MOBILE PRIVACY IN AN UNTRUSTWORTHY WORLD

A Dissertation Outline Presented

by

KEEN Y. SUNG

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

February 2018

College of Information and Computer Sciences

MOBILE PRIVACY IN AN UNTRUSTWORTHY WORLD

A Dissertation Outline Presented

by

KEEN Y. SUNG

Approved as to style and content by:

Brian N. Levine, Chair

Mark Corner, Member

Joydeep Biswas, Member

Dennis Goeckel, Member

James Allan, Chair
College of Information and Computer Sciences

ABSTRACT

MOBILE PRIVACY IN AN UNTRUSTWORTHY WORLD

FEBRUARY 2018

KEEN Y. SUNG

B.Sc., UNIVERSITY OF ALBERTA

M.S., UNIVERSITY OF MASSACHUSETTS

Directed by: Professor Brian N. Levine

As people carry devices that are more persistently connected to the Internet, their location privacy becomes an increasing concern. The crux of this problem is the link between a mobile device user's identity, and the locations that the identity has visited. A user may turn of her device completely to drastically reduce her location privacy risk; however, her device is no longer useful, and her location may still be inferred if she is traveling with somebody who has not taken the same precautions. I demonstrate the following: (1) a unified model of location profiling, privacy, and utility; (2) two studies where a user's location may be revealed without her permission; and (3) a practical mobile connectivity framework for preserving location privacy is still susceptible to location profiling.

First, I present a mathematical model of geolocation privacy risk. This model uses trajectory linking and location profiling to de-anonymize sequences of locations back

to a user. I plan to validate this model by collecting real-world data and synthesizing a dataset.

Subsequently, I investigate two attackers: web services and advertisers. First, I present a study where location is inferred by a streaming web service, who can monitor the bandwidth changes a phone incurs while traveling along a path. The attacker in this case is anyone who is able to send a constant stream of data to the phone. This study demonstrated that with 70% accuracy, a classifier could determine on which geographic route among 8 a cell phone is traveling. Second, I explore the possibilities open to an attacker who places geolocation code in a mobile advertisement to uniquely identify a user associated with an advertising identifier. I further demonstrate that users with the advertising identifier disabled may be at risk if they travel regularly with a group of people.

Finally, I look at mechanisms to thwart a cell service provider determining a user's location. Providers can trivially geolocate users in a typical cell network using cell tower triangulation. Using our framework, a privacy-conscious provider could provide service and accept payment without knowing a user's identity. I also present a method that would allow users to share or swap their mobile identifiers. In these cases, location profiling is mitigated but still possible. I present a model of utility and risk where a user can determine based on their own knowledge of location profiling how likely they would be identified among other users if they made or accepted a phone call. I plan to develop an app to locally collect data about a user and halt certain functions on the phone when privacy is at risk.

With the modern ubiquity of mobile devices, the ability of a user to be located at most times of the day in their lives is a new force to contend with. The convenience of staying connected constantly comes with a risk of being located or identified. In this thesis, I plan to make contributions that quantify risk, and make this information to

be transparent to users, so that they can make informed decisions about whether to remain connected.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

INTRODUCTION

Geographical privacy is very important to most users [16]. In a recent study, twelve percent had been stalked online, and 4% had had their online activities lead to physical danger. After the 2013 global surveillance disclosures [12], most Americans became more vigilant about privacy — 86% have taken steps to mask their digital footprints, and 61% wish they could do more to increase privacy [22].

The current state of users' location privacy is nebulous. A poor understanding of what is possible for attackers has made it difficult for a user to quantify the value of privacy. Moreover, access to privacy enhancing tools is limited to those who have technical proficiency and have put in the effort to learn about their options or evade surveillance. While a user may be disturbed by how much access some companies or governments have to their location information, their inability to quantify its value and the high barrier to access privacy enhancing technologies prevent them from taking steps to mitigate their concerns. In many cases, users irrationally choose immediate gratification at the cost of future consequences in terms of privacy [1].

The aim of this thesis is twofold. The first goal is to bring to light the practical ability of different actors — governments, service providers, or services — to threaten a user's location privacy. By quantifying the limits of location privacy, we gain a clearer understanding of which behaviors are risky, and which are safe, in terms of protecting their location information. The second goal is to develop privacy enhancing technologies, which make it easier to everyday users to guard against these potential threats.

Most past research in this field has been conducted within the context of *location based services* (LBS) — online maps and geotagging services, for example. I expand

this scope of study and focus on the location privacy issues in non-LBS contexts by developing a model of utility versus location privacy. I then explore several scenarios where use of a mobile device *outside* of the context of a location based service (*non*-LBS usage) may reveal location (e.g. identifying a phone's location by analyzing seemingly unrelated metadata). Finally, I discuss frameworks that could be used to allow for greater location privacy.

Contributions

I formalize the scope of this problem in terms of potential adversaries, vectors of attack, and user behaviours with a model that balances utility and privacy. Using this model, I evaluate threats to privacy in the context of different attackers: a streaming service, an ad vendor, and a mobile service provider; I also explore the effects of limiting usage of these services or applications as a way to increase privacy. Finally, I explore in detail a privacy-preserving anonymous mobile framework and its ability to increase location privacy. The following is a summary of the contributions in each chapter of this proposal.

1. Model and quantify non-LBS usage and location privacy. There have been several attempts to quantify location privacy in terms of location based services [15, 25]. These models typically define a risk model in terms of k-anonymity within a database, and do not consider risk from the perspective of the user, or the varying value of privacy in different locations to a user or attacker. Furthermore, many of the scenarios explored do not account for the fact that simply by being online or using a service, an anonymous user may be identified by location profiling if an attacker controls her means of connection. In Chapter 1, I demonstrate the novel framework to combine location profiling and trajectory linking to identify a anonymous trajectories. I plan to evaluate different strategies a user could attempt to avoid this attack. I also plan to conduct a field survey to evaluate the privacy-utility

balance in practice. This model, and results from the survey, provide a basis for the remainder of my dissertation.

2. Measure the potential for a webservice to attack location privacy. While a user or service may have the ability to protect explicit location information to some degree, a web service may still illegitimately infer a user's location from metadata. In Chapter 2, I present a method in which a music streaming service may determine the location of a user by analyzing the wavering connection quality. I show that by using sequence matching algorithms, a remote web service may reveal the geographic path of a user given several choices, with no upstream information from the user except TCP ACKs.

3. Measure the potential for an advertiser to compromise location privacy. While a user may give a certain LBS permission to use location information, that service may, unbeknownst to the user, forward that information to an ad service. In Chapter 3, I evaluate the threat of an advertiser to a user's location privacy. I explore broadly the possibility of cheaply deanonymizing a set of users, then look specifically at the threat of stalking. I plan to buy ads to target cities according to the public schedules of sports teams, and see whether someone within the group might reveal the location of the team by using a mobile app within the advertising network we select.

4. Present and evaluate a framework for convenient anonymous cell phone usage with trusted peers. With users' trust in mobile network operators eroding, they may seek a privacy-oriented alternative that does not require them to reveal their location. The solution is a mobile network that breaks the link between mobile identifier and actual user. In Chapter 4, I present a protocol that allows users to conveniently obtain a temporary mobile identifier, which can be changed as soon as location profiling becomes a risk.

I also present an alternative to using a privacy-oriented framework, where a user shares credentials with a peer in order to create a mix-zone of identifiers. A user is typically authenticated on a mobile network through an attach procedure that results in a temporary authentication key. By sharing this key, a user may provide some privacy protection to another user, while at the same time increasing their own privacy. I plan to evaluate the ability for users to minimize their risk of having their identity revealed when using an anonymous service. I also plan to analyze sharing behaviour in terms of risk and utility.

Collaborators

All research activities are conducted under the supervision of Brian Levine. Preliminary work for Chapter 2 was completed in collaboration with Hamed Soroush, Erik Learned-Miller, Marc Liberatore, Joydeep Biswas, and Brian Levine [26]. Preliminary work for Chapter 4 was completed in collaboration with Marc Liberatore and Brian Levine [27].

