Semantic Privacy Inference Preservation Algorithm for Indoor Trajectory

Abdullah Alamri
College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

***Abstract*—Indoor location services have become an increasingly important part of our everyday lives in recent years. Despite the numerous benefits these services offer, serious concerns have arisen about the privacy of users' locations. Adversaries can monitor user-requested locations in order to obtain sensitive information such as shopping patterns. Many users of indoor spaces want their movements and locations to be kept private so as not to reveal their visit to a particular zone inside buildings. Research on semantic indoor trajectory-based human movement data has primarily focused on finding routes without taking into account the protection of privacy. Hence, the servers on which trajectory data is stored are not completely secure. In this paper, we propose a semantic privacy inference preservation algorithm for an indoor trajectory that can issue pathfinding and navigation instructions while achieving good privacy protection of moving entities by generating ambiguous trajectory. The simulation of the proposed semantic indoor privacy algorithm was implemented in MATLAB.**

***Keywords*—Privacy; semantic ontology; indoor space; routing algorithm; spatial databases**

I. Introduction

With the widespread usage of smartphones, mobile crowd-sensing is now recognized as a promising means of collecting diverse and heterogeneous trajectory data for moving objects. This is especially useful for modeling human mobility patterns in either indoor or outdoor urban environments. The popularity of mobile positioning devices has resulted in the creation of several location-based services (LBSs) as well as vast volumes of locational data. Location-based services (LBSs) are being used in an increasing number of areas and have become an integral part of modern life [1, 2, 3]. Demand for location-based services is gradually extending from outdoors to indoors. Researchers and enterprises are increasingly interested in "indoor positioning systems (IPS)" and "indoor localization systems (ILS)" because they offer significant commercial opportunities for implementing indoor positioning, mapping, and navigation [4, 5].

Human mobility may be considered as a trajectory across a variety of indoor or outdoor spaces, each with its own distinct characteristics. While many studies have been conducted on outdoor trajectories, research has revealed that people spend more than 87% of their lifetime indoors in places such as shopping malls, airport terminals, and conference offices [6, 7, 8]. However, few studies have been conducted on safeguarding the privacy of indoor user trajectories. Instead, the emphasis has been on ensuring user privacy in outdoor environments despite the fact that most of our time is spent indoors where the same privacy issues apply.

Recognizing the promise of indoor LBSs, large technology corporations, governments, research institutions, and start-ups are making significant investments in this technology. While such technologies promise to make our lives easier, the privacy issues linked with indoor LBSs have raised many concerns, as the data they acquire is often sensitive and needs to be safeguarded. Indeed, misusing location data can result in the revealing of sensitive personal information about a user, such as personal interests and lifestyle habits. For example, users may want to visit stores while keeping their moves private, as an invasion of privacy can be exploited for advertising, spreading rumors, or other unauthorized or malicious purposes. Therefore, the protection of users' trajectories in indoor environments is critical.

Trajectory-based operations involving spatiotemporal data of moving objects are becoming increasingly essential in related research and applications. This is because it provides insight into human movement and has the potential to recognize patterns and predict future behavior. Over the past few years, several researchers have introduced a series of data models for semantic trajectories in indoor environments. However, the studies on semantic indoor trajectory-based human movement data have focused mainly on finding routes without considering the protection of privacy.

In this paper, we propose a solution that enables pathfinding and navigation instructions while achieving good privacy protection for moving entities by generating ambiguous trajectories. Semantic Web technologies provide strong representation tools for ubiquitous applications [9, 10, 11]. With location-based services and Semantic Web standards, trajectories can be linked and semantically annotated more easily, resulting in semantic trajectory descriptions. In this paper, we introduce semantic spatial ontology, which models indoor routing system needs while taking into account the protection of privacy. The contributions of this paper are as follows:

- Integrating semantic ontology/knowledge graphs and semantic privacy inference into indoor location-based services to improve accuracy and enrich navigation instructions with preserving the privacy of the user.
- Generating an ambiguous trajectory achieves privacy protection by safeguarding the actual trajectory of moving objects.

This paper has the following structure. Section II reviews the relevant literature and research on indoor routing and indoor/outdoor spatial privacy. Section III presents an overview of ontology modeling languages for the Semantic Web. Section IV describes the proposed semantic indoor trajectory privacy preservation algorithm. The architecture is comprised of two-level components: a semantic spatial ontology model for

indoor routing, and semantic ambiguous trajectory privacy inference preservation. Detailed explanations of each of the architecture's components are provided in Section IV. Section V provides a motivation example and validation experiment for the proposed semantic indoor trajectory privacy preservation algorithm. Section VI summarizes the paper and offers suggestions for future research directions.

II. Literature Review

This section describes the relevant literature and research on indoor routing and spatial privacy in both indoor and outdoor environments. Several studies have explored indoor routing and have conducted studies to determine the algorithms that are most effective for indoor routing and navigation, Fig. 1.

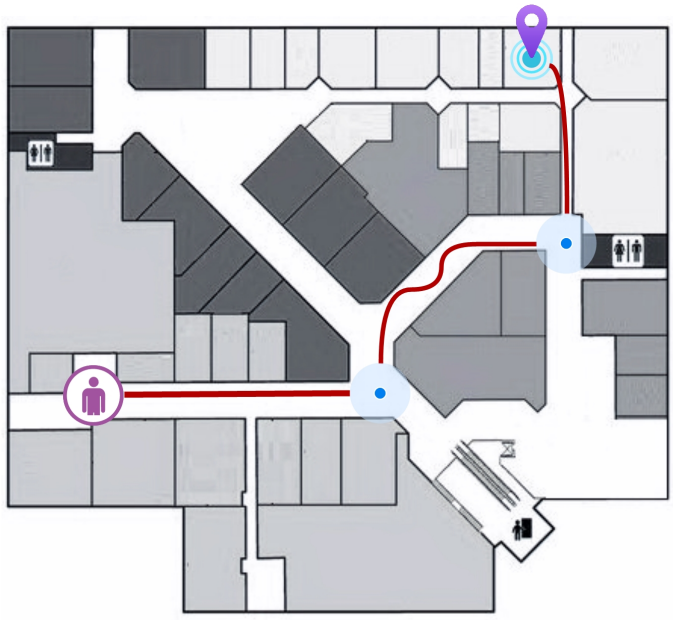

Fig. 1. Example of indoor navigation.

