IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 January 2024, accepted 23 January 2024, date of publication 5 February 2024, date of current version 16 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3361940

RESEARCH ARTICLE

An Advanced Dummy Position-Based Privacy Provisioning Framework for TTP-Based LBS System

M. USMAN ASHRAF[1] AND KHALID ALI ALMARHABI[2]
[1]Department of Computer Science, GC Women University, Sialkot 51310, Pakistan
[2]Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University, Makkah 24381, Saudi Arabia
Corresponding author: M. Usman Ashraf (usman.ashraf@gcwus.edu.pk)

ABSTRACT A location-based service (LBS) is an IP-capable mobile device application that requires an understanding of where the mobile device is placed. The LBS is renowned for providing quick services to clients. The extensive praxis of the LBS has led to a keen interest in user privacy, a fundamental requirement of every user. As such, the LBS is primarily concerned with protecting users' privacy. Three basic metrics are related to confidentiality in the LBS system: temporal, identity, and spatial privacy. Losing someone's privacy attribute can ultimately interfere with a user's privacy. To cope with this problem, we introduce a novel advanced Dummy Position-based Anonymization (ADPA) mechanism to achieve the confidentiality of mobile users who frequently use the LBS. The proposed ADPA technique is based on an adaptive fixed k-anonymization (A-K_f) technique that utilizes the characteristics of a trusted third-party (TTP) server and the cloaking region. User privacy is achieved by shielding all three attributes of privacy (spatial, temporal, and identity), for which dummy generation, query processing by anonymization server, and LBS server processing algorithms were designed to shield user confidentiality. Extensive simulations were also carried out to evaluate the efficiency of the model.

INDEX TERMS Privacy protection, location-based services, mobile computing.

I. INTRODUCTION

In recent years, Location-Based Services (LBSs) have become an integral aspect of daily life due to the rapid progress of mobile devices and wireless communication. The prevalence of location-based applications, readily available on platforms like the App Store and Google Play Store, has empowered users to seamlessly interact with LBS servers through their mobile devices, particularly smartphones. These applications enable users to effortlessly send queries and receive relevant service data, such as locating nearby metro stations or accessing hotel pricing information [1]. Consequently, LBSs have significantly transformed the way individuals navigate their daily routines. Location-based services use significant time geospatial data from a smart device to provide information, amusement, and privacy. The LBS uses GPS technology from a smartphone to monitor the location of a person if that person has enabled the system to do so. The service can define the area to a street address after a smartphone user has opted in, without the need for manual data input. Figure. 1 presents a broad overview of the first LBS system [1]. According to Figure. 1, an LBS system consists of three primary elements including LBS/mobile user(s), LBS server(s), and communication medium.

Conventionally, a mobile user posts a query to LBS system to find out his/her point of interest (POI) through a communication medium. Various elements, for example, positioning, mobile devices, services, and communication networks, are needed for the LBS to function. Despite the undeniable conveniences offered by LBSs, a notable concern arises regarding the potential compromise of users' privacy and security. Typically, when a user seeks a service, they must disclose precise location details and specific interests to an LBS server that may not be fully trusted. In this process,

The associate editor coordinating the review of this manuscript and approving it for publication was Khursheed Aurangzeb.

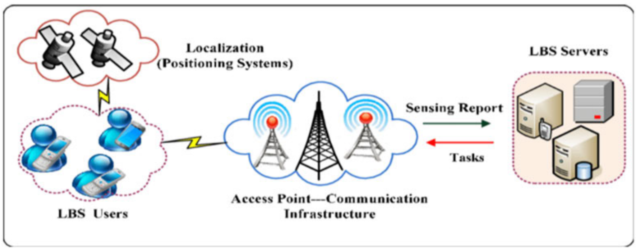


FIGURE 1. A fundamental architecture of Location Based Service system.

the server gains access to comprehensive information about the user, creating the possibility of direct user tracking or unauthorized disclosure of personal information to external parties [2]. The sensitivity of such information is paramount, and its mishandling could pose a substantial threat to the user's physical security if it falls into the wrong hands. Consequently, there is a critical need to prioritize the safeguarding of user privacy in the realm of LBSs.