CHAPTER 1

A MODEL OF LOCATION PRIVACY AND UTILITY

Many current models of location privacy primarily model threats from location based services, and propose defenses based on differential privacy strategies [2, 13]. However, the strategies studied in these works involve a service provider obfuscating databases of location logs, which requires the user to trust the service; this is not applicable from the point of a user who does not trust the service. In this chapter, I plan to generalize an existing method of quantifying location privacy [25], and extend it to allow for threats from non-LBS usage. In my preliminary work, I present a novel framework to identify a user from both location profiling (LP) and trajectory linking (TL). I propose to investigate game theoretic [11] and information theoretic models [24] to capture the varying worth of location privacy depending on the user and location. I will also evaluate the accuracy of the LP/TL framework and these models using a synthetic dataset created from a field survey. I will seek additional datasets as well.

1.1 Preliminary work: Framework for location profiling and trajectory linking

I summarize the different adversaries and types of threats against location privacy. Next, I develop a general model of location profiling and trajectory linking that can be used in various ways by these attackers. Finally, I evaluate some simple location profiling and trajectory linking algorithms.

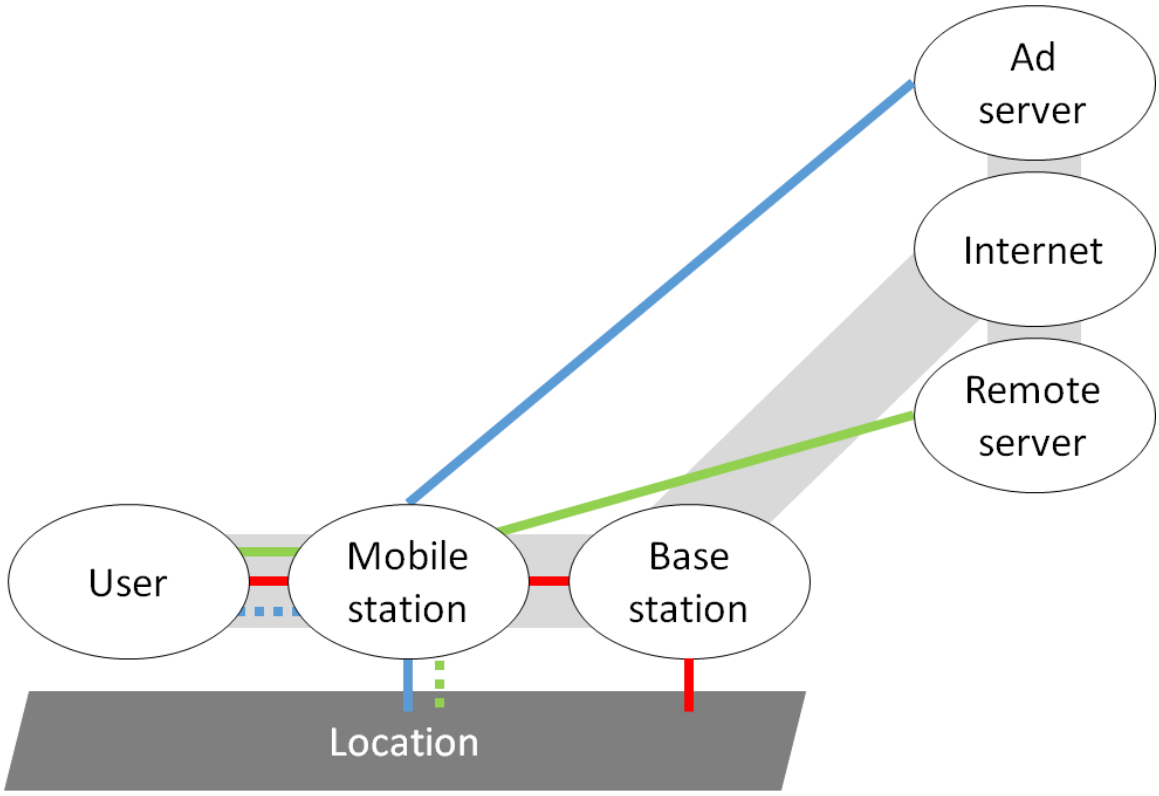

Figure 1.1. Exposure of information that may result in potential vulnerabilities in location privacy. The user, mobile device, and base station are in some physical location. The thick gray line indicates the communication path between a user and a service. Solid colored lines indicate links known to a potential attacker. Dotted colored lines indicate links that may be inferred by an attacker. Red lines indicate information known to a service provider; blue an advertising client; and green a web service.

Overview There are many ways people remain connected to the Internet, such as Wi-Fi, cellular network, and cable. In each of these cases, the time and location of a user connection is known to the service provider. There have been cases of IMSI-catchers being used dubiously to monitor individuals [7]. Additionally, passive eavesdropping techniques may intercept any mode of wireless signal, including Bluetooth, allow for a varying degree of granularity to localize an individual. We need a flexible framework to model these types of attacks. Such a framework would allow us to measure and quantify wireless geolocation privacy with varied settings and attacker models.

There are many attack vectors on a user's location privacy. Figure 1.1 diagrams the potential vulnerabilities from different classes of attackers. In Chapter 2, I look at a web service attacker. This service has information about who the user is and which device she is using, and may infer the location of the device (green lines). In Chapter 3, I look at advertiser attackers, who have information about the device's location, and may infer who the user is (blue lines). In Chapters 4 I look at service provider attackers, and how to defend against them. These attackers have concrete information about the user, device, and location, so we must break the link between user and device (red lines).

The following is a general framework that uses trajectory linking to improve location profiling. For simplicity, the following equations do not take into account the time of day, and other factors that may help determine the user of a trace. It contains no details about the location profiling and trajectory linking themselves.

Model Let U be the users in our database. These are users for which we have some location history data S_U. Let S^* be all sequences of locations L within some time range of interest. A sequence $\mathbf{s} \in S^* = s_0, \ldots; s_i \in L$.

The most likely user given an anonymous sequence of locations is

$$\arg\max_{u} p(u|\mathbf{s}), \tag{1.1}$$

where

$$p(u|\mathbf{s}) = p(u|s_0, \dots). \tag{1.2}$$

We can determine the most likely path for a user as

$$\arg\max_{\mathbf{s}} p(\mathbf{s}|u). \tag{1.3}$$

Trajectory linking is the most likely sequence given another sequence:

$$\arg\max_{\mathbf{s}} p(\mathbf{s}|\mathbf{s}'). \tag{1.4}$$

Finally, we can determine the most likely user of a sequence using information from possible additional trajectories. Let Z^s be the permutation of paths in S^* that are linkable to s (i.e., there is no overlap in time, and no impossibly fast transitions), then

$$p(u|\mathbf{s}) = \sum_{z \in Z^{\mathbf{s}}} p(z|\mathbf{s}) p(u|z). \tag{1.5}$$

Generating a permutation of paths and computing their probability is intractable for many tests, so we may use heuristics to include only obvious links.

If an attacker wishes to deanonymize an entire anonymized database, they would want to determine the most likely matching of users to traces.

We can determine the most likely corresponding (ordered) set of users $\hat{U}$, given some set of anonymous traces $S^{*'} \subseteq S^*$ as

$$\arg\max_{\hat{U}} p(\hat{U}|S^{*'}), \tag{1.6}$$

where

$$p(\hat{U}|S^{*'}) = \prod_i p(\hat{U}_i|S_i^{*'}). \tag{1.7}$$

To determine a set of users, given some anonymous set of traces, and consider possible links, we calculate

$$p(\hat{U}|S^{*'}) = \prod_i \big(\sum_{z \in Z^{S_i^{*'}}} p(z|S_i^{*'}) p(\hat{U}_i|z) \big). \tag{1.8}$$

Accordingly, the k-anonymity of a user u, given a trace s, is

$$k\text{-anonymity} = \text{rank}(\langle p(u|\mathbf{s}), u \rangle, U). \tag{1.9}$$

Linking algorithms There are effective, naive location profiling algorithms [8]. A simple location profiling algorithm can effectively determine the users of anonymous sequences. In the Reality Mining dataset [9], 95 anonymous users could be deanonymized with 80% accuracy (as I show in Chapter 4). However, most trajectory linking algorithms have been intended for improving positioning or object tracking, rather than from an adversarial perspective [14, 21, 29]. I investigate some trajectory linking strategies in this section.

I evaluated two methods of linking using traces of 300 000 cell phone users in a particular country[1], tracked two weeks at a time. Each user had a log of which location area code (LAC) among 1 666 they were present in every ten minutes.

