Journal of Universal Computer Science, vol. 24, no. 4 (2018), 417-443
submitted: 15/12/17, accepted: 15/4/18, appeared: 28/4/18 © J.UCS

Large Scale Mobility-based Behavioral Biometrics on the Example of the Trajectory-based Model for Anomaly Detection

Piotr Kałużny
(Poznan University of Economics and Business, Poland
piotr.kaluzny@ue.poznan.pl)

Agata Filipowska
(Poznan University of Economics and Business, Poland
agata.filipowska@ue.poznan.pl)

Abstract: The paper describes an implementation of a behavioral authentication system, working on sparse geographical data generated by mobile devices in the form of CDR logs. While providing a review of state of the art w.r.t. sensors and measures that can be used when creating a system detecting anomalies in the user behavior, it also describes domain specific authorization methods focusing on the user mobility.

The trajectory based stay-extraction model is utilized to build user mobility patterns, upon which the anomaly detection model measures the repeatability of human behavior in dimensions of: geography, time and sequentiality. The goal is to measure the extent to which the geographical aspect of the human mobility can be used in behavioral biometrics' systems i.e. in which scenarios geography may enable to describe (and differentiate between) user patterns – based on anomaly detection in cases resembling real life scenarios (phone theft or sharing between users). The research methods developed may be implemented on mobile devices to benefit from multiple sensors data in the authentication processes.

The model is evaluated on a large telecom dataset, with the use of similarity classes, what allows measuring the accuracy of the model in real-life scenarios and provides benchmarking guidelines for the future work on the topic.

Key Words: anomaly detection, mobility, trajectory based model, mobile phone data, user behavior, authentication, behavioral biometrics, biometric systems
Category: H.4.0, J.4, K.6.5, K.8

1 Introduction

Nowadays mobile devices have become truly ubiquitous. Due to this fact, they became both a valuable source of information [Fox et al. 2013] and a concern to assure privacy of their owner's data. Due to reasons connected with a user's negligence, possibly caused by the usability barrier of the currently used authentication approaches [Telesign 2016], about 40% of mobile phones remain unprotected by any means [Fridman et al. 2015]. The ease of use seems to be a significant factor in the adoption of new authentication methods [Telesign 2016, Trewin et al. 2012]. This enables behavioral biometrics to improve this

process by utilizing multi-factor authentication and cover the drawbacks of the traditional authentication methods.

The goal of this paper is to propose a working model for behavior based authentication applying anomaly detection performed over the user's mobility pattern. The issue was researched by application of the methodology described by Öesterle [Österle et al. 2011].

The structure of the paper is as follows. The description of the research problem is given in the introduction, analyzing issues of current authentication approaches and behavioral biometrics as a possible solution. Second chapter defines concepts used and provides an analysis of the literature - focusing on mobility as a base for behavioral authentication. The chapter also describes the advantages of the proposed approach over state of the art. In a third chapter a trajectory based model is described, and the anomaly detection method is presented along with a division of anomalies into dimensions of: geography, time, sequence and predictability. In the fourth chapter the model is evaluated on a large real world dataset. In the last chapter, the discussion on the comparability of the existing mobility-based behavioral authentication approaches is brought up along with some practical remarks. The future work is also discussed.

2 Related work

2.1 Traditional means of authentication

Traditional authentication factors have a few drawbacks. Among these drawbacks we may distinguish:

- **knowledge factors** represented by passwords, work as a point of entry mechanism which frustrates users [Telesign 2016] mostly due to the requirement of a user interaction and the issue of "stacking up" [Yan et al. 2004, Bonneau and Preibusch 2010]. They are also often simple and easy to break.
- **possession factors** connected with token devices are a good choice for high security situations. Nonetheless, they are rarely used due to economical and usability reasons[1].
- **inherence factors** connected with traditional biometry, offer a family of high accuracy methods including fingerprint recognition or new examples of facial features biometrics. The main issue with these methods is that they are not available for all devices. Biometry adoption among the produced mobile phones achieved about 40%, but its penetration rates among companies and

[1] Users are required to carry an additional device and interact with it to gain access. They also need not to lose or forget to take the device.

users are worse [Gartner 2013, Acuity 2016]. These methods also can't work continuously due to the battery drain and/or characteristics of the methods used.

The family of traditional methods can be extended with the concept of **behavioral biometrics**. Behavioral biometrics includes a variety of methods, consisting of: gait [Damaševičius et al. 2016a], keystroke dynamics [Ulinskas et al.2017], voice recognition [Mazhelis and Puuronen 2007] and many more. One of its fields covers the behavioral profiling, which tries to derive patterns from the user's behavior and interaction with a device, which are closely resembled by the data that is produced by the devices [Aledavood et al. 2015]. Behavioral profile model can consist of many aspects with a capture-able (quantifiable) regularity, where deviations from the observed behavior can lead to uncovering anomalies connected with a potential threat to user's data [Buthpitiya 2014]. In some of those cases, domain specific algorithms can be used for capturing and comparing the patterns (e.g. voice recognition [Połap and Woźniak 2017]).

This multi-aspect characteristics[2] allows for an **easy application of behavioral biometry models in multi-layer authentication**, widely adopted in tech companies [Telesign 2016]. Due to the fact, that those methods can be applied for a constant user authentication, they do not hinder the usability, while adding an additional layer of security. This makes the use of the behavioral system a good compliment to the password based or traditional biometric solutions (which do not work well in a multi-layer authentication [Trewin et al. 2012]). These facts confirm a significant demand for the services among companies, as seen in Figure 1. Deriving insight from the behavioral patterns provides also information about the current context of the user behavior, which is important in domains where observation of a user is crucial e.g. patients, elderly people [Damaševičius et al. 2016b] in case of health care applications.

2.2 Behavioral profiling on mobile devices

The behavior (or behavioral) profiling is defined as it: *"identifies people based upon the way in which they interact with the services of their mobile device. In a behavior profiling system, user's current activities (e.g. dialing a telephone number) are compared with an existing profile (which is obtained from historical usage) by using a classification method (e.g. a Neural Network). The users identity is determined based upon the comparison result." [Li et al. 2014].* The user's profile can include multiple aspects of his behavior [Mazhelis and Puuronen 2007]. Each of these aspects can be described by one or many measures (characteristics) that can be used for the pattern creation (presented in Figure

[2] Meaning there can be multiple aspects of a behavioral profile which can be modeled with different methods and work in various scenarios.

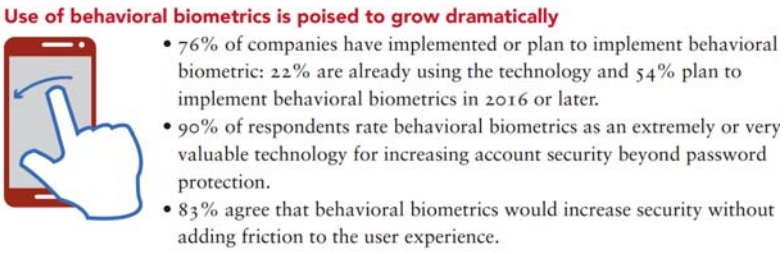

Figure 1: Findings of a report on a potential adoption of the behavioral biometrics. Source: [Telesign 2016]

2). It is clearly visible, that multitude of these factors point to a non trivial tasks of pattern recognition. An exemplary aspect is mobility. Considering a range of user travels (geographical area) along with the sequence of visited cells (routes taken) and information connected with the repeatable nature of human behavior [Gonzalez et al. 2008, Liu et al. 2014], identifying patterns is not an easy task. Domain specific algorithms are required to create user's mobility behavioral profile and measure potential anomalies and deviations from these patterns.