Parulian et al. [12] developed an indoor navigation system with guiding assistance depending on user location and desired destination. Dionti et al. [13] presented a three-dimensional space routing system implementation that represents data as an undirected graph with three-dimensional properties. The study compared four algorithms to determine which offered the shortest path in three dimensions. "The four algorithms are the Dijkstra Algorithm, A* Algorithm, Bellman-Ford Algorithm, and Floyd-Warshall Algorithm".

Alamri et al. [14] proposed an indoor multi-user routing algorithm for social distancing by considering and predicting user locations. The proposed indoor multi-user routing architecture consists of several components, including "indoor data structure, routing selection algorithm, density mechanism algorithm, and predictive routing algorithm". Dionti et al. [15] created a prototype routing system between buildings that combined outdoor and indoor routing systems.

Also, indoor navigation has been studied using semantic ontologies. The IndoorGML and BIGML data model have been applied to model indoor spatial information [16, 17]. Building Topology Ontology (BOT) was proposed to the W3C community group for Linked Building Data as "a simple ontology covering the core concepts of a building" [18].

Ontologies containing semantic representations of navigation path components were presented by Alamri [4] for an indoor navigation system with reasoning functionalities. The proposed system can be employed in navigation systems for route finding and presentation, along with crowd-density monitoring. ONALIN is an indoor routing ontology and algorithm that specifically takes into consideration the American Disability Act (ADA), presented by Doubts et al. [19].

Anagnostopoulos et al. [20] presented a hybrid modeling method for user navigation, called "OntoNav", that incorporates geometric and semantic information, as well as an ontological framework for processing routing requests. Sriharee [21] developed an ontology for indoor navigation based on symbolic information specified in Web Ontology Language (OWL). Wang et al. [22] proposed an ontology for expressing indoor navigation models using semantic location information.

Lee et al. [23] suggested ontology-based semantic queries to investigate indoor activities in a university environment. Yang et al. [24] investigated the use of ontologies for seamless navigation in both indoor and outdoor environments. Kim et al. [25] developed a spatiotemporal context-awareness knowledge model meant to recognize user objectives and help users when several paths are involved, such as hospital tasks.

Zlatanova and Liu [26] developed an indoor navigation space model (INSM) that uses semantic information to create connectivity graphs for buildings and identify several types of building spaces, such as inaccessible obstacles. Park et al. [27] built an expanded data model to assist persons with disabilities with indoor navigation by describing the relevant properties and relationships between PWD mobility and indoor environments. The IndoorGML application is used to support route planning that takes into account information regarding obstacles.

Maheshwari et al. [28] created an ontology for indoor places that considers both semantic and geometric properties. On the basis of this ontology, a space semantic model is developed, which can be used in a variety of applications. Li et al. [29] presented an indoor space dimensional model that allows for barrier-free path-finding by combining geometric, topological, and semantic layers.

All these recent works focus on data models and algorithms for indoor routing to support navigation systems for route finding and presentation. However, the collected data is usually sensitive, so the privacy issues raised by indoor routing are extensive. In fact, misuse of indoor location data can lead to the disclosure of sensitive personal information about users, such as personal interests and lifestyles.

Many works have been developed that focus on the privacy of moving objects' paths in outdoor environments. According to Wu et al. [30], location pair reorganization can be used to protect trajectory privacy. Differential privacy is a new privacy-preserving technology based on data distortion that secures sensitive data while maintaining statistical features by introducing random noise to data [31, 32, 33, 34]. Wang et

al. [35] generate dummy trajectories by rotating the user's real trajectory at the specified rotation point. Shaham et al. [36] choose dummy locations that have the same posterior probability as the real places.

Some studies have been concerned about related privacy-preserving methods in indoor positioning systems. Kim et al. [37] proposed a privacy protection strategy for indoor positioning. This approach suggests the usage of an application that changes the phone's MAC address on a regular basis. They choose this approach to protect the user's privacy by not revealing his or her identification to the server. Li et al. [38] introduced noise into user fingerprint data using differential privacy. Furthermore, differential privacy has been applied to data obfuscation approaches to generalize and specialize user fingerprints [39, 40]. Sazdar et al. [41] proposed creating dummy places to safeguard users' location privacy. Zhao et al. [42] presented a paradigm-driven privacy protection framework for indoor localization based on local differential privacy. A comprehensive review was presented in [43] for indoor localization, which analyzes previous studies on user privacy on devices, in data transmission, and on servers.

To the best of our knowledge, the studies on semantic indoor trajectory-based human mobility data have focused mostly on finding routes without taking the privacy issue into account. We are the first to consider user trajectory privacy in a semantic ontology-based indoor spatial information model. This paper incorporates semantic ontology and semantic privacy inference into indoor location-based services to improve accuracy and enrich navigation instructions with preserving the privacy of the user by generating an ambiguous trajectory. Users' sensitive points are identified and use random candidate points to replace them for a pruning process. Consequently, a protected semantic trajectory database is created that preserves semantic consistency and resembles the original semantic route while maintaining various levels of user privacy. In terms of semantic indoor privacy, the proposed algorithm has advantages. An option is provided for users to select whether privacy protection should be activated. The system also can ensure the privacy of moving objects in indoor environments by generating an ambiguous trajectory based on sensitive zones/points, which prevents an attacker from knowing the true route of a user. This can help the user preserve the privacy of his or her movements, as a breach of privacy could be used for advertising, propagating rumors, or other illegal objectives.