Motifs. Because the dataset had only 1666 LACs, the mobility data was very coarse. This means that our traces do not capture much mobility unless a user makes distant trips. I was unable to regular sequences of paths that are more than three locations. Among 100000 users, I was able to identify paths with 3-location trajectories linked once with another (6 locations long) with 40% accuracy. Note that the existence of these trajectories were exceptionally sparse in this dataset.

[1]I was unable to obtain permission to publish using this dataset; thus, I have abandoned these results, and will have to find an alternative for my thesis.

Estimated link frequency. To estimate the likelihood of a link occurring, we count the frequency of a link (i.e. a transition from location a to b) in the dataset. Assuming

$$Count(AppearsTogether(a,b)) = Count(a) + Count(b), \tag{1.10}$$

$$\text{then } E[p(a \to b|a,b)] = \frac{Count(a \to b)}{Count(a) + Count(b)} \tag{1.11}$$

However, it may be the case that a and b rarely appear together (in time). For example, a may appear a lot more than b, but b often transitions from a. This breaks the assumption in Equation 1.10. We can make the assumption that the probability b comes from a and a goes to b is similar when they appear together as when they do not, in which case, we have

$$E[p(a \to b|a,b)] = \frac{p(a|b) * p(b|a)}{p(b) * p(a)} \tag{1.12}$$

The results from this linking method is shown in Figure 1.2.

Multiple target tracking (MTT) algorithms [20] can be used as heuristics for trajectory linking. Because the dataset above contains only coarse data on time and physical location, MTT would be ineffective. To simulate the finer-grained location data that a cell tower would have, I use a dataset tracking over 300 taxis in the Rome metropolitan area over a month [6] to evaluate the effectiveness of a naive MTT algorithm[2] for trajectory linking, assuming no points are linked initially. Figure 1.4 shows that if location is updated constantly, taxis would still be identified with 40% accuracy without any initial linking.

[2] `http://soft-matter.github.io/trackpy`

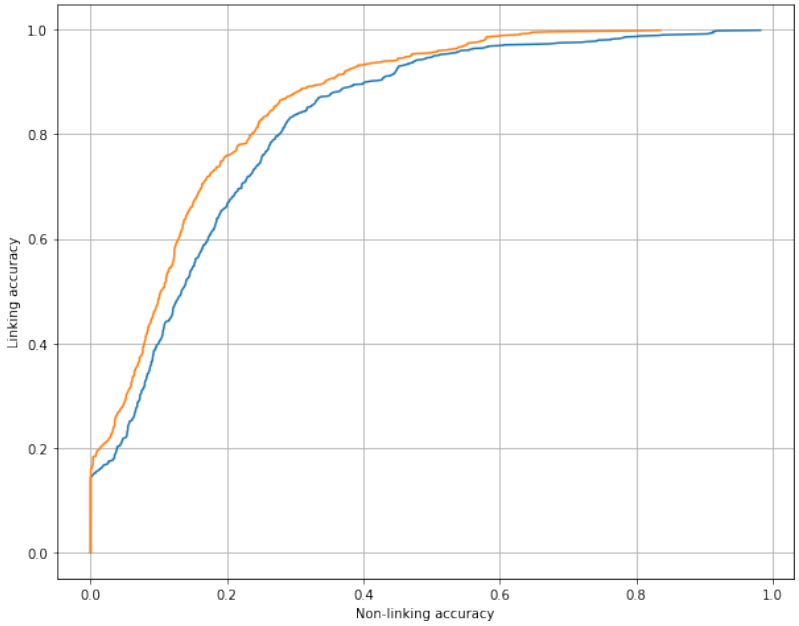

Figure 1.2. The x-axis represents accuracy of identifying a set of traces unlinked, and the y-axis represents the accuracy of the same set linked based on Equation 1.12. Red is a link before, and blue is a link after.

1.2 Proposed work: Fully implement a utility model and collect data to rigorously evaluate it

I was able to pilot trajectory linking and location profiling using several datasets; however, these datasets are insufficient to evaluate any algorithm (and one has not given us permission to publish). Additionally, many datasets are either old, crowd-sourced, or have been fuzzed with noise. To extend this chapter, I propose to answer a few key questions:

1. What are some properties of the wireless topology on a cell phone network in a rural or urban area? Knowing these properties would allow me to more accurately synthesize and validate a dataset.

2. How effective are LP/TL algorithms in de-anonymizing traces?

3. What is the utility cost to avoid being tracked by these algorithms?

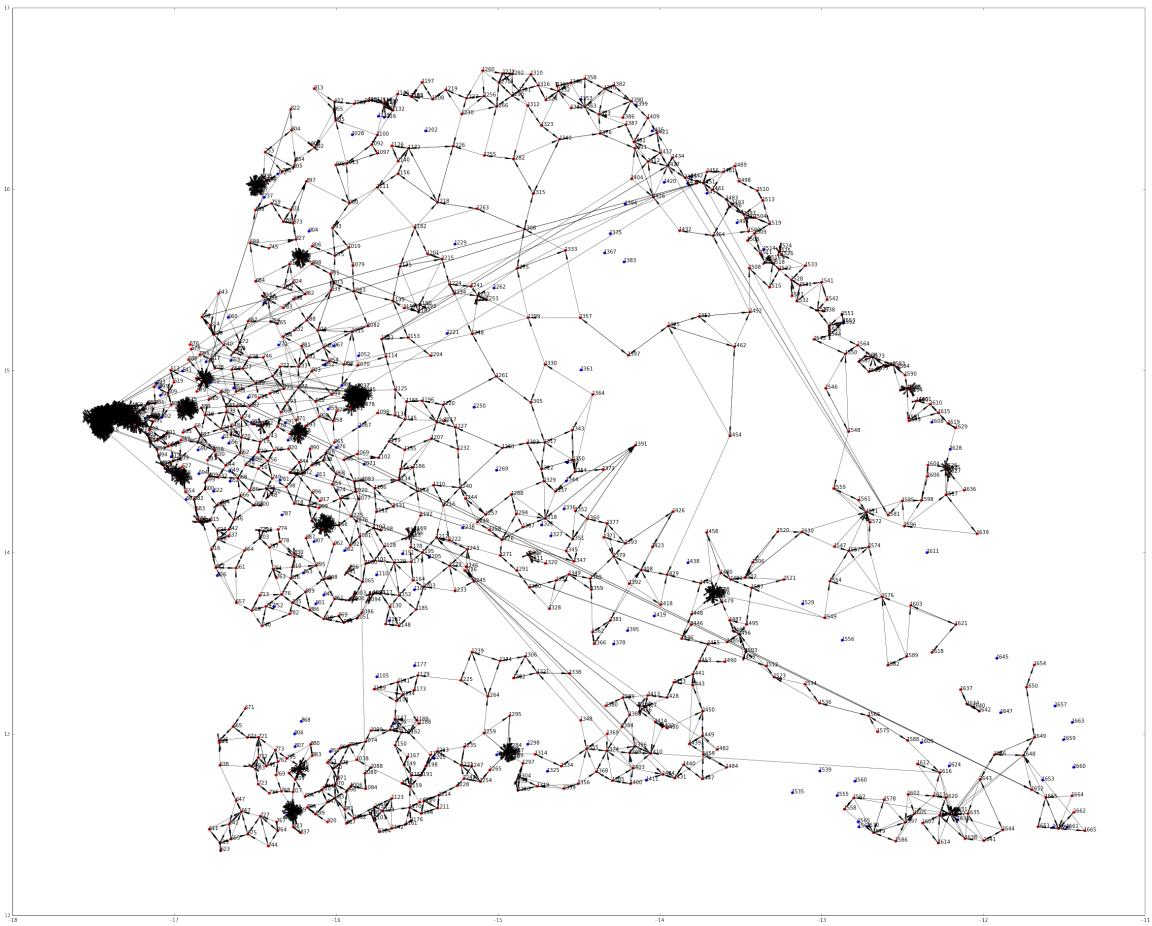

Figure 1.3. Most common LAC transitions in Senegal. Longer lines may indicate trips by air or sea.