To overcome the privacy challenges in LBS systems, several studies have been proposed over the past decade. These techniques can be categorized as follows:

- ***Space Transformation:*** To preserve their privacy, a mobile user employs a space-filling curve to convert their exact location into an alternative spatial representation.
- ***Spatial Clocking***: The fundamental concept behind spatial cloaking is to obscure a user's precise location by transforming it into a cloaked area that aligns with the user's privacy preferences.
- ***False Location***: Users ensure the protection of their privacy by providing either inaccurate locations or their authentic locations along with a set of fictitious locations, known as dummies, to the LBSs server.

Certainly, existing methodologies consistently ensure user privacy using established privacy metrics such as k-anonymity or entropy. Additionally, with the advent of blockchain, recent works [26], [27], [28], [29], [30], [31] have merged LBS and blockchain technologies to enhance location privacy, marking a noteworthy and growing trend.

However, existing approaches exhibit certain limitations. Firstly, the majority primarily concentrate on user location privacy [1], [11], [12], [13], [14], [15], [16], [17], [19], [20], [21], [22], [23], overlooking the interconnected nature of user privacy in LBSs, which encompasses both location and query privacy. A compromise in one area might jeopardize the other [25], necessitating the simultaneous protection of both. Secondly, numerous studies [11], [13], [14], [15], [16], [25] introduce a Trusted Third Party (TTP) server, known as the Location Anonymizer, for preserving user privacy in an LBS environment. Yet, TTP servers present drawbacks, including a potential single point of failure if compromised by adversaries, acting as a system performance bottleneck due to processing all queries, and facing challenges in finding a universally trusted third party. Thirdly, the repetitive querying of similar interests by many users poses a risk, as the LBS server repeatedly provides identical service data, escalating the exposure of user privacy.

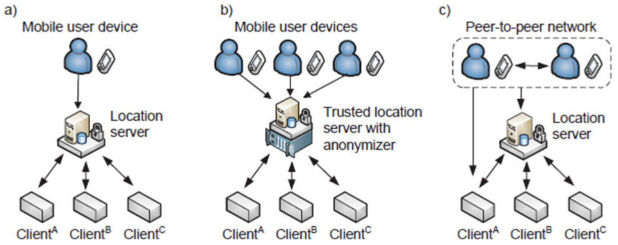

a)
Mobile user device
Location server
Client^A Client^B Client^C
b)
Mobile user devices
Trusted location server with anonymizer
Client^A Client^B Client^C
c)
Peer-to-peer network
Location server
Client^A Client^B Client^C

FIGURE 2. (a) NTTP-based LBS system architecture, (b) TTP-based LBS system architecture, and (c) peer-to-peer network-based LBS system architecture.

To address the aforementioned issues, this research work introduces an advanced dummy position-based anonymization (ADPA) technique for TTP-based LBS systems to adequately protect the user's identity, spatial information, and temporal information. The mian contributions of this paper can be summarized as follows:

- Introduce a novel ADPA model that guarantees user privacy in terms of spatial, temporal, and personal information using a trusted third party in the LBS system.
- The proposed algorithms included dummy generation, query processing by anonymization server, and LBS server processing that provided user confidentiality by using a dummy approach and identifying cloaked regions for users' POI.
- Secure mobile user's privacy in terms of identity, spatial information, and temporal information.
- Implementation of the proposed model in Riverbed Modeler simulation tool, which is considered as fundamental as an authentic approach to simulate according to real scenarios.

The remainder of the paper is as follows: Section II presents a literature review of the protection of the privacy of users while interacting with TTP-based LBS systems; Section III discusses the ADPA model and its concepts; Section IV describes the design and framework of the proposed algorithms; Section V presents the simulations that were carried out and the results that were obtained to check the efficiency of the model; while the conclusion is given in Section VI.

II. PRELIMINARIES

Almost every LBS application requires various vital aspects to control the critical work of positioning, exchanging information, and data processing. LBSs can be classified into three categories based on their conventional usage, namely, (a) non trusted third party (NTTP) based LBS systems, (b) trusted third party (TTP) based LBS systems, and (c) peer-to-peer LBS systems, as shown in Figure 2.