2.3 Mobility models

Use of data from various sensors connected with mobility and available on a device (GPS data, WiFi networks available or even IP address) is a broad field of study. In addition, the research around the usage of call logs (locally) or Call Detail Records (CDR) (on a server of a telco provider) is one of the most interesting areas due to the availability of this data on each phone. It was proven that geographical aspects of user whereabouts derived from CDR can be successfully used in modeling human mobility [Isaacman et al. 2011, Becker et al. 2013].

Humans have stable mobility patterns and a significant tendency to return to a few often visited locations[3] [Csáji et al. 2013, Gonzalez et al. 2008]. Despite the uncertainties, human mobility is predictable based on the historical behavior [Song et al. 2010a, Song et al. 2010b, Lu et al. 2013] regardless of the distance traveled [Bagrow and Lin 2012]. Due to this fact, even using sparse data like CDRs we are able to get a good approximation of user movement patterns.

In case of using Call Detail Logs for the analysis of user mobility, only very brief moments of his whereabouts are known. They are related to calls or other services used by a user that were handled by BTS[4]. This estimation of a user's location is not ideal, but its accuracy can be measured based on the density of

[3] Mostly identified as their home and workplace or their equivalents, like e.g. school.
[4] Base transceiver station.

Characteristic	Measures (observable variables)
Device's facilities usage	Type of program or service evoked; temporal interval between two consecutive evocations of a program or service of a same type
Sequences of actions followed	Sequences of *n* actions
Temporal lengths of actions	Temporal lengths of actions
Temporal intervals between actions in a sequence	Temporal intervals between subsequent actions
Retrieving contact details from the device's memory vs. entering them ad hoc	Way of entering or retrieving contact details
Use of shortcuts vs. use of menu	For each menu command with shortcut, the chosen option
Routes taken	Sequence of cells traversed between two consecutive prolonged stops
Speed of move conditioned on route/time	Speed of move conditioned on route and time
Length of work day	Time that the terminal is in the place affiliated with the user's workplace(s); day/time of main activities
Changes in behavior	Changes in behavioral characteristics
Words or phrases used more often	Frequency of different words used in a piece of handwriting (with stylus) or typing
Time of reading a unit of textual information	Time during which a document is open for reading
Time between incoming event and response conditioned on time of day	Temporal interval between reading an incoming message (e.g. e-mail or SMS) and writing the response
Accuracy in typing, menu item selection, etc.	The ratio of errors to the overall number of actions, i.e. the frequency of mistyped keystrokes, errors in menu item selection, etc.
Time devoted to communication	Time during a day spent for communication (using terminal) by different types of communication (calls, e-mails, etc.)
Pressure, direction, acceleration, and length of strokes	Pressure, direction, acceleration, and length of strokes
Temporal characteristics of keystrokes	Key duration time, inter-key latency time
Statistical characteristics of voice	Cepstrum coefficients of the signal power
People contacted with, conditioned on type of communication, time, etc.	Phone number, e-mail address, or other address information of the contacted people
Places visited, conditioned on time of day, week, etc.	Locations where prolonged stops were made
Changes in the choice of environment	Changes in environmental characteristics
Time, when the user is online	Time, during which the communication facilities of the terminal are not deliberately restricted
Set of installed software	Changes of device configuration
Current screen resolution	
Volume level	

Figure 2: List of distinctive measures proposed by Mazhelis et al. for mobile masquerader detection. Source: [Mazhelis and Puuronen 2007]

the towers. It proven to be sufficient to perform analysis of a human mobility on a small scale focusing on estimating temporal patterns of locations visited by a user and building a user's mobility profile [Liu et al. 2014, Çolak et al. 2015, Calabrese et al. 2011]. This task can be performed by a family of trajectory-based methods (often relying on a stay-extraction) to estimate the dwell time in each place the user visits [Xie et al. 2011, Iqbal et al. 2013, Widhalm et al. 2015, Maldeniya et al. 2015]. The user's profile built mostly utilizes the semi-structured patterns that can be observed when analyzing the mobility in a weekly manner in hourly bins, showcasing user behavior patterns [Phithakkitnukoon et al. 2010, Furletti et al. 2013, Andrienko et al. 2015]. The trajectory-based models have the advantage of being an understandable representation of an approximated user mobility pattern and can have multiple uses in the analysis and uncovering human behavior patterns, in contrary to the often classification-heavy purpose of Machine Learning Algorithms (MLA). Nonetheless, due to some unpredictability of the human behavior mobility, pattern models require

different learning periods depending on the data density and the task. They are also rather parameter heavy due to the fuzzy patterns users have - even having the perfectly sampled data, the upper threshold w.r.t. quality of prediction of user behavior is about 87% [Schneider et al. 2013].

2.4 Anomaly detection in mobility

To detect anomalies in the user mobility patterns, a wide variety of methods can be applied. The basic methods are based on the Bayesian decision rule system to classify the conditional probabilities of visiting BTS stations and mean residence times [Bushkes et al. 1998]. Another family of methods focuses on the sequence of visited locations. An approach proposed by Sun et al. [Sun et al. 2006] built a Markov model, utilizing EWMA (Exponentially Weighted Moving Average) mobility tries, based on cells visited by the user. By building a probability-based model of the routes user followed, the model was able to detect anomalies in new sequences of locations that were unlikely - had a lower probability of the user's appearance than a design threshold (Pth). In this case also oscillations and errors in classification of locations should be considered [Tandon and Chan 2009]. A few recent methods described in Table 1 provide extensions of these basic approaches. These examples provide interesting insights and give a rough approximation on the expected accuracy of the model. Nonetheless, they work on well sampled and small datasets - their use on a large scale, real world and sparse datasets was not tested.

2.5 Advantage over state of the art

The approach proposed in the paper benefits from the findings on human mobility. The proposed model describing patterns of the user's mobility is created using trajectory based methods [Xie et al. 2011, Liu et al. 2014, Iqbal et al. 2013, Widhalm et al. 2015, Maldeniya et al. 2015] and by clustering activities in weekly patterns with 1h time windows [Phithakkitnukoon et al. 2010, Furletti et al. 2013, Andrienko et al. 2015]. The model considers characteristics of the sparse data and possible errors in the observed movement connected with e.g. signal oscillations and load balancing [Tandon and Chan 2009, Schlaich et al. 2010]. The user's mobility profile is then used as a pattern for behavioral authentication based on anomaly detection, which utilizes a threshold method [Sun et al. 2004] based on 90th percentile of the normal behavior threat readings [Yazji et al. 2014]. The model includes a novel approach based on the division of the

[5] http://realitycommons.media.mit.edu/realitymining.html
[6] https://www.microsoft.com/en-us/research/publication/geolife-gps-trajectory-dataset-user-guide/
[7] http://realitycommons.media.mit.edu/realitymining.html

Table 1: Review of approaches for differentiation of user patterns, anomaly detection and authorization.