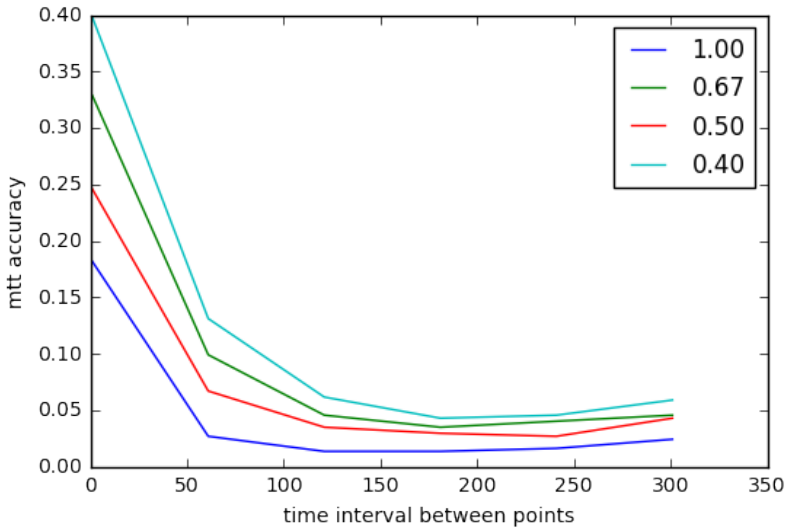

Figure 1.4. MTT accuracies for 374 taxi drivers around Rome over a period of 20 minutes. Colors represent different relative granularities.

To answer these questions, I will first do field surveys of the Amherst and Boston areas, to determine the density of cell towers and physical locations served. If I am able to recruit enough users, I will track how often a phone connects to the network to make a call. The call data in particular will be useful in Chapter 4.

Using this information, I will synthesize a larger dataset of mobility traces and calls, and validate this against any additional datasets I find. I will use these datasets to develop and evaluate several location profiling or trajectory linking algorithms.

Finally, I plan to develop a model to measure the balance between utility and privacy. I will alter traces in the aforementioned datasets to simulate evasive reduction of phone usage, and analyze the trade-off between usability and privacy. I will pay special attention to how much significant stays like home or work may make a use significantly more identifiable, but is information that is of little value to both targets and attackers. An economic model may better encapsulate these possibilities, if a user can assign different values to different locations.

CHAPTER 2

LOCATION PRIVACY THREATS FROM A STREAMING SERVICE

This chapter explores the threats to location privacy when a user downloads data while in motion, and presents an evaluation on the loss of utility if a user attempts to reduce these threats[1]. I propose to analyze in more detail some algorithms more suited to this problem, and the trade-offs between traffic-shaping to preserve privacy and utility.

2.1 Preliminary work: Identifying the path traveled using throughput

Despite features on smartphones to ensure location privacy, a user's whereabouts can be remotely deduced. A remote party communicating with a phone has a window into the complex interactions between phone and cell tower. These features can be used to reveal the phone's location, or at least significantly narrow the list of possible paths taken by a phone and its owner. This information is leaked regardless of application-level privacy settings. Cell phone users have such experiences intuitively in many common situations. For example, a caller may be able to tell when a friend has entered an elevator based solely on call quality; or a user may notice a loss in data throughput during a subway ride.

We collected hundreds of traces of music that we streamed to phones along four geographically separate routes in two directions each. We find that within small

[1]This chapter is based on work published at the Privacy Enhancing Technologies Symposium [26]

geographical areas, mean throughput is largely consistent and distinct. We examine the accuracy of three remote localization classifiers that leverage this consistency. Even a naive approach, trained on the mean throughput of each path, has some success. We compared this classifier against a k-nearest neighbors (k-NN) classifier, which trains on the ordered sequence of throughput values of each rout, a hidden Markov model (HMM) classifier, which exploits the consistency in throughput values at each location, and a Naive Bayes (NB-KDE) classifier that uses kernel density estimation of throughput at each second along a path. Our best performing approach, the NB-KDE classifier, can correctly determine with greater than the path taken by the phone from one of four longer paths to neighboring suburbs with greater than 90% accuracy, and the path and direction (8 choices) with 76% accuracy. In a separate experiment involving data collected only from within a 4km^2 area, in and around our campus, the NB-KDE approach could identify the direction and part of campus the user was traveling with 76% accuracy.

Data Our measurements[2] are based on four Android cell phones instrumented to record traces of GPS location and signal strength. A server in our building streamed music continuously to the phones during measurement trials. We logged TCP traces at the server during trials. We later combined sets of corresponding phone and server traces, synchronizing by the timestamps within the traces.

- **Mobile 3G Measurement Set — Paths to Towns**: We used four phones connected to the AT&T UMTS (3G) network to record traces. We collected data during a one-month period under varying traffic and weather conditions. Each measurement was taken as a phone traveled along one of four routes going either toward or away from our central location (point X in Figure 2.1). In total, we recorded 286 traces in this set.

[2]Traces from our experiments are available for download from `http://traces.cs.umass.edu`.

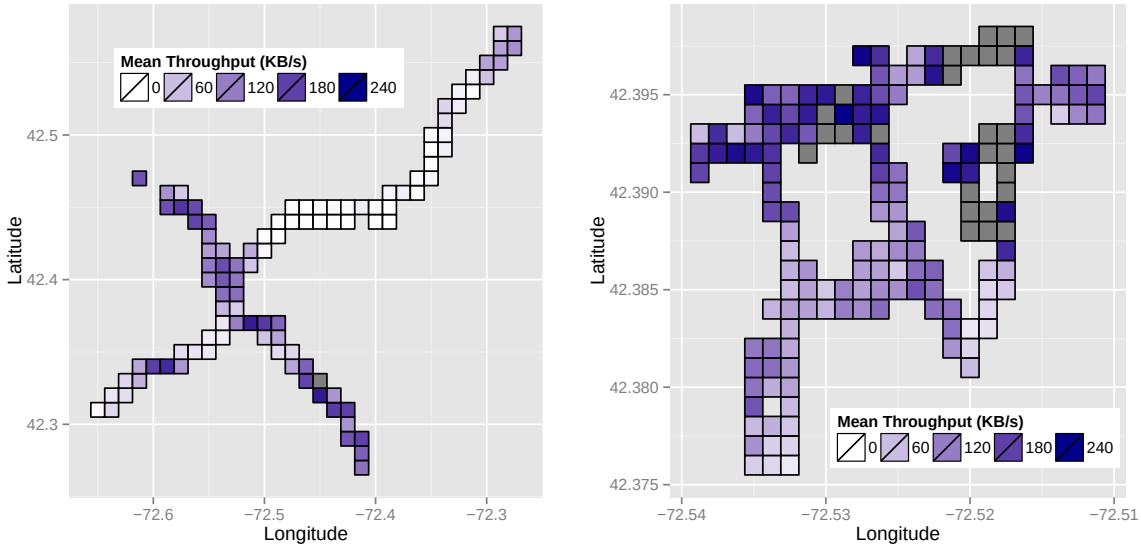

Figure 2.1. The mean throughput of locations around Amherst (left) and within UMass (right). 95% of areas have means that are statistically different from at least 90% of other areas. This data suggests that latent information linking throughput and geography is available for training a classifier.

- **Mobile 3G Measurement Set — Paths within Campus**: We recorded 141 traces from the same phones, along one of two directions around a bus loop on campus. Traces were collected over a period of eight months.
- **Stationary 3G Measurement Set**: We recorded 29 traces from stationary phones, connected to the UMTS (3G) network, located in different locations near our central location.

Algorithms I present a hidden Markov model (HMM), k-nearest neighbors (k-NN), and naive bayes (NB-KDE) classifier with respect to a motion-throughput model. Each classifier is derived from this model, with different assumptions. The HMM classifier is most general, and attempts to maximize the estimated hidden states and transitions. The k-NN and NB-KDE classifiers are more rigid, and make the assumption that users move through a certain path with consistent velocity. The k-NN classifier finds k of the closest traces by comparing the throughput at each time

point of the trace. The NB-KDE classifier determines the distribution of throughputs at each time point for each path, and finds the most likely trace.

In our evaluation, we tested the identification of a path rather than a sequence of locations. Therefore, we have split the location sequences into separate path classes.

For the HMM, The states are fixed as approximate square areas on the map. Emission probabilities at each state are determined by counting the number of occurrences of each throughput level in the training data in each area and normalizing. A throughput level $e = 0 \dots 15$ for 16 throughput levels. The probability of a certain throughput level occurring at a certain location is from a categorical distribution:

$$p(e|l) = \sum_{j \in N_l} [\mathcal{M}(o_j^l) = e]/N_l, \tag{2.1}$$

where $\mathcal{M}$ maps a throughput value b to an emission level e depending on which fixed range it is between.

