Imperial College London

Privacy-preserving Human Mobility and Activity Modelling

Yuting Zhan

2022

Imperial College London
Dyson School of Design Engineering

A thesis submitted to the Imperial College London for the degree of
Doctor of Philosophy
in the Faculty of Engineering

Abstract

The exponential proliferation of digital trends and worldwide responses to the COVID-19 pandemic thrust the world into digitalization and interconnectedness, pushing increasingly new technologies/devices/applications into the market. More and more intimate data of users are collected for positive analysis purposes of improving living well-being but shared with/without the user's consent, emphasizing the importance of making human mobility and activity models inclusive, private, and fair. In this thesis, I develop and implement advanced methods/algorithms to model human mobility and activity in terms of temporal-context dynamics, multi-occupancy impacts, privacy protection, and fair analysis.

The following research questions have been thoroughly investigated: i) whether the temporal information integrated into the deep learning networks can improve the prediction accuracy in both predicting the next activity and its timing; ii) how is the trade-off between cost and performance when optimizing the sensor network for multiple-occupancy smart homes; iii) whether the malicious purposes such as user re-identification in human mobility modelling could be mitigated by adversarial learning; iv) whether the fairness implications of mobility models and whether privacy-preserving techniques perform equally for different groups of users.

To answer these research questions, I develop different architectures to model human activity and mobility. I first clarify the temporal-context dynamics in human activity modelling and achieve better prediction accuracy by appropriately using the temporal information. I then design a framework *MoSen* to simulate the interaction dynamics among residents and intelligent environments and generate an effective sensor network strategy. To relieve users' privacy concerns, I design *Mo-PAE* and show that the privacy of mobility traces attains decent protection at the marginal utility cost. Last but not least, I investigate the relations between fairness and privacy and conclude that while the privacy-aware model guarantees group fairness, it violates the individual fairness criteria.

Declaration of originality

I hereby confirm that the content presented in this thesis is carried out by myself. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Copyright statement

Acknowledgements

I would like to express my sincere gratitude to so many people for their solid support, especially during the Coronavirus pandemic. Without their invaluable help, the successful completion of my PhD is impossible.

First and foremost I deeply acknowledge my supervisor **Dr.Hamed Haddadi** for his continuous support, guidance, and encouragement. During my PhD study, Dr.Haddadi helped me broaden research ideas, strengthen critical thinking, and widen collaboration networks. His immense knowledge and plentiful experience have encouraged me all the time in my academic research and daily life.

I would like to extend my sincere thanks to Dr.Afra Mashhadi for the great collaboration. I really learned a lot from the insightful comments and discussions. Also, many thanks to my examiners Dr.Sonia Ben Mokhtar from CNRS (external) and Dr.David Boyle (internal) for their time to review this thesis and for all their constructive and invaluable suggestions.

Being a part of the SysAL research group is a fantastic and impressive experience. I would like to thank group members, Ranya, Anna, Minos, Mohammad, Vincent, Yuchen and more, for the great support, discussions, and collaborations. My special thanks go out to my special partner, Senyou, whose support and encouragement were a necessity in these years. I would also like to thank and acknowledge my other friends, who are always available in tough times.

My gratitude extends to the Imperial-CSC Joint Scholarship to undertake my studies at the Dyson School of Design Engineering, and to the staff at CSC for all their support during my PhD.

Last but not least, I wholeheartedly appreciate the unwavering support and love I received from my family. Their endless kindness and belief in me are felt at all times.

Yuting Zhan

November 9, 2022

Contents

Word Count: 31437

List of figures

List of tables

Chapter 1

Introduction

1.1 Motivation

The term *Internet of Things* (*IoT*) is used to define a network of interrelated physical objects - things - with sensors, processing ability, software, and other technologies for the purpose of connecting any device to other connected devices and internet [1, 2]. Generally, an IoT device is something that has an internet connection [3, 4], including but not limited to smart consumer electronics (*e.g.*, smartwatches [3], appliances [4], security cameras [5]), industrial machinery [6], smart infrastructure [7], fleet and logistics (*e.g.*, vehicles, ships, aircraft) [8, 9], connected marketplaces [10], etc. According to the market and consumer data from *Statista* [11], with more than 13.1 billion connected devices in the world today, experts are expecting this number to grow to 29.4 billion by 2030[1]. The global IoT market size was worth around 389 billion U.S. dollars in 2020 and is forecast to rise to more than one trillion dollars in 2030, exhibiting a compound annual growth rate (CAGR) of 26.4% during the span of time[2] [11].

The exponential proliferation of digital trends has thrust the world onto digitalization and interconnectedness [3, 4, 12]. Among such a wide variety of IoT, the smartphone and smart home have the highest penetration rate and internet usage, where a higher usage generally means a more receptive market for new applications, investments, and innovations [11]. Since 2020, the COVID-19 pandemic has also driven dramatic shifts in human lives, unprecedented and staggeringly, which also accelerates a rapid and large-scale adoption of IoT devices and other tracing applications [13, 14]. This trend toward digital transformation and the digital economy are constantly pushing new technologies/devices into the market [15]. On the one hand, lives have been altered significantly in fighting the battle with the pandemic, including but not limited to zoom burnout, mask profiteering, virtual conferences, and work from home (WFH) [16, 17]. The pandemic has supercharged the trend that technology erodes the wall between work and home. People rely more heavily on consumer electronics, and more personal data have been collected with/without their consent. On the other hand, social isolation due to pandemics

[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
[2] https://www.statista.com/statistics/1194709/iot-revenue-worldwide/

on disadvantaged, marginalized, and vulnerable populations have consequences on their well-being and overall health, especially for the elderly [18, 19]. With social isolation, loneliness among seniors is linked to a higher rate of depression and anxiety, which is also associated with a greater risk of dementia and death from all causes [19].

In this digital trend, more and more intimate data of users are collected for a positive analysis purpose of improving living well-being while being shared with/without the user's consent [20, 21]. The facts of the high penetration of connected devices and large-scale data collection emphasize the importance of making human mobility and activity models inclusive, private, and fair [22, 23]. Hence, with diverse needs for a variety of intelligent scenarios, human mobility and activity modelling should always keep pace with the times, satisfy the users' needs practically, and also be more privacy-sensitive. In this thesis, advanced methods and algorithms are developed to model human mobility and activity in discussing the temporal-spatial impacts, multi-occupancy impacts, privacy protection, and fair analysis. The motivations of the work are concluded in three dimensions as follows:

I. Human Mobility Modelling

During the last decade, the growing number of internet and smartphone users has fundamentally reshaped the digital economy [4, 12]. Rapid and large-scale adoption of mobility devices brings unprecedented data for researchers and practitioners to analyze in sectors such as census estimates [24], tourism [25], marketing [26], urban planning [27], etc. Due to the pandemic, human mobility data has come to prominence with more applications again, including but not limited to community transmission risk, effectiveness, and impact of social distance policies [28]. A study conducted by De Montjoye *et al.* [29] examined human mobility data for one and a half million individuals over fifteen months and found that four spatio-temporal points are enough to uniquely identify 95% of the individuals. While there is no doubt about the usefulness of predictive applications for mobility data, privacy concerns regarding the collection and sharing of individuals' mobility traces have prevented the data from being utilized to their full potential [30–32]. All of these give room to privacy concerns and highlight the importance of exploring the privacy-utility trade-off of human mobility.

II. Human Activity Modelling

Apart from human mobility, human activity modelling (*i.e.*, human activity recognition, HAR) can be leveraged to provide human action information and build a behavioural profile. HAR is the central task to many intelligent systems such as smart homes [33], long-term healthcare [34], personal robotics [35], assisted living [36], and human-computer interaction [37]. As one of the most popular research scenarios, healthcare or eldercare utilized HAR to improve seniors' lifestyles and prolong their independent life by forecasting potential risks or dementia trends. To fully understand the context of HAR, the temporal-context dynamics are essential. Additionally, while multitudes of sensors extend the variety of information received, the het-

erogeneity of the devices [38] and the increasing number of the residents [39, 40] complicate the data collection system in real settings. Even for *single-occupancy scenarios*, where only a single individual is in the single space, the diversity of sensor settings or floorplans could affect the overall performance of sensor networks. Importantly, sensor networks designed for single-occupancy houses are never deployed in identical settings, and sensor selection in each system is diverse, varying from commercial products to self-built devices [41–44]. The price, stability, precision, and coverage range of different sensors affect the implementation and performance of sensor-based systems [44]. It isn't easy to find a uniform sensor integration system flexible to different homes, especially when the houses might have more than one resident, referring to the *multi-occupancy scenarios* in this thesis. Prior research has already specified the significance of multi-occupancy scenarios. Still, the complexity of the ongoing sensor networks and unknown uncertainties impede the actual implementation of the sensor network and further analysis [39, 45–48].

III. Privacy-preserving Mechanism

As the adoption of advanced human mobility and activity modelling rises in recent years, so as the concerns about the privacy protection of data utilization. New regulations such as the General Data Protection Regulation (GDPR) [49] in Europe and California's Consumer Privacy Act (CCPA) [50] in the US have emerged for the purpose of data privacy protection. There is no doubt that the increasing digital trend magnifies the uniqueness of individuals as more intimate information is unveiled. With increasingly intelligent devices and sensors being utilized to collect information about users' locations and activities, a malicious third party can derive increasingly intimate details about users' lives, from their social life to their preferences [51]. User re-identification and other sensitive inferences are major privacy threats when geolocated data are shared with cloud-assisted applications [52]. Hence, a mechanism capable of decreasing the chance of user re-identification against malicious attackers or untrusted SPs can offer enhanced privacy protection in mobility data applications, as human mobility traces are highly unique.

1.2 Objectives and Outlines

This thesis mainly focuses on the study of making human mobility and activity models inclusive, private, and fair. The studied scenarios and architectures with objectives are outlined as follows:

1.2.1 Human Activity Modelling in Mapping Contextual-temporal Dynamics

Chapter 2 - Existing activity recognition technologies empower the smart home to perceive the ambient environment. Efficient activity prediction, based on activity recognition, can enable the smart home to provide timely, personalized services. However, predicting the next activity and its specific occurrence period are challenging due to the complexity of modelling human behaviour. This chapter aims to understand whether the temporal information integrated into the deep learning networks can improve the prediction accuracy in predicting the next activity and its timing.

1.2.2 Human Activity Modelling in Multiple-Occupancy Smart Home

Chapter 3 - Smart home solutions increasingly rely on various sensors for behavioural analytics and activity recognition to provide context-aware applications and personalized care. Optimizing the sensor network is one of the most important approaches to ensuring classification accuracy and system efficiency. However, the trade-off between cost and performance is often a challenge in real deployments, particularly for multiple-occupancy smart homes. The majority of the feasible and practical solutions are limited to the *single-occupancy scenario*, where the system is not easily capable of identifying and assessing the target individual, without the use of costly and often privacy-invasive technologies. To aid in accelerating the adoption of practical sensor-based activity recognition technology, in this chapter, *MoSen* is introduced, a framework to simulate the interaction dynamics between sensor-based environments and multiple residents.

1.2.3 Privacy-aware Adversarial Network in Human Mobility Modelling

Chapter 4 - As mobile devices and location-based services are increasingly developed in different intelligent city scenarios and applications, many unexpected privacy leakages have arisen due to geolocated data collection and sharing. User re-identification and other sensitive inferences are major privacy threats when geolocated data are shared with cloud-assisted applications. To tackle malicious purposes such as user re-identification, in this chapter, I propose an LSTM-based adversarial mechanism (*i.e.*, *Mo-PAE*) with representation learning to attain a privacy-preserving feature representation of the original geolocated data (*i.e.*, mobility data) for a sharing purpose. These representations aim to maximally reduce the chance of user re-identification and full data reconstruction with a minimal utility budget (*i.e.*, loss).

1.2.4 Characterizing Mobility Data on the Privacy and Fairness

Chapter 5 - Preserving the individuals' privacy in sharing spatial-temporal datasets is critical to prevent re-identification attacks based on unique trajectories. Existing privacy techniques tend to propose ideal privacy-utility tradeoffs, however, they largely ignore the fairness implications of mobility models and whether such techniques perform equally for different groups of users. The quantification between fairness and privacy-aware models is still unclear, and no defined sets of metrics barely exist for measuring fairness in the spatial-temporal context. In this chapter, I define a set of fairness metrics designed explicitly for human mobility and investigate the fairness of privacy-aware models.

1.3 Contributions

In the *Human activity modelling in mapping contextual-temporal dynamics:*

- I develop two LSTM-based activity predictors, both with *deep contextualized word representation* on sensor labels, one with temporal information and one without;
- I discuss the contextual-temporal dynamics in modelling human activity prediction. The results highlight that if temporal information is used appropriately, the model with timestamp can outperform the model without.

In the *Human activity modelling in multiple-occupancy smart home:*

- To aid in accelerating the adoption of practical sensor-based activity recognition technology, I design *MoSen* [3], a framework to simulate the interaction dynamics between sensor-based environments and multiple residents;
- By using real indoor activity and mobility traces, floor plans, and synthetic multi-occupancy behaviour models, several multi-occupancy household scenarios with 2-5 residents are emulated and evaluated;
- I explore and quantify the trade-offs between the cost of sensor deployments and expected labelling accuracy in different scenarios. The evaluation across different scenarios shows that the performance of the desired context-aware task is affected by different localization resolutions, the number of residents, the number of sensors, and varying sensor deployments;

[3] https://github.com/YutingZhan/MoSen

- By evaluating the factors that affect the performance of the desired sensor network, *MoSen* provides a sensor selection strategy and design metrics for sensor layout in real environments. Using the selection strategy in a 5-person scenario case study, I demonstrate that *MoSen* can significantly improve overall system performance without increasing the deployment costs.

In the *Privacy-aware adversarial network in human mobility modelling:*

- To tackle malicious purposes such as user re-identification, I propose a **p**rivacy-aware **a**dversarial network to train an effective feature extractor $\boldsymbol{E}nc_L$ for **mo**bility privacy, namely *Mo-PAE* [4];
- I report the analysis of Mo-PAE by a comprehensive evaluation of four real-world representative mobility datasets;
- I provide an extensive analysis of different inference tasks and quantify the privacy and utility bound of the target mobility dataset, along with a trade-off analysis between these contrasting objectives;
- I compare the Mo-PAE with, i) a famous DP notion that developed on the idea from Geo-indistinguishability [53] (namely GI-DP); ii) a state-of-the-art GAN-based mechanism that attempts to generate synthetic privacy-preserving mobility data (namely TrajGAN [54]); iii) as well as the optimal LSTM-based inference models, and obtain favourable results.

In the *Characterizing mobility data on the privacy and fairness:*

- I define a set of fairness metrics designed explicitly for human mobility, based on structural similarity and entropy of the trajectories;
- Under these definitions, I examine the fairness of two state-of-the-art privacy-preserving models that rely on GAN and representation learning to reduce the re-identification rate of users for data sharing;
- The results show that while both models guarantee group fairness in terms of demographic parity, they violate individual fairness criteria, indicating that users with highly similar trajectories receive disparate privacy gain;
- I conclude that the tension between the re-identification task and individual fairness needs to be considered for future spatial-temporal data analysis and modelling to achieve a privacy-preserving fairness-aware setting.

[4] https://github.com/YutingZhan/Mo-PAE

1.4 Publications

This research accomplished from 2018 to 2022 led to 5 published, 1 under-review, and 1 in-preparation manuscript as the first author. The research outcomes have been also presented at 3 international and national conferences.

1. Yuting Zhan, Hamed Haddadi and Afra Mashhadi. Privacy or fairness? characterizing spatial-temporal data sharing techniques. *In submission*, 2022.
2. Yuting Zhan and Hamed Haddadi and Afra Mashhadi. Privacy-aware adversarial network in human mobility prediction. *The 23rd Privacy Enhancing Technologies Symposium (PETS)*, 2023.
3. Yuting Zhan and Hamed Haddadi and Afra Mashhadi. Privacy-aware human mobility prediction via adversarial networks. *The 4th IFAC Workshop on Cyber-Physical and Human Systems, (CPHS)*, 2022.
4. Afra Mashhadi, Ali Tabaraei, Yuting Zhan, and Reza M. Parizi. An auditing framework for analyzing fairness of spatial-temporal federated learning applications. *2022 IEEE World AI IoT Congress (AIIoT)*, 2022.
5. Senyou An, Yuting Zhan, Hassan Mahanid, Vahid Niasar. Kinetics of wettability alteration and droplet detachment from a solid surface by low-salinity: a lattice-Boltzmann method. *FUEL*, 2022
6. Yuting Zhan and Hamed Haddadi. MoSen: Activity modelling in multiple-occupancy smart homes. *19th IEEE International Conference on Pervasive Computing and Communications (PerCom WiP)*, 2021. Link.
7. Senyou An, Yuting Zhan, Jun Yao, Huidan Whitney Yu, and Vahid Niasar. A greyscale volumetric lattice boltzmann method for upscaling pore-scale two-phase flow. *Advances in Water Resources (AWR)*, 2020. Link.
8. Yuting Zhan and Hamed Haddadi. Towards automating smart homes: contextual and temporal dynamics of activity prediction. *In Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers (UbiComp/ISWC '19 Poster)*, 2019. Link.
9. Yuting Zhan and Hamed Haddadi. Activity prediction for improving well-being of both the elderly and caregivers. *The Second International Workshop on Computing for Well-being (WellComp, UbiComp/ISWC '19 Adjunct)*, 2019. Link.

Chapter 2

Activity Prediction in Mapping Contextual-Temporal Dynamics

Human activity recognition (HAR) technology is trendy in emerging domains (*e.g.*, smart home and healthcare) due to the increasing availability of sensors, accelerometers, images and videos [55]. It analyzes data acquired from these sensing devices and empowers the smart home to perceive the ambient environment [56]. Efficient activity prediction (*i.e.*, next activity forecasting), based on activity recognition, can enable the smart home to provide timely, personalized services. However, predicting the next activity and its specific occurrence period are challenging due to the complexity of modelling human behaviour. This chapter leverages sensor-based human activity datasets and aims to understand whether the temporal information integrated into the deep learning networks can improve the prediction performance or not. I develop and implement two LSTM-based activity predictors, both with *deep contextualized word representation* on sensor labels, one with temporal information and one without. The results highlight that if utilizing temporal information appropriately, the model with timestamp can outperform the model without. Therefore, comprehending contextual-temporal dynamics is highly important when modelling human activity prediction.

2.1 Introduction

As one of the prominent applications of HAR, the context-aware smart home is expected to improve the ubiquitous interaction between the residents and their intelligent environment. This ubiquitous interaction contributes to enhancing the residents' quality of life. Smart homes empowered by the advanced indoor monitoring and tracking systems, in this ubiquitous interaction, have the capability to perceive and cognize the ambient environment, where activity recognition plays an important role. Leveraging activity recognition, human behaviours can be recorded, modelled, and further analyzed. One promising application of smart homes is the long-term healthcare of the elderly group. Continuous daily monitoring not only can occasionally liberate caregivers [57] but also can clinicians use the data to prevent the degradation of an elder's health status at an early stage. At the same time, intelligent assistive technologies

contributed to a healthcare-based smart environment can mitigate the socioeconomic burden of the elderly and their families [58].

However, current research on activity recognition overlooks the interactions between humans and the environment, especially for cognitively or functionally impaired persons [59]. One promising bridge of the gap is to provide user-friendly, ubiquitous, and proactive services to particular groups that are being taken care of. With unobtrusive sensing technologies, activity recognition with predictive capability can build a more proactive ecosystem. Efficient activity prediction based on recognition labels can consolidate the expected ubiquitous interaction. Consider long-term healthcare as an example; successfully predicting the elder's intention or next activity can call caregivers' attention to helping them when needed, then relieving the caregiving burden and improving caregiving efficiency. It can also enhance the ecosystem response in a more proactive and user-friendly way.

Prediction of human activity is challenging because of the complexity of modelling human behaviours. Though human behaviours and activities are hard to model, the time series of human activity sequences are periodic, repetitive, and interdependent as human beings are a creature of habit [60]. More interestingly, in [61], the authors create a deep learning architecture to model human indoor activity and claim that none of the proposed options to take into account the timestamps improved the prediction performance. This phenomenon emphasises the importance of the study on the timestamps' effect on prediction performance. To this end, I train a persuasive predictor by answering the question: given the user's indoor activity history, which is a sequence of time-series sensor data, how to integrate the temporal information into a deep learning model (*i.e.*, LSTM-based) to achieve a better prediction performance? I conduct a series of experiments and leverage activity-level experiments to evaluate the performance of predictive models with integrated temporal information.

This chapter [62] highlights that a deep learning network with an integrated timestamp can have better prediction performance, which is important for further human behaviour modelling and prediction. I conclude how the contextual-temporal dynamics will exert influence on the final predictive model performance. The result demonstrates the improvement of the prediction accuracy for the next activity and time.

2.2 Related Work

2.2.1 Perception of Human Behavior

The research of machine perception motion conducted by Bobick [63] takes both time and context into consideration when recognizing a video sequence and breaks human behaviour into a tripartite hierarchy: *movement, activity, and action*. *Movement* refers to a motion of

which execution is consistent and can be expressed as a pixel-based description characterized by a defined space-time trajectory. For instance, consider the baseball game, *swinging the bat* is a typical movement, as one will see a slight variation in the motion from the current pixel to the next pixel. *Activity*, like *pitching a baseball*, contains more steps than a movement, composed of a series of movements. One of the most popular activity attracts researchers is gait recognition, consisting of a sequence of movements to configure different walking types. *Action*, which is at the boundary between perception and cognition, needs a full understanding of the context. For example, in the baseball game, *tagging out the runner* happens when a fielder with the ball causes his glove to come in contact with a base-runner who is not touching a base at the time. Recognizing an *action* requests the recognizer to have rich knowledge of the domain and be able to capture a semantic description of the motions. In summary, *movement* is the most primitive, requiring no contextual or sequence knowledge to be recognized; *activity* refers to sequences of movements or states and it only requires the knowledge of the sequence's statistics; *action* are large-scale events and typically include the interaction with environment [63].

In this thesis, the *activity-level* human behaviour is in the research scope, which also follows the most generalized definition of human activity. Advanced ubiquitous sensing technologies enable different kinds of sensors to gather human activity data in their daily life. These sensing technologies include but are not limited to wireless sensing, wearable sensors, and ambient environmental sensors. Those sensors can record a person's daily life as a time series of sensor data. Activity recognition aims to understand the metadata that emanated from multifarious sensors and transform them into a sequence of physical activities. Activity recognition, in a way, provides the researchers with a feasible approach to investigating and modelling human behaviour. With the rise of machine learning algorithms in the past decades, activity recognition is a well-research area with persuasive recognition precision.

In [64], the authors concluded the main activities considered in smart home scenarios and divided them into three categories (*i.e.*, basic ADLs, instrumented ADLs, and ambulatory activities) based on the seniors' independent living. Basic ADLs refer to the necessary self-care activities, such as bathing, brushing teeth, dressing, using the toilet, eating and drinking, and sleeping. Instrumented ADLs are those that are not strictly necessary but needed when an individual lives independently, such as preparing meals and drinks, resting, housekeeping, using a telephone, and taking medicine appropriately and promptly. Ambulatory activities are related to either specific motions or postures of the person, such as walking (up and down stairs), doing exercise (running, cycling, etc.), transitional activities (sit-to-stand, sit-to-lie, etc.), and stationary activities (sit on the sofa, lie in bed, etc.).

In [65], the authors addressed the definition of the time intervals in artificial intelligence, and this *Allen relations* [65] are commonly used to describe temporal links between activities. It used constraint propagation techniques to describe relationships between temporal intervals hierarchically. The author concluded thirteen temporal relationships, as shown in Figure 2.1.

Conceptualizing temporal relationships among different activities is crucial when accurately modelling human behaviours. Figure 2.2 represents the common temporal relationship between activities.

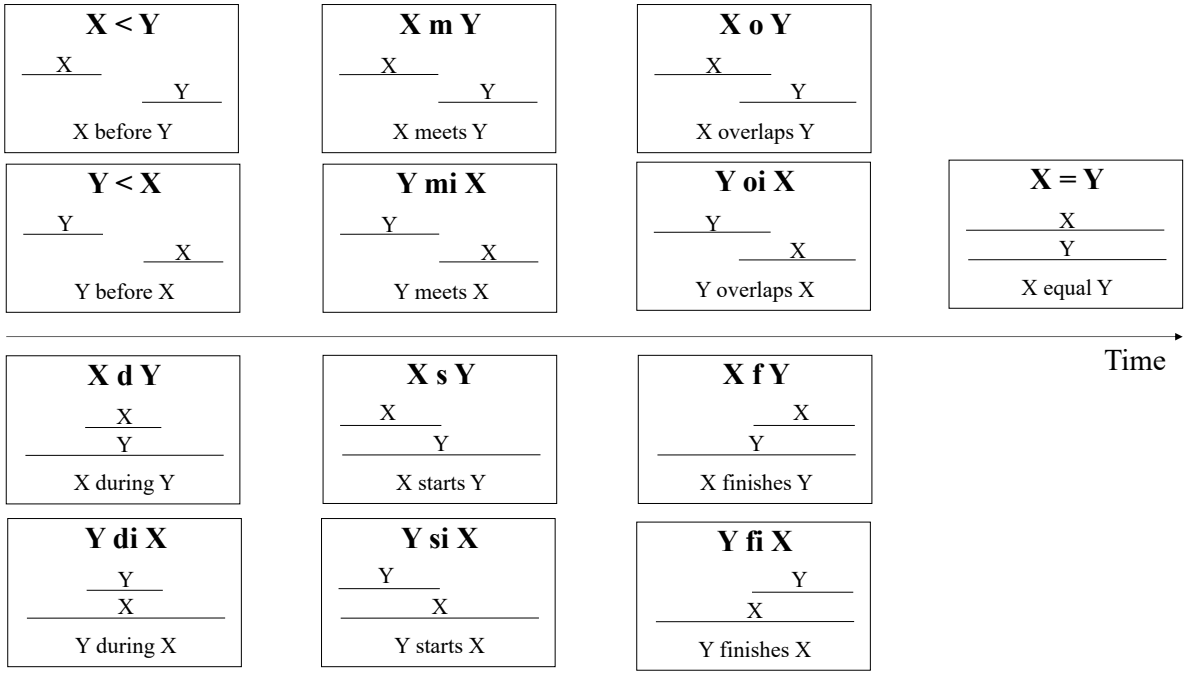
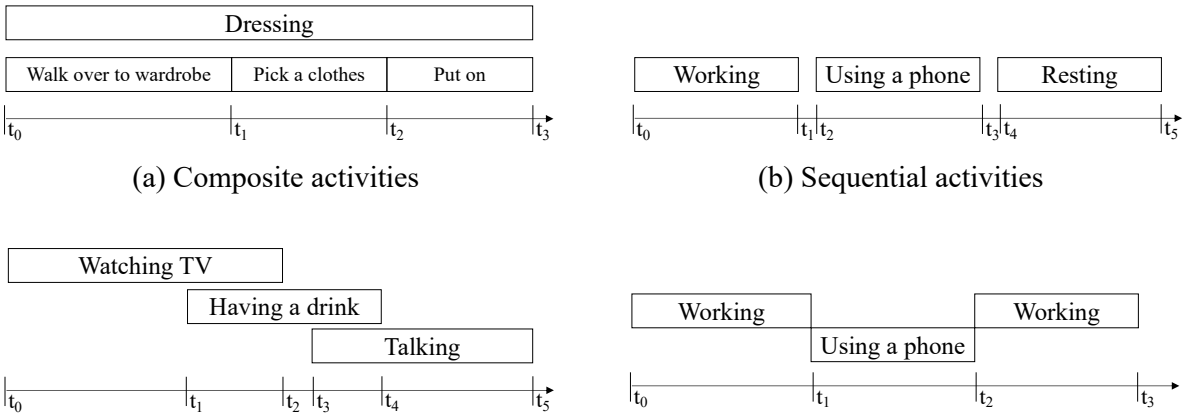


Figure 2.1: The thirteen possible temporal relationships concluded by Allen [65].



(a) Composite activities

(b) Sequential activities

(c) Concurrent activities

(d) Interleaved activities

Figure 2.2: The common temporal relationships between activities: (a) composite activities; (b) sequential activities; (c) concurrent activities; (d) interleaved activities.

2.2.2 Neural Network

Recurrent neural networks (RNN) is specialized for processing a temporal sequence of data $x(t) = x(1), \ldots, x(\tau)$ (*t is timestep*, $t = 1 \ldots \tau$), which allows it to exhibit temporal dynamic

behaviours, as shown in Figure 2.3. It is applicable to utilize previous outputs as inputs while having hidden states. The mathematical equation of RNN is as follows:

$$h^{<t>} = \phi_1(U_{xh}x^{<t>} + W_{hh}h^{t-1}) \tag{2.1}$$

For each time step, $h^{<t>}$ is hidden state, $h^{<t-1>}$ is the hidden state at $t-1$. $x^{<t>}$ is the input at t. U_{xh} is the input-to-hidden weight matrix for $x^{<t>}$ to $h^{<t>}$. W_{hh} is the hidden-to-hidden weight matrix for $h^{<t-1>}$ to $h^{<t>}$. V_{ho} is the hidden-to-output weight matrix for h^t to $o^{<t>}$. ϕ_1 and ϕ_2 are activation functions.

$$o^{<t>} = \phi_2(V_{ho}h^{<t>} + b_o) \tag{2.2}$$

The loss function is defined as follows:

$$\mathcal{L}(\hat{y}, y) = \sum_{t=1}^{T} \mathcal{L}(\hat{y}^{<t>}, y^{<t>}) \tag{2.3}$$

Back-propagation is done at each point in time:

$$\frac{\partial \mathcal{L}^{<t>}}{\partial W} = \sum_{t=1}^{T} \frac{\partial \mathcal{L}^{<t>}}{\partial W}|_{<t>} \tag{2.4}$$

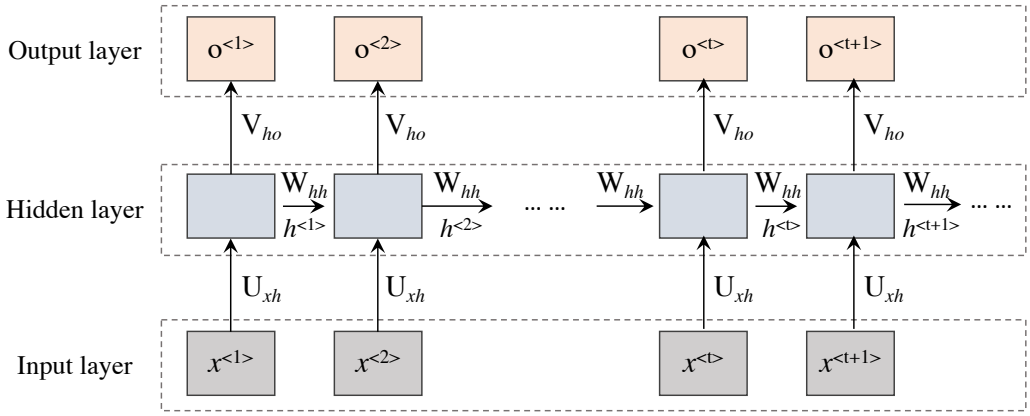


Figure 2.3: The basic architecture of standard RNN. The rectangles represent network layers, and the solid arrows represent weighted connections (*i.e.*, *V, W, U*). The entire network is designed with loops, which allow information from the previous time step to be passed as input to the current time step. In this manner, RNN processes sequences of inputs without losing track.

Long Short-Term Memory units, or LSTMs, proposed by Hochreiter and Schmidhuber in 1997 [66], is a prominent variant of RNN, shown as the flowchart in Figure 2.4. LSTM has been shown to exhibit brilliant performance in modelling entire sequences of data, especially

for linking remote causes and effects in time-series data. LSTM can efficiently handle the difficulty of learning long-term dependencies with gradient descent in a standard RNN. The capability of LSTM on remote dependencies empowers it to be one of the dominant networks in time-series-data analysis and sequence generation.

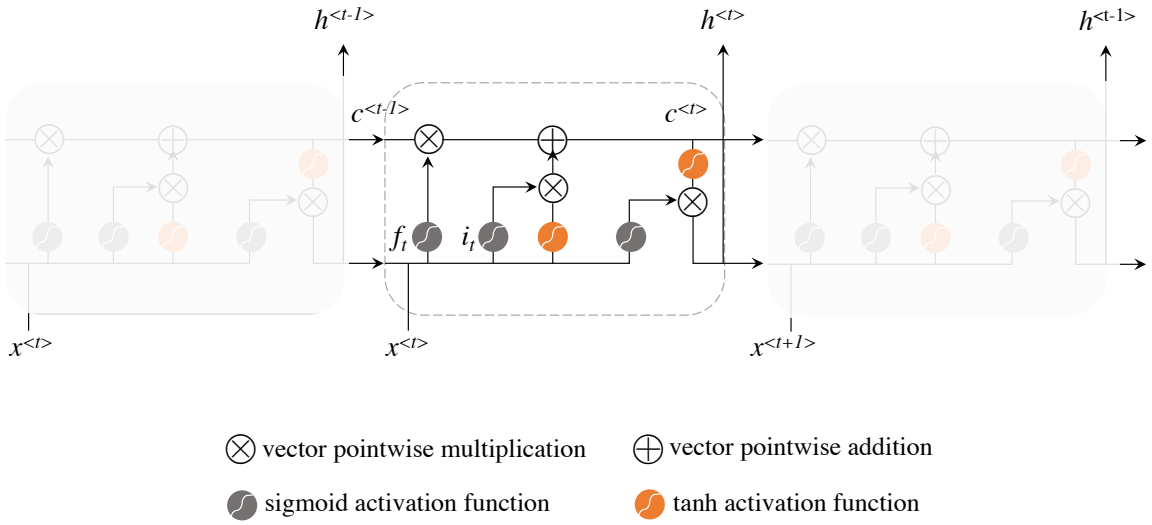


Figure 2.4: The repeating cell in a standard LSTM. The grey rectangle represents a chunk of neural networks with loops, which allows information to persist.

A common LSTM unit contains a cell $\tilde{c}_t$, an input gate i_t, an output fate o_t, and a forget gate f_t. The cell remembers values over arbitrary internals. The forget gate chooses the information from the previous timestep to be remained it to be forgotten. The input gate learns new formations from the new input. The output fate passes updated information to the next time step. The three gates simultaneously regulate the information to forward to the next node. Formally, the LSTM can be expressed as follows:

$$\begin{cases} \star = element-wise\ multiplication,\ + = element-wise\ addition \\ forget\ gate \text{ -> } f_t = \sigma(x^{<t>} \star U^f_{xh} + h^{<t-1>} \star W^f_{xh}) \\ input\ gate \text{ -> } i_t = \sigma(x^{<t>} \star U^i_{xh} + h^{<t-1>} \star W^i_{xh}) \\ output\ gate \text{ -> } o_t = \sigma(x^{<t>} \star U^o_{xh} + h^{<t-1>} \star W^o_{xh}) \\ cell\ output \text{ -> } \tilde{c}_t = \tanh(x^{<t>} \star U^g_{xh} + h^{<t-1>} \star W^g_{xh}) \end{cases} \tag{2.5}$$

$$\begin{cases} c^{<t>} = \sigma(f_t \star c^{<t-1>} + i_t \star \tilde{c}_t) \\ h^{<t>} = \tanh(c^{<t>} \star o_t) \end{cases} \tag{2.6}$$

2.2.3 Representation Techniques

In sequential data processing and learning, especially NLP, two of the most popular concept for vector representation techniques are one-hot embedding and word embedding.

One-hot embedding

In machine learning, a one-hot is a group of bits among which only one bit is *hot* (1) at any time and all the others *cold* (0) [67]. As a crucial part of feature learning, one-hot embedding converts categorical data variables and produces a binary vector with the same length of the number of categories [68]. For example, say convert colours *red, green, and blue* into binary vectors by using one-hot embedding, the numeric values are first assigned to each colour category (*i.e.*, red -> 1, green -> 2, blue -> 3), and then each integer value is converting to a binary vector with the index of the integer is marked with a 1 but others with 0 (*i.e.*, red -> [100], green -> [010], blue -> [001]). With one-hot embedding, each bit of state contributes to the representative vector. It is an easy and effective implementation in data transformation, especially when variables have no relation to each other. However, the biggest concern faced is the dummy variable trap problem [69], where the variables are highly correlated.

Word embedding

Word embedding techniques are developed to learn vector space representations of words, where words with similar meanings have a similar representation. Word2Vec [70] is one of the most popular vector-space word representations developed by Mikolov *et al.* at Google in 2013. Word2Vec is examined to better capture syntactic and semantic regularities in NLP, allowing vector-oriented reasoning based on the relation-specific offsets between words. GloVe is an extension to the Word2Vec, which developed by Pennington *et al.* in 2014 [71]. It simultaneously captures the global corpus statistics of matrix factorization techniques and local context-based learning in Word2Vec.

2.3 Proposed Architecture

Unlike some previous healthcare platforms driven by rule-based reminders, the proposed architecture in this chapter is sensor data-driven, autonomous and proactive. The overview of the proposed prediction architecture is shown in Figure 2.5. Data is emanated from the ubiquitous sensors and is further labelled as the sequences of activities. These labels are then represented as ELMo vectors [72] and fed into the LSTM model to train the activity predictor. At the same time, each activity class has its LSTM-based time predictor. When the prediction of

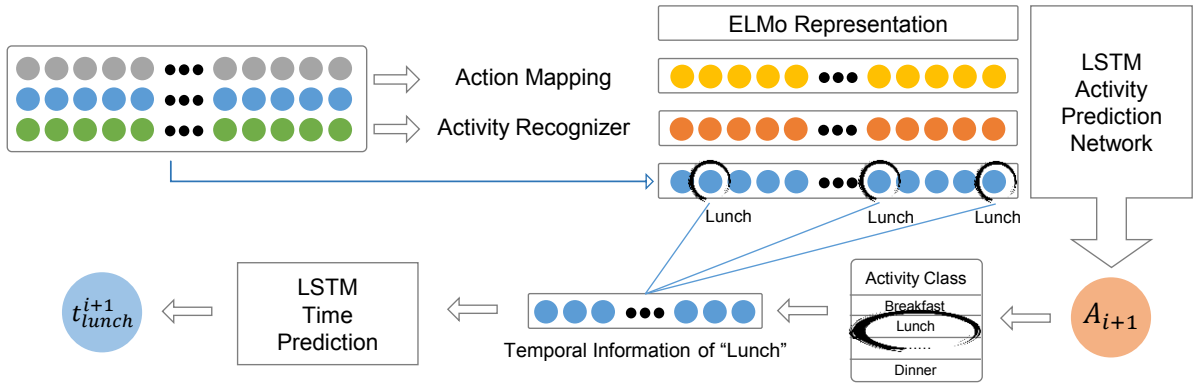


Figure 2.5: Overview of the proposed prediction architecture.

the next activity is generated, the corresponding time predictor will be triggered and predict the specific occurrence period, as shown in Figure 2.5. With this valuable information, caregivers can estimate the right time to provide appropriate help to the elderly.

2.3.1 Dataset Description

The proposed models use sensor data instead of cutting-edge wireless signal data, as existing wireless signal-based activity recognition methods have lower accuracy and can only recognize one or several activities. However, the quality of prediction depends on the diversity of the recognized activities. Three widely-used datasets of activity recognition literature are compared:

- CASAS datasets [42]: it is a sensor-based human activity dataset that records and collects human activity for 20 participants in the smart home using an infrared motion sensor, light sensor, door sensor, and temperature sensors. These participants are aged 21 to 62 years and have various backgrounds and technological familiarity. The activities recorded include bed-toilet transition, cooking, eating, entering the home, leaving home, personal hygiene, phone, relaxation, sleep, and work.
- Tapia dataset [73]: it collects data for 14 days in two single-occupancy apartments, one is occupied by a 30-year-old woman and another is an 80-year-old woman. The first apartment was installed unattended with 77 state-change sensors and 84 in the second apartment. The activities recorded include preparing lunch, toileting, preparing breakfast, bathing, dressing, grooming, preparing a beverage, doing laundry, and so on.
- Kasteren dataset [43]: it consists of 28 days of sensor data with annotations of a 26-year-old man, who lives alone in a three-room apartment where 14 state-change sensors were installed. Sensors are placed unattended on doors, cupboards, refrigerators, and a toilet

flushes sensor. It has 2120 sensor events and 245 activity instances. The activities recorded include idle, leaving, toileting, showering, sleeping, breakfast, dinner, and drinking.

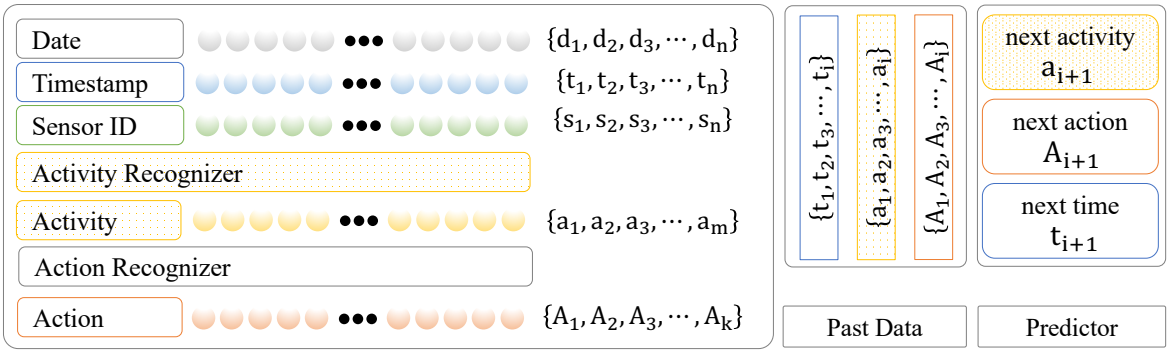


Figure 2.6: Dataset description. Each line in the dataset at least contains *date, timestamp and sensor ID*.

All chosen datasets to validate my assumptions are single-person apartment monitoring data that emanated from multiple sensors. Each line of data should at least contain *date, timestamp, sensor ID*, and *activity label*, as shown in Figure 2.6. Formally, one timestamp t_i is recorded as a result of one sensor trigger by the resident, and one sensor trigger is mapped as one activity a_i. The activity recognizer will generate the sequence of activities by analyzing the sensor data.

The prediction task can be formulated as a variant of the sequence generation task: given a sequence of resident's past activities $\{a_1, a_2, \ldots, a_i\}$ or past actions $\{A_1, A_2, \ldots, A_i\}$ in concerted with a sequence of timestamps $\{t_1, t_2, \ldots, t_i\}$ until time t_i, to predict the next activity a_{i+1} or next action A_{i+1} and their occurring time t_{i+1}.

2.3.2 ELMo Representation

The prominent word representation in the deep learning area is word embedding, and one of the most frequently-used word embeddings is *Word2Vec* embedding. However, the Word2Vec embedding and other similar word embeddings are now losing their dominance in *Natural Language Processing* (NLP) area due to the rise in availability of novel pre-trained language models. ELMo [72], the abbreviation of *Embedding from Language Models*, is a *deep contextualized word representation* which has shown the potential to improve the state-of-the-art performance of existing NLP tasks. Unlike other word vectors, the ELMo vector can be learned by a deep bidirectional language model pre-trained on a large text corpus [72]. Hence, ELMo representation can better model both semantic complexity and context-based polysemy. In the proposed model, I use ELMo representation to define each activity's embedding matrix, a 128-dimension vector, in the embedding layer of the LSTM model.