III. Semantic Web: The Concept of Ontology

The concept of the Semantic Web indicates the objective of encoding information in a way that both humans and computer systems can understand [44, 45, 46]. This includes creating new ways to represent increasingly complex knowledge for true semantic interoperability. Hence, paradigms for operating the Semantic Web require the formal definition of domain models. These formal models (referred to as ontologies) should contain a clearer and more effective description of the terms used and their relationships than the metadata [47, 48].

Ontologies have brought new ways of representing knowledge, adding the ability to derive new knowledge not explicitly derived from the analysis of existing data. This gives the system a more efficient way of reasoning and a common way of representing knowledge across different systems working towards the same goal. The World Wide Web Consortium (W3C) has established the Resource Description Framework (RDF) as "the standard paradigm for data exchange on the Web" [45, 46, 49, 50, 51, 52].

These considerations drive our decision to base our knowledge model on semantic web concepts and technology. Our work focuses on semantics in order to improve the proposed system with such capabilities. It serves as a semantic middleware, interlinking, capturing, and providing results. This is shown by the ontology component, in which diverse content is homogenized and stored locally in accordance with RDF triples within a knowledge base. More specifically, the model is employed using RDF edge-labeled graph, Fig. 2. With RDF, heterogeneous data can be integrated with different underlying schemas and distributed graphs can be represented semantically with the relevant reasoning capabilities.

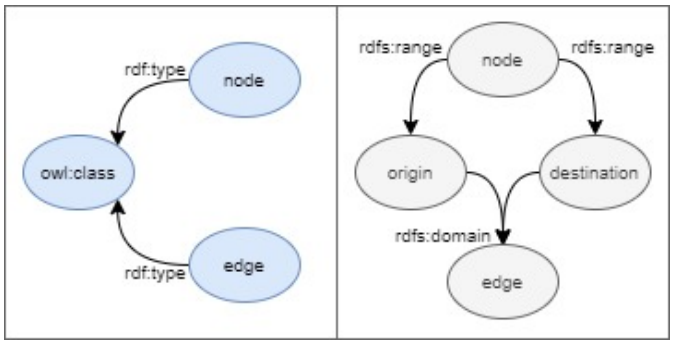

Fig. 2. RDF edge-labeled graph.

IV. Semantic Indoor Trajectory Privacy Preservation Algorithm

The proposed model architecture has been presented in Fig. 3. The architecture is comprised of two-level components: a semantic spatial ontology model for indoor routing, and semantic ambiguous trajectory privacy inference preservation. Each of the architecture's components is explained in more detail as follows:

In the top-level, a spatial ontology model is a routing system implemented in buildings and responsible for selecting the most accessible navigation path for users. The major issue with the spatial ontology routing model is understanding how to create the data structure that describes an indoor environment (Fig. 4). The increasing complexity of indoor spaces demands that the data model for indoor space's semantic division be able to handle efficiently the various features that are likely to be found in complex indoor spaces.

In the indoor space depicted in Fig. 4, it would be straightforward for a user to determine the optimal path from R1 to R2 within a building. However, the computer requires an accurate data structure that can describe corridors, rooms, and staircases. The semantic ontology of indoor space representation is depicted in Fig. 5.

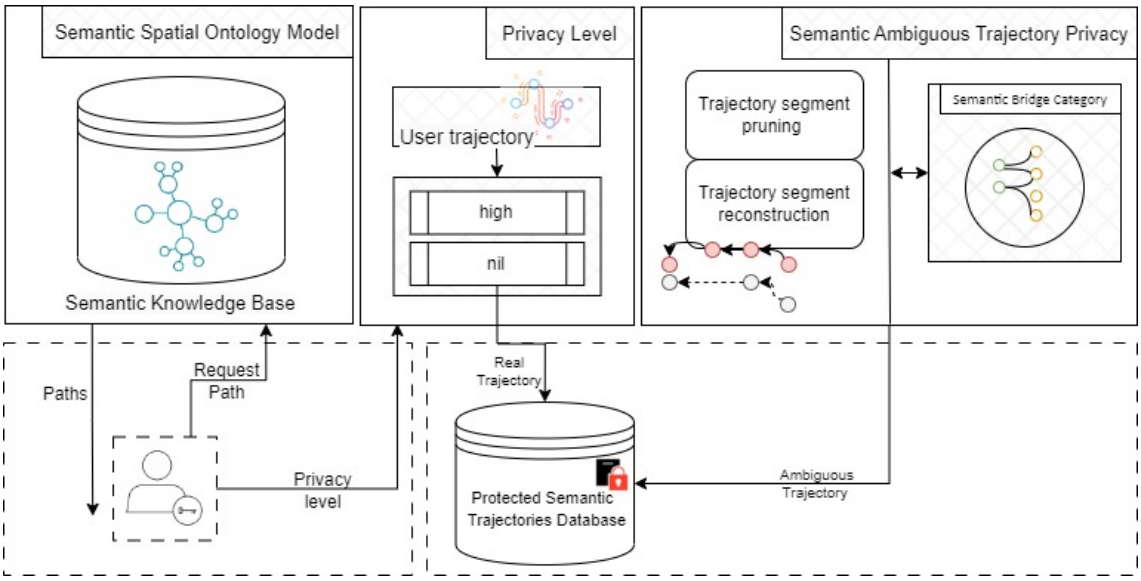

Fig. 3. Proposed system architecture.