Publication	Dataset	Method used	Accuracy
Mobility-based anomaly detection in cellular mobile networks [Sun et al. 2004]	A simulated dataset showcasing a graph resembling the cellular mobile network. Call durations are the same for all users and exponentially distributed with a mean value of 3 minutes. The higher the mobility level, the more cells traversed with a given speed - set between 20 and 60 miles/hour for testing purposes.	High order Markov Model Exponentially Weighted Moving Average used for creating a profile - the probability of each route the user took. The design parameter Δ is based on the entropy of a current trace and is used for changing the detection threshold. Anomaly detection based on calculating the distance between the current trace and the EWMA-based mobility trie.	89% accuracy with 13% FRR
Mobi Watchdog: You Can Steal, But You Can't Run! [Yan et al. 2009]	Reality mining dataset[5] – activities labeled with BTS cell id from 100 users, sampled every 30 minutes to showcase CDR granularity level. 30 days used to train the model and 30 to test the model performance.	HHMM (Hierarchical Hidden Markov Model). Decision is made after τ (design parameter) consecutive activities have been found anomalous (parameter in the model). Working authentication software raising alerts by requesting the device holder to re-authenticate himself when an observed mobility trace significantly deviates from the trained model.	Accuracy above 90%, for similar users between 50% and 70%. FRR about 13% for one anomalous activity window and 9% when using 3 activities.
Efficient location aware intrusion detection to protect mobile devices [Yazji et al. 2014]	Geolife dataset[6] - GPS trajectories from 178 users with about 5 second sampling. Reality mining dataset - 68 users chosen with an average of 2.5 min sampling. 100 sample batches of x (5, 15, 30, 60 minutes) used for testing.	Trajectory based mobility model on frequently visited locations with 30 mins stay time and a confidence interval of 90% for anomaly detection (accepting 90% of the user's normal behavior based on the trace samples). Zero probabilities for visiting new locations.	94% accuracy in anomaly detection with FRR <= 10% within 15 minutes - about 6 activities.
Active authentication for mobile devices utilizing behavior profiling [Li et al. 2014]	Reality mining dataset[7] - 76 users chosen. RBF tested on 20 users with the dataset divided in two halves.	Differentiating between user patterns (is this a user who he appears to be, based on other users' data). 7/10/14 used for learning, smoothing function applied to the tested activities for anomaly detection - up to 6 activities.	Best results: 9.8% EER with 10 days learning period and 6 activities smoothing. RBF neural network achieved 10,5% EER. Rule based approach - statistical occurrences 11% EER.

Source: own elaboration

mobility anomalies into different dimensions including: time, sequence (partially based on [Sun et al. 2006]) and a geographical area, along with the probability of a user visiting a given location. The proposed model is proved to be able to differentiate between the user patterns in a long term.

The paper, to the best of our knowledge, also presents the first large scale application of the mobility-based behavioral biometrics on sparse data (in this case CDR). The previous approaches focused on samples of: 76 [Li et al. 2014], 100 [Yan et al. 2009] or 178 users [Yazji et al. 2014]. This model was tested for 1000 users based on CDR logs. The respective test cases were chosen, based on the similarity metrics, from 252 174 inhabitants of Poznan area appointed by the home location detection algorithm. Also, a novel division of geographical similarity classes was introduced, transforming the approach described in the literature [Kaycik et al. 2014].

3 Trajectory-based model for the behavioral authentication scenario

3.1 Description of the dataset

The mobile phone data used for this work consists of more than 7 billion of anonimized records describing the activity of Orange SA clients in Poland for over 6 months between February and July 2013. This data is typical for publications dealing with the CDR processing [Çolak et al. 2015, Schneider et al. 2013]. Each data record used in this work consisted of:

- anonymized **id** of a user initiating the call, being the client of Orange and a **receiver** of the service,
- type of a **service** (call, sms, Internet use) used along with associated **measure** e.g. duration in seconds,
- accurate time stamp with a date together with a BTS station data and location_id connected with it[8].

3.2 Trajectory-based model of the mobility

To be able to detect anomalies in the user's behavior, the mobility patterns need to be created to compare new activities against them. Our approach was to use the trajectory-based mobility model and evaluate it in a task of the constant event-based anomaly detection. The process of creation of the mobility profile consists of the following steps:

[8] Meaning a set of BTSs sharing the same coordinates to ease the geographical analysis.

– extracting activity data,

– applying ABA method,

– creating movement blocks i.e. calculating stay time in a location,

– identifying important locations, passages and routes,

– creating dictionary of user's habits (user's mobility profile).

The process is depicted in the Figure 3. The details of our approach are presented in the following sections.

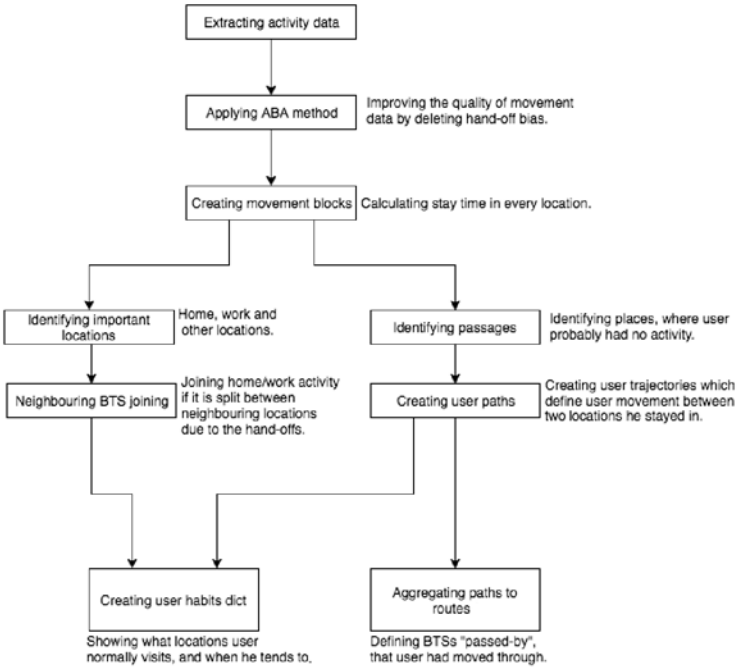

Figure 3: The process of creation of the mobility profile model used in this work. Source: own work

3.2.1 ABA method

Oscillations and quick location changes that appear between successive activities are often a case of the false displacement of a user [Liu et al. 2014], caused by the traffic balancing or user position between the signal range of two or more

stations [Tandon and Chan 2009]. To address these problems, a method based on an approach used to clear shifting locations observed in transportation travel proposed by Schlaich is utilized [Schlaich et al. 2010]. Therefore, to eliminate these errors, events meeting the following pattern are corrected:

1. First, there is an activity from a location A.
2. Next activity is observed within the next x (10 is chosen based on the literature [Iqbal et al. 2013]) minutes from the location B.
3. Third subsequent activity within x minutes from the second activity is labeled with location A.

If errors like that are observed, they are fixed and the sequence of visited locations becomes AAA.

3.2.2 Consecutive activities and stay time

Based on the previous work in the field, considering consecutive activities from the same location that are temporally close to each other can lead to a mostly true assumption that a user stayed in a target location during the time of his activities. The probability of a user staying in a location declines together with the time passing and an upper threshold needs to be introduced. For this work 1h was chosen based on the previous research [Iqbal et al. 2013, Wang et al. 2012, Maldeniya et al. 2015]. If activities are separated by a time less than $1hour$, we consider that the user had a constant stay time in a location.

Moreover, in contrary to the previous approaches, which consider single or temporally distant activities to have no influence on the pattern, different approach is proposed in this work. Due to the fact, that a user activity in a given BTS is considered as a certain information about his whereabouts in this period, we can assume he was there for at least a short period of time. This approach can be called **"weighted" activity labeling**. This method is similar to the time discretization mentioned in the recent literature [Widhalm et al. 2015] and based on our tests on the whole database, its use doesn't influence the structure of visited locations. The findings show that sparse activities that are separated by more than an hour are weighted and become at least 15 minutes long.

3.2.3 Identification of passages

With identification of locations with a significant stay time (derived from consecutive activities in a location), BTSs connected to the user movement need to be identified. Approach to distinguishing the "passed-by" locations, is as follows:

1. If a stay time in a location is longer than 30 minutes [Liu et al. 2014], it is a location where a user had some activity – it is a significant location and therefore a "non passed-by" location.

2. If the period between two consecutive activities is longer than 4 hours (value based on [Picornell et al. 2015]), the first activity is also labeled as a non "passed-by", to derive any trajectories from the sparse data and avoiding trajectories spanning for multiple days in case of rare activities.