2.3.3 Long Short-Term Memory Network

In this work, the LSTM network is well-suited to the sensor data, which is sparse, time-varying, and interdependent. In order to verify my hypothesis that the LSTM models that take into account the temporal information of sensor data will have better prediction performance than the ones without this information, I compare two LSTM models in a row. The first model has only one LSTM layer for activity embedding, while the other has an extra LSTM layer to integrate timestamps. These two models are referred to *One-LSTM* and *Temporal-LSTM*, respectively.

2.4 Evaluation and Results

Three different experiments are set up to evaluate the performance of the proposed architectures with integrated temporal information. These architectures' performances are compared with a baseline, which used *Word2Vec* embedding for action representation and an LSTM-based network for human behaviour modelling [61]. Prediction accuracy is one of the most important features for assessing the performance of the predictive model, thereby I use the prediction accuracy as the evaluation metric, from one- to five-attempt, which would keep horizontal comparison with the baseline.

2.4.1 Varying Context Size

Different lengths of the context size exert an effect on the prediction performance of a recurrent model [74]. By changing the length of the input activity (context size) from 1 to 200, I observed that the length of input activity has a high impact on the accuracy of two proposed LSTM models, as shown in Figure 2.7. Note that the optimal context size of the first model is situated at the interval $[40, 90]$, while the second model is at the interval $[70, 120]$.

Compared with the One-LSTM model, the Temporal-LSTM model performs better from all 1-attempt to 5-attempt predictions, especially for 1-attempt and 5-attempt, where the accuracy is higher than 0.5 and 0.9, respectively. The comparison between these two models also illustrates that even with the same dataset, different architectures would have different optimal values. When considering the temporal information, sufficient context improves performance while insufficient context decreases performance.

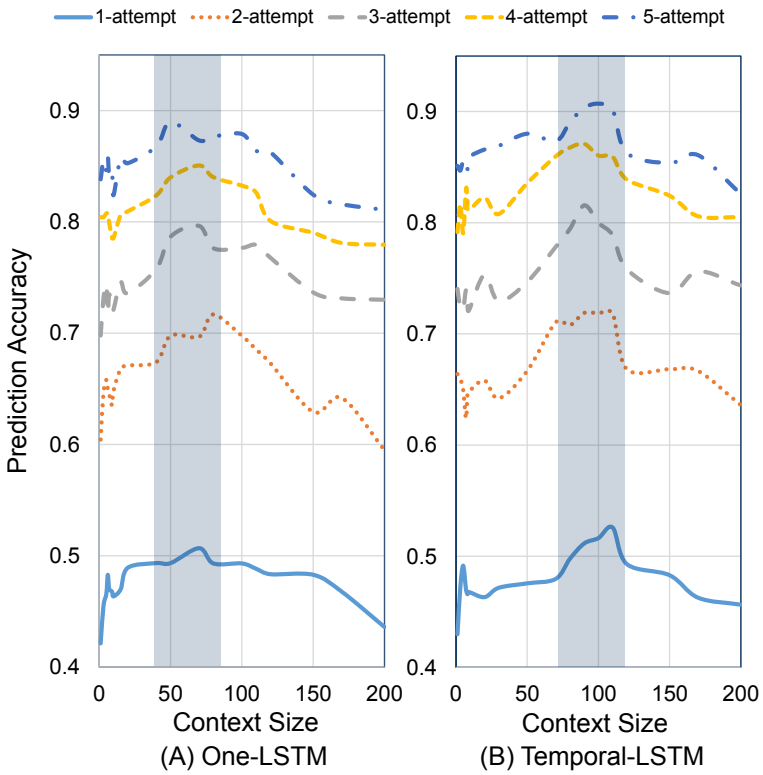


Figure 2.7: Prediction accuracy changes with the length of input activity (context size) in two LSTM models. Grey bins illustrate the optimal area of each model.

2.4.2 ELMo Embedding or Word2Vec Embedding

In the baseline experiment, Word2Vec embedding representation has been used in the embedding layer of LSTM to provide better performance than one-hot vectors [61]. In the proposed models, ELMo representation defines each activity's embedding matrix. The pre-trained language model generates a 128-dimension vector for each activity. Then these vectors are fed into the embedding layer of LSTM models.

In this contrast experiment, the ELMo embedding-based models are compared with the Word2Vec embedding-based models, as shown in Figure 2.8. The results illustrate that the ELMo representation can improve the prediction accuracy, where the increment is 5.93% averagely for the One-LSTM (1LSTM), and 8.57% for the Temporal-LSTM (2LSTM). With ELMo representation, the integration of time information (2LSTM) can also improve the performance, which demonstrates that ELMo representation has more potential to illustrate the contextual-temporal dynamics in activity prediction.

2.4.3 One-LSTM or Temporal-LSTM

In the baseline study [61], Almeida and Azkune evaluated three different fusion strategies on the LSTM network and found that all fusion strategies considering timestamps $\{t_1, t_2, \ldots, t_i\}$ were

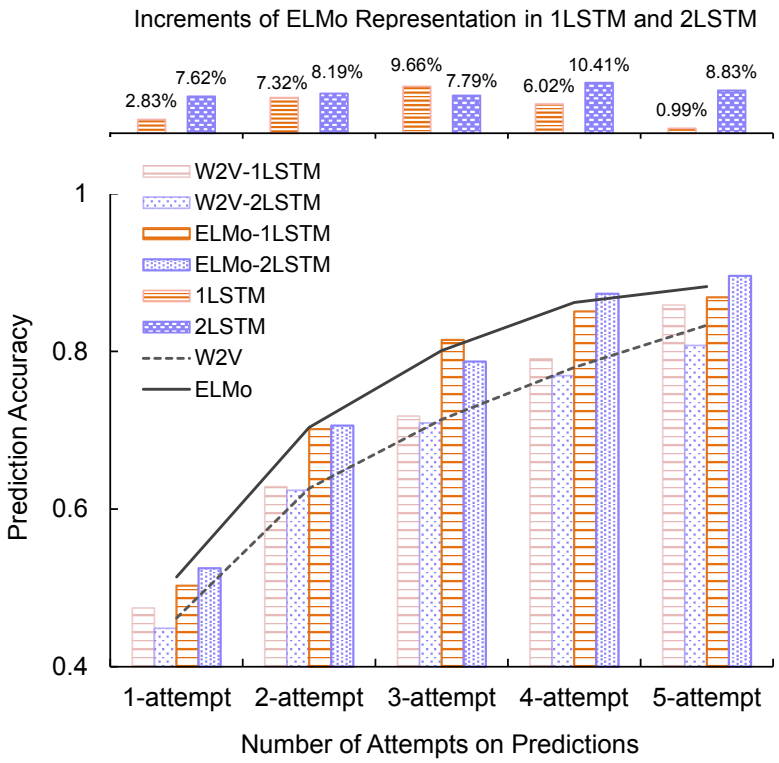


Figure 2.8: Improvement of ELMo representation when compared to Word2Vec embedding. The 2LSTM with ELMo representation outperforms the 1LSTM.

detrimental to the results. Their data is shown in the *w2v* line in Table 2.1, where Temporal-LSTM (2LSTM) has worse performance.

On the contrary, in the proposed LSTM models, the results in Table 2.1 admit that the time layer can improve the accuracy of prediction, especially for the increments at 1-attempt (top1) and 5-attempt (top5) situations. In general, the Temporal-LSTM (2LSTM) has better prediction accuracy than One-LSTM (1LSTM). I demonstrate that if temporal information can be used appropriately, the model can have better prediction results, especially for a small dataset.

2.5 Use Case

The topic of the ageing population has emerged as one of the most formidable socio-economic challenges faced by both developed and developing countries. The enormous elderly population increases the economic burden on the sophisticated well-being system, posing a critical challenge to long-term healthcare. In Europe, the number of people aged 65 and over is expected to grow to 28% of the population in 2060 [75]. The demographics of the elderly group afflicted by Alzheimer's disease and related dementia are proportional to the growing ageing population trend. By 2030, $2 trillion will be spent each year globally for the well-being of the dementia group [76].

		top1	top2	top3	top4	top5
w2v	1LSTM	0.4744	0.6282	0.7179	0.7905	0.8589
	2LSTM	0.4487	0.6239	0.7094	0.7692	0.8076
50	1LSTM	0.4844	0.6933	0.7822	0.84	0.8577
	2LSTM	**0.5112**	0.6712	0.7734	**0.84**	**0.8712**
70	1LSTM	0.5027	0.7014	0.8145	0.8507	0.8688
	2LSTM	**0.5249**	0.6787	0.7828	**0.8733**	**0.8869**

Table 2.1: Prediction accuracy of two ELMo-embedded LSTM models when context size is 50 and 70, respectively, are compared with the baseline (w2v). Note that in the baseline (w2v) experiment, the temporal information is detrimental to the final prediction, where 2LSTM has worse performance. For the ELMo-embedded LSTM models, the Temporal-LSTM (2LSTM) outperforms the One-LSTM (1LSTM), which means the contextual-temporal dynamics are well mapping when temporal information can be appropriately used in the predictive model.

Integrating assistive technologies into the smart home paradigm [57] is regarded as a potential trend for setting up care for different elderly groups, especially for candidates with dementia and other mild cognitive or functionally impaired elders. This approach can reduce time and cost expenditures of long-term healthcare while improving the quality of life for the target population and their caregivers. However, in current research, caregiver distress correlated with multifarious geriatric symptoms is overlooked, where there is a significant gap in relieving the psychological burden for caregivers [57]. For instance, the dementia group has a series of symptoms, including but not limited to agitation, irritability, depression, delusion, etc. Those symptoms torture and distress their formal or informal caregivers [57]. Caregiving with depression and frustration is detrimental to the wellness of both parties, which might escalate the tension and intensify potential conflicts between them [76].

One promising way to mitigate these negative effects is to implement efficient non-verbal communication, or collaboration, between the elderly group and their caregivers. Research by Koumakis *et al.* has emphasized the demand for cultivating an appropriate collaboration between those suffering from mild dementia and their caregivers [57].

The ability to model the elderly behaviours and predict their next activity is extremely valuable in cultivating this particular collaboration and smoothing their communication with each other. However, modelling human behaviours and predicting human next activity are highly challenging due to the complexity of human behaviours. Though human behaviours and activities are hard to model, they can be represented by a time series of periodic, repetitive, and interdependent sequence data, as humans are creatures of habit. These properties allow the sequence of human activity to be predictable. Especially for the elderly and the candidates for dementia, their lives are much more monotonous and repetitive.

In my proposed framework, by leveraging the indoor activity recognizer [74], an elder's activity can be recognized, recorded, and further analyzed. The results of such activity recog-

nition are then fed into the activity predictor, which can predict the next activity or intention of the group that is taken care of. The persuasive prediction can relieve the tension resulting in discrete wills between two groups. For long-term healthcare, successfully predicting the elder's next activity or intention can call caregivers' attention to helping them when needed, which can relieve the caregiving burden and improve efficiency and the quality of life for both groups.

Undoubtedly, activity prediction plays a vital role in this communication between the elderly and their caregivers. Hence, this chapter trains a more persuasive activity predictor by using the *deep contextualized word representation* (ELMo) [72] and integrating the temporal information of the data into the proposed LSTM framework. The results highlight that an appropriate utility of the temporal information can have better prediction accuracy. While better predictions in the proposed framework allow caregivers more personal time and relieve their psychological burden. With persuasive predictions, both groups' well-being is considered in their daily lives.

2.6 Discussions

The valuable information provided by activity prediction can build an efficient collaboration between the elderly and caregivers, a cornerstone of a better quality of life for both groups. In addition to effective communication between them, in long-term healthcare, successfully predicting an elder's intention or next activity can provide a series of activity-aware services, including penalizing the intelligent environment, prompting-based intervention, anomaly detection, etc. There is still a large potential improvement in prediction accuracy. A genuinely persuasive prediction can undoubtedly improve the elder's quality of life and well-being, so as the caregivers.

In real-time prediction settings, a well-trained activities recognizer recognizes the activities as inputs for the predictor. At the same time, the recognizer would also provide a baseline for the predictor to verify each prediction. However, there are three challenges: firstly, the current indoor activity recognizer utilized in the predictor depends mainly on ambient sensors, which cannot recognize micro-actions and realize continuous tracking; secondly, activity predictor based on the deep neural network still has low accuracy and low time sensitivity unexpectedly; thirdly, the multi-person scenario is always challenging and need feasible solutions.

Overall, the result of this chapter has shown that if temporal information can be used appropriately, the model can have better prediction accuracy, especially for a small dataset. This is a favourable outcome as if less data is required, the smaller the invasion of user privacy. However, at the same time, due to the scarcity of the big labelled sensor-based human activity datasets, the performance of the proposed model with more extensive datasets is limited and needs more investigation in the future.

Chapter 3

MoSen: Activity Modelling in Multiple-Occupancy Smart Homes

Smart home solutions increasingly rely on various sensors for behavioural analytics and activity recognition to provide context-aware applications and personalized care. Optimizing the sensor network is one of the most critical approaches to ensuring classification accuracy and system efficiency. However, the trade-off between cost and performance is often a challenge in real deployments, particularly for multiple-occupancy smart homes or care homes. In this chapter, using actual indoor activity and mobility traces, floor plans, and synthetic multi-occupancy behaviour models, I evaluate several multi-occupancy household scenarios with 2-5 residents. I explore and quantify the trade-offs between the cost of sensor deployments and expected labelling accuracy in different scenarios. The evaluation across different scenarios shows that the performance of the desired context-aware task is affected by different localization resolutions, the number of residents, the number of sensors, and varying sensor deployments. To aid in accelerating the adoption of practical sensor-based activity recognition technology, I design *MoSen* [77], a framework to simulate the interaction dynamics between sensor-based environments and multiple residents. By evaluating the factors that affect the performance of the desired sensor network, I provide a sensor selection strategy and design metrics for sensor layout in natural environments. Using the selection strategy in a 5-person scenario as the case study, the performance demonstrates that *MoSen* can significantly improve overall system performance without increasing the deployment costs.

3.1 Introduction

HAR is a central task of many intelligent systems such as smart homes [33], long-term healthcare [34], personal robotics [35], assisted living [36], and human-computer interaction [37]. Current works illustrate that human activity can be recognized using two main approaches: vision-based [78] and sensor-based [79]. Vision-based activity recognition utilizes cameras to capture or record individuals' motions [78], while sensor-based systems leverage wearable or ambient sensors to understand the movements of the subjects and the interactions between peo-

ple and the environment [80]. While vision-based approaches are often privacy-invasive, the sensor-based systems, which are highlighted in this thesis, are often more privacy-friendly and take advantage of their pervasiveness [48]. Currently, more and more sensors are getting embedded into the ambient environment, wearable electrical products, and intelligent appliances to aid with sensor-based activity recognition systems. The multi-modal sensor data enables the system to receive rich context information and to have the capability to process personalized behavioural analytics and provide context-aware applications [33].

While multitudes of sensors extend the variety of information that can be received, the heterogeneity of the devices [38] and the increasing number of residents [39, 40] complicate the data collection system in real settings. Even for *single-occupancy scenarios*, where only a single individual is in a single space, the diversity of sensor settings or floorplans could affect the overall performance of sensor networks. Importantly, sensor networks designed for single-occupancy houses are never deployed in identical settings, and sensor selection in each system is diverse, varying from commercial products to self-built devices [41–44]. The price, stability, precision and coverage range of different sensors affect the implementation and performance of sensor-based systems [44]. It is not easy to find a uniform sensor integration system flexible to distinct homes, especially when the homes might have more than one resident, referring to the *multi-occupancy scenarios* in this chapter. Prior research has already specified the significance of multi-occupancy scenarios, but the complexity of the ongoing sensor networks and unknown uncertainties impede the real implementation of the sensor network and further analysis [39, 45–48]. Hence, when designing a specific sensor network for the target home, especially in multi-occupancy scenarios, an efficient emulation that considers the real floorplan, the number of residents, sensor density, and device resolutions is beneficial.

In multi-occupancy smart homes, data associating problem (*i.e.*, identification annotation) is one of the central problems for the sensor-based activity recognition technology [39, 81–83]. It refers to labelling the time-series sensor events by mapping them with the resident causing its generation. A high-accuracy data-associating model is a prerequisite when leveraging mature HAR techniques of single-occupancy households into multi-occupancy ones. Current identification annotation solutions mainly rely on self-reporting [80] and camera-recording [45], where the former is biased, and the latter would invigilate privacy. The capability for automatically labelling the identification, hence, is significant for a practical smart home system. Researchers tend to use wearable sensors to reduce the complexity of the problem because wearable sensors can be utilized as the identification tag of different residents [47]. Another promising way is to leverage the real-time locating system (RTLS) to locate different residents when they are interacting with the environment. RTLS is a rising technology for detecting both the location and identification of the target, where the target could refer to an item, a person, or a vehicle [84, 85].

In this chapter, based on the RTLS-based approach, which is utilized to annotate sensor

events with identifications, different localization resolutions are emulated in the proposed system. To be specific, taking the automatic annotation problem as the desired context-aware task, I explore the interaction dynamics between the sensor-based environment and multiple residents by proposing the *MoSen* emulation environment. *MoSen* is designed to evaluate the way in which different localization resolutions, number of residents, number of sensors, and varying sensor deployments affect the performance of the pre-designed sensor network before real deployment. In order to investigate the dynamics of annotation accuracy, MoSen takes the multi-occupancy behaviour model, floor plan, sensor layout, and localization resolution as input, and outputs a series of results of different combinations. With these results, practitioners or designers are able to get insights into sensor selection strategy with metric-based design suggestions for the pre-designed sensor layout.

To be specific, by using real behaviour models and synthetic data, I emulate multi-occupancy scenarios in households with 2 to 5 residents. Given the scarcity of multi-occupancy datasets and difficulty in realistic data collection with existing technologies, especially during the COVID-19 pandemic with social distancing, I generate synthetic multi-occupancy behaviour models by modelling real single-occupancy datasets collected in real homes. The quality of the multi-occupancy behaviour model is validated by comparing the performance between synthetic and real double-occupancy datasets.

The main objective of this chapter is to offer an effective evaluation structure and feasible sensor selection strategy for *different* smart homes. By comparing real and synthetic datasets, I discuss potential challenges when adopting sensor-based activity recognition in different multi-occupancy scenarios. The main contributions of the chapter are as follows:

- I propose *MoSen* [1] to investigate the interaction dynamics between a sensor-based environment and multiple residents;
- I provide an algorithm to generate synthetic multi-occupancy behaviour models and compare the performance with the real dataset;
- I explore how the labelling accuracy is affected by different localization resolutions, the residents' quantity, sensor density, and varying deployment in multi-occupancy scenarios;
- I design a sensor selection strategy to balance the trade-off between deployment costs and expected labelling accuracy in different homes, which accelerates the practical adoption of sensor-based activity recognition in reality.

The rest of this chapter is organized as follows. Section 3.2 presents the related work, Section 3.3 gives an overview of *MoSen* system, and Section 3.4 describes the design methodologies

[1] https://github.com/YutingZhan/MoSen

applied in the proposed system. In Section 3.5, I evaluate the effect of localization device resolutions, residents' quantity and sensor density, respectively. With the analytical result, I provide a case study in Section 3.6, then present discussions in Section 3.7, and the final conclusion in Section 3.8.

3.2 Related Work

3.2.1 Activity Recognition

Human indoor activities are complex, diverse, and stochastic, making them challenging to define and quantify. A variety of advanced ubiquitous sensing technologies (*e.g.*, wireless sensing [86], wearable sensors [33], or ambient sensors [79]) have been adopted to collect human indoor activity data [41, 42, 87, 88]. Human activity recognition is central to accelerating automation integration in smart environments [35]. Prior works have illustrated modelling human activity patterns is valuable for providing personalized services [89] or context-aware interactions with the resident [90, 91].

Currently, human activity can be recognized using two main approaches: vision-based [78] and sensor-based [79]. Vision-based activity recognition utilizes cameras to capture or record individuals' motions [78], while sensor-based systems leverage wearable or ambient sensors to understand the movements of the subjects and the interactions between people and the environment [80]. With the rapid development of computer vision techniques, HAR is mostly dominated by vision-based approaches, which are further subdivided into RGB-camera-based, depth-camera-based and point-cloud-based [92]. As one of the most common approaches, RGB-camera-based HAR, which comprises background subtraction, human/object detection, and human tracking [93], utilized still images or live videos to capture human actions. These techniques have been well developed in simple activity recognition [94], however, they are limited due to the complexity of view-invariance and occlusion [56]. Different to traditional RGB cameras, depth-camera-based HAR leverages deep information captured by depth sensors to better handle illumination and privacy [94–96], which has remarkable progress in human daily activities [97, 98] and fall detection [99] over the last decade. Point-cloud-based HAR leverages a 3D points cloud, which is perceived by depth or LiDAR sensors, to perceive the geometric information of scenes accurately while being robust to different lighting conditions [94, 100]. While the latter two vision-based approaches show promising performance in handling the complexity of lighting, occlusion, and subject angle, the equipment requirement and cost hinder their real adoption outside the laboratory [94]. Moreover, when it comes to multi-occupancy smart home scenarios, these limitations become more burdensome, and residents' privacy is at considerable risk.

While vision-based approaches are often privacy-invasive, the sensor-based systems, which are highlighted in this chapter, are often more privacy-friendly and take advantage of their pervasiveness [48]. Additionally, more and more sensors are getting embedded into the ambient environment, wearable electrical products, and intelligent appliances to aid with sensor-based activity recognition systems. The multi-modal sensor data enables the system to receive rich context information and to have the capability to process personalized behavioural analytics and provide context-aware applications [33]. In this chapter, I mainly discuss sensor-based activity recognition.

Multi-person Activity Datasets

The majority of research in human activity recognition has investigated the *single-occupancy scenario* [43, 83], where only one resident lives in a single space. However, the real environment is usually inhabited by more than one resident and even with pets, which is referred to as *multi-occupancy scenario* [41] in this thesis. Multi-person activity recognition has less investigation, as many practical challenges are yet to be overcome in the single-occupancy scenario [39]. Recent pilot deployments demonstrate the applicability and adaptability of multi-occupancy scenarios by using different machine learning algorithms [39, 45, 47]. There are two publicly and widely-used multi-person datasets in current literature, the *CASAS Datasets* [42] and the *ARAS Datasets* [41]. I compare the synthetic multi-person behaviour models with these two real datasets to validate the quality of the synthetic model.

3.2.2 Real-time Locating System

The real-time locating system (RTLS) is a rising technology for detecting both the location and identification of the target, where the target could refer to an item, a person, or a vehicle [84, 85]. Different positioning technologies have been investigated in the last several decades, and these technologies perform a similar task with varying accuracy. I conclude 12 leading indoor positioning technologies in Tables 3.1 and 3.2, comparing the *positioning accuracy, coverage range, cost, infrastructure complexity, network, localization method, and frequently-used convention measurement* of different technologies.

Applications for RTLS, also called location-based services (LBSs), have already been broadly adopted in a variety of indoor location-aware scenarios [123, 124], from mapping and navigation services [125, 126] to human-robotics interaction [84]. In transitioning from a single-occupancy scenario to a multi-occupancy environment, it becomes significantly important to track each resident [127]. In Tables 3.1 and 3.2, I also conclude how these indoor positioning technologies perform in the multi-occupancy environment, by listing their basic experimental setting and locating accuracy. By tracking residents respectively in an efficient and accurate

	Infrared (IR)	Ultrasound	Acoustic Signal	Visible Light (VLC)	UWB-based	RFID-based
Positioning Accuracy	0.57 - 2.3m [101]	10mm [102]	5.4cm [103] - meters [104]	1mm [105] - 45cm [106]	10cm [107] - 50cm [108]	15cm [109] - meters [110]
Coverage Range	Sub-room	Room	Room	Room	Room	Sub-room
Cost	Low	High	Medium	Low	High	Medium
Infrastructure Complexity	High	Medium	Medium	Low	High	Medium
Network	IR sensor network + IR tags	Activation unit + 6 broadband US transmitters (Polaroid 600) [101]	Virtex 5 FPGA-based board + 4 speakers [111]	5 LED lights + 1 receiver [105]	DW1000 UWB ranging chip, processor STM32F105 ARM Cortex M3, omnidirectional antenna, nodes or tags [108]	RFID reader, reference tags, target tags [109]
Localization Method	Proximity detection, Trilateration	Trilateration	Watermarking, Trilateration	Lateration, Angulation, Fingerprinting	Multilateration	Triangulation, Fingerprinting, Proximity detection
Frequently-used Convention Measurement	ToA	RSS, ToF	ToF, TDoF Phase conherence ToA, TDoA	RSS, TDoA, AoA	ToF, ToA, TDoA	RSS, ToA, AoA
Multi-person Scenario	7m x 7m area, with 4 PIR sensors on the 4 corners, locate 3 persons within 1.25 meters [112]	4m x 4m area, with 16 receivers, locates more than 70 separate transmitters within 3cm [101]	3m x 3m area, with 4 speakers, locates persons within 20 cm [111]	3m x 3m area, with 4 LEDs, locates receivers within 33cm [113]	5m x 7m area, locates 3 persons within 11.7cm [45]	3.6m x 4.8m area, with 117 reference tags, locates 5 targets tags within 15cm [109]

VLC: Visible Light Communication; UWB: Ultra-Wideband; RFID: Radio Frequency Identification; ToA: Time of Arrival;
TDoA: Time Difference of Arrival ; RSS: Received signal strength; ToF: Time of Flight; TDoF: Time Difference of Flight; AoA: Angle of Arrival;

Table 3.1: Comparison of main indoor positioning technologies (I)

	WLAN-based	Bluetooth	Zigbee	Vision	Geomagnetism	Inertial Navigation (INS)
Positioning Accuracy	23cm [114] - 5m [108]	2m - 10m [85]	25cm - 5m	1cm [115] - 2m [116]	1m -5m [117]	1m - 10m [118]
Coverage Range	Multiple-Room	Multiple-Room	Multiple-Room	Sub-room	Building	Building
Cost	Medium	Medium	Medium	High	Low	Low
Infrastructure Complexity	Low	Low	Low	High	Low	Low
Network	Wi-Fi APs + Phones [87]	Beacon network + BLE Tags [119]	32 Zigbee nodes [46]	Cameras [116]	Magnetometer [120]	Inertial sensors [121]
Localization Method	Fingerprint, Trilateration	Proximity detection, Multilateration, Centroid determination	Proximity detection, Multilateration	Computer Vision	Fingerprint	Pedestrian Dead Reckoning
Frequently-used Convention Measurement	RSSI, CSI, ToF, AoA, TDoA	RSSI, AoA, ToF	RSSI, AoA, ToF	Traditional Image Analysis, AI	RSS	Inertial Measurement unit
Multi-person Scenario	3m x 3m area, with 4 Wi-Fi NICs, locates 3 person within 55 cm [86]	6.1m x 9.4m area, with 6 beacons in six rooms, locates 2 persons within 2 meters [119]	7m x 8.25m area, with 32 sensors, locates 5 persons within 55cm [46]	2.2m x 6m area, with two cameras, locates objects within 7.1cm [122]	58m x 42m area, locates persons within 2 meters [120]	Locates 5 persons within 1.62 meters [121]

WLAN: Wireless Local Area Network; INS: Inertial Navigation System; BLE: Bluetooth Low Energy; RSSI: Received Signal Strength Indicator; CSI: Channel State Information; AI: Artificial Intelligence

Table 3.2: Comparison of main indoor positioning technologies (II)

approach, the sensor events can be separated into different streams, as each resident would have an independent data-driven profile that serves for further personalized interaction provided by the smart environment.

Sensor-based Activity Recognition

Sensor-based activity recognition utilizes sensor readings to understand human activities. The metadata emanated from multifarious sensors embedded in the living environment. These data will be trained and learned by machine-learning or deep-learning algorithms [48]. In this thesis, I leverage human activity datasets from real homes deployed with different ambient sensors (*i.e.,* motion sensor, temperature sensor, light sensor) [41, 42].

Trajectory with identification

Recent works have shown the capability of tracking residents' trajectories with their identification by non-camera-based systems [101, 105, 108, 109, 111, 128]. These classes of technologies can be categorized into *device-based* systems and *device-free* systems. Device-based systems use smartphones, smartwatches, or other wireless tags embedded into the human body. These extra devices will be leveraged to identify different individuals [46, 87, 109, 119, 129]. Device-free system depends on wireless signals by analyzing the signal patterns from the breathing or heartbeat to perform identification [45, 88, 130].

Trajectory and Activity Recognition

The real-world experiment conducted by Nguyen *et al.* [131] emphasized the applicability of modelling complex activities from indoor human trajectories. Their work also demonstrates the feasibility of recognizing activities from new trajectories [131] by applying the hierarchical hidden Markov model (HHMM). Wilson and Atkeson [132] have demonstrated that localization accuracy and activity recognition can be beneficial to each other, especially in multi-occupancy environments. Lu and Fu [133] provide more fine-grained outcomes in a single-occupancy scenario to illustrate the possibility of location-aware activity recognition. These works on location-based activity recognition validate the feasibility of leveraging residents' locations to annotate the time-series sensor events.

3.2.3 Significance of Data Annotation

Recent advances in machine learning and deep learning accelerate sensor-based activity recognition but most of them require annotated datasets [48]. The quality of labels extends a signifi-

cant impact on the performance of machine learning models. However, collecting sensor data with ground-truth labels (*i.e.,*identification, activity) is still challenging, especially in longitudinal monitoring scenarios. Currently, ground-truth labels are obtained either from a resident's diary [134] or vision-based recording techniques [45]. In order to simplify the annotation process, some researchers also designed a simple graphical user interface (GUI) to help residents finish their diary reports [41]. However, this can be tedious, time-consuming, and inaccurate. Unlike the diary-based technique, the vision-based recording is unobtrusive and precise, incorporates significant privacy concerns and needs extra manual inputs. The capability of automatic annotation, hence, is the central primitive when building each resident's individual activity profile. Hamm *et al.* [135] have presented a flexible framework for combining heterogeneous sensory modalities with classifiers for sequence labelling automatically.

In this thesis, I am interested in the identification labelling for time-series sensor events and leave activity labelling for future research. Previous works (as listed in Section 3.2.2) have already demonstrated the capability of a trajectory to identify persons. Hence, in the proposed *MoSen* system, I leverage these identified trajectories to annotate sensor events automatically and instantly by integrating residents' respective locations and the sensor layout. For instance, in a 4-person scenario, where there are four residents in the home, the location information (refers to four respective location points) and the sensor layout are known, the proximity between each location point and the triggered sensor will be compared and the nearest location points from that sensor would be selected. Such a solution mainly depends on the accuracy of the localization techniques (as details are shown in Tables 3.1 and 3.2) and ambient-sensor density. I discuss the effects of different localization resolutions in different sensor layouts in Section 3.5.

3.2.4 Synthetic Sensor Data Generation

In order to protect users' privacy and increase data sharing, synthetic data generation has been developed as an alternative tool among data scientists [136, 137]. The generated data preserves the required statistical features as the real data in a non-adversarial setting and is hardly distinguishable from the real data when the generation structure is mandated by an adversarial network [138]. Effectively generating synthetic data can augment the labelled data and compensate for the data scarcity when the availability of labelled data is constrained [139]. Especially for sensor-based activity data, where data collection for even single-occupancy scenarios is low-fidelity, there are more challenges posed in multiple occupancy scenarios. The aforementioned gap demonstrates the importance of synthetic sensor-data generation in the multi-person setting.

Recent works on Generative Adversarial Networks (GAN) have demonstrated their capability in generating different types of data, from image generation [140, 141], text generation [142, 143], music composition [144], and time-series sensory data generation [145]. The research

published by [146] employed hidden Markov models (HMMs) to generate realistic synthetic smart home sensor data. The authors used data similarity measures to validate the realism of generated data, which are not random but preserve the underlying patterns or structures of the real data. In the experiment of this chapter, I compare the performance of the synthetic multi-person behaviour models with the real datasets to validate the effectiveness of the synthetic models.

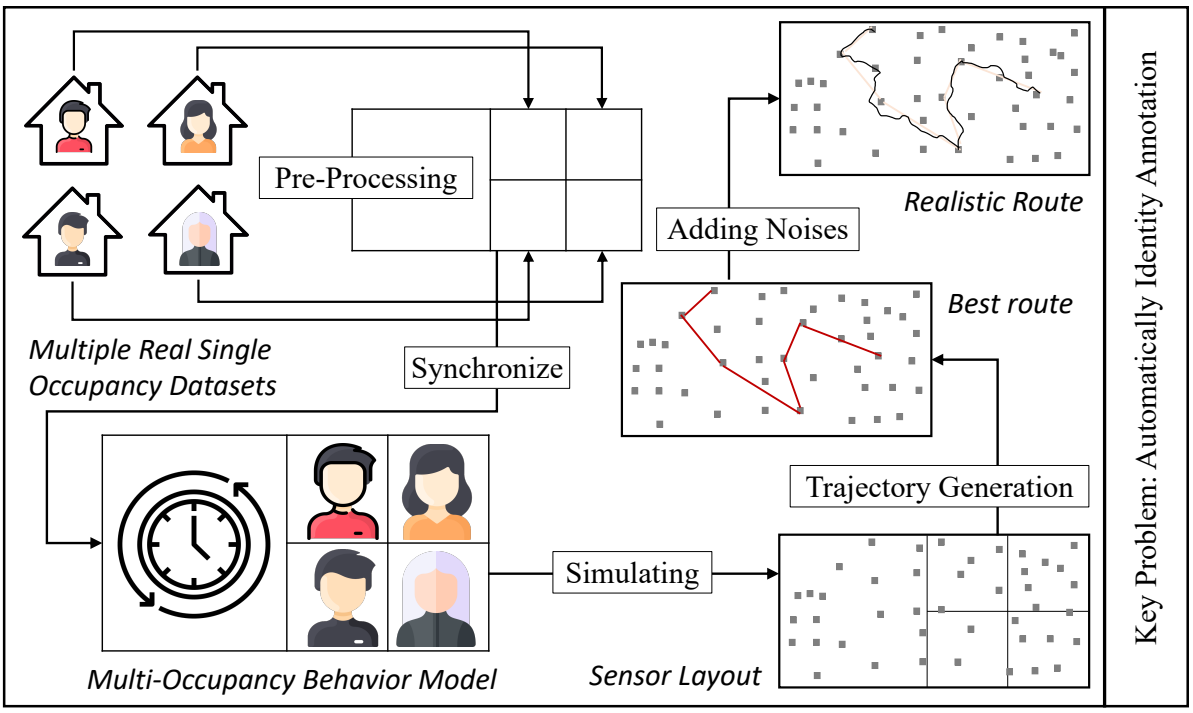


Figure 3.1: An overview of the *MoSen* system. Multiple single-person datasets are learned and utilized to generate synthetic multi-person datasets. Occupants' trajectories are based on the sensor-triggering list. Detected trajectories simulate the localization devices to locate the occupants. Automatic labelling analysis is based on these trajectories and the original sensor event list.

3.3 System Overview

The design of *MoSen* system is motivated by a need to accelerate the practical implementation of sensor-based activity recognition technologies in *multi-occupancy* settings. *MoSen* is adaptable to *different* customized indoor environment. Smart home designers or practitioners can leverage the analytical result of their pre-design sensor network in the specific context-aware task to better balance the trade-off between the deployment cost and system performance.

Figure 3.1 shows an overview of *MoSen* system in solving the identification annotation problem, which is one of the central problems for sensor-based activity recognition in multi-occupancy smart homes [39]. It refers to labelling the identifications of the time-series sensor

events by mapping each sensor event with the resident causing its generation. In this chapter, the identification annotation problem is handled by leveraging the *Graph and Rule-Based Algorithm* (*GR/ED*) proposed in [127], which was designed to track individuals in an ambient sensor setting. The core idea is that individuals trip sensors when they move from one location to another. Sensor events will then be separated into different streams by leveraging human trajectory or location information with the *nearest neighbour standard filter* (*NNSF*) [147], a classical data association method. To achieve the required labelling accuracy of identifications for time-series sensor events in the multi-occupancy environment, *MoSen* can additionally provide a *sensor selection strategy* that fits the user's requirements while optimizing the number of sensors and their placement (hence the installation cost) to achieve the highest labelling accuracy.

MoSen platform can emulate this annotation process with different sensor settings for diverse pre-designed smart homes. The platform assumes that the sensors provide only the sensor events without considering how heterogeneous or multi-modal sensing environments are meshed and combined. In a practical setting, the sensor event is recorded when a sensor is triggered. *MoSen* emulates triggering sensors by building realistic single-person activity patterns. In this way, I can add different representative activity patterns into *MoSen* to simulate multi-resident scenarios, noted as the *multi-occupancy behaviour model* in Figure 3.1. Due to the stochastic nature of my choices and the heterogeneity of chosen single-person datasets, residents who contribute to each activity pattern might have different backgrounds, habits, and daily routines.

I then leverage *Dijkstra's algorithms* [148] to emulate and generate each resident's daily trajectory. These trajectories are utilized as *ground-truth trajectories* of residents. Normally distributed noise, depending on the different resolutions of positioning technologies, is added to the ground-truth value to generate a new trajectory that emulates how localization devices work. This noise-added trajectory is referred to as the detected trajectory. *Labeling accuracy*, in this chapter, is defined as how *detected trajectory* from different sensor networks affects the identification annotation process.

With *MoSen*, by combing the real residents' activity pattern and floorplan, every multi-occupancy house can be emulated and evaluated before deploying a real sensor system, which I believe can accelerate the practical utility of sensor-based activity recognition systems in smart homes.

3.4 System Design Methodology

3.4.1 Dataset Description

In sensor-based activity recognition, multi-modal sensor readings are collected and represented as time-series data to describe human indoor activities. The dataset contains a series of sensor events ordered by time. Each sensor event is recorded when the respective sensor is triggered or activated when it is touched or walked around by residents. In this chapter, I choose two widely-used published datasets in the analysis, CASAS datasets [42] and ARAS datasets [41].

CASAS datasets

The CASAS group collected human activity datasets from the WSU smart apartment testbed [42]. Activity labels are annotated in CASAS datasets with respective start and end times, via a hand-written diary. The majority of datasets represent indoor activities as a series of sensor events, which contains the event timestamp, the sensor name, the sensor state and the activity label. Each sensor event should at least contains the following details: [*Timestamp, Sensor ID, Sensor Status, Activity Label*].

In this chapter, five single-occupancy testbeds chosen from CASAS datasets are leveraged to generate the synthetic multi-person behaviour model. These five testbeds are annotated as hh120, hh122, hh123, hh125, hh126 [79]. Details and properties of them are shown in Table 3.3. And the relations between these testbeds and synthetic multi-occupancy datasets are demonstrated in Table 3.4. Activity labels contained in single-occupancy testbeds include: *bed-toilet transition, cook, eat, enter the home, leave home, personal hygiene, phone, relax, sleep, work.*

Testbed	Timespan	Number of Sensors						
		D	L	LS	M	MA	T	Total
hh120	2012.1.28-3.31	3	7	15	11	4	4	44
hh122	2013.4.1-4.30	4	0	24	19	5	5	57
hh123	2013.3.2-4.1	2	0	14	4	10	6	36
hh125	2013.3.1-4.10	2	0	0	15	0	3	20
hh126	2013.8.1-9.6	0	0	0	15	0	0	15

”D” indicates magnetic door sensors; ”L” indicates light switches;
”LS” indicates light sensors; ”M” indicates infrared motion sensors;
”MA” indicates wide-area infrared motion sensors; ”T” indicates temperature sensors

Table 3.3: Details of the five CASAS single-occupancy testbeds

Multi-occupancy Model	Space Size	Relative Single-occupancy Dataset
2-Person Scenario	12.5 m × 8 m	hh120, hh122
3-Person Scenario	16.5 m × 8 m	hh120, hh122, hh123
4-Person Scenario	16.5 m × 8 m	hh120, hh122, hh123, hh125
5-Person Scenario	20.5 m × 8 m	hh120, hh122, hh123, hh125, hh126

Table 3.4: Correlation between real single-occupancy testbeds and synthetic multi-occupancy behaviour model

ARAS datasets

Different from the CASAS group collecting the activity in the lab setting, the ARAS group collected two pairs of residents' daily activities in their real houses by recording the ground truth labels with a designed Graphical User Interface (GUI) [41]. For each house, it consists of 30 days of sensor reading in the form of a 22×86400 matrix for each day, where the first 20 columns (*S1 - S20*) refer to the binary sensor reading and columns 21 (*P1*) and 22 (*P2*) are the activity labels for resident A and B. The activity labels, ranging from 1 to 27, represent 27 different activities. They are in order as follows:
going out, preparing breakfast, having breakfast, preparing lunch, having lunch, preparing dinner, having dinner, washing dishes, having snack, sleeping, watching TV, studying, having shower, toileting, napping, using internet, reading book, laundry, shaving, brushing teeth, talking on the phone, listening to music, cleaning, having conversation, having guest, changing clothes, others.

The data example below presents how the ARAS dataset represents sensor status every second and the activity labels of two residents.

Timestamp	*S1*	*S2*	*S3*	*S4*	*S5*	*S6*	*S7*	*S8*	*S9*	*S10*	*S11*	*S12*	*S13*	*S14*	*S15*	*S16*	*S17*	*S18*	*S19*	*S20*	*P1*	*P2*
86398	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	2
86399	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	3	2

S1 to S20 indicate the sensor identification, and their statuses are shown in binary form, where 0 refers to deactivated status and 1 refers to activated status; P1 and P2 indicate the activity label for Person A and Person B, respectively. For instance, 12 represents "watching TV", and 2 represents "going out".

Format of Synthetic Datasets

Two aforementioned datasets [41, 79] illustrate two main variations of data representations in the sensor-based activity recognition literature. In this chapter, further analysis of both datasets requires me to integrate them in a uniform way. By this motivation, I define the format of the synthetic dataset to include the critical information needed, as the sample data are shown as follows:

Timestamp	*P1*	*P2*	*P3*	*P4*	*P5*
t_1	S_1^1	S_2^1	S_3^1	S_4^1	S_5^1
t_2	S_1^2	S_2^2	S_3^2	S_4^2	S_5^2
...	...	...	...	...	...
t_i	S_1^i	S_2^i	S_3^i	S_4^i	S_5^i

Timestamp refers to *critical timestamps* in the multi-person scenario, where *critical* indicates that at least one sensor triggered in that second. This thesis also notes every critical sensor activation as one *sensor event*. *P1 to P5* represent five residents, respectively. S_n^i denotes the sensor ID triggered at t_i by the resident *Pn*. I leverage sensor activation annotated with effective activity labels from CASAS and ARAS datasets to model resident activity patterns, which are action-based behavioural models.

3.4.2 Data Pre-processing

Data pre-processing is responsible for unifying the format of the dataset from different sources. I pre-process the public single-occupancy datasets, by developing an algorithm to capture the critical timestamps for sensor status transition or activity transition, then format the data as discussed aforementioned in Section 3.4.1.

Capturing Critical Timestamps

In CASAS datasets [79], sensor events are recorded in order with timestamps that sensors are triggered. However, for the ARAS dataset [41], data is recorded every second, that is, the dataset has 86399 lines which refer to a day with 86399 seconds. Capturing critical timestamps for both datasets is the first step to uniform the data.