In the NTTP-based LBS system in Figure. 2 (a), the LBS user and LBS servers collaborate precisely without concern for any third factor. In this category of LBS system, the mobile user does not need any third party anonymizer to interact with LBS system. On the other hand, a TTP-based LBS system in Figure. 2 (b) facilitates transactions between the LBS user and server. This type of LBS system checks all the essential payment communications between LBS users and the LBS server based on the facility to detect fraudulent digital content. In the peer-to-peer LBS system in Figure. 2(c), the parties are directly connected to a transaction without a third-party intermediary. The peer-to-peer system exploits software to resolve the cost of trust, compliance, and data asymmetries that were historically determined by using the confidence of third parties. The implementation of an LBS concerning the advent of positioning systems and smartphone apps can watch and even record the behavior and position of a user in this Internet of Things (IoT) services [3], [4].

The provision of a LBS involves several challenges, including query efficiency, reliability, security, and privacy. In the LBS, when a user needs to know the location of a nearby ATM, café, or any other place using positioning technology, he/she must share his/her credentials with the LBS server, e.g., spatial privacy or trajectory could be revealed to other parties [5], [6], [7]. Under these circumstances, attackers can expose the privacy of users. While clients may enjoy the provided services, they are vulnerable to the danger of losing their privacy through the LBS providers in the Internet of Things [8], [9].

The privacy issues users face include spatial information, personal information, and temporal information. The user is said to be fully protected when these three factors are fully secure.

1) SPATIAL INFORMATION

Location privacy is an individual's ability to control accessibility to current and past information about their data [27]. It is very influential for users because the location information of a user can be used for unfair means if their data is leaked or accessed by unauthorized persons.

2) PERSONAL INFORMATION

A user's personal information comprises the user's ID, address, contact number, and other personal information used to identify the user [10]. If a client exposes his/her details to the location-based service, the user can be wrongly hacked/attacked by an unwanted individual, who might be an intruder/adversary. The aim is to hide the user's identity when he/she is using the LBS [11]. In the LBS, the user is entirely secure if, and only if, his/her personal information is completely shielded.

3) TEMPORAL INFORMATION

In the LBS, the user's temporal information is the time when the user makes a query. The user's temporal information is utterly secure if it is ultimately protected. It contains the moment or period when the user's position is correct [10].

III. RELATED WORK

Various studies have been conducted on user privacy, particularly when interacting with LBS systems. These privacy-preserving strategies can derive the user's location or personal information using his/her temporal information, which can threaten the privacy of the user. Different concepts like K-anonymity [2] and the pseudo-ID technique [4] efficiently ensure user spatial privacy in the LBS. The writers in [13], [14], and [15] provided approaches for overcoming the privacy issue. K-anonymity is used for the protection of privacy against different threats. Therefore, to precisely protect user spatial information, the authors in [16] designed a middleware architecture and algorithms for use with a centralized position broker network, and similarly, the authors in [17] suggested a preliminary investigation into privacy issues related to location-based services. They accurately established a risk assessment process for disclosing user identity by location information and provided preliminary ideas on strategies to prevent this from happening.

The authors guarantee that no private data is disclosed to the service provider when information is uniquely identified through a location-based quasi-identifier. A trusted database has the standard features of a position server. The concepts of service requests, linkability, and historical k-anonymity [18] are central to their structure. A trusted server not only contains a list of user-issued applications in the database array, but also a series of position data. They set out the preliminary intent of imposing a certain level of privacy and determining that privacy policies that ensure location-based services are appropriate for delivering access in some areas [17].

Work on the depersonalization of locations was motivated by restricted issues regarding spatial recognition. The authors evaluated location depersonalization from the perspective of privacy [19]. They tested the feasibility of the proposed methodology by conducting simulations under different conditions. The model, known as a location-sensitive gateway (LPAG), contains two client and server device components. The entropy theory takes the number and the duration of their visits into account. They also figured out the trajectory cloaking problem, and proposed a new approach that could camouflage the trajectory of a client very quickly [20].

Doohee et al. [21] proposed an anonymity of motion vector (AMV), which is a cloaking system model that gives anonymity to location queries. The AMV reduces a mobile user's CR with the use of vectors for motion by comparing it with a distributed grid-based continuous cloaking (DGCC) [22] minimum cycle region (MCR) [23], which yields circular CRs. The AMV also provides a set of check fields for the entities surrounding the closest neighbour (NN) to the querier that receives a CR-based request. The efficacy of the proposed AMV has been proven in simulation experiments. The efficiency of the AMV may be further investigated in the future via experiments, where the querier moves rather than stays stationary [21].