The Markov assumption [17] allows us to consider the probabilities of each transition independently:

$$p(\mathbf{l}|\mathbf{b}) = p(l_0|b_0)p(l_1|b_1, l_0), p(l_2|b_2, l_1, l_0) \dots \tag{2.2}$$

$$p(l_t|b_t, l_{t-1}, l_{t-2}, \dots, l_0) = p(l_t|b_t, l_{t-1}) \tag{2.3}$$

$$p(\mathbf{l}|\mathbf{b}) = \prod_t p(l_t|b_t, l_{t-1}) \tag{2.4}$$

$$p(\mathbf{l}|\mathbf{b}) = \prod_{t=1}^{|\mathbf{b}|} p(l_t|l_{t-1})p(b_t|l_t) \tag{2.5}$$

For the sequence-based k-NN and NB-KDE, we assumed that subjects travelled along the path at consistent speeds. Recall that for the k-NN and NB-KDE, $\mathbf{c} = l_0, l_1, \dots$ represent a virtual location for each second along a path, rather than directly mapping to a geographic location.

For the k-NN, we compute a distance between the test trace $\mathbf{b}$ and training traces $\mathbf{b}^{tr} \in B^{tr}$, as

$$\text{distance}(\mathbf{b}, \mathbf{b}^{tr}) = \sum_{t=0}^{|\mathbf{b}|} |\mathbf{b}_t - \mathbf{b}_t^{tr}|. \tag{2.6}$$

Subsequently, we rank the sequences $\mathbf{b}^{tr}$ by the computed distance from lowest to highest. We classify the instance as the label (i.e., the route) present in the largest fraction of the k-nearest neighbors. If there is a case of a tie, we increment k for that case until the tie is broken.

For the NB-KDE classifier, we determine

$$\arg\max_{\mathbf{c}} p(\mathbf{c}|\mathbf{b}). \tag{2.7}$$

Each location is associated with a kernel density estimator, with Gaussian kernel K:

$$f(b|l) = \frac{1}{N_l} \sum_{i=0}^{N_l} K(b - b_i^l) \tag{2.8}$$

We use the KDE to estimate the probability of a certain bandwidth at a location, so that

$$p(b_t|l_t) = f(b_t|l_t). \tag{2.9}$$

Therefore,

$$\arg\max_{\mathbf{c}} p(\mathbf{c}|\mathbf{b}) = \arg\max_{\mathbf{c}} \prod_{t=0}^{|\mathbf{c}|} f(b_t|l_t^{\mathbf{c}}). \tag{2.10}$$

Evaluation We evaluated the classifiers above with different scenarios using 3-fold cross-validation for hyperparameters, and leave-one-out cross-validation during

Experiment	Classes	NB-KDE	k-NN	HMM	Tput	Freq
4 paths× 1 (Outward)	4	**90.3**	51.4	18.8	7.3	36.6
4 paths× 1 (Inward)	4	**83.3**	43.9	42.4	3.7	28.6
4 paths (Western MA)× 2	8	**75.7**	25.4	26.1	1.7	20.4
2 paths (UMass)× 2	4	75.8	**77.6**	53.3	12.4	44.7

Table 2.1. Classification accuracy depending on which roads are included in the experiment. Bolded entries have the highest accuracy.

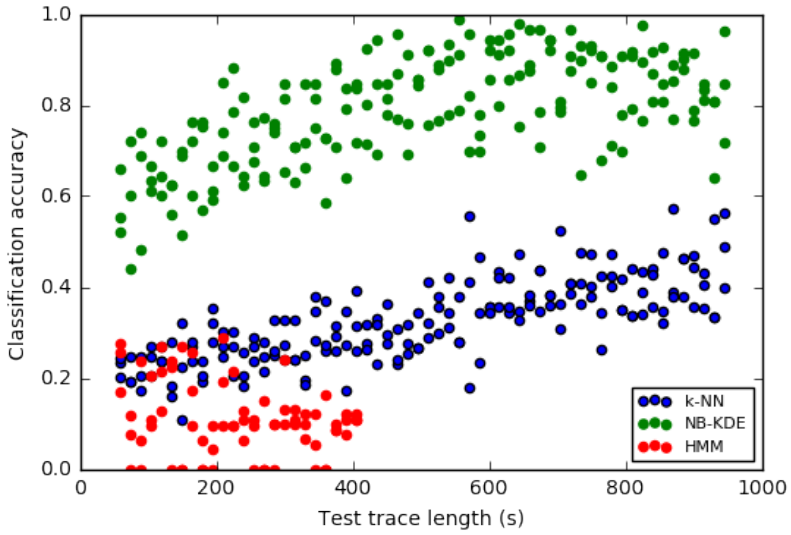

Figure 2.2. Accuracy of experiments (randomized test set) with varying trace lengths.

training. In general, the NB-KDE classifier performed the best. The HMM classifier performed poorly, because the errors in predicting speed variations propagate as the trace gets longer. Results for every experiments are shown in Table 2.1.

The NB-KDE classifier performed relatively well with short traces, as shown in Figure 2.2. Both the k-NN and NB-KDE classifiers increased in accuracy as length increased. This shows that while decreasing the length of the connection to the server does increase user privacy, it may not be enough; other traffic shaping options should be explored.

2.2 Proposed work

I do not propose additional work for this chapter, though in my final dissertation, I will include a version of the work to be submitted to a journal that is more detailed than both this summary and the version presented at the *Privacy Enhancing Technologies Symposium*.

CHAPTER 3

LOCATION PRIVACY THREATS FROM ADVERTISING SERVICES

In this chapter, I propose to study the possibility of an advertising service to be used for stalking users. I look particularly at stalking entourages and co-travelers.[1]

Location based services that contain mobile advertisements forward this information on to ad vendors and their clients. These include popular mobile apps such as Grindr and The Weather Channel. An advertiser can purchase advertising through an affiliate, and some affiliates allow for the client to run JavaScript in the ad. As soon as the ad is displayed on one of these apps, the script runs and in some cases sends data to the ad client along with a randomly chosen advertising ID that is unique to the device.

These mechanisms are designed to allow advertisers to target users depending on information such as location. Location information alone can allow advertisers to see where an app is used the most, and target future advertising to those locations. However, simply anonymizing location data does not protect a user from location profiling. De-anonymizing some of these users may be easy, if, for example, the user uses the app at work or at home the majority of the time. While users may trust the application they are using with location information, they likely do not trust advertising clients. As well, this information is rarely restricted by a privacy policy. Most alarmingly, anybody can be an advertiser and target any geographic location for a very low cost.

---

[1]We have received IRB approval for this project.

Malicious intent There are several ways location data obtained from advertising can be used maliciously. It would be very cost effective for an attacker to determine where, for example, gay users are located, by targeting advertising in a certain city and looking at the coordinates located in residential areas of users who used gay-dating app Grindr. As well, attackers could de-anonymize a particular user and target that user to see in realtime their location or predict their location based on history; this would allow them to stalk the user or determine if the user is home. While Grindr has made the sharing of proximity optional to a user, particularly because of privacy concerns[2], their location can still be found out by advertisers.

Stalking is a particularly real danger posed by advertising. If a stalker knows where a victim spends a lot of their time, and the victim happens to be using one of the popular apps that are part of the advertising network that the stalker is on, they can be followed. We explore this danger further by quantifying how many users are trackable this easily. We postulate that there are broadly three kinds of users: those who use apps at home for the most part, those who use them in a handful of places, and those who use them in many places. We principally use the advertising identifier (ad-ID) — a randomly generated pseudonym associated with each user to build an advertising profile — as ground truth in our experiments. We specifically look at mobile app advertisements, which are difficult for regular users to block.

We explore also the concept of mix zones [4], and how they may both be beneficial and harmful to a person's privacy. On the one hand, a user may want to choose a more populated area to use an app without being de-anonymized. On the other hand, if a person is part of an entourage that does not wish to be stalked, a single person in that entourage could compromise the entire group's privacy by using a privacy-leaking app.

---

[2]http://www.grindr.com/blog/grindr-security/

Experimental design To quantify the threat of stalking using an ad service, I plan to verify the following hypotheses.