Defining the Start and End Point

Critical timestamps are important to investigate how the sensor events or activities transit. In identifying the start or end points for sensor events, I leverage the *last sensor fired representation* [43], which means the last triggered sensor continues to retain its value as 1 and changes to 0 when the next sensor is triggered. In the data format, the transition between S_n^i and $S_n^i + 1$ represents this information, that is, the sensor triggered by resident *Pn* is changing. And the corresponding switching timestamp refers to *critical timestamp*.

	Area Size	Floorplan	Sensor Quantity (Sensor Density)	Sensor Event Occurrences
ARAS [41]	50 m^2	1 bedroom, 1 bathroom, 1 kitchen, 1 living room	20 0.4 sensor/m^2	187
2-Person Scenario	100 m^2	2 bedrooms, 1 bathroom, 1 kitchen, 1 living room	43 0.43 sensor/m^2	190
3-Person Scenario	118 m^2	3 bedrooms, 1 bathroom, 1 kitchen, 1 living room	51 0.43 sensor/m^2	253
4-Person Scenario	132 m^2	4 bedrooms, 1 bathroom, 1 kitchen, 1 living room	60 0.45 sensor/m^2	420
5-Person Scenario	150 m^2	5 bedrooms, 1 bathroom, 1 kitchen, 1 living room	69 0.46 sensor/m^2	565

Table 3.5: Descriptions of synthetic multi-occupancy models and the comparison with the ARAS dataset

Smoothing

To obtain critical timestamps, I select switching time points when transitions occur. However, this processing step includes both real activity switching time and noise values. The sensor data is sampled every second. The high-density data includes several kinds of unexpected noise values, *e.g.*, a break in continuous activity, loss of data, etc. These noisy values should be smoothed before the final mapping stage.

Mapping

By understanding and learning the relations between activities and sensors, I try to figure out the dynamics of the system's performance and the sensor layout.

3.4.3 Synthetic Multi-person Behavior Models

In this chapter, I leverage five different single-occupancy published datasets [79] to build synthetic multi-person datasets. The occupants from each dataset will act as residents in the emulated environment with their realistic activity data and learned patterns in different multi-person scenarios.

Properties of the dataset

Table 3.5 illustrates the properties of several multi-occupancy scenarios and infrastructures' detail in respective emulated environments. The synthetic multi-person datasets I used for further modelling contain information described in Section 3.4.1, consisting of important timestamps

and sensor ID triggered by residents. Figure 3.2 shows the sensor activation list in the four-person scenario. Four coloured lines represent four residents in the space, respectively.

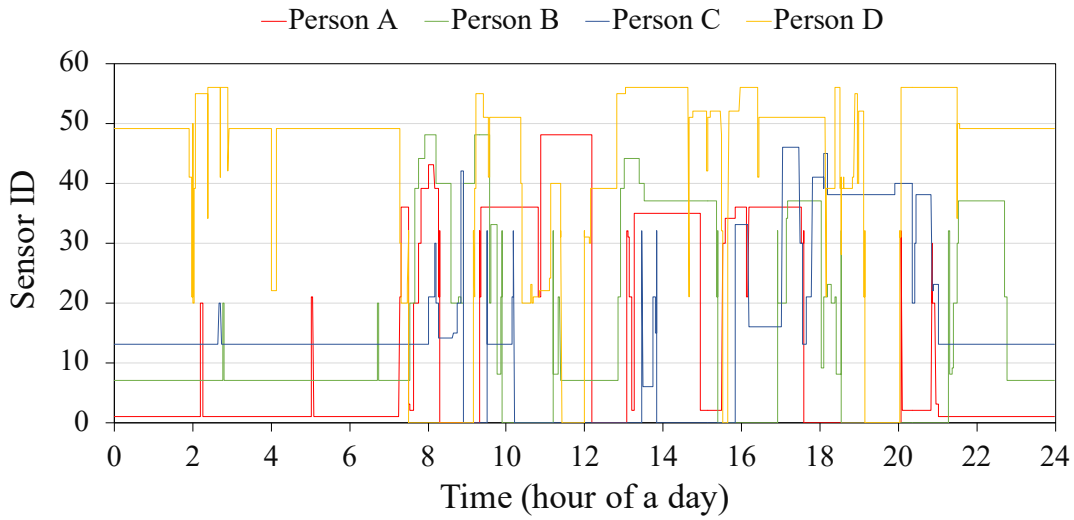


Figure 3.2: Overview of sensor activation list in a four-person scenario, where the x-axis represents the time and the y-axis represents the sensor ID; lines with red, green, blue, and yellow colours represent the lists of residents A, B, C, and D, respectively.

Validation of the methodology

In order to evaluate the quality of the synthetic multiple-occupancy datasets and validate whether the proposed synthetic methodology can represent characteristics of the real-environment datasets, I compare the similarity between the ARAS dataset [41], a real two-person dataset, and the synthetic two-person dataset. The ARAS dataset in ARAS(real) floorplan is defined as the baseline, referred to *Configuration I* in Figure 3.3. Then I compare the synthetic dataset in the ARAS floorplan (*Configuration II*), the ARAS dataset in the emulated floorplan (*Configuration III*), and the synthetic dataset in the emulated floorplan (*Configuration IV*) to the *Configuration I*.

To quantify the variation of localization resolution in different configurations, both labelling accuracy (*LA*) and corresponding decreasing rate (*DR*) of the same annotation task are analyzed, shown in Figure 3.3. I first investigate the similarity when using the ARAS (real) and synthetic datasets in the ARAS (real) floorplan, as shown in Figures 3.3a and 3.3b. Even though the synthetic dataset is stochastic and has no relation to the real dataset, it performs as well as the real dataset under an identical layout for the annotation task. I then compare the performance when the ARAS (real) and synthetic datasets with the same emulated floorplan, as the experiment results shown in Figures 3.3c and 3.3d, which also exert similar performance in the same task. This similarity demonstrates that the synthetic datasets I utilized for further analysis can provide convincing explanations for the annotation task in this chapter.

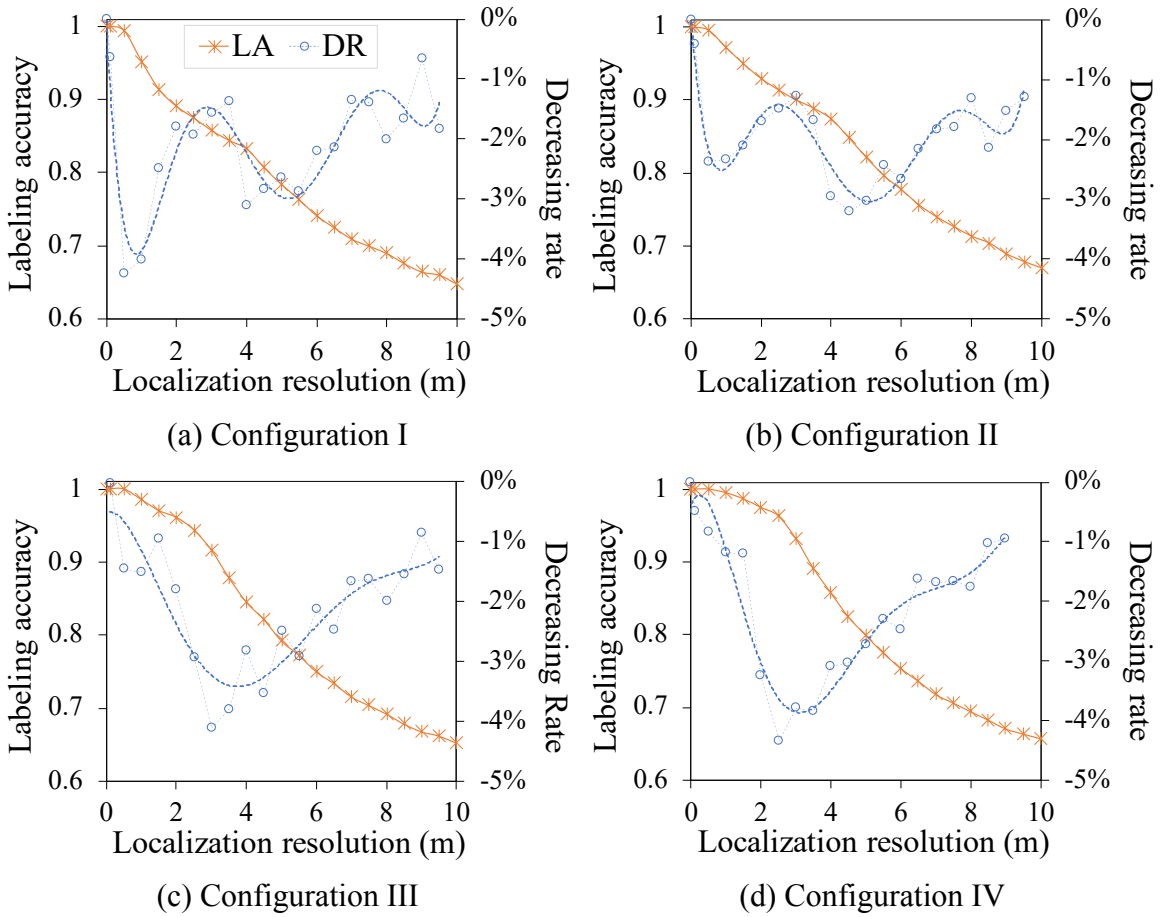


Figure 3.3: Similarities between four different configurations

3.4.4 Trajectory Generation

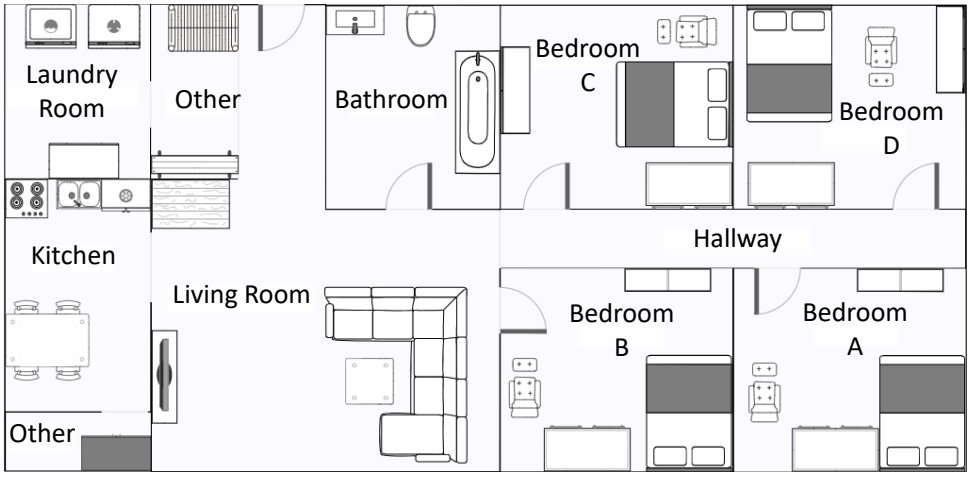
Based on the sensor activation versus time, I model *the real trajectory* by choosing optimal paths between adjacent sensor activities. The *detected trajectory* is synthesized under the real trajectory and the different localization resolutions.

Real Trajectory Generation

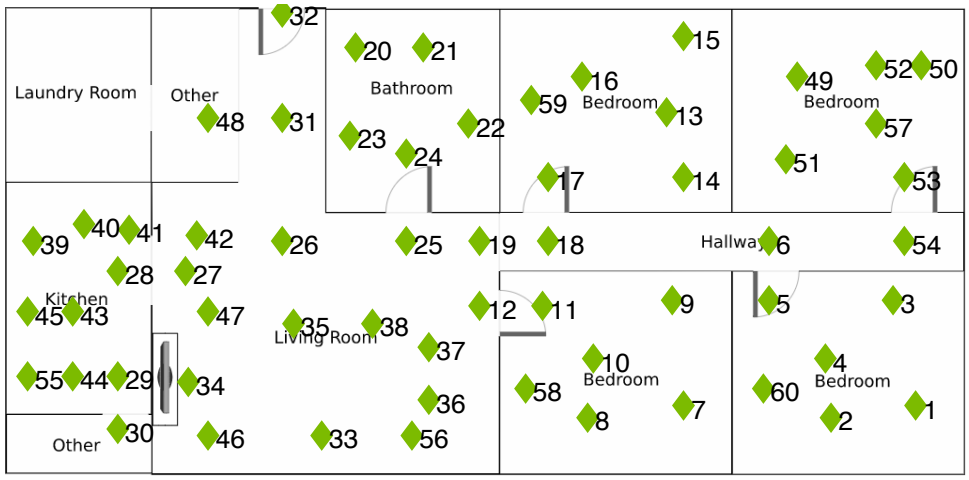
By leveraging the sensor activation lists with timestamps, the target resident's locations can be inferred by the sensor layout, as shown in Figure 3.4, and a series of location nodes would be considered to generate the *best route* when a resident moves from one sensor to another. The *best route* generated is utilized as *real trajectories* for residents in this chapter as people always choose the shortest route when moving from one node to another.

The nodes include *sensor locations* and *junction locations* to avoid obstacles, as shown in Figure 3.5. Sensors are attached to furniture or appliances that residents most frequently interact with. Some important nodes are added in the *Hallway* and *Living Room* as a transition point from

(a) 3D view



(b) Floorplan



(c) Sensor layout

Figure 3.4: The experimental space for the four-person scenario. Other multi-occupancy scenarios have similar settings.

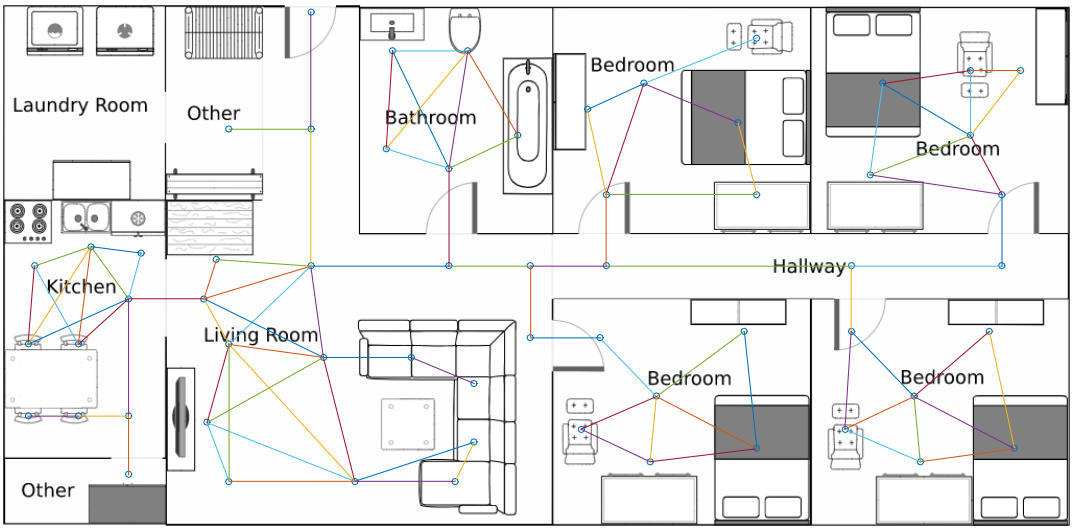


Figure 3.5: Sensor locations and bridge connections between nodes in a four-person scenario. Sensors are attached to furniture and appliances that residents are most frequently interacted with. Some important nodes are added in the Hallway and Living Room as the transition points from one sensor to another sensor. Bridges represent how people will move from one sensor to the nearby sensors.

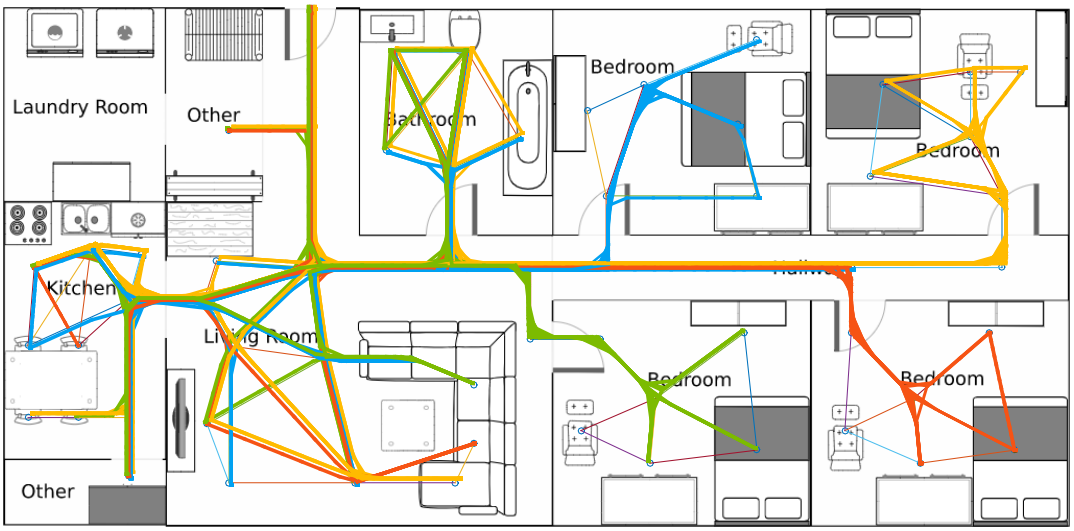


Figure 3.6: Residents move and interact with the environment in a day using the shortest routes; solid lines with red, green, blue, and yellow colours represent the trajectories of residents A, B, C, and D, respectively.

one sensor to another, which are referred to as *junction locations*. *Bridges* represent how people will move from one sensor to the nearby sensors. If the number of nodes is not big enough, the path will be intercepted by the walls. More nodes can result in a smoother moving path but will increase computational cost. Given nodes layout and possible path connections (edges), the *bridge map* can be graphed (in Figure 3.5). The *bridge map* includes all possible optimal ways in the room to move from one activity (sensor) to another one. Finding the shortest route between two sensors can be treated as a classic optimization problem. Several widely evolved navigation algorithms exist for finding an optimal path in 2D environments (*e.g.*, *Dijkstra's algorithms* [148], *A** [149], and *Depth First Search* (*DFS*) [150]).

Dijkstra's algorithm is a technique to find the optimal and shortest paths between two different nodes (*i.e.*, starting point and destination point). To accelerate the calculation, a *modified Dijkstra's algorithm* is adopted to synthesize the resident's *real trajectory* in this study. Setting the nodes $SL = \{1, \cdots, n\}$, the possible connections $E = \{1, \cdots, m\}$, the selection of optimal path can be done in $O\left(E + SL \log SL\right)$ step for each selection. During the selection, each edge should have one or multiple weights. The weights are used to evaluate the capacity and priority of edges. In this work, the only considered parameter is the distance, without additional priority factors. Each path can be endowed with priorities depending on the specific case to improve further. Figure 3.6 shows the emulated *real trajectories* based on four residents' sensor activation lists, respectively.

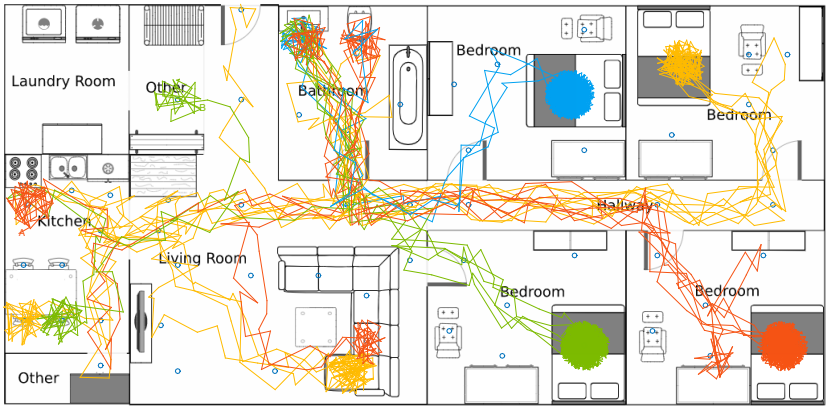
Detected Trajectory Generation

The RTLS devices can provide the *detected trajectory* within the respective resolution[101, 105, 109, 111, 128]. The localization range and resolution of the facilities depend on the different indoor positioning technologies [108]. After the *real trajectory* is generated, the possible resolution is incorporated into the trajectory with a given device (sensor) performance. Assuming the localization resolution is L and the possibility of each point in the error range being identical, the error can be added as Equation 3.1.

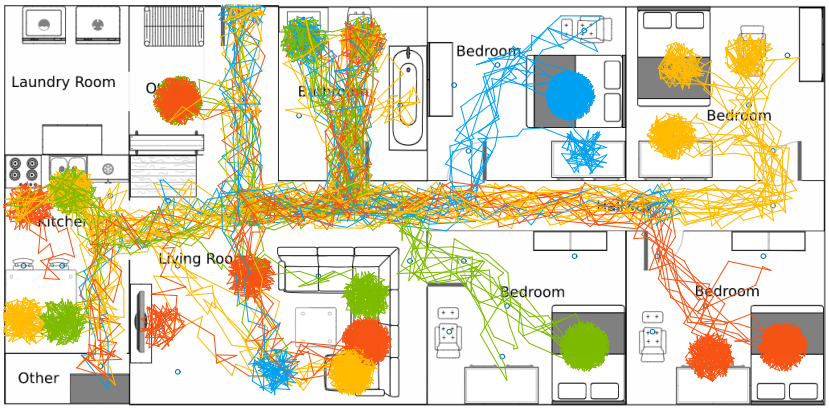
$$\begin{cases} x = x_r + E \cdot L \cos\theta_i \\ y = y_r + E \cdot L \sin\theta_i \end{cases} \tag{3.1}$$

where θ_i is the possible angle for sensor i from real location (x_r, y_r), (x, y) is the detected location and $E \in [0, 1]$ is error factor.

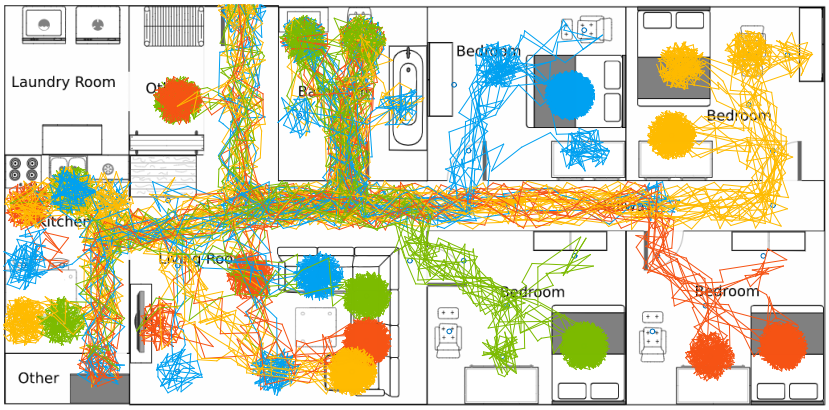
In this study, the distribution of added error is assumed to be uniform in all locations of the shooting range. Error factor E can be any value from zero to one with an identical possibility. If the resolution of a particular device (sensor) has a specific pattern (*e.g.*, *semi-normal distribution*), the error factor $E\left(x\right)$ should be controlled to have a changing possibility along with



(a) Time 00:00-08:00



(b) Time 00:00-16:00



(c) Time 00:00-23:59

Figure 3.7: Emulated deviations (0.5-meter resolution) are added to the route for four residents. Solid lines with red, green, blue and yellow colours represent the trajectories of residents A, B, C and D, respectively.

the distance from the sensor. If the sensor is attached to a wall, resulting in a sector detected range, the detecting location is controlled in a corresponding direction.

Figure 3.7 shows a representative trajectory (L = 0.5 meter), demonstrating how *MoSen* emulates localization devices to collect residents' data in a day. It gives a straightforward insight into how residents have different activity patterns that live in a single environment, which can be quite intricate.

3.5 Evaluation

3.5.1 MoSen Implementation

Typical studies in multi-occupancy scenarios may consider two residents in the same space, limited by costly devices, annotation problems, localization accuracy, or others. With the *MoSen* platform, I investigate different multi-person scenarios by emulating independent residents in *different* target sensor network. I then provide the sensor selection strategy for the sensor network by balancing the trade-off between deployment cost and system performance. The results of the experiments would inform real sensor deployment of the multi-resident smart home.

Design strategy of multi-occupancy environment

Because of the scarcity of multi-occupancy activity datasets in the sensor-based setting, few research studies consider more than two residents in a single space. Leveraging two real two-person datasets, noted as ARAS [41] and CASAS [79], I validate the efficiency of the two-person data generator in Section 3.4.3. I expand the generator and emulate multi-occupant scenarios in households with 2 to 5 residents. The 5-person scenario is considered due to the fact that the average person lives in a household of 4.9 people around the world [151].

MoSen platform is adaptable to different or customized indoor environments, and the critical inputs to the platform are the sensor locations in the target floorplan. In this evaluation, one design strategy chosen for the increasing multi-person scenarios is to maintain *similar* layout complexity and sensor density, only the number of bedrooms changes with the number of residents. Figure 3.4 shows the representative floorplan in the four-person scenario, and Table 3.4 demonstrates the space size of each scenario. Generally, every multi-person environment in this evaluation consists of:
Living room, kitchen, laundry room, bathroom, hallway, bedrooms (corresponding quantity is depending on the number of residents) and others.

Integration

Synthetic multi-person datasets and multi-occupancy environments are integrated to emulate residents' indoor trajectories. The emulation idea is based on when people move between two triggered sensors and would probably choose the shortest way from the current sensor location to the next. This shortest way is referred to as the *best route* in this chapter, as discussed in Section 3.4.4. I leverage these best routes as residents' *real trajectories*, while the *detected trajectories* emulate how different positioning resolutions of sensor networks track human activities.

However, different positioning technologies with respective resolutions exert varying accuracy when these technologies locate residents in a real environment, which also has diverse deployment costs [118]. For instance, when detecting human locations and trajectories, deviations from the ground-truth values are caused by different resolutions. For example, Estimote [152] announced their location beacons could achieve 1.5 meters accuracy, which means that the detected location and their real location might be away from each other at most 1.5 meters. In this chapter, with varying resolutions of different technologies (ranging from 0 meters to 10 meters), I add respective deviations to the *best route* and refer to the new trajectories as the *detected trajectories* that are obtained by the distinct localization devices.

Automatic identification labeling

Providing personalized services to different residents is one of the most important applications in multi-person smart homes. Profiling the resident's activity patterns and recording what sensors they have interacted with in their daily routines are the preliminary work in multi-person activity recognition.

Automatic identification labelling is the central problem when I try to model multi-occupancy activity recognition based on ambient-sensor networks. One feasible solution is to use residents' trajectories to label the triggered sensors by matching the location of the sensor and the resident. The *Graph and Rule-Based Algorithm* (*GR/ED*) [127] and the *nearest neighbour standard filter* (*NNSF*) [153] are leveraged in this chapter to solve the annotation problem, as detailed in Section 3.3. I compare the detected locations of all residents and the triggered sensor at every critical timestamp. The triggered sensor, hence, would be assigned to the resident who has the shortest straight-line distance. As illustrated in Section 3.4.4, in the *MoSen* emulation, the *best route* represents the ground-truth locations of every resident, while the *detected trajectories* are utilized in the realistic annotation process.

3.5.2 Performance

In this evaluation, I choose the automatic identification annotation problem as the central task to illustrate how *MoSen* platform evaluates the impact of the number of residents, the number of sensors, positioning technologies, and different sensor layouts. *MoSen* can additionally provide a *sensor selection strategy* that fits the user's requirement while optimizing the number of sensors and their placement (hence the installation cost) to achieve the highest labelling accuracy. While the real datasets leveraged to model the synthetic multi-occupancy datasets have data for more than one month (Table 3.3), only one-day data from the synthetic datasets are utilized in further analysis.

Labeling Performance

Resolution (meters)	2-Person	3-Person	4-Person	5-Person
0.5	100%	100%	99.89%	99.64%
1	99.64%	99.62%	99.35%	98.68%
2	98.19%	98.39%	**94.56%**	**94.03%**
3	95.57%	**93.88%**	**88.16%**	**86.71%**
4	**91.02%**	**87.61%**	80.49%	77.61%
5	**87.46%**	82.52%	74.57%	70.86%
6	84.64%	78.66%	70.00%	65.83%
7	82.63%	75.58%	66.64%	61.74%
8	81.01%	73.33%	63.65%	58.07%
9	79.52%	71.42%	60.75%	54.99%
10	78.41%	69.95%	58.13%	52.12%

Table 3.6: The percentage of labelling accuracy in different scenarios by increasing the number of residents, with different localization resolutions, from 0.5-meter to 10-meter localization resolution.

In Table 3.6, I first compare the performance of automatic identification labelling in several multi-occupancy scenarios. I use *similar* floorplans and sensor layouts to emulate multiple residents living in a single space. It generally provides information about the selection of localization devices when an application has a different demand on labelling accuracy. The labelling accuracy can be improved with a smaller resolution, but the cost of devices will also increase. Insights from this table could provide valuable information to designers or practitioners when designing the actual sensor deployments. For example, in a 2-person scenario, at least a 4-meter localization device is needed when a user requires a labelling accuracy higher than 90%, but in a 5-person scenario, a 2-meter resolution is required to achieve the same-level accuracy.

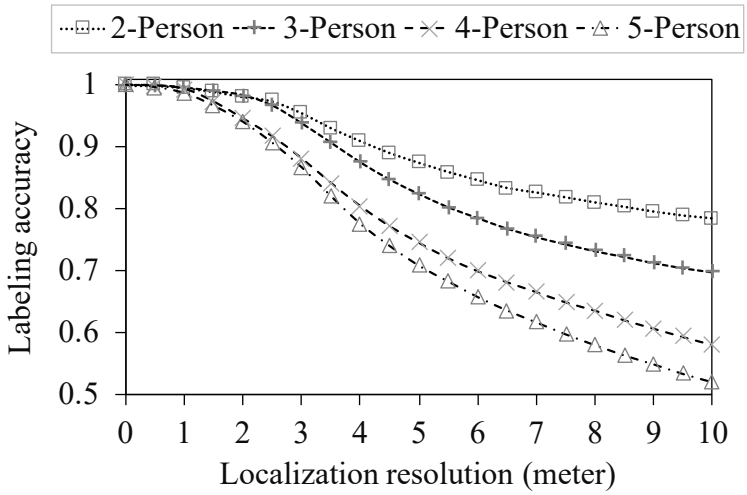


Figure 3.8: The effect of different localization resolutions on the automatic labelling accuracy in the 2-person, 3-person, 4-person and 5-person scenarios, respectively.

Scenario	Mean Distance (meter)	Variance	Transition Point Interval*
2-Person	1.6865	0.5305	3.0-3.1 meters
3-Person	1.7065	0.5278	3.4-3.5 meters
4-Person	1.6692	0.4337	3.0-3.1 meters
5-Person	1.6936	0.5714	3.2-3.3 meters

* *Transition point interval* refers to the interval that contains the highest decreasing point.

Table 3.7: Mean distance and variance for the sensor nodes distribution in several multi-occupancy scenarios

Varying Localization Resolution

Different techniques have varying performances in localizing individuals, and localizing multiple residents simultaneously is challenging. In this experiment, I evaluate how the varying localization resolutions affect the final labelling accuracy in multi-occupancy scenarios. In each scenario, I implement the same activity sequence in the proposed floorplan but increase the localization resolution. I increase the deviations of the residents' trajectories and add more noise to the *best route*. As shown in Figure 3.8, different declining sigmoid curves indicate how the labelling accuracy decrease with increasing resolution.

Effect of Resident Quantity

In order to understand the decreasing trend of labelling accuracy in different occupancy scenarios, I increase the number of residents in the same setting and investigate the change in labelling accuracy. Figure 3.9 shows the overview of the labelling performance when increasing the number of residents; Figures 3.10a and 3.10b demonstrate the decline rate of the labelling accuracy

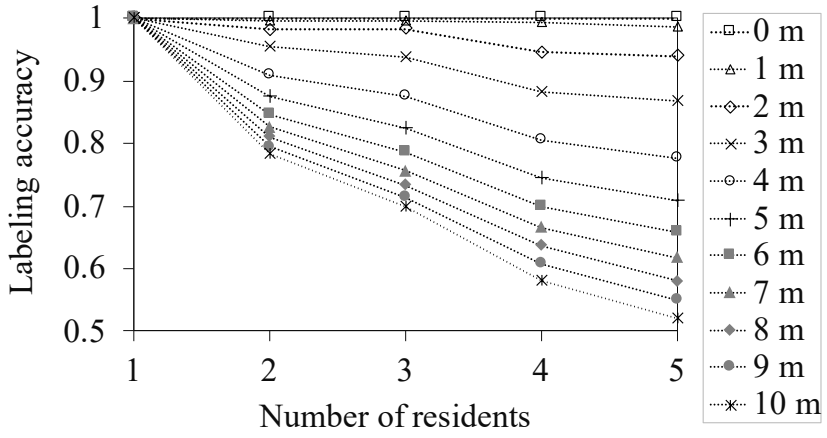
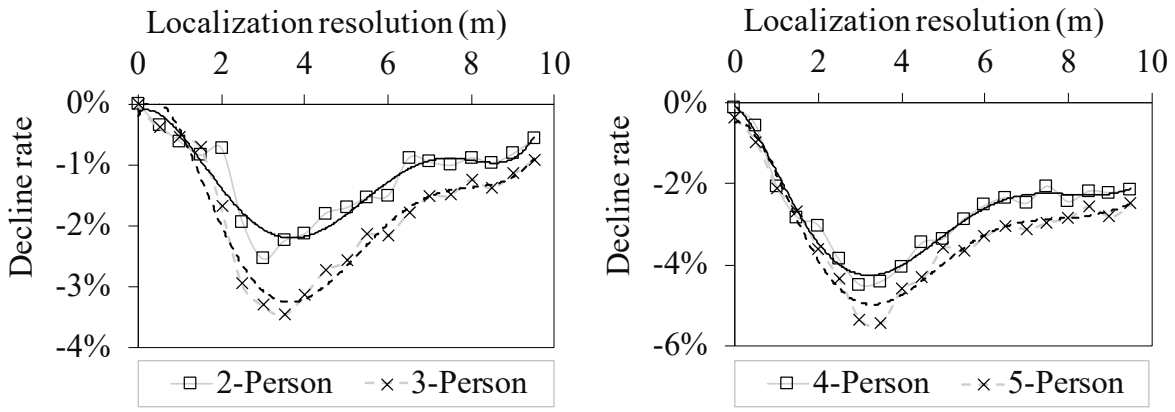


Figure 3.9: Effect of the number of residents on accuracy in different scenarios.



(a) Decline rate with 2 and 3 persons (b) Decline rate with 4 and 5 persons

Figure 3.10: Decline rate of automatic labelling in different scenarios.

for the four multi-occupancy scenarios, respectively. Labelling accuracy decreases when the number of residents increases. It is worth noting that the highest points of decline rate in these scenarios are all between 3 and 3.5 meters. The similarity between these four scenarios because I utilize a similar sensor density for them to keep the same complexity of the sensor deployments. In other words, the highest point of decline rate depends on the sensor deployments.

Effect of Sensor Density

In the experiments, the four multi-occupancy scenarios use four different floorplans as I described in Table 3.5, the number of *bedrooms* changes with the residents' quantity. However, I keep the same sensor density of these floorplans, as also shown in Table 3.5, the sensor density of four scenarios ranges from 0.43 to 0.46 sensors per m^2. I also utilize *mean distance* to compare the sensor density of four floorplans. The *Delaunay triangle method* [154] is adopted to connect each sensor node with neighbouring sensor nodes, while the length of these connections is leveraged to calculate *mean distance*. The distributions of the connections' lengths

are shown in Figure 3.11. After removing the outlier connection near the border, I calculate the average length for these connections. This average length refers to *mean distance*. In this setting, the same decreasing trends in all scenarios (shown in Figures 3.10a and 3.10b) indicate the effect of the same sensor density (0.43-0.46 sensor/m^2) of the floorplans. For instance, each sensor occupied 2.3 m^2 in the 2-person scenario on average, and the mean distance of nodes is 1.6865 meters, where the labelling accuracy decreases most dramatically changed during 3.0-3.1 meters. Since other scenarios also have similar sensor densities (shown as *mean distance* in Figure 3.11), the intervals of transition points for these scenarios are also similar. This impact is significant when a smart home designer considers the potential sensor layout to better fit the user's requirements.

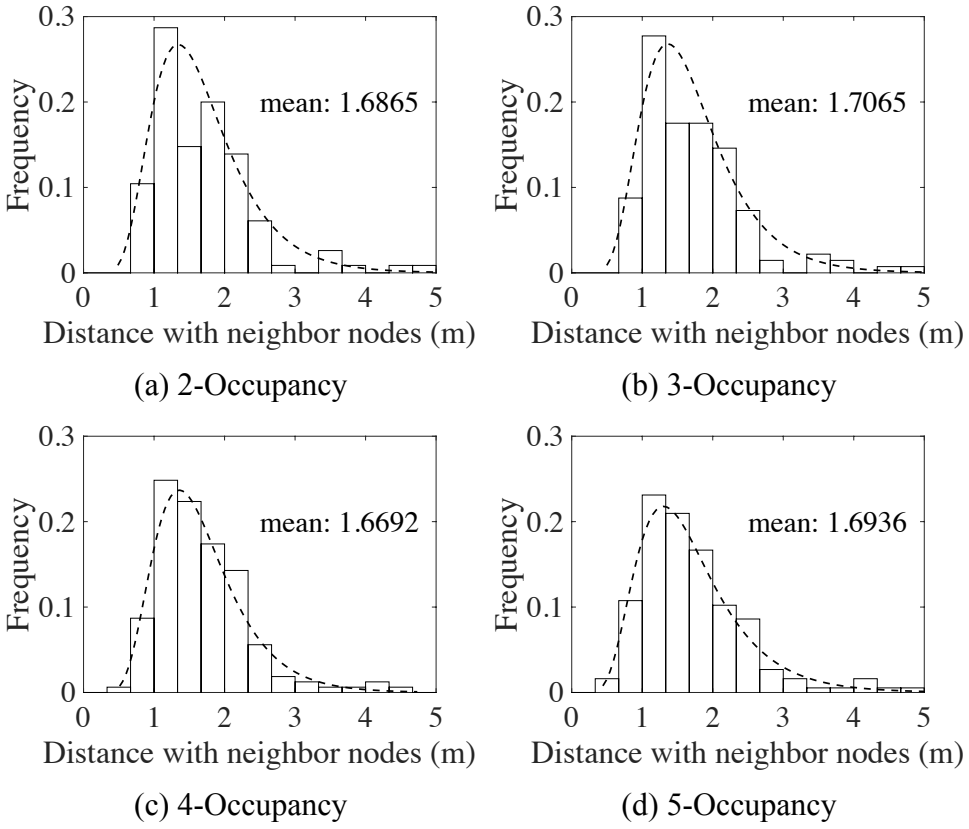
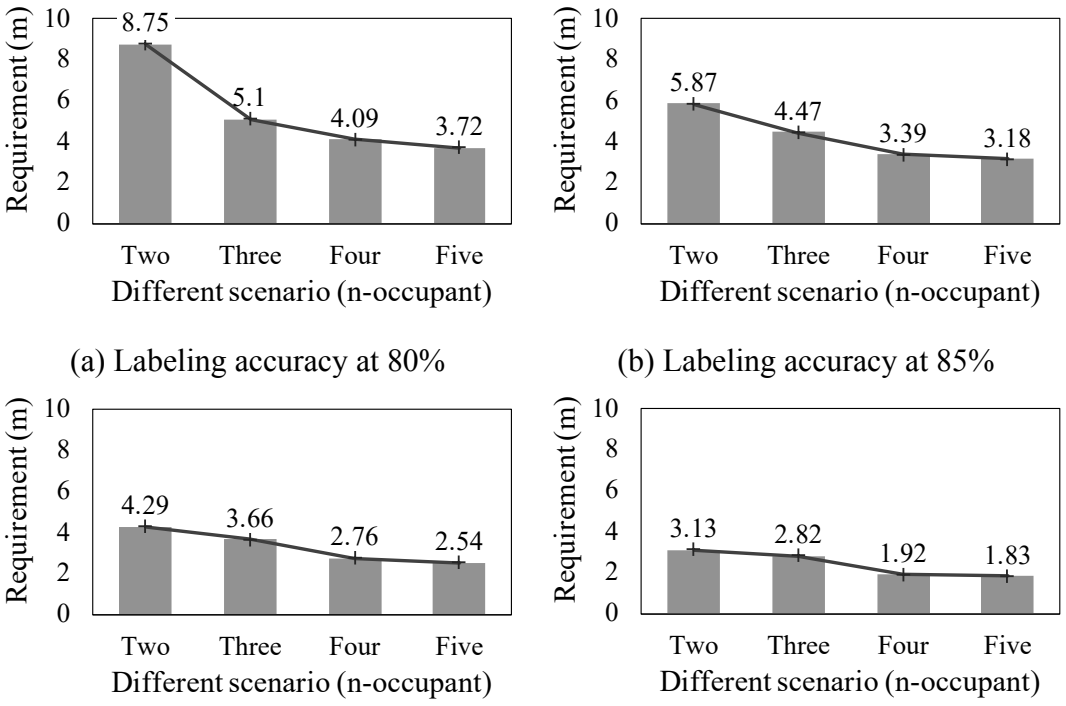


Figure 3.11: Distributions of the sensor connection length in four multi-occupancy scenarios. The x-axis represents the distance between nodes (sensors), and the y-axis represents the frequency of the corresponding distance between nodes.

3.6 MoSen's Sensor selection Strategy

In sensor-based activity recognition, different sensing systems are proposed to monitor indoor activities by leveraging various ambient sensors, which also have diverse performances. Previous works [155, 156] have emphasized the significance of sensor selection in multi-device environments (MDE). Dynamically selecting the best sensor for a specific activity recognition



(a) Labeling accuracy at 80%

(b) Labeling accuracy at 85%

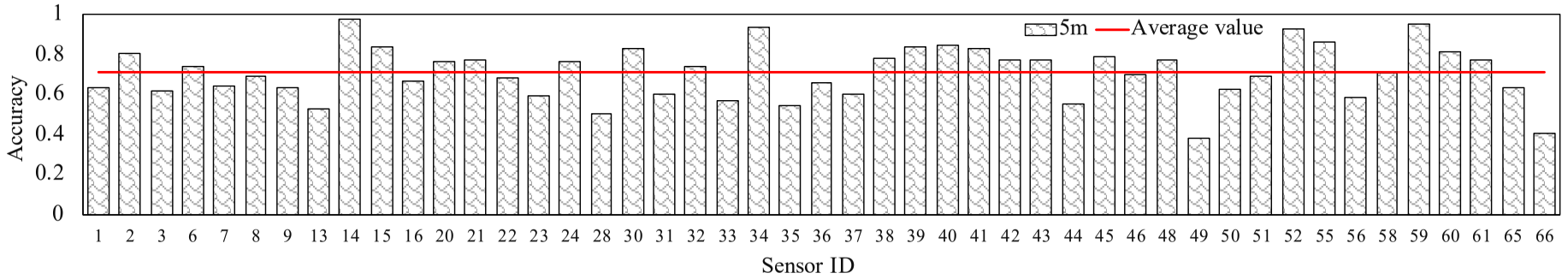
(c) Labeling accuracy at 90%

(d) Labeling accuracy at 95%

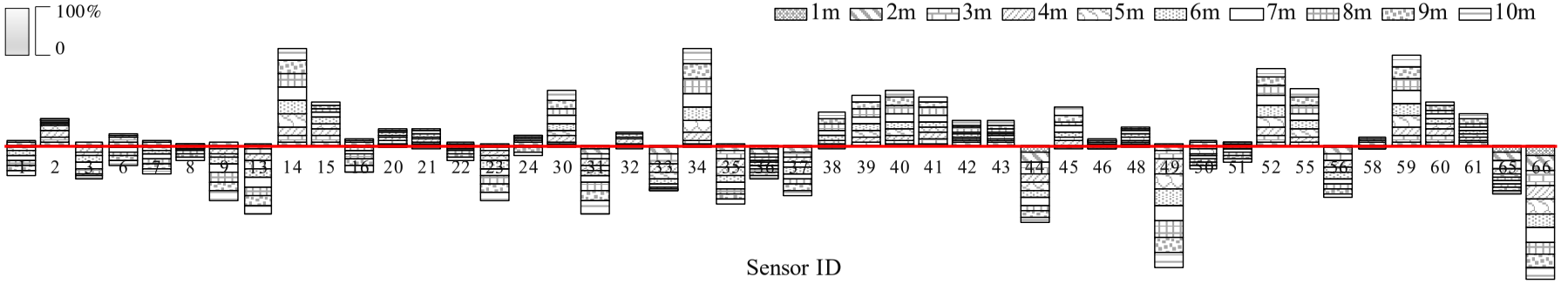
Figure 3.12: Requirements for localization resolution with the expected labelling accuracy, when the labelling accuracy is 80%, 85%, 90%, 95%, respectively.

system is a typical approach developed for context-aware MDE [156–158]. These works are mostly about body sensor networks (BSN), and proposed dynamic designing strategies in the BSN environment. Generally, four requirements (namely cost, acceptance, accuracy, and privacy [159]) are considered for a practical activity recognition system. Realizing recommendations on sensor selection for different smart homes is the key objective of the analysis to achieve a better trade-off between user requirement, labelling accuracy, and system cost. With MoSen, different sensor settings can be analyzed before the real deployment, and it provides more potential choices to users as they might have different budgets.