The idea of location labels was also introduced to distinguish between the position of mobile users and sensitive locations. The authors designed an algorithm based on the location label (LLB) to protect location confidentiality while reducing the LBS request response time. Network aggression protocols such as pseudo-ID exchange protocol, and enhanced PLAM protocol were used to reduce the response time of LBS device [25]. G. Sun enhanced the location-based approach by implementing a location label algorithm to protect user privacy while reducing the response time of the LBS device. The output was also tested and the correctness of the applied algorithm was verified through detailed simulations. Currently, the PLAM algorithms based on l-diversity and k-anonymity need to be checked on the route, unless there are more uncontrollable factors to be tested, such as the 4G network power.

In [26], the authors elaborated on the location-cloaking approach to avoid the occurrence of aggression and to reduce the possibility of disclosing the position of the requesting issuer to untrusted parties (1/k). Location cloaking is accessible to query tracking attacks, where the opponent can determine the querier by comparing the two sectors in the LBS queries. The proposed model addresses this issue and produces smaller cloaking regions by stationary users without sacrificing the confidentiality of the position of the querier. A structured design protects both the contents of the request and the CR from being revealed to ongoing spatial queries. An active A-Kf method of anonymization will reduce the CRs within the Kf (fixed k-anonymity) [27] and resist attacks on request monitoring. Existing location anonymization methods are facing security risks associated with ongoing queries. The anonymizer tests the current locations and destinations of customers, and as the Cn grows, the cost of processing increases, but the volume of the CR decreases. LBS clients are believed to be traveling and to be distributed equally across the grid cells. The suggested (A-k) determines the value of k based on the application of the query issuer, increases the satisfaction of the query issuer, and decreases the anonymization server workflow. Although the suggested approach preserves k-anonymity, smaller CRs are obtained compared to existing position anonymization techniques.

Ruchika and Rao [28] illustrated the advantages of cloaking and obfuscation methods, and minimized the drawbacks. A hybrid approach to achieve location confidentiality has been proposed for mobile users who regularly use location services. The hybrid scheme is based on the collaborative pre-processing of location information and the homomorphic encryption [29]. A simulation scenario was developed, and the same was enforced in Java by executing it on a 3.20-GHz Intel Core machine with 4 GB of RAM running the Linux OS. The innovation of the proposed hybrid approach arose from the fact that third-party intervention can be added to perform computations only, while the TP has no awareness of the actual position of the client. The proposed HYB model maintains the confidentiality of the user's position at two points, namely, at the level of proximity, when establishing congregation, and at a distant point, when submitting an encrypted location to a credible/trusted party.

Arielle and Garbinato [30] proposed the ResPred, a system that enables the LBS to predict a user's location. This location prediction framework is called ResPred, with res and pred implying both respect (i.e., security for consumer privacy) and prediction. The ResPred system is developed at the level of the operating system of the mobile device, and is trustworthy regarding both the ResPred system and the positioning system. The first aspect focuses on localization, while the second aspect focuses on location protection. It can achieve 100 times the same location in the sense of the measurement with a spatial grid because the grid layout is set, and overlaps in a particular place, with the nearest position being still the same. The ResPred was tested from the perspectives of utility and security by using real user locations to equate the privacy system to existing techniques.

Gurjeet and Sachdeva [31], suggested an authentication system, where users of mobile phones can submit database requests for certain services. First, a location check is done; the server checks the identification of the user/device. The flow of information between the client and the server is managed safely. Encryption algorithms play a significant role in the information assurance system, and the encryption time is used to determine the throughput of an encryption scheme. The proposed architecture is divided into two main components: confirmation of position, and identification of device/user. The first part uses an android application that can either check the GPS coordinates or the BTS cell ID [32] to which the mobile device is connected or both. User identification of the second component and device can only be accessed after proper validation by the application for location verification.

Further dummy position based variety of models proposed to address the privacy issue in LBS systems. In dummy position approach, mobile user posts his/her actual query along with N number of dummy position form a certain region to LBS system. On receiving results, the query response is broadcasted to that region and actual user access the query results easily without any inference. Most of the dummy position based models assume that the attacker always chooses the location randomly without any background knowledge. To overcome this issue, Ben et al., [13] proposed E-DLS model where the dummy positions are selected to enhance the privacy with respect to entropy and clocking region. Gang et al. [33] improved the E-DLS and proposed a new scheme where the user's region is designated as clocking region instead of actual region. However, location cloaking is accessible to query tracking attacks, where the opponent can determine the querier by comparing the two sectors in the LBS queries. Similarly, Alsubhi et al. [37] proposed HBLP privacy protection scheme using PID and PLAM protocols in a peer to peer (P2) model. HBLP improved overall privacy while a user interacts with LBS system but all the query content was depended on forest user. The dependency of one entity can cause a major issue if information is disclosed by forest user. To overcome the middle layer dependency, a novel approach is required that can protect user's spatial as well as temporal information while interacting with LBS system.