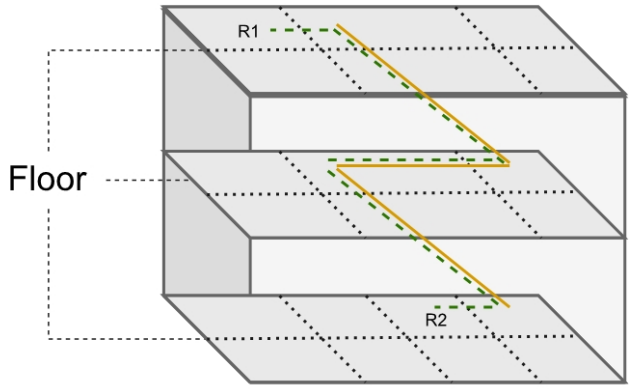

Fig. 4. Indoor space illustration.

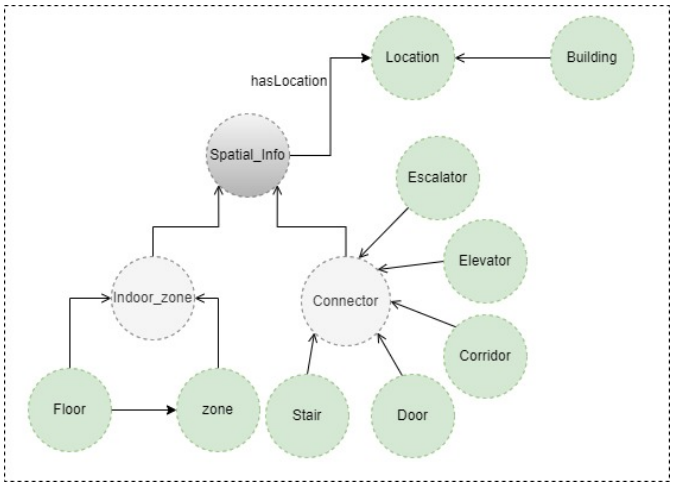

Fig. 5. Semantic ontology of indoor space.

The model presents a semantic model for indoor space that contains both syntactic and semantic information about spaces. In this model, the semantically enhanced representation of indoor space that we propose is a layered multigraph. Its node classes represent indoor spatial spaces symbolically, and its edges provide topological connection information between those spaces. Static semantic information about the indoor space is represented via node classes and attributes that relate to it, as well as node-edge layering. This is determined by the shape of the space, its connectivity with other spaces, and its functional features. We defined two main semantic node classes for the indoor space taxonomy. In order to show the overall hierarchy of floors inside a building, indoor zone space is the primary subclass to which the room and floor. The other is connector space which indicates the connection between the indoor zone and the different floors. The specific semantic partition model is defined as:

- Indoor zone space
  - Room
  - Floor
- Connector space
  - Corridor
  - Stair
  - Door
  - Elevator
  - Escalator

Definition 1 (Taxonomy of Indoor Space): The ontology for indoor space taxonomy consists of two main ontology classes: *"Indoor zone* $\wedge$ *connector"*,

- *"Indoor zone space"* specifies the major subclass to which the room and floor belong in order to describe the overall hierarchy of floors within a building.
- *"The connector space"* indicates the link between the indoor_zone and the various floors.

Definition 2 (User Route): A user route, which consists of a series of sample points, is usually associated with a specific moving object as Tr_i= (P_s, $cp_i \cdots cp_n$, P_d) where:

- P_s identifies the moving object current point/zone location.
- $cp_i \cdots cp_n$ represents the obtained trajectory connection points.
- P_d identifies the end point (destination zone).

The system can receive two inputs: the first provides the current point/zone location, and the second contains the location of the endpoint zone of the user's destination. The system then presents the user with routes from the starting point to the destination. An algorithm for building a routing approach for an indoor environment can be summarized as the pseudo-code shown in Algorithm 1. Once the best route has been followed and the user reaches the endpoint, the system will begin protecting privacy if the user requests privacy protection.

In the lower level, semantic ambiguous trajectory privacy inference preservation is employed to safeguard the actual trajectory of moving objects. The result is a protected semantic trajectory database that preserves semantic consistency and a form resembling the original semantic route while meeting various user privacy requirements.

Definition 3. A privacy level is defined as P = Privacy_level, Privacy_level $\in$ [high, nil].

Specifically, the privacy level is organized into two levels: Nil privacy (nil), and High privacy (high). Privacy level acts as a confidence level to register path. In the case of nil privacy, the actual trajectory of the moving object is registered. With high privacy, the user achieves privacy protection by safeguarding the actual trajectory of moving objects.

Our goal is to protect the sensitive points while still publishing a trajectory, albeit one consisting of a sequence of ambiguous points. The general idea of semantic ambiguous trajectory privacy is that an adversary with access to the protected semantic trajectories database comes to the same conclusion as whether an individual's trajectory data is included in the database or not. If ambiguous trajectory privacy is achieved in publishing trajectory data, it can assure the user that the released data will not leak his/her privacy whether or not his/her trajectory is in the database. Also, ambiguous trajectory data is published to confuse adversaries due to their similar shape and semantic attributes. When a user wants his or her trajectory's privacy inferences to be protected, the algorithm will collect trajectory data for the user from a data-centric semantic trajectory. First, to protect the privacy of this user's trajectory, we replace two connection points - the starting point and the destination point - with other random points.

Then, in the ambiguous trajectory generation stage, we map these two points by matching them with other random candidate semantic points (from the same or next level) and assume that they have the same semantic attribute. Finally, the algorithm will reconstruct the fake user trajectory by replacing all sensitive points. In this way, the semantic-protected trajectory database that is published will contain a sequence of ambiguous points.