1. Users can be seen multiple times, at low cost. We can manipulate how many times each user sees an ad through the bidding settings.

2. There are significant numbers of users who have 0, 1, or 2 *significant stays*. Users with 0 significant stays are nomadic, users with 1 may primarily use their phones at home, users with 2 may be using them at home and work.

3. It should be fairly easy to identify a user if she has any significant stays. There are two likely scenarios: 1. Consider a person whose details we know about (home, work), and we wish to identify. In our experiments, the identified significant stays serve as a surrogate for the outside information we'd have for the person. 2. Consider a user who has an (ad-ID) initially, and then turns off her ad-ID. Can we de-anonymize a query from that location?

4. Given a list of locations, we can identify nomads by targeting ad-IDs in certain locations. We can validate this by predicting their locations based on a public schedule using information from our advertising logs.

5. Nomads with anonymous ids may be de-anonymized by cotravelers with de-anonymized ids. We call this the *entourage attack*. This would mean that it is risky to travel in a group, if there are no strict policies on an entourage member's personal device.

6. Users can be targeted and stalked at a low financial cost to the advertiser. The cost is proportional to how easily a group can be targeted, which in turn is proportional to the population with the area of interest.

Preliminary analysis The existing dataset contains 350 000 impressions from 141 000 users. I validate the first three hypotheses using this dataset.

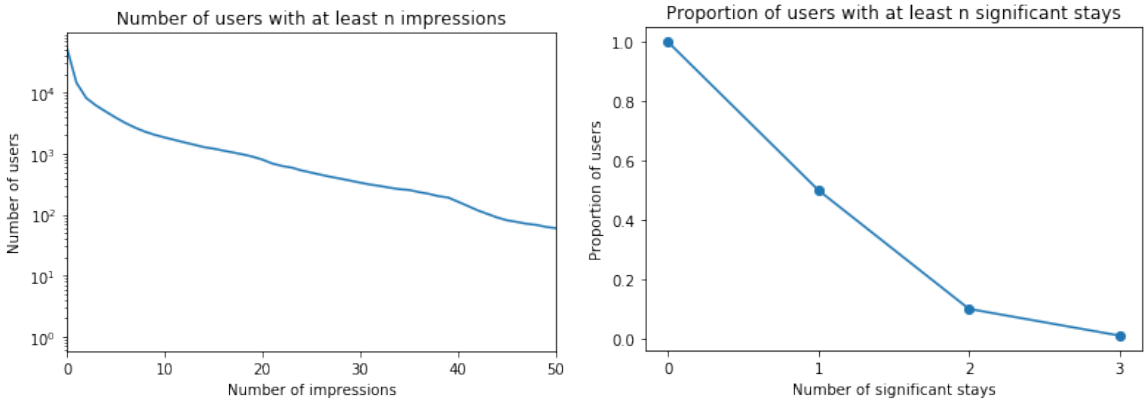

Figure 3.1. Left: Number of users with at least n impressions. Right: Proportion of users with 10 or more impressions that have at least n significant stays.

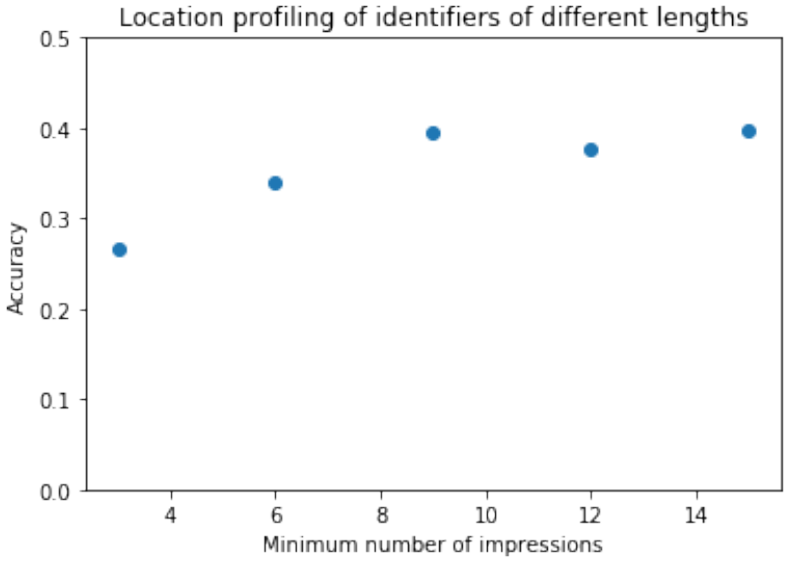

Figure 3.2. Location profiling accuracy depending on the number of impressions

I first do a survey of types of users in our dataset. 3% of users have 10 or more impressions (see Figure 3.1 for more details). Of these users, 50% are seen at the same one location for at least 3 times a week, 10% at two locations, 1% at 3 locations. There are significant amounts of users in the 1- and 2-stay categories. However, 50% have no geographic signature. For users with 10 or more impressions, deanonymization based on location is accurate 39% of the time, testing and training before and after the median times of access. This means even the most naive location profiling methods are effective if we consider significant stays.

Targeting sports teams Despite having no geographic signature in location history, users such as elected officials, celebrities, and sports teams have public schedules. This makes them a viable target for stalking via ads. We target professional sports teams during their active season in 2017. Their travel schedule is public, and relatively unique. As well, there is a cohort of assistants and staff that may reveal the location of the team, whom may want to keep a low profile.

I plan to target NBA and NHL teams in the United States, as well as Premier League teams in the United Kingdom. I build a database of the team's true cities and times from public available information, and target those specific cities for advertising, showing each user the advertisement only once so that travelers are more likely to be reached. I then determine how well advertising identifiers correlate with known location.

There is a risk in targeting sports teams, in that they typically play in large cities, where it is more costly to target tourists or newcomers to the area. If this does not work, I will also attempt to target performers, whom have a public touring schedule and small entourage, but may travel to less populated areas.

Hiding the identifier Users may disable advertising identifiers on their phones. However, users may still be identified by device fingerprinting, depending on the

parameters of the advertising network. I plan to look at fingerprinting techniques, including location features, and how linkable they are depending on a user's location. As well, users may be deanonymized by their entourage, which may also help with linking. I also look at the feasability of location profiling co-travelers as a group.

Summary of proposed work I will continue with this work in three directions. First, using the existing ads dataset, I will develop some methods to target users who regularly travel together or meet up. These users would be especially susceptible to the entourage attack. Second, I will collect additional data by targeting locations of sports games to de-anonymize ad-IDs of users who are part of sports teams. Finally, I will target locations of protests for ad-IDs, and follow those ad-IDs to see whether co-travelers can be identified (i.e. whether I can predict the location of someone with no advertising identifier using the location of someone previously physically close to them).

CHAPTER 4

LOCATION PRIVACY WITHOUT CARRIER COOPERATION

In this chapter, I present methods for users to achieve cell phone anonymity without requiring trust in the service provider[1]. In the preliminary work, I present a GSM-compatible framework that allows for virtual SIM cards so that a user could change her identity regularly. I also present a simple analysis that shows even such a system is susceptible to location profiling, and may not afford the user the desired privacy.

4.1 Preliminary work: Anonymous cell phone systems and vulnerabilities

In this chapter, I prevent several methods a user may pursue to break the link between herself and the cell phone's identifier on the network (i.e. this is an identifier associated with an electronic serial number on the phone or SIM card). These methods are fully compatible with deployed GSM protocols and infrastructure, from 2G systems typically deployed in poor regions of the world to the new 4G standards deployed in Europe and the US. In our attacker model, we consider carriers that are at best uncooperative, and at worst active adversaries.

Methods for anonymous cell phone usage The most naive method to achieve location privacy is to *anonymously purchase many burner phones*, and use each of

[1]This chapter is based in part on work published at the IEEE Workshop on Mobile System Technologies [**?**]

them depending on context. This comes at a high cost, and limits the amount of identifiers a user may have access to. I propose two additional methods: one is a software-based authentication scheme (*ZipPhone*) that requires the cooperation of a mobile virtual network operator (MVNO) that is privacy proactive; the second is a SIM-sharing scheme (*Spartacus*) that allows users to form mix-zones with other users to swap identities.

I plan to investigate the effectiveness of each of these methods, including ease of use, monetary cost, vulnerabilities, and privacy achieved.

