the data gathered here to make absolute predictions of when the system’s accuracy is likely to be at fault, rather than an actual theft attempt. With this in mind, it seems that this evaluator is not appropriate to apply to the anti-theft domain in its current state.

Bibliography

[1] BenAbddelkader, C., R. Cutler, and L. Davis. "Stride and Cadence as a Biometric in Automatic Person Identification and Verification." *Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on* (2002): 372-77. Web.

[2] Brooke, John. *SUS: A Quick and Dirty Usability Scale*. Earley: Redhatch Consulting Ltd, n.d. PDF.

[3] Brown, Dwayne. "California Legislators To Outline Bill Requiring Cell Phone 'Kill Switches'" *KPBS Public Broadcasting*. KPBS, 19 Feb. 2014. Web.

[4] Campisi, P., E. Maiorana, M. Lo Bosco, and A. Neri. "User Authentication Using Keystroke Dynamics for Cellular Phones." *IET Signal Processing* 3.4 (2009): 333. Print.

[5] "Carriers Reject Kill Switch for Stolen Smartphones." *ABC Owned Television Stations*. N.p., 20 Nov. 2013. Web.

[6] Casale, Pierluigi, Oriol Pujol, and Petia Radeva. "Personalization and User Verification in Wearable Systems Using Biometric Walking Patterns." *Personal and Ubiquitous Computing* 16.5 (2012): 563-80. Print.

[7] Cunado, David, Mark S. Nixon, and John N. Carter. "Automatic Extraction and Description of Human Gait Models for Recognition Purposes." *Computer Vision and Image Understanding* 90.1 (2003): 1-41. Print.

[8] Gafurov, D., E. Snekkenes, and T. Buvarp. "Robustness of Biometric Gait Authentication Aainst Impersonation Attack." *OTM Workshops* (2006): n. pag. Web.

[9] Gaines, R., W. Lisowski, S. Press, and N. Shapiro. "Authentication by Keystroke Timing: Some Preliminary Results." (1980): n. pag. Web.

[10] Gershenson, Carlos. *Artificial Neural Networks for Beginners*. N.p.: n.p., n.d. PDF.

[11] Giroux, S., R. Wachowiak-Smolikova, and M. P. Wachowiak. "Keystroke-based Authentication by Key Press Intervals as a Complementary Behavioral Biometric." *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on* (2009): 80-85. Web.

[12] Gross, Doug. "Apple Adding 'kill Switch' to IPhones." *CNN*. Cable News Network, 11 June 2013. Web. 13 June 2013.

[13] Hayfron-Acquah, James B., Mark S. Nixon, and John N. Carter. "Automatic Gait Recognition by Symmetry Analysis." *Pattern Recognition Letters* 24.13 (2003): 2175-183. Print.

[14] Hayfron-Acquah, James B., Mark S. Nixon, and John N. Carter. "Automatic Gait Recognition by Symmetry Analysis." *Pattern Recognition Letters* 24.13 (2003): 2175-183. Print.

[15] Kerr, Dara. "New York AG to Cellular Carriers: Why Was Antitheft Switch Killed?" *CNET*. N.p., 11 Dec. 2013. Web.

[16] Kohavi, R. "A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection." *A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection* (1995): n. pag. Web.

[17] Kwapisz, J.R, G.M Weiss, and S.A Moore. "Cell Phone-based Biometric Identification." *," Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on* (2010): 1-7. Web.

[18] Monrose, Fabian, and Aviel D. Rubin. "Keystroke Dynamics as a Biometric for Authentication." *Future Generation Computer Systems* 16.4 (2000): 351-59. Print.

[19] "MotionEvent." *Android Developers*. N.p., n.d. Web. <http://developer.android.com/reference/android/view/MotionEvent.html>.

[20] "MultilayerPerceptron." *MultilayerPerceptron*. N.p., n.d. Web. <http://weka.sourceforge.net/doc.dev/weka/classifiers/functions/MultilayerPerceptron.html>.

[21] Pal, S.k., and S. Mitra. "Multilayer Perceptron, Fuzzy Sets, and Classification." *IEEE Transactions on Neural Networks* 3.5 (1992): 683-97. Print.

[22] Parivar, Nima, and Wayne C. Westerman. Gesture and Touch Input Detection Through Force Sensing. Apple Inc., assignee. Patent 20140028575. N.d. Print.

[23] "Reproducibility in Computer Science." *Reproducibility in Computer Science*. University of Arizona Computer Science Department, n.d. Web. 10 May 2014. <http://reproducibility.cs.arizona.edu/>.

[24] Saevanee, H., and P. Bhattarakosol. "Authenticating User Using Keystroke Dynamics and Finger Pressure." *Consumer Communications and Networking Conference* (2009): 1-2. Web.

[25] "SB 962 Senate Bill - AMENDED." *SB 962 Senate Bill - AMENDED*. N.p., 24 Mar. 2014. Web.

[26] Schneiderman, Eric T. "AT&T_Letter." Letter to Randall L. Stephenson. 10 Dec. 2013. MS. N.p. Open letter regarding killswitch technology. Available at: http://www.ag.ny.gov/pdfs/AT&T_Letter_Dec_10_2013.pdf

[27] "SensorEvent." *Android Developers*. N.p., n.d. Web. <http://developer.android.com/reference/android/hardware/SensorEvent.html>.

[28] Trewin, Shari, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. "Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption." *Proceedings of the 28th Annual Computer Security Applications Conference(ACSAC '12). ACM* (2012): 159-68. Web.

[29] Wang, Liang, Weiming Hu, and Tieniu Tan. "A New Attempt to Gait-based Human Identification." *Recognition, Proceedings. 16th International Conference on* (2002): 115-18. Web.

[30] "With 1.6 Million Smart Phones Stolen Last Year, Efforts under Way to Stem the Losses – Consumer Reports News." *With 1.6 Million Smart Phones Stolen Last Year, Efforts under Way to Stem the Losses*. N.p., 3 June 2013. Web.