The ambiguous trajectory generation method involves trajectory processing based on sensitive zones/points and other semantic information to prevent an attacker from determining the user's actual trajectory. The most common targets are the start-end points. There are two types of ambiguity-generation methods: trajectory segment pruning and ambiguity trajectory reconstruction. The pruning method eliminates sensitive points from the trajectory segment and uses random candidate points from the semantic bridge category to replace the corresponding start and stop points.

Semantic mappings between different location points are expressed via a semantic bridge category. To formalize this concept, we provide the following definition. Each location point is formalized with a prefix index in order to make it distinct from the others. For example, we use the i prefix to show the original start/end location point. Similarly, we use the j prefix index to signify the candidate location point.

Definition 4 (Semantic Bridge Category): The semantic bridge category can be expressed as: Mapping $P_{si} \xrightarrow{\triangleright} P_{sj} \wedge P_{di} \xrightarrow{\triangleright} P_{dj}$ where:

- P_{si} and P_{di} identify original start and end zones/points.
- P_{sj} and P_{dj} identify random start and end zones/points.
- $\xrightarrow{\triangleright}$ is the mapping bridge between points.

The proposed trajectory reconstruction algorithm is demonstrated in Algorithm 1. First, we locate a starting point in the trajectory segment P_{si}. Similarly, we locate an end point P_{di} on the segment and generate mapping bridge between these location points based on semantic bridge category $P_{si} \xrightarrow{\triangleright} P_{sj} \wedge P_{di} \xrightarrow{\triangleright} P_{dj}$. We generate a certain number of connection points on the segment (P_{sj}, $cp_j \cdots cp_n$, P_{dj}). Various trajectory segments can be obtained. Finally, we utilize the trajectory segment $P_{sj} \cdots P_{dj}$ to replace the original trajectory segment. Subsequently, a new trajectory segment is created, thereby protecting user privacy. These trajectories are illustrated in Fig. 6.

V. Experimental Validation

In this section, we use a software engineering strategy and validation experiments to ascertain the effectiveness of the proposed algorithm. The experiment test cases are designed to test ontology-based spatial information and ambiguous trajectory generation for privacy protection. For this experiment, using the indoor space ontology, we created a virtual dataset corresponding to a hypothetical two-floor building.

Assume a user visits a building for the first time and wishes to be directed to a certain zone without disclosing her/his location to the building's manager or any other party. This situation is common in, for example, malls, airports, hospitals, and university campuses. It necessitates the use of an autonomous application running on the user's mobile terminal that can provide the necessary location data as well

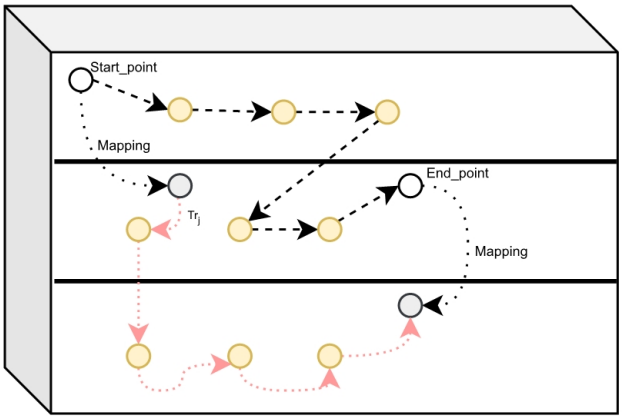

Fig. 6. Deriving a new trajectory segment.

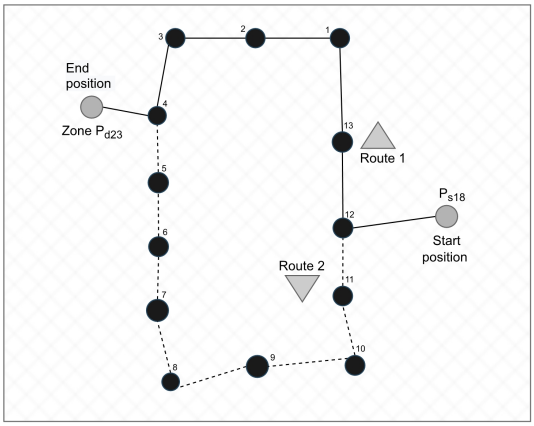

Fig. 8. The connection points to zone d_{23}.

as the information required for the generation of navigation directions.

We give an example of the simulation of the proposed privacy routing algorithm. Examples of the routes are shown in Fig. 7 and 8. Here, moving object o_i wants to visit zone P_{d23} and her/his start position was zone P_{s18}. Based on the trajectory connection points from $P_{s18} \cdots P_{d23}$, the expected route P_{s18}, cp_{12}, cp_{13}, cp_1, cp_2, cp_3, cp_4, zone P_{d23} or P_{s18}, cp_{11}, cp_{10}, cp_9, cp_8, cp_7, cp_6, cp_5, cp_4, zone P_{d23}. The user o_1 can reach the zone by following one of these routes. When the user uses the optimal route and reaches the endpoint, our proposed algorithm is meant to ensure privacy protection.

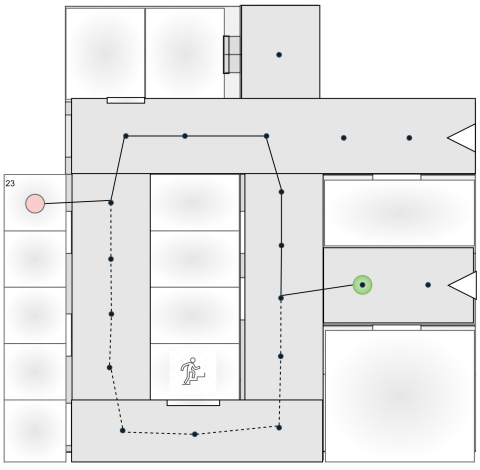

Fig. 7. The route to room/zone d_{23}.

