LOCATION PRIVACY IN CELLULAR NETWORKS

A Thesis Submitted to
the Graduate School of Engineering and Sciences of
İzmir Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in Computer Engineering

by
Okan YAMAN

December 2022
İZMİR

ACKNOWLEDGMENTS

Doing research is a lifelong journey with no destination. However, it has some stops, such as a Ph.D. degree which is also a challenging sub-journey. I have gathered many life lessons, besides academic skills, during my Ph.D. study. Hence, they have further equipped me with insight into this sub-journey toward my doctoral thesis. I want to express my gratitude to some prominent actors who have contributed to this sub-journey by supporting, sympathizing, motivating, and funding.

First of all, I could not have finished this sub-journey if my advisor, Assoc. Prof. Tolga AYAV and my co-advisor, Prof. Yusuf Murat ERTEN, had not supported me. I am highly grateful to both of them for their encouraging and motivating me. Their communication and patience are very precious. They trusted me to research my areas of interest independently. Therefore, having such advisers was my luck during this study.

Special thanks to Assoc. Prof. Kasper RASMUSSEN for accepting me as a visiting researcher at the University of OXFORD, the milestone of this sub-journey, and his invaluable support in finding and developing the dissertation topic. I learned how to do research well through discussions with his research group and our meetings. Hence, I owe him a lot for his continued support, discipline, and patience.

I would like to thank Asst. Prof. Serap ŞAHİN and Assoc. Prof. Ahmet Tuncay ERCAN, for being member of my thesis monitoring committee and for their valuable comments.

I would also like to express my gratitude to Asst. Prof. Nesli ERDOĞMUŞ and Assoc. Prof. Kaya OĞUZ, for assessing my dissertation during the thesis defense exam. Your contributions are highly beneficial.

Many thanks to Dr. Emre Eren KORKMAZ and Ozan UÇAR for their tremendous support on my way to Oxford.

I would also like to thank the Turkey Council of Higher Education (YÖK) for funding me through 100 / 2000 Doctoral Scholarship Program.

Finally, I want to thank Ümit GÜNER for his loyal friendship dates back to our Middle East Technical University (METU) years. Special thanks to my family, especially my mum Hanife YAMAN, who always supports me. I consider myself blessed to have had all of you on this sub-journey.

ABSTRACT

LOCATION PRIVACY IN CELLULAR NETWORKS

Many third-party utilities and applications that run on devices used in cellular networks keep track of our location data and share it. This vulnerability affects even the subscribers who use dumbphones. This thesis defines three location tracing attacks which are based on utilizing the background data and compares them with the most relevant known attacks. We have demonstrated that any attacker who knows two associated cells of a subscriber with adequate background data can deduce the intermediate cell IDs. Also, utilizing the Hidden Markov Model (HMM) increases the accuracy of an attack.

In this dissertation, we introduced novel accuracy metrics for all the anticipated attacks and exploited these for detailed analysis of the threats in a real-life case, a 5G network. This work demonstrates improvements in the current privacy-preserving methods, including adaptation to 5G, and provides insights into preventing this location privacy breach.

Various methods have been proposed to overcome these threats and preserve privacy against possible attacks based on this information. A friendly jamming (FJ) based solution, which offers efficient usage of resources, including computing power and energy, was introduced as a solution for these problems. However, one of the tradeoffs of FJ is its viability. Although some studies try to cope with this challenge, they are complicated and focus on old technologies. We propose a lightweight and flexible FJ scheme to address these challenges. We also demonstrate that our model has the same performance as one of the mentioned studies above in a more straightforward way.

ÖZET

HÜCRESEL AĞLARDA KONUM MAHREMİYETİ

Birçok üçüncü taraf uygulaması ve cep telefonu özellikleri konumumuzu bulmaya ve deşifre etmeye çalışır. Telekomünikasyon firmaları doğal olarak abonelerinin hücresel verilerini izlediği için, tuşlu telefon kullanıcıları bile bu tehdite maruz kalır. Olası saldırı senaryolarını baz alarak sorunun çözümüne ve mahremiyeti korumaya yönelik birçok yöntem önerilmiştir. Bu tez, saldırganların ön verisine bağlı olarak üç tehdit tanımlar ve bunlara en çok benzeyen bilindik saldırılarla kıyaslar. Eğer kullanıcının bağlandığı iki hücre biliniyorsa, yeterli ön veriye sahip saldırgan bunlar arasındaki hücre numaralarını elde edebilir. Gizli Markov Modeli kullanımı da saldırının etkisini artırır.

Bu doktora tezinde, her tehdit için etki ölçüsü tanmladık. Bunları da gerçek dünya örneği olarak bir 5G ortamında ayrıntılı saldırı çözümlesinde kullandık. Bu çalışma 5G'ye uyarlanmaları dahil olmak üzere mahremiyet koruma yöntemlerindeki gelişmeleri gösterir. Ayrıca bu konum mahremiyeti açığının önlenmesine yönelik genel bilgiler de verir.

Son olarak, hesaplama gücü ve enerji gibi kaynakları verimli kullandığı için tanımlanan tehditlere dostça boğma (DB) bazlı bir çözüm önerdik. Ancak DB'nin ödünlemelerinden biri de uygulanabilirliğidir ve bunu çözmeyi amaçlayan çalışmalar da karmaşıktır ve eski teknolojilere dayanır. Bizse bu nedenle daha basit ve esnek olan bir DB yöntemini sunduk. Ayrıca, modelimizin bahsettiğimiz çalışmalardan biriyle aynı performansı daha kolay bir şekilde elde ettiğini gösterdik.

To my beloved mum, dad, and Ümit...

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

CHAPTER 1

INTRODUCTION

In this thesis, we examined data privacy vulnerabilities in cellular networks. There are various problems with privacy in cellular networks, especially the carriers that have access to all the users' data. In this study, we specifically focused on users' location data and simulated location tracking possibilities using real-world 5G network data.

In the proceeding subsections, the problem is explained in more detail.

1.1. Motivation

As human beings are social creatures, communication is one of our basic needs, and we have been trying to improve our communication techniques for ages. However, 20^{th} and 21^{st} centuries witnessed the most rapid development that started with wired methods such as the cable telephone and telegraph. Although we rarely use them nowadays, they were all disruptive technologies for their time as the mobile phone is today.

Cellular (mobile) networks have evolved from 1G analog wireless networks for limited users and places to today's 5G digital wireless networks that everyone can use everywhere. Therefore, mobile networks are now ubiquitous, and we will probably be exploiting this technology as one of the primary communication techniques in the foreseeable future.

One of the application areas of 5G is intelligent homes and cities. Our mobile phones and house appliances, such as TVs, fridges, ovens, and washing machines, can exchange data through this network. From a broader perspective, our vehicles can do the same. Moreover, the Internet of Things (IoT) has emerged as a buzzword. It gives an idea of the trend and current state of the ubiquitous computing that the number of devices with Internet access, thus the amount of transmitted data, will rise continuously. Undoubtedly, location information is one of the mobile entities' most significant transmitted data.

As we experience daily, this technological advancement makes our lives easier. In an emergency, it is a matter of seconds to locate us. We can easily find the closest restaurants and sightseeing places with related data, including audio and video guides. Some other usage areas of Location-Based Services (LBSs) are social networking, location-based advertisements, and tracking systems.

Unfortunately, the above advantages brought severe privacy concerns at the same time. Inherently, LBSs have to exploit users' position data to operate, and manual management of some of our data sharing policies is possible through mobile phones. Moreover, subscribers might use trusted LBSs to preserve their privacy. However, there is no way out of that black hole, the data gathering procedure of the LBSs, since current Big Brothers, the carriers, surveil us constantly. Indeed, this black hole can attract subscribers with dumbphones by using their associated Cell IDs.

Researchers have proposed several solutions to preserve location privacy and escape the black hole as much as possible. Most schemes rely on computational techniques, such as anonymization, obfuscation, and Bayesian inference. We will compare them in this study and also analyze the Hidden Markov Model (HMM), which is one of the main methods in the attacker models of the mentioned schemes. Section 3.3.1 will explain HMM process and give the necessary background on it. Although there are many solutions in the literature, they need to be updated for emerging technologies such as 5G. Section 2.1.4 will provide a brief highlight for 5G-specific countermeasures, and security professionals must be aware of such potential threats to develop 5G-adaptive solutions. We also proposed a solution to the problem defined (see Chapter 5).

In this thesis, we attempt to reveal that an adversary with inadequate data can guess the missing Cell IDs. Indeed, inferring the trace will not be so complicated whenever the attacker has the same data as the carriers. Since contemporary Big Brothers (telecommunication companies and governments) inherently possess our private data, they can perform these attacks without extraordinary effort. Furthermore, some of the required data for proposed threats, such as road junction coordinates, can easily be gathered through any map application. Therefore, the stated attacks have consistency with any real-world threat. We also try to maintain the consistency on the proposed solution to the attacks. There are three criteria that we take into account for the solution: maximum performance, minimum side-effect, and resource (computational power and energy) efficiency. We demonstrate that our friendly jamming approach fulfills the mentioned criteria (see Chapter 5).

1.2. Contributions of the Thesis

In this thesis, there are four significant contributions.

First of all, we introduced two novel attacks that breach location privacy preserving mechanisms (LPPMs). The first is trace deduction which employs the HMM. The other is the missing Cell ID finding attack. If an attacker knows the origin and destination cells in advance, it is straightforward to guess the absent cells of the user's trace with high accuracy. We also compared the proposed attacks and the most related ones in the literature.

Secondly, we improved the HMM process of Shokri et al. (2011) and Shokri et al. (2011) (see Section 2.1.4 for comparison). Therefore, an adversary can infer a finer-grained subscriber trace, resulting in a more severe threat.

Thirdly, we introduced new accuracy definitions for each threat and simulated them on a real-world dataset. The cell types are similar to microcells. Hence, we can assume it is a 5G environment, and present LPPMs can exploit our study to improve themselves.

Finally, we proposed a 5G-adaptive countermeasure due to its properties mentioned in detail (see Chapter 5).

1.3. Organization of the Study

The remaining sections of the thesis are as follows: Chapter 2 provides the related work of both Chapter 3 and 5. Moreover, we compare the most related models in the literature and the proposed one in this dissertation. Chapter 3 gives some background information on the location privacy problem we addressed. After having stated the problem mathematically in Section 3.1, we propose the threat model in Section 3.2. Then the explanation of trace deduction mechanisms of attackers follow it in Section 3.3. Chapter 4 evaluates our model with a real-world dataset similar to 5G. The evaluation includes a detailed analysis of each attacker. Then we proposed a countermeasure for the attacks defined in Chapter 5 which begins with a brief introduction and motivation section in Section 5.1. Section 5.2 describes the system model. The results are shared and discussed in the Section 5.3. Chapter 6 consists of a brief discussion on risks, limits and future directions of our research. Moreover, there exits prospective counter attack scenarios against the FJ model in the same chapter. Finally, we conclude the thesis with Chapter 7. There are also appendices which comprised of five chapters. Transition and emission matrices used in section 3.3 can be found in Appendix A. We provide exploited algorithms for Chapter 4 in Appendix B. Some extended simulations reside in Appendix C and D. Finally, there are some extended analysis of little brother in Appendix E, and association rate-based (density) analysis of BSs in Appendix F.

1.4. Publications

The thesis lies on top of the following studies:

- Okan Yaman, Kasper Rasmussen, Tolga Ayav, and Yusuf Murat Erten, "Big Brother is Watching You: A Case Study on The Amount of Deduced Data Through Cell-IDs," under review
- Okan Yaman, Tolga Ayav, and Yusuf Murat Erten, "A Ligthweight Self-Organized Friendly Jamming," to be published by the International Journal of Information Security Science

CHAPTER 2

RELATED WORK

2.1. Location Privacy in Cellular Networks

Many techniques have been proposed in the last decades to keep location data private for various networks such as wireless sensor networks, cognitive radio networks, internet of things (IoT) networks, and mobile (cellular) networks. Jiang et al. (2019) (Jiang, Han, Wang, and Guizani 2019) expressed a detailed survey on wireless sensor networks (WSNs) and a systematic summary of existing position privacy protection research. Another survey on WSN is by Conti et al. (2013) (Conti, Willemsen and Crispo 2013). It is a comprehensive and, to the best of our knowledge, unique survey on source location privacy (SLP) in WSNs. The main contributions are classifying adversaries, discussing each countermeasure, and gaining insight into attacking capabilities. Grissa et al. (2017) (Grissa, Hamdaoui, and Yavuz 2017) try to determine the vulnerabilities of current Location Privacy Preservation Mechanisms (LPPMs) on cognitive radio networks (CRNs) and discuss the potential countermeasures on it. Zakhary et al. (2018) (Zakhary and Benslimane (2018)) explain privacy-protection solutions for opportunistic mobile networks. In that study, there is also location privacy research and its applicability, a taxonomy of current approaches, and a unified framework with its application.

Most of the proposed solutions are based on computational location privacy methods. Primault et al. (2018) (Primault, Boutet, Mokhtar, and Brunie 2019) present a survey that examines classical to modern approaches. They divide LPPMs into online and offline use cases with evaluation metrics for assessment. Another comprehensive survey on computational location privacy is the study of Krumm (2009). He examines the location privacy perception of people and computation attacks with countermeasures on leaked location data.

The studies mentioned above focus on a specific topic, either a network or a method. However, Liu et al. (2018) (Liu, Zhou, Zhu, Gao, and Xiang 2018) and Jiang et al. (2021) (Jiang and Li, Zhao, Zeng and Xiao, Iyengar 2021) are comprehensive studies. Therefore, we exploited both of these in classifying LPPMs. Liu et al. (2018) (Liu, Zhou, Zhu, Gao, and Xiang 2018) examine an in-depth systematic study on location privacy and its applications based on five elements: location privacy definition, attacks and attackers, countermeasures, location privacy metrics, and the current status of location privacy applications. There is a qualitative and quantitative comparison and analysis of LPPMs in Jiang et al. (2021) (Jiang and Li, Zhao, Zeng and Xiao, Iyengar 2021). They also discuss their applicability.

Although there are various classifications for LPPMs, we divide them into three main groups: anonymization, obfuscation, and cryptography.

2.1.1. Anonymization

Anonymization techniques try to prevent leakage of both the user identity and corresponding location data. Hence no attacker can correctly match the mentioned information to the owner, if these methods are performed successfully.

2.1.1.1. K-Anonymity

K-anonymity is based on rendering locations indistinguishable among other (k-1) records. Moreover, that method is the underlying mechanism of the cloaking, and Jiang et al. (2021) (Jiang and Li, Zhao, Zeng and Xiao, Iyengar 2021) define the technique of Gruteser and Grunwald (2003), and Gedik et al. (2005) (Gedik and Liu (2005)) as cloaking as well. Although suppression and generalization techniques of Samarati et al. (1998) (Samarati and Sweeney (1998)) provide privacy by trying to obscure the data behind its other (k-1) counterparts, Liu et al. (2018) (Liu, Zhou, Zhu, Gao, and Xiang 2018) define them as k-anonymity instead of cloaking (see Gedik and Liu (2005), Gruteser and Grunwald (2003), Xu and Cai (2008), Huo et al. (2011), and Bettini et al. (2009)). K-anonymity assumes that a trusted authority (TA) is responsible for the LBS which possess each users location data and perform the operation of anonymization. If users send their position data in a query, the TA creates a set of k users and declare an obfuscation region with k locations including the corresponding position data (see Krumm (2007)).

Two methods are defined in the following studies: the multiple distributed server-based (Zhong and Hengartner (2009), Li et al. (2015)) or peer to peer transmission-based (Chow et al. (2011)). The model of Solanas et al. (2008) (Solanas, Sebe, and Domingo-Ferrer 2008), p-sensitivity, seeks to provide that there exists at least p distinct records for all private attributes. We can guarantee that position of users cannot be identified among l distinct locations through l-diversity (see Machanavajjhala et al. (2007) and Bamba et al. (2008)). In a similar manner, Li et al. (2007) (Li, Li, and Venkatasubramanian 2007) presented a technique called t-closeness to compensate for limitations found in the l-diversity mechanism. Moreover, Mascetti et al. (2009) (Mascetti, Bettini, Wang, Freni, and Jajodia 2009) achieve the same for moving entities by the method of historical k-anonymity.

These techniques can be exposed to some threats, including inference attacks whenever the LBS exploits any kind of user identity to perform its operations (Krumm (2007), Palanisamy and Liu (2014a)).

2.1.1.2. Mix-Zones

The other anonymization method, mix-zones, differs from the k-anonymity in terms of user-id data. According to the model of Beresford et al. (2003) (Beresford and Stajano (2003)), names of users of pseudonyms are modified continuously to provide privacy. They were pioneers of this approach and hence, inspired many other studies. For example, Carianha et al. (2011) (Carianha, Barreto, and Lima 2011), Gerlach (2006), Hoh et al. (2005) (Hoh and Gruteser (2005)), Li et al. (2006) (Li, Sampigethaya, Huang, and Poovendran 2006), Sun et al. (2010) (Sun, Su, Zhao, and Su 2010) extended the same idea to rectangular or circular areas. The main drawback of these extensions is that they are susceptible to timing attacks as asserted by Palanisamy et al. (2012) (Palanisamy, Liu, Lee, Singh, and Tang 2012), and some countermeasures are proposed such as, Buttyán et al. (2007) (Buttyan, Holczer, and Vajda 2007), Freudiger et al. (2007) (Freudiger, Raya, Felegyhazi, Papadimtratos, and Hubaux 2007), Freudiger et al. (2009) (Freudiger, Shokri, and Hubaux 2009), and Palanisamy et al. (2011) (Palanisamy and Liu (2011)). However, those are not remedies for transition attacks. Therefore, Palanisamy et al. (2014b) (Palanisamy and Liu (2014b)) and Palanisamy et al. (2014) (Palanisamy, Liu, Lee, Meng, Tang, and Zhou 2014) tried to cope with this threat.

A dynamic scheme for vehicular networks is presented by Ying et al. (2013) (Ying, Matrakis, and Mouftah 2013). It creates mix-zones upon the request of vehicles. Palanisamy et al. (2014a) (Palanisamy and Liu (2014a)) propose the MobiMix framework which is based on road networks. Lu et al. (2011) (Lu, Lin, Luan, Liang, and Shen 2012) employ transforming pseudonyms at social stops, however Gao et al. (2013) (Gao, Ma, Shi, Zhan, and Sun 2013) propose a mix-zone model for mobile crowdsensing applications. Xu et al. (2016) (Xu, Zhang, and Yu 2016) introduce a mixed-integer programming model to reduce the duration of data leakage is less than a privacy threshold.

All anonymization techniques are designed to satisfy a degree of privacy, such as Freudiger et al. (2012) (Freudiger, Manshaei, Hubaux, and Parkes 2012). They propose a game-theoretic approach for modeling the behavior of mobile nodes, and each actor tries to minimize their cost while maximizing their privacy. The aim of Xiao et al. (2015) (Xiao and Xiong (2015)) is modeling the behavior of user decision. Yang et al. (2013)

(Yang, Fang, and Xue 2013) describe auction-based approaches. Gong et al. (2015) (Gong, Chen, Xing, Shin, Zhang, and Zhang 2015) exploit social group utility approach to provide location privacy. Chatzikokolakis et al. (2017) (Chatzikokolakis, Palamidesi, and Pazii 2017) provide a comparative study on location privacy.

2.1.2. Obfuscation

The general aim of obfuscation methods is to decrease the precision of location data through addition of dummy locations or external noise, or intentionally depleting the precision of locations sent to the LBS server.

2.1.2.1. Dummy Locations

The first model was proposed by Kido et al. (2005b) (Kido, Yanagisawa, and Satoh 2005b). As its name implies, the target of this method is to hinder actual locations of users by transmitting fake location entries (dummies) to the LBS server besides the actual ones. Kido et al. (2005a) (Kido, Yanagisawa, and Satoh 2005a) choose the dummy entries randomly, therefore, no server need to be trusted, and satisfactory degrees of privacy can be gathered with no significant loss of accuracy.

The conventional dummy technique deals with only single points. However, You et al. (2007) (You, Peng, and Lee 2007) generate dummy trajectory of users by rotating or random patterns. Lei et al. (2012) (Lei, Peng, Su, and Chang 2012) rotate the trajectory of a user to perform the distance deviation for preventing any attacker from distinguishing true trajectory from the dummies.

Krumm (2009) tries to spoof the driving motions of a user through a dataset consisting true GPS tracks of 253 drivers. Moreover, Chow et al. (2009) (Chow and Golle (2009)) employ Google Maps to increase the degree of privacy. Do et al. (2016) (Do, Jeong, Choi, and Kim 2016) describe a conditional probability-based model for adversaries having some background knowledge, such as spatio-temporal data. Hara et al. (2016) (Hara, Suzuki, Iwata, Arase, and Xie 2016) design a model to produce natural dummies that fulfills requirements of the real world. Chen et al. (2016) (Chen and Shen (2016)) choose dummies by maximizing minimum distance (MaxMinDistDS) and its refined version.

2.1.2.2. Differential Privacy

Differential privacy (DP) is based on adding random noise to the required data. The original idea of DP relies on the study of Dwork (2006) which is designed to protect privacy for statistical databases. Moreover, as shown by Gursoy et al. (2018) (Gursoy, Liu, Truex, Yu, and Wei 2018) DP has mathematically proven privacy-protection hence, can be considered as a standard privacy-protection technique in practice.

Dewri (2012) designes a k-anonymity-based DP model to preserve privacy. Andrés et al. (2013) (Andres, Bordenabe, Chatzikolakis, and Palamidessi 2013) define the concept of geo-indistinguishability for providing privacy of users exact locations. Chatzikokolakis et al. (2014) (Chatzikolakis, Palamidessi, and Stronati 2014) exploit bogus position data when the user is in its vicinity. Chatzikokolakis et al. (2015) (Chatzikolakis, Palamidessi, and Stronati 2015) improve this study by considering density of the network. Another extension of DP belongs to Bordenabe et al. (2014) (Bordenabe, Chatzikolakis, Palamidessi 2014). They consider time complexity to provide privacy. Kifer et al. (2011) (Kifer and Machanavajjhala (2011)) and Olteanu et al. (2016) (Olteanu, Huguenin, Shokri, Humbert, and Hubaux 2016), on the other hand, demonstrate some vulnerabilities of the DP.

2.1.2.3. Location Obfuscation (Path Confusion)

Location obfuscation and path confusion are the two definitions used by Liu et al. (2018) (Liu, Zhou, Zhu, Gao, and Xiang 2018) and Jiang et al. (2021) (Jiang and Li, Zhao, Zeng and Xiao, Iyengar 2021), respectively. As shown by Gruteser et al. (2005) (Gruteser and Hoh (2005)), the most probable trace of a user can be deduced by exploiting spatio-temporal data. They also demonstrate that anonymized pseudonyms cannot be a countermeasure for it.

