

# Anonymous Trajectory Method for Indoor Users for Privacy Protection

Sultan Alamri(✉)

School of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
salamri@seu.edu.sa

**Abstract.** The privacy of the trajectories of indoor space users is just as important as that of the users of outdoor spaces. Many users of indoor spaces consider it very important to maintain the privacy of their movements within buildings and not reveal their visit to a certain room/cell inside buildings. In this paper, we propose a cloaking diversity approach for moving entities in indoor spaces. This new privacy-assurance approach uses the cloaking concept adapted with processing diversity trajectories to safeguard user privacy in an indoor space. Extensive simulations and evaluations have demonstrated that the proposed privacy approach algorithm performs well and at a low cost.

**Keywords:** Indoor space · Privacy · Indoor trajectories · Cloaking

## 1 Introducing

Generally, people spend spent most of their lives in indoor spaces [1–4]. However, little research has been done on securing the privacy of users' trajectories indoors [5–7]. Instead, the focus has been on the privacy of user locations in outdoor space. However, since we spend most of our time indoors, and often in very large buildings, the privacy issue is the same as that related to outdoor privacy. For example, a certain user might like to visit a certain room and keep his/her movements private, as a breach of this privacy could be used for advertising purposes, to spread rumours, or for other unauthorized purposes. Therefore, protecting the users' trajectories in indoor spaces is essential for many users [8–11].

In this paper, we proposed a cloaking diversity approach for moving objects in indoor environments. The algorithm will choose the shortest path for the user which maintain his privacy and allowing him/her to the optional for cloaking a certain cell/room for protecting the user privacy. For user privacy in indoor environments, the new privacy solution adapts the cloaking concept with providing a diversity of trajectories. Here the user will be associated more to dynamic rooms in order to protect his/her privacy. Extensive simulations and tests revealed that the proposed privacy approach algorithm functions well and at a reasonable cost, as well as successfully protecting the user trajectory privacy.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022, LNCS 13375, pp. 104–112, 2022.
https://doi.org/10.1007/978-3-031-10522-7_8

This paper is organized as follows. Section 2 gives an overview of previous works on indoor path routing and spatial cloaking. Section 3 describes the system methodology and the cloaking algorithms. Section 4 explains the testing of the system's performance, and presents the analysis of results. Section 5 concludes the paper and indicates future research directions.

## 2 Related Works

In this section, we discuss previous research on indoor routing, and spatial privacy in outdoor spaces.

Many studies have been conducted in order to find the best indoor routing algorithms [6,8,12]. In Tiara, for example, a three-dimensional space implementation of a routing system is proposed. In this study, four algorithms were compared to determine the one that provided the best shortest path in three-dimensional spaces. These algorithms are: Dijkstra algorithm, A* algorithm, Bellman-Ford algorithm, and Floyd-Warshall algorithm. The results indicated that the A* Algorithm performed the best in a three-dimensional setting.

On the other hand, some works saw the mobility of an object in an interior environment being controlled or directed in a way similar to that in an outdoor spatial road network me2. Some works have focused on indoor zoning as a means of controlling social distancing, especially in open indoor spaces where large social, entertainment or sporting events are held [8]. Furthermore, in the presence of crowds, the indoor crowd-aware, fastest-way query finds the path with the shortest travel time, whereas the indoor least-crowded path query identifies the route containing the fewest items [13].

Many works have focused on the privacy of moving objects' trajectories in outdoor space [10,14–16]. For example, spatial cloaking was used in many works as a means of protecting the privacy of the user. For instance, anonymity was achieved by reporting a cloaked area large enough to include the group size required to fulfill the targeted anonymity restriction citation [16]. Figure 1, shows an example of a cloaked zone (region) in an outdoor space. Another study focused on the mixed-one concept [15]. Mix-zones, where the user's disguise is renewed, were proposed. The term 'mix-zones' is derived from the fact that the temporal order in which users enter and exit these zones must be obscured (mixed), otherwise the adversary may be able to link the new disguise to the old one [14].

To the best of our knowledge, we are the first to consider the privacy of trajectories in indoor spaces. Indoor spaces have several features that distinguish them from outdoor spaces such as obstacles (e.g., doors), various structures such as dynamic rooms (corridors), stairs etc. Therefore, this paper focuses on first obtaining the best path for the moving user, and then protecting his/her privacy by concealing the room/cell which is being visited.

## 3 Cloaking Cells Algorithms

In this section, we present and explain in detail the algorithms proposed for protecting the user's privacy in an indoor space.