The system generates an ambiguous trajectory and reconstructs it to create new segments of the trajectory for the user. It generates a mapping bridge between start/end location points and computes new traversable routes between two new points. Fig. 9 shows the route of validation on MATLAB, from the current position to zone P_{d23}. Fig. 10 shows a new trajectory segment that has been produced by the system for the user, thereby protecting user privacy.

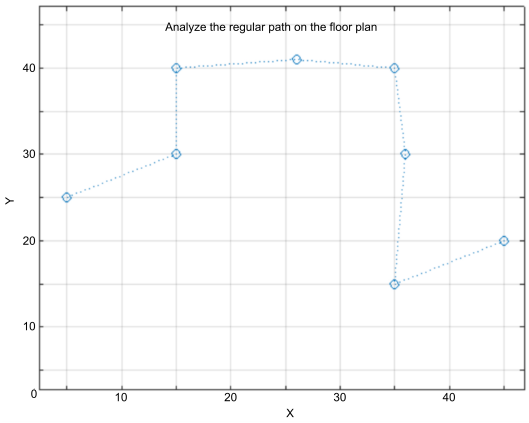

Fig. 9. Validate regular path under MATLAB.

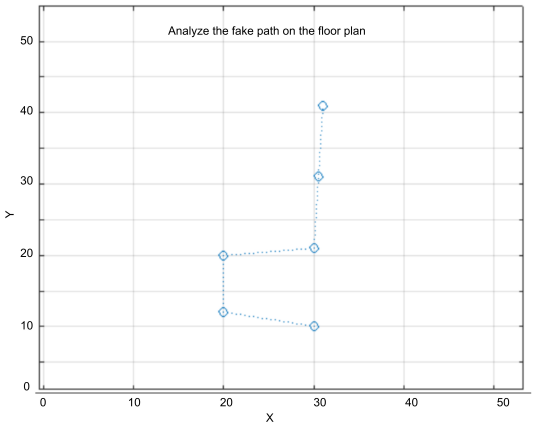

Fig. 10. Validate fake path under MATLAB.

Algorithm 1: Semantic Privacy Inference Preservation Algorithm

Begin
  Input: P_{si}: initial node, P_{di} the destination node, O: the ontology knowledge
  Output: Tr: trajectories from $P_{si} \rightarrow P_{di}$
  Procedure generate routes from $P_{si} \rightarrow P_{di}$
  Function `main()`
    Tr[] = ∅; // list of Trajectories
    Route = BuildRoute(P_{di});
    Tr[] = Route;
    Privacy_level = PrivacyInference();
  Function `BuildRoute(`*dest*`)`
    explored[] = ∅; //list of explored route segment
    initial = P_{si};
    insert P_{si} in explored;
    if *initial == dest* **then**
      return initial;
    end
    foreach *i ← 0 len(dest) -1* **do**
      find connect points of nodes;
      initS = P_{si};
      destD= P_{di};
      Routing.merge(verticalPassage(initS, destD))
    end
  Function `verticalPassage(`*initS, destD, explored*[]`)`
    RouteSegment= explored[];
    if *initS.floor = destD.floor* **then**
      cp = selectcp(initS.floor); // select all cp in the unit of destD
      sort using EuclideanDistance(initS, cp);
      destD = cp;
      RouteSegment.merge(initS,destD);
    end
    else
      select cp that connect to the other floor
      newD= destD.unit.get(destD.floor);
      RouteSegment.merge(initS,newD, destD);
    end
    Tr[] ← explored[i]
    check another route Extra_Route();
  Function `Extra_Route()`
    if *y adjacent to the* P_{si} **then**
      foreach *y* **do**
        Find y not in RouteSegment;
        update y to the new route: explored[$i+1$]
        Tr[] ← explored[$i+1$]
      end
    end

The results demonstrate that the proposed semantic indoor privacy method has advantages. It enables the user to choose whether or not to activate privacy protection. It can also protect the trajectory of moving entities in indoor environments by employing an ambiguous trajectory generation mechanism based on sensitive zones/points and other semantic information to prevent an attacker from determining the user's actual route.

  Function `PrivacyInference()`
    if *Privacy_level = nil* **then**
      Generate and store original user trajectory
    end
    else
      if *user reached →* P_{di} **then**
        Activate ambiguous trajectories generation stage
        Find a start/endpoints in the trajectory segment: P_{si}, P_{di}
        Generate $\xrightarrow{mapping}$ Bridge_Category
        $P_{si} \xrightarrow{\triangleright} P_{sj}$
        $P_{di} \xrightarrow{\triangleright} P_{dj}$
        Compute traversable routes between two new points: $P_{sj} \cdots P_{dj}$
        Tr_j = (P_{sj}, $cp_j \cdots cp_n$, P_{dj})
        Derive new trajectory segment
      end
    end
end

This can assist the user to protect the privacy of his or her movements, as a breach of privacy could be exploited for advertising, spreading rumors, or other unauthorized purposes. In the future, more research will be conducted to improve the experiment. A comparison with similar approaches is provided. Furthermore, we would like to assess its effectiveness and performance in recreating user trajectory through real-world usage.

VI. Conclusion and Future Work

In this paper, we proposed an algorithm for safeguarding the semantic privacy inference of entities moving within indoor environments. Previous studies on the privacy of spatial trajectory have focused mostly on outdoor environments, whereas this work focuses exclusively on indoor environments. The proposed algorithm finds the best route for users while preserving their privacy and offering the user the choice to activate privacy protection. The proposed privacy solution involves the generation of an ambiguous trajectory generation based on sensitive zones/points and other semantic information to prevent an attacker from determining the user's actual trajectory in an indoor environment. By means of this algorithm, users can easily find a specific place in a building and achieve adequate privacy protection as the algorithm conceals the user's trajectory.