The literature mentioned above focuses on protecting the personal and spatial information of users. Multiple strategies

TABLE 1. Comparative analysis of existing techniques concerning privacy protection goals.

State of the Art methods	Identity Info	Spatial Info	Temporal Info
k-anonymity [2]	√	√	×
Location based Quasi-Identifiers [5]	√	√	×
Location Depersonalization using feeling based location privacy [6]	√	√	×
Anonymity of motion factor [7]	×	√	×
Location labels [9]	×	√	×
Location clocking [10]	√	√	×
Hybrid method [11]	√	√	×
Anonymous communication using dummies [12]	×	√	×
Query authentication mechanism [13]	√	×	×
Middleware architecture [18]	√	√	×
Star clock [19]	√	×	√
Mandatory access model [20]	√	√	×
Pseudonym transaction method [21]	√	×	×
User defined location sharing for mOSNS [23]	×	√	×
Preliminary investigation [21]	√	×	×
Expanded anonymous server [24]	√	×	×
Bloom Filter [25]	√	×	×
Cryptography using RSA [26]	×	√	×
Protection at Service Provider End [27]	×	√	×
ResPred [30]	√	√	×
Smart authentication system [31]	√	×	×
E-DLS [33]	√	√	×

are targeted at multiple scenarios to provide user privacy, but none of the techniques concentrate primarily on temporal information, whereas the user is ultimately protected only if all three attributes (spatial, temporal, and identity) are fully guarded. In this research, the preservation of user privacy by securing all attributes simultaneously was explored.

We observe that in existing studies temporal information is not adequately protected in the context of spatial-temporal privacy within Location-Based Service Systems. While spatial privacy often receives considerable attention, overlooking or insufficiently addressing the temporal aspect creates a vulnerability. The potential consequences include the exposure of users' movement patterns, routines, and the duration of their stays at specific locations over time. However, there are still multiple key aspects that are required to be addressed such as:

A. INCOMPLETE PRIVACY PROTECTION

Many studies primarily focus on spatial privacy, neglecting the temporal dimension. This leaves users susceptible to profiling based on their historical movement data.

B. TEMPORAL CORRELATION

Failure to protect temporal information may lead to the identification of users based on their regular schedules, habits, or recurring visits to specific locations, compromising their anonymity.

C. COMPREHENSIVE PRIVACY MEASURES

Existing research may lack comprehensive approaches that integrate both spatial and temporal privacy protection measures, leaving a gap in providing users with holistic privacy safeguards.

D. DYNAMIC PRIVACY CONCERNS

As users' locations change over time, the dynamic nature of temporal privacy concerns requires specialized attention. Neglecting this aspect may result in incomplete protection for users' evolving patterns.

E. USER BEHAVIOR ANALYSIS

In the absence of robust temporal privacy protection, adversaries may exploit patterns in user behavior over time, posing threats to individual privacy.

Considering the above privacy protection gap in the field of LBS systems, we propose a novel privacy protection approach described in following section.

IV. PROPOSED ADPA FRAMEWORK

While all the existing methods are very helpful in protecting the privacy of users, they still fail to cover all the required identity, spatial, and temporal privacy simultaneously. The above methods offer user protection, but not a total degree of gratification, so that with these techniques there is still a chance that the privacy of the user will be violated. To overcome this problem and to preserve user privileges, a dummy position-based anonymizer server (ADPA) was designed, the architecture of which is shown in Figure. 3. The architecture is based on the adoptive fixed K-anonymization (A-Kf), and the user is completely secure from any threat of information leakage. The main elements involved in the ADPA system are the anonymizer server (AS), dummies, and user (querier), and the LBS server. A hierarchical system was followed in this work, with the participation of a trusted anonymizer. AS is a trusted party in the architecture, protecting the confidential information of the user from leakage. Dummies and real users were involved in this model. A querier can fix the other users