One of the traditional spatial obfuscation mechanisms is designed by Ardagna et al. (2009) (Ardagna, Cremonini, di Vimercati, and Samarati 2009) and Ardagna et al. (2007) (Ardagna, Cremonini, di Vimercati, and Samarati 2007). Here, the user declares a circular region rather than the exact location to the LBS server. Gutscher (2006) introduces a method that relies on coordinate transformation, such as rotating and shifting. Apart from spatial obfuscation, there are also studies on its temporal counterpart. Hwang et al. (2013) (Hwang, Hsueh, and Chung 2013) design a fresh time-obfuscating approach. They dispatch user queries intermittently to spoof the LBS server. Terrovitis et al. (2008) (Terrovitis and Mamoulis (2008)) exploit spatio-temporal obfuscation to keep the declared traces private. Likewise, Ghinita et al. (2009) (Ghinita, Damiani, Silvestri, and Bertino 2009) describe a spatio-temporal mechanism based on cloaking.

Duckham et al. (2005) (Duckham and Kulik (2005)), have a more sophisticated attacker model, and they exploit obfuscation graphs on road networks. Ghinita et al. (2009) (Ghinita, Damiani, Silvestri, and Bertino 2009) use background map data similarly. Xiao et al. (2015) (Xiao and Xiong (2015)) presented a scheme that consider the temporal similarities in position records.

As demonstrated by Eckhoff et al. (2011) (Eckhoff, German, Sommer, and Dressler 2011), Hoh et al. (2010) (Hoh, Gruteser, Xiong, and Alrabady 2010), and Meyerowitz et al. (2009) (Meyerowitz and Roy Choudhury (2009)) path confusion exploits the relationship among users to provide privacy. Meyerowitz et al. (2009) (Meyerowitz and Roy Choudhury (2009)) introduced a mechanism, CacheCloak, to improve the performance of path confusion.

2.1.3. Cryptography

Cryptographic methods for LPPMs employ encryption to provide location privacy, and Jiang et al. (2019) (Jiang and Li, Zhao, Zeng and Xiao, Iyengar 2019) divide them into the following groups:

2.1.3.1. Space Transformation (ST)

As its name implies, this technique is based on transforming the location data and queries to another space. The operation takes place before sending the mentioned data to the LBS server and processing the queries in that space.

Khoshgozaran et al. (2007) (Khoshgozaran and Shahabi (2007)) are the pioneers of ST. They employ some cloaking mechanisms to provide position privacy. The main drawback of their study is precisely determining all neighbors, and Lin et al. (2008) (Lin, Bertino, Cheng, and Prabhakar 2008) try to keep the closeness of transformed records to the original ones. Khoshgozaran et al. (2013) (Khoshgozaran, Mehr, and Shahabi 2013) propose an encrypted hash function based-model. Their aim is having a robust system against adversaries with substantial background data.

2.1.3.2. Secure Multiparty Computation (SMC)

The main motivation of this method is to spoof an unreliable third party or LBS servers. Multiple parties perform the same operation, and they are unaware of the inputs used by each other which is the main key point of SMC.

Marias et al. (2005) (Marias, Delakouridis, Kazatzopoulos, and Georgiadis 2005) exploit the secret sharing technique. They split the private position data, and disseminate to each LBS server. Stirbys et al. (2017) (Stirbys, Nabah, Hallgren, and Sabelfeld 2017) exploit homomorphic encryption to perform SMC for keeping the closeness of positions. Chen et al. (2018) (Chen, He, Yuan, Chen, Du, and Xiang 2018) utilize homomorphic encryption to satisfy location privacy and efficiency of LBSs at the same time.

2.1.3.3. Private Information Retrival (PIR)

The aim of PIR is to guarantee that it is impossible for the server to distinguish the confidential query object, if it is queried by a client.

Ghinita et al. (2008) (Ghinita, Kalnis, Khoshgozaran, Shahabi, Tan 2008) have been the first to propose the concept of PIR. They design a Hilbert curve based-scheme for closest neighbor queries, and hence there will be no dependency on any trusted third party (TTP). A k^{th} nearest neighbor (KNN) and range query extension of PIR methods was carried out by Khoshgozaran et al. (2011) (Khoshgozaran, Shahabi, and Mehr 2011). Mouratidis et al. (2012) (Mouratidis and Yiu (2012)) introduce a countermeasure relying on PIR for finding the shortest path.

2.1.4. Comparison of Most Related Proposed Models

In this section, there is a qualitative comparison among the proposed attacks in this study and those in the most relevant studies discussed in previous sections. We have defined the necessary and sufficient criteria as being related to the type and methodology of the attacks. Additionally, some of the other works have accuracy definitions which are mathematically different from our accuracy models. Moreover, URL links to the dataset used by some studies no longer exist. For these cases, it is not logical to compare the studies quantitatively, and a qualitative comparison should be used instead. For a brief comparison between our model and the most related works, see Table 2.1.

Shokri et al. (2011) (Shokri, Theodorakopoulos, Le Boudec, and Hubaux 2011) and Shokri et al. (2011) (Shokri, Theodorakopoulos, Danezis, Hubaux, Le Boudec 2011) have the same type (Location Exposure) and method (HMM) of attacks. They also have accuracy definitions. Among all the studies in Table 2.1, the model of Shokri et al. (2011) (Shokri, Theodorakopoulos, Danezis, Hubaux, Le Boudec 2011) is the closest to our model, and we have improved their HMM approach by employing a finer-grained Markov

Table 2.1. Comparison of our model and the most related works

WORK	TYPE	METHOD	ACCURACY
Shokri et al. (2011)	Location exposure	Detailed HMM	+
Shokri et al. (2011)	Location exposure	HMM	+
De Mulder et al. (2008)	Identification	Markovian process	+
Cheng et al. (2006)	Tracing	Velocity & time	-
Wang and Liu (2009)	Replay	Anonymization re-run	-
Fawaz and Shin (2014)	Tracing	Location updates	-
This study	Trace deduction*	HMM**	+***

*Novel trace deduction attacks
**Fine-grained HMM
*** Threat specific accuracy definitions

chain model. Similar to our model, theirs introduced a transition matrix to calculate transition probability from one region to another; however, by exploiting past n locations, we were able to create a finer-grained algorithm, providing greater accuracy.

The purpose of attacks defined by De Mulder et al. (2008) (De Mulder, Danezis, Batina, and Preneel 2008) is user identification. Their methods are the Markovian model and the Sequence of Cell-IDs, and they also use accuracy evaluations. Their usage of the Markovian model in cellular networks is similar to ours. Cheng et al. (2006) (Cheng, Zhang, Bertino, and Prabhakar 2006) examine an inference attack that results in tracing the users path, exploiting the users velocity and time data. Some solutions were proposed, such as data cloaking, patching, and delaying. Introducing track inference attacks in mobile networks shows similarity with our work in terms of deducing location data. A replay attack examined by Wang et al. (2009) (Wang and Liu (2009)) use the anonymization re-run technique, and the solutions proposed are: k-anonymity and l-diversity. The similarities with the current study are introducing a road network and mobile services. The final study for comparison is Fawaz et al. (2014) (Fawaz and Shin (2014)). Three types of attack are anticipated: tracing, identification, and profiling. Attackers achieve their goal in a method very similar to the current study, i.e., by location updates sent by users, which allow accessing users' locations. Their proposed solution is named LP-Guardian.

There are also many proposed solutions against these attacks in the literature. We discuss the 5G-specific prospective countermeasures, which are the most relevant to the current study. These studies focus on three areas: data privacy, location privacy, and identity privacy, and we investigate the second of these, in line with the nature of our proposed attacks.

The problem of privacy leakage in Vehicular Social Networks (VSNs) in 5G has been examined by Liao et al. (2018) (Liao, Li, Sun, Zhang, Chang 2018), with authors asserting that the best-known solution is the combination of Mix-Zone and Group Signature technology, the Mix-Group method. To tackle real-world implication difficulties of this method, they propose the Dynamic Group Division Algorithm (DGD). 5G base stations (GnodeBs) have shorter coverage ranges than their earlier counterparts, which may lead to privacy leakage threats that are the subject of Qu et al. (2020) (Qu, Zhang, Li, Zhang, Zhai, and Yu 2020). Hence, they propose a model for the Generative Adversarial Network (GAN) to augment position privacy through cloaking.

The study of Checa et al. (2020) (Checa and Tomasin (2020)) focuses on privacy leakage in 5G mmWave devices. The authors introduce a novel beamformer scheme that lies on the Angle of Destination (AoD) of the paths produced by User Equipment (UE). This model functions by blocking the receiving BS to estimate the AoD. Yang et al. (2021) (Yang, Wang, Wu, Wang, Song, and Ma 2021) examined the problem of trajectory privacy of truck drivers in intelligent logistics, proposing the Quadtree-based location perturbation (OLP) and Quadtree-based joint location perturbation (QJLP) algorithm as a solution. Similar to previous studies, Tomasin et al. (2021) (Tomasin, Centenaro, Seco-Granados, Roth, and Sezgin 2021), location-privacy issues of 5G are addressed, and three countermeasures are proposed. The first is Virtual Private Mobility Networks (VPMs) for helping end users to cover their positions. The second is anonymization techniques for providing security in the physical layer, and the final recommendation is an independent authentication and billing authority. Boualouache et al. (2021) (Boualouache, Sedjelmaci, Engel 2021) consider position-privacy in 5G-enabled Vehicular Fog Computing (VFC), recommending a consortium blockchain-based cooperative model that provides cooperative Pseudonym Changing Processes (PCPs), providing a sense of security for users. The final countermeasure is suggested by Cui et al. (2021) (Cui, He, Chen, Jin, Xiang, Yang 2021). They examine position privacy issues in the 5G-facilitated Mobile Edge Computing (MEC) environment. The proposed scheme is the "LBS@E", allowing mobile users to reach LBSs without revealing their actual positions.

These proposed countermeasures are highly likely to be effective against the attacks proposed in this study, and as future research, it is planned to apply each of them in response to our proposed attacks and evaluate their performance.

2.2. Friendly Jamming

The idea of jamming lies on top of disrupting communication by decreasing the signal to noise ratio (SNR). However, we exploit this concept as a defensive countermeasure as many other studies mentioned below. Hence, it is called as "friendly."

There exist many friendly jamming (FJ) models in the literature. Authors of Li et al. (2021) (Li, Dai, Shukla, Li, Xu, and Imran 2021) provide a survey on IoT and various emerging technologies. Another survey can be seen in Shaaban et al. (2021) (Shaaban and Faruque (2021)). They present a comprehensive survey on physical layer security and countermeasures for 5G.

An energy-efficient jamming model to provide the Physical Layer Security (PLS) in Visible Light Communication (VLC) is presented in Pham et al. (2021) (Pham and Pham (2021)). The authors of Li et al. (2022) (Li, Lei, Diamantoulakis, Fan, and Karagiannidis 2022) propose a friendly jammer scheme to increase the secrecy sum rate for the Non-Orthogonal Multiple Access (NOMA). In Kim et al. (2021) (Kim, Biswas, Bohacek, Mackey, Samoohi, and Patel 2021), jamming-aware routing and MAC protocols based on the intermittent FJ are described. According to the model, friendly mobile nodes are informed in advance based on the schedule of jamming. Dang-Ngoc et al. (2022) (Dang-Ngoc, Nguyen, Ho-Van, Hoang, Dutkiewicz, Pham, and Hwang 2022) designed a cooperative FJ scheme for swarm unmanned aerial vehicle (UAV) assisted networks . They tried to suffice the energy efficiency due to the limited energy sources of UAVs. In Li et al. (2020) (Li, Dai, Wang, Imran, Li, and Imran 2020), a scheme to improve the PLS of cooperative wireless networks can be seen. Multiple trusted and friendly relays are exploited without the attacker's channel state information (CSI). There are novel secrecy capacity (SC) schemes and assessments of the FJ efficiency in Jin et al. (2019) (Jin, Zeng, and Zhang 2019). Kim et al. (2016) (Kim and Choi (2016)) have an optimal power allocation approach exploiting FJ for PLS by increasing the secrecy outage probability (SOP). In Li et al. (2018) (Li, Wang, Dai, and Wang 2018), a novel FJ-based defense mechanism is proposed against eavesdropping for industrial crowdsensing networks. Moreover, a detailed model that considers some channel conditions can be found.

A scheme of FJs residing on access points (APs) is designed in Berger et al. (2016) (Berger, Gringoli, Facchi, Martinovic, and Schmitt 2016). It is the first real-world evaluation in a campus network with IEEE 802.11 protocol. The authors of Wang et al. (2019) (Wang, Dai, Wang, Xu, and Sangaiah 2019) use multiple UAV FJs against eavesdropping. There also exist the deployment flexibility and a negligible effect on the legitimate transmission. In Berger et al. (2014) (Berger, Gringoli, Fachi, Martinovic, and Schmitt 2014), the applicability of FJ on real-world IEEE 802.11 AP is discussed. The FJ model for the internet of medical things (IoMT) is examined with two case studies Li et al. (2020) (Li, Dai, Wang, Imran, Dengwang, and Imran 2020). The effect of cooperative FJ on the security of wireless networks is investigated in Vilela et al. (2010) (Vilela, Bloch, Barros, and McLaughlin 2010). Mobini et al. (2018) (Mobini, Mohammadi, and Tellambura 2019) proposed a full-duplex jammer protocol with a half-duplex version for energy harvesting and security . In Martinovic et al. (2009) (Martinovic, Pichota, and Schmitt 2009), the combination of the broadcast medium, frequency jamming, and multipath propagation is introduced to provide message authentication. A novel scheme, ally-friendly jamming, is also proposed for authentic communication through secret keys by Shen et al. (2013) (Shen, Ning, He, and Dai 2013). A game-theoretic scheme is presented to exploit non-altruistic users as cooperative jammers for secure communication in Stanojev et al. (2013) (Stanojev and Yener (2012)). The authors of Mostafa et al. (2014) (Mostafa and Lampe (2014)) discuss the PLS of the VLC model based on FJs. The amount of confidentiality gathered by exploiting FJs is evaluated in Tippenhauer et al. (2013) (Tippenhauer, Malisa, Ranganathan, and Capkun 2013). They consider an attacker with multiple antennas. An FJ-based security model is proposed in Vilela et al. (2011) (Vilela, Bloch, Barros, and McLaughlin 2011), and analysis for different CSIs is presented to provide optimal jamming.

There is also an increasing attention to the implementation of the FJ for 5G. The cooperative jamming for a two-tier 5G Heterogeneous Network (HetNet) is designed by the authors ofHuo et al. (2019) (Huo, Fan, Ma, Cheng, Tian, and Chen 2019). They also introduce three secrecy transmission algorithms. Two case studies on PLS of UAVs are discussed in Li et al. (2019) (Li, Fei, Zhang, and Guizani 2019).

CHAPTER 3

LOCATION PRIVACY IN CELLULAR NETWORKS

This chapter will discuss the Cell ID-based trace deduction problem and its threat model.

3.1. Statement of Problem

Let $R = \{r_1, r_2, ..., r_N\}$ be a set of N different regions that partitions an area where a mobile subscriber s moves and assume time is discrete. Let $T = \{1, ...,\text{T}\}$ be a set of time instances the associated cells of s are observed. The precision of the subscriber's mobility is related to the granularity of Z and T.

Assume there are four subscribers s_1, s_2, s_3 and s_4. The duration between two consecutive time instances Δt and their types of cells are illustrated below (see Table 3.1).

	Type of Cell	Δt
s_1	Macrocell	10 seconds
s_2	Microcell	10 second
s_3	Macrocell	1 second
s_4	Microcell	1 second

Table 3.1. Mobile subscribers' granularity comparison

Since the type of cell of s_4, microcell, is the smallest, we can call that subscriber the finest. Similarly, s_1 can be considered the coarsest since it has the largest cell type and duration. s_4 is finer than s_3 and s_3 is coarser than s_2 considering Δt and types of cells, respectively.

The spatiotemporal subscriber information can be defined by incidents and paths. Let a binary tuple (r, t) be an incident where $r \in R$ and $t \in T$. $a = \{a_1, ..., a_T\}$ refers to the actual path of s for the time period t such that $t \in T$. Moreover, all the elements of a belong to the actual incident of s. Assume that M is an integer and $b = \{b_1, ..., b_M\}$ is the set of background data that an attacker possesses. Then a probability distribution function (success probability) of an adversary is as follows:

$$Ad_{\widetilde{b}}(\widetilde{a}) = P(A = \widetilde{a}|B = \widetilde{b}). \tag{3.1}$$

where A and B are random variables that take $\widetilde{a} \in a$ and $\widetilde{b} \in b$.

3.2. Threat Model

There are three attackers with varying amounts of background data. The attacker who has the most information is Big Brother, as in the dystopia of G. Orwell. The second adversary, Little Brother, is equipped with less data, and Step Brother is the final attacker who possesses the least information. Apart from carriers, applications of the subscribers' phones can also be considered possible brothers depending on their background data. The brothers' accuracy, attack techniques, and outcome analysis will be examined (see Chapter 4).

3.2.1. Big Brother

Big Brother is the carrier of the mobile subscriber, which intrinsically possesses two kinds of background data. We can consider the associated cell towers of the subscriber as the first. Thus, it is straightforward to gather the full trace of cell IDs, a. The cell neighborhood information, R, is the second background data. Moreover, the trace deduction process of a mobile subscriber requires location data of road junctions and their connectivity matrix. Therefore, we can easily deduce the followed trace of a subscriber by using HMM (see Section 3.3.1).

3.2.2. Little Brother

Different from Big Brother, he has no access to the full trace of the subscriber, a. He can deduce the hidden knowledge by exploiting two cell IDs and cell adjacency information; nevertheless, the trace is either partially or fully anonymized. Therefore, he can deduce the full path if the attacker possesses other required background data mentioned. Two cell IDs are assumed to be provided and are part of the actual trace, a.

The attackers method of finding these IDs is outside the scope of the study.

3.2.3. Step Brother

The most insignificant adversary, Step Brother, possesses only one incident: the location of the associated Cell ID at a particular instance, a_i, where $i \in T$. However, more precise results can be achieved by exploiting received signal strength indication (RSSI) data in the corresponding cell, as Bshara et al. (2011). However, we will ignore this threat because path inference, the primary aim of the thesis, is impossible through only one incident.

3.3. Path Inference Mechanisms

In this section, the attackers and their prospective threats will be discussed in detail.

3.3.1. Mechanism of Big Brother

This threat can occur through HMM, and its method works by showing a system in terms of a Markov model statistically. It is not wrong to represent the system as a Markov chain with the "hidden" set of states, H. Let V be a set of visible states which is dependent on H. Thus, we can reach the basic goal of the process, inferring H, by observing V, but this goal can only be achieved with state transition and emission matrices.

The locations of base stations (cell towers) and coordinates of road junctions constitute the visible and hidden states, respectively. The HMM process is illustrated in Figure 3.1. Let L_1 be the starting point, origin, of a subscriber's travel, and L_6 be the destination in our grid-like network. The edges represent a segment of the road, and junctions are shown as vertices, as well. Furthermore, each edge has its own probability, P_{i-j}, and it refers to likelihoods of state transitions from i^{th} to j^{th} junction where $1 \leq i, j \leq M$ such that i, j are integers and M refers to the number of states. The summation of the likelihoods equals 1 when the edges are members of the same vertex. Hence, the sum of the elements of any row is 1, as well. For instance, the summation of P_{8-4} and P_{8-10} is equal to 1. For simplicity, all the likelihoods are distributed equally, and reflexive probability, P_{i-i}, is assumed to be 0 for all i. It is worth noting that $P_{i-j} \neq P_{j-i}$, due to the varying number of edges and their likelihoods. For example, P_{4-1} and P_{1-4} equal to 0.25 and 0.33, respectively. HMM is probabilistic; therefore $0 \leq P_{i-j} \leq 1$ for all i and j.

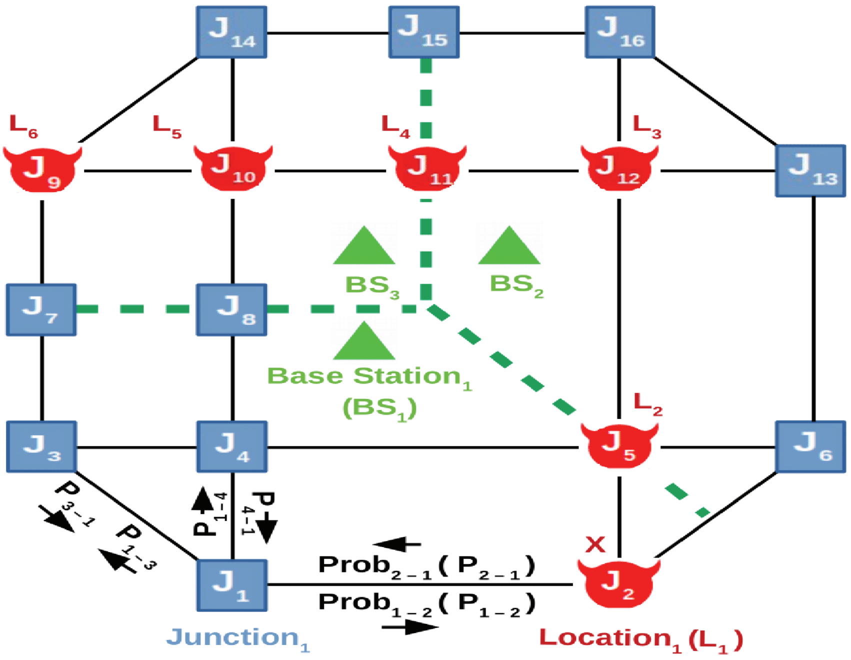


Figure 3.1. An example network and trace for trace deduction by Big Brother.

A value close to 1 should refer to an extremely likely incident, and correspondingly, an infinitesimally small number should be used whenever extremely unlikely.

Figure 3.2 shows the M hidden-stated transition matrix. In Appendix A, the example network's transition matrix can also be seen. There are 16 junctions (states) in our case. Hence, that is a square matrix with 16 rows.

$$\begin{array}{cc} & \begin{array}{cccc} \boldsymbol{S_1} & \boldsymbol{S_2} & \dots & \boldsymbol{S_M} \end{array} \\ \begin{array}{c} \boldsymbol{S_1} \\ \boldsymbol{S_2} \\ \vdots \\ \boldsymbol{S_M} \end{array} & \begin{pmatrix} P_{1-1} & P_{1-2} & \dots & P_{1-M} \\ P_{2-1} & P_{2-2} & \dots & P_{2-M} \\ \vdots & \vdots & \ddots & \vdots \\ P_{M-1} & P_{M-2} & \dots & P_{M-M} \end{pmatrix} \end{array}$$

Figure 3.2. Canonical transition matrix which represents hidden state transition probabilities where S and P refer to states and probabilities, respectively

The green lines represent the coverage zone borders of BS_1, BS_2, and BS_3 in terms of Voronoi cells in Figure 3.1. BS_1 and BS_2 are the associated cell towers when X resides in L_1 and L_3, respectively. Likewise, BS_3 is the associated cell tower while X stays in L_5. Nevertheless, L_2 and L_4 are points where handovers take place. L_2 resides in the border of BS_2 and BS_1. Similarly, BS_2 and BS_3 are the associated cell towers for the case of L_4. These can be defined as gate junctions among cells and can be represented in the emission matrix in Fig. A.2 (see Appendix A) under the columns E_{2-3} and E_{1-2}, respectively. For simplicity, let $E_{3-2} = E_{2-3}$ and $E_{1-2} = E_{2-1}$. Reflexive emission, E_{i-i}, refers to the interior zone of the cell i. Furthermore, handover emissions between cell i and j are $E_{i-j} = E_{j-i}$. Likewise the case of the transition matrix, emission inputs must reside between 0 and 1. The corresponding likelihood while X resides in the interior zones must be a number extremely close to 1, otherwise close to 0. Handovers are assumed to take place with at most two cell towers. Hence, their likelihoods would be equal to 0.5. The canonical emission matrix in Figure 3.3. illustrates M invisible and N visible states (emissions).

$$\begin{array}{c c}
 & \begin{array}{cccc} \boldsymbol{E_1} & \boldsymbol{E_2} & \dots & \boldsymbol{E_N} \end{array} \\
\begin{array}{c} \boldsymbol{S_1} \\ \boldsymbol{S_2} \\ \vdots \\ \boldsymbol{S_M} \end{array} &
\begin{pmatrix} E_{1-1} & E_{1-2} & \dots & E_{1-N} \\ E_{2-1} & E_{2-2} & \dots & E_{2-N} \\ \vdots & \vdots & \ddots & \vdots \\ E_{M-1} & E_{M-2} & \dots & E_{M-N} \end{pmatrix}
\end{array}$$

Figure 3.3. Canonical emission matrix which shows transition probabilities of emissions where S and E refer to states and emissions, respectively

Whenever observing states, it is straightforward to build the emission matrix and infer the trace with the most likelihood trace utilizing the Viterbi Algorithm. Nevertheless, the matrix is not square as the preceding. There exist sixteen invisible and nine visible states (emissions). Therefore, it is a 16 x 9 matrix (see Appendix A).