It is anticipated that future studies will improve on the experiment described in this research and conduct related experiments in an actual indoor space environment. Additionally, several challenges need to be addressed. We intend to evaluate the impact of the overall performance of the proposed algorithm on the reconstruction of user trajectory.

References

[1] W. Wu, W. Shang, R. Lei, and X. Yang, "A trajectory privacy protect method based on location pair reorganiza-

tion," *Wireless Communications and Mobile Computing*, vol. 2022, 07 2022.

[2] A. Alamri, "Cloud of things in crowd engineering: A tile-map-based method for intelligent monitoring of outdoor crowd density," *Sensors*, vol. 22, no. 9, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/9/3328

[3] S. Shaham, M. Ding, B. Liu, S. Dang, Z. Lin, and J. Li, "Privacy preservation in location-based services: A novel metric and attack model," *IEEE Transactions on Mobile Computing*, vol. 20, no. 10, pp. 3006–3019, 2021.

[4] A. Alamri, "Semantic-linked data ontologies for indoor navigation system in response to covid-19," *ISPRS International Journal of Geo-Information*, vol. 10, no. 9, 2021. [Online]. Available: https://www.mdpi.com/2220-9964/10/9/607

[5] Y. Deng, H. Ai, Z. Deng, W. Gao, and J. Shang, "An overview of indoor positioning and mapping technology standards," *Standards*, vol. 2, no. 2, pp. 157–183, 2022. [Online]. Available: https://www.mdpi.com/2305-6703/2/2/12

[6] J. K. Nagar, A. Akolkar, and R. Kumar, "A review on airborne particulate matter and its sources, chemical composition and impact on human respiratory system," *International Journal of Environmental Sciences*, vol. 5, no. 2, pp. 447–463, 2014.

[7] N. E. Klepeis, W. C. Nelson, W. R. Ott, J. P. Robinson, A. M. Tsang, P. Switzer, J. V. Behar, S. C. Hern, and W. H. Engelmann, "The national human activity pattern survey (nhaps): a resource for assessing exposure to environmental pollutants," *Journal of Exposure Science & Environmental Epidemiology*, vol. 11, no. 3, pp. 231–252, 2001.

[8] P. Wang, J. Yang, and J. Zhang, "Indoor trajectory prediction for shopping mall via sequential similarity," *Information*, vol. 13, no. 3, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/3/158

[9] D. L. McGuinness, F. Van Harmelen *et al.*, "Owl web ontology language overview," *W3C recommendation*, vol. 10, no. 10, p. 2004, 2004.

[10] G. Klyne, "Resource description framework (rdf): Concepts and abstract syntax," *http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/*, 2004.

[11] A. Alamri, "Ontology middleware for integration of iot healthcare information systems in ehr systems," *Computers*, vol. 7, no. 4, 2018. [Online]. Available: https://www.mdpi.com/2073-431X/7/4/51

[12] J. M. Parulian, K. M. Adhinugraha, and S. Alamri, "Indoor navigation guidance for mobile device," in *Proceedings of the 20th International Conference on Information Integration and Web-Based Applications & amp; Services*, ser. iiWAS2018. New York, NY, USA: Association for Computing Machinery, 2018, p. 345–349. [Online]. Available: https://doi.org/10.1145/3282373.3282412

[13] T. A. Dionti, K. M. Adhinugraha, and S. Alamri, "Indoor routing in three dimensional spaces," in *2017 5th International Conference on Information and Communication Technology (ICoIC7)*, 2017, pp. 1–5.

[14] A. Alamri, R. A. Alturki, and S. Alamri, "Multi-user routing algorithm for indoor spaces – adapted for social distancing," *Journal of King Saud University - Computer and Information Sciences*, 2022.

[15] T. A. Dionti, K. M. Adhinugraha, and S. M. Alamri, "Inter-building routing approach for indoor environment," in *International conference on computational science and its applications*. Springer, 2017, pp. 247–260.

[16] J.-S. Kim, S.-J. Yoo, and K.-J. Li, "Integrating indoorgml and citygml for indoor space," in *International Symposium on Web and Wireless Geographical Information Systems*. Springer, 2014, pp. 184–196.

[17] M. Kessel, P. Ruppel, and F. Gschwandtner, "Bigml: A location model with individual waypoint graphs for indoor location-based services," 2010.

[18] M. H. Rasmussen, M. Lefrançois, G. F. Schneider, and P. Pauwels, "Bot: the building topology ontology of the w3c linked building data group," *Semantic Web*, vol. 12, no. 1, pp. 143–161, 2021.

[19] P. M. Dudas, M. Ghafourian, and H. A. Karimi, "Onalin: Ontology and algorithm for indoor routing," in *2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*. IEEE, 2009, pp. 720–725.

[20] C. Anagnostopoulos, V. Tsetsos, P. Kikiras *et al.*, "Ontonav: A semantic indoor navigation system," in *1st Workshop on Semantics in Mobile Environments (SME05), Ayia*. Citeseer, 2005.

[21] G. Sriharee, "A symbolic-based indoor navigation system with direction-based navigation instruction," *Procedia Computer Science*, vol. 52, pp. 647–653, 2015.

[22] X. Wang, J. Shang, F. Yu, and J. Yan, "Indoor semantic location models for location-based services," *Int. J. Smart Home*, vol. 7, no. 4, pp. 127–136, 2013.

[23] K. Lee, J. Lee, and M.-P. Kwan, "Location-based service using ontology-based semantic queries: A study with a focus on indoor activities in a university context," *Computers, Environment and Urban Systems*, vol. 62, pp. 41–52, 2017.

[24] L. Yang and M. Worboys, "A navigation ontology for outdoor-indoor space: (work-in-progress)," in *Proceedings of the 3rd ACM SIGSPATIAL international workshop on indoor spatial awareness*, 2011, pp. 31–34.