From these trajectories, paths and routes are created that aggregate the user movement. A path is a vector of the user's movement with its start and end in locations with a significant stay time. The path may contain passed-by BTSs that a user moved through to get from the start to the end location, if any were identified. Each path is a trajectory of a user. The routes on the other hand aggregate all paths between points A and B. They are structures that describe the possible passed-by BTSs, when users moved from a point A to B giving probability values to a given sequence of passed-by BTSs. They will be referred to as probability tries later in this work.

3.2.4 Important locations - home/work

Based on the time a user spent in a given BTS station, the most visited, important locations can be distinguished. The home location is the BTS where a user spends most of his time between 19 and 7 in a week. The work location label is assigned to the location with the most time spent between 10 and 18 on weekdays, excluding the home location. To address an additional time spent in neighboring BTSs, the joining algorithm is used to negate the effects of possible hand-off errors in the data.

3.2.5 Data structure of the profile - the dictionary of habits

By identifying locations visited by a user along with the time he visits these locations, a user's mobility profile can be built. A model containing regularly visited locations and user movements between these locations, kept in a weekly-calendar data structure is called **user habits' dictionary**[9]. Each timeframe (1 hour is used in this work) is assigned with locations and routes a user took in the observed period along with their accuracy levels.

3.2.6 Accuracy of the model

Our model calculates the approximated user dwell time for each visited location. A ratio of the time spent in each cell of the habits dict (distinct pair of a day

[9] Also referred to as dict due to its programming dictionary-like structure.

and an hour) compared to the sum or all locations in this timeframe can be calculated. This measure is independent of how active the user was[10], but rather indicates how much time a user spends in a given place during the time period in comparison to other locations that appear during this time. This structure becomes closer to the ground truth for active users[11]. The accuracy values split among locations in a timeframe tell us how predictable the user was in a given period.

3.3 Anomaly detection model

In our model we define **anomalies in mobility as situations where a user appears (has an activity) in a location that is not present in his regular movements or the current movement varies significantly from his typical pattern (considering time, geographical area or sequence of places visited and probability of user being in a given location)**. Due to this fact, a model that includes these multiple dimensions of mobility needs to be introduced.

3.3.1 Time

To consider and study the time aspect of a user movement, a simple approach based on the fact that users tend to have distinct daily patterns is used. Each activity threat measure is equal to a number of time frames between observed and behaviors present in patterns in comparison to a max distance (achieving its max at 24h difference between the activities). Given the activity x in a timeframe t (x_t) and the maximal allowed difference in timeframes dt_{max}, considering the distance d in timeframes $d_t(x_t, T)$ between the activity x_t and all of the visits of a given location in other timeframes described in a set T, we can define the time threat as:

$$Threat(x) = min(\frac{d_t(x_t, T)}{dt_{max}}, 1) \tag{1}$$

3.3.2 Geography

Due to the fact that users tend to spend most of their time in already visited locations and their movement is highly predictable, the geographical aspect of a user movement plays an important role in the anomaly detection. Users also tend to move only within a small area of few kilometers around their habitat [Bagrow

[10] Very sparse activity with only one location in a timeframe gives it an accuracy of 1.
[11] Meaning the structure of visited locations is really close to the true time spent in these locations.

and Lin 2012]. When a user is present at one of his "important"[12] locations, the geographical threat measure equals 0.

The geographical threat for a test activity x, equals 1 minus the distance in meters to a closest location from a set of important locations L, compared to the average distance traveled daily d_{daily}.

$$Threat(x) = min(\frac{d(l_t, L)}{d_{daily}}, 1) \tag{2}$$

3.3.3 Sequence

With the added layer of the mobility information about user routes[13] a probability based model of the user movement can be built. It can utilize the built trie routes' model. By updating the routes and paths with counters that assign probabilities to certain trajectories the user took (based on the probability tries), we can extend the probability over the basic "stationary" model of accuracy. The model considers the weighted probabilities of a user following a given trajectory (ordered set of locations). This translates to utilizing an Markov Chain model on the sequence of n visited locations between the stay points extracted.

Reading a test activity x on a level i, means it is an *i-long* sequence[14]. Let $X = (X_1, X_2, ..., X_i)$ be a sequence of locations visited by a user, with a length ($|X|$) being equal to i, where the first place visited in the observed sequence is X_1 and the last is X_i. Then we define the set A that includes all sequences of length i.

$$\bigwedge X,\ if\ |X| = i,\ then\ X \in A \tag{3}$$

Based on this definition, a given test sequence X_t which is of length i and $X_t \in A$, we can define the threat as:

$$Threat(x) = 1 - P(X_t) \tag{4}$$

The probability $P(X_t)$ is calculated by comparing the number of times (C) this sequence appeared compared to the number of all sequences of this length.

$$P(X_t) = \frac{C(X_i|X_1, X_2, ..., X_{i-1})|_{X=X_t}}{\sum\limits_{X|A} C(X_i|X_1, X_2, ..., X_{i-1})} \tag{5}$$

[12] Regularly visited with more than 5% accuracy.
[13] And the predicted accuracy of the BTS appearing in comparison to the routes in the pattern.
[14] E.g. for i=3 we consider all sequences that are of length 3, like: ABD, ABC, ACE.

3.3.4 Probability of visiting a location

Considering the mobility patterns of a user, we can focus on the probability of vising a place and distribution of the time spent there. The proposed approach involves creating a structure in which every location is assigned a probability of user's appearance based on the training data set. This probability gives a rough approximation of the time spent in this location as compared to the other locations in this period. It gives a rough approximation of user's movement pattern in a given time-frame and in our case is showcased by the accuracy parameter.

The interpretation of this measure is as follows: "How probable it is that a user is in this location in this timeframe (exact hour and day) compared to the other places he visits". If a user visits a location that is present in the timeframe[15], including passed-by locations that match his currently traveled route, the uncertainty measure is calculated as follows. For a location l in a timeframe t, where the accuracy of an activity x in a location l and a timeframe t is denoted as $a(l,t)$:

$$Threat(x) = 1 - a(l,t) \tag{6}$$

The following sections will present the evaluation of the proposed method.

4 Evaluation of the method: using mobility in the behavioral authentication scenario

In order to verify the usability of the user's profile in the authentication and non binary authorization scenario, its outputs - namely threat levels, need to be tested to better describe everyday mobility behavior and differences between users.

4.1 Preparation of data

First a sample, consisting of users that shared a similarity in a geographical profile (being from Poznan area), was chosen to test the model in a scenario that would be close to real life applications of the model[16]. This also allowed to build a "hierarchy" of users based on the probable increase in similarity of mobility profiles to test model for different cases.

Based on the requirements of the model, home and work locations for all users that appeared in the Poznan area in March 2013 were calculated. The

[15] In our CDR dataset case - an hour.

[16] As it is obvious that selecting a random user for the anomaly detection will yield positive results in the anomaly detection but is not the case for most of the real life scenarios e.g. when the phone is stolen.

area was chosen based on the TERYT[17] mapping. This returned 173 distinct location_id's that were considered being in Poznan area as shown in Figure 4.