Let a subscriber's origin and destination be $Cell_1$ and $Cell_2$, respectively. Assume that $Cell_3$ is the second stop. Then the visible states (emission) are nothing but (1, 3, 2). It follows that (E_{1-1}, E_{1-3}, E_{3-3}, E_{3-2}, E_{2-2}) refers to their corresponding emissions. Therefore, we can get the following outcome from the Viterbi Algorithm of Octave Free Software Foundation (2018): [4, 8, 10, 11, 12].

The likelihood of the inferred path and the number of all prospective traces affect the adversary's accuracy. Assume there exist two cases with an inferred trace probability P. The same likelihood needs more precision. Hence, the more accurate one is the case with the greater number of prospective traces and vice versa. When two cases have the same number of prospective traces, M, the more significant accuracy requires a greater number of inferred paths. Hence, the accuracy has a direct correlation with the probability of the inferred path and the number of prospective traces as follows:

$$Acc = log_{10}(Ad_{\widetilde{b}}(\widetilde{a}).M). \tag{3.2}$$

such that M is the number of all prospective traces and $\widetilde{b} = \{b_1, b_2, b_3, b_4\}$. The complete trace of the subscriber, associated cell IDs, is represented by b_1. b_2 refers to the cell neighborhood matrix. The road junction locations in the zone and junction neighborhood matrix are shown as b_3 and b_4, respectively. There can be millions of prospective traces in real networks. Hence, it is better to take a logarithm for simplicity.

3.3.2. Mechanism of Little Brother

Little Brother possesses less background data than Big Brother, as mentioned. The adversary has an incomplete subscriber's trace, at least two associated cells, and the cell neighborhood matrix. Thus, that attack can take place when the stated information is provided.

The number of possible paths (the product of the adjacent cells of inferred cells and the adjacent cells of the first given cell), the likelihood of the deduced path, and the number of inferred cells affect the accuracy of the threat. Let P be the probability of two inferred traces. The more deduced cells lead to more accuracy. Assume two traces with the same number of inferred cells, M. The greater likelihood provides better accuracy than the other trace. Last but not least is the effect of the number of possible paths. Reaching the same probability value is more difficult when the number of inferred cells is kept constant. Therefore, the accuracy has a relation of direct proportion with all the parameters and can be defined as follows

$$Acc = \prod_{i=1}^{M} Acc(IC_i), \tag{3.3}$$

where M and IC_i refer to the number of inferred cells and the i^{th} inferred cell, respectively. It follows that

$$Acc(IC_i) = \#PC_i.Ad_{\widetilde{b}}(\widetilde{a}_i), \tag{3.4}$$

such that $\widetilde{a}_i \in a$ and the number of adjacent cells of i^{th} possible cell is $\#PC_i$. All of the cells possess the same background data. Hence, $\widetilde{b} = \{b_1, b_2, b_3\}$ is the same for each inferred cell. Nevertheless, differing elements of paths $\widetilde{a}_i$ must exist by definition. Instances of destination and origin cells are demonstrated by b_2 and b_1, respectively. b_3 refers to the cell neighborhood matrix. If Equation (3.4) is substituted into Equation (3.3), then:

$$Acc = \prod_{i=1}^{M} \#PC_i . \prod_{i=1}^{M} Ad_{\widetilde{b}}(\widetilde{a}_i)., \tag{3.5}$$

There exist lots of possible cells for increasing the number of inferred cells. Hence, it is required to take the logarithm, and the final form is as follows

$$Acc = log_{10}(\prod_{i=1}^{M} \#PC_i.P(T)). \tag{3.6}$$

such that $P(T)$ is the deduced trace probability.

CHAPTER 4

EVALUATION: AMOUNT OF INFERRED INFORMATION FROM CELL-IDs IN 5G

The defined threats are tested in this section on a real-life dataset that is also used by Li et al. (2021) (Li, Zhou, Ma, and Wang 2021), Guo et al. (2020) (Guo, Wang, Zhou, Xu, Yuan, and Hsu 2020), and Wang et al. (2021) (Wang, Guo, Zhang, Yang, Zhou, and Shen 2021). Shanghai Telecom provides a dataset of monthly records consisting of timestamps with IDs of subscribers and coordinates of base stations in the city of Shanghai, China (see Shanghai Telecom (2014)). Blue Voronoi cells and black dots refer to the cells of the network and base stations of the dataset, respectively (see Figure 4.1). The distance between base stations, especially in the city center, is too small, as shown in Figure 4.1. Thus, we consider all the cells as microcells and 5G NR gNodeB without loss of generalization, and any analysis based on that dataset can be assumed as a 5G simulation.

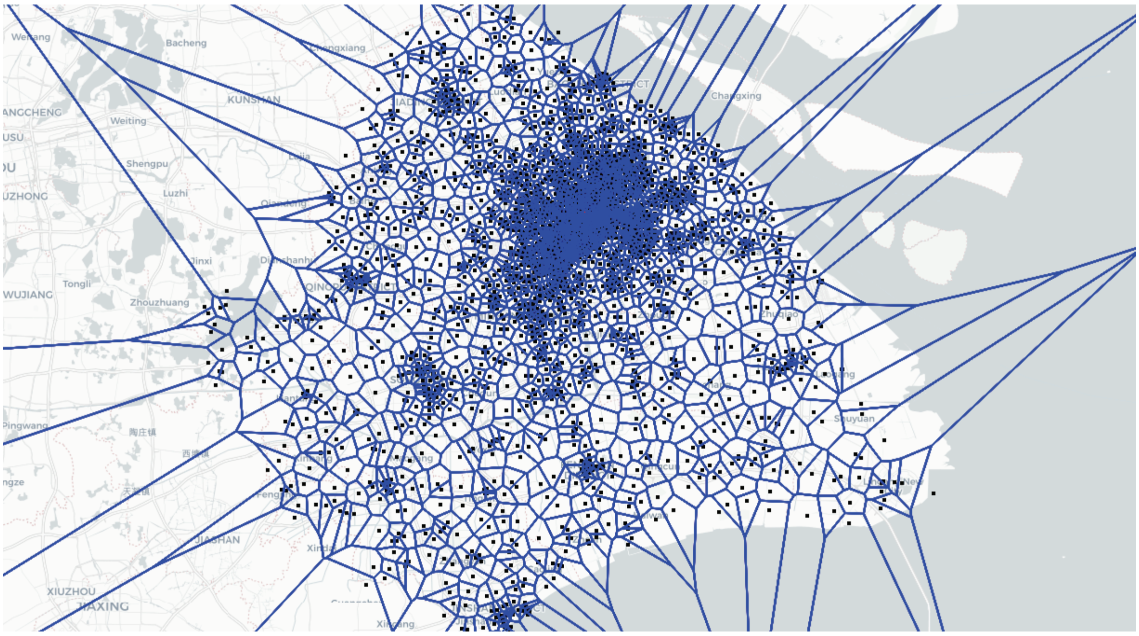


Figure 4.1. Cell network of the dataset.

4.1. Path Inference by Little Brother

The mechanism of path inference utilized by Little Brother is examined in this section through an example trace with five inferred cells and its analysis. We select the cell ID of origin as 711, illustrated by light green with the cell ID of the destination. More inferred cells are gathered and depicted in red with their IDs and orders. The other cells are demonstrated as blue Voronoi cells with black dots inside. Moreover, dark green arrows show the direction of the inferred path. Algorithm 1 in Appendix B, a PYTHON script with geoplotlib library of Cuttone et al. (2016), determines the likelihood of the deduced path $At_{\tilde{d}}(\widetilde{a})$ and the missing (inferred) cells.

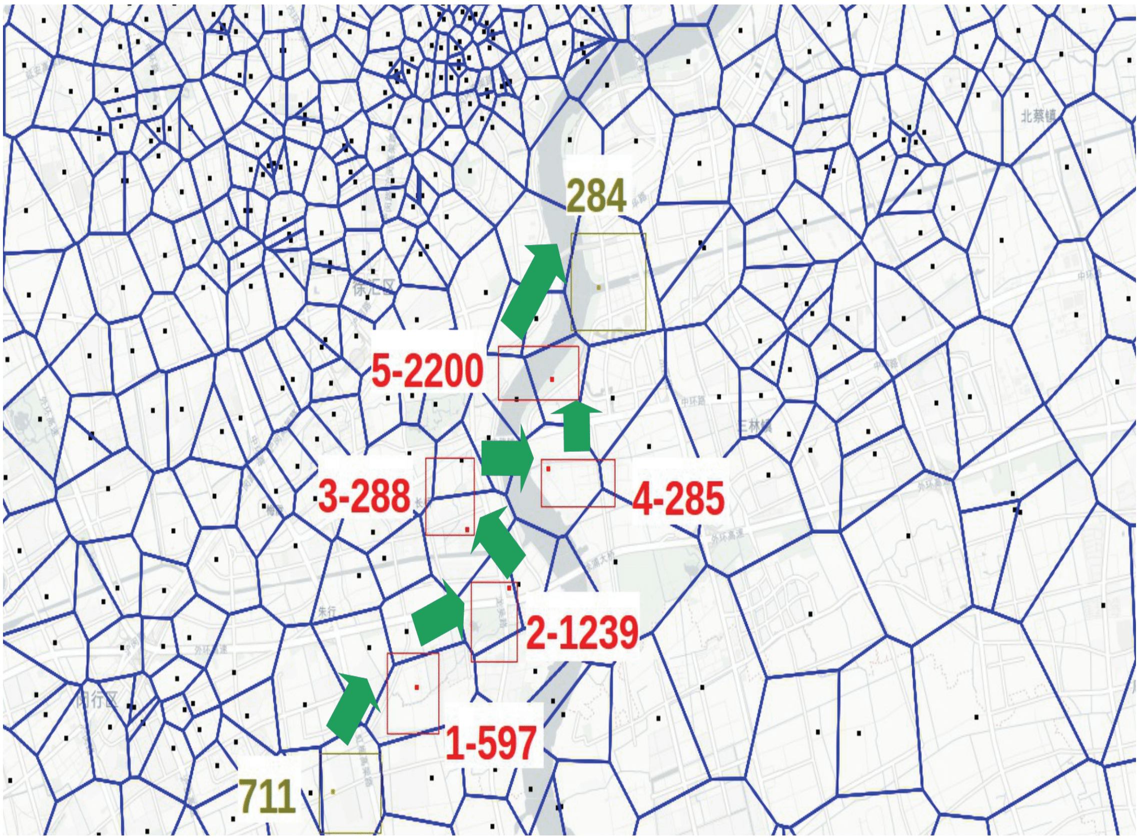


Figure 4.2. A case of 5 inferred cells with their IDs.

4.1.1. Analysis of Little Brother

Cells of the shortest path from the origin and destination cell are inferred by our algorithm (see Fig. 4.2). Four cells are deduced when the destination is 2200. Likewise, one, three, and eight cells are inferred if the destinations are 281, 285, and 2000, respectively (see Appendix C.1).

The accuracy, the likelihood of the inferred trace, and the number of possible paths (the product of the number of adjacent cells) can be considered as required factors for the number of inferred cells. The dashed curve shows the total mean with a confidence interval of 90% for all the graphs from Figure 4.3 to Figure 4.5. The red points in the plots represent the sample inputs.

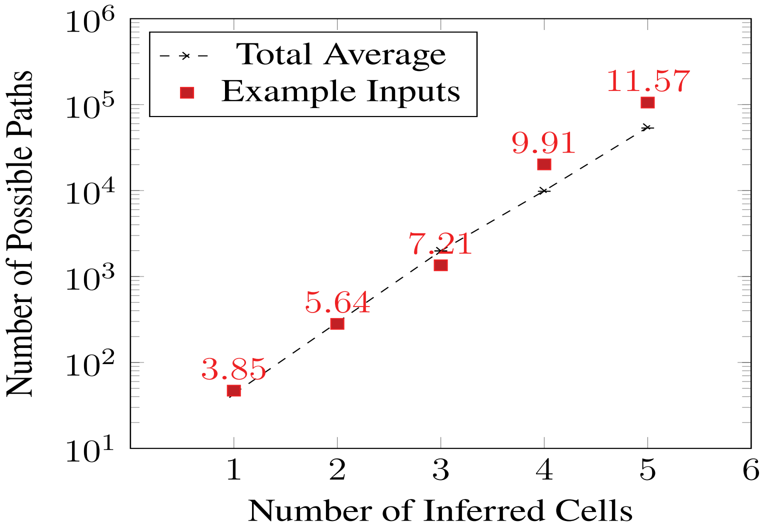


Figure 4.3. The effect of inferred cells on number of possible cells.

All the inferred cells between their adjacent cells have been determined, and a significant rise, nearly from forty to a hundred thousand, is observed in Figure 4.3. Thus, the logarithmic scale has to be utilized to demonstrate the results. More inferred cells lead to more possible paths. Thus, that increase is not a surprise. The likelihood of the deduced trace reduces in similar orders of magnitude for the increasing number of possible paths since inferred cells and the number of prospective traces have direct proportional relation (see Fig. 4.4).

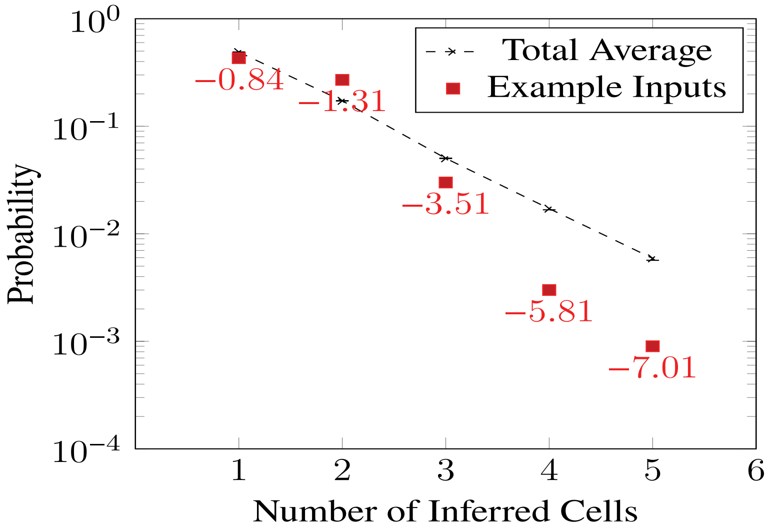


Figure 4.4. The relation of inferred trace likelihood and number of inferred cells.

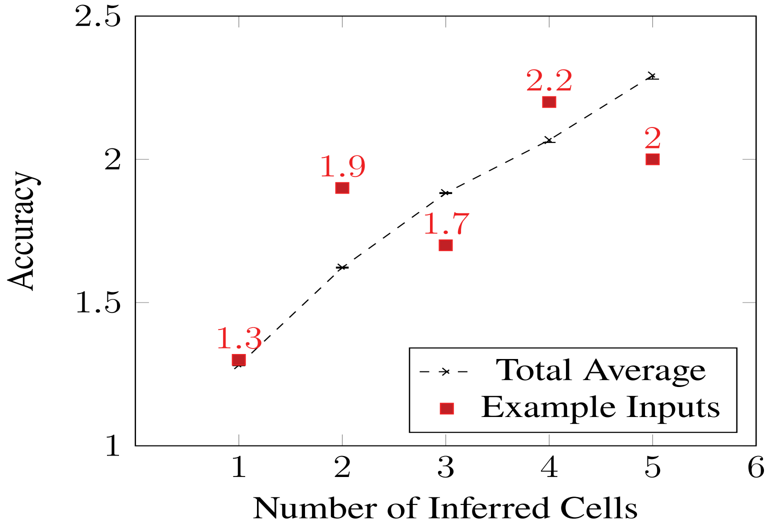


Figure 4.5. The impact of inferred cells on accuracy.

We can not conclude a decrease in accuracy, although a dramatic fall occurs in the probability values. Substituting the inputs of Figure 4.4. into Equation (3.6) leads to the outcome in Figure 4.5. Thus, greater accuracy is gathered for the rising number of inferred cells. Apart from these, an analysis of the hit rate and association rate can be found in Appendix E and F, respectively.

4.2. Path Inference by Big Brother

It is worth noting that the connectivity matrix of road junctions and their locations are required data for Big Brother. We utilized 2640 locations of main street junctions, and hence, it is possible to build a 1-1 correspondence among cells. A script in PYTHON, Algorithm 2 in Appendix B, inferred the most probable trace through the geoplotlib library (Cuttone et al. (2016)).

The dataset has some errors, including missing timestamps and typos. For simplicity, subscribers' IDs were defined by long hash data, all of which were replaced with a unique integer. There are jumps among some cells, timestamps, and subscribers' weird behaviors. Hence, by "best," we mean cases with the closest junctions of the inferred trace, and we will present an example 4-celled trace (see Fig. 4.6).

The example trace illustrates a case of subscriber 1772 from day 3. It is straightforward to observe that the emission states of the case and its corresponding emissions are (1, 2, 3, 4), (1-1, 1-2, 2-2, 2-3, 3-3, 3-4, 4-4), respectively. Base stations are represented in black. Red depicts interior junctions, and blue demonstrates boundary junctions. The green arrows refer to the direction of the trace. The nearest junction to base station 1 is chosen by Algorithm 2 between the junctions in $Cell_1$ represented as 1-1. The selection of the nearest junction to 2-2 demonstrated as 1-2 from the boundary zone among 1 and 2 follows that operation. The remaining trace can be obtained in the same manner.

4.2.1. Analysis of Big Brother

In this section, Big Brother is analyzed in detail. Black curves represent the average of best cases with a confidence interval of 90%, and red points show the results of example best cases. On the day 17, the subscriber 86 infers five cells. The subscriber 361 deduces six cells on the day 23. Seven cells are extracted by subscriber 136 on the day 5. Finally, subscriber 2127 infers eight cells in day 18 (see Appendix D).

The effect of the number of cells on the number of traces can be observed in Figure 4.7. More cells lead to more covered junctions. Hence, a dramatic increase in prospective

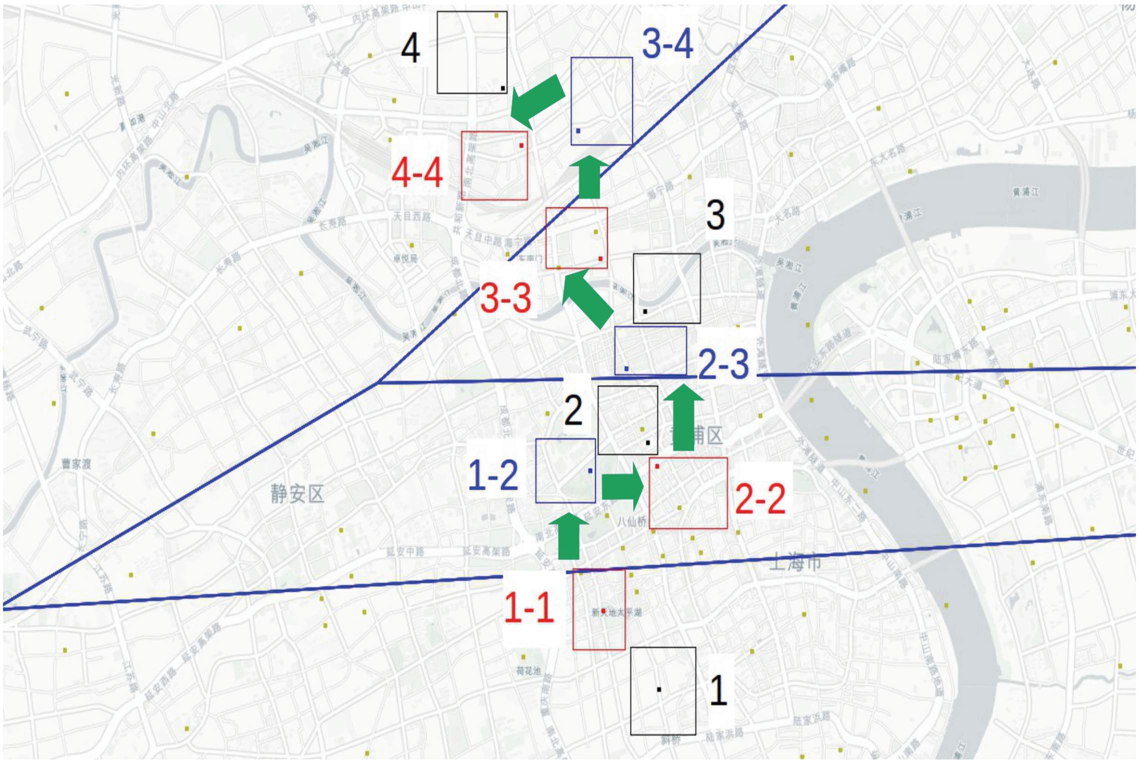


Figure 4.6. A 4-celled case (Day: 3, User: 1772)

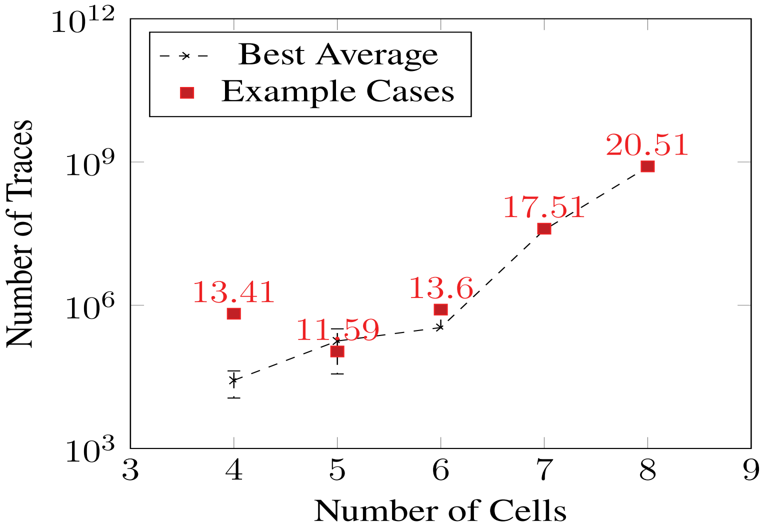


Figure 4.7. The effect of number of cells on all possible paths.

paths occurs from nearly half a million to one billion, and a logarithmic scale is required to illustrate the change.