[25] G. Kim, M. Han, J. Park, H. Park, S. Park, L. Kim, and S. Ha, "An owl-based knowledge model for combined-process-and-location aware service," in *Symposium on Human Interface*. Springer, 2009, pp. 159–167.

[26] L. Liu and S. Zlatanova, "A semantic data model for indoor navigation," in *Proceedings of the Fourth ACM SIGSPATIAL International Workshop on Indoor Spatial Awareness*, 2012, pp. 1–8.

[27] S. Park, K. Yu, and J. Kim, "Data model for indoorgml extension to support indoor navigation of people with mobility disabilities," *ISPRS International Journal of*

Geo-Information, vol. 9, no. 2, p. 66, 2020.

[28] N. Maheshwari, S. Srivastava, and K. S. Rajan, "Development of an indoor space semantic model and its implementation as an indoorgml extension," *ISPRS International Journal of Geo-Information*, vol. 8, no. 8, p. 333, 2019.

[29] W. Li, D. Hu, and Z. Lin, "Indoor space dimensional model supporting the barrier-free path-finding," in *2018 Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS)*, 2018, pp. 1–9.

[30] W. Wu, W. Shang, R. Lei, and X. Yang, "A trajectory privacy protect method based on location pair reorganization," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[31] R. Tan, Y. Tao, W. Si, and Y.-Y. Zhang, "Privacy preserving semantic trajectory data publishing for mobile location-based services," *Wireless Networks*, vol. 26, no. 8, pp. 5551–5560, 2020.

[32] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Computer Networks*, vol. 135, pp. 32–43, 2018.

[33] X. Liu, A. Liu, X. Zhang, Z. Li, G. Liu, L. Zhao, and X. Zhou, "When differential privacy meets randomized perturbation: a hybrid approach for privacy-preserving recommender system," in *International Conference on database systems for advanced applications*. Springer, 2017, pp. 576–591.

[34] R. Tan, Y. Tao, W. Si, and Y.-Y. Zhang, "Privacy preserving semantic trajectory data publishing for mobile location-based services," *Wireless Networks*, vol. 26, no. 8, pp. 5551–5560, 2020.

[35] T. Wang, J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation based on a fog structure for cloud location services," *IEEE Access*, vol. 5, pp. 7692–7701, 2017.

[36] S. Shaham, M. Ding, B. Liu, S. Dang, Z. Lin, and J. Li, "Privacy preservation in location-based services: A novel metric and attack model," *IEEE Transactions on Mobile Computing*, vol. 20, no. 10, pp. 3006–3019, 2020.

[37] S. Kim, S. Yoo, and J. Kim, "Privacy protection mechanism for indoor positioning systems," *International Journal of Applied Engineering Research*, vol. 12, no. 9, pp. 1982–1986, 2017.

[38] S. Li, H. Li, and L. Sun, "Privacy-preserving crowdsourced site survey in wifi fingerprint-based localization," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, pp. 1–9, 2016.

[39] Y. Zhu, Y. Wang, Q. Liu, Y. Liu, and P. Zhang, "Wifi fingerprint releasing for indoor localization based on differential privacy," in *2017 IEEE 28th Annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*. IEEE, 2017, pp. 1–6.

[40] Y. Wang, M. Huang, Q. Jin, and J. Ma, "Dp3: A differential privacy-based privacy-preserving indoor localization mechanism," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2547–2550, 2018.

[41] A. M. Sazdar, S. A. Ghorashi, V. Moghtadaiee, A. Khonsari, and D. Windridge, "A low-complexity trajectory privacy preservation approach for indoor fingerprinting positioning systems," *Journal of Information Security and Applications*, vol. 53, p. 102515, 2020.

[42] P. Zhao, H. Jiang, J. C. Lui, C. Wang, F. Zeng, F. Xiao, and Z. Li, "P 3-loc: A privacy-preserving paradigm-driven framework for indoor localization," *IEEE/ACM Transactions on Networking*, vol. 26, no. 6, pp. 2856–2869, 2018.

[43] S. Holcer, J. Torres-Sospedra, M. Gould, and I. Remolar, "Privacy in indoor positioning systems: a systematic review," in *2020 international conference on localization and GNSS (ICL-GNSS)*. IEEE, 2020, pp. 1–6.

[44] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web," *Scientific american*, vol. 284, no. 5, pp. 34–43, 2001.

[45] A. Alamri, "Semantic health mediation and access control manager for interoperability among healthcare systems," in *Data Analytics in Medicine: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2020, pp. 169–181.

[46] D. Kalibatiene and O. Vasilecas, "Survey on ontology languages," in *International Conference on Business Informatics Research*. Springer, 2011, pp. 124–141.

[47] G. Antoniou and F. Van Harmelen, *A semantic web primer*. MIT press, 2004.

[48] A. Alamri, P. Bertok, and J. A. Thom, "Authorization control for a semantic data repository through an inference policy engine," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 6, pp. 328–340, 2013.

[49] D. L. McGuinness, F. Van Harmelen *et al.*, "Owl web ontology language overview," *W3C recommendation*, vol. 10, no. 10, p. 2004, 2004.

[50] G. Klyne, "Resource description framework (rdf): Concepts and abstract syntax," *http://www. w3. org/TR/2004/REC-rdf-concepts-20040210/*, 2004.

[51] G. Antoniou and F. v. Harmelen, "Web ontology language: Owl," in *Handbook on ontologies*. Springer, 2004, pp. 67–92.

[52] A. Alamri, "Development of ontology-based indoor navigation algorithm for indoor obstacle identification for the visually impaired," in *2023 9th International Conference on Engineering, Applied Sciences, and Technology (ICEAST)*, 2023, pp. 38–42.