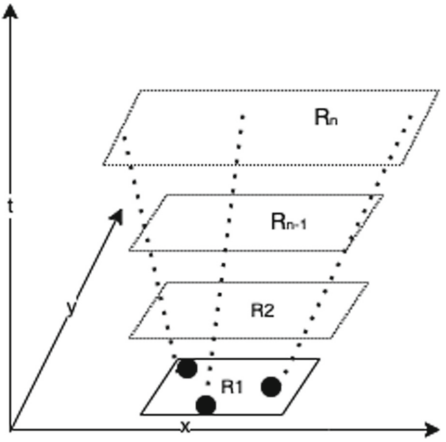


**Fig. 1.** Outdoor cloaked spatial regions $R_1, R_2, ..R_n$

First, we describe the indoor structure on which this algorithm will be based. The basic data structure for the indoor environments will be the indoor space that will be divided into cells (i.e., cellular indoor s pace).

**Definition 1.** Let $P$ be a set of indoor cells $C_1$, $C_2$, $C_3$,..*etc*, where the cells are classified as follows:
$C_i$ is a dynamic cell if it is a connection between other cells such as corridors, pathways, stairs or common paths or stairways. $C_j$ is a static cell if it does not provide a connection between other cells.

The focus here will be on the static cells. These are cells that might be visited by users who want to protect the privacy of their visit, and do not want the locations of the cells to be revealed. The algorithm will start choosing the most suitable path for the user by determining the user's trajectory, using the hop distance approach.

**Definition 2.** The shortest path from cell $C_x$ to $C_y$ is the lowest number of static cells of the trajectory from $C_x$ to $C_y$.

An example of the shortest path is shown in Fig. 2. Here, user $A$ wants to visit *cell*22 and then his last destination was room 18 ($C_{18}$). Based on the adjacent cells, the shortest path will be $C_13, C14d, C21, C22, C15a, C15b, C_18$ which is a distance of 7 hops. However, with our proposed algorithm intended to ensure privacy protection, we include a greater number of dynamic cells rather than traversing more static cells. In addition, this approach allows users to apply the cloak cell approach by themselves without exposing their exact cell to third parties. The basic idea of the algorithm is to cloak the cell (a specific static cell) of the user while showing a greater number of dynamic cells. The system architecture of the trajectory cloak is shown in Fig. 3.

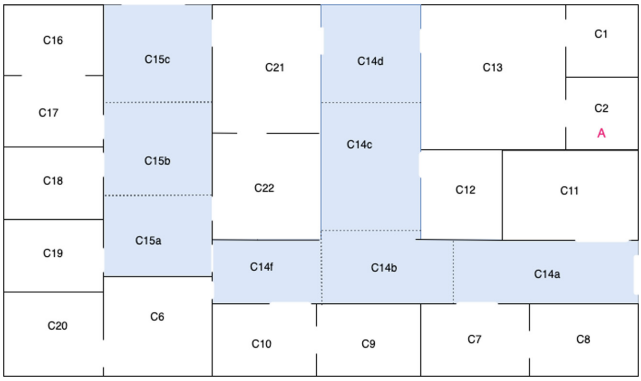


**Fig. 2.** Example of indoor space where blue shading indicates the dynamic cells

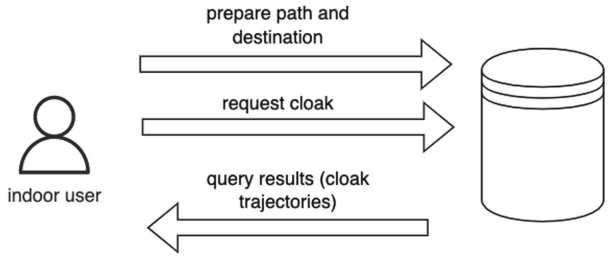


**Fig. 3.** System architecture

Here, when a user requests a cloaking for his trajectory, the algorithm will return the first candidate path to the destination cell, which will include as many dynamic cells as possible, such as one or more corridors and common cells (common rooms). Figure 4, illustrates a requested trajectory with a cloaks option where in (b) the algorithm focuses more on retrieving dynamics cell along the path to the user's destination cell(s).