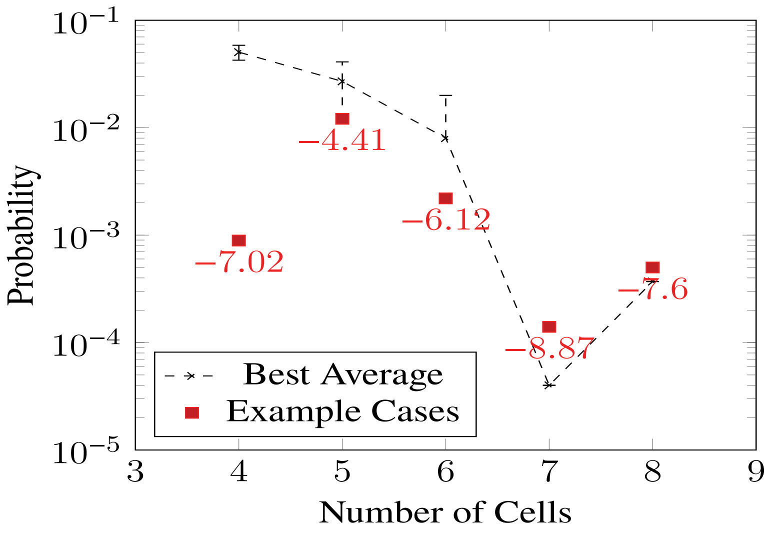


Figure 4.8. The effect of number of cells on inferred trace likelihood.

We again depict the effect of the number of cells on the likelihood of prospective traces through the logarithmic scale in Figure 4.8. A fall is observed after the 5^{th} best case. However, it is impossible to conclude a decrease in accuracy since significant fluctuations of prospective traces lead to that result.

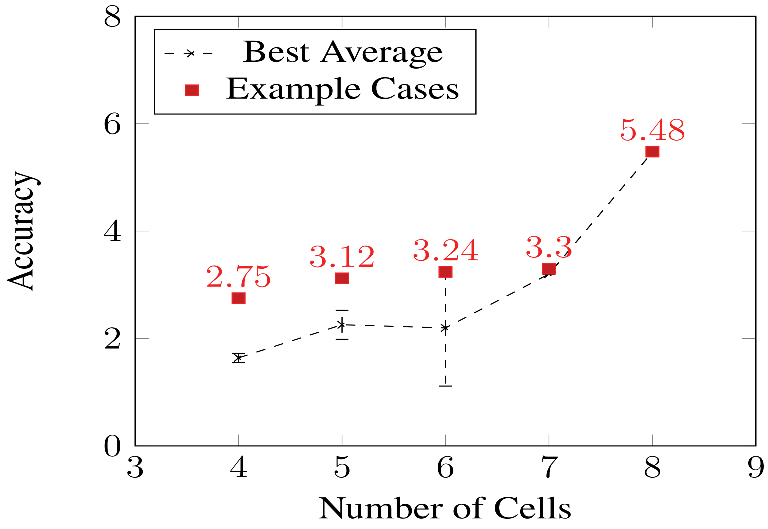


Figure 4.9. The effect of number of cells on accuracy.

The accuracy rises for the increasing number of cells, as shown in Figure 4.9. Thus, it is possible to infer that the greater the number of inferred cells, the more accurate the trace deduction process.

CHAPTER 5

A LIGHTWEIGHT SELF-ORGANIZED FRIENDLY JAMMING AS A COUNTERMEASURE

5.1. Introduction and General Motivation

The easily accessible nature of wireless networks can be considered both an advantage and a disadvantage. Communication technology constitutes a wide-range of backbone infrastructure from contactless payments to satellites which is an advantage. However, this operation of acquiring, processing, and emitting personal private data brings severe security and privacy concerns. Furthermore, the easily accessible nature of wireless networks renders them more vulnerable to threats than their wired counterparts.

Conventionally, the security of wireless networks is based on cryptographic techniques. However, these consume significant computational power and energy. Thus, current resource-constraint technologies require more efficient solutions. In this regard, friendly jamming is considered by researchers to be a promising defense mechanism, although it can be considered as a threat from the attacker's perspective. The fundamental principle of jamming is to block communication by reducing the signal-to-noise ratio (SNR) by introduction external noise. This attack can also be exploited for defensive purposes if it disrupts illegitimate communication, such as eavesdroppers.

Due to its efficiency in terms of computation and energy, various emerging technologies, such as 5G Li et al. (2021) (Li, Dai, Shukla, Li, Xu, and Imran 2021), Shaaban and Faruque (2021), Huo et al. (2019) (Huo, Fan, Ma, Cheng, Tian, and Chen 2019), Li et al. (2019) (Li, Fei, Zhang, and Guizani 2019), Industrial IoT (Internet of Things) Wang et al. (2019) (Wang, Dai, Wang, Xu, and Sangaiah 2019), Industrial Crowdsensing Network Li et al. (2018) (Li, Wang, Dai, and Wang 2018), Internet of Medical Things (IoMT) Li et al. (2020) (Li, Dai, Wang, Imran, Li, and Imran 2020), IoT Dang-Ngoc et al. (2022) (Dang-Ngoc, Nguyen, Ho-Van, Hoang, Dutkiewicz, Pham, and Hwang 2022), Mobile Ad-hoc Networks (MANETs) Kim et al. (2021) (Kim, Biswas, Bohacek, Mackey, Samoohi, and Patel 2021), Visible Light Communication (VLC) Shaaban and Faruque (2021), Pham and Pham (2021), Mostafa and Lampe (2014), and Wireless Sensor Networks (WSNs) Martinovic et al. (2009) (Martinovic, Pichota, and Schmitt 2009) exploit the friendly jamming approach. However, the mentioned models above have to tackle the following challenges

- Compliance with real-world conditions, such as Rayleigh fading and shadowing
- Maximum performance (disrupting illegitimate communication as much as possible)
- Minimum side-effect (disrupting legitimate communication as little as possible)
- Energy efficiency

Although some studies try to meet real-world requirements Berger et al. (2016) (Berger, Gringoli, Facchi, Martinovic, and Schmitt 2016), Berger et al. (2014) (Berger, Gringoli, Fachi, Martinovic, and Schmitt 2014), they are complicated models and need to be updated for new technologies. Therefore, our primary motivation and the contribution in this study is to propose a mechanism that is well-posed to meet real-world needs with the following features

- simplicity
- flexibility

In this thesis, we are dealing with generating jamming signals based on the received signal power. In our study, the asserted approach, jamming power optimization, provides both efficient energy utilization and viability as covered in Section 3 in detail. In this approach, radio emissions diminish proportional to the path loss exponent of the corresponding medium. Although it is straightforward to determine the free space loss, implementing a more viable approach requires thorough work, as illustrated in Kyösti et al. (2008).

We utilized a mobile network scenario with the same transmit power for each node. Generating a signal whose power matches the signal received from the furthest node in the region is required to disrupt the communication inside the target range.

According to the lost-power-based models, blocking all communication can be performed by adding transmit power to the power lost due to the distance between them. Nevertheless, those models have two drawbacks: (i) calculating the precise loss is impossible due to the uncertainty of real-life effects; (ii) the calculation process is complicated (see Madara et al. (2016) and the following sections). Nevertheless, they can be observed precisely, which is also the center of our approach. We substituted the lost power with the difference between the received and transmitted power, leading to identical results. Observing the precise real-world information, the received signal, solve the first drawback. Moreover, no calculation is required anymore since we can gather empirical observations. Thus, our approach addresses those challenges thoroughly.

The remainder of this chapter is as follows: we stated the proposed model and its proof in Section 5.2, and in Section 5.3, the evaluation was provided, which constitutes model validation through simulations.

5.2. System Model

The first step in addressing the issue is optimizing the jamming power. A function of distance, the sum of the path loss and the transmit power, is exploited to state the problem mathematically. Nevertheless, the path loss is substituted by the difference between the received and transmission power. Hence, two gains are achieved. First is the perspective of receiving power which is also the contribution. Second is ensuring the equality of received power and the adequate transmit signal for jamming the nodes at the desired range.

Theorem 5.2..1 (Optimized Jamming Power) *Consider a mobile network with m user equipment (UE) all of which has the same transmit power T. Let* $J(d)$ *be the optimum power to jam the distance d. Assume that* $C = (\frac{v}{4.\pi.f})^2$ *such that f is the carrier frequency and v is the speed of light. Let* γ *be the path loss constant where* $2 \leq \gamma \leq 6$. *The optimized jamming power for the distance d is*

$$J(d) = T - 10.log_{10}C + 10.\gamma.log_{10}d \tag{5.1}$$

Proof: Assume that R is the receiving power. According to the simple path loss model, the received power from the k^{th} nearest node is

$$R(k) = 10.log_{10}C - 10.\gamma.log_{10}d + T \tag{5.2}$$

Assume that L(k) is the lost power of the k^{th} nearest UE. Since the largest power is adequate to jam the network, the optimized jamming power is

$$J(Network) = max(J(d_1), J(d_2), ..., J(d_m)) \tag{5.3}$$

The receiving signal from the jammer must be at least T and we must add the path loss. Hence,

$$J(Network) = max(L(1) + T, L(2) + T, ..., L(m) + T) \tag{5.4}$$

Since $L(m)$ is larger than the others, it follows that

$$J(d_m) = L(m) + T \tag{5.5}$$

Since $L(m) = T - R(m)$, then

$$J(d_m) = (T - R(m)) + T \tag{5.6}$$

If we substitute into Equation 5.2, then

$$J(d_m) = 10.\gamma.log_{10}d_m - 10.log_{10}C + T \tag{5.7}$$

$$J(d) = 10.\gamma.log_{10}d - 10.log_{10}C + T \tag{5.8}$$

Corollary 5.2..1.1 (Finding Path Loss Exponent) *Let d be the present distance to jam and γ be the regarding path loss exponent. Let d' be the desired distance to jam. Then the regarding path loss exponent is*

$$\gamma' = \gamma.\frac{log_{10}d}{log_{10}d'} \tag{5.9}$$

provided that

$$J(d) = J(d') \tag{5.10}$$

Proof: Let J be the optimum jamming power and J(d) be the optimum power to jam the distance d. According to Theorem 1, we can find the following equation

$$J(d) = T - 10.log_{10}C + 10.\gamma.log_{10}d \tag{5.11}$$

In the same manner,

$$J(d') = T - 10.log_{10}C + 10.\gamma'.log_{10}d \tag{5.12}$$

Since

$$J(d) = J(d') \tag{5.13}$$

It follows that

$$\gamma' = \gamma.\frac{log_{10}d}{log_{10}d'} \tag{5.14}$$

Corollary 5.2..1.2 (Center of d and γ) *Consider a mobile network with m user equipment. Let d_i be the distance to the i^{th} node and γ_i be the path loss exponent of the i^{th} node where $1 \leq i \leq n$. Let d_c be the center of distance to jam and γ_c be the center of path loss* *exponent to jam. Then,*

$$d_1{}^{\gamma_1}.d_2{}^{\gamma_2}...d_n{}^{\gamma_m} = d_c{}^{m.\gamma_c} \tag{5.15}$$

Proof: Let J be the optimum jamming power, $J(d_i)$ be the optimum power to jam the distance d_i such that $1 \leq i \leq m$ and $J(d_c)$ be the optimum power to jam the center of distances. It follows that

$$J(d_1) + ...J(d_m) = m.J(d_c) \tag{5.16}$$

According to Theorem 1

$$J(d_i) = T - 10.log_{10}C + 10.\gamma_i.log_{10}d_i \tag{5.17}$$

$$log_{10}(d_1{}^{\gamma_1}.d_2{}^{\gamma_2}...d_n{}^{\gamma_m}) = log_{10}d_c{}^{\gamma_c.m} \tag{5.18}$$

Therefore,

$$d_1{}^{\gamma_1}.d_2{}^{\gamma_2}...d_m{}^{\gamma_m} = d_c{}^{m.\gamma_c} \tag{5.19}$$

5.3. Evaluation

In this section, the proposed model is validated using Monte Carlo simulations in MATLAB, and simulations were run 1000 times (see Algorithm 3 in Appendix B). Moreover, the results of our approach and the proposed model in Madara et al. (2016) were compared and discussed using the same parameters shown in Table 5.1.

Table 5.1. Parameters in the Madara et al. (2016)

PARAMETER	QUANTITY
MIN_{SNR}	9 dB
MAX_{Power}	-15 dBm
Carrier frequency	1880 MHZ
Jamming distance	10 m
Free Space Loss	58 dB

By its definition, SNR is as follows

$$SNR(dB) = Signal(dB) - Noise(dB) \tag{5.20}$$

Here, Noise is the jamming power at the receiver, input power.

$$MIN_{SNR} = MAX_{Power} - Noise(dB) \tag{5.21}$$

$$Noise(dB) = -24dBm \tag{5.22}$$

The path loss has to be added to calculate jamming power,

$$Power_{Jamming} = FreeSpaceLoss + Noise \tag{5.23}$$

$$Power_{Jamming} = 58 + (-24) \tag{5.24}$$

$$Power_{Jamming} = 34dBm \tag{5.25}$$

In Figure 5.1, there is a comparison of two jamming power models, which is directly proportional to distance. Thus, it is natural to observe a rising curve. Moreover, the two

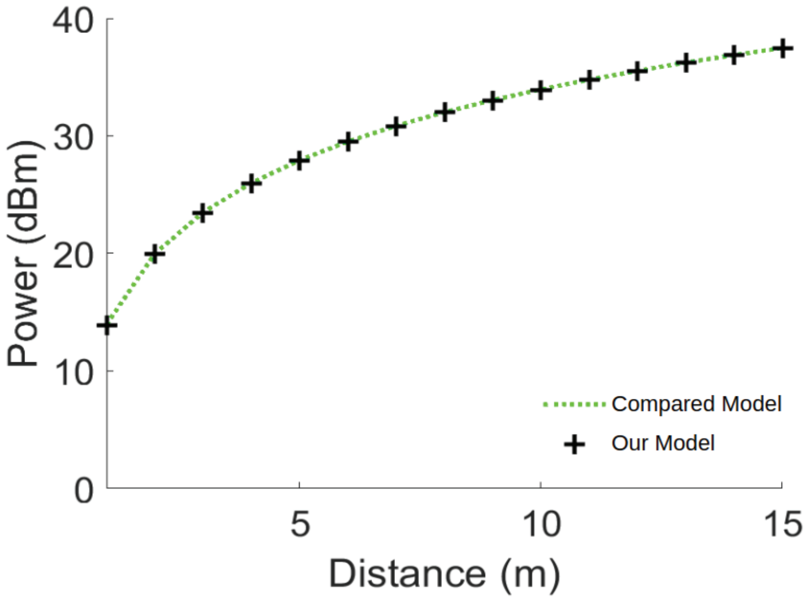


Figure 5.1. Jamming power comparison for varying distances

models overlap entirely and can be considered as the most critical inference, which shows that our proposed model achieves the same performance as the model of Madara et al. (2016) in free space.

The receiving jamming powers of the models are illustrated in Figure 5.2. Our model assumes that each UE in the network has the same transmission power. Receiving powers must be equal to the transmission power of target UEs preventing them from hearing each other.

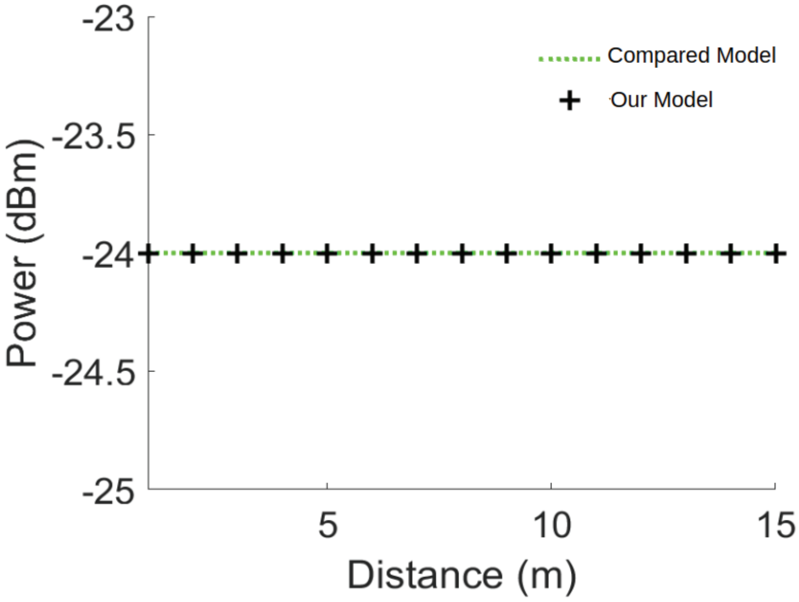


Figure 5.2. Received jamming power comparison for varying distances

The coverage of the models is illustrated in Figure 5.3. Figure 5.1 demonstrates the optimized jamming signal. The receiving signal in our model is equal to the noise in the compared model (see Figure 5.2). Hence, no UE can hear anything due to noise with the same level of their transmission. Thus, $\%100$ coverage of jamming can be achieved for the desired range on top of the first two simulations. After finding the exponents of path loss, it is straightforward to calculate the optimized power of jamming. Unsurprisingly, the power level received from 100 m is lower than that from 10 m. Similarly, the 10-metered power of jamming is less than the 100-metered case (see Figure 5.4).

Last but not least is the side effects of our model, basically disrupting legitimate communication. To minimize that effect, we have to choose the desired range to jam as the diameter of the corresponding cell in which the attacker resides. Thus, only the transmission inside that cell will be affected. Moreover, the network's density should be considered for improving the effectiveness by exploiting some models, such as Yaman et al. (2018), Eroğlu et al. (2019).

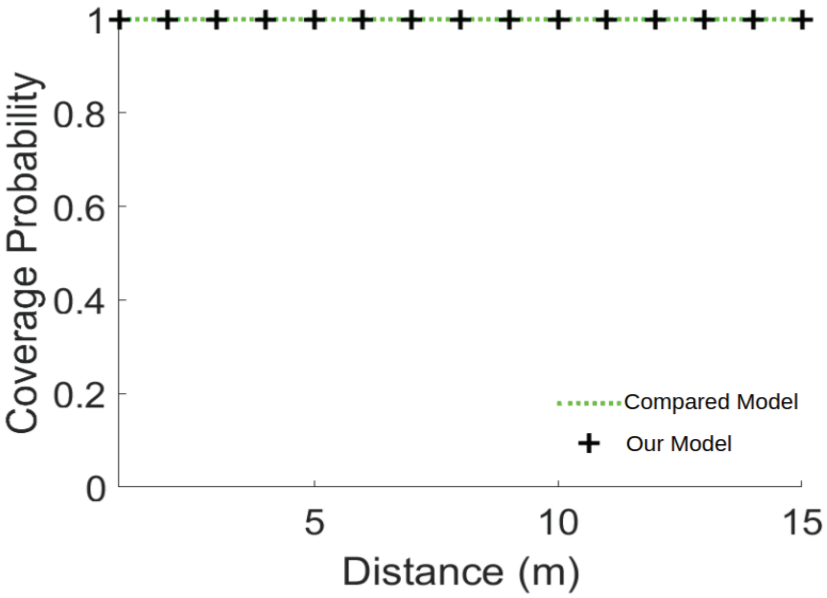


Figure 5.3. Coverage probability comparison for varying distances

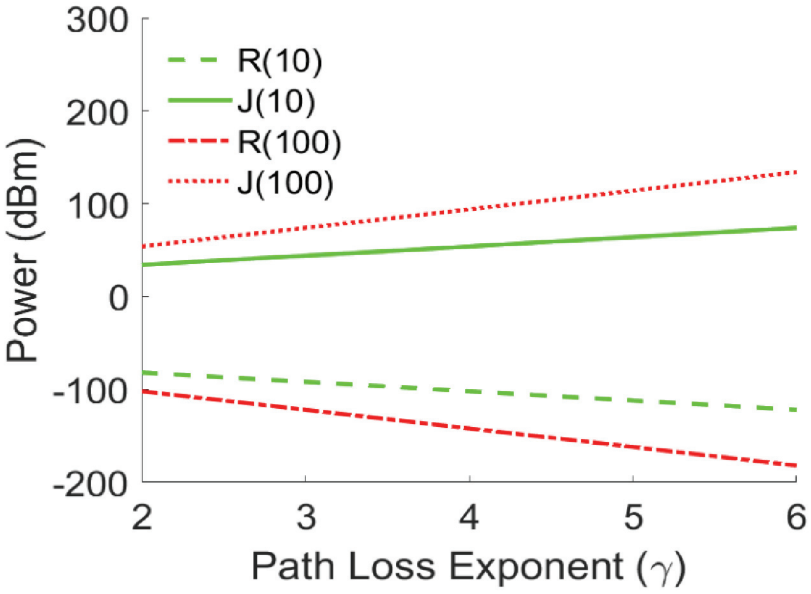


Figure 5.4. Jamming and received power comparison with respect to path loss exponent

CHAPTER 6

DISCUSSION

In this chapter, there is a brief discussion on risks and limitations of our research. Then we mention some possible counter attacks against our FJ model.

6.1. Risks and Limitations

6.1.1. Location Privacy

- The substantial source of location privacy problem is the centralized architecture of mobile networks, nonetheless many LPPMs have been proposed all of which can be breached
- Big Brothers, carriers, were reluctant to share real data with us and hence cooperate to detect privacy gaps in the system. The more data and studies will unfold more flaws
- Non-governmental organizations (NGOs) and in general society have to force governments to enact necessary legal restrictions providing privacy of mobile subscribers.

6.1.2. Friendly Jamming

- Although we have validated our proposed model through Monte Carlo simulations, it is still in need to be checked on real world conditions with different kinds and sizes of networks, such as IoT networks for varying densities
- There is still risk of disrupting legitimate transmission, nevertheless the proposed model employ optimum jamming power. We can observe this effect as well while performing physically as mentioned
- We need to examine the FJ model for various counter attacks (see section 6.2)

6.2. Possible Counter Attacks Against FJ Model

We assume that the proposed FJ model can be a countermeasure for Little Brother which can be considered as an eavesdropper. If the Little Brother is able to realize while performing FJ, he can implement a counter attack. Hence, more sophisticated FJ mechanisms are needed to be employed for various types attackers (see Section 6.3.2).

6.3. Future Directions

6.3.1. Location Privacy

- We are planning to extend our research by considering association rates of Base Stations (see Appendix F). Moreover, some density estimators, such as Eroğlu et al. (2019) and Yaman et al. (2018) will definitely improve robustness.

6.3.2. Friendly Jamming

- One of the more sophisticated FJ mechanism is intermittent jamming instead of continuous jamming. Hence, the attacker might think that nothing has happened, since he can still listen to the channel and get some data
- The LPPMs mentioned in Chapter 2 can be adopted to develop more robust solutions to block counter attacks
- We are planning to extend this study by considering the above mentioned issues

CHAPTER 7

CONCLUSION

The nature of wireless networks is a double-edged sword. On the one hand, it is possible to easily share and reach information, including our private data, anywhere and anytime, provided that we are in the coverage area. On the other hand, attackers can also exploit the convenience of this prevailing world. They inherently devise unprecedented attacks with new toolsets for each novel technology.