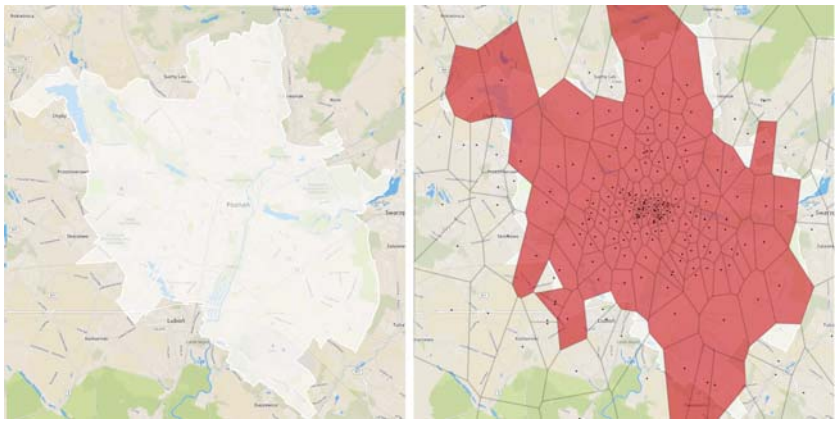

Figure 4: Visualization of Poznan administrative borders on a city level (on the left) along with the BTS stations laying inside this area with their Voronois colored (on the right). Source: own work

4.2 Division of users into classes

The studies mentioned in the literature did not set a stable testing environment, therefore a definition of such a testing approach was needed. This approach to testing methods on anomaly detection is novel and may be applied by other researchers in the field. Such an approach may enable future comparison of results between various approaches. We propose to evaluate similar methods addressing different levels of similarity to the tested user behavior, including:

- **the same user** - choosing the unobserved new data of a user allows to test the extent of predictability of human patterns and sensitivity of the threat measures, while giving a clear answer about the **false rejection rate** for anomaly detection cases.
- **A random user** - similarly to the most of the approaches in the literature, a random user from the sample was chosen. This showcased how the trajectory model compares to the approaches in the literature.

[17] The Polish administrative areas' territorial mapping.

- **A user from the same town** - by choosing a user that has a home location that falls into the same town, which more closely resembles a phone theft than a random user choice does.
- **A user with the same home location** - potential success in differentiation of these patterns would allow us to differentiate between e.g. family members sharing a phone.
- **A user with the same home and work location** - in this scenario the goal was to verify whether the characteristics of the mobility differs between just visiting the same locations (in sequences taken, time of visits etc.).

4.3 Identifying deviations in the mobility by measuring the activity threat levels

The evaluation of the model concerned checking, if the model is capable to differentiate between user patterns using threat values for new activities of the same and other users (from the similarity classes). The tests were performed on the sample of 1000 users from one month for whom corresponding samples in all of the test classes could be found. The statistics of this sample are shown in Table 2. The movement list is a structure that aggregates phone activities into a stay time labeled parts of trajectories - effectively aggregating activities that lengthen the stay in one location, meaning users have an average of 4 temporally distant activities daily (139,2 monthly). The distribution of a distance showcased a long tailed distribution, where a half of users has a daily distance shorter than 11.29 km. Home and work location accuracy levels state that users spend on average 70% of their night time at a home location, and a little above 50% of their work daytime at a work location.

Each user chosen for the test had his/her user profile built on the available data from one month. For each of them first **40 activities from the following month of their activity** were tested against the profile.

The results of the experiment prove that in the long run (with the average values for 40 activities) we can differentiate between user classes as shown in the Table 3 and Figure 6. Given enough data, the distinction between a user and someone very similar to him in terms of mobility is possible and the distinction is clearly visible in the average threat values. The distribution of average threat levels observed during the testing for each similarity class shows that classes influence the threat level distribution. High threat levels regarding the same town scenario also show a possibility to evaluate methods regarding fraud detection given much shorter timespan. The same user class threat distribution presented in Figure 5 depicts to what extent the user pattern is consistent over time on a sparse data (from CDR). On average, users show some level of unpredictability visible in the average threats generated by users, but this measure is

Table 2: Monthly statistics describing users who were the reference users in the class-based comparisons of the threat activity labeling.

	Activities in the movement list	Distinct locations visited	Average daily distance (km)	Home location accuracy	Work location accuracy
Min	2	1	0,003	0,05	0
Max	680	340	295,06	1	1
Mean	139,2	26	22,03	0,70	0,57
1st Quartile	77	11	5,6	0,51	0,34
Median	120	18,5	11,29	0,75	0,57
3rd Quartile	175,2	32	22,35	0,91	0,80
Std dev	87,79	26,77	33,76	0,24	0,27
Skewness	1,83	3,92	3,91	-0,51	-0,07

Source: own work

not a normalized definition. No conclusions can be made just out of this fact, without deeper analysis of the variables influencing repeatability level of mobility patterns. **The higher the threat level presented in the table and in the pictures, the more the pattern measured differs from the user's pattern (the lower is the uncertainty).**

Table 3: Comparison of the average threat levels for user classes.

class type	Average geographical threat	Average sequence threat	Average time threat	Average uncertainty threat	Average of threats
same_user	0.06	0.26	0.32	0.69	0.33
home_work	0.14	0.39	0.45	0.77	0.44
home	0.26	0.58	0.62	0.84	0.58
town	0.47	0.96	0.98	0.99	0.85
random	0.95	1.00	1.00	1.00	0.99

Source: own work based on CDR data

4.4 Anomaly detection on Poznan sample

Based on the findings of the above experiment, the structure of threat levels was described depending on the similarity level to a user. These findings allow for identification of anomalies based on the threat level measure observed. **The uncertainty measure was omitted** in this classification due to the fact that it provides high threat values and could not be used for the threat threshold creation later. Nonetheless, it remains as an interesting characteristics of the movement as the more dense is the data, the more useful it would be due to the fact that with regularly sampled data (average sampling rate equal to time

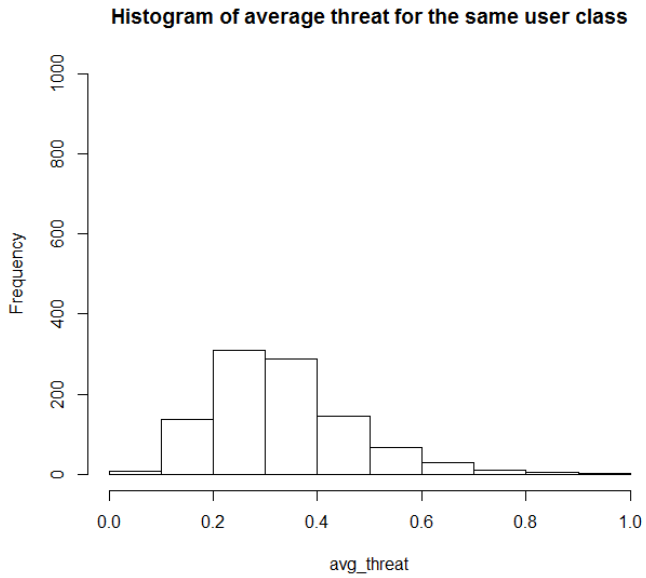

Figure 5: The histogram showcasing the values of the average user threat levels (of 40 test activities) for 'the same user' scenario, x axis indicates the threat levels and y describes a number of occurrences. Source: own work based on CDR data

frame length) it closely resembles the real mobility and time spent in a location patterns of a user. The use of this measure for regularly sampled phone data would make this measure directly applicable in the model.

Since users vary heavily, when it comes to their mobility profiles and habits, the model which takes this phenomenon into consideration needs to be created. The model should minimize the false rejection rate for users with highly varying profiles, while also minimizing the false acceptance rate for users with more stable and predictable behavior. To address this challenge, an approach of calculating confidence intervals for the three threats (time, geography, sequence) is presented. For each of these threats, it is set as a 90th percentile of the corresponding threat values calculated on the validation data set of user activities [Yazji et al. 2014]. To check if the tested activity is an anomaly, we analyze all three threats for this activity and if at least for one of them a confidence interval for the target threat is exceeded, the model marks this activity as an anomaly in this dimension. Whether one or more scores need to exceed the threshold to classify an activity as an anomaly remains a matter of future work, and is a parameter in the proposed model. Setting this value high can cause higher