Many researchers choose the sensor-based activity recognition system primarily due to its non-obtrusiveness and privacy protection [48]. The trade-off between the remaining two factors leaves an interesting but tricky balance to attain. The sensor configuration often depends on the installation cost and sensor prices. I define *sensor sensitivity* to identify the way a sensor's location and interaction frequency with residents affect the labelling accuracy. This information is valuable for choosing the best and the most cost-effective sensor network for the smart home environment. In this section, I focus on identifying *sensor sensitivity* and recommendations on the final sensor selection for a specific layout. I use a five-person scenario here as the case study to illustrate the proposed sensor selection strategy. The insights from the case study are extendable to other scenarios and *different* new floorplan and sensor layout.



(a) Example of the way each sensor affects the final annotation accuracy; in a 5-person scenario with 5-meter resolution. The red line represents the overall accuracy, compared to different sensors' performance (grey bars), individually.



(b) The effect of all sensors in a 5-person scenario, from 1-meter to 10-meter resolution. Each pattern-painted block represents the numerical difference compared to the average performance in the respective scenario. The grey block in the corner represents the scale.

Figure 3.13: Effects on each sensor to overall accuracy in the five-person scenario.

Identification annotation accuracy. The initial analysis of the specific layout (a five-person scenario in this case study) is emulated in the *MoSen* system, where annotation accuracy is regarded as one of the most important factors in the system. The related analysis has been described in Section 3.5, and the results show how the localization resolution and sensor density affect the accuracy. Figure 3.12 shows the requirement for localization resolution with varying labelling accuracy, ranging from 80% to 95%, respectively. For the five-person scenario, if the labelling accuracy is 80%, the localization resolution requirement should be at least 3.72 m or more precise. When the accuracy changes to 90%, the resolution should attain at least 1.83m, which has higher accuracy but is also more expensive than the former one.

Sensor individual effect. Each sensor is evaluated in order to identify the individual effect on the integrated performance, as shown in Figure 3.13, and the x-axis represents the sensor ID. With different localization resolutions, sensors might have different performances, and the cumulative effect is shown in this figure. Each rectangle represents the sensor's individual effect under different localization resolutions. For example, Sensor 6 might have opposite effects when the resolution is varying, but for sensor 14, all effects are positive. This cumulative result leads to a more intuitive concept for *sensor sensitivity*. Some sensor IDs are absent here as they were not triggered in the experiment.

Sensor sensitivity. A sensor's effect is represented as *sensor sensitivity*, and recommendations will be provided based on sensor sensitivity and sensor cost, as well as the localization resolution and labelling accuracy. *Sensor sensitivity* integrates the activity patterns of the resident and how frequently residents interact with a specific sensor. As shown in Figure 3.14, the different radii of the circles represent different sensor sensitivities, where a larger radius allows a larger detection area (with lower sensitivity).

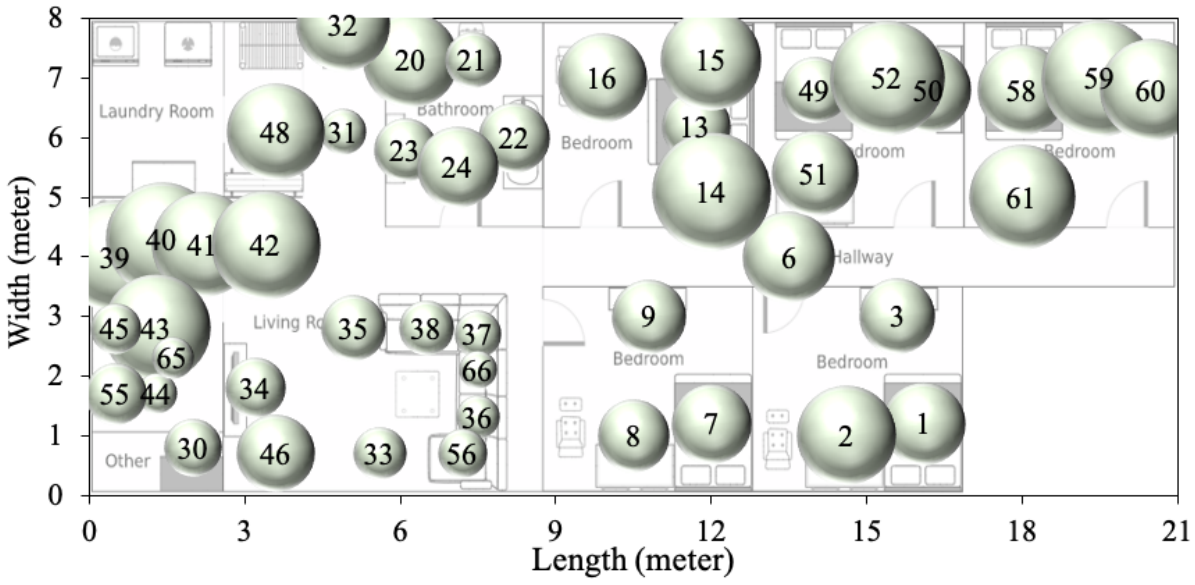


Figure 3.14: Sensor sensitivity in a five-person scenario. A larger radius of the circle means less sensitivity to the distance and allows it to have a bigger detection area, and vice versa.

3.7 Discussions

3.7.1 Data Scarcity On Multi-occupancy Scenarios

Designing activity recognition systems for multi-occupancy scenarios has been challenging for researchers. First, the complexity of human activity increases dramatically when there is more than one person within the same environment. Different from the single-occupancy scene, the interactions between residents introduce uncertainty when defining indoor activities. Second, annotating the triggered sensor with corresponding identification and activity is challenging in the multi-resident scenario. The lack of ground-truth values is deficient to the multiple-resident with advanced machine learning or deep learning technologies. Third, data privacy is a big concern when collecting real human data. Even for the sensor-based activity recognition system, which does not invade privacy as severely as the vision-based systems do, there still is a need to attain the trade-off between data utility and privacy. Fourth, there are still numerous challenges that need to be overcome in the single-occupancy environment [39]. These gaps, hence, impede the practical data collection on the multi-occupancy scenario.

3.7.2 Generality of *MoSen* System

MoSen system is designed and built to investigate the multi-occupancy scenarios by generating a synthetic multi-occupancy behaviour model based on real human activity patterns and emulating these models in a virtual environment. I use collected datasets from real installations to represent the activity patterns of individuals. However, available datasets often do not have a direct interaction between residents. Due to the data scarcity of the multi-occupancy scene, the synthetic method bridges the gap, and the analysis is valuable for the public to design a real multi-occupancy scenario in the future. The strategies proposed in *MoSen* system can extend to *different* floorplan, and initial analysis of each specific scenario provide designers on how to better design a sensor-based system in balancing the cost and accuracy. I choose identification labelling as the key question in this chapter and leave other parameters for future research.

3.7.3 Towards Practical Utility of Sensor-based System

Human activities are hard to model in a uniform way, especially when they have different backgrounds, diverse habits, and varied activity performances [160]. The uncertainty from the spatial and temporal difference also increases this difficulty [42]. In the multi-occupancy scenario, activity recognition becomes more sophisticated and challenging with the increasing number of residents. There is also a trade-off between the RTLS localization resolution and sensor costs. Often, researchers in a lab setting prefer the best technology with the highest accuracy, while

the accumulated cost is hard to afford in real home designs. Finally, the floorplans and furniture are diverse between different homes, which results in highly diverse sensor layouts in a real environment. The proposed system enables reasonable evaluations and design recommendations for each particular home.

3.7.4 Limitations of Vision-based System and Fusion of Multimodal Systems

In this chapter, the sensor-based system is highlighted due to the high privacy invigilation of the vision-based system. However, when with the remarkable progress of the vision-based system in the last decades, it faces similar challenges as the sensor-based one, the ability to recognize human activity in multi-occupancy scenarios is limited [94]. The expensive computation cost of continuous tracking by a vision-based system is another hinder when practitioners consider it in real applications [161, 162]. The combination of vision-based and sensor-based systems is another emerging topic. While these multimodal systems leverage the advantages of different methods, the techniques of data synchronization [163] and fusion [164] of these multimodal systems bring new challenges to the researchers [165–167]. Due to the data dimensionality, acquired data are hard to process and the complexity of activity modelling will be increased.

3.8 Conclusions

Often, researchers in a lab setting prefer the best technology with the highest accuracy, while the accumulated cost is hard to afford in real home designs. The floorplans and furniture are diverse between different designs, which results in highly diverse sensor layouts in the real environment. In this chapter, I presented *MoSen*, a framework for accelerating the real implementation of sensor-based activity recognition systems by analyzing the trade-off between the overall system performance and cost. I investigated the multi-occupancy scenarios by emulating the synthetic multi-occupancy behaviour models, which are generated by real single human activity patterns, in a virtual environment. The *MoSen* platform can extend to *any* floorplan or sensor configuration. The initial analysis of different specific sensor configurations will provide the designers or practitioners with an effective sensor selection strategy. More quantified results will be shown in future work.

In this chapter, I evaluate the efficacy of the *MoSen* platform with an automatic identification annotation task using experiments on synthetic datasets and show how the annotation accuracy is affected by the number of residents, different localization resolutions, and sensor density. Through the trace-driven simulations, the effect of each sensor is also analyzed. Then the sensor selection strategy on the system is provided. Other context-aware tasks will be emulated in future work.

Chapter 4

Privacy-Aware Human Mobility Prediction via Adversarial Networks

As mobile devices and location-based services are increasingly developed in different smart city scenarios and applications, many unexpected privacy leakages have arisen due to geolocated data collection and sharing. User re-identification and other sensitive inferences are major privacy threats when geolocated data are shared with cloud-assisted applications. Significantly, four spatio-temporal points are enough to uniquely identify 95% of the individuals, which exacerbates personal information leakages. To tackle malicious purposes such as user re-identification, I propose an LSTM-based adversarial mechanism with representation learning to attain a privacy-preserving feature representation of the original geolocated data (*i.e.*, mobility data) for a sharing purpose [168]. These representations aim to maximally reduce the chance of user re-identification and full data reconstruction with a minimal utility budget (*i.e.*, loss). I train the mechanism by quantifying the privacy-utility trade-off of mobility datasets in terms of trajectory reconstruction risk, user re-identification risk, and mobility predictability. I report an exploratory analysis that enables the user to assess this trade-off with a specific loss function and its weight parameters. The extensive comparison results on four representative mobility datasets demonstrate the superiority of the proposed architecture in mobility privacy protection and the efficiency of the proposed privacy-preserving features extractor, where the privacy of mobility traces attains decent protection at the cost of marginal mobility utility. The results also show that by exploring the Pareto optimal setting, the proposed model can simultaneously increase both privacy (45%) and utility (32%).

4.1 Introduction

Geolocation and mobility data collected by location-based services (LBS) [169], can reveal human mobility patterns and address various societal research questions [170]. For example, Call Data Records (CDR) have been successfully used to provide real-time traffic anomaly as well as event detection [171, 172], and a variety of mobility datasets have been used in shaping policies for urban communities [173] and epidemic management in the public health

domain [174, 175]. From an individual-level perspective, users can benefit from personalized recommendations when they are encouraged to share their location data with third parties or other service providers (SPs, *e.g.*, social platforms) [176]. Human mobility prediction based on users' traces, a popular and emerging topic, supports a series of important applications. For instance, one of the prerequisites for a successful LBS-recommendation system is the ability to predict users' activities or locations ahead of time, tracking their intentions and forecasting where they will go [177].

While there is no doubt about the usefulness of predictive applications for mobility data, privacy concerns regarding the collection and sharing of individuals' mobility traces have prevented the data from being utilized to their full potential [30–32]. A mobility privacy study conducted by De Montjoye *et al.* [29] illustrates that four spatio-temporal points are enough to identify 95% of the individuals, which exacerbates the user re-identification risk and could be the origin of many unexpected privacy leakages. Additionally, with increasingly intelligent devices and sensors being utilized to collect information about users' locations, a malicious third party can derive increasingly intimate details about users' lives, from their social life to their preferences. Hence, a mechanism capable of decreasing the chance of user re-identification against malicious attackers or untrusted SPs can offer enhanced privacy protection in mobility data applications, as human mobility traces are highly unique.

In the past decade, the research community has extensively studied the privacy of geolocated data via various location privacy protection mechanisms (LPPM) [178, 179]. Some traditional privacy-preserving approaches (*e.g.*, k-anonymity and geo-masking) have shown to be insufficient to prevent users from being re-identified [29, 180–182]. Differential privacy (DP), another popular notion, is shown to be a limited metric for location trace privacy since temporal correlations are not taken into account [30]. Erdemir *et al.* [176] also states that DP and k-anonymity are meant to ensure the privacy of a single data point in time. In general, many DP for LBS (DP-L) mechanisms [53, 183, 184] attempt to protect the *user's location* instead of the *user's identity*, which is different from the problem's scope of this thesis. More recently, some related works have successfully applied machine-learning- or deep-learning-based approaches to explore effective LPPMs. Rao *et al.* proposed a model based on Generative Adversarial Network (GAN) [185] to generate privacy-preserving synthetic mobility datasets for data sharing and publication [54]. Feng *et al.* investigated human mobility data with privacy constraints via federated learning, achieving promising prediction performance while preserving the personal data on the local devices [186]. Though these works provide promising architectures to protect location privacy, the mobility data's privacy protection and utility degradation have not been thoroughly investigated, especially in reducing the chance of user re-identification. My proposed model extends these machine-learning-based mechanisms and explores the privacy-utility trade-off on mobility data in terms of declining the effectiveness of privacy inference attacks while maintaining its predictability. Moreover, research on human mobility shows that

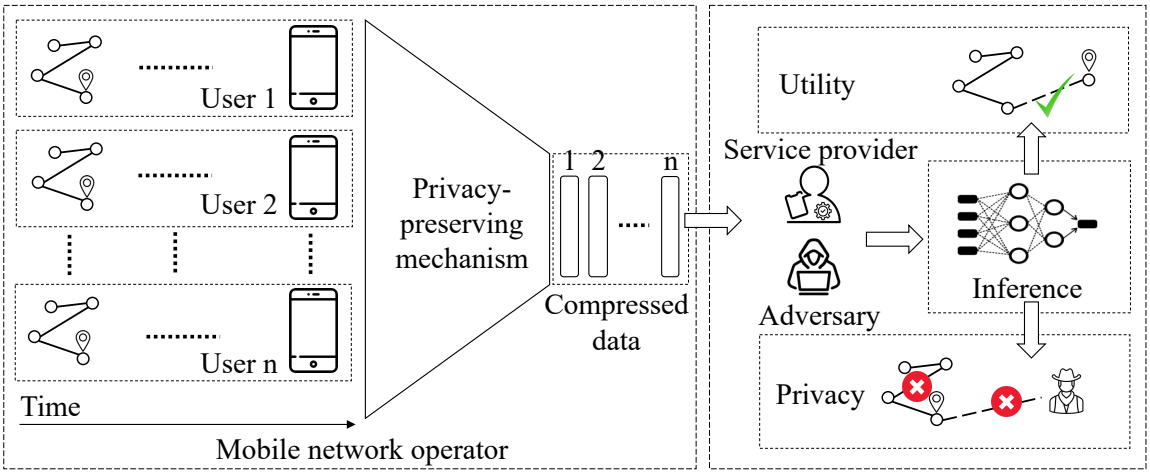


Figure 4.1: Privacy protection in user's location data collection and sharing. Users share their daily traces with a trusted mobile network operator; these traces are aggregated with a privacy-preserving mechanism and shared as a compressed data format; the compressed data should allow utility inference and avoid privacy inference.

the predictability of users' location trajectories or mobility, and the particular constraints of users' movements, are sufficient to reconstruct and/or identify anonymous or perturbed locations [187]. This specific confrontation makes the trade-off between mobility predictability and users' identity more challenging.

Consider a scenario, shown in Figure 4.1, where users share their daily traces to a trusted mobile network operator, which then aggregates these traces in a privacy-preserving approach and sends them to third parties or other SPs with/without users' consent. These users may want to minimize the risk of being re-identified and trajectory reconstructed by those who will access these released data. However, they would like to keep receiving potential effective services from SPs. Therefore, a privacy-preserving mechanism, which can release required information for the services (*i.e.*, utility) while features or patterns that facilitate full data reconstruction or user re-identification are obscured (*i.e.*, privacy), is beneficial. The compressed data encoded by this privacy-preserving mechanism is freely accessed by SPs for the inference tasks, and SPs are free to use any prediction algorithms of their choice.

To this end, I propose a **p**rivacy-aware **a**dversarial network to train a feature extractor $\boldsymbol{E}nc_L$ for **mo**bility privacy, namely Mo-PAE. It is based on representation learning and aims to ease data sharing privacy concerns from privacy inference attacks. Inspired by PAN (privacy adversarial network) [188], I employ adversarial learning to better balance the potential trade-off between privacy and utility. In contrast to PAN, which focuses on the privacy of images, the proposed approach is designed for complex time-series data that exhibits spatial-temporal characteristics. At the core of my architecture lies an auto-encoder (AE) and long short-term memory (LSTM) layers with three branches, corresponding to the three training optimization objectives of the feature extractor Enc_L: i) to *maximize* the loss associated with the reconstructed

output by generative learning, ii) to *minimize* the prediction loss using the learned representation from the Enc_L by discriminative learning, and iii) to *minimize* the percentage of users who are re-identifiable through their trajectories by discriminative learning. I explore and quantify the privacy-utility trade-off provided by Mo-PAE in terms of data reconstruction risk, user re-identification risk, and mobility predictability. The results show that the proposed mechanism achieves a better privacy level with the same utility loss and vice versa.

The contributions of this chapter are the following:

- I propose a **p**rivacy-aware **a**dversarial network to train an effective feature extractor $\boldsymbol{E}nc_L$ for **mo**bility privacy, namely Mo-PAE [1];
- I report the analysis of Mo-PAE by a comprehensive evaluation of four real-world representative mobility datasets;
- I provide an extensive analysis of different inference tasks and quantify the privacy and utility bound of the target mobility dataset, along with a trade-off analysis between these contrasting objectives;
- I compare my model with, i) a famous DP notion that developed on the idea from Geo-indistinguishability [53] (namely GI-DP); ii) a state-of-the-art GAN-based mechanism that attempts to generate synthetic privacy-preserving mobility data (namely TrajGAN [54]); iii) as well as the optimal LSTM-based inference models, and obtain favourable results.

The rest of this chapter is structured as follows: I review the related work in Section 4.2; the proposed Mo-PAE is described in detail in Section 4.4; I describe the experimental settings in Section 4.5; I demonstrate an evaluation of my mechanism over four mobility datasets with baseline comparisons in Section 4.6; Section 4.7 reports an in-depth discussion of the experimental setting; finally, I conclude the chapter with future work directions in Section 4.8.

4.2 Related work

4.2.1 Notions of Location Privacy

Diverse privacy notions, *direct* or *indirect*, for the LBSs have been proposed and evaluated in the literature. In [53], various *direct notions* of location privacy and the techniques to achieve them are examined and concluded, including but not limited to expected distance error, k-anonymity, differential privacy (DP), and other location-privacy metrics. First, the expectation of distance error reflects the accuracy when an adversary guesses the user's real location in a location-obfuscation mechanism by using the available side information. In [187], an optimal LPPM

[1] https://github.com/YutingZhan/Mo-PAE

strategy and its corresponding optimal inference attack are obtained by formalizing the mutual optimization of user-adversary objectives (location privacy vs correctness of localization). Second, k-anonymity is the most widely used privacy notion for the LBSs [189]. These systems aim to protect the *user's identity*, requiring that the attacker cannot infer the correct user among a set of k different users. Third, DP [137] is an emerging notion initially formulated in the context of statistical databases and aims to protect an individual's data while publishing aggregate information about the dataset. More precisely, a randomization mechanism M gives ϵ-differential privacy for all neighbouring datasets D and D', and the difference between D and D' is within a bound of e^{ϵ}. One of the popular mechanisms to achieve DP perturb the original query result using random noise that is calibrated with the privacy budget ϵ and defines a global sensitivity for all neighbouring D and D' [190]. The work in [191] reviews research works done in differential privacy targeted toward location data from a data flow perspective, including collection, aggregation, and mining. [53] proposed a Geo-indistinguishability notion based on differential privacy and a planar Laplace mechanism. Significantly, different from the systems in k-anonymity category aim at protecting *user's identity*, DP mechanisms are interested in protecting the *user's locations* [53, 183, 184, 192]. Apart from three mainstream approaches, the location cloaking mechanism tries to define the uncertainty region and measure privacy by the size of the cloak and by the coverage of sensitive regions; the inaccuracy of the sensing technology tries to achieve a certain level of privacy by increasing uncertainty, and transformation-based approach tries to make user's location invisible to the service provider.

On the other hand, *indirect* notions of location privacy arise with the emerging machine learning-based mechanism, which assesses the privacy guarantee by measuring the effectiveness of target inference attacks [193–195]. In general, for any LBS, their main privacy concerns can be concluded in two categories. One is the attack on the *user's identity* which can be re-identified maliciously. For instance, even if the adversary is assumed to be unaware of the user identity of a trace, they can infer *user's identity* or additional sensitive information due to the location information leakage based on publicly accessible background information. The other attack is the one on *user's location* while the adversary has legible access to *user's identity*. In this manner, *user's locations* are sensitive, which could exert a significant impact on other sensitive personal details, such as religious affiliation, sexual orientation, economic condition, health status, and so on.

In this work, I am interested in protecting *user's identity* as the privacy scope, which is similar to the location privacy notion defined by the k-anonymity, and taking the real/distorted *user's location* as input for the personal recommendation model to provide contextual services for their future travels. In general, DP paradigms have the most formal privacy guarantee than others, however, they are not immune to inference attacks [196, 197]. I will also compare the proposed model with one popular DP paradigm on location privacy to illustrate the ineffectiveness of DP to the research question. More details on the privacy definitions are in Section 4.4.

4.2.2 Location Privacy Preserving Mechanisms

An effective location-privacy preserving mechanism (LPPM) must consider three fundamental elements: i). the privacy requirements of the users (namely, *privacy gain*); ii). the adversary's knowledge and capabilities; iii). and maximally tolerated service quality degradation stemming from the obfuscation of true locations (namely, *utility loss*) [187]. The literature on location privacy can be roughly classified into three categories: the design of LPPMs [198]; recovering actual user traces from anonymized or perturbed traces; the formal analysis and the search for an appropriate location privacy metric that allows for the fair comparison between LPPMs [187, 199]. Generally, typical LPPMs use some obfuscation methods - like spatial cloaking, cell, merging, location precision reduction, or dummy cells - to manipulate the probability distribution of the user's location. The most popular approach to protect location privacy is to send a space- or time-obfuscated version of the users' actual traces to the trusted or untrusted third parties [187]. Xiao *et al.* [200] investigate how to obtain location privacy under temporal correlations with an optimal DP-based LPPM. Another mainstream approach tries to issue dummy requests from fake locations to the services provider, the location privacy is hence protected as these fake locations increase the uncertainty of the adversary about the users' real movements [187]. The other popular alternative utilizes mixed zones or silent periods to hide users' locations, as the adversary cannot link those who enter with those who exit the region when several users traverse the zone simultaneously.

In general, any LPPM would alter the location information, resulting in a severe distortion of data. Therefore, designing an optimized privacy-preserving algorithm with constrained utility degradation according to user privacy requirements is one critical dimension of LPPMs [198]. There is no way to optimally address location privacy issues for all types of location-based systems, and the design of a specific LPPM requires carefully considering the application scenario and the realistic privacy requirements of mobile users [201]. Hence, if a user prefers high service quality rather than the concerns of privacy leakage, then a more flexible system could be applied to guarantee service quality. The proposed model in this chapter, in this way, can perform flexibly in application scenarios when users have different focuses on privacy or service.

4.2.3 Privacy Preserving Techniques for Spatial-Temporal Data

Current privacy-preserving techniques for spatial-temporal data focus on two research streams. One is the DP approach to grouping and mixing the trajectories from different users so that the identification of individual trajectory data is converted into a k-anonymity problem [53, 200, 202]. For example, a recent Privacy-Preserving Trajectory Framework (PPTPF) [203] applies the k-indistinguishability to anonymize trips for each user by condensing them into

$k-1$ trajectories and determining $k-1$ anonymized clusters of trips.

The other stream focuses on synthetic data generation [204–207]. Synthetic data generation methods have been extensively studied in recent years as a way of tackling privacy concerns of location-based datasets. The majority of existing mobility synthesis schemes are mainly categorized into two approaches: one is a more traditional, simulation-based approach, while the other is a more recent, neural network-based generative modelling approach that utilizes recurrent autoencoders and generative adversarial networks to produce realistic trajectories [208]. Simulation-based approaches generate mobility traces by modelling overall user behaviour as a stochastic process, such as a Markov chain model of transition probabilities between locations, and then drawing random walks, potentially with additional stochastic noise added, as demonstrated in Xiao *et al.* [209]. These approaches require considerable feature engineering effort and struggle to capture longer-range temporal and spatial dependencies in the data [210] and are thus limited in their ability to preserve the utility of the original datasets. In contrast, the generative neural network approach synthesizes user mobility traces by learning via gradient descent back-propagation, and then the optimal weights are utilized for decoding a high-dimensional latent vector representation into sequences that closely resemble the original data. Such traces can maintain important statistical properties of the original data while taking advantage of noise introduced in the reconstruction process, to improve data subject anonymity. Huang *et al.* [205] demonstrates the use of a variational autoencoder network to reconstruct trajectory sequences, while Ouyang *et al.* [207] utilizes a convolutional GAN, but neither work directly makes a quantitative assessment of the extent of privacy protection that their algorithms provide [205, 207]. The TrajGAN by Rao *et al.* [54] is a state-of-the-art example of the generative trajectory modelling approach, which quantifies its privacy protection by demonstrating a significant decline in the performance of a second user ID classifier model on the synthetic outputs compared to the original input trajectories. For these reasons, I use TrajGAN as a baseline for comparison.

My proposed model takes the neural network-based generative modelling approach, but differs from existing methods, where I utilize a combined, multi-task adversarial neural network to simultaneously reconstruct trajectories, predict next locations, and re-identify users, from the same learned latent vector representation. I seek an optimal trade-off between the three tasks' individual losses by optimizing a sum loss function with per-task weights, improving the controllability of the relative utility and privacy of the outputs.

4.3 Preliminaries

4.3.1 Generative Adversarial Network

Generative adversarial network, also known as GAN for short, is a popular machine learning framework for estimating generative models G via adversarial process D, designed by Goodfellow *et al.* in 2014 [211]. In general, GAN simultaneously trains generative models G and discriminative model D in the form of a zero-sum game. To be specific, considering the contest operates in terms of data distribution, the generative model generates fake data based on real data with distribution p_g while the discriminative model distinguishes real from the fake one. Typically, the objective of the generative model is to generate data as realistically as possible to fool the discriminate model, while the objective of the discriminate model is to maximize the probability of assigning the correct label to real samples and fake ones from G. Formally, the two-player minimax game between D and G can be expressed as value function $V(G, D)$:

$$\min_G \max_D V(D, G) = \mathbb{E}_{\boldsymbol{x} \sim p_{data}(\boldsymbol{x})}[\log D(\boldsymbol{x})] + \mathbb{E}_{\boldsymbol{z} \sim p_{\boldsymbol{z}}(\boldsymbol{z})}[\log(1 - D(G(\boldsymbol{z})))] \tag{4.1}$$

4.3.2 Differential Privacy

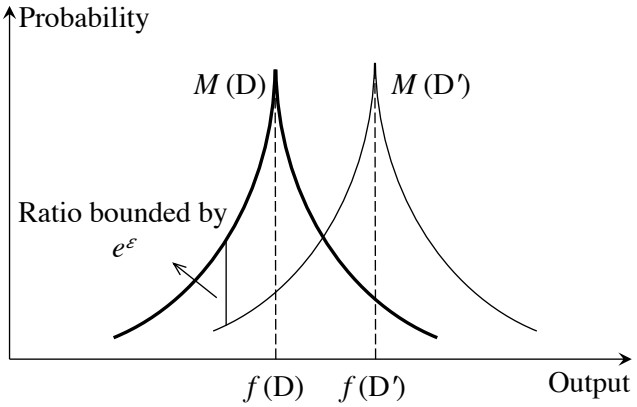


Figure 4.2: Illustration of differential privacy definition with Laplace-distributed noise. $M[D]$ represents the probability of receiving a certain c give D; $M[D']$ represents the probability of receiving a certain c give D'; for every c, the ratio of $Pr(M[D] = c)$ and $Pr(M[D'] = c)$ must be bounded by e^{ϵ}.

Motivated by the increasing need for a robust, meaningful, and mathematically rigorous definition of privacy, differential privacy is proposed by Dwork in 2006 [190].

Definition 1. *Adjacent Databases: Database D and D' are considered neighbours if they are differed by only a single record.*

$$||D' - D||_1 \leq 1 \tag{4.2}$$

Definition 2. *Differential Privacy 1 [190]: A mechanism $M[\cdot]$ is ϵ-differential private if f or all possible output S $\in$ Range [M], and all adjacent databases D, D'.*

$$\frac{P_r(M[D] \in S)}{P_r(M[D'] \in S)} \leq e^{\epsilon} \tag{4.3}$$

Definition 3. *Differential Privacy 2 [190]: A mechanism $M[\cdot]$ is (ϵ, δ)-differential private if for all possible output S $\in$ Range [M], and all adjacent databases D, D'.*

$$P_r(M[D] \in S) \leq e^{\epsilon} P_r(M[D'] \in S) + \delta \tag{4.4}$$

As shown in Figure 4.2, the ϵ parameter is the privacy budget and controls the privacy loss when $M[\cdot]$ is run on the D. $M[D]$ represents the probability of receiving a certain c give D; $M[D']$ represents the probability of receiving a certain c give D'; for every c, the ratio of $Pr(M[D] = c)$ and $Pr(M[D'] = c)$ must be bounded by e^{ϵ}. A larger ϵ represents weaker assurances of privacy. That is, the probability for $M[D]$ is much higher than $M[D']$, which means they are more distinguishable.

4.3.3 Laplace Mechanism

The Laplace mechanism is one of the most classic mechanisms developed based on differential privacy. It takes a deterministic function $f[\cdot]$ of a database D and Laplace-distributed noise is added to the result $M_L[D]$ to make it ϵ-differential private.

Consider the private data $x \in D$, the Laplace mechanism is defined as:

$$M_L(D, \epsilon) = D + Lap(\frac{s}{\epsilon}) \tag{4.5}$$

The term s is the sensitivity of $f[\cdot]$, which represents the output of $f[\cdot]$ change when its input changes by 1. As $M_L[\cdot]$ is differentially private, it provides plausible deniability of the true result, hence, larger noise brings better privacy protection, but a higher expense of accuracy degradation.

There are other definitions of differential privacy. For example, the exponential mechanism is able to provide differentially private protection to results whose responses are non-numeric. The Gaussian mechanism, which is adding Gaussian noise instead of Laplace noise, only satisfies a weaker form of differential privacy, (ϵ, δ)-differential privacy.

4.4 Design of Mo-PAE

4.4.1 Definition of Important Terms

Mobility Trace

The raw geolocated data or other mobility data commonly contain three elements: user identifiers $u \in U$, timestamps $t \in T$, and location identifiers $l \in L$. Hence, each location record *r* could be denoted as $r_{(u,i)} = [u, t_i, l_i]$, while each location sequence *S* is a set of ordered location records $S_{(u,n)} = \{r_{(u,1)}, r_{(u,2)}, r_{(u,3)}, \cdots, r_{(u,n)}\}$, namely *mobility trace* of *user u*. Therefore, given the past mobility trace $S_{(u,n)}$, the mobility prediction task is to infer the most likely location l_{n+1} at the next timestamp t_{n+1} for the user u. The data fed into the proposed architecture are a list of traces with a specific sequence length (*i.e.*, *SL*). For instance, if the sequence length is 10, that indicates each trace contains 10 history location records *r*, $S_{10} = \{r_1, r_2, r_3, \cdots, r_{10}\}$, and $SL = 10$. In this thesis, I assume that different users' mobility traces are collected and aggregated (denoted as data X) by trusted telecom operators or social platforms and shared with third-party SPs.

User Re-identification

The user re-identification risk arises because of the high uniqueness of human traces [29] and could be the origin of many unexpected privacy leakages. I assume each trace *S* is originally labeled with a corresponding user identifier *u*, and the user re-identification is to infer the user *u* to whom the target trace $S_n = \{r_1, r_2, r_3, \cdots, r_n\}$ belongs. I thereby leverage the user identifiers *u* as the ground-truth values for the user identity classes. This identity information is what I want to protect in the proposed adversarial network.

4.4.2 Problem Definition

Definition of Utility and Privacy

On the one hand, mobility datasets are of great value for understanding human behaviour patterns, smart transportation, urban planning, public health issue, pandemic management, etc. Many of these applications rely on the next location forecasting of individuals, which in the broader context, can provide an accurate portrayal of citizens' mobility over time and inform the allocation of public resources and community services. Therefore, in this thesis, I focus on the capability of *mobility prediction* (*next location forecasting*) and leverage the accuracy of the prediction as an important metric for quantifying the *data utility*. On the other hand,

with increasing intelligent devices and sensors being utilized to collect information about human activities, the traces also increasingly expose intimate details about users' lives, from their social life to their preferences. In this manner, the capability of user re-identification is important to balance the risks and benefits of mobility data usage, for all data owners, third parties, and researchers. I then leverage the efficient reduction of data reconstruction risk and user re-identification risk as the *privacy protection* metrics. Moreover, research in [187] shows that the predictability of users' mobility, and the particular constraints of users' movements, are sufficient to reconstruct and/or identify anonymous or perturbed locations [187]. This confrontation makes the trade-off between keeping mobility predictability and reducing the chance of user re-identification more interesting. For instance, an adversary can re-identify anonymous users' traces given the users' mobility profile [212]; infer the users' next activities from the frequency of location visits [177]; even obtain the personal home or working address from the trajectories [213].

In this chapter, I design a model to protect location privacy regarding users' identity and data integrity while simultaneously minimizing the service quality (*i.e.*, accuracy of next location forecasting) degradation stemming from the obfuscation of true data. Specifically, users' mobility traces are collected and fed into this proposed model, encoded as privacy-preserving representations that allow third parties and other SPs freely access. At the same time, two built-in adversaries, which try to achieve maximum accuracy in user re-identification and trace reconstruction during the adversarial training, are simulating the strong privacy adversaries that can attain disclosed sensitive information and examine the quality of feature representations instantly. Overall, the encoded privacy-preserving representations should retain as little user-identifiable information as possible, as well as the data reconstruction information, to decrease the user re-identification accuracy and increase the location obfuscation.

Hence, I summarize the *Utility*, *Privacy I* and *Privacy II* of the encoded feature representations as follows:

Utility (U): the encoded representations should retain information about mobility predictability (*i.e.*, forecasting accuracy, higher accuracy indicates higher utility).

Privacy I (PI): the encoded representations should contain little information advantage to the data reconstruction (*i.e.*, more information loss in the reconstruction process); represented as the distortion increment (*i.e.*, *Euclidean* [214] and *Manhattan* distance [215]) between the reconstructed data X' and the original data X.

Privacy II (PII): the encoded representations should contain little information advantage to the user re-identification task (*i.e.*, the user de-identification effectiveness); measured by the degradation of the user re-identification accuracy.

Privacy vs. Utility Trade-off

An effective LPPM must consider three fundamental elements: i). the privacy requirements of the users (namely *privacy gain*); ii). the adversary's knowledge and capabilities; iii). and maximally tolerated service quality degradation stemming from the obfuscation of true locations (namely, *utility loss*) [187]. There is an inherent trade-off between location privacy protection and utility degradation [201]. That is, achieving a better level of privacy protection may require sacrificing the service quality provided by the data. Such a trade-off is omnipresent in various privacy protection mechanisms, especially in location obfuscation mechanisms. Higher privacy protection is achieved when the probability of an adversary inferring the true location of the user decreases, however, the result of a query based on the obfuscated location is significantly different from the actual interest of the user. The privacy-utility trade-off, hence, needs to be examined and analyzed to guarantee the efficiency of the privacy protection mechanism.

In this thesis, *utility loss* denotes the accuracy degradation after the proposed privacy protection mechanism is applied, and the *privacy gain* (in terms of *PI* and *PII*) quantifies the protected privacy information. To be specific, a more obfuscated dataset will tend to perform better at preserving privacy, but worse at preserving utility, and vice versa. Hence, monitoring these two performance metrics in tandem allows users to select the optimal privacy-utility trade-off for their use cases, given their hyperparameter selections. The Mo-PAE model is designed to train a features Encoder $Enc_L(X)$ that could convey more information on the utility but less on privacy and investigate a better trade-off between them. More details will be discussed in the following sub-section.

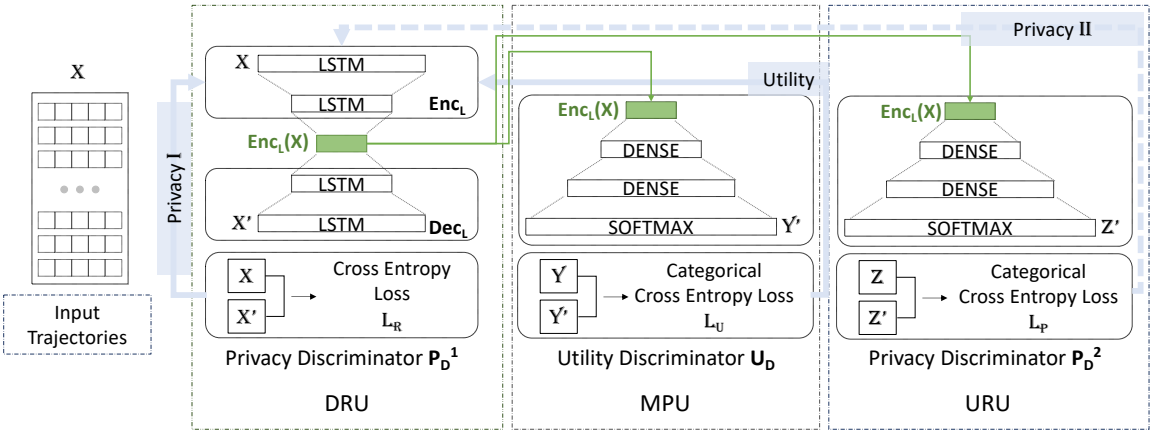
4.4.3 Mo-PAE Overview

The proposed **p**rivacy-preserving **a**dversarial feature **e**ncoder on mobility data, denoted as the *Mo-PAE*, is based on representation learning and adversarial learning and aims to ease data sharing privacy concerns. Figure 4.3 presents the basic workflow of the proposed Mo-PAE. It composes of three crucial units: data reconstruction risk unit (DRU), mobility prediction unit (MPU), and user re-identification risk unit (URU).

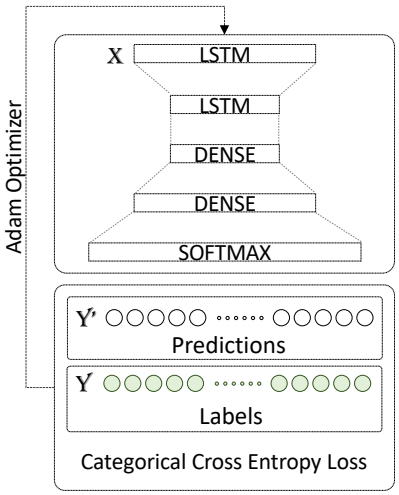
Composition Units of Mo-PAE

I. Mobility Prediction Unit (*MPU*):

The MPU unit is composed of three parts, the input part with the multi-modal embedding of trace information, the sequential part with LSTM layers [216], and an output part with the softmax activation function. As per the definition mentioned earlier, the traces in this chapter



(a) Mo-PAE



(b) Optimal-IMs

Figure 4.3: (a) Schematic overview of the proposed privacy-preserving adversarial architecture (Mo-PAE), consisting of data reconstruction risk unit (DRU), mobility prediction unit (MPU), and user re-identification risk unit (URU); (b) The baseline LSTM network for optimal classifiers (Optimal-IMs).

are shown as location sequences S. First, the location identifiers l and timestamps t are converted into one-hot vectors. I then employ LSTM layers to model the mobility patterns and sequential transition relations in these mobility traces. As a prominent variant of the recurrent neural network, LSTM networks exhibit brilliant performance in modelling the entire data sequences, especially for learning long-term dependencies via gradient descent [217]. Following the sequential module, the softmax layer outputs the probability distribution of the prediction results. This probability distribution is converted to the top-n accuracy metrics to illustrate the unit performance.

II. Data Reconstruction Risk Unit (*DRU*):

The DRU is the encoder Enc_L unit in reverse, also denoted as Dec_L, which is regarded as

the first *privacy discriminator* P_D^1 in the proposed architecture. It is designed to evaluate the distance $d(\cdot,\cdot)$ (*i.e.*, *Privacy I*) between the reconstructed data X' and the original input data X. A malicious party is free to explore any machine learning model and reconstruct the data if they have the shared extracted features f. I use a layer-to-layer reverse architecture of the proposed encoder Enc_L to build the *data reconstruction unit* to act as a robust built-in adversary. To compare with baseline models and keep the comparison in a line, I measure the distance $d(\cdot,\cdot)$ between the X and X' by leveraging the *Euclidean* and *Manhattan* distance as the metrics. Both of them are widely used in location privacy literature [53, 176].