In this study, the attackers were classified based on their authority to access to the background data. We exploited a fine-grained HMM to develop the precision of the trace inference process of adversaries. Moreover, metrics of accuracy are introduced for each attack. The proposed attacks and their mechanisms were compared with the most relevant ones in the literature, allowing us to demonstrate the studys novel aspects and contributions. A real-life data enabled simulation of the threats, and the outputs of the rigorous analysis revealed that the greater the quantity of background data, the more accurate the trace and the greater the precision. The utilized dataset is extremely close to a 5G network. Hence, present LPPMs can be improved through our results.

Most conventional LPPMs are based on cryptography, which consumes significant energy and computing power. However, these techniques fail to meet the requirements of some current technologies, such as 5G and IoT, since eligible devices for them have energy and computing power constraints. Moreover, any attacker with significant resources can make these methods ineffective. Therefore, friendly jamming (FJ) is a promising solution to these challenges due to its operability with considerably low energy and computation sources. Besides the advantages, there are also disadvantages of FJ, such as the applicability. Although some models are proposed to tackle that issue, they are not straightforward and must be updated for new technologies. In this dissertation, we propose a lightweight and flexible FJ model that is well-posed for the mentioned drawbacks of the studies. It is also clearly illustrated that our model has the same performance as one of the mentioned studies above in a more straightforward way. Therefore, the proposed model in this study is energy-efficient and computationally cheap, which is also viable for new technologies. As future research, we aim to improve the proposed attacks and evaluate our model for different environments, such as IoT.

REFERENCES

Andrés, M. E., N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi (2013). Geo-indistinguishability: Differential privacy for location-based systems. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 901–914.

Ardagna, C. A., M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati (2007). Location privacy protection through obfuscation-based techniques. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 47–60. Springer.

Ardagna, C. A., M. Cremonini, S. D. C. di Vimercati, and P. Samarati (2009). An obfuscation-based approach for protecting location privacy. *IEEE Transactions on Dependable and Secure Computing 8*(1), 13–27.

Bamba, B., L. Liu, P. Pesti, and T. Wang (2008). Supporting anonymous location queries in mobile environments with privacygrid. In *Proceedings of the 17th international conference on World Wide Web*, pp. 237–246.

Beresford, A. R. and F. Stajano (2003). Location privacy in pervasive computing. *IEEE Pervasive computing 2*(1), 46–55.

Berger, D. S., F. Gringoli, N. Facchi, I. Martinovic, and J. Schmitt (2014). Gaining insight on friendly jamming in a real-world ieee 802.11 network. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, pp. 105–116.

Berger, D. S., F. Gringoli, N. Facchi, I. Martinovic, and J. B. Schmitt (2016). Friendly jamming on access points: Analysis and real-world measurements. *IEEE Transactions on Wireless Communications 15*(9), 6189–6202.

Bettini, C., S. Mascetti, X. S. Wang, D. Freni, and S. Jajodia (2009). Anonymity and historical-anonymity in location-based services. In *Privacy in location-based applications*, pp. 1–30. Springer.

Bordenabe, N. E., K. Chatzikokolakis, and C. Palamidessi (2014). Optimal geo-indistinguishable mechanisms for location privacy. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pp. 251–262.

Boualouache, A., H. Sedjelmaci, and T. Engel (2021). Consortium blockchain for cooperative location privacy preservation in 5g-enabled vehicular fog computing. *IEEE Transactions on Vehicular Technology 70*(7), 7087–7102.

Bshara, M., U. Orguner, F. Gustafsson, and L. Van Biesen (2011). Robust tracking in cellular networks using hmm filters and cell-id measurements. *IEEE Transactions on Vehicular Technology 60*(3), 1016–1024.

Buttyán, L., T. Holczer, and I. Vajda (2007). On the effectiveness of changing pseudonyms to provide location privacy in vanets. In *European Workshop on Security in Ad-hoc and Sensor Networks*, pp. 129–141. Springer.

Carianha, A. M., L. P. Barreto, and G. Lima (2011). Improving location privacy in mix-zones for vanets. In *30th IEEE International Performance Computing and Communications Conference*, pp. 1–6. IEEE.

Chatzikokolakis, K., E. ElSalamouny, C. Palamidessi, P. Anna, et al. (2017). Methods for location privacy: A comparative overview. *Foundations and Trends® in Privacy and Security 1*(4), 199–257.

Chatzikokolakis, K., C. Palamidessi, and M. Stronati (2014). A predictive differentially-private mechanism for mobility traces. In *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 21–41. Springer.

Chatzikokolakis, K., C. Palamidessi, and M. Stronati (2015). Constructing elastic distinguishability metrics for location privacy. *Proc. Priv. Enhancing Technol. 2015*(2), 156–170.

Checa, J. J. and S. Tomasin (2020). Location-privacy-preserving technique for 5g mmwave devices. *IEEE Communications Letters 24*(12), 2692–2695.

Chen, J., K. He, Q. Yuan, M. Chen, R. Du, and Y. Xiang (2018). Blind filtering at third parties: An efficient privacy-preserving framework for location-based services. *IEEE Transactions on Mobile Computing 17*(11), 2524–2535.

Chen, S. and H. Shen (2016). Semantic-aware dummy selection for location privacy preservation. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 752–759. IEEE.

Cheng, R., Y. Zhang, E. Bertino, and S. Prabhakar (2006). Preserving user location privacy in mobile data management infrastructures. In *International Workshop on Privacy Enhancing Technologies*, pp. 393–412. Springer.

Chow, C.-Y., M. F. Mokbel, and X. Liu (2011). Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *GeoInformatica 15*(2), 351–380.

Chow, R. and P. Golle (2009). Faking contextual data for fun, profit, and privacy. In *Proceedings of the 8th ACM workshop on Privacy in the electronic society*, pp. 105–108.

Conti, M., J. Willemsen, and B. Crispo (2013). Providing source location privacy in wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials 15*(3), 1238–1280.

Cui, G., Q. He, F. Chen, H. Jin, Y. Xiang, and Y. Yang (2021). Location privacy protection via delocalization in 5g mobile edge computing environment. *IEEE Transactions on Services Computing*.

Cuttone, A., S. Lehmann, and J. E. Larsen (2016). Geoplotlib: a python toolbox for visualizing geographical data.

Dang-Ngoc, H., D. N. Nguyen, K. Ho-Van, D. T. Hoang, E. Dutkiewicz, Q.-V. Pham, and W.-J. Hwang (2022). Secure swarm uav-assisted communications with cooperative friendly jamming. *IEEE Internet of Things Journal*.

De Mulder, Y., G. Danezis, L. Batina, and B. Preneel (2008). Identification via location-profiling in gsm networks. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, pp. 23–32.

Dewri, R. (2012). Local differential perturbations: Location privacy under approximate knowledge attackers. *IEEE Transactions on Mobile Computing 12*(12), 2360–2372.

Do, H. J., Y.-S. Jeong, H.-J. Choi, and K. Kim (2016). Another dummy generation technique in location-based services. In *2016 International Conference on Big Data and Smart Computing (BigComp)*, pp. 532–538. IEEE.

Duckham, M. and L. Kulik (2005). A formal model of obfuscation and negotiation for location privacy. In *International conference on pervasive computing*, pp. 152–170. Springer.

Dwork, C. (2006). Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener (Eds.), *Automata, Languages and Programming*, Berlin, Heidelberg, pp. 1–12. Springer Berlin Heidelberg.

Eckhoff, D., R. German, C. Sommer, F. Dressler, and T. Gansen (2011). Slotswap: Strong and affordable location privacy in intelligent transportation systems. *IEEE Communications Magazine 49*(11), 126–133.

Eroğlu, A., O. Yaman, and E. Onur (2019). Density-aware cellular coverage control: Interference-based density estimation. *Computer Networks 165*, 106922.

Fawaz, K. and K. G. Shin (2014). Location privacy protection for smartphone users. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 239–250.

Free Software Foundation (2018). Gnu octave. Accessed: 2018-03-13, Version: 4.2.2, https://www.gnu.org/software/octave.

Freudiger, J., M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes (2012). Non-cooperative location privacy. *IEEE Transactions on Dependable and Secure Computing 10*(2), 84–98.

Freudiger, J., M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux (2007). Mix-zones for location privacy in vehicular networks. In *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, Number CONF.

Freudiger, J., R. Shokri, and J.-P. Hubaux (2009). On the optimal placement of mix zones. In *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 216–234. Springer.

Gao, S., J. Ma, W. Shi, G. Zhan, and C. Sun (2013). Trpf: A trajectory privacy-preserving framework for participatory sensing. *IEEE Transactions on Information Forensics and Security 8*(6), 874–887.

Gedik, B. and L. Liu (2005). Location privacy in mobile systems: A personalized anonymization model. In *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, pp. 620–629. IEEE.

Gerlach, M. (2006). Assessing and improving privacy in vanets. *ESCAR, Embedded Security in Cars*.

Ghinita, G., M. L. Damiani, C. Silvestri, and E. Bertino (2009). Preventing velocity-based linkage attacks in location-aware applications. In *Proceedings of the 17th ACM SIGSPATIAL international conference on advances in geographic information systems*, pp. 246–255.

Ghinita, G., P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan (2008). Private queries in location based services: anonymizers are not necessary. In *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, pp. 121–132.

Gong, X., X. Chen, K. Xing, D.-H. Shin, M. Zhang, and J. Zhang (2015). Personalized location privacy in mobile networks: A social group utility approach. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 1008–1016. IEEE.

Grissa, M., B. Hamdaoui, and A. A. Yavuz (2017). Location privacy in cognitive radio networks: A survey. *IEEE Communications Surveys & Tutorials 19*(3), 1726–1760.

Gruteser, M. and D. Grunwald (2003). Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services*, pp. 31–42.

Gruteser, M. and B. Hoh (2005). On the anonymity of periodic location samples. In *International Conference on Security in Pervasive Computing*, pp. 179–192. Springer.

Guo, Y., S. Wang, A. Zhou, J. Xu, J. Yuan, and C.-H. Hsu (2020). User allocation-aware edge cloud placement in mobile edge computing. *Software: Practice and Experience 50*(5), 489–502.

Gursoy, M. E., L. Liu, S. Truex, L. Yu, and W. Wei (2018). Utility-aware synthesis of differentially private and attack-resilient location traces. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 196–211.

Gutscher, A. (2006). Coordinate transformation-a solution for the privacy problem of location based services? In *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*, pp. 7–pp. IEEE.

Hara, T., A. Suzuki, M. Iwata, Y. Arase, and X. Xie (2016). Dummy-based user location anonymization under real-world constraints. *IEEE Access 4*, 673–687.

Hoh, B. and M. Gruteser (2005). Protecting location privacy through path confusion. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pp. 194–205. IEEE.

Hoh, B., M. Gruteser, H. Xiong, and A. Alrabady (2010). Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking. *IEEE Transactions on Mobile Computing 9*(8), 1089–1107.

Huo, Y., X. Fan, L. Ma, X. Cheng, Z. Tian, and D. Chen (2019). Secure communications in tiered 5g wireless networks with cooperative jamming. *IEEE Transactions on Wireless Communications 18*(6), 3265–3280.

Huo, Z., Y. Huang, and X. Meng (2011). History trajectory privacy-preserving through graph partition. In *Proceedings of the 1st international workshop on Mobile location-based service*, pp. 71–78.

Hwang, R.-H., Y.-L. Hsueh, and H.-W. Chung (2013). A novel time-obfuscated algorithm for trajectory privacy protection. *IEEE Transactions on Services Computing 7*(2), 126–139.

Jiang, H., J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar (2021). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys (CSUR) 54*(1), 1–36.

Jiang, J., G. Han, H. Wang, and M. Guizani (2019). A survey on location privacy protection in wireless sensor networks. *Journal of Network and Computer Applications 125*, 93–114.

Jin, R., K. Zeng, and K. Zhang (2019). A reassessment on friendly jamming efficiency. *IEEE Transactions on Mobile Computing 20*(1), 32–47.

Khoshgozaran, A. and C. Shahabi (2007). Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In *International symposium on spatial and temporal databases*, pp. 239–257. Springer.

Khoshgozaran, A., C. Shahabi, and H. Shirani-Mehr (2011). Location privacy: going beyond k-anonymity, cloaking and anonymizers. *Knowledge and Information Systems 26*(3), 435–465.

Khoshgozaran, A., H. Shirani-Mehr, and C. Shahabi (2013). Blind evaluation of location based queries using space transformation to preserve location privacy. *GeoInformatica 17*(4), 599–634.

Kido, H., Y. Yanagisawa, and T. Satoh (2005a). An anonymous communication technique using dummies for location-based services. In *ICPS'05. Proceedings. International Conference on Pervasive Services, 2005.*, pp. 88–97. IEEE.

Kido, H., Y. Yanagisawa, and T. Satoh (2005b). Protection of location privacy using dummies for location-based services. In *21st International conference on data engineering workshops (ICDEW'05)*, pp. 1248–1248. IEEE.

Kifer, D. and A. Machanavajjhala (2011). No free lunch in data privacy. In *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data*, pp. 193–204.

Kim, J., P. K. Biswas, S. Bohacek, S. J. Mackey, S. Samoohi, and M. P. Patel (2021). Advanced protocols for the mitigation of friendly jamming in mobile ad-hoc networks. *Journal of Network and Computer Applications 181*, 103037.

Kim, J. and J. P. Choi (2016). Cancellation-based friendly jamming for physical layer security. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6. IEEE.

Krumm, J. (2007). Inference attacks on location tracks. In *International Conference on Pervasive Computing*, pp. 127–143. Springer.

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

Kyösti, P., J. Meinilä, L. Hentila, X. Zhao, T. Jämsä, C. Schneider, M. Narandzic, M. Milojevi, A. Hong, J. Ylitalo, V.-M. Holappa, M. Alatossava, R. Bultitude, Y. Jong, and T. Rautiainen (2008, 02). Winner ii channel models. *IST-4-027756 WINNER II D1.1.2 V1.2*.

Lei, P.-R., W.-C. Peng, I.-J. Su, C.-P. Chang, et al. (2012). Dummy-based schemes for protecting movement trajectories. *Journal of Information Science and Engineering 28*(2), 335–350.

Li, B., Z. Fei, Y. Zhang, and M. Guizani (2019). Secure uav communication networks over 5g. *IEEE Wireless Communications 26*(5), 114–120.

Li, J., X. Lei, P. D. Diamantoulakis, L. Fan, and G. K. Karagiannidis (2022). Security optimization of cooperative noma networks with friendly jamming. *IEEE Transactions on Vehicular Technology*.

Li, J., H. Yan, Z. Liu, X. Chen, X. Huang, and D. S. Wong (2015). Location-sharing systems with enhanced privacy in mobile online social networks. *IEEE Systems Journal 11*(2), 439–448.

Li, M., K. Sampigethaya, L. Huang, and R. Poovendran (2006). Swing & swap: user-centric approaches towards maximizing location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pp. 19–28.

Li, N., T. Li, and S. Venkatasubramanian (2007). t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering*, pp. 106–115. IEEE.

Li, X., H.-N. Dai, M. K. Shukla, D. Li, H. Xu, and M. Imran (2021). Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5g and beyond communications. *Computer Standards & Interfaces 78*, 103540.

Li, X., H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran (2020). Securing internet of medical things with friendly-jamming schemes. *Computer Communications 160*, 431–442.

Li, X., Q. Wang, H.-N. Dai, and H. Wang (2018). A novel friendly jamming scheme in industrial crowdsensing networks against eavesdropping attack. *Sensors 18*(6), 1938.

Li, Y., A. Zhou, X. Ma, and S. Wang (2021). Profit-aware edge server placement. *IEEE Internet of Things Journal*.

Liao, D., H. Li, G. Sun, M. Zhang, and V. Chang (2018). Location and trajectory privacy preservation in 5g-enabled vehicle social network services. *Journal of Network and Computer Applications 110*, 108–118.

Lin, D., E. Bertino, R. Cheng, and S. Prabhakar (2008). Position transformation: a location privacy protection method for moving objects. In *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, pp. 62–71.

Liu, B., W. Zhou, T. Zhu, L. Gao, and Y. Xiang (2018). Location privacy and its applications: A systematic study. *IEEE access 6*, 17606–17624.

Lu, R., X. Lin, T. H. Luan, X. Liang, and X. Shen (2011). Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE transactions on vehicular technology 61*(1), 86–96.

Machanavajjhala, A., D. Kifer, J. Gehrke, and M. Venkitasubramaniam (2007). l-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD) 1*(1), 3–es.

Madara, D. S., E. Ataro, and S. Sitati (2016). Design and testing of a mobile-phone-jammer. *Innovative systems design and engineering 7*(7), 7–18.

Marias, G. F., C. Delakouridis, L. Kazatzopoulos, and P. Georgiadis (2005). Location privacy through secret sharing techniques. In *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, pp. 614–620. IEEE.

Martinovic, I., P. Pichota, and J. B. Schmitt (2009). Jamming for good: a fresh approach to authentic communication in wsns. In *Proceedings of the second ACM conference on Wireless network security*, pp. 161–168.

Mascetti, S., C. Bettini, X. S. Wang, D. Freni, and S. Jajodia (2009). Providenthider: An algorithm to preserve historical k-anonymity in lbs. In *2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*, pp. 172–181. IEEE.

Meyerowitz, J. and R. Roy Choudhury (2009). Hiding stars with fireworks: location privacy through camouflage. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, pp. 345–356.

Mobini, Z., M. Mohammadi, and C. Tellambura (2018). Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications. *IEEE Transactions on Information Forensics and Security 14*(3), 621–634.

Mostafa, A. and L. Lampe (2014). Securing visible light communications via friendly jamming. In *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 524–529. IEEE.

Mouratidis, K. and M. L. Yiu (2012). Shortest path computation with no information leakage. *arXiv preprint arXiv:1204.6076*.

Olteanu, A.-M., K. Huguenin, R. Shokri, M. Humbert, and J.-P. Hubaux (2016). Quantifying interdependent privacy risks with location data. *IEEE Transactions on Mobile Computing 16*(3), 829–842.

Palanisamy, B. and L. Liu (2011). Mobimix: Protecting location privacy with mix-zones over road networks. In *2011 IEEE 27th International conference on data engineering*, pp. 494–505. IEEE.

Palanisamy, B. and L. Liu (2014a). Attack-resilient mix-zones over road networks: architecture and algorithms. *IEEE Transactions on Mobile Computing 14*(3), 495–508.

Palanisamy, B. and L. Liu (2014b). Attack-resilient mix-zones over road networks: architecture and algorithms. *IEEE Transactions on Mobile Computing 14*(3), 495–508.

Palanisamy, B., L. Liu, K. Lee, S. Meng, Y. Tang, and Y. Zhou (2014). Anonymizing continuous queries with delay-tolerant mix-zones over road networks. *Distributed and Parallel Databases 32*(1), 91–118.

Palanisamy, B., L. Liu, K. Lee, A. Singh, and Y. Tang (2012). Location privacy with road network mix-zones. In *2012 8th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, pp. 124–131. IEEE.

Pham, T. V. and A. T. Pham (2021). Energy-efficient friendly jamming for physical layer security in visible light communication. In *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6. IEEE.

Primault, V., A. Boutet, S. B. Mokhtar, and L. Brunie (2018). The long road to computational location privacy: A survey. *IEEE Communications Surveys & Tutorials 21*(3), 2772–2793.

Qu, Y., J. Zhang, R. Li, X. Zhang, X. Zhai, and S. Yu (2020). Generative adversarial networks enhanced location privacy in 5g networks. *Science China Information Sciences 63*(12), 1–12.

Samarati, P. and L. Sweeney (1998). Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression.

Shaaban, R. and S. Faruque (2021). An enhanced indoor visible light communication physical-layer security scheme for 5g networks: Survey, security challenges, and channel analysis secrecy performance. *International Journal of Communication Systems 34*(4), e4726.

Shanghai Telecom (2014). The telecom dataset. Accessed: 2020-07-17, http://sguangwang.com/TelecomDataset.html.

Shen, W., P. Ning, X. He, and H. Dai (2013). Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In *2013 IEEE Symposium on Security and Privacy*, pp. 174–188. IEEE.

Shokri, R., G. Theodorakopoulos, G. Danezis, J.-P. Hubaux, and J.-Y. Le Boudec (2011). Quantifying location privacy: the case of sporadic location exposure. In *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 57–76. Springer.

Shokri, R., G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux (2011). Quantifying location privacy. In *2011 IEEE symposium on security and privacy*, pp. 247–262. IEEE.

Solanas, A., F. Sebé, and J. Domingo-Ferrer (2008). Micro-aggregation-based heuristics for p-sensitive k-anonymity: one step beyond. In *Proceedings of the 2008 international workshop on Privacy and anonymity in information society*, pp. 61–69.

Stanojev, I. and A. Yener (2012). Improving secrecy rate via spectrum leasing for friendly jamming. *IEEE Transactions on Wireless Communications 12*(1), 134–145.

Stirbys, S., O. A. Nabah, P. Hallgren, and A. Sabelfeld (2017). Privacy-preserving location-proximity for mobile apps. In *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, pp. 337–345. IEEE.

Sun, Y., X. Su, B. Zhao, and J. Su (2010). Mix-zones deployment for location privacy preservation in vehicular communications. In *2010 10th IEEE International Conference on Computer and Information Technology*, pp. 2825–2830. IEEE.

Terrovitis, M. and N. Mamoulis (2008). Privacy preservation in the publication of trajectories. In *The Ninth international conference on mobile data management (mdm 2008)*, pp. 65–72. IEEE.

Tippenhauer, N. O., L. Malisa, A. Ranganathan, and S. Capkun (2013). On limitations of friendly jamming for confidentiality. In *2013 IEEE symposium on security and privacy*, pp. 160–173. IEEE.

Tomasin, S., M. Centenaro, G. Seco-Granados, S. Roth, and A. Sezgin (2021). Location-privacy leakage and integrated solutions for 5g cellular networks and beyond. *Sensors 21*(15), 5176.

Vilela, J. P., M. Bloch, J. Barros, and S. W. McLaughlin (2010). Friendly jamming for wireless secrecy. In *2010 IEEE International Conference on Communications*, pp. 1–6. IEEE.

Vilela, J. P., M. Bloch, J. Barros, and S. W. McLaughlin (2011). Wireless secrecy regions with friendly jamming. *IEEE Transactions on Information Forensics and Security 6*(2), 256–266.

Wang, Q., H.-N. Dai, H. Wang, G. Xu, and A. K. Sangaiah (2019). Uav-enabled friendly jamming scheme to secure industrial internet of things. *Journal of Communications and Networks 21*(5), 481–490.

Wang, S., Y. Guo, N. Zhang, P. Yang, A. Zhou, and X. Shen (2021, mar). Delay-aware microservice coordination in mobile edge computing: A reinforcement learning approach. *IEEE Transactions on Mobile Computing 20*(03), 939–951.

Wang, T. and L. Liu (2009). Privacy-aware mobile services over road networks. *Proceedings of the VLDB Endowment 2*(1), 1042–1053.