Figure 5, illustrates the cloak method. When a user determines a destination cell, if the cell is a static cell that for reasons of user privacy should not be disclosed, if the user visits the cell/location ($C_i$) a cloak diversion will be initiated as follows : the destination cell here will be associated with user $A$ and at least one semantically different object in the cell. For example, in the previous example, to achieve l-diversity with $l = 3$, the server needs to consider three other cells of the designation cell adjacent (from level 1 or the next level) containing different semantic objects, which will contain 3 different trajectories containing the one from user $A$, and two from fake users $A_x$, and $A_y$ located in the other cells. The algorithm will continue building the trajectory until the last destination cell is reached. These trajectories are illustrated in Fig. 8. Note that when the LBS returns all results to the anonymity server, the latter filters out the results for the fake users and returns to the relevant result to the legitimate user.

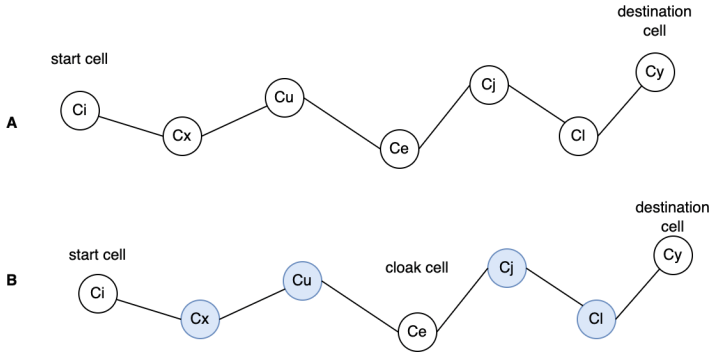


**Fig. 4.** Retrieving dynamic cells within the path with cloaks option

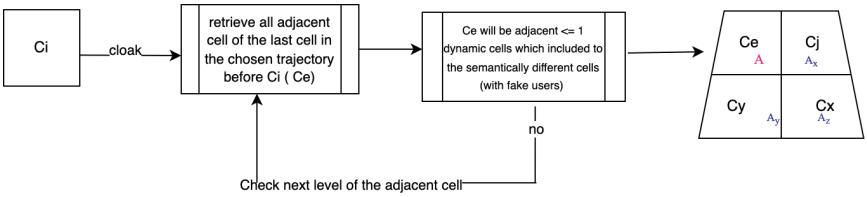


**Fig. 5.** Diversity-cloak method

**Definition 3.** Let $C_e, C_j, C_h, C_t$, be chosen for the cloak diversity of the adjacent cells of $C_i$, if the dynamic cells adjacent $\leq 1$ (e.g. $C_h, C_j$ are dynamic cells).

## 4 Results and Evaluation

In this section, we present the experimental data used to assess the performance of the proposed indoor privacy algorithm. The simulation was carried out on a PC with a 2.60 GHz Intel Core i7-9750H CPU and 16 GB of RAM running 64-bit Windows 10 Enterprise. MATLAB was used to implement the strategy.

In this experiment, we used a synthetic dataset for an indoor environment which was comprised of 25 room/cells. There are 8 dynamic cells which is the common area for the movement between the cells, and 17 regular cells. Note that all the tested paths are assumed based on realistic scenarios. It is worth noting that the processes were carried out eight times before the average was calculated.

We began by measuring the construction cost of the proposed privacy algorithm. Previous cloaking diversity algorithms proposed for the indoor environment used an undirected graph for indoor cells where metric distance was applied. However, we used the hop distances. Figures 6 and 7 show that the proposed algorithm is cost-efficient. The application of the algorithm to two different scenarios yielded an interesting result: when the number of cells increases,

**Algorithm 1.** privacy indoor trajectory

```
Input: Indoor S, objects O, indoor cell C
Output: cloaking indoor cells trajectory for indoor users
s_i request shortest path to c_i
while s_i loctaed in C do
    if s_i activate cloak option then then
        confine the dynamic cell dc
        confine the static cell sc
        return candidate path
        if dc > sc then then
            return path p_i
        end if
        if sc is part of p_i then then
            apply cloak to sc
        end if
    else
        return 1st candidate path to c_i
    end if
end while
```

the construction cost increases slightly. Figure 6, depict slightly longer paths, whereas Fig. 7 shows the construction costs for scenarios with shorter paths.

We also tested the cost construction of the anonymity server, which basically filters out the results for the fake users and returns to the relevant result to the legitimate user. Figure 9 shows that in all three scenarios comprising different paths, the server filters to their original paths efficiently. Although in path 3 (in all scenarios), there is a relatively larger number of cells, which incurs a small increase in filtering costs, the algorithm still performs efficiently.