III. User Re-identification Risk Unit (*DRU*):

The URU is regarded as the second *privacy discriminator* P_D^2 in the proposed architecture. The unit is composed of three parts, the input part with the one-hot embedding of user identity, the sequential part with LSTM layers, and an output part with softmax function. First, the user identity list is converted into one-hot vectors. Similar to the MPU, the URU also applies LSTM layers to better extract the spatial and temporal characteristics of the context. A softmax function with a cross-categorical entropy loss function is applied to output a categorical probability distribution of the user re-identification task. I then use the top-n accuracy of this classifier as the metric of user re-identification privacy risk (*i.e.*, *Privacy II*). The more accurately a classifier can re-identify the user when given a trajectory, the higher the risk of disclosing private data. Same as P_D^1, P_D^2 is designed as the built-in adversary to infer the ability of generated features in protecting users' sensitive information.

The overall architecture eventually learns to fool both built-in adversaries, P_D^1 and P_D^2, while maintaining mobility predictability. In this manner, both adversaries are assumed to be free to access the exclusive feature representations and the entire encoder network, which allows them to have the optimal decoder setting. I will discuss the effectiveness of two privacy inference attacks in Section 4.6.3.

Overall Design

When three units train concurrently, the MPU is regarded as the *utility discriminator* U_D, while DRU and MPU act as two built-in adversaries and are regarded as the two *privacy discriminators*, P_D^1 and P_D^2, respectively. The built-in adversary has been used as an effective adversarial regularization to prevent inference attacks, *e.g.* in the classification setting [218] or in various GAN models [219] for privacy-preserving purpose. In the proposed mechanism, P_D^1 and P_D^2 are simulating malicious SPs, who attempt to obtain sensitive information (*i.e.*, maximize the accuracy of privacy inference tasks), while the encoder Enc_L is trained to produce feature representations f to the advantage of U_D but to the disadvantage of P_D^1 and P_D^2, by jointly optimizing the hybrid losses of the DRU, MPU, and URU simultaneously, during ad-

versarial training. Therefore, in the Mo-PAE, the encoder Enc_L, and three discriminators U_D, P_D^1, P_D^2 play a multi-player game to minimaximize the value function $V(Enc_L, U_D, P_D^1, P_D^2)$:

$$\begin{aligned}&\min_{(Enc_L,U_D)}\max_{(P_D^1,P_D^2)} V(Enc_L, U_D, P_D^1, P_D^2) = \mathbb{E}_{x\sim X}[logU_D(Enc_L(x))]+\\&\mathbb{E}_{x\sim X}[log(1-P_D^1(Enc_L(x)))] + \mathbb{E}_{x\sim X}[log(1-P_D^2(Enc_L(x)))]\end{aligned} \tag{4.6}$$

As described in Equation 4.6, I design a multi-task adversarial network to learn an LSTM-based encoder $Enc_L(X;\theta)$ with parameter set $\theta \in \Theta$, which can generate the optimized feature representations $f = Enc_L(X;\theta)$ via lowering the privacy disclosure risk of user identification information and improving the task accuracy (*i.e.*, mobility predictability) concurrently. Two potential malicious privacy leakages from URU and DRU, are attempted to retrieve sensitive information from the feature representations f. As built-in adversaries, they have full access to the feature representations f and the entire encoder network with parameter set $f = Enc_L(X;\theta)$. In this manner, they have the optimal decoder setting. Hence, the notion of privacy (*privacy gain*), is measured by the decline of the effectiveness of target inference attacks (*i.e.*, user re-identification attack and data reconstruction attack).

Details of Mo-PAE

I define the raw mobility data I want to protect as $\mathcal{X}$, trained features as $\mathcal{F}$, and reconstructed data as $\mathcal{X}'$. Given mobility raw data $\mathcal{X}$ for P_D^1 (DRU), the ground-truth label z_i for P_D^2 (URU), and the ground-truth label y_i for utility U_D (MPU), I train the encoder Enc_L to learn the representation $\mathcal{F} = Enc_L(\mathcal{X};\theta_E)$. I design a specific loss function, namely *sum loss* $\mathcal{L}_{sum}$, for this optimization process.

Specifically, when reconstructing the data $\mathcal{X}'$, a decoder Dec_L attempts to recreate the data based on the features $\mathcal{F}$, that is $Dec_L(\mathcal{F};\theta'_D) : \mathcal{F} \to \mathcal{X}'$. This DRU, the first privacy discriminator P_D^1, is trained as a built-in adversary and tries to achieve sensitive information as much as possible. Hence, the DRU is primarily trained by minimizing the reconstruction loss $\mathcal{L}_{\mathcal{R}}$:

$$\min \mathcal{L}_{\mathcal{R}} \Rightarrow \mathcal{L}_{\mathcal{R}} = d(\mathcal{X}, \mathcal{X}') = \underset{\mathcal{F};\theta'_R}{\operatorname{argmin}} \|Dec_L(\mathcal{F}, \theta'_R) - \mathcal{X}\|^2 \tag{4.7}$$

The URU, the second privacy discriminator $P_D^2(\mathcal{F};\theta')$, is trained to re-identify to whom the target trajectory belongs. It outputs a probability distribution of predicted user identifiers among Z potential classes. Then in this privacy discriminator, the user re-identification loss $\mathcal{L}_{\mathcal{P}}$

is primarily trained to minimize, denoted as min $\mathcal{L}_{\mathcal{P}}$:

$$\min \mathcal{L}_{\mathcal{P}} \Rightarrow \mathcal{L}_{\mathcal{P}} = \underset{\mathcal{F};\theta'_P}{\operatorname{argmin}} \sum_{i=1}^{\mathbf{Z}} z_i \log(P_D^1(\mathcal{F};\theta'_P)) \tag{4.8}$$

The MPU, the utility discriminator $U_D(\mathcal{F};\theta')$, is trained to output a probability distribution of the next location of interest, and this distribution has Y potential classes. Discriminative training of U_D maximizes the prediction accuracy by minimizing the utility loss $\mathcal{L}_{\mathcal{U}}$ concurrently with minimizing the $\mathcal{L}_{sum}$, denoted as min $\mathcal{L}_{\mathcal{U}}$.

$$\min \mathcal{L}_{\mathcal{U}} \Rightarrow \mathcal{L}_{\mathcal{U}} = \underset{\mathcal{F};\theta'_U}{\operatorname{argmin}} \sum_{i=1}^{\mathbf{Y}} y_i \log(U_D(\mathcal{F};\theta'_U)) \tag{4.9}$$

The overall training is to achieve a privacy-utility trade-off by adversarial learning on $\mathcal{L}_{\mathcal{R}}$, $\mathcal{L}_{\mathcal{U}}$, and $\mathcal{L}_{\mathcal{P}}$, concurrently. The encoder $Enc_L(\mathcal{X};\theta_E)$ should satisfy high predictability (*min* $\mathcal{L}_{\mathcal{U}}$) and low user re-identification accuracy (*max* $\mathcal{L}_{\mathcal{P}}$) of the mobility data when maximizing the reconstruction loss (*max* $\mathcal{L}_{\mathcal{R}}$) in reverse engineering, where the training objective transformed from Equation 4.6 can be written as:

$$\min \mathcal{L}_{sum} = \min_{\mathcal{L}_U} \max_{\mathcal{L}_R,\mathcal{L}_P} (\sum_{x=i}^{\mathcal{X}} \left(\mathcal{L}_U\left(f_i\right), \mathcal{L}_P\left(f_i\right), \mathcal{L}_R\left(f_i\right)\right)) \tag{4.10}$$

I use Equation 4.10 to guide the first version of Mo-PAE, denoted as *Model I*. In order to fully investigate the range of trade-offs, I leveraged the Lagrange multipliers [147] as hyperparameters to control the privacy-utility trade-offs in the Mo-PAE, and this weighted-controlled model is denoted as *Model II*. Accordingly, the optimization function of the training objective is:

$$\begin{aligned}
\min \mathcal{L}_{sum} &= \min_{\mathcal{L}_U} \max_{\mathcal{L}_R,\mathcal{L}_P} (\sum_{x=i}^{\mathcal{X}} \left(\lambda_1\mathcal{L}_R\left(f_i\right), \lambda_2\mathcal{L}_U\left(f_i\right), \lambda_3\mathcal{L}_P\left(f_i\right)\right)) \\
&= \underbrace{-\lambda_1\left(\max \mathcal{L}_{\mathcal{R}}\left(f_i\right)\right)}_{\text{Privacy I}} + \underbrace{\lambda_2\left(\min \mathcal{L}_{\mathcal{U}}\left(f_i\right)\right)}_{\text{Utility}} \underbrace{-\lambda_3\left(\max \mathcal{L}_{\mathcal{P}}\left(f_i\right)\right)}_{\text{Privacy II}} \\
&= -\lambda_1 \| Dec_L(\mathcal{F}) - \mathcal{X} \|^2 + \lambda_2(\sum_{i=1}^{\mathbf{Y}} y_i \log(U_D(\mathcal{F}))) \\
&- \lambda_3(\sum_{i=1}^{\mathbf{Z}} z_i \log(P_D(\mathcal{F})))
\end{aligned} \tag{4.11}$$

where y_i is the ground-truth label for *Utility*, z_i is the ground-truth value for *Privacy II*; λ_1, λ_2 and λ_3 are non-negative, real-valued weights, as the hyperparameters that control the privacy-utility trade-off in the Mo-PAE.

Algorithm 1: Training of the Mo-PAE (*Model II*)

Input : Mobility data **X**, real mobility prediction labels **Y**, real user identification labels **Z**, weights: λ_1, λ_2, λ_3

Output: Adversarial Encoder $Enc_L(X; \theta_E, \theta_R, \theta_U, \theta_P)$

Initialize model parameters $\theta_E, \theta_R, \theta_U, \theta_P$;
for *n epochs* **do**
  for $k = 1, \cdots, K_t$ **do**
    1. Sample a mini-batch of mobility trajectories x, prediction labels y, identification labels z
    2. Update θ_E with Adam optimizer on mini-batch loss $L_{sum}(\theta_E, \theta_R, \theta_U, \theta_P, \lambda_1, \lambda_2, \lambda_3)$
    3. Update θ_R with Adam optimizer on mini-batch loss $L_R(f; \theta_R)_{(x,\hat{x})}$: min L_R
    4. Update θ_U with Adam optimizer on mini-batch loss $L_U(f; \theta_U)_{(y,\hat{y})}$: min L_U
    5. Update θ_P with Adam optimizer on mini-batch loss $L_P(f; \theta_P)_{(z,\hat{z})}$: min L_P
  end
  Update with the gradient descent on $L_{sum}(\theta_E, \theta_R, \theta_U, \theta_P, \lambda_1, \lambda_2, \lambda_3)$: min L_{sum}
end

As shown in the Algorithm 1, the gradient of the loss (*i.e.*, θ_E, θ_R, θ_U, θ_P) back-propagates through the LSTM network to guide the training of the encoder Enc_L. The encoder is updated with the *sum loss* function $\mathcal{L}_{sum}$ until convergence. It is tricky to investigate all possible weight combinations practically, and I look for the optimal combinations through training [182] with Equation 4.11 by brute-force evaluation. Then I approximate the required data utility reserved and reformulate the optimization problem in Equation 4.11 as a maxima privacy optimization problem.

$$\begin{aligned} &\min_{Enc_L(P_D^1, P_D^2)} \max V_{\lambda \to U_D}(Enc_L, P_D^1, P_D^2) = \mathbb{E}_{x \sim X}[log(1 - P_D^1(Enc_L(x)))] \\ &+ \mathbb{E}_{x \sim X}[log(1 - P_D^2(Enc_L(x)))] \end{aligned} \tag{4.12}$$

Additionally, another key contribution is the flexibility of the *sum loss* function $\mathcal{L}_{sum}$, which could be regulated to satisfy different requirements on privacy protection level and service quality. That is, different combinations of weights control the relative importance of each unit and guide the overall model to find the maxima or minima given the specific trade-off choices.

4.5 Experimental Setting

4.5.1 Datasets

Experiments are conducted on four representative mobility datasets: Mobile Data Challenge Dataset (MDC) [220], Priva'Mov [221], GeoLife [222], and FourSquare [223].

MDC: it is recorded from 2009 to 2011 and contains a large amount of continuous mobility data for 184 volunteers with smartphones running a data collection software in the Lausanne/Geneva area. Each record of the *gps-wlan* dataset represents a phone call or an observation of a WLAN access point collected during the campaign [220].

Dataset-City	Bounding Box				Record Counts		Number	
	Latitude		Longitude		Train	Test	User ID	POI
MDC-Lausanne	46.50	46.61	6.58	6.73	77393	19429	143	149
Priva'Mov-Lyon	45.70	45.81	4.77	4.90	62077	16859	58	129
GeoLife-Beijing	39.74	40.07	116.23	116.56	95038	24578	145	960
FourSquare-NYC	40.55	40.99	-74.28	-73.68	43493	11017	466	1712

Table 4.1: Overview of four mobility datasets after pre-processing. The bounding box represents the range of the considered locations/traces.

Priva'Mov: the PRIVA'MOV crowd-sensing campaign took place in the city of Lyon/France, from October 2014 to January 2016. Data collection was contributed by roughly 100 participants, including university students, staff, and family members. The crowd-sensing application collected GPS, WiFi, GSM, battery, and accelerometer sensor data. For this thesis, I only used the GPS traces from the dataset [221].

GeoLife: it is collected by Microsoft Research Asia from 182 users in the four-and-a-half-year period from April 2007 to October 2011 and contains 17,621 trajectories [222]. This dataset recorded a broad range of users' outdoor movements, including life routines like going home and going to work and some entertainment and sports activities, such as shopping, sightseeing, dining, hiking, and cycling. It is widely used in many research fields, such as mobility pattern mining, user activity recognition, location-based social networks, location privacy, and location recommendation.

FourSquare NYC: it contains check-ins in NYC and Tokyo collected during the approximately ten months from 12 April 2012 to 16 February 2013, containing 227,428 check-ins from 1,083 subjects in New York City [223].

Once imported into the proposed architecture, each dataset was filtered and pre-processed individually to derive their respective train and test sets illustrated in Table 4.1. I filter locations to a bounding box defining a city or region of interest and then transform continuous GPS coordinates by tessellating the space and encoding location as a discrete grid position to attain the location identifiers (*i.e.*, POI). In these spatial transformations, I convert the GPS coordinates to the discretizing locations via the Geohash algorithm [224] with rectangular cells. For instance, each bounding box defines the grid size of the interested region, and the grid granularity is 0.01 degrees, where each grid represents a 0.01 longitude $\times$ 0.01 latitude area.

4.5.2 Baseline Models

I. Optimal Inference Models (Optimal-IMs)

Optimal-IMs comprise three independent inference models, namely the data reconstruction model, mobility prediction model, and user re-identification model. Each model has a sim-

ilar layer design as the corresponding unit in the Mo-PAE, however, these three models are completely independent and have no effect on each other. Unlike the Mo-PAE, which leverages adversarial learning to finally attain an extracted feature representation f that satisfies the utility requirements and privacy budgets simultaneously, the Optimal-IMs are only trained for optimal inference accuracy at the individual tasks to characterize the original data.

II. LSTM-TrajGAN (TrajGAN) [54]

It is an end-to-end deep learning model to generate synthetic data which preserves essential spatial, temporal, and thematic characteristics of the real trajectory data. Compared with other standard geo-masking methods, TrajGAN can better prevent users from being re-identified. The TrajGAN work claims to preserve essential spatial and temporal characteristics of the original data, verified through statistical analysis of the generated synthetic data distributions, which aligns with the mobility prediction-based utility metric in this thesis. Hence, I train an optimal mobility prediction model for each dataset and evaluate the mobility predictability of synthetic data generated by the TrajGAN. In contrast to the TrajGAN that aims to generate synthetic data, the proposed Mo-PAE is training an encoder Enc_L that forces the extracted representations f to convey maximal utility while minimizing private information about user identity via adversarial learning.

III. GI-DP [193]

The principle of geo-indistinguishability (*i.e.*, GI) [53], is a formal notion of privacy that protects the user's exact location with a level of privacy that depends on radius r, which corresponds to a generalized version of differential privacy (DP). GI-DP is a mechanism for achieving geo-indistinguishability when the user releases his location repeatedly throughout the day. It fulfils desired protection level by perturbing the actual location with random noises and achieving an optimal trade-off between privacy and utility (*i.e.*, service quality). I re-implement the geo-indistinguishability of optimal utility with graph spanner [193], namely GI-DP in this thesis, to attain the released version data that satisfied the DP guarantees. I then train a series of Optimal-IMs to evaluate the effectiveness of target inference attacks on the released version data in a line to compare with the proposed mechanism.

4.5.3 Training

Training of Mo-PAE

The main goal of the proposed adversarial network is to learn an efficient feature representation based on the utility and privacy budgets, using all users' mobility histories. In most experiments in this chapter, the trajectory sequences consist of 10 historical locations with timestamps (*i.e.*, $SL = 10$), and the impact of the varying sequence lengths is discussed in Section 4.7.2. After data pre-processing, 80% of each user's records are segmented as the training set and the remaining 20% as the testing set. I utilize the mini-batch learning method with a size of 128 to train the model until the expected convergence. I take a gradient step to optimize the *sum loss* L_{sum} (*i.e.*, Equation 4.11) in terms of L_R, L_U, and L_P concurrently. Meanwhile, the *sum loss* L_{sum} is optimized by using the Adam optimizer. All the experiments are performed with the Tesla V100 GPU; a round of training would take 30 seconds on average, and each experiment trains for 1000 rounds.

Training of the TrajGAN

To provide a state-of-the-art machine learning-based model for comparison, I re-implement the TrajGAN model described in [54] using the same hyperparameters, setting latent vector dimension to 100, using 100 LSTM units per layer, a batch size of 256, utilizing the Adam optimizer with learning rate 0.001 and momentum 0.5, and training for 200 epochs (where one epoch is a pass through the entire training set). I train TrajGAN independently on the training split of each benchmark mobility dataset and then use it to generate synthetic trajectories from the test set. Then I train the proposed Mo-PAE on the same training data and use it to generate a feature extraction from the same test data. Finally, I evaluate the performance of the user re-identification unit and mobility prediction unit on the real and synthetic test sets generated by TrajGAN and compare the changes in accuracy to assess the relative utility and privacy of the TrajGAN and Mo-PAE.

Training of the DP-GI

I re-implement the DP-GI model described in [193] using the default settings. That is, I set $epsilon\ \epsilon = 0.5$, $dilation\ \delta = 1.1$, the *distance matrix* d_x is defined by Euclidean distance. From [193], let X be a set of locations with metric d_x, and let $G(X, E)$ be a $\delta - spanner$ of X, if a mechanism K for X is $\frac{\epsilon}{\delta} d_G$-private, then K is ϵd_x-private. The dilation of G is calculated as:

$$\delta = \max_{x \neq x' \in X} \frac{d_G(x, x')}{d_x(x, x')} \tag{4.13}$$

$$d_G(x, x') \geq d_x(x, x') \quad \forall x, x' \in X \tag{4.14}$$

I re-implement the GI-DP to attain the released version data that satisfied the DP guarantees. I then train a series of Optimal-IMs to evaluate the effectiveness of target inference attacks on the released version data in a line to compare with the proposed mechanism.

4.5.4 Metrics

I set *Euclidean* [214] and *Manhattan* distance [215] as the evaluation metrics for the DRU to evaluate the quality of the reconstructed data X' generated from extracted features f. Both distance metrics are widely used in location privacy literature [53, 176]. For instance, the work introducing Geo-Indistinguishability [53] utilizes a privacy level that depends on the *Euclidean* distance. *Euclidean* distance gives the shortest or minimum distance between two points. In contrast, *Manhattan* distance applies only if the points are arranged in a grid, and both definitions are feasible for the problem I am working on. Note that these two distances have limited capability in showing the quality of the reconstructed data X', however, they intuitively capture the differences between the original data X and the reconstructed data X'.

For both MPU and URU, I leverage the top-n accuracy as the evaluation metric. The accuracy of the MPU is one of the most important factors in evaluating the utility of the extracted feature representation *f*, where predictability of the f increases as much as it can during the adversarial training. On the other hand, the competing training objective is to decrease the accuracy of the user re-identification unit to enhance the privacy of *f*. The top-n metric computes the number of times the correct label appears among the predicted top n labels. The top-n metric takes n predictions with higher probability into consideration, and it classifies the prediction as correct if one of them is an accurate label. The top-1 to top-5 accuracies are leveraged in this chapter to discuss the performance of the proposed model.

4.6 Architecture Evaluation

In this section, I present the comparison results between the proposed Mo-PAE and three baseline models under the same training setting. The evaluation in this section is mainly on the trade-off between U and PII, as the main contribution of the Mo-PAE is to protect users' identities, while I also consider the scope of users' locations as an auxiliary measurement.

Datasets	Models		Privacy I		Utility (% for loss)			Privacy II (% for gain)			Utility-PII trade-offs (%)
			Euc	Man	top-1	top-3	top-5	top-1	top-3	top-5	
MDC	Optimal-IMs		0.0000	0.0000	0.9347	0.9837	0.9922	0.9247	0.9819	0.9911	-
	TrajGAN		0.0434	3.6923	-46.32%	-24.16%	-15.98%	+20.32%	+8.13%	+4.02%	-26.00%
	GI-DP		**0.2341**	**56.8764**	-97.34%	-93.25%	-89.44%	**+97.47%**	**+93.71%**	**+90.12%**	0.13%
	Mo-PAE	I	0.0025	0.4501	-54.56%	-34.74%	-25.10%	+69.80%	+50.44%	+39.95%	15.24%
		II	0.0697	13.6168	**-13.43%**	**-6.26%**	**-3.95%**	+65.51%	+45.11%	+34.86%	**52.08%**
Priva'Mov	Optimal-IMs		0.0003	0.0058	0.9482	0.9878	0.9954	0.5643	0.8215	0.8765	-
	TrajGAN		0.0815	9.6843	-6.60%	-1.89%	-0.93%	+14.17%	+14.35%	+8.88%	7.57%
	GI-DP		0.1899	**38.6712**	-91.20%	-83.53%	-72.37%	**+85.49%**	**+63.80%**	**+53.31%**	-5.71%
	Mo-PAE	I	0.0009	0.0437	**-3.36%**	**-1.59%**	**-0.81%**	+27.02%	+14.19%	+9.19%	23.66%
		II	**0.2347**	10.2239	-10.81%	-6.83%	-4.91%	+35.29%	+14.97%	+10.05%	**24.48%**
Geolife	Optimal-IMs		0.0008	0.0670	0.4705	0.6842	0.7636	0.6572	0.8690	0.9294	-
	TrajGAN		0.4010	50.3620	-62.31%	-50.45%	-43.72%	+66.73%	+47.89%	+37.22%	4.42%
	GI-DP		**1.2332**	**312.9972**	-97.74%	-96.56%	-95.36%	**+91.57%**	**+84.13%**	**+78.65%**	-6.17%
	Mo-PAE	I	0.0006	0.0310	-31.45%	-25.02%	-21.90%	+54.88%	+39.59%	+30.81%	23.43%
		II	0.4351	89.2209	**-21.13%**	**-18.78%**	**-17.11%**	+55.49%	+40.40%	+32.34%	**34.36%**
FourSquare	Optimal-IMs		0.0052	0.6691	0.6468	0.8210	0.8823	0.8780	0.9735	0.9892	-
	TrajGAN		**1.4341**	**117.9181**	-26.30%	-22.30%	-18.75%	+51.86%	+32.49%	+23.49%	25.56%
	GI-DP		0.5826	86.096	-69.35%	-59.23%	-53.36%	**+77.29%**	**+66.58%**	**+59.82%**	7.94%
	Mo-PAE	I	0.0060	0.7845	-51.05%	-41.45%	-35.20%	+53.47%	+35.26%	+25.86%	2.42%
		II	0.7985	99.9212	**-2.54%**	**-3.14%**	**-2.84%**	+51.08%	+34.39%	+26.16%	**48.54%**

Table 4.2: Performance comparison between Mo-PAE with other baseline models. The *Model I* is the proposed architecture without weights, and the *Model II* is the one with multipliers ($\lambda_1 = 0.1$, $\lambda_2 = 0.8$, and $\lambda_3 = 0.1$). The results shown in this table are all with trace sequence length 10 (*i.e.*, $SL = 10$). The *Privacy I* intuitively shows the difference between the raw data and reconstructed data; the *Utility*(%) represents the utility loss; and the *Privacy II*(%) represents the privacy gain calculated via the decline of the user re-identification accuracy.

4.6.1 Performance Comparison

I first compare the proposed models with the Optimal-IMs, TrajGAN, and DP-GI on four representative mobility datasets, as shown in Table 4.2. The overall performance is evaluated in terms of the *utility level* provided by the MPU and the *privacy protection* provided by DRU and URU. The *Model I* is the proposed architecture without applying the Lagrange multipliers (*i.e.*, where each unit is weighted equally). The *Model II* is the one with Lagrange multipliers (*i.e.*, λ_1, λ_2, λ_3) and different weights are given to units (*i.e.*, $\lambda_1 = 0.1,\ \lambda_2 = 0.8,\ \lambda_3 = 0.1$ for the results in Table 4.2). In this table, the sequence length of the input traces is 10, that is $SL = 10$. I will discuss why I choose SL=10 and the impact of the SL in Section 4.7.

As I mention in Section 4.5.2, Optimal-IMs are trained without considering the privacy-utility trade-offs; hence, they can be leveraged to explain the optimal inference accuracy achieved. That is, before any privacy-preserving mechanism applies, the accuracy of the target or private tasks with raw data. For instance, the accuracy of the *Privacy II* (0.9247 (MDC), 0.5643 (Priva'Mov), 0.6572 (GeoLife), 0.8780 (FourSquare)) demonstrates that an adversary can accurately infer user identity from raw data before any privacy protection.

Different from Optimal-IMs, the other models consider privacy-utility trade-offs, and I measure privacy protection and data utility by the effectiveness of the inference units. First, for the *Privacy I*, the distance indexes (*i.e.*, *"Euc"* and *"Man"*) are leveraged to intuitively represent the difference between the original data X and reconstructed data X', where a larger value indicates numerical differences between X and X'. For the distance index, I am interested in the distance between each trace, hence, I consider the quantity of trace for datasets X_D and get these distance indexes by averaging the corresponding record numbers N_D, that is (take *"Euc"* for example):

$$Euc(X_D, X'_D) = \frac{\sqrt{\sum_{i=1}^{N_D}(x_i - x'_i)^2}}{N_D}, \quad N_D = N'_D \tag{4.15}$$

Different to the *Privacy I*, the *Utility loss* and *Privacy II gain* are in a percentage format (%), compared with the accuracy of Optimal-IMs. To compare the trade-off between them more intuitively, I list the "Utility-PII trade-off" column, where "trade-offs = Utility (% for loss) + Privacy II (% for gain)". Table 4.2 demonstrates that the proposed models, especially *Model II*, outperform the TrajGAN and GI-DP across various datasets. For instance, with the MDC dataset, the *Model II* achieves the best trade-offs when compared with other models, as the utility loss is only 13.43% but with 65.51% privacy gain, while 46.32% utility loss and 20.32% privacy gain with the TrajGAN, and 97.34% utility loss and 97.47% privacy gain with the GI-DP. The extreme performance on the GI-DP illustrates that while the DP paradigm is a robust privacy-preserving technique in protecting *user's location*, it is not appropriate in protecting the *user's identities*.

More intuitively, in the column of "trade-off", *Model II* achieves all the best trade-offs among four datasets (52.08% (MDC), 24.48% (Priva'Mov), 34.36% (GeoLife), and 48.54% (FourSquare)). *Model I* has worse performance than *Model II*, in general, but is still superior to TrajGAN and DP-GI, where the latter two might even get *negative* trade-offs (*i.e.*, TrajGAN got -26.00% with MDC and GI-DP got -5.71% with Priva'Mov). Moreover, for the Priva'Mov dataset, although the utility loss of the TrajGAN is 4.21% smaller than the *Model II*, both two privacy metrics of the TrajGAN are worse than the *Model II*. Again, the proposed model has better overall trade-offs, as 23.66% for *Model I* and 24.48% for *Model II*. The performance on Geolife and FourSquare are similar but inverse, where the utility of the proposed model is better than TrajGAN and with slightly weaker privacy preservation.

In summary, GI-DP always has the highest privacy gain among the four datasets, however, the utility loss is also very high, resulting in inadequate and unexpected privacy-utility trade-offs. This trend also shows that the DP mechanism is not an appropriate metric for the location privacy of *user's identity*, which is also in line with the conclusions from other related work [30, 176]. The comparisons between *Model I* and *Model II* also illustrate the importance of the Lagrange multipliers, which provides flexibility to the Mo-PAE, enabling its application in different scenarios and enhancing the privacy-utility trade-offs in this case.

4.6.2 Trade-off Comparison

In this section, I present the privacy-utility trade-off analysis between the proposed Mo-PAE and TrajGAN in terms of mobility prediction accuracy (*i.e.*, U) and user de-identification efficiency (*i.e.*, *PII*). Figure 4.4 presents the trade-off comparisons of the four datasets, where the *hollow squares* and *hollow diamonds* show the trade-offs provided by the proposed Mo-PAE in $SL = 5$ and $SL = 10$, respectively. The *solid points* present the results of the TrajGAN under the same experimental setting. As can be seen from these results, in all four cases, the synthetic dataset generated by the TrajGAN is not *Pareto-optimal*. That is, the proposed Mo-PAE is able to achieve a better privacy level for a dataset with the same utility value. Compared with the TrajGAN, Mo-PAE improves utility and privacy simultaneously on four datasets. Especially for the performance of MDC, the privacy improves 45.21% more than the TrajGAN, while the utility also increases by 32.89%. These results illustrate that the Mo-PAE model achieves promising performance in training a privacy-sensitive encoder Enc_L for different datasets.

After evaluating the superior performance of the proposed model, I discuss the privacy guarantee that Mo-PAE provided in terms of data reconstruction (*PI*, *"Euc"* in Table 4.3) and user re-identification (*PII*, *privacy gain* in Figure 4.5). As I mentioned in Section 4.2, the privacy guarantee of Mo-PAE differs from that of DP paradigms and is given in the declined effectiveness of inference attacks.

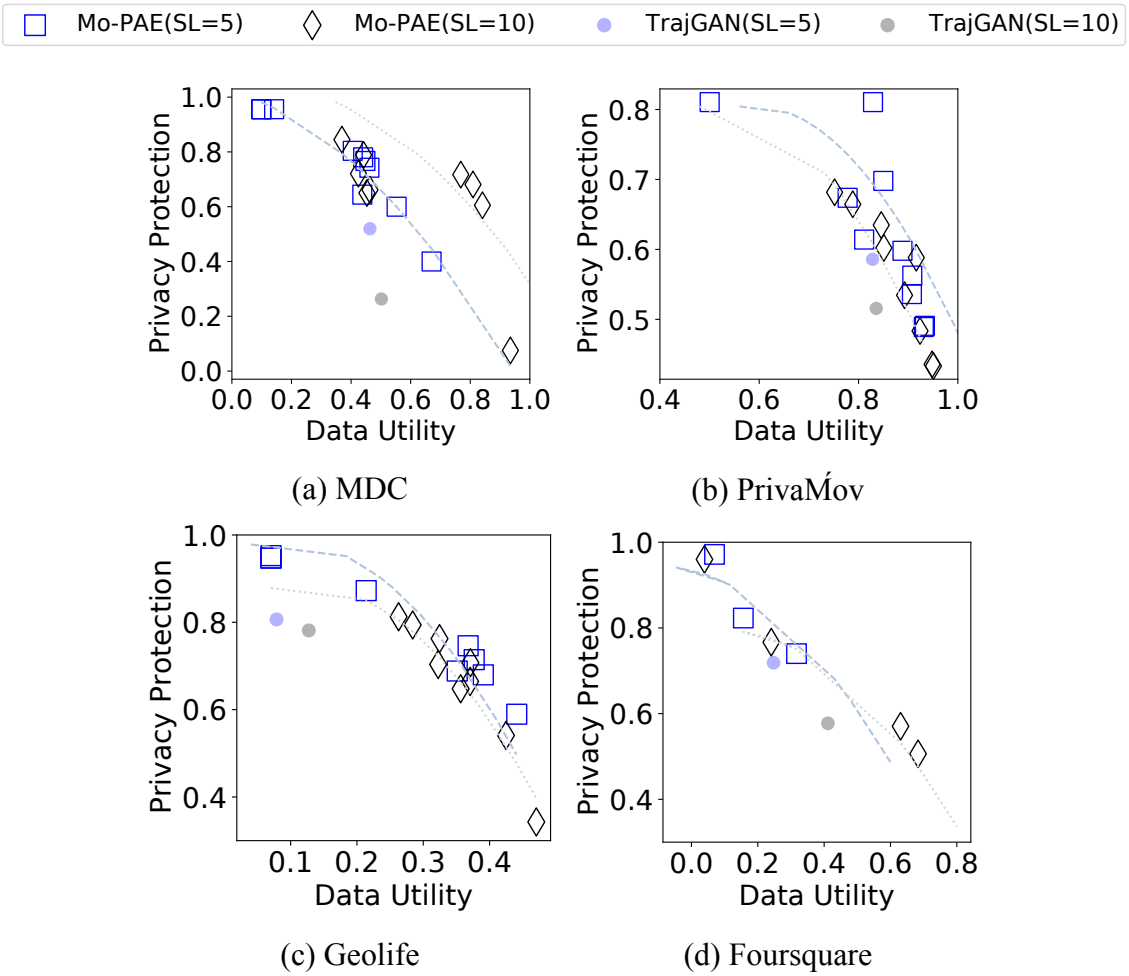


Figure 4.4: Pareto Frontier trade-off analysis on four datasets. The hollow squares and diamonds present the results of the proposed models Mo-PAE. solid points present the results of the TrajGAN. Blue colour means $SL = 5$. Black colour means $SL = 10$.

4.6.3 Privacy Guarantee Analysis: Effectiveness of Privacy Inference Attacks

In this section, I discuss the impact of Mo-PAE on the effectiveness of two privacy inference attacks (*i.e.*, *PI* and *PII*), respectively.

Effectiveness of Data Reconstruction Attacks - PI

Table 4.3 shows the impact of the proposed mechanisms on the data reconstruction accuracy(*PI*). The *"Euc"* in the table follows the definition in Equation 4.15. Overall, *Model II* performs better than *Model I* in limiting the accuracy of data reconstruction regardless of the value of weights. Take the result of the GeoLife dataset as an example, *Model II-i* achieves a bigger distance than *Model I* (*i.e.*, 0.4343 > 0.0057), while it still gets better utility (*i.e.*, -9.94% > -17.9%). Nevertheless, both *Model I* and *Model II* have effectively defended the data reconstruction attack (MDC: 0.0697 > 0.0017 > 0.0000; Priva'Mov: 0.0453 > 0.0009 > 0.0003; GeoLife: 0.4343

Settings					MDC		Priva'Mov		Geolife		FourSquare	
		λ_1	λ_2	λ_3	Euc	Utility	Euc	Utility	Euc	Utility	Euc	Utility
Model I	-	-	-	-	+0.0017	-30.27%	+0.0009	-2.72%	+0.0057	-17.9%	+0.0069	-33.75%
Model II	i	0.1	0.8	0.1	+0.0697	-12.55%	+0.0453	-2.71%	+0.4343	-9.94%	+0.7933	-1.64%
	ii	0.2	0.6	0.2	+0.0791	-33.29%	+0.0738	-10.72%	+0.4889	-18.21%	+1.2722	-50.50%
	iii	0.3	0.4	0.3	+0.0889	-58.10%	+0.0782	-16.56%	+0.5220	-29.95%	+1.9586	-60.71%
	iv	0.1	0.6	0.3	+0.0822	-49.27%	+0.0776	-10.28%	+0.4717	-18.64%	+1.4139	-57.40%

Table 4.3: Impact of Mo-PAE on the data reconstruction accuracy (*PI*) and relative utility loss (*U*) on four mobility datasets. I list *Model I* and four different settings of *Model II*'s weight combinations to discuss the potential range of the trade-offs.

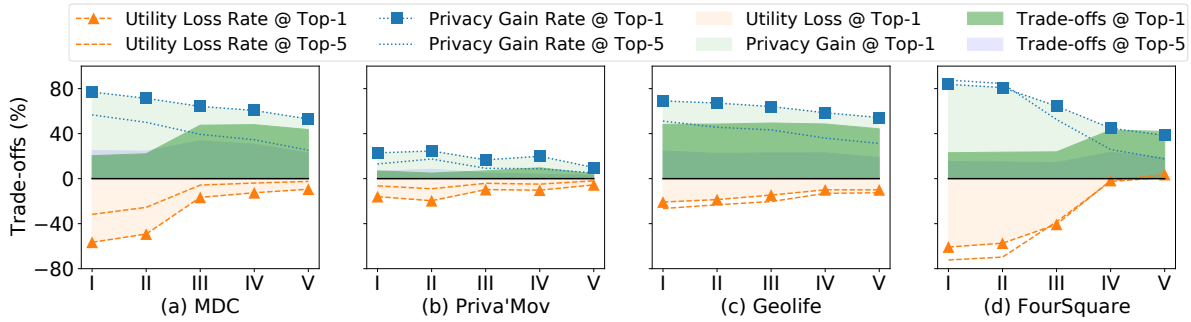


Figure 4.5: Impact of Mo-PAE on the user re-identification accuracy (PII) and relative utility loss (*U*) on four datasets. The orange area represents the utility loss, while the light-green area represents privacy gain. The dark-green area represents the trade-offs between utility achievement and privacy budgets. The x-axis shows five different model settings, and the y-axis shows the trade-offs.

> 0.0057 > 0.0008; FourSquare: 0.7933 > 0.0069 > 0.0052), while only at the marginal cost of mobility utility (MDC: -12.55%; Priva'Mov: -2.71%; GeoLife: -9.94%; FourSquare: -1.64%). The data of the Optimal-IMs are in Table 4.2. I list four representative settings here to make a comprehensive comparison of PII and U. From setting i to iv, one can expect more original data features loss to result in a more significant utility loss. This trend is indeed the case with different weight combinations. However, as the results show, especially for setting i, the privacy of the traces attains decent protection at the marginal cost of mobility utility.

Effectiveness of User Re-identification Attacks - PII

Figure 4.5 presents the impact of the *Model II* on the user re-identification accuracy(*PII*). In this figure, I list five different settings, I to V ($\lambda_1 = 0.1$, over the range of λ_2 = {0.5, 0.6, 0.7, 0.8, 0.9}), respectively. The *Zero* line (*i.e.*, y = 0%) in each sub-figure is leveraged to indicate the original accuracy of the raw data (*i.e.*, Optimal-IMs). The *"Privacy Gain Rate"* (blue square line) shows the effectiveness of the Mo-PAE in defending the user re-identification attacks. That is, after applying *Model II*, the decline range of effectiveness of user re-identification attacks. For instance, with the MDC dataset, in setting I, the effectiveness of user re-identification attacks declines as high as 80%. At the same time, this high privacy protection is at the cost

of nearly 55% of utility (orange triangle line). Things are better in setting V, where the Mo-PAE can get 60% privacy protection only at the cost of less than 10% utility. The x-axis shows five settings of the model, and the y-axis shows the trade-offs (*i.e.*, *trade-offs = privacy gain + utility loss*). The orange area represents the utility loss while the light-green area represents the privacy gain when compared with Optimal-IMs. The dark-green area represents the trade-offs between utility and privacy budgets.

In summary, these trade-offs are all positive in different model settings on four different datasets. The performance on the GeoLife data is the best, while less than 20% utility loss but more than 50% privacy gains. The performance on MDC and FourSquare also show promising privacy-utility trade-offs, especially for setting V on the FourSquare dataset, and both the utility and privacy increase. The uniqueness of human mobility trajectories is high, and these trajectories are likely to be re-identified even with a few location data points [29]. The results emphasize that the concern of user re-identification risk could be alleviated effectively with the proposed model.

In real applications, the trade-off of Mo-PAE is achieved continuously over time. New trajectories will be encoded with the pre-trained encoder to attain respective feature representation and utilized by SP for following task-oriented scenarios (no need to retrain). The pre-trained encoder and discriminators are assumed to be updated offline within a fixed duration for best performance purposes. Additionally, while the architecture focuses on specific application scenarios (*i.e.*, mobility prediction), it could be applicable to different task-oriented scenarios.

4.7 Discussions

In this section, I further discuss the impact of the temporal granularity of traces, the varying sequence length and weights on the composition units on the Mo-PAE performance.

4.7.1 Impact of Temporal Granularity

The timestamp is one of the essential components of the mobility trace, and different choices on the temporal granularity affect the final performance of any dataset. Figure 4.6 shows the impact of the varying temporal granularity on the proposed architecture. I present the top-1, top-5, and top-10 accuracies for both utility and privacy dimensions. For instance, when temporal granularity is 10-min, it indicates a location record r is taken every 10 minutes from the raw data. When using more coarser temporal granularity, the number of points of interest decreases so does the difficulty of mobility prediction. However, the uniqueness of the trajectory decreases due to ignoring many of the unique locations of each user, resulting in better privacy. To summarize from Figure 4.6, the impact of temporal granularity on the Priva'Mov is mini-

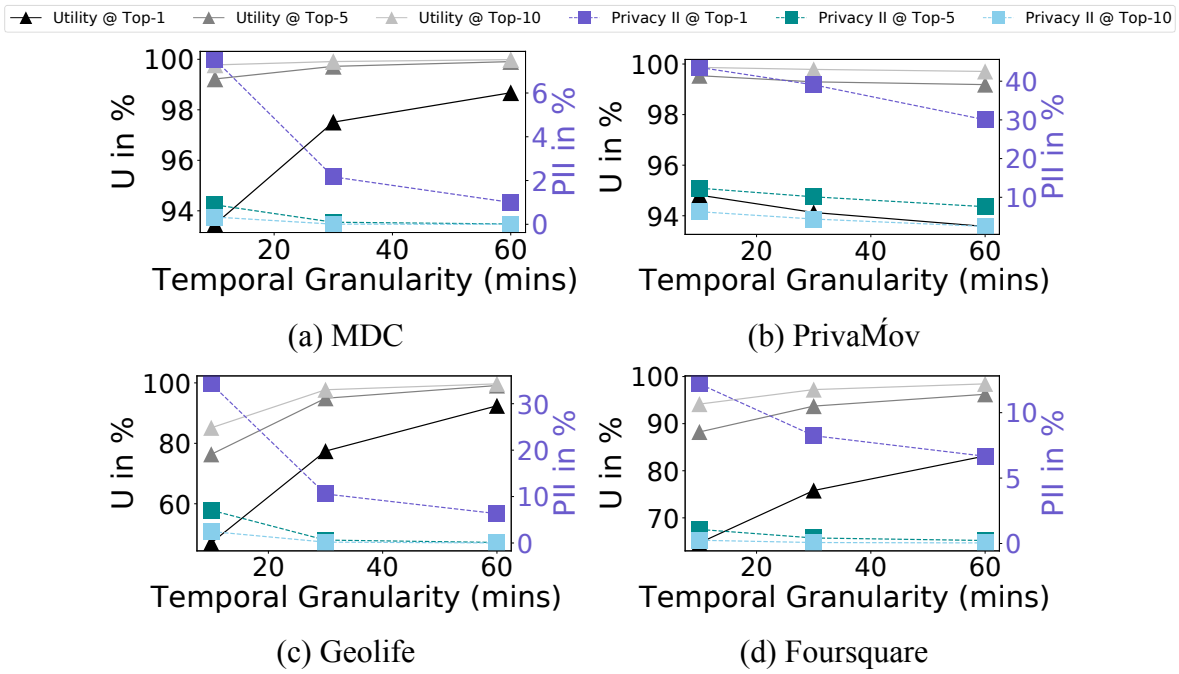


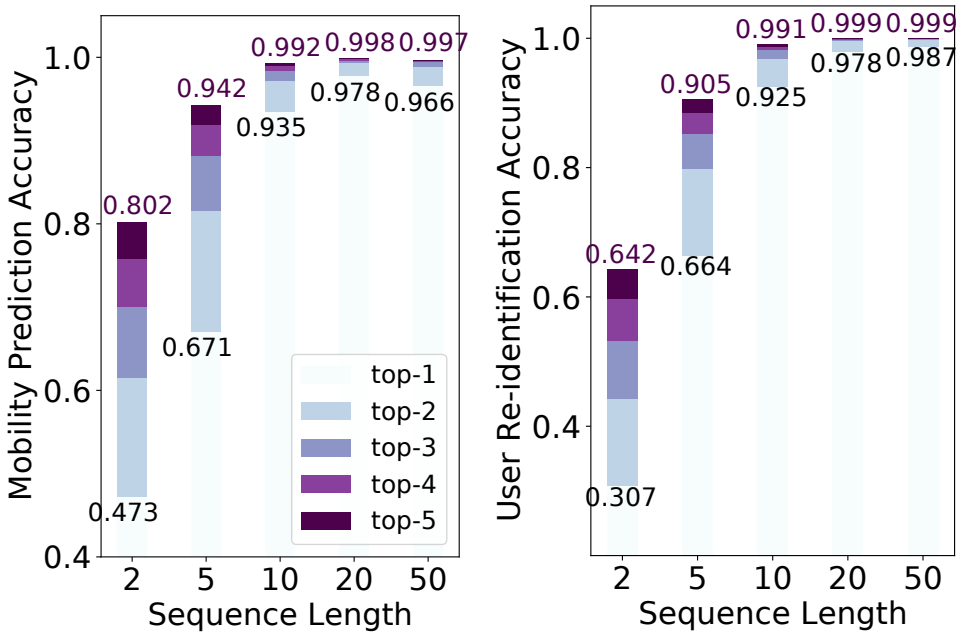
Figure 4.6: The effect of temporal granularity on the model performance of four mobility datasets.

mal. In terms of utility (mobility prediction), Priva'Mov is the only dataset for which accuracy decreases with increasing temporal granularity. This subtle decline emphasizes the trajectory features only have a small change when varying granularity, in line with the university students' mobility.