Xiao, Y. and L. Xiong (2015). Protecting locations with differential privacy under temporal correlations. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 1298–1309.

Xu, T. and Y. Cai (2008). Exploring historical location data for anonymity preservation in location-based services. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 547–555. IEEE.

Xu, Z., H. Zhang, and X. Yu (2016). Multiple mix-zones deployment for continuous location privacy protection. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 760–766. IEEE.

Yaman, O., A. Eroglu, and E. Onur (2018). Density-aware cell zooming. In *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pp. 1–8. IEEE.

Yang, D., X. Fang, and G. Xue (2013). Truthful incentive mechanisms for k-anonymity location privacy. In *2013 Proceedings IEEE INFOCOM*, pp. 2994–3002. IEEE.

Yang, Z., R. Wang, D. Wu, H. Wang, H. Song, and X. Ma (2021). Local trajectory privacy protection in 5g enabled industrial intelligent logistics. *IEEE Transactions on Industrial Informatics 18*(4), 2868–2876.

Ying, B., D. Makrakis, and H. T. Mouftah (2013). Dynamic mix-zone for location privacy in vehicular networks. *IEEE Communications Letters 17*(8), 1524–1527.

You, T.-H., W.-C. Peng, and W.-C. Lee (2007). Protecting moving trajectories with dummies. In *2007 International Conference on Mobile Data Management*, pp. 278–282. IEEE.

Zakhary, S. and A. Benslimane (2018). On location-privacy in opportunistic mobile networks, a survey. *Journal of Network and Computer Applications 103*, 157–170.

Zhong, G. and U. Hengartner (2009). A distributed k-anonymity protocol for location privacy. In *2009 IEEE International Conference on Pervasive Computing and Communications*, pp. 1–10. IEEE.

APPENDIX A

MATRICES

$$
\begin{array}{c|cccccccccccccccc|}
 & J_1 & J_2 & J_3 & J_4 & J_5 & J_6 & J_7 & J_8 & J_9 & J_{10} & J_{11} & J_{12} & J_{13} & J_{14} & J_{15} & J_{16} \\
J_1 & \widetilde{0} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_2 & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_3 & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_4 & \frac{1}{4} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_5 & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_6 & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_7 & \widetilde{0} & \widetilde{0} & \frac{1}{2} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{2} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_8 & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{2} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{2} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_9 & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} \\
J_{10} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{4} & \frac{1}{4} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} \\
J_{11} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{2} & \widetilde{0} & \frac{1}{2} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_{12} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \frac{1}{4} & \widetilde{0} & \widetilde{0} & \frac{1}{4} \\
J_{13} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} \\
J_{14} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \frac{1}{3} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \widetilde{0} \\
J_{15} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{2} & \widetilde{0} & \frac{1}{2} \\
J_{16} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \frac{1}{3} & \frac{1}{3} & \widetilde{0} & \frac{1}{3} & \widetilde{0}
\end{array}
$$

Figure A.1. Transition matrix of Figure 3.1 ($\widetilde{0}$ shows a value close to 0)

$$\begin{array}{c|ccccccccc|}
 & E_{1-1} & E_{1-2} & E_{1-3} & E_{2-1} & E_{2-2} & E_{2-3} & E_{3-1} & E_{3-2} & E_{3-3} \\
J_1 & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_2 & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_3 & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_4 & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_5 & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_6 & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_7 & \widetilde{0} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \widetilde{0} \\
J_8 & \widetilde{0} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \widetilde{0} \\
J_9 & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{\mathbf{1}} \\
J_{10} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{\mathbf{1}} \\
J_{11} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} \\
J_{12} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_{13} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} \\
J_{14} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{\mathbf{1}} \\
J_{15} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} & \mathbf{\frac{1}{2}} & \widetilde{0} \\
J_{16} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{\mathbf{1}} & \widetilde{0} & \widetilde{0} & \widetilde{0} & \widetilde{0}
\end{array}$$

Figure A.2. Emission matrix for Figure 3.1 ($\widetilde{1}$ and $\widetilde{0}$ show numbers close to 1 and 0, respectively).

APPENDIX B

ALGORITHMS

Algorithm 1 Path inference by Little Brother

```
Input1 : $O$ (Coordinates of the origin cell)
Input2 : $D$ (Coordinates of the destination cell)
Input3 : $M$ (Cell connectivity matrix)
Output: Cells between $O$ and $D$ with their likelihood
$geoplotlib.voronoi(A)$                                    ▷ Voronoi cells are built
$i1 \leftarrow 1$
$C \leftarrow O$                                           ▷ $C$ : Controlling cell
$minimum - distance \leftarrow N$                          ▷ $N$: A very large number
while $minimum - distance \neq 0$ do
    $i2 \leftarrow 1$
    $num - of - neighbors[i1] \leftarrow |N(C)|$
    while $i2 \leq |N(C)|$ do                              ▷ $|N(C)|$: Number neighbors of $C$
        $distance[i1][i2] \leftarrow |D - C_{i2}|$         ▷ $C_{i2}$: $i2^{th}$ neighbor of $C$
        if $|D - C_{i2}| < minimum - distance$ then
            $minimum - distance \leftarrow |D - C_{i2}|$
        end if                                             ▷ $|D - C_{i2}|$: Distance between $D$ & $C_{i2}$
        $i2 \leftarrow i2 + 1$
    end while
    if $minimum - distance \neq 0$ then
        $minimum - distances[i1] \leftarrow minimum - distance$
        $missing - cells[i] \leftarrow C_{i2}$
        $C \leftarrow C_{i2}$
    end if
    $i1 \leftarrow i1 + 1$
end while                                                  ▷ Missing cells are extracted
$i1 \leftarrow 1$
while $i1 \leq |missing - cells|$ do
    $i2 \leftarrow 1$                                      ▷ $|missing - cells|$: Number of missingcells
    $dummy \leftarrow 0$
    while $i2 \leq number - of - neighours[i1]$ do
        $dummy \leftarrow dummy + 1/(distance[i1][i2])^2$
        $i2 \leftarrow i2 + 1$
    end while
    $constant[i1] \leftarrow dummy$                        ▷ $constant[i1]$: $i1^{th}$ likelihood constant
    $i1 \leftarrow i1 + 1$
end while
$i1 \leftarrow 1$
while $i1 \leq |missing - cells|$ do
    $P(i1) \leftarrow [1/constant[i1]]/(minimum - distances[i1])^2$
end while                                                  ▷ Missing cell probabilities are determined
$geoplotlib.show(missing - cells)$                         ▷ Missing cells are plotted
```

Algorithm 2 Path inference by Big Brother

```
Input1 : $p(s, d)$ (Path from day d of subscriber s)
Input2 : $J$ (Locations of junctions)
Input3 : $M$ (Connectivity matrix of J)
Output1: Inferred path of junctions
Output2: Inferred path likelihood
geoplotlib.voronoi(p(d,s))                                   ▷ Voronoi cells are built
$i1 \leftarrow 1$                                            ▷ $|J|$: Number of junctions
while $i1 \le |J|$ do                                        ▷ $C_1$ : The first cell & $J_{i1}$ : $i1^{th} junction$
    $i2 \leftarrow 1$                                        ▷ $|C_1 - J_{i1}|$: Distance between $C_1$ and $J_{i1}$
    $minimum \leftarrow |C_1 - J_{i1}|$                      ▷ $Z(J_{i1})$: Zone of $J_{i1}$
    $Z(J_{i1}) \leftarrow I(C_1)$                            ▷ $I(C_1)$: Interior zone of $C_1$
    while $i2 \le |C|$ do                                    ▷ $|C|$: Number of cells
        if $|C_{i2} - J_{i1}| < minimum$ then
            $Z(J_{i2}) \leftarrow I(C_{i2})$
        end if
    end while
end while                                                    ▷ Zones of all junctions are found
$i1 \leftarrow 1$
while $i1 \le |J|$ do
    $i2 \leftarrow 1$
    while $i2 \le |N(J_{i1})|$ do                            ▷ $|N(J_{i1})|$: # neighbors of $J_{i1}$
        if $Z(J_{i1}) \neq Z(J_{i2})$ then
            $Z(J_{i1}) \leftarrow B_{Z(J_{i1})-Z(J_{i2})}$
            $Z(J_{i2}) \leftarrow B_{Z(J_{i1})-Z(J_{i2})}$
        end if                                               ▷ $B_{Z(J_{i1})-Z(J_{i2})}$:Boundary between $Z(J_{i1})$ & $Z(J_{i2})$
    end while
end while                                                    ▷ Boundary junctions are found
$i1 \leftarrow 1$
while $i1 \le |J|$ do
    $i2 \leftarrow 1$
    while $i2 \le |C|^2$ do
        if $i2 = Z(J_{i1})$ then
            if $Z(J_{i1}) = I(C_{i2})$ then
                $E(i1, Z(J_{i1})) \leftarrow \tilde{1}$      ▷ Interior case
            else
                $E(i1, Z(J_{i1})) \leftarrow 0, 5$           ▷ Boundary case
            end if
        else
            $E(i1, i2) \leftarrow \tilde{0}$                 ▷ Exterior case
        end if
    end while
end while                                                    ▷ Emission matrix E is created
$i1 \leftarrow 1$
while $i1 \le |C|$ do
    $Constant(i1) \leftarrow 0$                              ▷ $Constant(i1)$: Probability constant
    $i2 \leftarrow 1$
    while $i2 \le |I(C_{i1})|$ do                            ▷ $|I(C_{i1})|$: Number of Junctions in $I(C_{i1})$
        if $|J(I_{i2}) - C_{i1}| \le 1.5$ km then            ▷ $J(I_{i2})$: $J_{i2}$ in $I$
            $Distance(i2) \leftarrow |J(I_{i2}) - C_{i1}|$
            $Constant(i1) \leftarrow Constant(i1) + 1/Distance(i2)^2$
        end if
    end while
    $i2 \leftarrow 1$
    while $i2 \le |I(C_{i1})|$ do
        $P(I_{i2}) \leftarrow [1/Constant(i2)]/Distance(i2)^2$
        $T_I(i1, i2) \leftarrow P(I_{i2})$                   ▷ $P(I_{i2})$: $i2^{th}$ interior probability
    end while
end while                                                    ▷ Interior transition matrix $T_I$ is created
$i1 \leftarrow 1$
while $i1 < |C|$ do
    $Constant(i1) \leftarrow 0$
    $i2 \leftarrow 1$
    while $i2 \le |I(C_{i1})|$ do
        if $|J(I_{(i1+1)}) - J_{i2}| \le 1.5$ km then
            $Distance(i2) \leftarrow |J(I_{(i1+1)}) - J_{i2}|$
            $Constant(i1) \leftarrow Constant(i1) + 1/Distance(i2)^2$
        end if
    end while
    $i2 \leftarrow 1$
    while $i2 \le |I(C_{i1})|$ do
        $P(B_{i2}) \leftarrow [1/Constant(i2)]/Distance(i2)^2$
        $T_B(i1, i2) \leftarrow P(B_{i2})$                   ▷ $P(B_{i2})$: $i2^{th}$ boundary probability
    end while
end while                                                    ▷ Boundary transition matrix $T_B$ is built
$P_I \leftarrow viterbi(p(s, d), T_B, T_I)$                  ▷ $P_I$: Inferred path
geoplotlib.show($P_I$)                                       ▷ $P_I$ is plotted
```

Algorithm 3 The MATLAB algorithm of FJ simulations

```
$simcnt = 1000$    ▷ Simulation count
$Pt = 10^{-2.4}$    ▷ Transmit power in mW
$PtdBm = 10 * log_{10} Pt$    ▷ Transmit power in dBm
$f = 1.88 * 10^9$    ▷ Frequency in Mhz
$Gt = 1$    ▷ Transmitting antenna gain
$Gr = 1$    ▷ Receiving antenna gain
$gamma = 2$    ▷ Path loss exponent
$wavelength = 2.99 * 10^8 / f$    ▷ Wavelength in Mhz
$C = Gt * Gr * (wavelength/(4 * \pi))^2$    ▷ Constant based on selected wavelength
$r1 = 1 : 1 : 15$    ▷ Distance
$OurPr = C * Pt * (r_1)^{-2}$    ▷ Our received transmit power in mW
$OurPrdBm = 20 * (log_{10}(2.99 * 10^8) - log_{10}4 - log_{10}\pi - log_{10}r1 - log_{10}f) + PtdBm$    ▷ Our Pr in dBm
$OurJ = 2 * Pt - OurPr$    ▷ Our jamming power in mW
$OurJrdBm = 20 * (log_{10}(2.99 * 10^8) - log_{10}4 - log_{10}\pi - log_{10}r1 - log_{10}f) + OurJdBm$    ▷ Our received J in dBm
$PaperFspldBm = 32.44 + 20 * log_{10}(r1 * 10^{-3}) + 20 * log_{10}1880$    ▷ Free space loss of Madara et al. (2016) in dBm
$PaperJdBm = PaperFspldBm + PtdBm$    ▷ Jamming power of Madara et al. (2016) in dBm
$PaperRdBm = PaperJdBm - PaperFspldBm$    ▷ Received power of Madara et al. (2016) in dBm
$OurCounter = OurJrdBm \geq PtdBm$    ▷ Condition for coverage probability
$OurSimulation = Ourcounter/simcnt$    ▷ Our coverage probability
$PaperCounter = PaperRdBm \geq PtdBm$    ▷ Condition for coverage probability of Madara et al. (2016)
$PaperSimulation = PaperCounter/simcnt$    ▷ Coverage probability of Madara et al. (2016)
```

APPENDIX C

EXTENDED SIMULATIONS OF LITTLE BROTHER

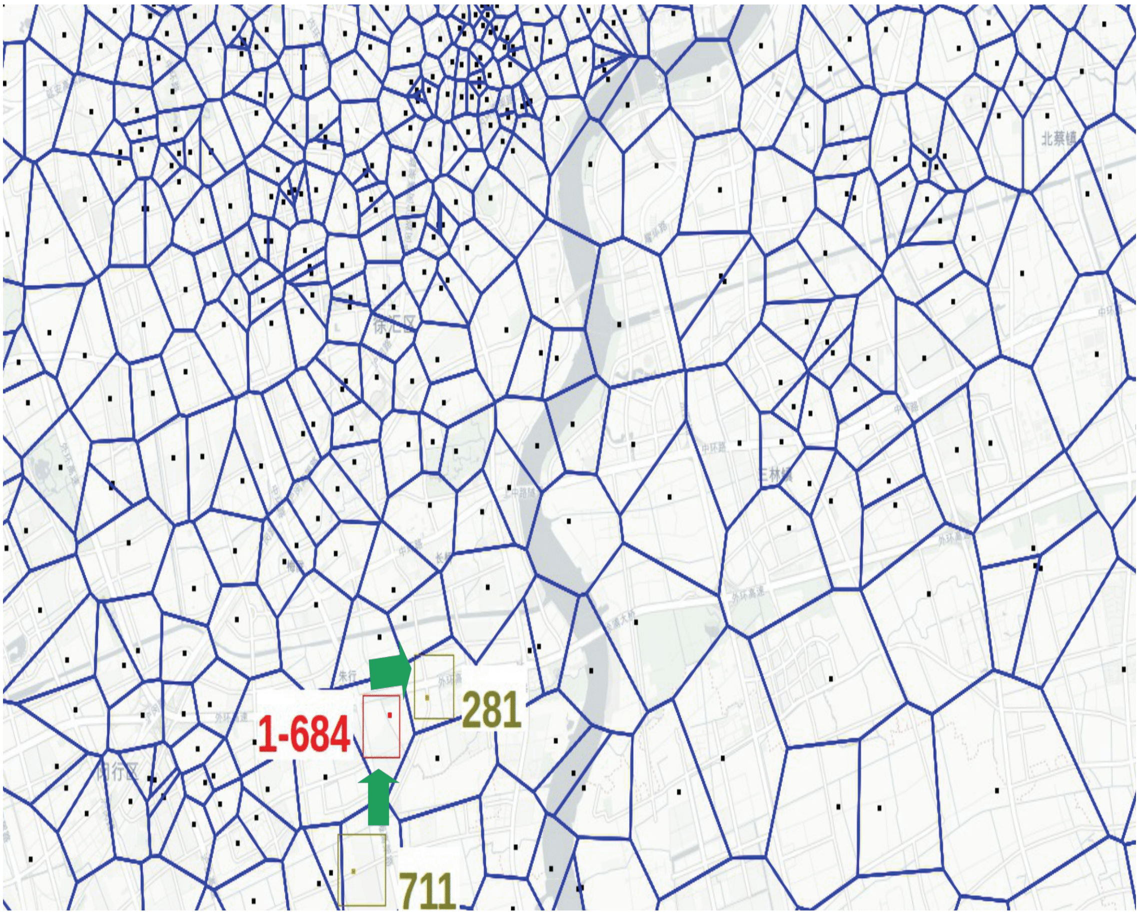


Figure C.1. A case of 1 deduced cell with its ID.

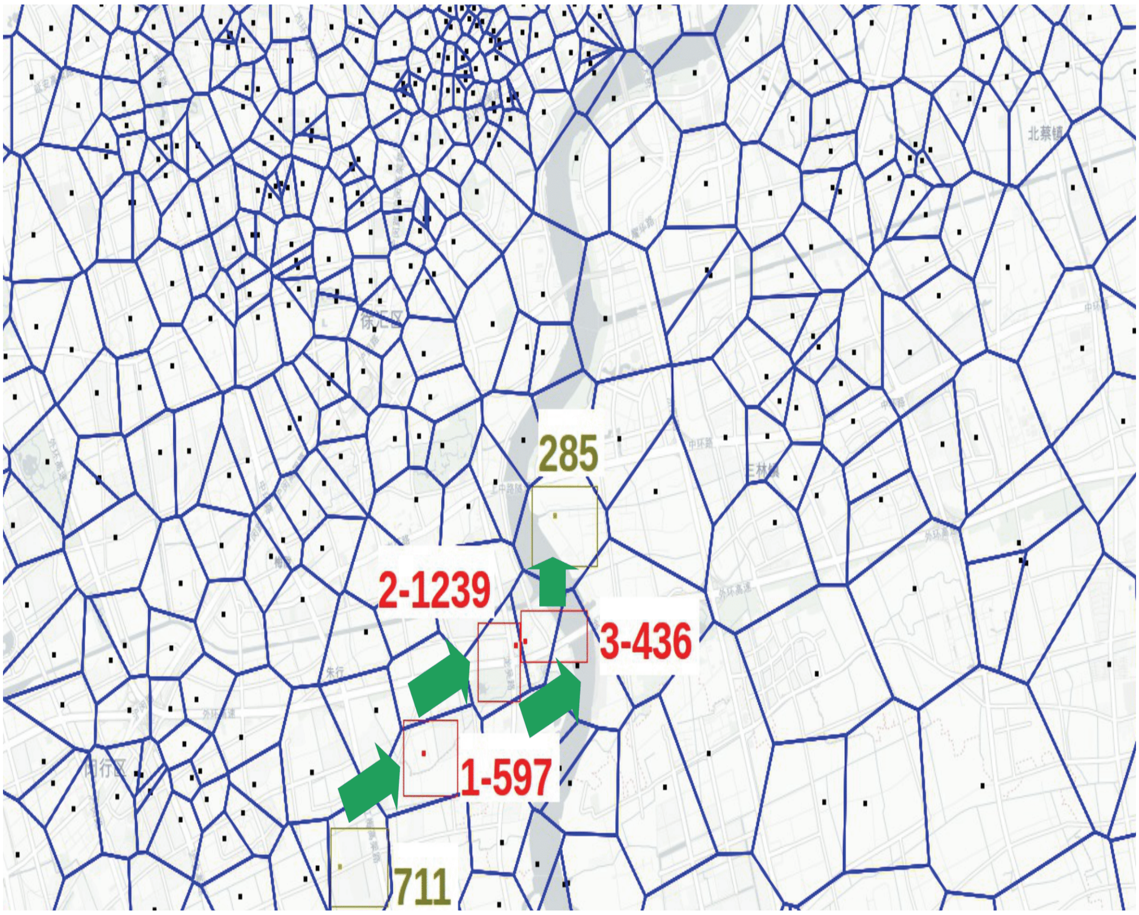


Figure C.2. A case of 3 deduced cells with their IDs.

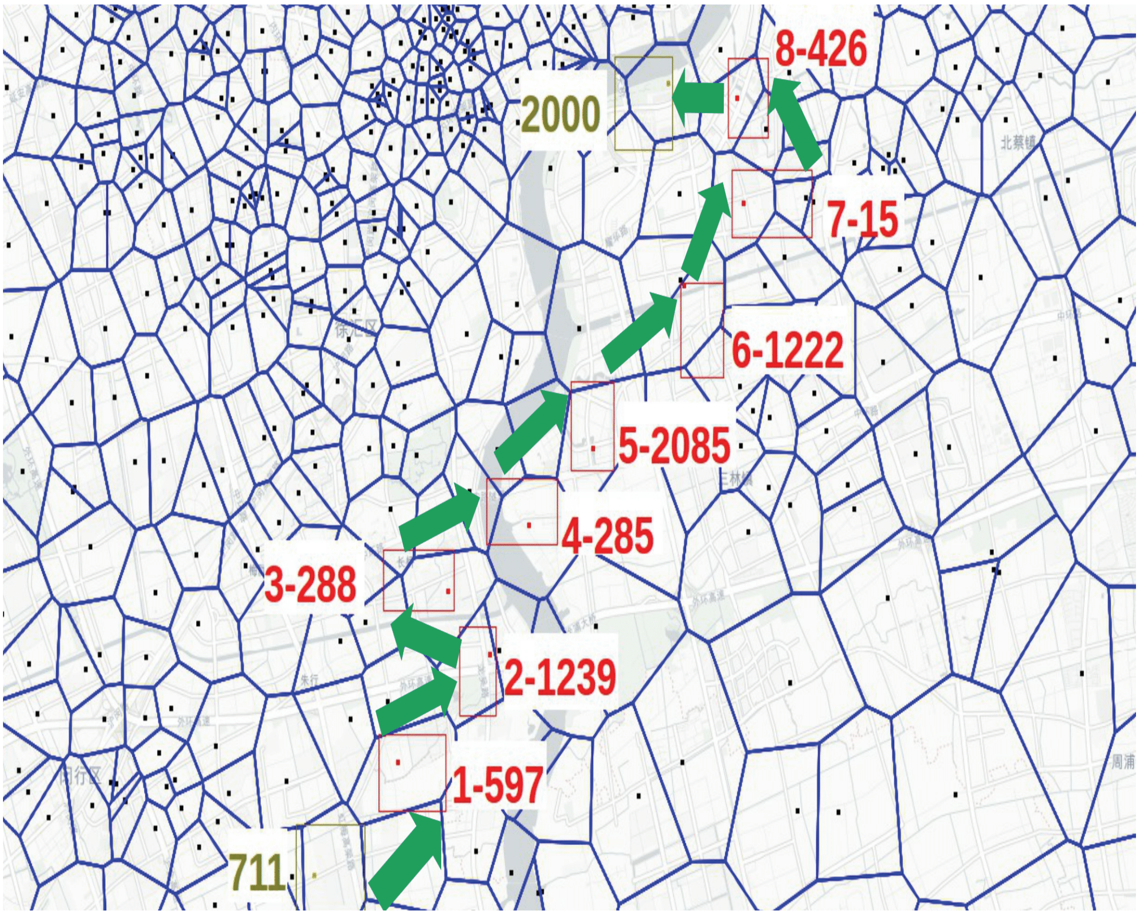


Figure C.3. A case of 8 deduced cells with their IDs.