ZipPhone Using a WiFi connection not observable to the cellular carrier, a user bootstraps ZipPhone by paying an MVNO for service using an anonymous electronic currency [3, 5, 18]. Upon payment, the user receives one or more IMSIs. This step delinks users and identifiers. The user is now ready to use make and receive calls using VOIP. To do so, they connect to the GSM network, authenticating themselves with the IMSI, which the MNO will verify via signaling to the MVNO (see [**?**] for details).

The user periodically discards IMSIs to avoid the gathering of sufficient geographical information by the carrier to classify successfully against known profiles of users. If the user wishes to purchase additional ZipPhone IMSIs, they need not necessarily utilize WiFi again. They can use their carrier-provided data connection, and contact the ZipPhone MVNO using secure protocols over the Internet to do so.

Spartacus A SIM owner can leave an extra Internet-connected phone at their house or other preferred location (perhaps with the actual SIM) and instruct it to connect to the network remotely; this setup allows the owner to reclaim without necessarily revealing their current location. Peers that wish to lend out use of their SIM can retrieve the K_i key stored in it (this is done only once), or do a man-in-the-middle attack between the phone and SIM during each remote authentication. They can then

produce the K_c and SRES values for a remote ZipPhone requester, who can relay via Wi-Fi (or existing cellular connection) the *random number* issued by the carrier to the peer during a location update. Keys for encryption with GPRS/EDGE also are based on knowledge of K_i and can be similarly relayed.

Location profiling The effectiveness of the classifier is shown in Figure 4.1. In all cases, the attacker is given a preceding month's data as ground truth for training. The blue line is a recreation of results from Mulder et al.: a randomly selected 1-month-long sequence of the cells a user is associated with results in a high accuracy of 80%; Mulder et al. saw[2] about 82%. A random sample of up to 1-hour of cell locations is identifiable 38% of the time; Mulder et al. saw about 44%. In both cases, random chance would be correct about 1% of the time.

Fake pages In modern GSM networks, phones communicate to specific towers only when a call (or SMS text or GPRS data packet) is incoming or originated, rather than whenever a new tower is in range [23, 28]. However, a more advanced and aggressive attacker will proactively cause a phone to communicate with its nearest tower [10] based on an SMS *Class 0* message, ICMP ping, or similar technique.

We can defend against these pages with page-knocking, where the handset answers data pages only after a correct sequence is received (all other pages are ignored). Specifically, the VoIP proxy agree on a function (e.g., a cryptographic hash) that accepts as input a shared secret key and the current time (in minute granularity). The output of the function is then take one bit at a time: if the bit is zero, no packets are sent (and thus no pages) for d seconds; if the bit is one, a packet (and one page) is sent and then it pauses d seconds. The handset can answer at any time; the proxy

[2]These small differences are due to our use of an additional month from the data set.

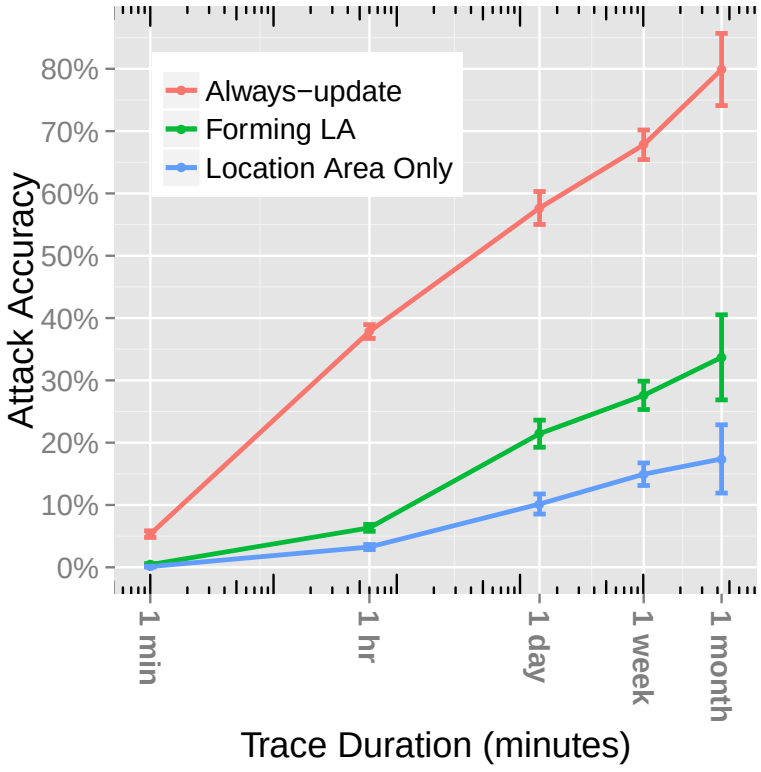

Figure 4.1. The accuracy of the attack defined by Mulder et al. [19] under the always-update policy (top, blue line) and forming LA policy (middle, red line). Our results match well with [19]: an attacker achieves a 38% success rate against users that update their SIM-based identifiers once an hour. Under the latter, more realistic, forming location area update policy, the attacker's success rate falls to 6% when SIM-based identifiers are updated once an hour. The bottom, green line shows the lower bound on any scheme: it represents an unrealistic location management scheme where the carrier learns only the location area but not the cell a user is associated with. Errorbars represent 95% c.i.

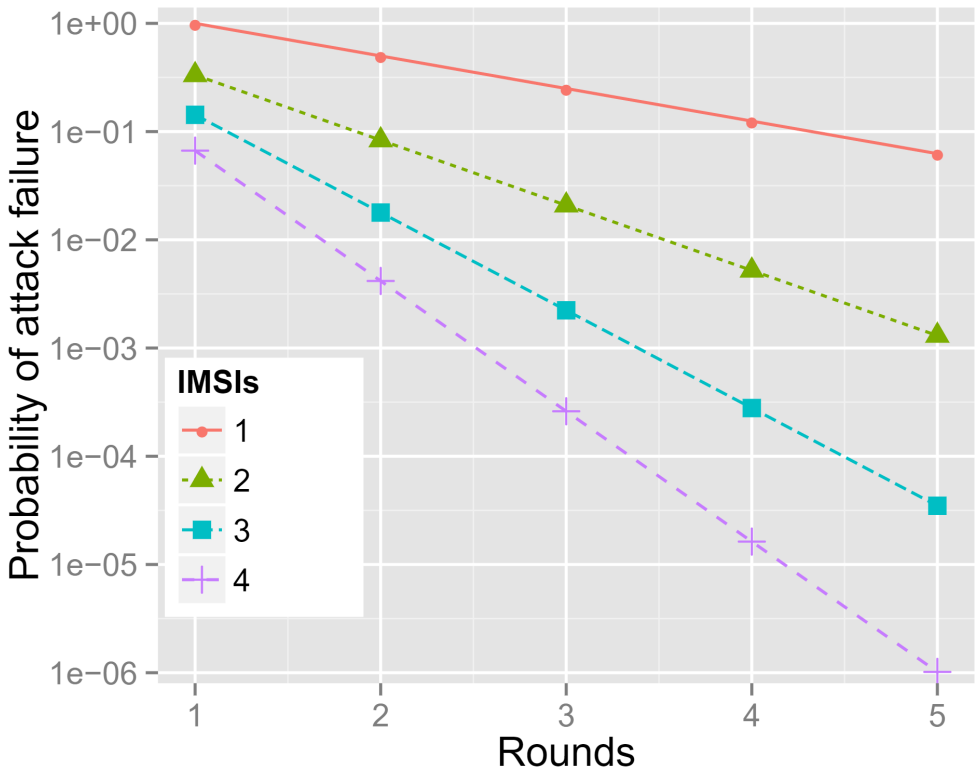

Figure 4.2. The probability that an attacker succeeds in crafting a fake page for varying numbers of rounds r and concurrent IMSIs m, based on Eq. 4.1.

doesn't need to know the value n. An initial non-empty page is required to start the sequence.

The chances that the carrier can falsify the sequence is 2^{-n} for an n-bit sequence. The cost is that the user must wait $(n+1)d$ seconds before answering incoming pages for VoIP calls. On Verizon, I have measured d to be $5.12 * 2$ seconds.