4.7.2 Impact of Varying Sequence Lengths

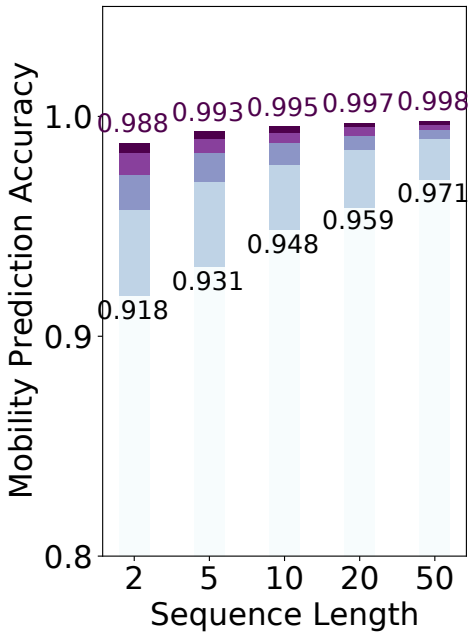
The performance of the utility discriminator U_D (MPU) and the privacy discriminator P_D^2 (URU) exert a significant impact on the overall performance of the proposed Mo-PAE. The trace length is the most critical factor affecting these units' performance. I use two representative datasets (*i.e.*, MDC and Priva'Mov) to present the impact of the varying sequence length on both discriminators.

As shown in Figure 4.7, by changing the lengths of trace sequence SL from 1 ($SL = 1$) to 50 ($SL = 50$), I observe that SL has a significant impact on different tasks' accuracy (*i.e.*, mobility prediction accuracy for U_D and user re-identification accuracy for P_D^2) of two different datasets. Overall, the impact in the MDC dataset is much higher than in the Priva'Mov dataset. Comparing the Figures 4.7a and 4.7c, there is a much sharper increase on the MDC dataset. More specifically, when the sequence length is increased from 2 to 20, the top-1 mobility prediction accuracy on MDC increases from 0.473 to 0.978 (*i.e.*, +50.5%), while accuracy on Priva'Mov increases from 0.918 to 0.959 (*i.e.*, only +4.1%). Similarly, more rapid growth appears in the user re-identification accuracy on MDC, which is +68.0%, while the increase for

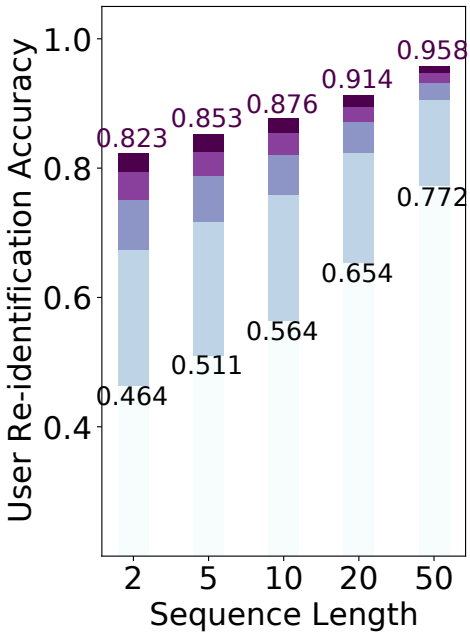


(a) U_D, MDC

(b) P_D^2, MDC



(c) U_D, Priva'Mov



(d) P_D^2, Priva'Mov

Figure 4.7: Mobility prediction accuracy and user re-identification accuracy change with the trace sequence length (SL) in the proposed U_D and P_D^2. The colour bars indicate the accuracy from top-1 to top-5, the black texts indicate the top-1 accuracy, and the purple texts indicate the top-5 accuracy. For instance, the top-1 mobility prediction accuracy on MDC with $SL = 2$ is 0.473, and the top-5 one is 0.802.

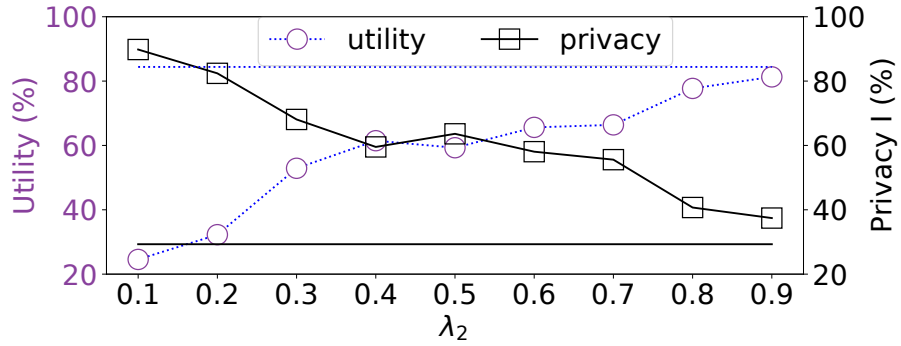
Priva'Mov is only +30.8%. I conclude that the mobility predictability and user re-identification accuracy of a dataset might have a special link. The mobility predictability of Priva'Mov is very high, almost higher than 90%, but the user re-identification accuracy is always lower than 80%, which also means the uniqueness of trajectories in this dataset is low. This low uniqueness suggests that the users in this dataset might share similar daily routes, which is reasonable, as I know these trajectories are collected from students at the same university. For the MDC dataset, when $SL = 10$, the user re-identification accuracy is relatively high, indicating that the locations are more sparse in this dataset. However, the mobility predictability here is also high, which emphasizes that this sparseness does not affect predictability. These phenomena indicate that the deep training of MPU and URU might share similar extracted features, while the proposed architecture attempts to extract features more suitable for mobility predictability but less suitable for user re-identification.

I note that the varying trace sequence length not only exerts impacts on the model performance but also has a significant influence on the computation time. For instance, the computation time at $SL = 50$ costs six times as much as that at $SL = 5$. The computation time also varies between datasets. Hence, an appropriate choice of trajectory sequence length can avoid time-consuming computation and achieve expected task inference accuracy. In this evaluation, I place greater focus on the trace sequence lengths ranging from 5 to 10, which exhibit great performance in both the U_D and P_D while also keeping a low computation time.

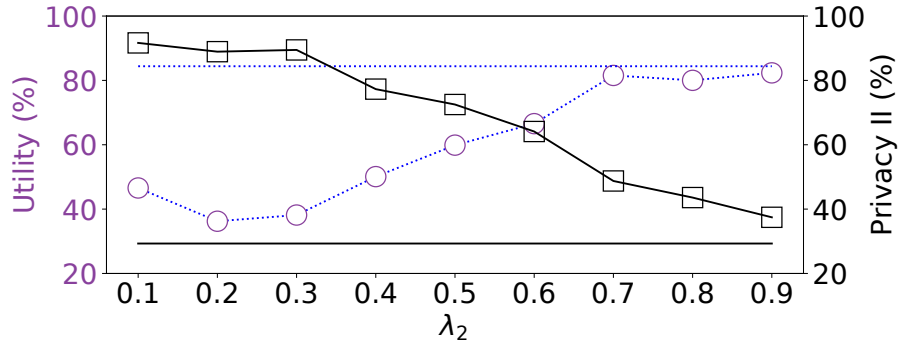
4.7.3 Impact of Varying Weights

As I discussed in Section 4.4.3, the *sum loss function* L_{sum} of *Model II* is a linear combination of L_R, L_U, and L_P with different weights (*i.e.*, Lagrange multipliers). I evaluate the influence of different weights' combinations (λ_1, λ_2, and λ_3) on the *Model II*, as the results shown in Figure 4.8.

I compare the overall model performance in U_D and P_D^1 by fixing the $\lambda_3 = 0$, and vary the other two multipliers by subjecting to $\lambda_1 = 1 - \lambda_2$, as shown in Figure 4.8a. Figure 4.8b illustrates the effect between U_D and P_D^2 by setting the $\lambda_1 = 0$. It could be observed in both settings that the utility increases with a larger λ_2, which means when the MPU is given more weight in the Mo-PAE model, it would exert a positive impact on the data utility. I conclude that the privacy-utility trade-offs could be tuned by varying these weights; the results in Figure 4.8 also verify the effectiveness of the proposed adversarial architecture. It is noted that the balance of three units is far more complicated than the balance of two. From the extensive experiment I conducted, initialling $\lambda_1 = 0.1$, $\lambda_2 = 0.6$, $\lambda_3 = 0.3$ can guide the model to achieve the trade-off most efficiently. However, as the experiment results show, there is no dataset-independent privacy interpretation for λ_1, λ_2 and λ_3, and I leave a more efficient approach using reinforcement learning to initialise these hyperparameters for different datasets in future work.



(a) $\lambda_1 = 1 - \lambda_2,\ \lambda_3 = 0$



(b) $\lambda_3 = 1 - \lambda_2,\ \lambda_1 = 0$

Figure 4.8: Varying weights can tune the privacy-utility trade-offs. The primary y-axis (dashed line) represents utility, and the secondary y-axis (solid line) represents privacy. The x-axis represents the value of the target λ.

4.8 Conclusion

In this chapter, I presented a privacy-preserving architecture Mo-PAE based on adversarial networks. The proposed model considers three different optimization objectives and searches for the optimum trade-off for the utility and privacy of a given dataset. I reported an extensive analysis of the model performances and the impact of its hyperparameters using four real-world mobility datasets. The weights $\lambda_1,\ \lambda_2$, and λ_3 bring more flexibility to the proposed framework, enabling it to satisfy different scenarios' requirements according to the relative importance of utility requirements and privacy budgets. I evaluated the framework on four datasets and benchmarked the results against an LSTM-GAN approach and a DP mechanism. The comparisons indicate the superiority of the proposed framework and the efficiency of the proposed privacy-preserving feature extractor Enc_L. Expanding this chapter, I will consider other utility functions for the proposed models, such as community detection based on unsupervised clustering methods or deep embedded clustering methods. In future work, I will leverage automated search techniques, such as deep deterministic policy gradient algorithm and reinforcement learning, for efficiency in searching for optimal weight combinations.

Chapter 5

Privacy or Fairness? Characterizing Spatial-Temporal Data Sharing Techniques

Preserving the individuals' privacy in sharing spatial-temporal datasets is critical to prevent re-identification attacks based on unique trajectories. Existing privacy techniques tend to propose ideal privacy-utility tradeoffs, however, they largely ignore the fairness implications of mobility models and whether such techniques perform equally for different groups of users. The quantification between fairness and privacy-aware models is still unclear, and no defined sets of metrics barely exist for measuring fairness in the spatial-temporal context. In this chapter, I define a set of fairness metrics designed explicitly for human mobility, based on structural similarity and entropy of the trajectories. Under these definitions, I examine the fairness of two state-of-the-art privacy-preserving models that rely on GAN and representation learning to reduce the re-identification rate of users for data sharing. The results show that while both models guarantee group fairness in terms of demographic parity, they violate individual fairness criteria, indicating that users with highly similar trajectories receive disparate privacy gain. I conclude that the tension between the re-identification task and individual fairness needs to be considered for future spatial-temporal data analysis and modelling to achieve a privacy-preserving fairness-aware setting.

5.1 Introduction

Understanding human mobility based on location data from smartphones has become a fundamental part of urban and environmental planning in cities [210]. Through the collection of these geo-traces, it has become possible for the scientific community and policy-makers to model citizens' daily mobility patterns using crowd-sensed car-share data [225], city bicycles [226], and RFID transportation cards [227], or to build predictive algorithms to estimate people's flows [228, 229] and community structure [230]. However, location-based traces corresponding to human mobility, even at an aggregate level, have raised numerous privacy con-

cerns [29, 180, 231].

In the past decades, the research community has examined various ways of ensuring the privacy of mobility traces. Previous work ranges from Differential Privacy [200, 232], k-anonymity [233] to information-theoretic metrics [234, 235]. More recently, *Privacy-Utility Trade-off* (*PUT*) models based on machine learning or deep learning techniques that aim to optimize both privacy and prediction accuracy have been studied. These approaches can be summarized as representation learning [205], GAN-based approaches [54, 207], reinforcement learning [236, 237], etc. In all these works, researchers have shown that it is possible to design and implement frameworks that enhance the privacy protection of individual trajectories while reducing utility depreciation.

A dimension that has been vastly overlooked is whether privacy-preserving algorithms work equally for all users or whether they could lead to unexpected consequences of protecting the privacy of only a group of people. Indeed, as recent evidence from the broader machine learning domain has shown, autonomous decision-making has shifted the systematic discrimination and fairness against different groups in decision-making from people to algorithms [238, 239]. In many applications, discrimination may be defined by different protected attributes, such as race, gender, and religion, that directly prevent favourable outcomes for a minority group in societal resource allocation, education equality, employment opportunity, etc [240]. Similarly, in the context of spatial-temporal data, mobility demand prediction algorithms have been shown to offer higher service quality to neighbourhoods with more white people [241]. However, in such contexts, only a handful of recent studies exist that examine the fairness of location-based systems [242–244], with little consensuses on how fairness should be defined and measured for spatial-temporal applications.

In this work, I measure and evaluate the fairness of the privacy-preserving algorithms that are applied to mobility traces. I seek to answer the research question as to *whether the outcome of the PUT models satisfies fairness*. That is, whether these models preserve the privacy and prediction accuracy of similar groups of users equally. In order to do so, I first posit a set of metrics grounded on the broader fairness literature [245] for measuring *individual* fairness based on trajectories. I measure the similarity of users' trajectories in terms of the structural similarity of their heatmap images as well as the entropy of their trajectories. I then examine two of the state-of-the-art privacy-preserving approaches, TrajGAN [54] and PAE [246] in comparison with the original inference tasks that optimize only for privacy or for prediction. I evaluate these models on two real-life mobility datasets: Geolife [247] and MDC [220]. The results indicate that both PAE and TrajGAN models do not guarantee individual fairness; users with similar trajectories might receive different privacy gain outcomes. The results of group fairness show that there is no demographic disparity in the privacy and prediction outcome. However, as I discuss this observation is highly reflective of the socio-cultural settings in that these traces have been collected, and less of the by-product of the privacy-preserving models. In terms of

individual fairness, I observe that the privacy-aware algorithms violate fairness criteria. More specifically, I observe that for the users with similar trajectories even when the outcome of the prediction task is similar, the privacy gain amongst those users is highly different, leading to some users not advantaging from obfuscation as others do.

The contributions of this chapter are as follows:

- I offer a set of individual fairness metrics specifically defined based on mobility characteristics that can help the broader research community in measuring fairness for spatial-temporal applications.
- I examine the privacy-preserving algorithms and show their deficiencies in accounting for fairness can lead to undesired consequences.

The rest of this chapter is structured as follows: In Section 5.2, I describe the previous works in fairness in Machine Learning literature and give a background to the privacy methods for spatial-temporal data. Section 5.3, I define a set of fairness metrics for spatial-temporal datasets. Section 5.4 details the setup of experiments by describing the datasets I used in the analysis and offering an overview of the privacy performance of the models I evaluated. In Section 5.5, I present the results of the fairness analysis of the PUT models in terms of individual and group fairness metrics. Section 5.6 discusses the limitation and implications of this study and lays a future roadmap. Finally, Section 5.7 concludes this chapter.

5.2 Related work

5.2.1 Fairness in Machine Learning

Literature on fairness in machine learning tends to focus on *the absence of any prejudices or favouritism toward an individual or group based on their inherent or acquired characteristics* [248]. Most fairness research strives to avoid the decision made by automated systems being skewed toward the advantaged groups or individuals. In [245], authors proposed a framework for understanding different definitions of fairness through two views of the world: i) *We are all equal* (*WAE*), and ii) *What you see is what you get* (*WYSIWYG*). The framework shows that the fairness definitions and their implementations correspond to different axiomatic beliefs about the world described as two worldviews that are fundamentally incompatible. The most adopted metrics for fairness in machine learning are widely based on group-based fairness which is also known as Statistical parity and Demographic parity [249]. These metrics aim to ensure that there is independence between the predicted outcome of a model and sensitive attributes of age, gender, and race. Variations of statistical parity exist, which concentrate on relaxation of

this measure by ensuring that groups from sensitive attributes and non-sensitive attributes meet the same misclassification rate (False Negative Rate, also known as Equalized Odds [250]), or equal True Positive Rate (also known as Equal opportunity [250]).

In the context of mobility data and its applications such as equitable transportation, attention has been mainly devoted to group fairness. Transportation equity heavily employs statistical tests for equity analysis, which is appropriate for discovering unfairness [243]. Such metrics are often defined based on census tract-level information which offers an aggregate demographic characteristic of the residing population. Yan *et al.* define fairness in terms of region-based fairness gap and assess the gap between mean per capita ride-sharing demand across groups over a period of time. The two metrics differ from each other, as one is based on a binary label associated with the majority of the sub-population (*e.g.*, white) versus a continuous distribution of the demographic attributes. To the best of my knowledge, the research of Yan *et al.* is the only work in literature that offers a group-based fairness metric for spatial-temporal data.

On the other hand, individual fairness claims that similar individuals (with respect to a specific task) should be treated similarly with respect to that task. For example, in making hiring decisions, the algorithm has to possess perfect knowledge of how to compare the ”qualification” of two individuals. In most cases, the difficulty with individual fairness lies in the notion of measuring *similarity*. For example, Yan uses the population and employment density of each area of the city for achieving individual fairness in bike sharing demand prediction. The difficulty again lies in the fact that there is often a lack of perfect knowledge to determine the similarity in demand between two areas. In broader spatial-temporal data and application, the definitions of individual fairness are almost non-existence.

In this work, I offer a set of individual fairness metrics defined based on the literature on mobility.

5.2.2 Privacy Methods for Spatial-Temporal Data

Large-scale human mobility data contain crucial insights into understanding human behaviour but due to their highly sensitive nature are hard to share in non-aggregated form. Decades of research on privacy have examined various anonymous human trajectories [200, 232, 233]. A mobility privacy study conducted by De Montjoye *et al.* [29] illustrates that four spatial-temporal points are enough to identify 95% of the individuals in a certain granularity. More recently, PUT models that aim to optimize both data privacy protection and data utility have been studied. In these lines of work, researchers have focused on the objective of training neural network models that optimize for reducing privacy leakage risk of individual trajectories while at the same time minimizing the depreciation in the mobility utility. Various state-of-the-art models have been proposed based on adversarial networks [54, 207], representation learning [205] and those of

Reinforcement Learning [236, 237]. In this chapter, two PUT models that I selected for fairness analysis are mainly focused on temporal correlations in time-series data and aim to reduce the user re-identification risk (*i.e.*, privacy) while minimizing the downgrade in the accuracy of mobility prediction task (*i.e.*, utility). I then describe the details of these two privacy-aware spatial-temporal models:

TrajGAN [54]: it is an end-to-end deep learning model to generate synthetic data which preserves essential spatial, temporal, and thematic characteristics of the real trajectory data. Compared with other common geomasking methods, TrajGAN can better prevent users from being re-identified. TrajGAN claims to preserve essential spatial and temporal characteristics of the original data, verified through statistical analysis of the generated synthetic data distributions, which is in a line with the data utility assessment based on the mobility prediction task in this work. Hence, I train a TrajGAN-based PUT model to evaluate the mobility predictability and privacy protection of synthetic data generated by TrajGAN.

PAE [246]: it is a **p**rivacy-preserving **a**dversarial feature **e**ncoder. In contrast to the TrajGAN that aims to generate synthetic data, PAE trains an encoder Enc_L that forces the extracted representations f to convey maximal utility while minimizing private information about user identities, via adversarial learning. It consists of a multi-task adversarial network to learn an LSTM-based encoder Enc_L, which can generate the optimized feature representations $f = Enc_L(X)$ via lowering privacy disclosure risk of user identification information (*i.e.*, privacy) and improving the mobility prediction accuracy (*i.e.*, utility) concurrently.

5.3 Fairness Definition and Metrics

In this section, I define the metrics for measuring fairness in spatial-temporal applications.

5.3.1 Formulation of the Problem

In this work, I measure and evaluate the fairness of the privacy-preserving algorithms that are applied to mobility traces. I seek to figure out whether these models preserve the privacy and prediction accuracy of similar groups of users equally. Both individual-based to group-based fairness analyses are discussed.

I first introduce some basic definitions: individuals are labelled as *u*, if individuals u_i and u_j are similar, that is $u_i \backsim u_j$; sensitive or protected attributes are denoted as *S*; raw data without sensitive attributes is denoted as X; Y is the ground-truth labels for a specific inference task and Y' is the predicted one, which is the variant that depends on S and X. The true positive rate (*i.e.*, TPR, recall, or sensitivity) of each user is utilized to judge the performance of the multi-categorical classifiers, which refers to the proportion who should be predicted accurately

that received a positive result. In the mobility prediction task and user re-identification task of the examined models, I use the TPR as the measure of the *task accuracy*.

5.3.2 Group Fairness

Group fairness [245] states that demographic groups should receive similar decisions, which is inspired by the civil rights law in different countries [251]. To be specific, group fairness argues that a disadvantaged group (in terms of the sensitive attributes) should receive similar treatment to the advantaged group, that is:

$$P(Y' = 1|S = 0, Y = 1) = P(Y' = 1|S = 1, Y = 1) \tag{5.1}$$

While S is not an input to the PUT models, it is possible that specific demographic groups of users exhibit certain properties that could lead to a less favourable outcome for the models. For instance, age and employment status can highly influence peoples' day-to-day trajectory. As an example, a user whose trajectory data is limited to his home and office location only could be highly predictable by PUT models but also highly re-identifiable (low privacy gain). This means the notion of group fairness in the context of this study is highly dependent on the examined *dataset*. I elaborate more on this discussion in Section 5.6.

In order to quantify the group fairness in a more statistical approach, *group fairness score* (*i.e.*, *GFS*) are calculated by disparate impact for disadvantaged groups:

$$GFS = P(Y' = 1|S = advantaged, Y = 1)/P(Y' = 1|S = disadvantaged, Y = 1) \tag{5.2}$$

5.3.3 Individual Fairness

Individual fairness [249] states that individuals who are similar, with respect to a specific task, should be treated similarly (*i.e.*, $P_{u_i} \backsim P_{u_j}$ when $u_i \backsim u_j$) [252]:

$$P(Y'|u_i, S, X) = P(Y'|u_j, S, X) \tag{5.3}$$

To measure individual fairness in the context of this work, I need two sets of definitions corresponding to the similarity between users' *trajectories*, and the similarity of the *outcome* of the PUT models. I define each next:

Similarity of Trajectories

Grounded on the literature on mobility [180, 230, 253], I define the measure metrics of trajectory similarity based on the *structural similarity index* of mobility heatmap images and *entropy* of trajectories.

Structural Similarity Index Measure (SSIM): SSIM is originally designed to quantify image quality degradation caused by processing such as data compression or by losses in data transmission, which leverages the differences between the reference image and the processed image [254]. To apply it in this work, heatmap images are constructed from the raw geo-located data with the methodology proposed by [230]. Figure 5.1 shows some sample heatmap images with spatial granularity coarsening from left to right from 50 meters to 900 meters. These heatmap images structurally represent mobility features extracted from mobility traces, which use pixel intensity to encode the *frequency* of the visit spent in a given area; hence, the brighter pixels denote the more frequently visited locations of the user. SSIM has been shown to be a well-suited metric to compute the image similarity of the heatmap images [230, 253]. That is because, unlike Mean Square Error (MSE), the SSIM metric has been shown not to be significantly impacted by the changes in luminosity and contrast.

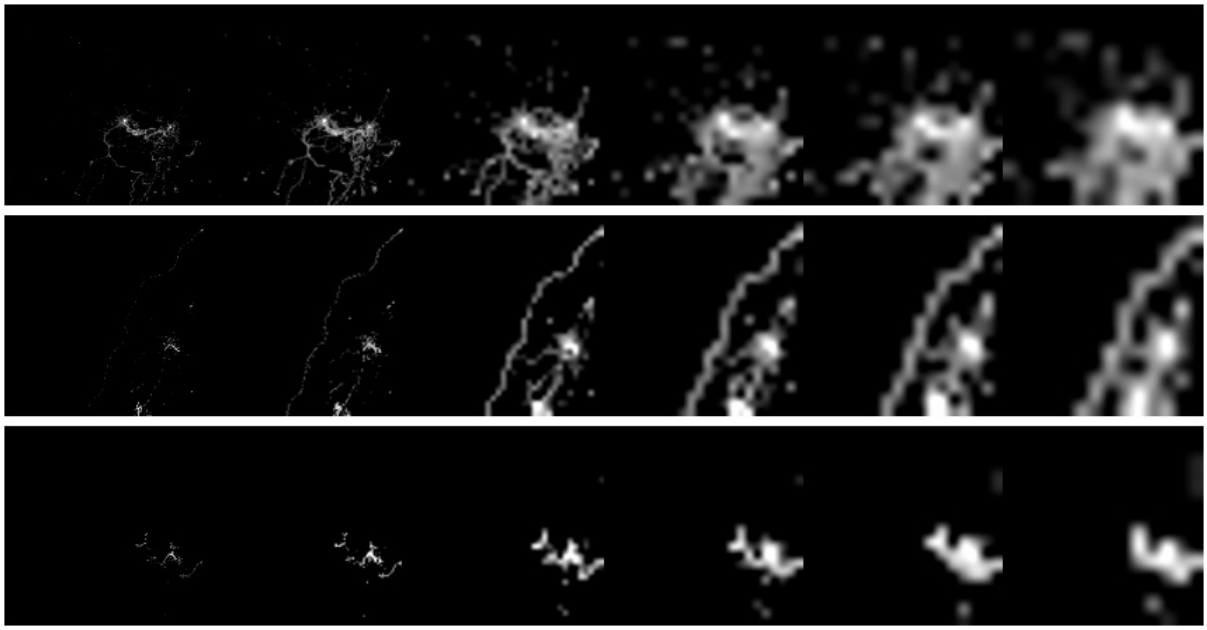
In this work, I formulate the SSIM measure as the perceptual difference between two similar users' heatmap images H_i and H_j:

$$SSIM(H_i, H_j) = \frac{(2\mu_i\mu_j + c_1)(2\sigma_{ij} + c_2)}{(\mu_i^2 + \mu_j^2 + c_1)(\sigma_i^2 + \sigma_j^2 + c_2)}, (c_1 = (k_1 L)^2,\ c_2 = (k_2 L)^2) \tag{5.4}$$

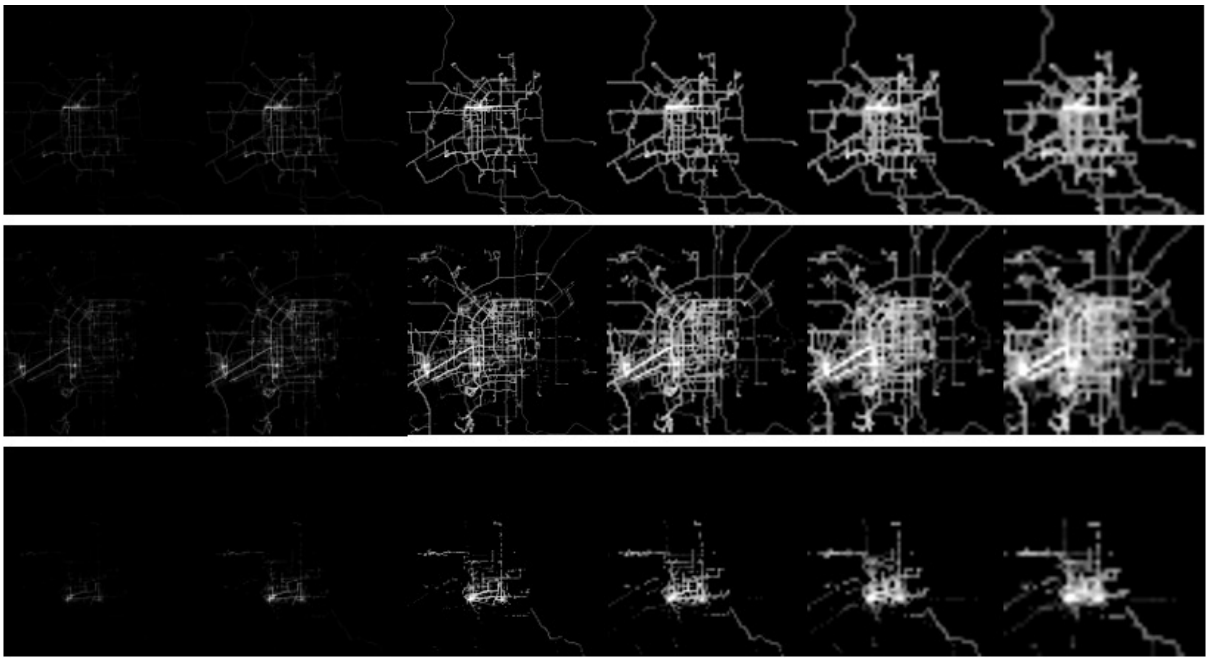
where μ_i and μ_j are the averages, σ_i and σ_j are the variances, and σ_{ij} is the covariance of H_i and H_j; L is the dynamic range of the pixel-values, $k_1 = 0.01$ and $k_2 = 0.03$ by default.

I leverage the integrated heatmap image, which combines all user trajectories, to calculate the effective SSIM index that indicates the trajectory similarity of users. The SSIMs between individual trajectory and integrated trajectory are estimated by calculating the SSIM *maps* (*i.e.*, local values of the SSIM). To lower the impact of the unreached areas, only the swept area in the integrated heatmap image was selected. The average SSIM value of the selected points is defined as effective SSIM in this work. As this metric relies on heatmap images, it is highly influenced by spatial granularity, as each pixel in the image corresponds to the spatial boundary of the data. Intuitively, in Figure 5.1, as the granularity coarsens the trajectories become more blurry and thus more similar to each other. The impact of the spatial granularity on the SSIM index will discuss in Section 5.5.1.

Entropy of Trajectories: Mobility literature defines the highest potential accuracy of predictability of any individual, termed as "maximum predictability" (Π_{max}) [255]. Maximum predictability is defined by the *entropy* of information of a person's trajectory (frequency, se-

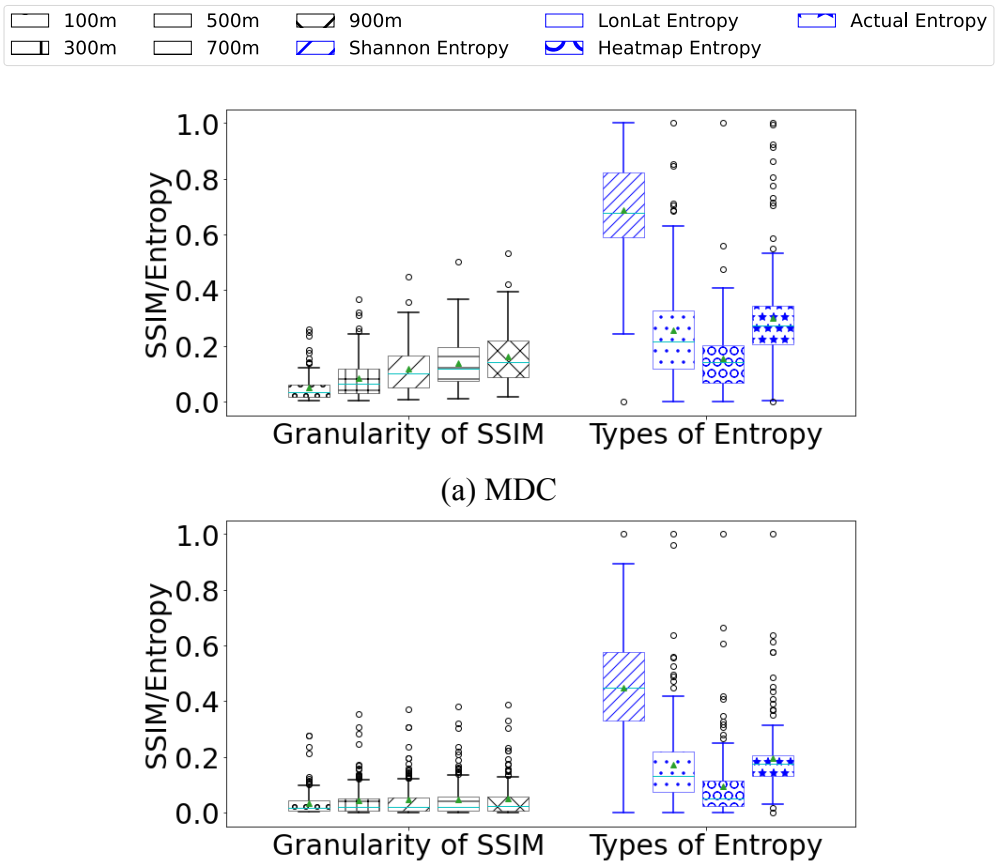


(a) MDC



(b) Geolife

Figure 5.1: Sample mobility heatmap images with various spatial granularities of MDC and Geolife. Three different trajectories are shown with different granularities ranging from 50 m to 900 m.



(a) MDC

(b) Geolife

Figure 5.2: Overview of SSIM and entropy distribution of trajectories of MDC and Geolife datasets. Different granularities of SSIM are compared in a row, where the granularity are ranging from 100-meter to 900-meter.

quence of location visits, etc.). Hence, some similar characteristics of user spatial-temporal patterns are able to be captured by leveraging the entropy of trajectory. In this chapter, I define four types of entropy to measure trajectory similarity for spatial-temporal applications: first, the entropy based on the probabilities of visited location distribution; second, the entropy based on the geo-located locations in a time-series format; third, the entropy based on the users' heatmap images; fourth, the entropy of capturing full spatial-temporal order present in user's mobility pattern. Figure 5.2 shows the overview of SSIM and different entropy distributions of trajectories of MDC and Geolife datasets.

Shannon Entropy (*SE*): As a classic definition of data uncertainty, I first calculated the Shannon entropy (E_h) to characterize the probabilities of visited location distribution. A larger entropy indicates greater disorder, and consequently reduces the predictability of an individual's movements. I define entropy following notion in [255, 256] and measure SE as:

$$E_h = -\sum_{i=1}^{n} P(x_i) \log_2[P(x_i)] \tag{5.5}$$

where n is the length of the probability vector, $P(x_i)$ is the probability of location x_i considering only temporal pattern.

LonLat Entropy (*LE*): Considering the spatial-temporal pattern of the mobility data, the entropy of visited locations in terms of longitudes and latitudes are separately estimated by using the fuzzy entropy E_f. This entropy model reflects the probability of a new sub-string and is able to quantify the irregularity or complexity of the time-series data. The E_f of visited longitudes and latitudes are integrated as the LE:

$$E_f = \ln \Phi^m(r, n) - \ln \Phi^{m+1}(r, n) \tag{5.6}$$

where the threshold r, the definition of the function $\Phi^m(r, n)$, the details, and the default values can be found in Chen *et al.*, Flood *et al.*

Heatmap Entropy (*HE*): In contrast to the aforementioned entropy models, I define a two-dimensional entropy (E_{2D}) to quantify the irregularity (i.e, unpredictable dynamics) of the user's heatmap image. The entropy of trajectory heatmap images was calculated using the two-dimensional sample entropy method ($SampEn_{2D}$) [259]. In a trajectory heatmap image (L^2), the features of the image were extracted by accounting for the spatial distribution of pixels in different m-length square windows with origin at $u(i, j)$.

$$E_{2D}\left(u, m, r\right) = -\ln \frac{U^{m+1}(r)}{U^m(r)} \tag{5.7}$$

$$U^m(r) = \frac{1}{N_m} \sum_{i,j,a,b=1}^{i,j,a,b=L-m} P\left[x_m(a, b) | d\left[x_m(i, j), x_m(a.b)\right] \leq r, (a, b) \neq (i, j)\right] \tag{5.8}$$

where r a similarity threshold, N_m is the total number of square windows, P is the probability of pixels set $x(i, j)$ satisfying specific conditions, $U_m(r)$ is the average probability, and d is a distance function to calculate the difference of corresponding points.

Actual Entropy (*AE*): To capture the full spatial-temporal order present in a user's mobility pattern, Song *et al.* proposed an actual entropy model using the Lempel-Ziv algorithm. Different to other types of entropy, actual entropy depends not only on the frequency of visited locations but also on the order in which the nodes were visited and the time spent at each location [180]. In this chapter, the given area is segmented using structured grids, where each grid is initialized as 0. Then the visited locations and whether the person reached the cell previously are tracked. If the person visits an unreached cell, the location is marked as 1, which finally generates time-series binary data to characterize the trajectory. The actual entropy E_a is calculated using:

$$E_a = \left(\frac{1}{n} \sum_i \Lambda_i \right)^{-1} \ln(n) \tag{5.9}$$

where Λ_i is the length of the shortest sub-string starting at position i which does not previously appear from position 1 to $i-1$, and n is the length of the binary trajectory data.

Similarity of Outcome

In order to understand whether users with similar trajectories receive similar outcomes from the models, I first need to define what it means to receive a similar outcome. As the objective of the PUT models is to optimize privacy and prediction accuracy, I consider privacy gain and utility gain as a positive outcome and measure the *differences* in privacy and utility gains of similar users. I do so based on two techniques, one by simply measuring *pair-wise differences* of outcomes: That is for u_i and u_j with similarity greater than a ϵ threshold, I measure difference in privacy gain outcome, D_{pri}, as $\Delta D_{pri} = 1 - D_{pri}(u_i)/D_{pri}(u_j)$ and utility gain outcome, D_{uti}, as $\Delta D_{uti} = 1 - D_{uti}(u_i)/D_{uti}(u_j)$.

Alternative to thresholding, a second approach is to rely on a *clustering* technique to group similar users together. I use k-means clustering to cluster users based on their SSIM and Entropy features together. I apply the Elbow method and Silhouette method [260] to determine the number of clusters (k values). The resulting clusters present a group of highly similar users together. I then calculate the average pairwise differences ΔD_{pri} and ΔD_{uti} for all the members of each cluster.

Regardless of the grouping technique, I argue that ΔD_{pri} or ΔD_{uti} satisfies fairness if it is within $1-\epsilon$, otherwise I consider the PUT model to have *violated individual fairness* for user pair u_i and u_j. The threshold of different combinations of entropy and SSIM are utilized to distinguish similar users and map all users into a list of *pairs* with trajectory similarity and performance discrepancy. To measure the fairness of systems as a whole for each model and outcome, I report the percentage of user pairs for whom fairness was violated (*i.e.*, *violation*% or *V*%). As I will show, in the experiments, I set $\epsilon = 0.8$ to correspond to users with at least 80% similarity of trajectory which imposes the outcome of the model to be within 20% difference between the similar users. The choice of $\epsilon = 0.8$ is based on the *Four-Fifths Rule*, which is the adverse impact measure used by Uniform Guidelines on Employee Selection Procedures [261, 262].

5.4 Experiment Setup

In this section, I describe the datasets I used for evaluating the fairness of the PUT models and the steps I took to set up the PUT models for examination.

5.4.1 Datasets

In order to evaluate the fairness of the examined models, I use two datasets that the original studies used to evaluate the privacy level of their models.

MDC

The MDC dataset, recorded from 2009 to 2011, contains a large amount of continuous mobility data for 184 volunteers with smartphones running a data collection software, in the Lausanne/Geneva area. Each record of the *gps-wlan* dataset represents a phone call or an observation of a WLAN access point collected during the campaign [220]. In addition to the trajectory data, MDC includes individual user demographic information: categorical age groups, gender, and employment status. To the best of my knowledge, MDC is the only dataset that has published users' demographic information along with their trajectories.

Geolife

The Geolife dataset was collected by Microsoft Research Asia from 182 users in the four-and-a-half-year period from April 2007 to October 2011 and contains 17,621 trajectories, mostly at a 5-second sampling rate [247]. As the Geolife dataset does not include demographic attributes of individual users, I am unable to measure the group fairness for this dataset and the analysis suffices for individual fairness.

As mentioned in Section 5.3.3, in Figure 5.1, with the granularity coarsens the trajectories become more blurry and thus more similar to each other. Figure 5.2 confirms this observation by illustrating the SSIM and entropy-based similarity of all the users for varying spatial granularity for both datasets. I can see that as the spatial granularity coarsens I observe an increase in the SSIM values, with users becoming more similar to each other. Furthermore, as different types of entropy are taking different features of the spatial-temporal data into consideration, Figure 5.2 presents the expected similarity of users for each of the entropy-based measures. In addition to the distribution of the entropy values presented in Figure 5.2 for each dataset, I observe that across both datasets, SSIM along with Shannon and Actual Entropy correspond to the most relaxed measure of similarity, LonLat and Heatmap Entropy correspond to stricter measures

of similarity. The corresponding percentage of user pairs that meet each similarity criterion is described in Table 5.1.