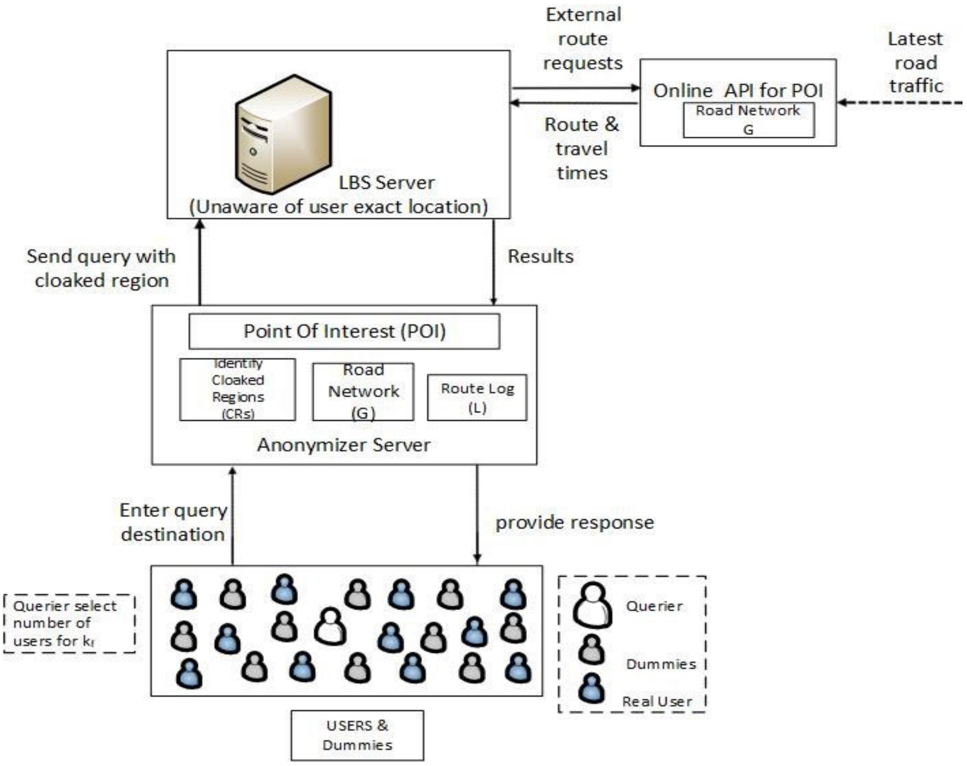


FIGURE 3. Architecture of the proposed dummy position-based anonymizer server.

with him/her, but he/she cannot attempt to infer the privacy of other users. Figure. 3 shows that the working of the ADPA architecture can be split into three key phases: anonymizer server (AS), LBS server, and dummies and user (querier).

A. DUMMIES AND USERS

The users involved in this case are the dummies and actual users. The querier is the real user who sends an encrypted request to the AS. The querier can fix other specific users as well. The users closest to the queriers are chosen as the fixed members of the cloaked region (CR) for the POI. The querier along with other users located in the grid area, G sends a query, q along with the selected fixed users and multiple dummies to the anonymizer server for the POI, which is stored in a 2-D array, and the AS responds to the querier.

A dummy position strategy presented in Algorithm 1, is implemented to preserve the privacy of the user, where the mobile user located in the grid area, G sends a query, q along with selected fixed users and multiple dummies to the anonymizer server for the POI, which is stored in a 2-D array.

According to the suggested solution, before sending a request to the LBS, the query is encrypted and determines the minimum lower limits (WL, HL) and maximum upper limits (WU, HU) of the height and width of the region defined as the "G" chart. The purpose of determining (WL HL, WU, HU) the coordinates/dimensions is to make the partition "G" equal to the number of cells, "Ci". The vertices are measured outside each cell to produce dummy positions, and one cell location is added to the real position of the mobile customer. In addition to creating dummy locations, vertices are determined outside any cell, and individual cell locations are appended to the real position of the device customer. Ultimately, by following the proposed Algorithm 1 (dummy generation), an array is generated, which includes all the dummy K positions and the actual user location index, keeping the querier secure from any intruder by creating dummies around him.