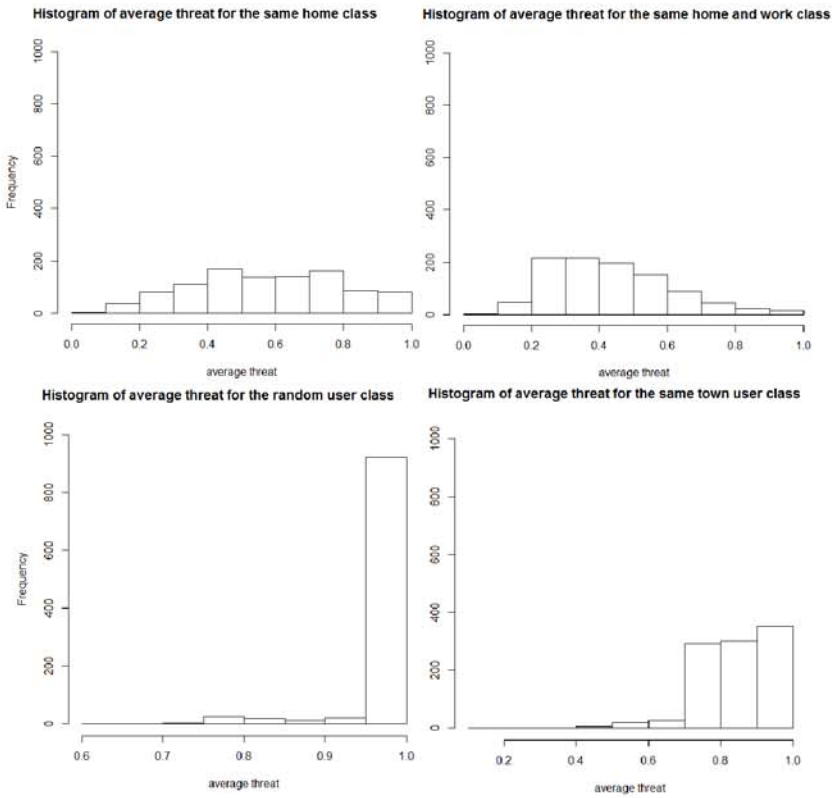

Figure 6: The histogram showcasing values of the average user threat levels (of 40 test activities) in the test classes scenario, x axis indicates the threat levels and y describes a number of occurrences. Source: own work based on CDR data

false acceptance rate for tested activities, resulting in less anomalies detected. The approach that is proposed for the model learning and anomaly detection is presented in Figure 7.

To create confidence intervals for all three measures:

- user's mobility profile needs to be created from the learning data period,
- target threat values for all activities from the validation data set need to be assigned,
- smoothing function is applied by using the moving average on the threat values,
- 90th percentile of the above mentioned moving averages is defined as a target threat threshold for each of the threats.

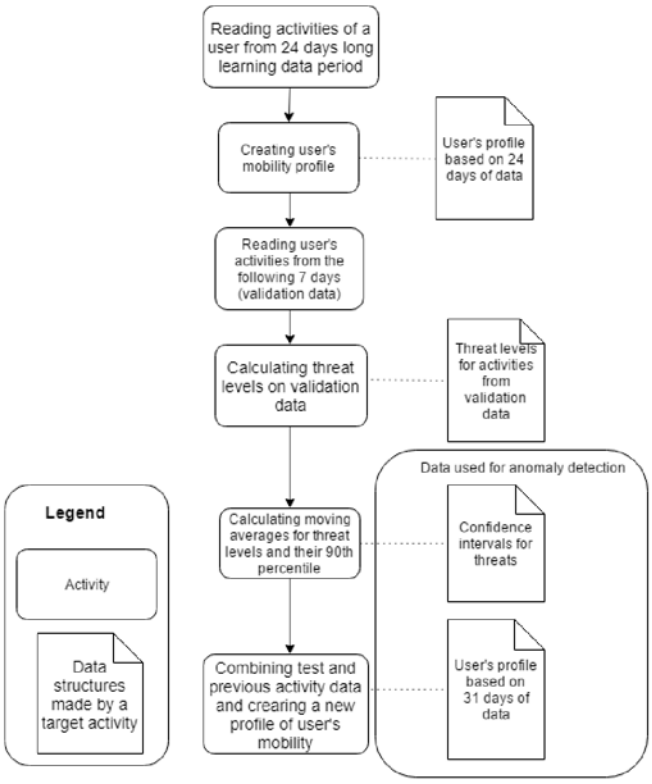

Figure 7: The approach used to define threat intervals and enable application of a user's profile for anomaly detection. Source: own work

Smoothing function that treats a number of successive activities as one event was introduced to deal with the mobile user's inconsistent and variable usage behavior. Therefore, a decision is made based upon the combined events rather than a single occurrence [Li et al. 2014]. In our approach an **interval size equal to 3** is used. The moving average is calculated in each respective threat value to smooth it. This is a parameter in the method which can be adjusted e.g. based on how active the user is to achieve the lowest number of false positives, while detecting an anomaly for a user in an acceptable timespan.

4.5 Results

Based on the confidence intervals, an anomaly detection experiment was carried out. Its results are shown in Table 4. By exclusion of users having all of the threat intervals equaling 1[18], about 7% of the sample was removed. Each excluded user

[18] Meaning no anomaly could be ever be detected using this model.

had his/her threshold levels equaling 1 in all three dimensions. This group of users did not have a stable pattern overall and could not be used for the model based checking of anomalies in the behavior.

To increase the method's performance, an improvement was tested that decreased the values of anomaly thresholds iteratively by one percentile below 90 for all users that had unpredictable patterns. This resulted in the reduction of percentage of excluded users to 0.8% and improved the model accuracy.

The FRR in the scenario was equal to the fraction of situations, where the valid user data from the test period was classified as an anomaly measure - accuracy in same user class. On the other hand, the remaining accuracy values indicated a number of situations, where activities of users from another class were properly labeled as anomalies - this related to the effectiveness of the algorithm in detecting a change of the user.

Table 4: The results of an anomaly detection method (FRR) with the use of 3 activities batch length and 2 measures classified as anomaly. Source: own work

Approach	Static 90'th percentile		Iterative		
% of users rejected due to the unstable pattern	7%		0.8%		
Number of measures needed to classify an anomaly	1	2	1	2	3
Results					
Class	Measure (% of anomalies classified in)				
random class	99,33%	85,16%	99,58%	99,57%	97,17%
same town class	88,50%	72,32%	96,65%	91,63%	70,84%
same home location class	60,40%	44,18%	70,17%	53,64%	37,29%
same home and work location class	43,80%	26,04	53,21%	32,03%	20,09%
same user class (FRR)	20,80%	8,83%	32,68%	13,79%	6,33%

The results of the method, while using 3 measures show that when we define anomalies as a travel beyond the user's geographical area, we can achieve authentication methods with an accuracy similar to the approaches in the literature (the proposed model achieved about 97% accuracy, with the FRR staying close to 6% and FAR to 3% in the random class). This also clarifies why simple probability based methods achieve good results based solely on coordinates, visited locations or area of movement. The best outcome of the model was achieved using 2 measures for the anomaly classification[19]. The model proved to be effec-

[19] For clarification, this means that two distinctive measures out of three (geography, sequence, time) needed to exceed their respective thresholds for the model to consider an activity batch to be anomalous and and not belong to an original possessor of the

tive in detecting anomalies in same town class scenario (an example of probable theft), while still remaining to be quite effective in differentiating people living in the same area (same home location class). The differentiation between similar users still seems to be an issue based solely on mobility and maybe other behavioral features would be the most successful when applied in these scenarios.

It is worth to underline, that the model achieved an accuracy similar to the approaches presented in Table 1, while working on much more sparse and unevenly sampled dataset. This proves that CDR derived authentication methods can achieve accuracy similar to the presented methods working on a device level data. Due to the fact, that characteristics of the data and the parametrization of the models (e.g. time window used for anomaly detection) plays a great role in the accuracy of the model. Therefore, the methodology for future comparisons of authentication methods needs to be discussed.