APPENDIX D

EXTENDED SIMULATIONS OF BIG BROTHER

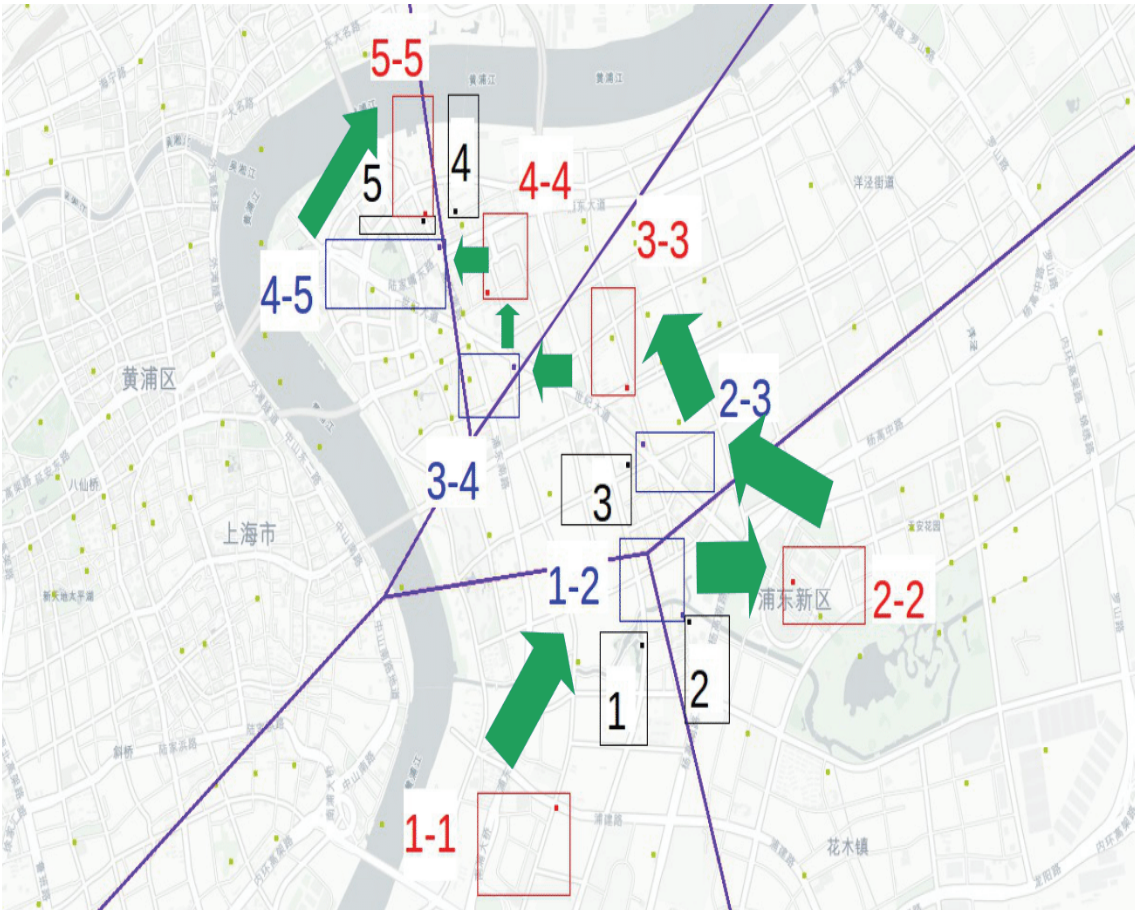


Figure D.1. A 5-celled case (Day: 17, User: 86)

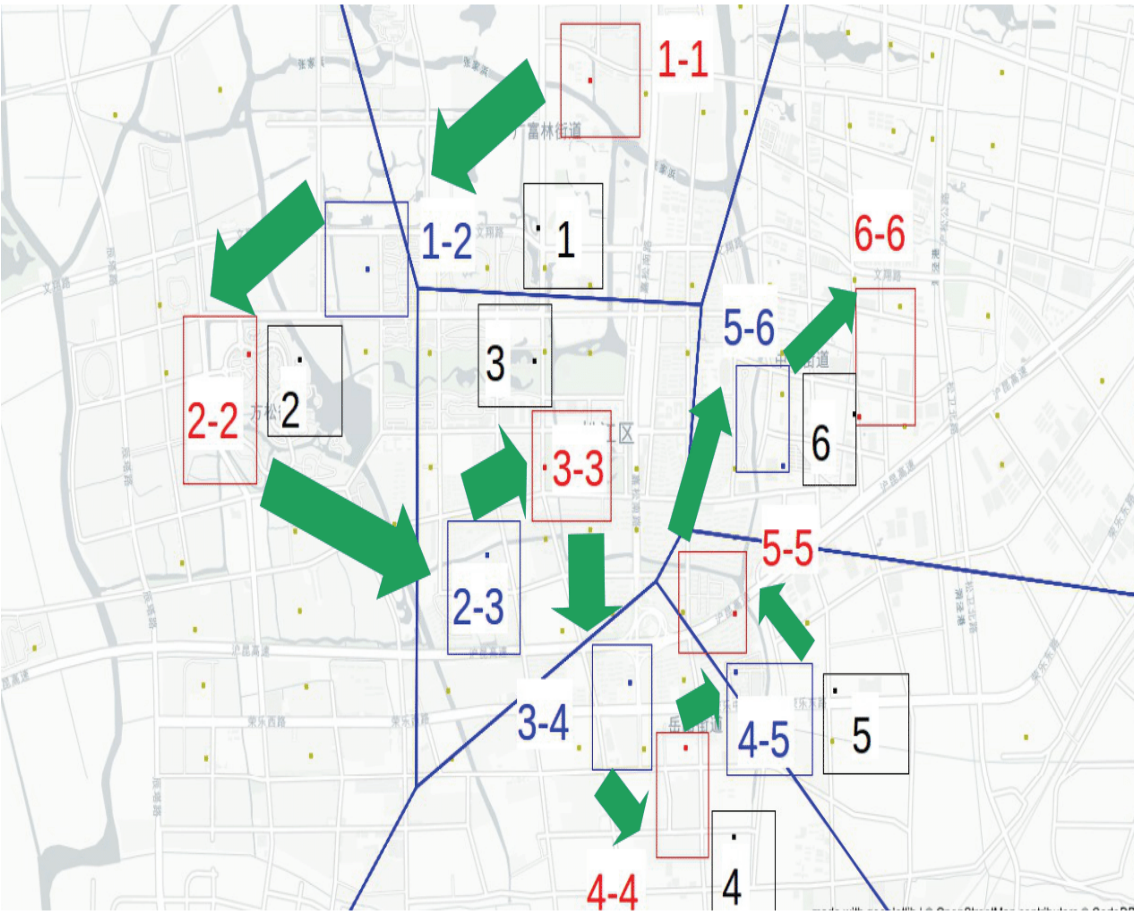


Figure D.2. A 6-celled case (Day: 23, User: 361)

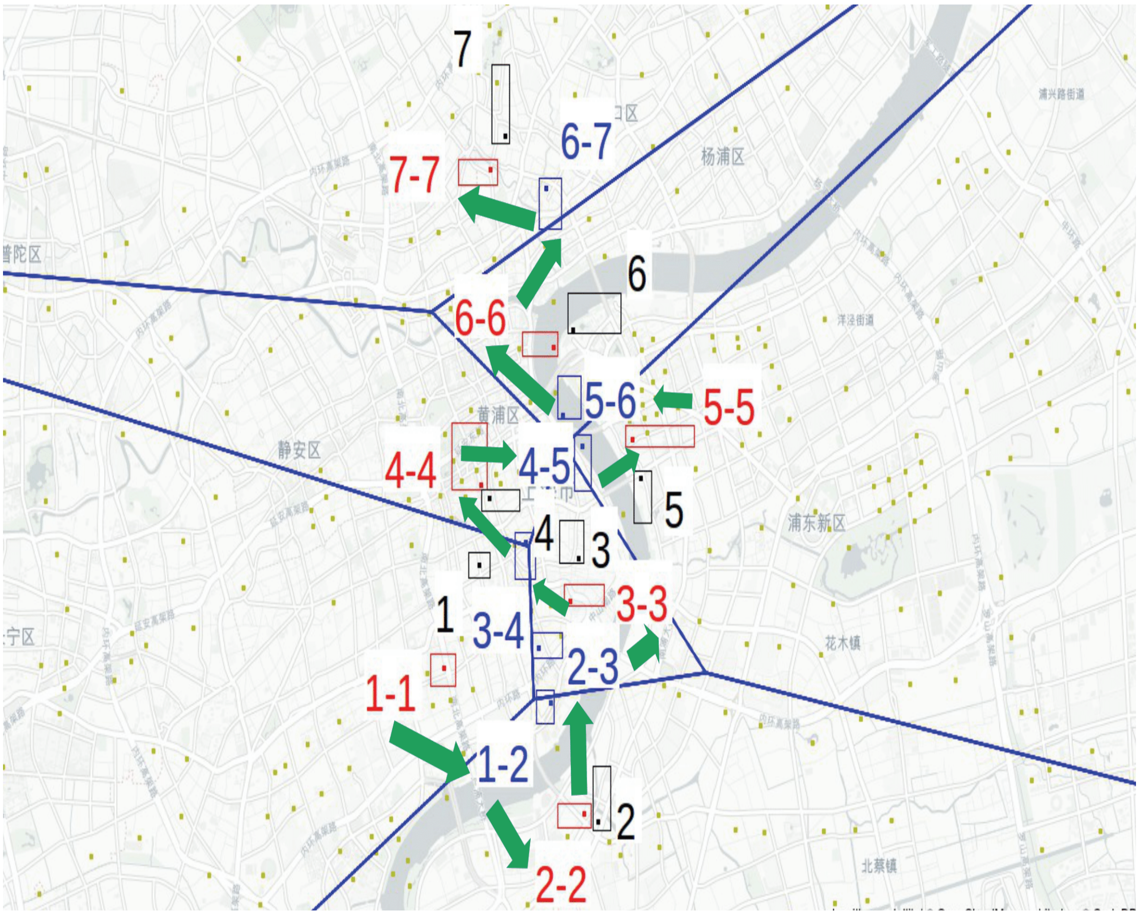


Figure D.3. A 7-celled case (Day: 5, User: 136)

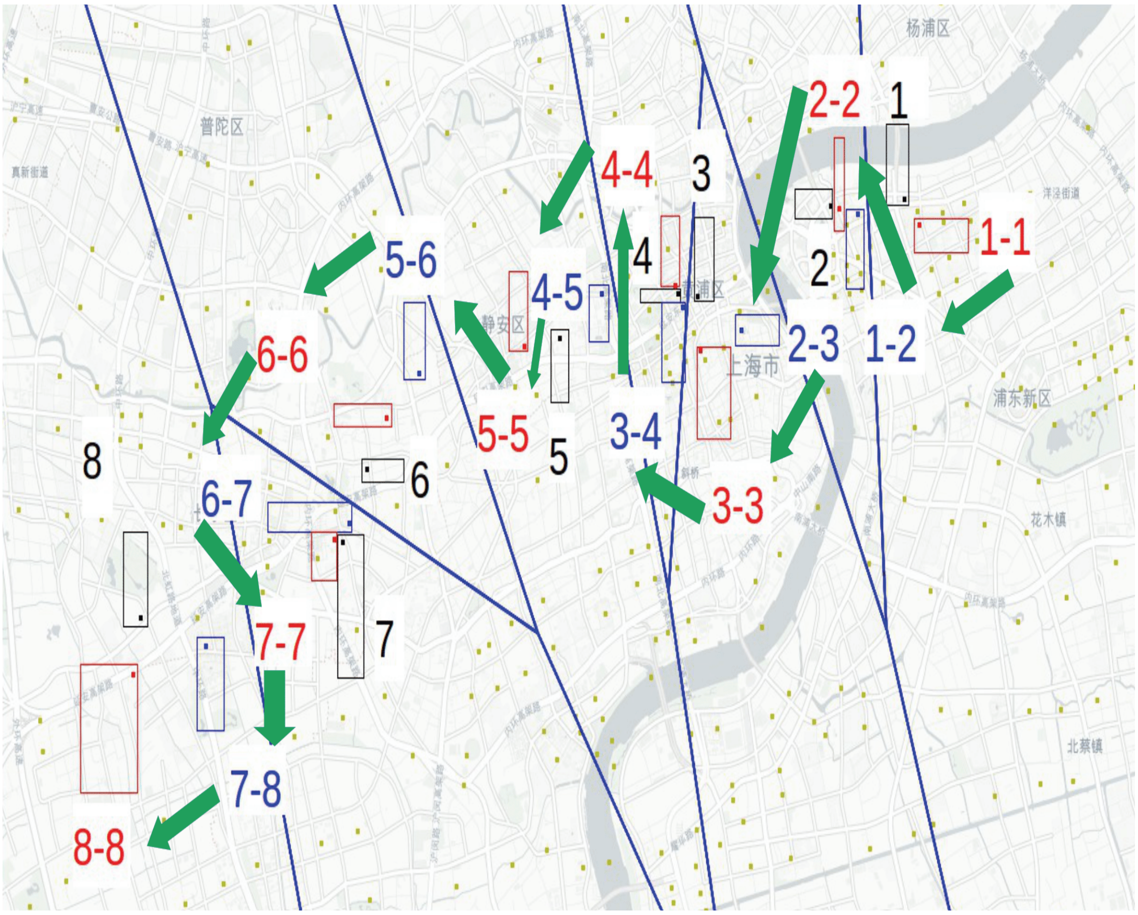


Figure D.4. An 8-celled case (Day: 18, User: 2127)

APPENDIX E

EXTENDED ANALYSIS OF LITTLE BROTHER

We mean the correct deduction of cells by "hit." As can be seen in Fig. E.1, the algorithm performs best when two cells are deduced. Inherently the probability of the deduced path decreases for increasing inferred cells. Hence, we gather less hits.

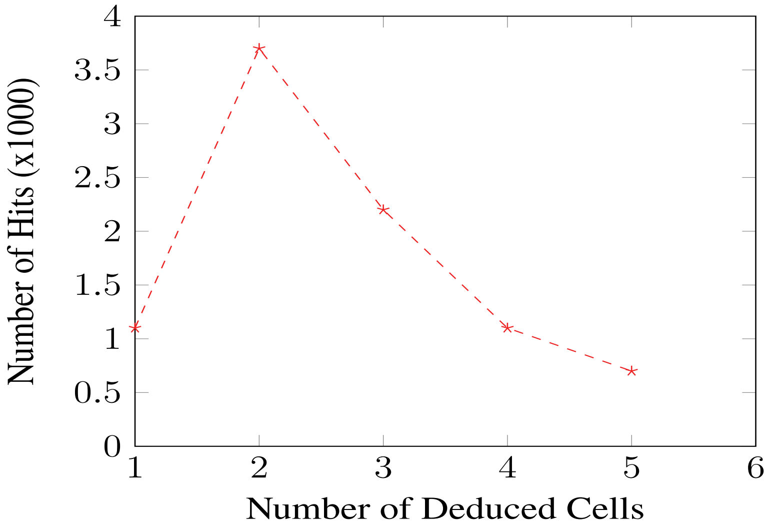


Figure E.1. The effect of deduced cells on the number of hits.

The results in Fig. E.2 and Fig. E.3 are also expected. The number of shorter paths are more than its longer counterparts. Therefore, number of all deduced cells decreases as the number of deduced cells increase.

Hit Rate

We can find the hit rates per number of paths as the following:

$$h(\#Paths) = \frac{\#Hits}{\#Paths} \tag{E.1}$$

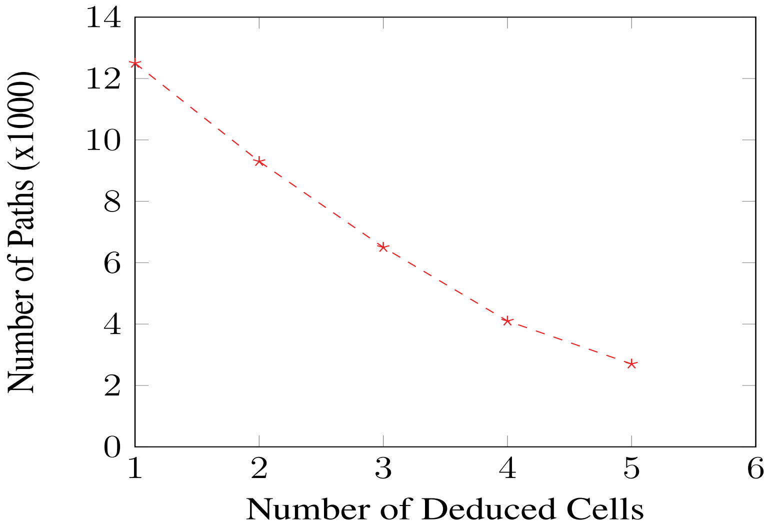


Figure E.2. The effect of deduced cells on the number of paths.

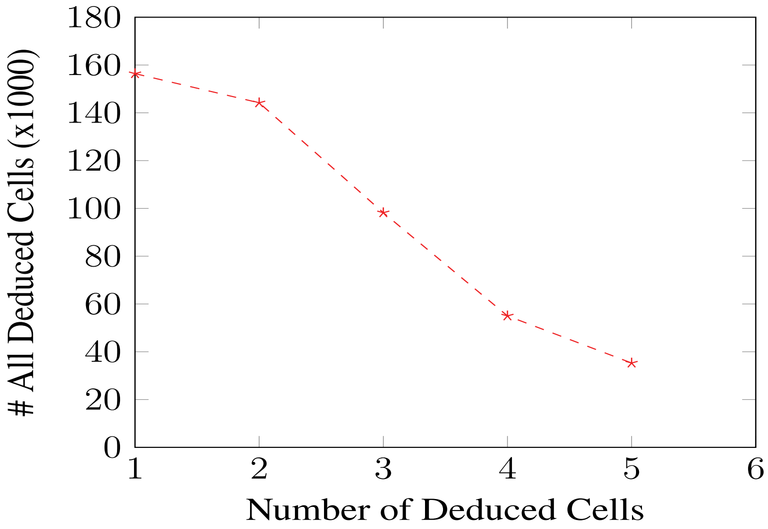


Figure E.3. The effect of deduced cells on the number of all deduced cells.

Similarly, the hit rate per number of all deduced cells is

$$h(\#All - Deduced - Cells) = \frac{\#Hits}{\#All - Deduced - Cells} \tag{E.2}$$

Since extremely large number of deduced cells, from 35000 to 156000, overwhelms the number of hits, h(#All-Deduced-Cells) has a more stable curve than h(#Paths). However, h(#Paths) has a fluctuating trend which reaches the peak when two cells are deduced. Note that, although number of paths for two cells are more than the cases of three, four and five, number of hits compensate that difference.

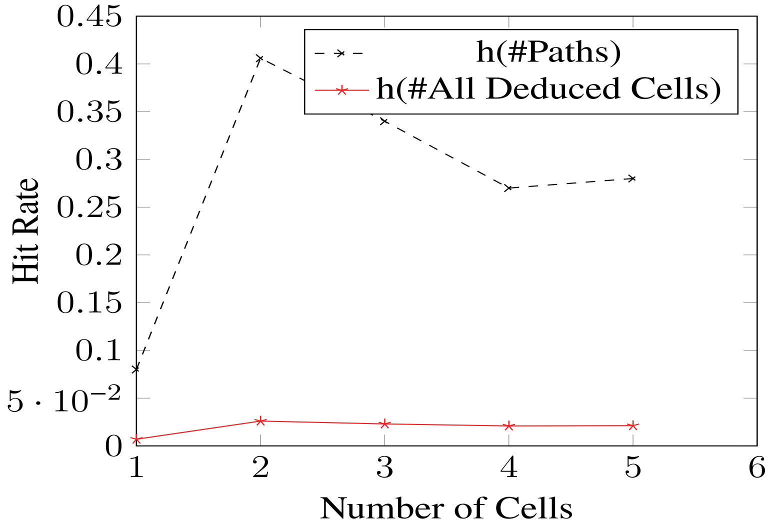


Figure E.4. The correlation between hit rate and number of deduced cells.

APPENDIX F

EXTENDED ANALYSIS ON ASSOCIATION RATE (DENSITY OF BS)

Here, association rate refers to the total number of association for a BS by any user. According to Fig. F.1, the most associated (dense) is the 652^{nd} BS with 25 times association. However, one of the least associated (sparse) BS is the 1784^{th} BS with a single association.