B. ANONYMIZER SERVER (AS)

AS is a trustworthy party involved in the system to maintain the point of interest (POI), route log (L), and road network (G) for the available POI. The cloaked regions (CRs) for the querier are also listed for the appropriate POI along with the fixed users (Kf). The anonymizer server sends encrypted data to the querier offering temporal privacy to shield the user information from any kind of assault. The AS communicates with the LBS system by supplying queries with the cloaked region to obtain services for that region.

After the generation of dummies and the fixing of users, an anonymizer server that knows the positions of the users and produces blurred positions for them, will test the positions of all the users, Ci and create a total cloaked region (CR) that requires K users, including the querier. The querier first decides the POI, K (fixed users (KF), +non-fixed users (KNF)), and the CN (number of clients) to pick the KF.

Algorithm 1 Dummies generation

```
Declarations:
P key → primary key          G→Road Network
S key → secret key           L→Route Log
A → Anonymous_Area           m→message/query
CR→Cloaked Region
$W_U$, $H_U$ →Upper limit width and height
$W_L$, $H_L$ → Lower limit width and height
$K_{NF}$ →Number of non-fixed clients
$m_{CR}$ →message with cloaked region
$K_F$ →Number of clients fixed by the user
K→Number anonymous clients
Ci→$i^{th}$ client
$C_N$ → User has set of K near to querier DPs→Dummy Positions
Input: User location (X, Y), A, number of clients for location anonymity (K and $K_f$), query issuer $q_i$, Fixed users was chosen by query issuer, Enc (m, $P_{key}$) → c,
Output: DPs, POI, $K_f$ member clients, Dec (c, $S_{key}$) → m
Procedure:
G($W_U$, $H_U$), G($W_L$, $H_L$) \\ Calculate Both Height and Width
C ← $\sqrt{G}$ \\ Determine the number of cells in G
(V, E) ∈ C \\ Resolve the edges and vertices of each cell.
$P_X$ ← Random (0, v(C-1)), $P_Y$ = ← Random (0, v(C-1))
array[0 to C][ 0 to C] \\ Load 2-D array
q= 0, r =0, x,y=0 \\ Initialize values up to x-axis, y-axis
While(q < (C-1)) \\ Fill up the number of dummy positions
While(r<(C-1))
DPs=Sybil query(Num of dummies) //cryptography through RSA algorithm
$Qery_{enc}$ = enc($query_{act}$+DPs);
if(m=CRs||m=POI||m=G||m=L)
return result(POI) using anonymizer query processing for CRs
Else
return result (POI) using LBS server processing
end loop
end loop
```

A nearest-neighbour query is then given by the querier, as shown in Algorithm 2. The anonymizer scans the actual positions and the customers' POI. The computing expense rises as the CN grows, but the scale of the CRs decreases. When a user sends an encrypted query [34] to the anonymizer server, it executes the request and seeks the necessary results from the local log (L), point of interest (POI,), cloaked regions (CRs) and the road network G), if it is identified, and then returns the encrypted results to the user; otherwise, it sends the CRs to the LBS server for the latest data.

Algorithm 2 Query Processing by Anonymization Server

```
Input: Present location and destination of the query sender, CR selected by the querier, K and $K_f$ (user number for location anonymity), query information
Output: $K_f$ member, K-anonymous users in a minimum CR, POI
Procedure:
Determine the minimum distance ($K$, $K_F$, $K_{NF}$, $K[i]$ = null);
if $|K| < K_F + K_{NF} - 1$
then return 0
$e \leftarrow 0$ // e numerical constant having value 2.71828
while $e = /|K|$
$e \leftarrow |K|$
$K[i] = e$ ;
$i++$;
if ( $i < K - 2$);
continuous;
$Qery_{dec}$ = dec($query_{act}$);
else end if;
end while;
if(regularly measure clock regions(CRs) of dist(q, $K[i]$) and arrange CRs in ascending order (i.e., from lower to the highest))
return $K[i]$; \\ $i$th position from 1 to $K$
```

C. LBS SERVER

The LBS server is the server that holds all the information and services that should be provided to the user in the LBS system. If any POI is not available on the LBS server, it may communicate by sending external route requests to the online route API containing the road network (G). In this case, the LBS returns the results to the anonymizer server, which gives a response to the querier. When the POI of the querier is not found at the anonymizer server, then the anonymizer server sends an identified CR to the LBS server. At that point, the LBS server checks for the POI, and if it is not available in the LBS server, then, it will obtain the POI from an online API, and returns to the anonymizer server. The anonymizer server sends a decrypted query to the querier. According to a given scenario, the user sends the encrypted query using encryption [34] to the anonymizer server after selecting the fixed users (Kf), as shown in Algorithm 1, to create dummies. The anonymizer server generates CRs and checks points of interests (POI), the route log (L), and road network (G), identifying the user requirements. If the POI is not found in the anonymizer server, then, the query is transferred to the LBS server, which gives a response to the anonymizer server using an online API for the POI, as shown in Algorithm 3.