A more efficient scheme where the phone registers m IMSI values (one at a time) from a single physical phone, all provided by the ZipPhone MVNO will take about 10–15 seconds to complete. Whenever the proxy needs to contact the ZipPhone user, it selects a particular non-empty, unordered subset of the m values, and pages each IMSI value in that order. Each IMSI can be paged once every 5.12 seconds with overlapping windows.

For m IMSI values, the number of non-empty unordered subsets for the first round is $\sum_{i=2}^{m} \binom{m}{i} = 2^m - 1$. Because the empty subset can be included in subsequent rounds, for an r-round sequence, the probability of the carrier guessing the correct sequence is

$$\frac{1}{(2^m - 1)(2^m)^{r-1}}. \tag{4.1}$$

Figure 4.2 plots Eq. 4.1. For example, when $m = 3$ IMSIs are used, the registration delay upon entering a new MSC region is 30–45 seconds. When $r = 3$, the probability the carrier can guess the correct sequence of pages is 0.002.

4.2 Proposed work

Some questions remain from the above work:

1. How effective would location profiling and trajectory linking be in de-anonymizing ZipPhone or Spartacus users?

2. How often would users need to go offline or significantly disrupt usage to avoid tracking?

To answer these questions, I plan to simulate ZipPhone or Spartacus using data collected in Chapter 1. I will evaluate different de-anonymization algorithms, and different methods of evasion.

I will also try to implement Spartacus using SIMTrace hardware and simlabTrace[3], which is able to sniff and perform a man-in-the-middle attack between the SIM card and phone. This would be a significant engineering effort to implement a modified handshake during the device's attach procedure to the network, and send information between devices.

[3]https://github.com/kamwar/simlabTrace/wiki

CHAPTER 5

TIMELINE

I plan to produce a draft by the beginning of Fall 2017, and defend by the end of that semester. Several significant efforts remain to complete these studies.

1. Submit my recent work on throughput localization (Chapter 2) to a journal (March 2017).

2. Investigate utility and information theory models for location privacy (April 2017)

3. Find relevant datasets available for academic research and evaluate location profiling and trajectory linking algorithms (May 2017).

4. Investigate simlabTrace as a way to implement Spartacus (May 2017)

5. Develop an experiment to evaluate methods of purchasing targeted advertisements based on sports teams and performers, and de-anonymizing users based on information from co-travelers (March 2017).

6. Data collection of advertisements (March – June 2017).

7. Develop a data collection protocol and perform a field survey of Amherst and surrounding area (March – May 2017).

8. Synthesize a dataset and evaluate these algorithms using surveyed data (June 2017).

9. Use the dataset to simulate scenarios for ZipPhone and Spartacus (July 2017).

BIBLIOGRAPHY

[1] Acquisti, Alessandro. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (2004), ACM, pp. 21–29.

[2] Andrés, Miguel E, Bordenabe, Nicolás E, Chatzikokolakis, Konstantinos, and Palamidessi, Catuscia. Geo-indistinguishability: Differential privacy for location-based systems. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (2013), ACM, pp. 901–914.

[3] Ben-Sasson, Eli, Chiesa, Alessandro, Garman, Christina, Green, Matthew, Miers, Ian, Tromer, Eran, and Virza, Madars. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *Proc. IEEE Symp. Security & Privacy* (May 2014), pp. 459–474.

[4] Beresford, A.R., and Stajano, F. Mix zones: user privacy in location-aware services. In *Proc. Pervasive Computing and Communications Wrkshps* (2004), pp. 127–131.

[5] Bissias, George, Ozisik, A Pinar, Levine, Brian N, and Liberatore, Marc. Sybil-Resistant Mixing for Bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (2014), pp. 149–158.

[6] Cunha, Felipe D, Alvarenga, Davidysson A, Viana, Aline C, Mini, Raquel AF, and Loureiro, Antonio AF. Understanding interactions in vehicular networks through taxi mobility. In *Proceedings of the 12th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks* (2015), ACM, pp. 17–24.

[7] Dabrowski, Adrian, Pianta, Nicola, Klepp, Thomas, Mulazzani, Martin, and Weippl, Edgar. Imsi-catch me if you can: Imsi-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference* (2014), ACM, pp. 246–255.

[8] De Mulder, Yoni, Danezis, George, Batina, Lejla, and Preneel, Bart. Identification via location-profiling in gsm networks. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society* (2008), ACM, pp. 23–32.

[9] Eagle, Nathan, and Pentland, Alex Sandy. Reality mining: sensing complex social systems. *Personal and ubiquitous computing 10*, 4 (2006), 255–268.

[10] Ficek, Michal, Pop, Tomáš, and Kencl, Lukáš. Active tracking in mobile networks: An in-depth view. *Computer Networks 57*, 9 (2013), 1936 – 1954.

[11] Freudiger, Julien, Manshaei, Mohammad Hossein, Hubaux, Jean-Pierre, and Parkes, David C. On non-cooperative location privacy: a game-theoretic analysis. In *Proceedings of the 16th ACM conference on Computer and communications security* (2009), ACM, pp. 324–337.

[12] Greenwald, Glenn, and MacAskill, Ewen. Boundless informant: the nsas secret tool to track global surveillance data. *The Guardian 11* (2013).

[13] Ho, Shen-Shyang, and Ruan, Shuhua. Differential privacy for location pattern mining. In *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS* (2011), ACM, pp. 17–24.

[14] Jaqaman, Khuloud, Loerke, Dinah, Mettlen, Marcel, Kuwata, Hirotaka, Grinstein, Sergio, Schmid, Sandra L, and Danuser, Gaudenz. Robust single-particle tracking in live-cell time-lapse sequences. *Nature methods 5*, 8 (2008), 695–702.

[15] Krumm, John. A survey of computational location privacy. *Personal and Ubiquitous Computing 13*, 6 (2009), 391–399.

[16] LEE RAINIE, SARA KIESLER, RUOGU KANG, and MADDEN, MARY. Anonymity, privacy, and security online.

[17] Markov, Andreĭ. Theory of algorithms.

[18] Miers, Ian, Garman, Christina, Green, Matthew, and Rubin, Aviel D. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *Proc. IEEE Symposium on Security and Privacy* (2013), pp. 397–411.

[19] Mulder, Yoni De, Danezis, George, Batina, Lejla, and Preneel, Bart. Identification via Location-profiling in GSM Networks. In *Proc. ACM Wrkshp on Privacy in the Electronic Society* (2008), pp. 23–32.

[20] Nillius, Peter, Sullivan, Josephine, and Carlsson, Stefan. Multi-target tracking-linking identities using bayesian network inference. In *Computer Vision and Pattern Recognition, 2006 IEEE Computer Society Conference on* (2006), vol. 2, IEEE, pp. 2187–2194.

[21] Qin, Zhen, and Shelton, Christian R. Improving multi-target tracking via social grouping. In *Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on* (2012), IEEE, pp. 1972–1978.

[22] Rainie, Lee. The state of privacy in post-snowden america.

[23] Razavi, Sara Modarres. *Tracking Area Planning in Cellular Networks [Elektronisk resurs] : Optimization and Performance Evaluation*. Linköping, 2011.

[24] Sankar, Lalitha, Rajagopalan, S Raj, and Poor, H Vincent. Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security 8*, 6 (2013), 838–852.

[25] Shokri, Reza, Theodorakopoulos, George, Le Boudec, Jean-Yves, and Hubaux, Jean-Pierre. Quantifying location privacy. In *Security and privacy (sp), 2011 ieee symposium on* (2011), IEEE, pp. 247–262.

[26] Soroush, Hamed, Sung, Keen, Learned-Miller, Erik, Levine, Brian Neil, and Liberatore, Marc. Turning off gps is not enough: Cellular location leaks over the internet. In *International Symposium on Privacy Enhancing Technologies Symposium* (2013), Springer, pp. 103–122.

[27] Sung, Keen, Levine, Brian Neil, and Liberatore, Marc. Location Privacy without Carrier Cooperation. In *Proc. IEEE Workshop on Mobile System Technologies (MoST)* (May 2014).

[28] Wong, V. W.-S., and Leung, V. C.M. Location Management for Next-generation Personal Communications Networks. *IEEE Network 14*, 5 (Sept. 2000), 18–24.

[29] Yang, Bo, and Nevatia, Ram. An online learned crf model for multi-target tracking. In *Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on* (2012), IEEE, pp. 2034–2041.