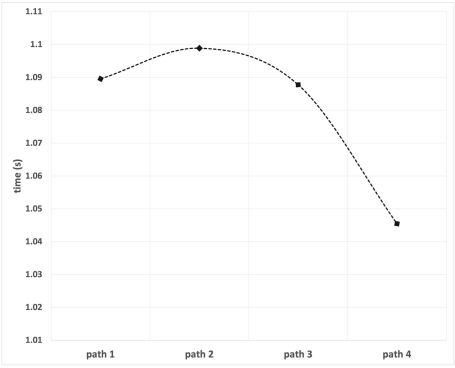


**Fig. 6.** The construction cost of the proposed algorithm in longer paths scenarios

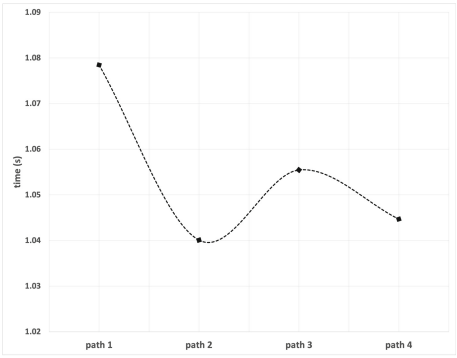


**Fig. 7.** The construction cost of the proposed algorithm in shorter paths scenarios

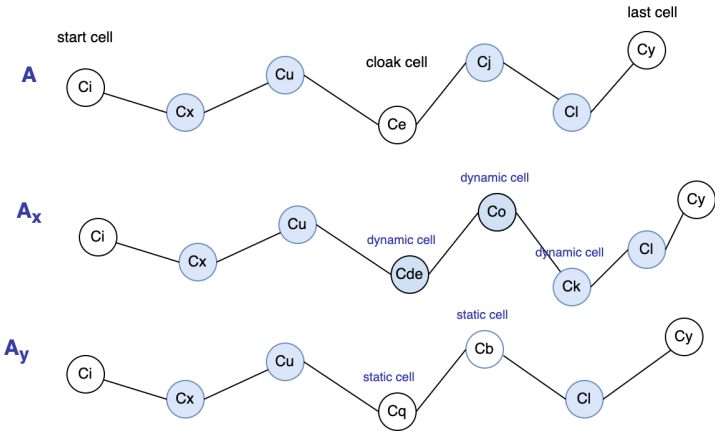


**Fig. 8.** Retrieving 3 diversity trajectories from user $A$

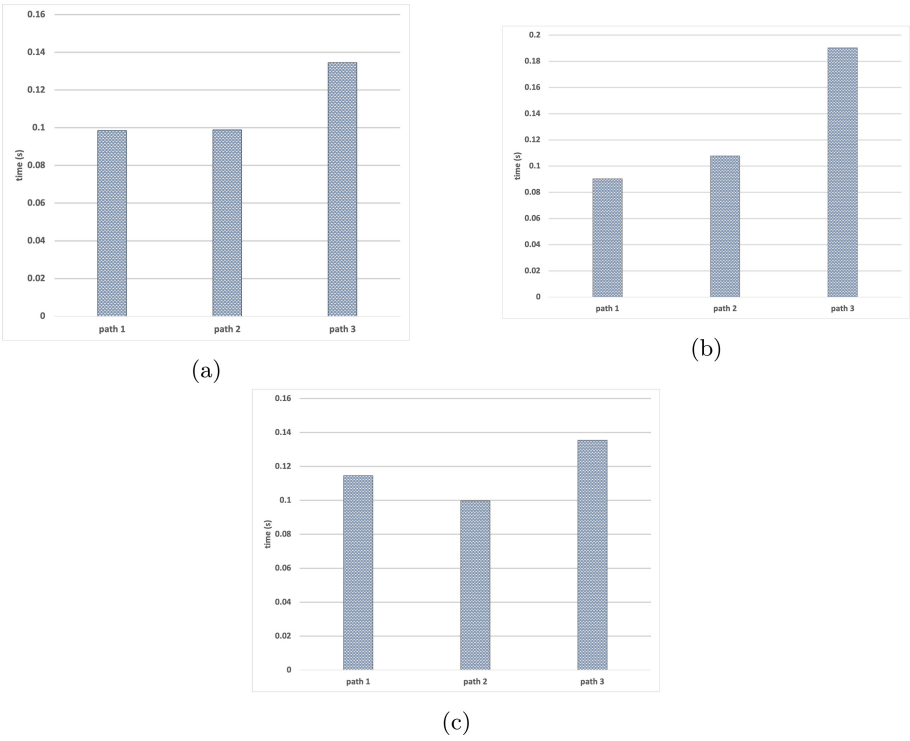


**Fig. 9.** The cost of the filtering the of three different scenarios

## 5 Conclusion

In this paper, we proposed a cloaking diversity approach for moving objects in indoor environments. Since previous research on the privacy of spatial trajectories has been done in the context of outdoor spaces, this work focuses uniquely on the privacy of the indoor spatial trajectories. The algorithm will find the shortest path for the user while maintaining his/her privacy, while giving the user the option to cloak a specific cell/room. For user privacy in indoor environments, the proposed privacy solution uses the cloaking principle with the inclusion of several trajectories. In order to maintain privacy, the user will be more attached to the dynamic rooms. Extensive simulations and tests demonstrated that the proposed privacy approach method works well and is cost-efficient, also successfully safeguarding the privacy of the user's trajectory.

## References

1. Shao, Z., Cheema, M.A., Taniar, D., Lu, H., Yang, S.: Efficiently processing spatial and keyword queries in indoor venues. IEEE Trans. Knowl. Data Eng. **33**(9), 3229–3244 (2021)

2. Alamri, S.: An efficient shortest path routing algorithm for directed indoor environments. ISPRS Int. J. Geo-Inf. **7**(4), 133 (2018)
3. Alamri, S.: Spatial data managements in indoor environments: current trends, limitations and future challenges. Int. J. Web Inf. Syst. **14**(4), 402–422 (2018)
4. Alamri, S., Taniar, D., Nguyen, K., Alamri, A.: C-tree: efficient cell-based indexing of indoor mobile objects. J. Ambient. Intell. Humaniz. Comput. **11**(7), 2841–2857 (2019). https://doi.org/10.1007/s12652-019-01397-w