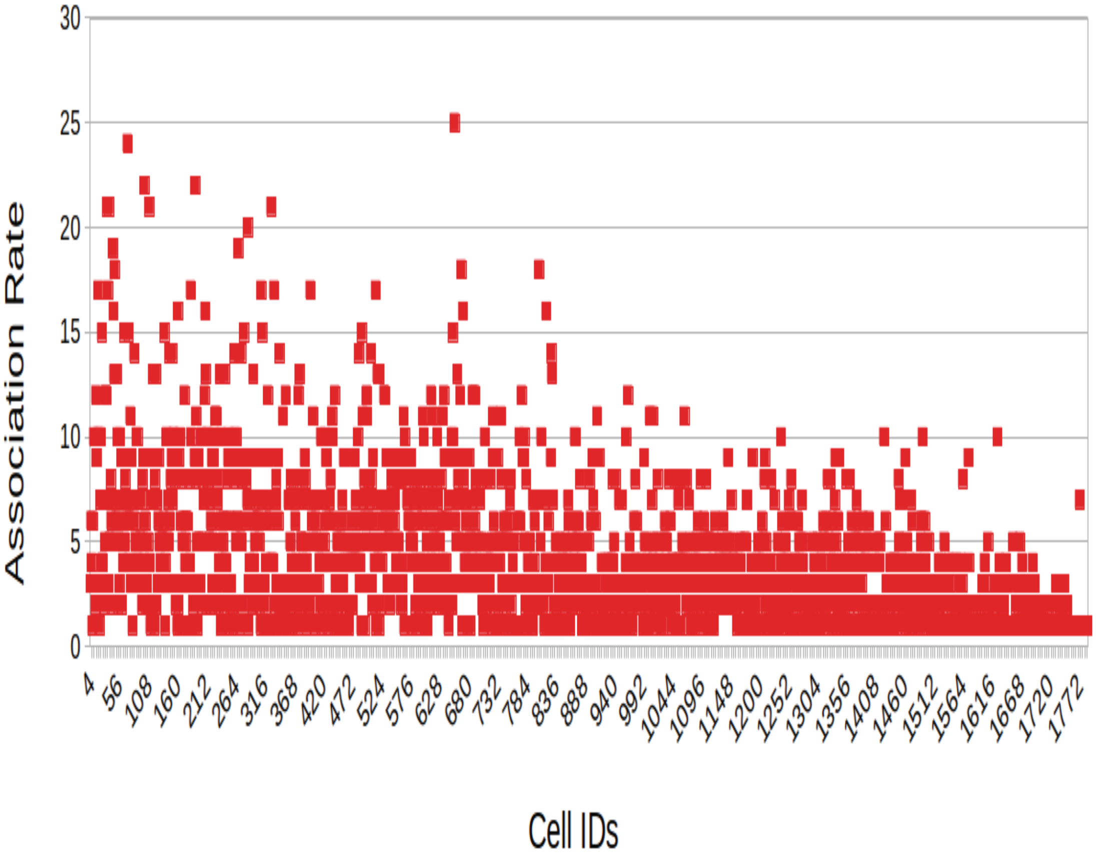
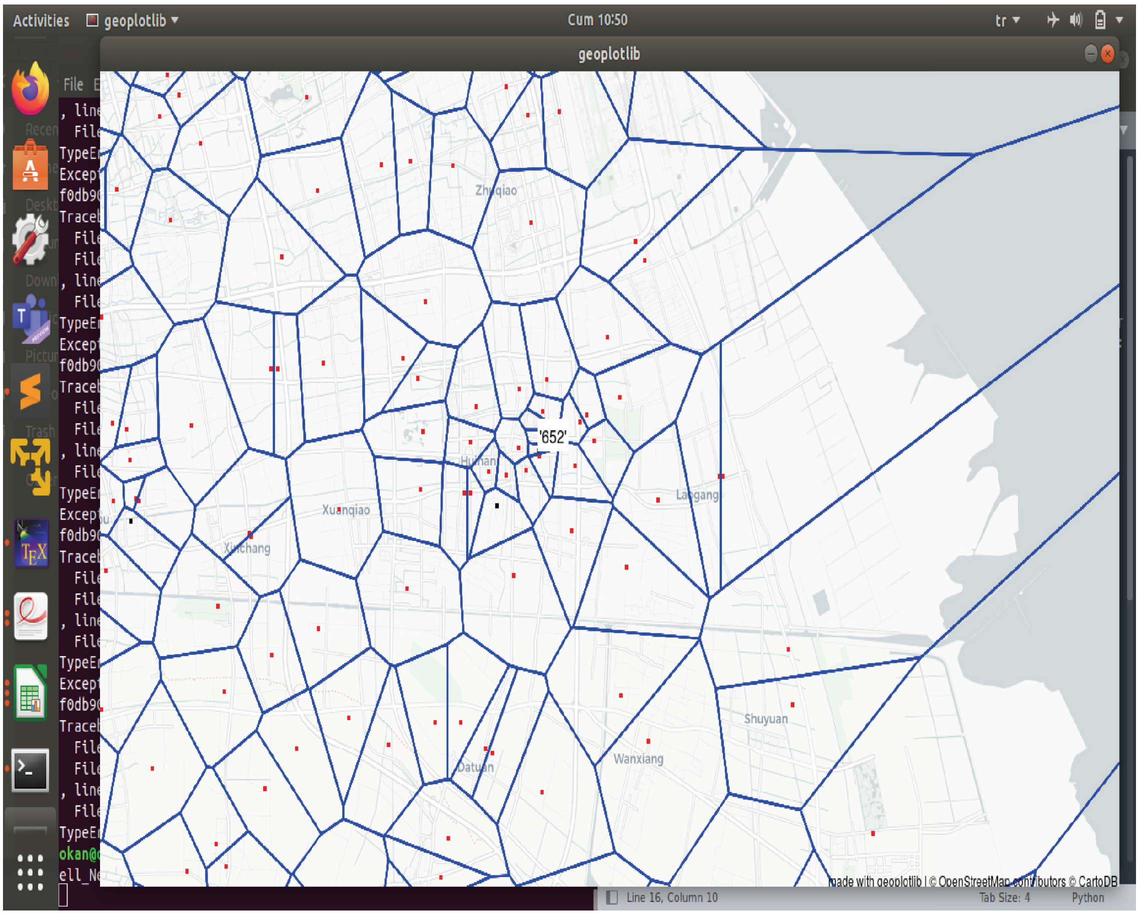
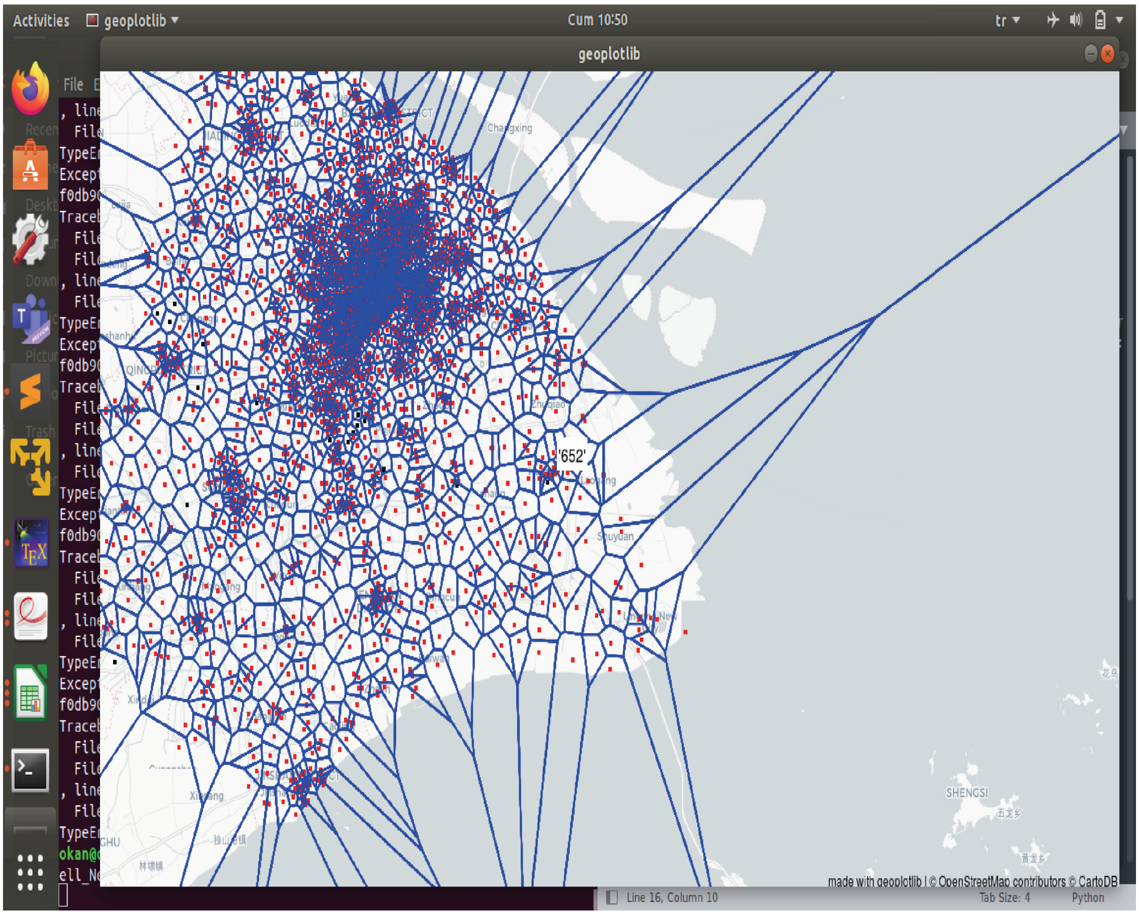


Figure F.1. Association rates of cell IDs for the first day



```
, line
  File
TypeE
Excep
f0db9c
Trace
  File
  File
, line
  File
TypeE
Excep
f0db9
Trace
  File
  File
, line
  File
TypeE
Excep
f0db9
Trace
  File
  File
, line
  File
TypeE
Excep
f0db9
Trace
  File
  File
, line
  File
TypeE
okan@
ell_Ne
```

Figure F.2. Location of the most associated BS with ID 652



```
, line
  File
TypeEr
Except
f0db9c
Traceb
  File
  File
, line
  File
TypeEr
Except
f0db9c
Traceb
  File
  File
, line
  File
TypeEr
Except
f0db9c
Traceb
  File
  File
, line
  File
TypeEr
Except
f0db9c
Traceb
  File
  File
, line
  File
TypeEr
okan@c
ell_Ne
```

Figure F.3. Location of the most associated BS with ID 652 in a sky view

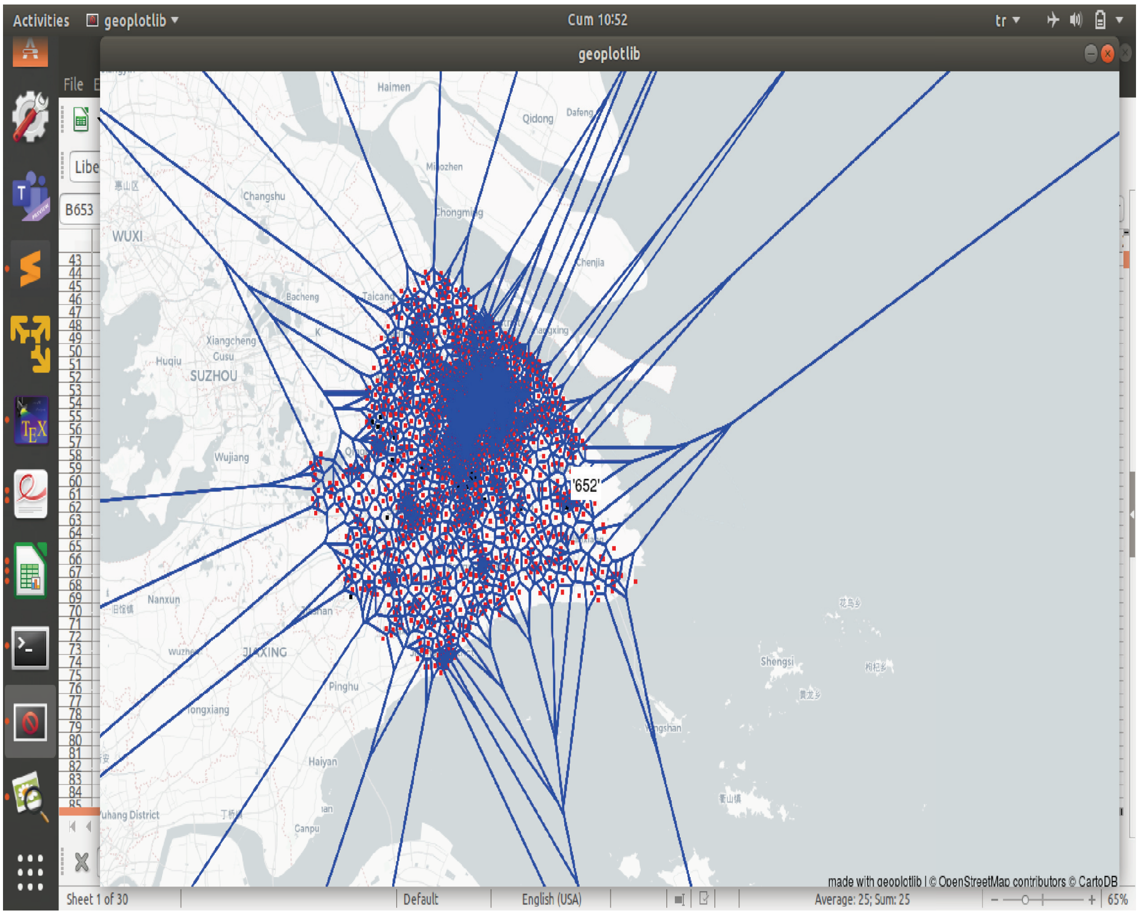


Figure F.4. Location of the most associated BS with ID 652 in a broader sky view

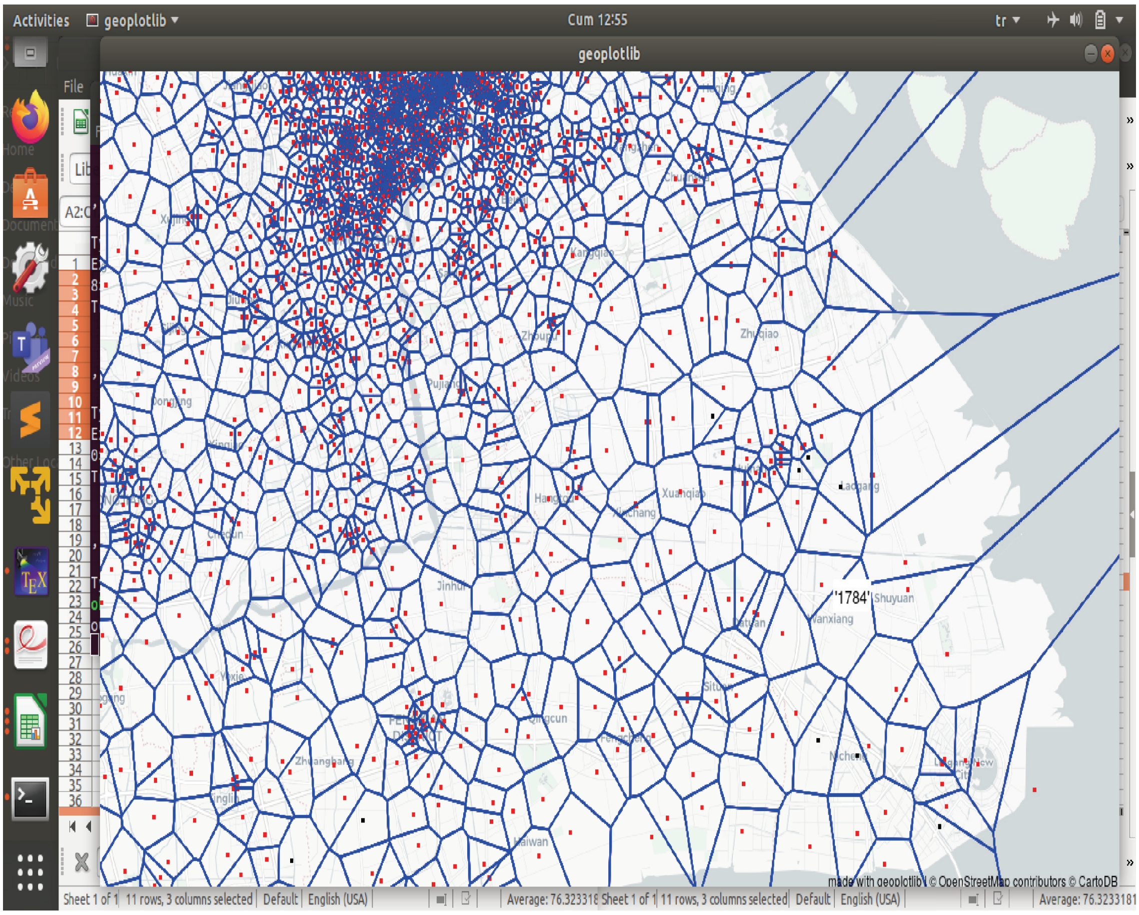


Figure F.5. Location of one of the least associated BS with ID 1784

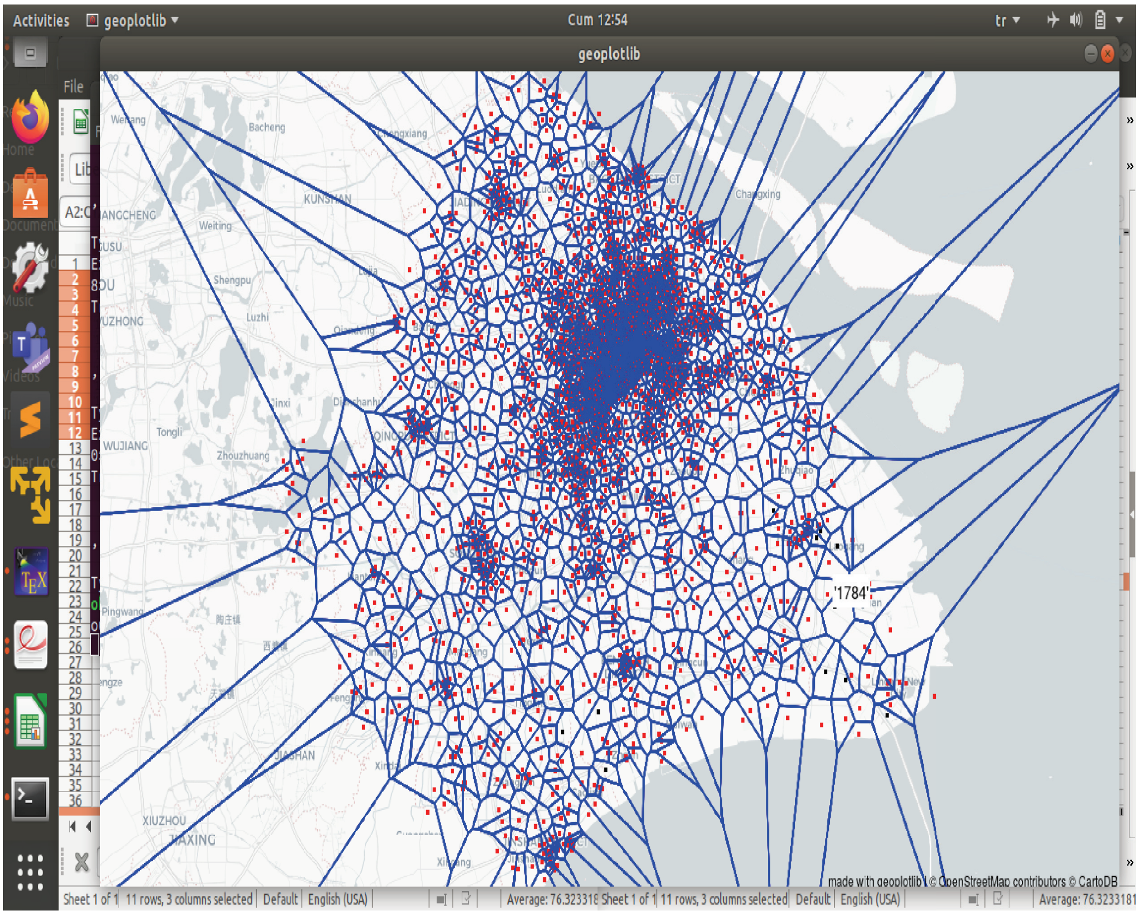

Activities
geoplotlib
Cum 12:54
tr
geoplotlib
File
'1784'
KUNSHAN
WUJIANG
JIASHAN
XIUZHOU
JIAXING
Changxing
Bacheng
Weiting
Shengpu
Luzhi
Tongli
Zhouzhuang
Pingwang
made with geoplotlib | © OpenStreetMap contributors © CartoDB
Sheet 1 of 1 | 11 rows, 3 columns selected | Default | English (USA) | Average: 76.323318

Figure F.6. Location of one of the least associated BS with ID 1784 in a sky view

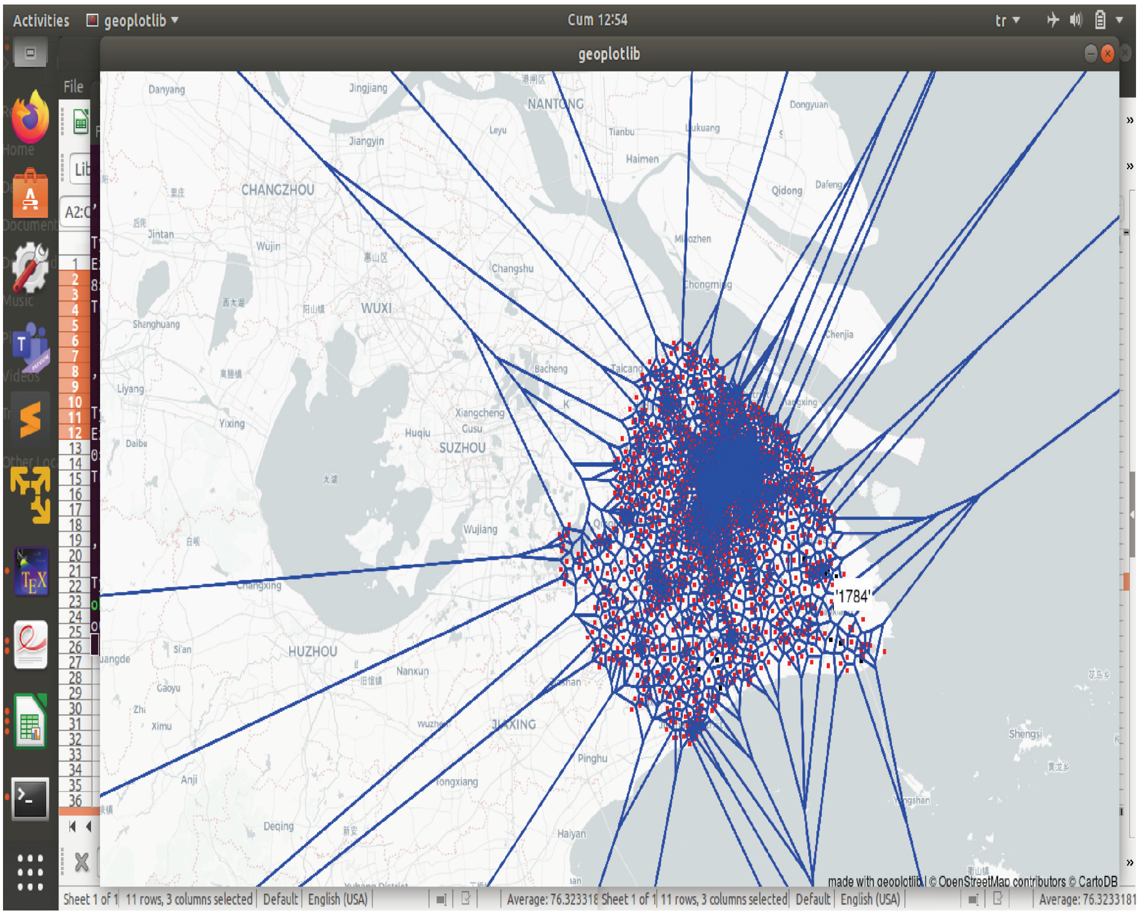


Figure F.7. Location of one of the least associated BS with ID 1784 in a broader sky view

VITA

In 2012, Okan YAMAN received his BS in Mathematics from the Middle East Technical University (METU), Ankara, TURKEY, and became an honor student in the spring semester. Okan earned an MS in Computer Engineering (CENG) from METU in 2016. Then, just after graduation, he worked at Armada Consultancy, Ankara, TURKEY as a computer engineer and transport modeler for the Turkish National Transport Master Plan EU project. Next year he was recruited by Leadonly Corporation, which provides lead automation for the health sector. In 2018, one of his former studies, "Density-aware Cell Zooming," supervised by Prof. Ertan ONUR, was accepted and published as the proceedings of the 21st Innovations in Cloud Internet and Networking (ICIN) Conference supported by IEEE and IFIP. An extension of this study, "Density-aware Cellular Coverage Control: Interference-based Density Estimation," was published in the journal of Computer Networks in 2019.

Moreover, he was accepted as a visiting researcher by Kasper RASMUSSEN (Prof. in the University of OXFORD Computer Science Department) in the same year. Okan also supported IEEE Access as a referee for some studies in 2019. His latest study, "A Novel Countermeasure for Selective Forwarding Attacks in IoT Networks" supervised by Prof. Yusuf Murat ERTEN and Assoc. Prof. Tolga AYAV, was published by the 3rd International Informatics and Software Engineering Conference in 2022. His another study which is also a part of this dissertation was accepted by the International Journal of Information Security Science in 2022 as well. He was a YOK 100/2000 Doctoral Scholar.