5.4.2 Original Properties of the Trajectory

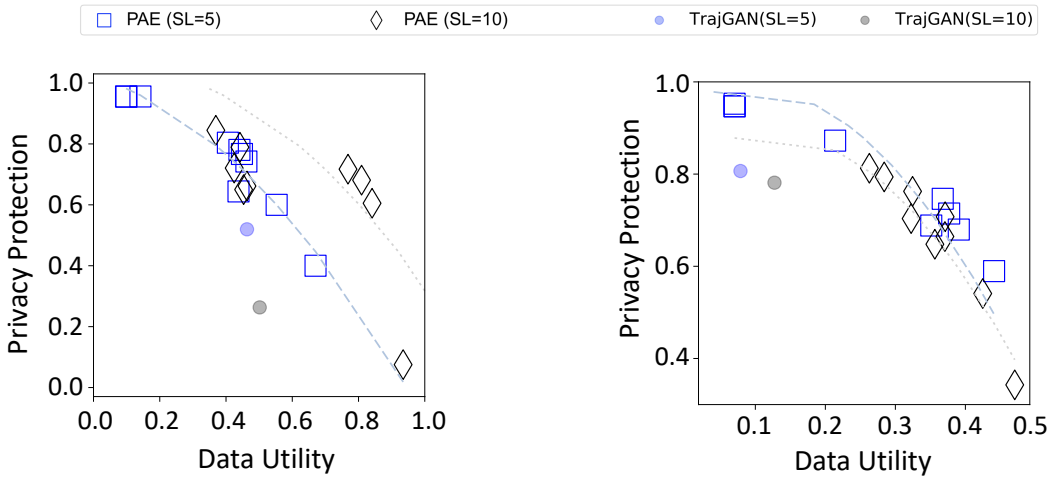
Before describing the privacy and utility trade-off for mobility trajectories of the PUT models, I first give brief definitions of two popular inference tasks (*i.e.*, *user re-identification and mobility prediction*), which are also applied to assess the privacy gain and utility decline in the PUT models I discussed. These two popular inference tasks are named *original tasks* in this chapter, where *original* demonstrates the nature of the data before being processed by any privacy-aware model. These *original* tasks are leveraged to assess the native characteristics of data in terms of *trajectory uniqueness* and *mobility predictability*, respectively.

User Re-identification Task (UR)

The accuracy of the user re-identification task is leveraged to assess the *trajectory uniqueness* of the mobility trajectory. With more and more intelligent devices and sensors being utilized to collect information about human activities, the trajectories also expose increasingly intimate details about users' lives, from their social life to their preferences. A mobility privacy study conducted by De Montjoye *et al.* [29] illustrates that four spatial-temporal points are enough to identify 95% of the individuals in a certain granularity. As human mobility traces are highly unique, a mechanism capable of reducing the user re-identification risk can offer enhanced privacy protection in mobility data sharing. The enhanced privacy protection is referred to *privacy gain* (or *PG*) in the PUT models.

Mobility Prediction Task (MP)

The accuracy of the mobility prediction task is leveraged to assess the *predictability* of the mobility trajectory. Mobility datasets are of great value for understanding human behaviour patterns, smart transportation, urban planning, public health issue, pandemic management, etc. Many of these applications rely on the next location forecasting of individuals, which in the broader context can provide an accurate portrayal of citizens' mobility over time. For the mobility prediction task in this work, the raw geolocated data or other mobility data commonly contain three elements: user identifier u, timestamps t, and location identifiers l. Hence, each location records r could be denoted as $r_i = [u_i, t_i, l_i]$, while each location sequence S is a set of ordered location records $S_n = \{r_1, r_2, r_3, \cdots, r_n\}$, namely *mobility trajectory*. Therefore, given the past mobility trajectory $S_n = \{r_1, r_2, r_3, \cdots, r_n\}$, the mobility prediction task is to infer the most likely location l_{n+1} at the next timestamp t_{n+1}. The results of two PUT models



(a) MDC (b) Geolife

Figure 5.3: Pareto Frontier trade-off of Utility and Privacy on two datasets. The hollow squares and diamonds present the results of the PAE models. The solid points present the results of the TrajGAN. Blue colour presents sequence length $SL = 5$. Black colour presents $SL = 10$.

indicate that a bit of mobility prediction accuracy is sacrificed in exchange for higher privacy protection. The sacrificed prediction accuracy is referred to *utility decline* in the PUT models.

5.4.3 Performance of the Privacy-Utility Trade-off Models

Before examining fairness, I first offer an analysis and comparison of the two described PUT models that I am investigating in terms of fairness. Figure 5.3 presents the privacy utility trade-off of PAE and TrajGAN over the two described datasets. The y-axis presents the privacy gain brought to the raw dataset by applying these models, whereas the x-axis presents the decline in privacy prediction due to this privacy gain. The data fed into the PAE [246] are a list of trajectories with specific sequence length SL, that is $\{S^1_{sl}, S^2_{sl}, S^3_{sl}, \cdots, S^j_{sl}\}$. For instance, if the sequence length is 10, that indicates each trajectory contains 10 history location records r, S_{10} = $\{r_1, r_2, r_3, \cdots, r_{10}\}$, and $SL = 10$.

As PAE is highly dependent on the sequence length and Lagrange multipliers that indicate to what extent privacy or utility must be optimized, each point on the corresponding plots presents experiments with one set of hyper-parameters. These results show that as the PAE achieves maximum privacy protection it comes with the cost of degrading the prediction accuracy. Similarly, TrajGAN achieves 80% privacy gain when applied on Geolife Dataset but it highly degrades the utility. For the Lagrange multipliers setting of the PAE in this work, I choose $\lambda_1 = -0.1$, $\lambda_2 = 0.8$, $\lambda_3 = -0.1$, as this combination exerts the most promising privacy-utility trade-off in the PAE model.

Although these results are helpful in quantifying the Pareto Frontier limit of privacy and

utility they fail to indicate whether the achieved *privacy* or *utility* is the same for all the users in the datasets or whether such models perform better for a group of users, and fail for others. In the next section, I tackle this research question by measuring individual and group fairness.

5.5 Fairness Analysis

In this section, I present the analysis to study whether the PUT models can be considered fair. To do so, I analyze these models in terms of individual fairness and group fairness. The similarity applied in the individual fairness is defined by SSIM and different types of entropy, and the one in the group fairness is based on demographic attributes such as gender, age, and employment status.

5.5.1 Individual Fairness

The metrics of trajectories' similarity are crucial for the quantification of individual fairness. As discussed in Section 5.3.3, the similarity of trajectories can be quantified by SSIM and different types of entropy. In this section, I discuss individual fairness with two different similarity quantification approaches. First, the trajectories' similarity is discriminated against based on thresholding metrics of entropy and SSIM directly. Second, k-means clustering based on the entropy and SSIM characteristics aforementioned is leveraged to classify similar users.

Similarity Based on Thresholding

Table 5.1 presents the individual fairness based on thresholding metrics of entropy and SSIM among different models. The threshold of different combinations of entropy and SSIM are utilized to distinguish similar users ($u_i \backsim u_j$) and map all users into a list of *pairs* with trajectory similarity and performance discrepancy. Based on fairness thresholding criteria defined in Section 5.3.3, *similar users* (*i.e.*, *user pairs*) imply at least 80% pairwise similarity of their trajectories. *"% of pairs"* in the table represents the percentage of the user pairs that meet the corresponding metric threshold requirements. For instance, with the MDC dataset, 36.17% of *user pairs* have a more than 80% similarity when under SE metric. That is, under the SE metric, 36.17% user pairs are qualified for further analysis of outcome similarity.

The *user pair* is defined to achieve individual fairness when the outcome difference (ΔD_{pri} or ΔD_{uti}) between u_i and u_j is within 20%. Table 5.1 shows the percentage of *user pairs* that commit fairness violation (*i.e.*, V% = % of (ΔD>0.2)). For instance, in Table 5.1, with the MDC dataset under the SE metric, there are only 10.50% and 11.11% of the *qualified user pairs* violate the fairness criteria in two original tasks, which implies that individual fairness is

	Metrics	% of pairs	Original, V% of (DIFF>0.2)		PAE, V% of (DIFF>0.2)		TrajGAN, V% of (DIFF>0.2)	
			Trajectory Uniqueness	Mobility Predictability	Privacy Gain	Utility Decline	Privacy Gain	Utility Decline
MDC	SE	36.17%	*10.50%*	*11.11%*	87.69%	39.75%	41.65%	27.32%
	LE	12.85%	*8.31%*	*7.90%*	88.81%	36.95%	41.32%	**25.10%**
	HE	14.11%	*12.89%*	*9.60%*	86.88%	41.30%	**38.23%**	27.14%
	AE	33.05%	*12.64%*	*10.28%*	87.10%	35.95%	**45.26%**	**29.42%**
	SSIM	65.06%	***14.57%***	***13.17%***	**88.98%**	**42.02%**	39.50%	27.50%
	4 Entropy	1.73%	***6.10%***	***1.22%***	84.76%	**30.49%**	44.51%	27.44%
	4 Entropy+SSIM	1.64%	*6.45%*	*1.29%*	**83.87%**	31.61%	43.23%	28.39%
Geolife	SE	33.16%	57.91%	61.09%	94.14%	71.84%	67.85%	58.58%
	LE	9.11%	**57.41%**	61.20%	**94.32%**	71.50%	65.09%	56.05%
	HE	7.29%	61.37%	**63.47%**	94.09%	70.43%	69.78%	58.87%
	AE	27.03%	57.44%	59.36%	93.23%	72.96%	71.96%	58.54%
	SSIM	63.52%	59.88%	61.49%	94.13%	**74.77%**	**63.53%**	**53.05%**
	4 Entropy	0.62%	61.54%	58.46%	**89.23%**	66.15%	**78.46%**	**72.31%**
	4 Entropy+SSIM	0.61%	**62.50%**	**57.81%**	89.06%	**65.63%**	78.13%	71.88%

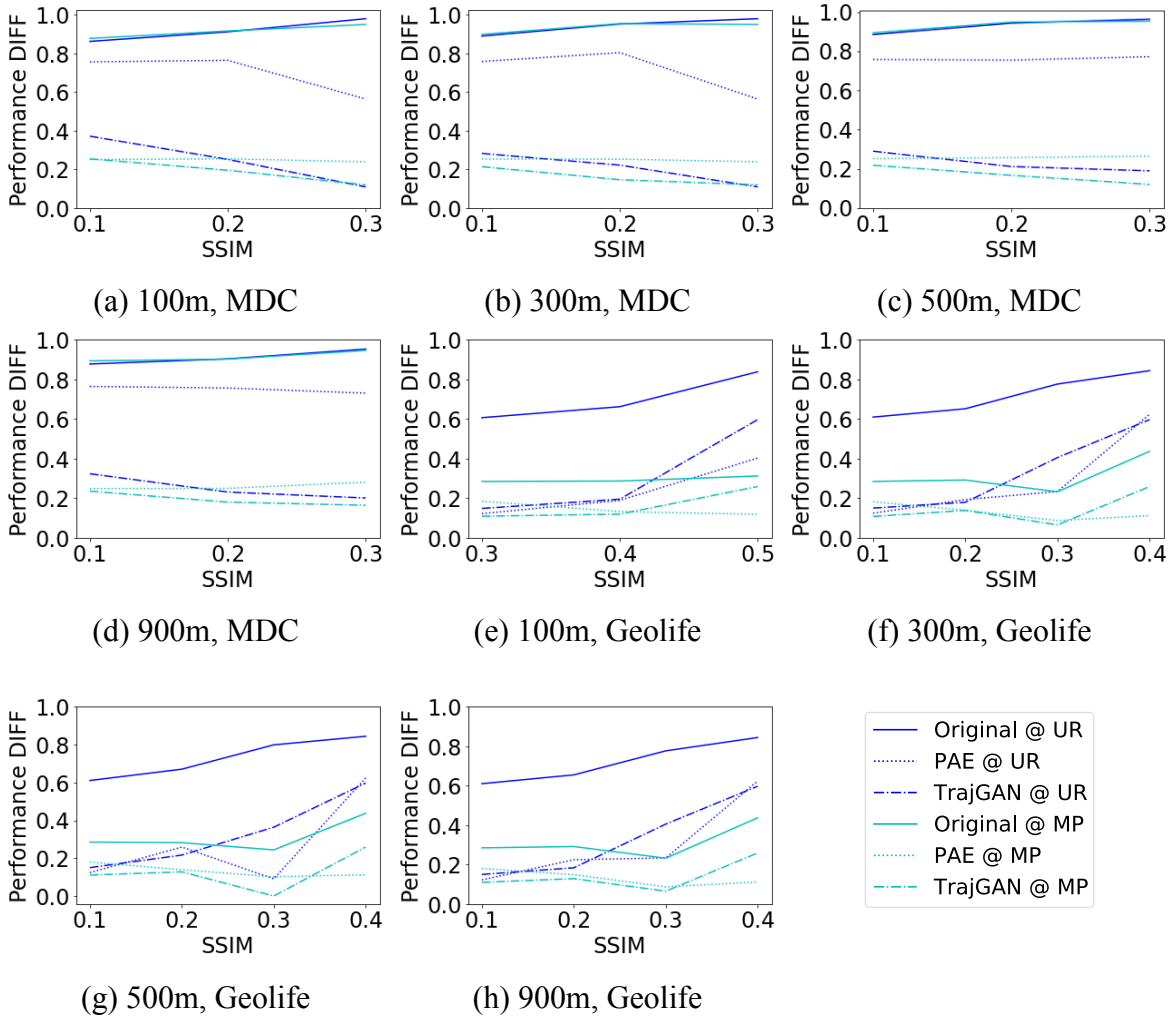
Table 5.1: Individual fairness among diverse models and datasets that are based on SSIM and different types of entropy. SE represents *shannon entropy*; LE represents *lonlat entropy*; HE represents *heatmap entropy*; AE represents *actual entropy*; *4 Entropy* means the chosen trajectory mates are restricted by SE, LE, HE and AE in the same time; *4 Entropy+SSIM* then apply the SSIM restriction with the *4 Entropy*. *% of pairs* represents the ratio of the pairs that meet the thresholding requirements. The maximum/minimum instances of each column are highlighted in **bold font**.

achieved, as both V% are within 20%. Different from the original tasks, two PUT models have V% that are all higher than 20%, hence, the performance of two PUT models violates individual fairness. The higher V% indicates that more disparities in performance are caused by the model. The values in the *italic format* present the cases where the outcome meets individual fairness (*i.e.*, $V\% \leq 20\%$) in Table 5.1.

Overall, individual fairness is not achieved in the two selected PUT models. Especially for the unfairness of the privacy gain, which is generally higher than the utility decline. When comparing two different privacy models in a row, TrajGAN achieves less fairness violation rate than PAE in both privacy gain and utility decline outcomes. For instance, in the MDC dataset, when 45.26% and 29.42% of user pairs commit fairness violations in privacy gain and utility decline, respectively, the PAE reports twice as many fairness violations for both outcomes. While both the Geolife and MDC data exhibit individual unfairness, the Geolife is worse in both the PUT models and the accuracy of the *original tasks*. In both original tasks, Geolife's unfairness rate is as high as 60%, and this inequity is exacerbated when with PUT models. In contrast to Geolife, the performance of the MDC in the original tasks conforms to the definition of individual fairness, that is, the performance difference of task accuracy in MDC is within 20% in both user re-identification tasks and mobility prediction tasks.

Impact of Spatial Granularity on Similarity: After the overall comparison of threshold metrics, I discuss the model discrepancy when trajectory similarity is based on the SSIM index under varying granularity. As a crucial metric in distinguishing the trajectory similarity, the SSIM index could be affected by different parameters, which will result in subtle performance disparities in the quantification of individual fairness. The spatial granularity of trajectory is the most important one among these parameters. These disparities could be intuitively observed in the heatmaps (Figure 5.1). In contrast to the SSIM, the spatial granularity has less impact on different types of entropy, hence, they are not in discussion here.

Figure 5.4 then shows the impact of varying spatial granularity on the model discrepancy. The model which achieves individual fairness should perform less discrepancy when with higher SSIM. The accuracy of original tasks and two PUT models are compared in granularity at 100 meters, 300 meters, 500 meters, and 900 meters. In conclusion, different models have diverse sensitivities of varying granularities. For both original tasks (UR and MP) in two datasets, they all have an increasing difference when with a higher SSIM index, which means that they violate individual fairness. For the PAE, individual fairness is met on MDC data but not on Geolife. The PAE is also the most sensitive model for varying granularities. For instance, when granularity changes from 100-meter (Figure 5.4a) to 900-meter (Figure 5.4d), PAE has the most obvious change of its line trend on the UR (*i.e.*, privacy gain), and the decreasing trend at 100-meter granularity is lost at 900-meter. Overall, the selection of SSIM granularity has a significant impact on the judgement of the individual fairness of a model. However, these impacts become subtle when the SSIM is applied to the trajectory similarity distinction, as the user



(a) 100m, MDC (b) 300m, MDC (c) 500m, MDC

(d) 900m, MDC (e) 100m, Geolife (f) 300m, Geolife

(g) 500m, Geolife (h) 900m, Geolife

Figure 5.4: The model performance discrepancy when trajectory similarity is based on the SSIM in different granularities (*i.e.*, 100 m, 300 m, 500 m, and 900 m). Figures (a) to (d) are the results of the MDC dataset, and Figures (e) to (h) are of Geolife. UR is short for user re-identification task, MP is for the mobility prediction task. The performance discrepancy (*i.e.*, Performance DIFF) of each model in different granularities compares in each sub-figure.

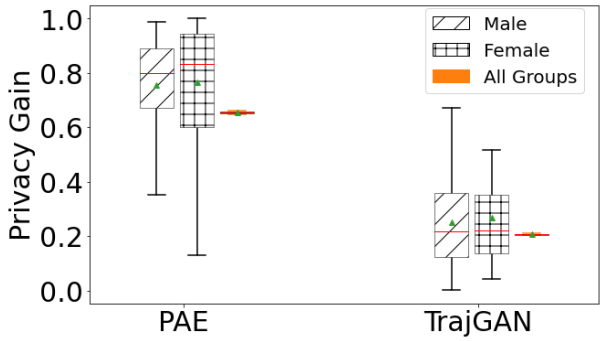
pairs table reduced the granularity impact to some extent. For the remaining of the analysis, the granularity of the SSIM is chosen as 100-meter.

Similarity Based on K-means Clustering

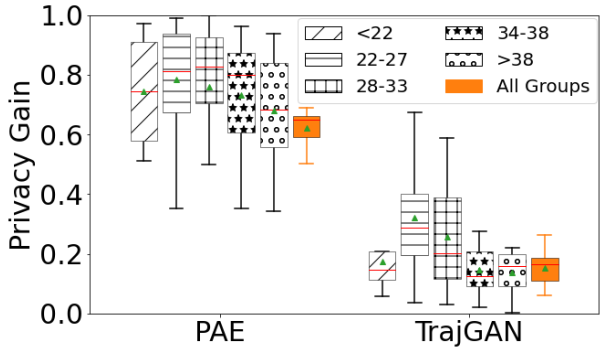
Alternative to the results presented based on the similarity thresholding, Table 5.2 demonstrates the results of individual fairness based on the clustering technique described in Section 5.3.3. Based on applying the Elbow method and Silhouette method, the number of clusters (k) for MDC and Geolife are 4 and 5, respectively. For each cluster, the table reports the percentage of users whose individual fairness was violated for a given outcome and under various models. More precisely, the results presented here indicate that the original model that objectifies a single task (prediction or privacy) is able to meet the individual fairness criteria for the MDC

	Metrics	Cluster Size	Original, V% of (DIFF>0.2)		PAE, V% of (DIFF>0.2)		TrajGAN, V% of (DIFF>0.2)	
			Trajectory Uniqueness	Mobility Predictability	Privacy Gain	Utility Decline	Privacy Gain	Utility Decline
MDC	Cluster 1	26	*14.77%*	*15.38%*	**83.69%**	**48.92%**	50.77%	33.85%
	Cluster 2	5	***0.00%***	***0.00%***	**90.00%**	***0.00%***	40.00%	***0.00%***
	Cluster 3	43	***17.39%***	***17.17%***	88.15%	48.84%	**55.92%**	**43.63%**
	Cluster 4	24	***0.00%***	***0.00%***	86.23%	*16.67%*	**35.87%**	*17.75%*
	Clusters Average	-	*12.99%*	*12.18%*	88.86%	39.36%	51.26%	34.49%
Geolife	Cluster 1	21	**55.71%**	***13.81%***	**60.00%**	*1.43%*	*18.57%*	***0.00%***
	Cluster 2	17	46.32%	*8.09%*	49.26%	*13.97%*	*16.91%*	***0.00%***
	Cluster 3	9	***13.89%***	*11.11%*	38.89%	**16.67%**	***13.89%***	***11.11%***
	Cluster 4	10	31.11%	***0.00%***	40.00%	***0.00%***	**44.44%**.	*4.44%*
	Cluster 5	36	44.92%	*8.57%*	**29.84%**	*5.56%*	23.02%	*0.16%*
	Clusters Average	-	43.91%	*9.15%*	47.11%	*7.55%*	26.53%	*2.02%*

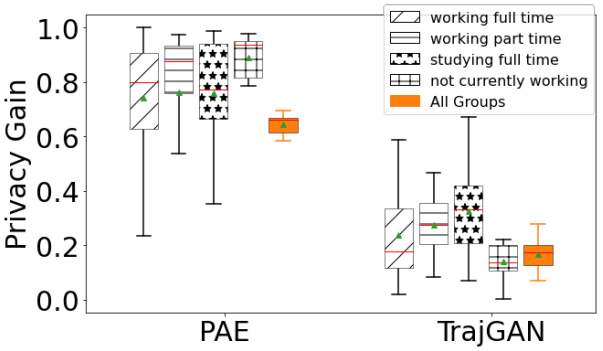
Table 5.2: K-means-clustering-based individual fairness among diverse models and datasets. The numbers present the percentage of users for whom individual fairness was violated based on their difference in the outcome being greater than 0.2. The fair instances are highlighted in *italic font*. The maximum/minimum instances of each column are highlighted in **bold font**.



(a) Gender



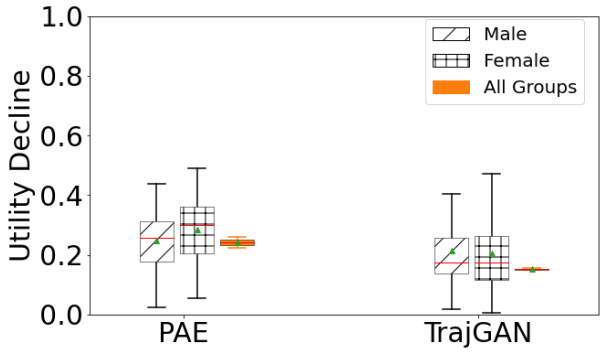
(b) Age



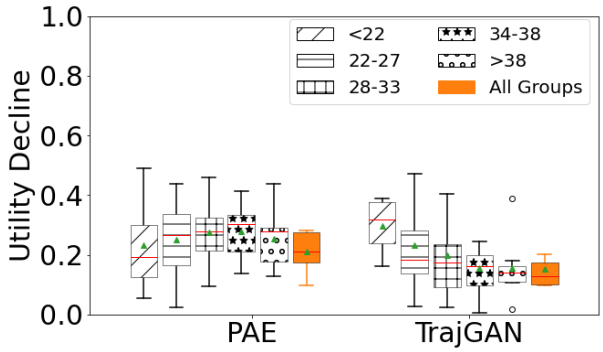
(c) Working Status

Figure 5.5: The privacy protection outcome of PUT models across different demographic groups for the MDC dataset. The black box shows how the privacy gain varies across the individual within the same demographic group. The orange box denotes the differences across the groups, the smaller box means the model satisfies more group fairness.

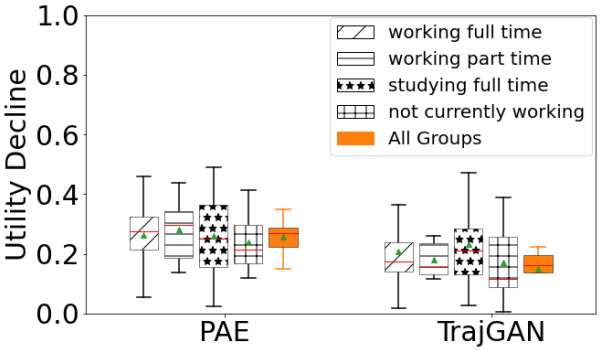
dataset. It can be observed that in the case of the PAE model, the privacy gain across exhibits high variations across users in the same clusters. Even in the cases where the model satisfies individual fairness by performing similarly in terms of utility decline (clusters 2 and 4 of MDC and all clusters of Geolife), the privacy gains of those users are very different from each other.



(a) Gender



(b) Age



(c) Working Status

Figure 5.6: The prediction accuracy outcome of PUT models across different demographic groups for the MDC dataset. The black box shows how the privacy gain varies across the individual within the same demographic group. The orange box denotes the differences across the groups, the smaller box means the model satisfies more group fairness.

5.5.2 Group Fairness

Group fairness states that demographic groups should receive similar decisions. To be specific, group fairness argues that a disadvantaged group should receive similar treatment to the advantaged group. Figure 5.5 presents the discrepancy of the *privacy gain* from two PUT models for different demographic groups, and Figure 5.6 presents the *utility decline*. It is observed that both PAE and TrajGAN perform equally for different gender attributes, as shown in Figure 5.5a, where the orange boxes (labelled as *All Groups*) on both are very small. That is while the privacy gain varies across individuals within the same gender, the model achieves group fairness when grouping individuals by gender. The same observations could be made for the age and employment status, which exist bigger differences across the classes than gender, but they still achieve group fairness as $\Delta D < 20\%$. Similarly, in Figure 5.6, both models equally meet the group fairness criteria on the utility decline.

In order to quantify the group fairness of the *disadvantaged groups* in a more statistical approach, the results of the *group fairness score* (*GFS*) are shown in Table 5.3. For instance, for different age groups, the subgroup with ages between 22 and 27 (*i.e.*, "22 - 27") is regarded as the *advantaged* group, as it has the dominant user number for all age groups. The other age groups' GFSs are calculated based on the disparate impact between them and the *advantaged* group. Then, compare all GFSs against the fairness threshold of 0.8, which is defined in Section 5.3.3, that is, $GFS \geq 80\%$ indicates the fairly treat the disadvantaged group and $GFS < 80\%$ indicates the unfairly treating. For example, the result of the "28-33" group (*i.e.*, $GFS = 98.65\%$) then indicated that the model satisfies the group fairness as 98.65% > 80%.

In conclusion, except for two subgroups with age attribute (*i.e.*, "<21" and ">39") violating the four-fifths rule, the other subgroups satisfy the group fairness. Finally, it is worth noting that the results presented here are highly dependent on the studied dataset, which will be discussed in detail in the next section.

5.6 Discussion

In this section, I describe the limitations and implications of this work and discuss possible future directions.

5.6.1 Limitation

Despite my efforts, the presented chapter also has its limitations. Firstly, the collected mobility dataset are often biased as they only present a subset of the population who took part in data collection. In many cases, the users are limited to students or those affiliated with the research

		users #	Original, GFS		PAE, GFS		TrajGAN, GFS	
			Uniqueness	Predictability	PrivacyGain	UtilityDecline	PrivacyGain	UtilityDecline
Gender	Male	56	-	-	-	-	-	-
	Female	33	98.07%	96.35%	98.04%	90.13%	96.57%	95.00%
Age	<21	5	94.48%	99.10%	**46.09%**	85.86%	84.73%	87.38%
	22-27	38	-	-	-	-	-	-
	28-33	29	98.65%	94.49%	96.97%	97.36%	90.16%	93.74%
	34-38	11	97.98%	98.54%	91.13%	99.55%	81.81%	92.74%
	>39	9	95.76%	99.73%	**75.51%**	94.05%	83.47%	91.30%
Working	Full-time work	48	-	-	-	-	-	-
	Part-time work	8	95.80%	96.44%	82.58%	85.24%	99.67%	94.81%
	Full-time student	26	98.09%	99.23%	97.83%	88.16%	85.77%	88.37%
	Others	8	95.80%	99.33%	98.70%	93.59%	95.36%	99.07%

Table 5.3: Group fairness scores (*GFS*) of three models with different demographic attributes. $GFS \geq 80\%$ indicates the fairly treating the minority subgroup; $GFS < 80\%$ indicates the unfairly treating.

team that has collected the dataset. This means the examined trajectories are not representative of everyone's mobility behaviour. Furthermore, the demographics of the participants are also limited in terms of age and socio-economic diversity.

Secondly, in this chapter, I reported that I did **not** observe any violation of group fairness across gender, age and employment level for the examined PUT models. However, I acknowledge that the results presented regarding group fairness are highly influenced by the city and societal structures that data collected. In the case of MDC, the trajectories of users correspond to a level of socio-economic and cultural freedom that is associated with life in Switzerland. Such observations will surely differ if I was to examine other cultures such as those in the United States or Asian countries where there exists a wider socio-economic and gender inequality gap. I also believe the availability of datasets with rich demographic information could enable future work to examine the intersection of individual fairness within demographic groups.

5.6.2 Implication

This chapter has multiple important implications: first, this work offers a novel methodology for defining fairness in the context of spatial-temporal datasets. I believe works such as this will help shape the future roadmap of fairness in Machine Learning studies by offering the possibility to measure equity within different systems such as those of mobility-based ones (*e.g.*, transportation). The choice of which of the proposed similarity metrics to select for evaluating individual fairness is also another important dimension that could be highly context and application-dependent. For example, for applications where there is a need for strict fairness measurement, corresponding to the WYZIWIG worldview [245], a strict similarity measure such as Combined Entropy could be chosen. In contrast for applications where the groups are not necessarily equal, but for the purposes of the decision-making process, I would prefer to treat them as if they were, a less sensitive similarity measure such as coarse grain SSIM could be used.

Although this chapter focus on fairness analysis of the PUT models, I believe this study can be the first step towards implementing fairness interventions that are embedded in these models. For example, in-processing approaches rely on adjusting the model during the training to enforce fairness goals to be met and optimized in the same manner as accuracy is. This is often achieved through adversarial networks or fair representation learning approaches such as [263], model induction, model selection, and regularization [243]. I believe designing privacy-aware models to become fairness-aware is a research direction that would receive significant attention in the future.

5.7 Conclusion

Intuitively, fairness has a close relationship to privacy, no matter structural data or unstructured data in machine learning. But the quantification between them is still unclear. In this chapter, I proposed different metrics for measuring individual fairness in the context of spatial-temporal mobility data. I compared different location privacy-protection mechanisms, PUT models, on the defined metrics for both individual and group-based. The results on two real trajectory datasets show that the privacy-aware models achieve fairness at the group level but violate individual fairness. The findings raise questions regarding the equity of the privacy-preserving models when individuals with similar trajectories receive a very different level of privacy gain. I leverage the empirical results of this chapter to make valuable suggestions for the further integration of fairness objectives into the PUT models.

Chapter 6

Summary and Outlook

6.1 Conclusions and Contributions

Undoubtedly, the pandemic accelerated the digital transformation of the world. With the purpose of making human mobility and activity models more inclusive, private, and fair, it is exceptionally beneficial to explore and build more realistic and reliable models within a privacy-preserving framework. In this thesis, I developed and implemented advanced methods/algorithms to model human mobility and activity in terms of temporal-context dynamics, multi-occupancy impacts, privacy protection, and fair analysis. The main conclusions are summarized as follows:

- Towards mapping contextual-temporal dynamics in human activity modelling, I conducted a series of experiments and leveraged activity-level experiments to evaluate the performance of predictive models with integrated temporal information. This work highlighted that a deep learning network with an integrated timestamp could have better prediction performance, which is essential for further human behaviour modelling and prediction. I concluded how the contextual-temporal dynamics will exert influence on the final predictive model performance. The result demonstrated the performance improvement of the prediction accuracy for the next activity and time.
- To model human activity in multiple-occupancy smart homes, I presented *MoSen*, a framework for accelerating the actual implementation of sensor-based activity recognition systems by analyzing the trade-off between the overall system performance and cost. Often, researchers in a lab setting prefer the best technology with the highest accuracy, while the accumulated cost is hard to afford in actual home designs. Moreover, the floorplans and furniture layouts are unique for each home, which results in highly diverse sensor layouts in the real environment. *MoSen* emulates multiple-occupancy scenarios with synthetic multi-occupancy behaviour models and can be extended to *different* floorplan or sensor configuration. I evaluated the efficacy of the *MoSen* with an automatic identification annotation task using experiments on synthetic datasets and show how the annotation accuracy

is affected by the number of residents, different localization resolutions, and sensor density. Through the trace-driven simulations, I also analyzed the effect of each sensor. Then the sensor selection strategy for the system will be provided. The initial analysis of different sensor configurations will provide the designers or practitioners with an effective sensor selection strategy.

- To explore an effective privacy-aware network in human mobility modelling, I implemented a privacy-preserving architecture based on adversarial networks (*i.e.*, Mo-PAE). The proposed model considered three different optimization objectives and searched for the optimum trade-off for the utility and privacy of a given dataset. I reported an extensive analysis of the proposed model performances and the impact of its hyperparameters using four real-world mobility datasets. The weights $\lambda_1,\ \lambda_2$, and λ_3 bring more flexibility to the proposed framework, enabling it to satisfy different scenarios' requirements according to the relative importance of utility requirements and privacy budgets. I evaluated the framework on four datasets and benchmarked the results against an LSTM-GAN approach and a DP mechanism. The comparisons indicated the superiority of the proposed framework and the efficiency of the proposed privacy-preserving feature extractor Enc_L.
- To characterize mobility data on privacy and fairness, I proposed different metrics for measuring individual fairness in the context of spatial-temporal mobility data. Intuitively, fairness is closely related to privacy, whether structural or unstructured data in machine learning. But the quantification between them is still unclear. I examined the fairness of two state-of-the-art privacy-preserving models that rely on GAN and representation learning to reduce the re-identification rate of users for data sharing. The results on two real trajectory datasets show that the privacy-aware models achieve fairness at the group level but violate individual fairness. The findings raise questions regarding the equity of the privacy-preserving models when individuals with similar trajectories receive a very different level of privacy gain.

6.2 Discussion and Future Work

With the increasing digital trend, the proliferation of IoT and smart homes will push different devices/applications to occupy every corner of our lives. Towards the smart home scenario, especially for healthcare purposes, future work should systematically integrate the temporal information into deep learning algorithms to provide a time-sensitive model with higher prediction accuracy. Furthermore, indoor wireless signal-based activity recognition technologies are expected to have better continuity in the near future, as the longer time duration of the dataset might provide better performance. Different data fusion to build a multimodal intelligent predictive ecosystem is beneficial. In the past, when anticipating future activity, researchers would

like to choose an activity level or action level but were less focused on two-level comparisons. In future work, the activity prediction problem from both levels will be more beneficial.

Another challenge in activity prediction and even activity recognition is the multi-person scenario. First, different from the single-occupancy scene, the interactions between residents introduce uncertainty when defining indoor activities. The interaction between multiple residents can make the predictive model more intricate and obscure in generating plausible inferences. Second, annotating the triggered sensor with corresponding identification and activity is challenging in the multi-resident scenario. The lack of ground-truth values is deficient to the multiple-analysis with advanced machine learning or deep learning technologies. Due to the data scarcity of the multi-occupancy scene, the synthetic method bridges the gap. The analysis is valuable for researchers or practitioners to design a real multi-occupancy scenario in the future. Third, data privacy is a big concern when collecting real human data. Even for the sensor-based activity recognition system, which does not invade privacy as severely as the video-based systems, there still is a need to attain the trade-off between data utility and privacy. Fourth, numerous challenges still need to be overcome in the single-occupancy environment [39]. Human activities are hard to model uniformly, especially when they have different backgrounds, diverse habits, and varied activity performances [160]. The uncertainty from the spatial and temporal difference also increases this difficulty [42]. In the multi-occupancy scenario, activity recognition becomes more sophisticated and challenging with the increasing number of residents. There is also a trade-off between the RTLS localization resolution and sensor costs. Finally, the floorplans and furniture layouts are unique for each home, which results in highly diverse sensor layouts in a real environment. These gaps impede the practical data collection on the multi-occupancy scenario. *MoSen* system can extend to *different* floorplans, and the initial analysis of each specific scenario provides designers with information on designing a sensor-based system with a better cost-accuracy balance. But more should be explored to make the activity recognition technology beneficial for each home.

Privacy and fairness will be increasingly important with the proliferation of IoT technologies. By expanding Mo-PAE, other utility functions could be considered, such as community detection based on unsupervised or deep-embedded clustering methods. Additionally, automated search techniques, such as deep deterministic policy gradient algorithm and reinforcement learning, could be leveraged to search for the optimal weight combinations efficiently. More scenarios of different data utilities could improve the robustness of the proposed architecture. When it terms to the relationships between fairness and privacy, I investigated the fairness analysis of the PUT models. This study can be the first step toward implementing fairness interventions embedded in these models. For example, in-processing approaches rely on adjusting the model during the training to enforce fairness goals to be met and optimized in the same manner as accuracy. This is often achieved through adversarial networks or fair representation learning approaches such as [263], model induction, model selection, and regularization [243].

I believe designing privacy-aware models to become fairness-aware is a research direction that will receive significant attention in the future.

Bibliography

[1] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[3] S. Li, L. D. Xu, and S. Zhao, "The internet of things: A survey," *Information systems frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[4] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of cleaner production*, vol. 140, pp. 1454–1464, 2017.

[5] M. Satyanarayanan *et al.*, "Edge analytics in the internet of things," *IEEE Pervasive Computing*, vol. 14, no. 2, pp. 24–31, 2015.

[6] R. Zhang, F. Hao, and X. Sun, "The design of agricultural machinery service management system based on internet of things," *Procedia Computer Science*, vol. 107, pp. 53–57, 2017.

[7] R. Mehmood, S. S. I. Katib, and I. Chlamtac, *Smart infrastructure and applications*. Springer, 2020.

[8] S. Hussain, U. Mahmud, and S. Yang, "Car e-talk: An iot-enabled cloud-assisted smart fleet maintenance system," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9484–9494, 2020.

[9] Y. Ding, M. Jin, S. Li, and D. Feng, "Smart logistics based on the internet of things technology: An overview," *International Journal of Logistics Research and Applications*, vol. 24, no. 4, pp. 323–345, 2021.

[10] B. Krishnamachari, J. Power, S. H. Kim, and C. Shahabi, "I3: An iot marketplace for smart communities," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, 2018, pp. 498–499.

[11] L. J. Bowman, "Statista," *Journal of Business & Finance Librarianship*, pp. 1–6, 2022.

[12] R. B. Bouncken and S. Kraus, "Entrepreneurial ecosystems in an interconnected world: Emergence, governance and digitalization," *Review of Managerial Science*, vol. 16, no. 1, pp. 1–14, 2022.

[13] S. Dash and V. Suryanarayana, "Personal safety monitoring devices in wake of covid19: Application of iot and sensor technology," in *High Performance Computing and Networking*, Springer, 2022, pp. 331–343.

[14] R. P. Singh, M. Javaid, A. Haleem, and R. Suman, "Internet of things (iot) applications to fight against covid-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp. 521–524, 2020.

[15] A. Kumar, P. K. Gupta, and A. Srivastava, "A review of modern technologies for tackling covid-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp. 569–573, 2020.

[16] A. Bick, A. Blandin, K. Mertens, *et al.*, *Work from home after the covid-19 outbreak*, 2020.

[17] K. A. Karl, J. V. Peluchette, and N. Aghakhani, "Virtual work meetings during the covid-19 pandemic: The good, bad, and ugly," *Small Group Research*, vol. 53, no. 3, pp. 343–365, 2022.

[18] D. Talevi *et al.*, "Mental health outcomes of the covid-19 pandemic," *Rivista di psichiatria*, vol. 55, no. 3, pp. 137–144, 2020.

[19] D. Banerjee, "The impact of covid-19 pandemic on elderly mental health," *International journal of geriatric psychiatry*, vol. 35, no. 12, p. 1466, 2020.

[20] S. Madakam, V. Lake, V. Lake, V. Lake, *et al.*, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[21] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in iot: A survey," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1667–1693, 2020.

[22] H. Lin and N. W. Bergmann, "Iot privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[23] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "Iot privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.

[24] R. M. Smith and Z. D. Blizard, "A census tract level analysis of urban sprawl's effects on economic mobility in the united states," *Cities*, vol. 115, p. 103 232, 2021.

[25] J. K. Puar, "Circuits of queer mobility: Tourism, travel, and globalization," *GLQ: A Journal of Lesbian and Gay Studies*, vol. 8, no. 1, pp. 101–137, 2002.

[26] A. Taniguchi and S. Fujii, "Promoting public transport using marketing techniques in mobility management and verifying their quantitative effects," *Transportation*, vol. 34, no. 1, pp. 37–49, 2007.

[27] V. Nikulina, D. Simon, H. Ny, and H. Baumann, "Context-adapted urban planning for rapid transitioning of personal mobility towards sustainability: A systematic literature review," *Sustainability*, vol. 11, no. 4, p. 1007, 2019.

[28] O. Gatalo, K. Tseng, A. Hamilton, G. Lin, and E. Klein, "Associations between phone mobility data and covid-19 cases," *The Lancet Infectious Diseases*, vol. 21, no. 5, e111, 2021.

[29] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific reports*, vol. 3, p. 1376, 2013.

[30] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *2011 IEEE symposium on security and privacy*, IEEE, 2011, pp. 247–262.

[31] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46–55, 2003.

[32] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[33] V. Bianchi, M. Bassoli, G. Lombardo, P. Fornacciari, M. Mordonini, and I. De Munari, "Iot wearable sensor and deep learning: An integrated approach for personalized human activity recognition in a smart home environment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8553–8562, 2019.

[34] A. Subasi, M. Radhwan, R. Kurdi, and K. Khateeb, "Iot based mobile healthcare system for human activity recognition," in *2018 15th Learning and Technology Conference (L&T)*, IEEE, 2018, pp. 29–34.

[35] F. J. Rodriguez Lera, F. Martín Rico, A. M. Guerrero Higueras, and V. M. Olivera, "A context-awareness model for activity recognition in robot-assisted scenarios," *Expert Systems*, vol. 37, no. 2, e12481, 2020.

[36] A. Patel and J. Shah, "Sensor-based activity recognition in the context of ambient assisted living systems: A review," *Journal of Ambient Intelligence and Smart Environments*, vol. 11, no. 4, pp. 301–322, 2019.

[37] M. M. Hassan, M. Z. Uddin, A. Mohamed, and A. Almogren, "A robust human activity recognition system using smartphone sensors and deep learning," *Future Generation Computer Systems*, vol. 81, pp. 307–313, 2018.

[38] A. Stisen *et al.*, "Smart devices are different: Assessing and mitigatingmobile sensing heterogeneities for activity recognition," in *Proceedings of the 13th ACM conference on embedded networked sensor systems*, 2015, pp. 127–140.

[39] A. Benmansour, A. Bouchachia, and M. Feham, "Multioccupant activity recognition in pervasive smart home environments," *ACM Computing Surveys (CSUR)*, vol. 48, no. 3, pp. 1–36, 2015.

[40] V. L. Erickson, M. Á. Carreira-Perpiñán, and A. E. Cerpa, "Occupancy modeling and prediction for building energy management," *ACM Transactions on Sensor Networks (TOSN)*, vol. 10, no. 3, pp. 1–28, 2014.

[41] H. Alemdar, H. Ertan, O. D. Incel, and C. Ersoy, "Aras human activity datasets in multiple homes with multiple residents," in *2013 7th International Conference on Pervasive Computing Technologies for Healthcare and Workshops*, IEEE, 2013, pp. 232–235.

[42] D. J. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan, "Casas: A smart home in a box," *Computer*, vol. 46, no. 7, pp. 62–69, 2012.