5. Alamri, S., Taniar, D., Safar, M., Al-Khalidi, H.: A connectivity index for moving objects in an indoor cellular space. Pers. Ubiquit. Comput. **18**(2), 287–301 (2013). https://doi.org/10.1007/s00779-013-0645-3
6. Alamri, S., Taniar, D., Safar, M.: A taxonomy for moving object queries in spatial databases. Future Gener. Compt. Syst. **37**, 232–242 (2014)
7. Fariña, A., Gutiérrez-Asorey, P., Ladra, S., Penabad, M.R., Rodeiro, T.V.: A compact representation of indoor trajectories. IEEE Pervasive Comput. **21**(1), 57–64 (2022)
8. Alamri, S.: An efficient spatial zoning algorithm for maintaining social distancing in open indoor spaces. Int. J. Web Grid Serv. **18**(2), 194–212 (2022)
9. Tan, R., Tao, Y., Si, W., Zhang, Y.-Y.: Privacy preserving semantic trajectory data publishing for mobile location-based services. Wirel. Netw. **26**(8), 5551–5560 (2019). https://doi.org/10.1007/s11276-019-02058-8
10. Sazdar, A.M., Alikhani, N., Ghorashi, S.A., Khonsari, A.: Privacy preserving in indoor fingerprint localization and radio map expansion. Peer-to-Peer Network. Appl. **14**(1), 121–134 (2020). https://doi.org/10.1007/s12083-020-00950-1
11. Zhao, Y., Zhao, X., Chen, S., Zhang, Z., Huang, X.: An indoor crowd movement trajectory benchmark dataset. IEEE Trans. Reliab. **70**(4), 1368–1380 (2021)
12. Mura, C., Pajarola, R., Schindler, K., Mitra, N.J.: Walk2Map: extracting floor plans from indoor walk trajectories. Comput. Graph. Forum **40**(2), 375–388 (2021)
13. Liu, T., et al.: Shortest path queries for indoor venues with temporal variations. In: 2020 IEEE 36th International Conference on Data Engineering (ICDE), pp. 2014–2017 (2020)
14. Sweeney, L.: K-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl. Based Syst. **10**(5) 557–570 (2002)
15. Chow, C.-Y., Mokbel, M.F.: Trajectory privacy in location-based services and data publication. SIGKDD Explor. Newsl. **13**(1), 19–29 (2011)
16. Khoshgozaran, A., Shahabi, C.: A taxonomy of approaches to preserve location privacy in location-based services. Int. J. Comput. Sci. Eng. **5**(2), 86–96 (2010)