5 Discussion

The performance of the anomaly detection algorithms relies highly on the characteristics of the dataset and the model. Due to this fact, comparing the results of the methods working on different datasets may prove difficult - in our case we were able to achieve the same accuracy with more sparse data, but the scenario of the same town class is more useful to assess the quality of the model than the random class used in the literature. This makes the detailed comparison of result's metrics a good area for further work, which would not fit into the scope of the paper.

Based on the findings of this work, the requirements for benchmarks of algorithms in the future should include:

- **Spatial homogeneity of the dataset** (proposed approach: describing the area of study) – an area of the study should concern users of very similar patterns (like students/employers of a university) what may prove to be more challenging than just comparing random CDR users and influence the results.
- **Spatial homogeneity of a model compared to the test data** (proposed approach: division of the results in the comparison classes) – comparing a test profile with a random user always produces a high accuracy, the task becomes harder when comparing users that share locations visited with the base user. This also allows for building pattern differentiating methods that would be able to distinguish between family members sharing a phone and could be applicable not only on mobility data.

device.

- **Sampling frequency** (proposed approach: calculating inter-event time or an average number of activities/day per user) – the activity based data like CDR varies in its characteristics depending on the users and their inclinations to more often phone activities. GPS frequently sampled data remains at a very different resolution and may provide significantly better results even with the use of naive methods.
- **Learning period length** (propose approach: stating the length of time period used for the model learning) – due to the fact that human mobility differentiates between days of the week, and pattern stabilizes only about after two weeks, the length of the dataset remains important. Also very lengthy learning period may require model updates or recent data weighting.
- **Approach requirements** (proposed approach: stating number of activities (or time) needed for classification) – especially important in case of identification approach, where data from all users is compared to ensure uniqueness of the pattern. In case of anomaly detection, only extensive data on the user is needed. While pattern identification requires data for all (or many) of users to learn a model, an authentication approach uses only the user data as a one-class classifier.
- **Accuracy and type of the geographical label used** (proposed approach: stating or calculating geographical bias of used sensor, or providing density and average BTS area) – the average size of BTS area can be a good measure of accuracy for the CDR data. This also allows data to be comparable e.g. by introducing artificial bias when comparing results with more dense areas.
- **Other data used included in the model** besides of the tested aspect (proposed approach: measure the influence of other variables e.g. accelerometer readings on the performance of the model) - any other feature used besides the one tested (in this example geography) should be excluded from the base model to remain comparable to the current approaches.

6 Summary

In this paper we described advantages of using the behavioral authentication on mobile devices, along with the possible measures and methods that can be used. A trajectory based model was introduced along with the defined measures and definitions of anomalies in the dimensions of: geography, time, sequentiality and predictability. The model was tested on a large sample of CDR data and provided to be effective in dealing with sparse datasets. The results of the anomaly detection were satisfying in differentiating between the users and the model was proven to be effective in detecting the possible theft scenarios. What is worth to

note, is that the modular design of the proposed solution allows for an ensemble of machine learning (or other domain based) methods to be easily utilized in the model. Nonetheless, the additional insight and findings concerning the repeatability of paths users traveled would not have been possible, if machine learning methods or probability based naive classifiers were used to detect anomalies.

The unpredictability of the user movement - captured by the FRR (6%) was similar to the studies in the literature and the accuracy of the model was also similar (97%). The model proved valuable in detecting a simulated theft scenario and provided insight into causes of good results of other methods. Differentiating between similar users proved to be difficult with the CDR data. Utilizing only mobility in this scenario may not be enough to differentiate between users living in a close proximity. Nonetheless, the mobility pattern may be of use in a more complicated system utilizing more behavioral factors.

The division on anomaly classes allowed to create a benchmark for the mobility based anomaly detection models considering the similarity of users. However, parameters used in the model (such as the length of the activity batch) and the dataset characteristics can also influence the outcomes.

6.1 Future work

The influence of the time and the number of activities needed for classification is one of the main areas for further testing of the model, along with the comparison on various datasets (including the whole CDR database). As the model was tested on a sparse dataset, considering the influence of this characteristics on the output of the presented methods, and testing the model on the phone generated data could provide accuracy scores more comparable to the other algorithms.

For directly improving the accuracy, developing methods that would calculate the **similarity of trajectories** and including **less rigorous thresholds on the time aspect** would definitely improve the performance of the model. Adding a **semantic aspect** on the visited places[20] could also improve the model but would significantly increase the complexity. Exchanging the methods used for the threat definition with machine learning algorithms that would be tailored and suitable for a given aspect of human mobility e.g. RNN (Recursive Neural Networks) would probably cope well with learning sequential patterns. Similarly SVM or density based methods would work well on estimating the geographical area that a user travels through based on the coordinates. The use of those methods could potentially help in achieving a higher accuracy (after the initial insight provided by this model has shown their potential areas of application). Nonetheless, it

[20] If a user is visiting a grocery store in a constant time period, being in an unobserved location where the grocery store is located should not generate a high level of threat, when we consider the semantics of the place.

would greatly influence the computational complexity of the model and would require an ensemble of methods to utilize all dimensions.

After focusing mainly on one aspect of a behavioral biometry - mobility, the model could be also extended over different behavioral aspects like analysis of touchscreen interaction to better distinguish between users in high similarity classes.

References

[Acuity 2016] Market research - biometric smartphone model list. `http://www.acuity-mi.com/BSP.php`, 2016. Accessed: 2016-07-19.

[Aledavood et al. 2015] T. Aledavood, E. López, S. G. Roberts, F. Reed-Tsochas, E. Moro, R. I. Dunbar, and J. Saramäki. Daily rhythms in mobile telephone communication. *P*loS one, 10(9):e0138098, 2015.

[Andrienko et al. 2015] N. Andrienko, G. Andrienko, G. Fuchs, and P. Jankowski. Scalable and privacy-respectful interactive discovery of place semantics from human mobility traces. *I*nformation Visualization, page 1473871615581216, 2015.

[Bagrow and Lin 2012] J. P. Bagrow and Y.-R. Lin. Mesoscopic structure and social aspects of human mobility. *P*loS one, 7(5):e37676, 2012.

[Becker et al. 2013] R. Becker, R. Cáceres, K. Hanson, S. Isaacman, J. M. Loh, M. Martonosi, J. Rowland, S. Urbanek, A. Varshavsky, and C. Volinsky. Human mobility characterization from cellular network data. *C*ommun. ACM, 56(1):74–82, jan 2013.

[Bonneau and Preibusch 2010] J. Bonneau and S. Preibusch. The password thicket: Technical and market failures in human authentication on the web. In *W*EIS, 2010.

[Bushkes et al. 1998] R. Buschkes, D. Kesdogan, and P. Reichl. How to increase security in mobile networks by anomaly detection. In *C*omputer Security Applications Conference, 1998. Proceedings. 14th Annual, pages 3–12. IEEE, 1998.

[Buthpitiya 2014] S. Buthpitiya. Modeling mobile user behavior for anomaly detection. 2014.

[Calabrese et al. 2011] F. Calabrese, G. Di Lorenzo, L. Liu, and C. Ratti. Estimating origin-destination flows using mobile phone location data. *I*EEE Pervasive Computing, 10(4):0036–44, 2011.

[Çolak et al. 2015] S. Çolak, L. P. Alexander, B. G. Alvim, S. R. Mehndiratta, and M. C. González. Analyzing cell phone location data for urban travel: current methods, limitations, and opportunities. *T*ransportation Research Record: Journal of the Transportation Research Board, (2526):126–135, 2015.

[Csáji et al. 2013] B. C. Csáji, A. Browet, V. A. Traag, J.-C. Delvenne, E. Huens, P. Van Dooren, Z. Smoreda, and V. D. Blondel. Exploring the mobility of mobile phone users. *P*hysica A: Statistical Mechanics and its Applications, 392(6):1459–1473, 2013.

[Damaševičius et al. 2016a] R. Damaševičius, R. Maskeliūnas, A. Venčkauskas, and M. Woźniak. Smartphone user identity verification using gait characteristics. *S*ymmetry, 8(10):100, 2016.