[43] T. Van Kasteren, A. Noulas, G. Englebienne, and B. Kröse, "Accurate activity recognition in a home setting," in *Proceedings of the 10th international conference on Ubiquitous computing*, ACM, 2008, pp. 1–9.

[44] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat monitoring: Application driver for wireless communications technology," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 2 supplement, pp. 20–41, 2001.

[45] F. Adib, Z. Kabelac, and D. Katabi, "Multi-person localization via rf body reflections," in *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*, 2015, pp. 279–292.

[46] M. Bocca, O. Kaltiokallio, N. Patwari, and S. Venkatasubramanian, "Multiple target tracking with rf sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1787–1800, 2013.

[47] G. Mokhtari, A. Anvari-Moghaddam, Q. Zhang, and M. Karunanithi, "Multi-residential activity labelling in smart homes with wearable tags using ble technology," *Sensors*, vol. 18, no. 3, p. 908, 2018.

[48] J. Wang, Y. Chen, S. Hao, X. Peng, and L. Hu, "Deep learning for sensor-based activity recognition: A survey," *Pattern Recognition Letters*, vol. 119, pp. 3–11, 2019.

[49] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[50] E. Goldman, "An introduction to the california consumer privacy act (ccpa)," *Santa Clara Univ. Legal Studies Research Paper*, 2020.

[51] C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, "Big data privacy in the internet of things era," *IT Professional*, vol. 17, no. 3, pp. 32–39, 2015.

[52] M. Malekzadeh, R. G. Clegg, and H. Haddadi, "Replacement AutoEncoder: A Privacy-Preserving Algorithm for Sensory Data Analysis," en, *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 165–176, Apr. 2018, arXiv: 1710.06564. DOI: 10.1109/IoTDI.2018.00025. [Online]. Available: http://arxiv.org/abs/1710.06564 (visited on 10/23/2020).

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

[54] J. Rao, S. Gao, Y. Kang, and Q. Huang, "Lstm-trajgan: A deep learning approach to trajectory privacy protection," *arXiv preprint arXiv:2006.10521*, 2020.

[55] C. Jobanputra, J. Bavishi, and N. Doshi, "Human activity recognition: A survey," *Procedia Computer Science*, vol. 155, pp. 698–703, 2019.

[56] L. M. Dang, K. Min, H. Wang, M. J. Piran, C. H. Lee, and H. Moon, "Sensor-based and vision-based human activity recognition: A comprehensive survey," *Pattern Recognition*, vol. 108, p. 107 561, 2020.

[57] L. Koumakis, C. Chatzaki, E. Kazantzaki, E. Maniadi, and M. Tsiknakis, "Dementia care frameworks and assistive technologies for their implementation: A review," *IEEE reviews in biomedical engineering*, vol. 12, pp. 4–18, 2019.

[58] I. Vedel, M. Monette, F. Beland, J. Monette, and H. Bergman, "Ten years of integrated care: Backwards and forwards. the case of the province of québec, canada," *International journal of integrated care*, vol. 11, no. Special 10th Anniversary Edition, 2011.

[59] M. Ienca, T. Wangmo, F. Jotterand, R. W. Kressig, and B. Elger, "Ethical design of intelligent assistive technologies for dementia: A descriptive review," *Science and engineering ethics*, vol. 24, no. 4, pp. 1035–1055, 2018.

[60] T. Kurashima, T. Althoff, and J. Leskovec, "Modeling interdependent and periodic real-world action sequences," in *Proceedings of the 2018 World Wide Web Conference on World Wide Web*, International World Wide Web Conferences Steering Committee, 2018, pp. 803–812.

[61] A. Almeida and G. Azkune, "Predicting human behaviour with recurrent neural networks," *Applied Sciences*, vol. 8, no. 2, p. 305, 2018.

[62] Y. Zhan and H. Haddadi, "Activity prediction for improving well-being of both the elderly and caregivers," in *WellComp2019, Proceedings of the 2019 ACM International Symposium on Wearable Computers*, 2019, pp. 1214–1217.

[63] A. F. Bobick, "Movement, activity and action: The role of knowledge in the perception of motion," *Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences*, vol. 352, no. 1358, pp. 1257–1265, 1997.

[64] Q. Ni, A. B. Garcia Hernando, and I. P. De la Cruz, "The elderly's independent living in smart homes: A characterization of activities and sensing infrastructure survey to facilitate services development," *Sensors*, vol. 15, no. 5, pp. 11 312–11 362, 2015.

[65] J. F. Allen, "Maintaining knowledge about temporal intervals," *Communications of the ACM*, vol. 26, no. 11, pp. 832–843, 1983.

[66] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9(8):1735-1780, 1997. [Online]. Available: `https://www.bioinf.jku.at/publications/older/2604.pdf`.

[67] D. Harris and S. L. Harris, *Digital design and computer architecture*. Morgan Kaufmann, 2010.

[68] P. Rodríguez, M. A. Bautista, J. Gonzalez, and S. Escalera, "Beyond one-hot encoding: Lower dimensional target embedding," *Image and Vision Computing*, vol. 75, pp. 21–31, 2018.

[69] W. H. Greene, *Econometric analysis*. Pearson Education India, 2003.

[70] T. Mikolov, W.-t. Yih, and G. Zweig, "Linguistic regularities in continuous space word representations," in *Proceedings of the 2013 conference of the north american chapter of the association for computational linguistics: Human language technologies*, 2013, pp. 746–751.

[71] J. Pennington, R. Socher, and C. D. Manning, "Glove: Global vectors for word representation," in *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*, 2014, pp. 1532–1543.

[72] M. E. Peters *et al.*, "Deep contextualized word representations," *arXiv preprint arXiv:1802.05365*, 2018.

[73] E. M. Tapia, N. Marmasse, S. S. Intille, and K. Larson, "Mites: Wireless portable sensors for studying behavior," in *Proceedings of Extended Abstracts Ubicomp 2004: Ubiquitous Computing*, 2004.

[74] D. J. Cook and N. C. Krishnan, *Activity learning: discovering, recognizing, and predicting human behavior from sensor data*. John Wiley & Sons, 2015.

[75] E. Commission, "The 2015 ageing report. economic and budgetary projections for the 28 eu member states (2013–2060)," *European Economy*, vol. 3, pp. 1–120, 2015.

[76] M. J. Prince, *World Alzheimer Report 2015: the global impact of dementia: an analysis of prevalence, incidence, cost and trends*. Alzheimer's Disease International, 2015.

[77] Y. Zhan and H. Haddadi, "Mosen: Activity modelling in multiple-occupancy smart homes," *19th IEEE International Conference on Pervasive Computing and Communications (PerCom 2021)*, 2021.

[78] A. Jalal, Y.-H. Kim, Y.-J. Kim, S. Kamal, and D. Kim, "Robust human activity recognition from depth video using spatiotemporal multi-fused features," *Pattern recognition*, vol. 61, pp. 295–308, 2017.

[79] D. Cook, K. D. Feuz, and N. C. Krishnan, "Transfer learning for activity recognition: A survey," *Knowledge and information systems*, vol. 36, no. 3, pp. 537–556, 2013.

[80] E. M. Tapia, S. S. Intille, and K. Larson, "Activity recognition in the home using simple and ubiquitous sensors," in *International conference on pervasive computing*, Springer, 2004, pp. 158–175.

[81] Y.-T. Chiang, K.-C. Hsu, C.-H. Lu, L.-C. Fu, and J. Y.-J. Hsu, "Interaction models for multiple-resident activity recognition in a smart home," in *2010 IEEE/RSJ International Conference on Intelligent Robots and Systems*, IEEE, 2010, pp. 3753–3758.

[82] L. Leal-Taixé, C. Canton-Ferrer, and K. Schindler, "Learning by tracking: Siamese cnn for robust target association," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2016, pp. 33–40.

[83] M. Prossegger and A. Bouchachia, "Multi-resident activity recognition using incremental decision trees," in *International Conference on Adaptive and Intelligent Systems*, Springer, 2014, pp. 182–191.

[84] M. N. K. Boulos and G. Berry, "Real-time locating systems (rtls) in healthcare: A condensed primer," *International journal of health geographics*, vol. 11, no. 1, pp. 1–8, 2012.

[85] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[86] C. R. Karanam, B. Korany, and Y. Mostofi, "Tracking from one side: Multi-person passive tracking with wifi magnitude measurements," in *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, 2019, pp. 181–192.

[87] M. Abbas, M. Elhamshary, H. Rizk, M. Torki, and M. Youssef, "Wideep: Wifi-based accurate and robust indoor localization system using deep learning," in *2019 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, IEEE, 2019, pp. 1–10.

[88] F. Adib, H. Mao, Z. Kabelac, D. Katabi, and R. C. Miller, "Smart homes that monitor breathing and heart rate," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 837–846.

[89] T. Sztyler and H. Stuckenschmidt, "Online personalization of cross-subjects based activity recognition models on wearable devices," in *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, IEEE, 2017, pp. 180–189.

[90] L. Cao, Y. Wang, B. Zhang, Q. Jin, and A. V. Vasilakos, "Gchar: An efficient group-based context—aware human activity recognition on smartphone," *Journal of Parallel and Distributed Computing*, vol. 118, pp. 67–80, 2018.

[91] Y. Lee, S. Kang, C. Min, Y. Ju, I. Hwang, and J. Song, "Comon+: A cooperative context monitoring system for multi-device personal sensing environments," *IEEE Transactions on Mobile Computing*, vol. 15, no. 8, pp. 1908–1924, 2015.

[92] S. K. Yadav, K. Tiwari, H. M. Pandey, and S. A. Akbar, "A review of multimodal human activity recognition with special emphasis on classification, applications, challenges and future directions," *Knowledge-Based Systems*, vol. 223, p. 106 970, 2021.

[93] M. Vrigkas, C. Nikou, and I. A. Kakadiaris, "A review of human activity recognition methods," *Frontiers in Robotics and AI*, vol. 2, p. 28, 2015.

[94] D. R. Beddiar, B. Nini, M. Sabokrou, and A. Hadid, "Vision-based human activity recognition: A survey," *Multimedia Tools and Applications*, vol. 79, no. 41, pp. 30 509–30 555, 2020.

[95] L. Chen, H. Wei, and J. Ferryman, "A survey of human motion analysis using depth imagery," *Pattern Recognition Letters*, vol. 34, no. 15, pp. 1995–2006, 2013.

[96] P. Wang, W. Li, P. Ogunbona, J. Wan, and S. Escalera, "Rgb-d-based human motion recognition with deep learning: A survey," *Computer Vision and Image Understanding*, vol. 171, pp. 118–139, 2018.

[97] C. Chen, R. Jafari, and N. Kehtarnavaz, "Fusion of depth, skeleton, and inertial data for human action recognition," in *2016 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, IEEE, 2016, pp. 2712–2716.

[98] A. Martínez-González, M. Villamizar, O. Canévet, and J.-M. Odobez, "Real-time convolutional networks for depth-based human pose estimation," in *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, IEEE, 2018, pp. 41–47.

[99] E. Cippitelli *et al.*, "Time synchronization and data fusion for rgb-depth cameras and inertial sensors in aal applications," in *2015 IEEE international conference on communication workshop (ICCW)*, IEEE, 2015, pp. 265–270.

[100] H. Fan, X. Yu, Y. Ding, Y. Yang, and M. Kankanhalli, "Pstnet: Point spatio-temporal convolution on point cloud sequences," *arXiv preprint arXiv:2205.13713*, 2022.

[101] R. F. Brena, J. P. García-Vázquez, C. E. Galván-Tejada, D. Muñoz-Rodriguez, C. Vargas-Rosales, and J. Fangmeyer, "Evolution of indoor positioning technologies: A survey," *Journal of Sensors*, vol. 2017, 2017.

[102] H. Schweinzer and M. Syafrudin, "Losnus: An ultrasonic system enabling high accuracy and secure tdoa locating of numerous devices," in *2010 International Conference on Indoor Positioning and Indoor Navigation*, IEEE, 2010, pp. 1–8.

[103] J. N. Moutinho, R. E. Araújo, and D. Freitas, "Indoor localization with audible sound—towards practical implementation," *Pervasive and Mobile Computing*, vol. 29, pp. 1–16, 2016.

[104] I. Rishabh, D. Kimber, and J. Adcock, "Indoor localization using controlled ambient sounds," in *2012 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, IEEE, 2012, pp. 1–10.

[105] U. Nadeem, N. Hassan, M. Pasha, and C. Yuen, "Highly accurate 3d wireless indoor positioning system using white led lights," *Electronics Letters*, vol. 50, no. 11, pp. 828–830, 2014.

[106] M. Afzalan and F. Jazizadeh, "Indoor positioning based on visible light communication: A performance-based survey of real-world prototypes," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–36, 2019.

[107] Y. Cheng and T. Zhou, "Uwb indoor positioning algorithm based on tdoa technology," in *2019 10th International Conference on Information Technology in Medicine and Education (ITME)*, IEEE, 2019, pp. 777–782.

[108] A. R. J. Ruiz and F. S. Granja, "Comparing ubisense, bespoon, and decawave uwb location systems: Indoor performance analysis," *IEEE Transactions on instrumentation and Measurement*, vol. 66, no. 8, pp. 2106–2117, 2017.

[109] H. Xu, Y. Ding, P. Li, R. Wang, and Y. Li, "An rfid indoor positioning algorithm based on bayesian probability and k-nearest neighbor," *Sensors*, vol. 17, no. 8, p. 1806, 2017.

[110] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "Landmarc: Indoor location sensing using active rfid," in *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.(PerCom 2003).*, IEEE, 2003, pp. 407–415.

[111] T. Aguilera, F. Seco, F. J. Álvarez, and A. Jiménez, "Broadband acoustic local positioning system for mobile devices with multiple access interference cancellation," *Measurement*, vol. 116, pp. 483–494, 2018.

[112] T. Yang, P. Guo, W. Liu, X. Liu, and T. Hao, "A deep-learning-based method for pir-based multi-person localization," *arXiv preprint arXiv:2004.04329*, 2020.

[113] Q. Liang and M. Liu, "Plugo: A vlc systematic perspective of large-scale indoor localization," *arXiv preprint arXiv:1709.06926*, 2017.

[114] J. Xiong and K. Jamieson, "Arraytrack: A fine-grained indoor location system," in *Presented as part of the 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*, 2013, pp. 71–84.

[115] A. Mulloni, D. Wagner, I. Barakonyi, and D. Schmalstieg, "Indoor positioning and navigation with camera phones," *IEEE Pervasive Computing*, vol. 8, no. 2, pp. 22–31, 2009.

[116] A. Morar *et al.*, "A comprehensive survey of indoor localization methods based on computer vision," *Sensors*, vol. 20, no. 9, p. 2641, 2020.

[117] S. He and K. G. Shin, "Geomagnetism for smartphone-based indoor localization: Challenges, advances, and comparisons," *ACM Computing Surveys (CSUR)*, vol. 50, no. 6, pp. 1–37, 2017.

[118] G. M. Mendoza-Silva, J. Torres-Sospedra, and J. Huerta, "A meta-review of indoor positioning systems," *Sensors*, vol. 19, no. 20, p. 4507, 2019.

[119] K. Komai, M. Fujimoto, Y. Arakawa, H. Suwa, Y. Kashimoto, and K. Yasumoto, "Beacon-based multi-person activity monitoring system for day care center," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, IEEE, 2016, pp. 1–6.

[120] Y. Ma, Z. Dou, Q. Jiang, and Z. Hou, "Basmag: An optimized hmm-based localization system using backward sequences matching algorithm exploiting geomagnetic information," *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7472–7482, 2016.

[121] W. Kang and Y. Han, "Smartpdr: Smartphone-based pedestrian dead reckoning for indoor localization," *IEEE Sensors journal*, vol. 15, no. 5, pp. 2906–2916, 2014.

[122] J.-H. Shim and Y.-I. Cho, "A mobile robot localization using external surveillance cameras at indoor," *Procedia Computer Science*, vol. 56, pp. 502–507, 2015.

[123] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: Applications, challenges and implementations," in *Proceedings of the 9th workshop on Mobile computing systems and applications*, 2008, pp. 60–64.

[124] A. S. Uttama Nambi, A. Reyes Lua, and V. R. Prasad, "Loced: Location-aware energy disaggregation framework," in *Proceedings of the 2nd acm international conference on embedded systems for energy-efficient built environments*, 2015, pp. 45–54.

[125] Y. Bendavid, "Rfid-enabled real-time location system (rtls) to improve hospital's operations management: An up-to-date typology," *International Journal of RF Technologies*, vol. 5, no. 3-4, pp. 137–158, 2013.

[126] A. Moreira, M. J. Nicolau, F. Meneses, and A. Costa, "Wi-fi fingerprinting in the real world-rtls@ um at the evaal competition," in *2015 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, IEEE, 2015, pp. 1–10.

[127] A. S. Crandall and D. J. Cook, "Tracking systems for multiple smart home residents," in *Human behavior recognition technologies: Intelligent applications for monitoring and security*, IGI Global, 2013, pp. 111–129.

[128] S. Pan, N. Wang, Y. Qian, I. Velibeyoglu, H. Y. Noh, and P. Zhang, "Indoor person identification through footstep induced structural vibration," in *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, 2015, pp. 81–86.

[129] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," *IEEE Communications magazine*, vol. 48, no. 9, pp. 140–150, 2010.

[130] H. Mshali, T. Lemlouma, M. Moloney, and D. Magoni, "A survey on health monitoring systems for health smart homes," *International Journal of Industrial Ergonomics*, vol. 66, pp. 26–56, 2018.

[131] N. T. Nguyen, D. Q. Phung, S. Venkatesh, and H. Bui, "Learning and detecting activities from movement trajectories using the hierarchical hidden markov model," in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, IEEE, vol. 2, 2005, pp. 955–960.

[132] D. H. Wilson and C. Atkeson, "Simultaneous tracking and activity recognition (star) using many anonymous, binary sensors," in *International Conference on Pervasive Computing*, Springer, 2005, pp. 62–79.

[133] C.-H. Lu and L.-C. Fu, "Robust location-aware activity recognition using wireless sensor network in an attentive home," *IEEE Transactions on Automation Science and Engineering*, vol. 6, no. 4, pp. 598–609, 2009.

[134] S. S. Intille, J. Rondoni, C. Kukla, I. Ancona, and L. Bao, "A context-aware experience sampling tool," in *CHI'03 extended abstracts on Human factors in computing systems*, 2003, pp. 972–973.

[135] J. Hamm, B. Stone, M. Belkin, and S. Dennis, "Automatic annotation of daily activity from smartphone-based multisensory streams," in *International Conference on Mobile Computing, Applications, and Services*, Springer, 2012, pp. 328–342.

[136] J. Jordon, J. Yoon, and M. van der Schaar, "Pate-gan: Generating synthetic data with differential privacy guarantees," in *International Conference on Learning Representations*, 2018.

[137] C. Dwork, “Differential privacy: A survey of results,” in *International conference on theory and applications of models of computation*, Springer, 2008, pp. 1–19.

[138] S. M. Bellovin, P. K. Dutta, and N. Reitinger, “Privacy and synthetic datasets,” *Stan. Tech. L. Rev.*, vol. 22, p. 1, 2019.

[139] M. M. Masud *et al.*, “Facing the reality of data stream classification: Coping with scarcity of labeled data,” *Knowledge and information systems*, vol. 33, no. 1, pp. 213–244, 2012.

[140] A. Brock, J. Donahue, and K. Simonyan, “Large scale gan training for high fidelity natural image synthesis,” *arXiv preprint arXiv:1809.11096*, 2018.

[141] M. Frid-Adar, I. Diamant, E. Klang, M. Amitai, J. Goldberger, and H. Greenspan, “Gan-based synthetic medical image augmentation for increased cnn performance in liver lesion classification,” *Neurocomputing*, vol. 321, pp. 321–331, 2018.

[142] Y. Zhang *et al.*, “Adversarial feature matching for text generation,” *arXiv preprint arXiv:1706.03850*, 2017.

[143] T. Xu *et al.*, “Attngan: Fine-grained text to image generation with attentional generative adversarial networks,” in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 1316–1324.

[144] R. Kulkarni, R. Gaikwad, R. Sugandhi, P. Kulkarni, and S. Kone, “Survey on deep learning in music using gan,” *International Journal of Engineering Research & Technology*, vol. 8, no. 9, pp. 646–648, 2019.

[145] M. Alzantot, S. Chakraborty, and M. Srivastava, “Sensegen: A deep learning architecture for synthetic sensor data generation,” in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, IEEE, 2017, pp. 188–193.

[146] J. Dahmen and D. Cook, “Synsys: A synthetic data generation system for healthcare applications,” *Sensors*, vol. 19, no. 5, p. 1181, 2019.

[147] B. Beavis and I. Dobbs, *Optimisation and stability theory for economic analysis*. Cambridge university press, 1990.

[148] E. W. Dijkstra *et al.*, “A note on two problems in connexion with graphs,” *Numerische mathematik*, vol. 1, no. 1, pp. 269–271, 1959.

[149] P. E. Hart, N. J. Nilsson, and B. Raphael, “A formal basis for the heuristic determination of minimum cost paths,” *IEEE transactions on Systems Science and Cybernetics*, vol. 4, no. 2, pp. 100–107, 1968.

[150] R. Tarjan, “Depth-first search and linear graph algorithms,” *SIAM journal on computing*, vol. 1, no. 2, pp. 146–160, 1972.

[151] K. Stephanie, H. Conrad, S. Anna, and N. Haley, “Religion and living arrangements around the world,” *PEW Research Center*, 2019.

[152] M. Mycek, M. Sznajder, G. Krukiewicz-Gacek, L. Kostka, and J. Krzych, *Systems and methods for object tracking with wireless beacons*, US Patent 9,622,208, Apr. 2017.

[153] J. C. McMillan and S. S. Lim, "Data association algorithms for multiple target tracking," DEFENCE RESEARCH ESTABLISHMENT OTTAWA (ONTARIO), Tech. Rep., 1990.

[154] S. An, S. Hasan, H. Erfani, M. Babaei, and V. Niasar, "Unravelling effects of the pore-size correlation length on the two-phase flow and solute transport properties; gpu-based pore-network modelling," *Water Resources Research*, e2020WR027403, 2020.

[155] C. Min, A. Montanari, A. Mathur, and F. Kawsar, "A closer look at quality-aware runtime assessment of sensing models in multi-device environments," in *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*, 2019, pp. 271–284.

[156] M. Keally, G. Zhou, G. Xing, J. Wu, and A. Pyles, "Pbn: Towards practical activity recognition using smartphone-based body sensor networks," in *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, 2011, pp. 246–259.

[157] P. Zappi *et al.*, "Activity recognition from on-body sensors: Accuracy-power trade-off by dynamic sensor selection," in *European Conference on Wireless Sensor Networks*, Springer, 2008, pp. 17–33.

[158] Y. Lee, C. Min, Y. Ju, S. Kang, Y. Rhee, and J. Song, "An active resource orchestration framework for pan-scale, sensor-rich environments," *IEEE Transactions on Mobile Computing*, vol. 13, no. 3, pp. 596–610, 2013.

[159] S. Chernbumroong, S. Cang, A. Atkins, and H. Yu, "Elderly activities recognition and classification for applications in assisted living," *Expert Systems with Applications*, vol. 40, no. 5, pp. 1662–1674, 2013.

[160] Y. Zhan and H. Haddadi, "Activity prediction for mapping contextual-temporal dynamics," in *UbiComp/ISWC '2019*, 2019, pp. 246–249.

[161] Z. Cao, T. Simon, S.-E. Wei, and Y. Sheikh, "Realtime multi-person 2d pose estimation using part affinity fields," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 7291–7299.

[162] J. Wu, C. Leng, Y. Wang, Q. Hu, and J. Cheng, "Quantized convolutional neural networks for mobile devices," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 4820–4828.

[163] K. Liu, C. Chen, R. Jafari, and N. Kehtarnavaz, "Fusion of inertial and depth sensor data for robust hand gesture recognition," *IEEE Sensors Journal*, vol. 14, no. 6, pp. 1898–1903, 2014.

[164] H. Wei, R. Jafari, and N. Kehtarnavaz, "Fusion of video and inertial sensing for deep learning–based human action recognition," *Sensors*, vol. 19, no. 17, p. 3680, 2019.

[165] S. Münzner, P. Schmidt, A. Reiss, M. Hanselmann, R. Stiefelhagen, and R. Dürichen, "Cnn-based sensor fusion techniques for multimodal human activity recognition," in *Proceedings of the 2017 ACM International Symposium on Wearable Computers*, 2017, pp. 158–165.

[166] L. Martínez-Villaseñor, H. Ponce, J. Brieva, E. Moya-Albor, J. Núñez-Martínez, and C. Peñafort-Asturiano, "Up-fall detection dataset: A multimodal approach," *Sensors*, vol. 19, no. 9, p. 1988, 2019.

[167] R. Miotto, F. Wang, S. Wang, X. Jiang, and J. T. Dudley, "Deep learning for healthcare: Review, opportunities and challenges," *Briefings in bioinformatics*, vol. 19, no. 6, pp. 1236–1246, 2018.

[168] Y. Zhan and H. Haddadi, "Privacy-aware human mobility prediction via adversarial networks," *CPHS22*, 2022.

[169] H. Huang, G. Gartner, J. M. Krisp, M. Raubal, and N. Van de Weghe, "Location based services: Ongoing evolution and research agenda," *Journal of Location Based Services*, vol. 12, no. 2, pp. 63–93, 2018.

[170] K. W. Kolodziej and J. Hjelm, *Local positioning systems: LBS applications and services*. CRC press, 2017.

[171] E. Toch, B. Lerner, E. Ben-Zion, and I. Ben-Gal, "Analyzing large-scale human mobility data: A survey of machine learning methods and applications," *Knowledge and Information Systems*, vol. 58, no. 3, pp. 501–523, 2019.

[172] S. Wang, J. Cao, and P. Yu, "Deep learning for spatio-temporal data mining: A survey," *IEEE Transactions on Knowledge and Data Engineering*, 2020.

[173] D. L. Ferreira, B. A. A. Nunes, C. A. V. Campos, and K. Obraczka, "A Deep Learning Approach for Identifying User Communities Based on Geographical Preferences and Its Applications to Urban and Environmental Planning," en, *ACM Transactions on Spatial Algorithms and Systems*, vol. 6, no. 3, pp. 1–24, May 2020, ISSN: 2374-0353, 2374-0361. DOI: 10.1145/3380970. [Online]. Available: https://dl.acm.org/doi/10.1145/3380970 (visited on 10/05/2020).

[174] N. Oliver, A. Matic, and E. Frias-Martinez, "Mobile network data for public health: Opportunities and challenges," *Frontiers in public health*, vol. 3, p. 189, 2015.

[175] N. Oliver *et al.*, *Mobile phone data for informing public health actions across the covid-19 pandemic life cycle*, 2020.

[176] E. Erdemir, P. L. Dragotti, and D. Gunduz, "Privacy-Aware Time-Series Data Sharing with Deep Reinforcement Learning," en, *arXiv:2003.02685 [cs, math, stat]*, Jun. 2020, arXiv: 2003.02685. [Online]. Available: http://arxiv.org/abs/2003.02685 (visited on 04/28/2021).

[177] J. B. Gomes, C. Phua, and S. Krishnaswamy, "Where will you go? mobile data mining for next place prediction," in *International conference on data warehousing and knowledge discovery*, Springer, 2013, pp. 146–158.

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

[179] Gedik and Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2007.

[180] C. Song, Z. Qu, N. Blumm, and A.-L. Barabási, "Limits of predictability in human mobility," *Science*, vol. 327, no. 5968, pp. 1018–1021, 2010.

[181] M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi, "Understanding individual human mobility patterns," *nature*, vol. 453, no. 7196, pp. 779–782, 2008.

[182] M. Malekzadeh, R. G. Clegg, A. Cavallaro, and H. Haddadi, "Privacy and utility preserving sensor-data transformations," *Pervasive and Mobile Computing*, vol. 63, p. 101 132, 2020.

[183] T. Cunningham, G. Cormode, and H. Ferhatosmanoglu, "Privacy-preserving synthetic location data in the real world," in *17th International Symposium on Spatial and Temporal Databases*. New York, NY, USA: Association for Computing Machinery, 2021, pp. 23–33, ISBN: 9781450384254. [Online]. Available: https://doi.org/10.1145/3469830.3470893.

[184] X. He, G. Cormode, A. Machanavajjhala, C. M. Procopiuc, and D. Srivastava, "Dpt: Differentially private trajectory synthesis using hierarchical reference systems," *Proceedings of the VLDB Endowment*, vol. 8, no. 11, pp. 1154–1165, 2015.

[185] I. Goodfellow *et al.*, "Generative adversarial nets," *Advances in neural information processing systems*, vol. 27, 2014.

[186] J. Feng, C. Rong, F. Sun, D. Guo, and Y. Li, "Pmf: A privacy-preserving human mobility prediction framework via federated learning," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, no. 1, pp. 1–21, 2020.

[187] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 617–627.

[188] S. Liu, J. Du, A. Shrivastava, and L. Zhong, "Privacy adversarial network: Representation learning for mobile data privacy," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 4, pp. 1–18, 2019.

[189] J. Wang, Z. Cai, and J. Yu, "Achieving personalized k-anonymity-based content privacy for autonomous vehicles in cps," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4242–4251, 2019.

[190] C. Dwork, A. Roth, *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2006.

[191] F. Z. Errounda and Y. Liu, "An analysis of differential privacy research in location data," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, IEEE, 2019, pp. 53–60.

[192] M. E. Gursoy, V. Rajasekar, and L. Liu, "Utility-optimized synthesis of differentially private location traces," in *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, GA, USA: IEEE, 2020, pp. 30–39.

[193] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "Geo-indistinguishability: A principled approach to location privacy," in *Distributed Computing and Internet Technology*, R. Natarajan, G. Barua, and M. R. Patra, Eds., Cham: Springer International Publishing, 2015, pp. 49–72, ISBN: 978-3-319-14977-6.

[194] V. Primault, S. B. Mokhtar, C. Lauradoux, and L. Brunie, *Differentially private location privacy in practice*, 2014. DOI: 10.48550/ARXIV.1410.7744. [Online]. Available: https://arxiv.org/abs/1410.7744.

[195] M. E. Gursoy, L. Liu, S. Truex, L. Yu, and W. Wei, "Utility-aware synthesis of differentially private and attack-resilient location traces," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18, Toronto, Canada: Association for Computing Machinery, 2018, pp. 196–211, ISBN: 9781450356930. DOI: 10.1145/3243734.3243741. [Online]. Available: https://doi.org/10.1145/3243734.3243741.

[196] C. Clifton and T. Tassa, "On syntactic anonymity and differential privacy," in *2013 IEEE 29th International Conference on Data Engineering Workshops (ICDEW)*, Brisbane, QLD, Australia: IEEE, 2013, pp. 88–93.

[197] J. Hamm, "Minimax filter: Learning to preserve privacy from inference attacks," *The Journal of Machine Learning Research*, vol. 18, no. 1, pp. 4704–4734, 2017.

[198] V. Bindschaedler and R. Shokri, "Synthesizing plausible privacy-preserving location traces," in *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA: IEEE, 2016, pp. 546–563. DOI: 10.1109/SP.2016.39.

[199] R. P. Lippmann *et al.*, "Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation," in *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, IEEE, vol. 2, 2000, pp. 12–26.

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

[201] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–36, 2021.

[202] A. Aktay *et al.*, "Google covid-19 community mobility reports: Anonymization process description (version 1.1)," *arXiv preprint arXiv:2004.04145*, 2020.

[203] J. Yang, M. Dash, and S. G. Teo, "PPTPF: Privacy-Preserving Trajectory Publication Framework for CDR Mobile Trajectories," en, *ISPRS International Journal of Geo-Information*, vol. 10, no. 4, p. 224, Apr. 2021, Number: 4 Publisher: Multidisciplinary Digital Publishing Institute. DOI: 10.3390/ijgi10040224. [Online]. Available: https://www.mdpi.com/2220-9964/10/4/224 (visited on 04/23/2021).

[204] A. Rezaei, C. Xiao, J. Gao, and B. Li, "Protecting sensitive attributes via generative adversarial networks," *arXiv preprint arXiv:1812.10193*, 2018.

[205] D. Huang *et al.*, "A variational autoencoder based generative model of urban human mobility," in *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, IEEE, 2019, pp. 425–430.

[206] S. Choi, J. Kim, and H. Yeo, "Trajgail: Generating urban vehicle trajectories using generative adversarial imitation learning," *Transportation Research Part C: Emerging Technologies*, vol. 128, p. 103 091, 2021.

[207] K. Ouyang, R. Shokri, D. S. Rosenblum, and W. Yang, "A non-parametric generative model for human trajectories," in *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18*, International Joint Conferences on Artificial Intelligence Organization, Jul. 2018, pp. 3812–3817. DOI: 10.24963/ijcai.2018/530. [Online]. Available: https://doi.org/10.24963/ijcai.2018/530.

[208] S. Shin, H. Jeon, C. Cho, S. Yoon, and T. Kim, "User mobility synthesis based on generative adversarial networks: A survey," in *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, IEEE, 2020, pp. 94–103.

[209] Y. Xiao, L. Xiong, S. Zhang, and Y. Cao, "Loclok: Location cloaking with differential privacy via hidden markov model," *Proceedings of the VLDB Endowment*, vol. 10, pp. 1901–1904, Aug. 2017. DOI: 10.14778/3137765.3137804.

[210] M. Luca, G. Barlacchi, B. Lepri, and L. Pappalardo, *A survey on deep learning for human mobility*, 2021. arXiv: 2012.02825 [cs.LG].

[211] I. J. Goodfellow *et al.*, "Generative Adversarial Networks," en, *arXiv:1406.2661 [cs, stat]*, Jun. 2014, arXiv: 1406.2661. [Online]. Available: http://arxiv.org/abs/1406.2661 (visited on 10/21/2020).

[212] E. P. de Mattos, A. C. Domingues, and A. A. Loureiro, "Give me two points and i'll tell you who you are," in *2019 IEEE Intelligent Vehicles Symposium (IV)*, IEEE, 2019, pp. 1081–1087.

[213] V. Primault, A. Boutet, S. B. Mokhtar, and L. Brunie, "The long road to computational location privacy: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2772–2793, 2018.

[214] W. W. R. Ball, *A short account of the history of mathematics*. Courier Corporation, 1960.

[215] P. E. Black *et al.*, "Dictionary of algorithms and data structures," 1998.

[216] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[217] Y. Zhan and H. Haddadi, "Towards automating smart homes: Contextual and temporal dynamics of activity prediction," in *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*, 2019, pp. 413–417.

[218] M. Nasr, R. Shokri, and A. Houmansadr, "Machine learning with membership privacy using adversarial regularization," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18, Toronto, Canada: Association for Computing Machinery, 2018, pp. 634–646, ISBN: 9781450356930. DOI: 10.1145/3243734.3243855. [Online]. Available: https://doi.org/10.1145/3243734.3243855.

[219] S. Mukherjee, Y. Xu, A. Trivedi, N. Patowary, and J. L. Ferres, "Privgan: Protecting gans from membership inference attacks at low cost to utility," *Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. 3, pp. 142–163, 2021.

[220] J. K. Laurila *et al.*, "The mobile data challenge: Big data for mobile computing research," Tech. Rep., 2012.

[221] S. B. Mokhtar *et al.*, "PRIVA'MOV: Analysing human mobility through multi-sensor datasets," in *NetMob 2017*, 2017.

[222] Y. Zheng, H. Fu, X. Xie, W.-Y. Ma, and Q. Li, *Geolife gps trajectory dataset - user guide*, Geolife GPS trajectories 1.1, Geolife GPS trajectories 1.1, Jul. 2011. [Online]. Available: `https://www.microsoft.com/en-us/research/publication/geolife-gps-trajectory-dataset-user-guide/`.

[223] D. Yang, D. Zhang, V. W. Zheng, and Z. Yu, "Modeling user activity preference by leveraging user spatial temporal characteristics in LBSNs," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 1, pp. 129–142, 2014.

[224] G. M. Morton, "A computer oriented geodetic data base and a new technique in file sequencing," 1966.

[225] J. Ke, H. Zheng, H. Yang, and X. M. Chen, "Short-term forecasting of passenger demand under on-demand ride services: A spatio-temporal deep learning approach," *Transportation Research Part C: Emerging Technologies*, vol. 85, pp. 591–608, 2017.

[226] Y. Li, Y. Zheng, H. Zhang, and L. Chen, "Traffic prediction in a bike-sharing system," in *Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 2015, pp. 1–10.

[227] R. Silva, S. M. Kang, and E. M. Airoldi, "Predicting traffic volumes and estimating the effects of shocks in massive transportation systems," *Proceedings of the National Academy of Sciences*, vol. 112, no. 18, pp. 5643–5648, 2015.

[228] M. X. Hoang, Y. Zheng, and A. K. Singh, "Fccf: Forecasting citywide crowd flows based on big data," in *Proceedings of the 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 2016, pp. 1–10.

[229] J. Zhang, Y. Zheng, and D. Qi, "Deep spatio-temporal residual networks for citywide crowd flows prediction," in *Thirty-First AAAI Conference on Artificial Intelligence*, 2017.

[230] D. L. Ferreira, B. A. Nunes, C. A. V. Campos, and K. Obraczka, "A deep learning approach for identifying user communities based on geographical preferences and its applications to urban and environmental planning," *ACM Transactions on Spatial Algorithms and Systems (TSAS)*, vol. 6, no. 3, pp. 1–24, 2020.

[231] M. De Domenico, A. Lima, and M. Musolesi, "Interdependence and predictability of human mobility and social interactions," *Pervasive and Mobile Computing*, vol. 3, pp. 798–807, 6 Dec. 2013.

[232] N. Saleheen *et al.*, "Msieve: Differential behavioral privacy in time series of mobile sensor data," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2016, pp. 706–717.

[233] A. Aristodimou, A. Antoniades, and C. S. Pattichis, "Privacy preserving data publishing of categorical data through k-anonymity and feature selection," *Healthcare technology letters*, vol. 3, no. 1, pp. 16–21, 2016.

[234] K. P. Puttaswamy *et al.*, "Preserving location privacy in geosocial applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 159–173, 2012.

[235] W. Zhang, M. Li, R. Tandon, and H. Li, "Online location trace privacy: An information theoretic approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 235–250, 2018.

[236] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-aware time-series data sharing with deep reinforcement learning," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 389–401, 2020.

[237] E. Erdemir, P. L. Dragotti, and D. Gunduz, "Privacy-aware location sharing with deep reinforcement learning," in *2019 IEEE International Workshop on Information Forensics and Security (WIFS)*, IEEE, 2019, pp. 1–6.

[238] M. Kasy and R. Abebe, "Fairness, equality, and power in algorithmic decision-making," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 2021, pp. 576–586.

[239] H. Heidari, M. Loi, K. P. Gummadi, and A. Krause, "A moral framework for understanding fair ml through economic models of equality of opportunity," in *Proceedings of the conference on fairness, accountability, and transparency*, 2019, pp. 181–190.

[240] P. Sattigeri, S. C. Hoffman, V. Chenthamarakshan, and K. R. Varshney, "Fairness gan: Generating datasets with fairness properties using a generative adversarial network," *IBM Journal of Research and Development*, vol. 63, no. 4/5, pp. 3–1, 2019.

[241] A. E. Brown, *Ridehail revolution: Ridehail travel and equity in Los Angeles*. University of California, Los Angeles, 2018.

[242] A. Yan and B. Howe, "Fairst: Equitable spatial and temporal demand prediction for new mobility systems," in *Proceedings of the 27th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 2019, pp. 552–555.

[243] Yan, "Fairness in practice: A survey on equity in urban mobility," *A Quarterly bulletin of the Computer Society of the IEEE Technical Committee on Data Engineering*, vol. 42, no. 3, 2020.

[244] Y. Ge, C. R. Knittel, D. MacKenzie, and S. Zoepf, "Racial and gender discrimination in transportation network companies," National Bureau of Economic Research, Tech. Rep., 2016.

[245] S. A. Friedler, C. Scheidegger, and S. Venkatasubramanian, "The (im) possibility of fairness: Different value systems require different mechanisms for fair decision making," *Communications of the ACM*, vol. 64, no. 4, pp. 136–143, 2021.

[246] Y. Zhan, A. Kyllo, A. Mashhadi, and H. Haddadi, *Privacy-aware human mobility prediction via adversarial networks*, 2022. arXiv: 2201.07519 [cs.LG].

[247] Y. Zheng, X. Xie, and W.-Y. Ma, "GeoLife: A Collaborative Social Networking Service among User, Location and Trajectory," *IEEE Data Eng. Bull.*, vol. 33, pp. 32–39, Jun. 2010.

[248] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A survey on bias and fairness in machine learning," *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–35, 2021.

[249] C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, "Fairness through awareness," in *Proceedings of the 3rd innovations in theoretical computer science conference*, 2012, pp. 214–226.

[250] M. Hardt, E. Price, and N. Srebro, "Equality of opportunity in supervised learning," *arXiv preprint arXiv:1610.02413*, 2016.

[251] S. Barocas and A. D. Selbst, "Big data's disparate impact," *Calif. L. Rev.*, vol. 104, p. 671, 2016.

[252] J. E. Roemer, "Equality of opportunity: A progress report," *Social Choice and Welfare*, vol. 19, no. 2, pp. 455–471, 2002.

[253] A. Mashhadi, J. Sterner, and J. Murray, "Deep embedded clustering of urban communities using federated learning," 2021.

[254] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, no. 4, pp. 600–612, 2004.

[255] X. Lu, E. Wetter, N. Bharti, A. J. Tatem, and L. Bengtsson, "Approaching the limit of predictability in human mobility," *Scientific reports*, vol. 3, no. 1, pp. 1–9, 2013.

[256] Y. Wang, A. Yalcin, and C. VandeWeerd, "An entropy-based approach to the study of human mobility and behavior in private homes," *PLoS one*, vol. 15, no. 12, e0243503, 2020.

[257] W. Chen, Z. Wang, H. Xie, and W. Yu, "Characterization of surface emg signal based on fuzzy entropy," *IEEE Transactions on neural systems and rehabilitation engineering*, vol. 15, no. 2, pp. 266–272, 2007.

[258] M. W. Flood and B. Grimm, "Entropyhub: An open-source toolkit for entropic time series analysis," *Plos one*, vol. 16, no. 11, e0259448, 2021.

[259] L. E. V. Silva, A. Senra Filho, V. Fazan, J. Felipe, and L. M. Junior, "Two-dimensional sample entropy: Assessing image texture through irregularity," *Biomedical Physics & Engineering Express*, vol. 2, no. 4, p. 045 002, 2016.

[260] R. Lletı, M. C. Ortiz, L. A. Sarabia, and M. S. Sánchez, "Selecting variables for k-means cluster analysis by using a genetic algorithm that optimises the silhouettes," *Analytica Chimica Acta*, vol. 515, no. 1, pp. 87–100, 2004.

[261] P. Bobko and P. L. Roth, "The four-fifths rule for assessing adverse impact: An arithmetic, intuitive, and logical analysis of the rule and implications for future research and practice," in *Research in personnel and human resources management*, Emerald Group Publishing Limited, 2004.

[262] M. Feldman, S. A. Friedler, J. Moeller, C. Scheidegger, and S. Venkatasubramanian, "Certifying and removing disparate impact," in *proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining*, 2015, pp. 259–268.

[263] T. Hu *et al.*, "Fairnn-conjoint learning of fair representations for fair decisions," in *International Conference on Discovery Science*, Springer, 2020, pp. 581–595.