[Damaševičius et al. 2016b] R. Damaševičius, M. Vasiljevas, J. Šalkevičius, and M. Woźniak. Human activity recognition in aal environments using random projections. *C*omputational and mathematical methods in medicine, 2016, 2016.

[Fox et al. 2013] B. Fox, R. van den Dam, and R. Shockley. Analytics: Real-world use of big data in telecommunications. *I*BM Institute for Business Value, 2013.

[Fridman et al. 2015] L. Fridman, S. Weber, R. Greenstadt, and M. Kam. Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location. 2015.

[Furletti et al. 2013] B. Furletti, L. Gabrielli, C. Renso, and S. Rinzivillo. Analysis of GSM calls data for understanding user mobility behavior. *P*roceedings - 2013 IEEE International Conference on Big Data, Big Data 2013, pages 550–555, 2013.

[Gartner 2013] Mobile devices secure or security risk? `https://www.gartner.com/doc/2595417`, 2013. Accessed: 2017-10-10.

[Gonzalez et al. 2008] M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi. Understanding individual human mobility patterns. *N*ature, 453(7196):779–782, 2008.

[Iqbal et al. 2013] M. S. Iqbal, C. F. Choudhury, P. Wang, and M. C. González. Development of origin–destination matrices using mobile phone call data. *T*ransportation Research Part C: Emerging Technologies, 40:63–74, 2014.

[Isaacman et al. 2011] S. Isaacman, R. Becker, R. Caceres, S. Kobourov, M. Martonosi, J. Rowland, and A. Varshavsky. Ranges of human mobility in Los Angeles and New York. *2*011 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2011, pages 88–93, 2011.

[Kaycik et al. 2014] H. G. Kayacik, M. Just, L. Baillie, D. Aspinall, and N. Micallef. Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. *a*rXiv preprint arXiv:1410.7743, 2014.

[Li et al. 2014] F. Li, N. Clarke, M. Papadaki, and P. Dowland. Active authentication for mobile devices utilising behaviour profiling. *I*nternational journal of information security, 13(3):229–244, 2014.

[Liu et al. 2014] F. Liu, D. Janssens, J. Cui, Y. Wang, G. Wets, and M. Cools. Building a validation measure for activity-based transportation models based on mobile phone data. *E*xpert Systems with Applications, 41(14):6174–6189, 2014.

[Lu et al. 2013] X. Lu, E. Wetter, N. Bharti, A. J. Tatem, and L. Bengtsson. Approaching the limit of predictability in human mobility. *S*cientific reports, 3, 2013.

[Maldeniya et al. 2015] D. Maldeniya, S. Lokanathan, S. Lanka, A. Kumarage, and S. Lanka. Origin-Destination Matrix Estimation for Sri Lanka Using the Four Step Model. (May):785–794, 2015.

[Mazhelis and Puuronen 2007] O. Mazhelis and S. Puuronen. A framework for behavior-based detection of user substitution in a mobile context. *c*omputers & security, 26(2):154–176, 2007.

[Österle et al. 2011] H. Österle, J. Becker, U. Frank, T. Hess, D. Karagiannis, H. Krcmar, P. Loos, P. Mertens, A. Oberweis, and E. J. Sinz. Memorandum on design-oriented information systems research. *E*uropean Journal of Information Systems, 20(1):7–10, Jan 2011.

[Phithakkitnukoon et al. 2010] S. Phithakkitnukoon, T. Horanont, G. Di Lorenzo, R. Shibasaki, and C. Ratti. Activity-aware map: Identifying human daily activity pattern using mobile phone data. In *H*uman Behavior Understanding, pages 14–25. Springer, 2010.

[Picornell et al. 2015] M. Picornell, T. Ruiz, M. Lenormand, J. J. Ramasco, T. Dubernet, and E. Frías-Martínez. Exploring the potential of phone call data to characterize the relationship between social network and travel behavior. *T*ransportation, 42(4):647–668, 2015.

[Połap and Woźniak 2017] D. Połap and M. Woźniak. The use of wavelet transformation in conjunction with a heuristic algorithm as a tool for feature extraction from signals. *I*nformation Technology and Control, 46(3):372–381, 2017.

[Schlaich et al. 2010] J. Schlaich, T. Otterstatter, and M. Friedrich. Generating Trajectories from Mobile Phone Data. *T*ransportation Research Board 89th Annual Meeting, pages 1–18, 2010.

[Schneider et al. 2013] C. M. Schneider, V. Belik, T. Couronne, Z. Smoreda, and M. C. Gonzalez. Unravelling Daily Human Mobility Motifs. *J*ournal of The Royal Society Interface, 10(84):20130246(1–8), 2013.

[Song et al. 2010a] C. Song, T. Koren, P. Wang, and A.-L. Barabási. Modelling the scaling properties of human mobility. *N*ature Physics, 6(10):818–823, 2010.

[Song et al. 2010b] C. Song, Z. Qu, N. Blumm, and A.-L. Barabási. Limits of predictability in human mobility. *S*cience, 327(5968):1018–1021, 2010.

[Sun et al. 2006] B. Sun, Z. Chen, R. Wang, F. Yu, and V. C. Leung. Towards adaptive anomaly detection in cellular mobile networks. In *t*he IEEE consumer communications and networking conference, volume 2, pages 666–670, 2006.

[Sun et al. 2004] B. Sun, F. Yu, K. Wu, and V. Leung. Mobility-based anomaly detection in cellular mobile networks. In *P*roceedings of the 3rd ACM workshop on Wireless security, pages 61–69. ACM, 2004.

[Tandon and Chan 2009] G. Tandon and P. K. Chan. Tracking user mobility to detect suspicious behavior. In *S*DM, pages 871–882. SIAM, 2009.

[Telesign 2016] Beyond the password: The future of account security. `https://www.telesign.com/wp-content/uploads/2016/06/Telesign-Report-Beyond-the-Password-June-2016-1.pdf`, 2016. Accessed: 2016-09-10.

[Trewin et al. 2012] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *P*roceedings of the 28th Annual Computer Security Applications Conference, pages 159–168. ACM, 2012.

[Ulinskas et al.2017] M. Ulinskas, M. Woźniak, and R. Damaševičius. Analysis of keystroke dynamics for fatigue recognition. In *I*nternational Conference on Computational Science and Its Applications, pages 235–247. Springer, 2017.

[Wang et al. 2012] P. Wang, T. Hunter, A. M. Bayen, K. Schechtner, and M. C. González. Understanding road usage patterns in urban areas. *S*cientific reports, 2, 2012.

[Widhalm et al. 2015] P. Widhalm, Y. Yang, M. Ulm, S. Athavale, and M. C. González. Discovering urban activity patterns in cell phone data. *T*ransportation, 42(4):597–623, 2015.

[Xie et al. 2011] R. Xie, Y. Ji, Y. Yue, and X. Zuo. Mining individual mobility patterns from mobile phone data. In *P*roceedings of the 2011 international workshop on Trajectory data mining and analysis, pages 37–44. ACM, 2011.

[Yan et al. 2009] G. Yan, S. Eidenbenz, and B. Sun. Mobi-watchdog: you can steal, but you can't run! In *P*roceedings of the second ACM conference on Wireless network security, pages 139–150. ACM, 2009.

[Yan et al. 2004] J. J. Yan, A. F. Blackwell, R. J. Anderson, and A. Grant. Password memorability and security: Empirical results. *I*EEE Security & privacy, 2(5):25–31, 2004.

[Yazji et al. 2014] S. Yazji, P. Scheuermann, R. P. Dick, G. Trajcevski, and R. Jin. Efficient location aware intrusion detection to protect mobile devices. *P*ersonal and Ubiquitous Computing, 18(1):143–162, 2014.