Lemma: *Privacy Assurance in Location-Based Service (LBS) Systems with fixed K-anonymization and Dummy Positions*

Let U be the set of users in a Location-Based Service (LBS) system, where each user ui is associated with a real

Algorithm 3 LBS server processing

```
Input:Message with a cloaked region
Output:desired results POI
Procedure:
  1. if (POI=CR) //Check CR for this POI from the LBS server;
  2. return result to anonymizer server;
  3. else if(POI!=CR)
  4. contact online API for POI; // using Online API to LBS server
  5. else if(POI=API)
  6. return result to LBS server;
  7. else
  8. no result found
```

geographical location *Lri*. In the presence of an anonymizer server and the integration of dummy positions, the following lemma establishes a mathematical foundation for privacy analysis within the LBS system.

1) ANONYMIZER SERVER (AS) FUNCTION

Let *AS* represent the anonymizer server function. For each user *ui*, the anonymizer server function$AS(ui)$ transforms the real location *Lri* into an anonymized location *Lai*, such as

$$AS : Lri \mapsto Lai \tag{1}$$

2) DUMMY POSITION FUNCTION

Define *DP* as the dummy position function. For each user *ui*, $DP(ui)$ generates a set of dummy positions *Dui* in the vicinity of the real location *Lri*, representing potential user locations, i.e., $DP{:}Lri \mapsto Dui$.

3) PRIVACY METRIC

Let *P* be a privacy metric that quantifies the level of privacy achieved. It can be formulated as a function of the divergence between the real locations and their corresponding anonymized or dummy positions, expressed as Privacy Score in equation 2 as follows:

$$P : \{Lri, Lai, Dui\} \mapsto PrivacyScore \tag{2}$$

4) PRIVACY ASSURANCE LEMMA

The combined effect of the anonymizer server and dummy positions provides privacy assurance by minimizing the information leakage about real user locations. The privacy assurance lemma is mathematically expressed in equation 3 as follows:

$$P(\{Lri, Lai, Dui\}) \leq \epsilon, \tag{3}$$

where ϵ is a predefined privacy threshold, and the privacy metric *P* ensures that the divergence between the real and transformed or dummy locations remains within an acceptable range.

This lemma establishes a formal framework for privacy analysis in LBS systems, emphasizing the role of the anonymizer server and dummy positions in safeguarding user location information. The privacy metric *P* quantifies the effectiveness of these mechanisms, providing a measurable foundation for assessing the privacy guarantees offered by the integrated approach.

V. EXPERIMENTS AND RESULTS

To determine the effectiveness of the proposed ADPA model, extensive simulations were performed. The simulation scenario in this portion was defined, and then the outcomes of the simulations were interpreted. The results were also compared with the fixed K-anonymization (K_f) [26] and active fixed K-anonymization (A-K_f) [27]. The simulation tool, Riverbed Modeler [35], was used to execute the simulations. The output of the proposed model was authenticated using different privacy metrics. Thus, complicated network topologies were designed, and the intensity of transmitting or receiving messages was simulated. The French highway network was used for this simulation, as illustrated in Figure. 4. Throughout the simulation, specific nodes that accurately represented the position of the user to determine the closest route to an ATM system, restaurants, etc., were picked. To retain the personal information of the user along with the produced dummy places, various queries were transferred to the location server via a wireless network when they were posted to the LBS framework, and when it was recognized, the outcome of the query was evaluated by setting a week.

Scenario 1:

There are 40 users distributed in area A in a grid having a width (W) and height (H), where changing the number of clients can define the cloaked region for them.

Scenario 2:

Out of 39 users, the querier can fix other clients. By fixing a different number of client's every time, the number of objects available for fixed clients can be checked.

Scenario:

The effects of knowing how the number of objects can be related to or available in the cloaked region can also be explained.

We assume a region R of 200m x 200m. The Ethernet and bus topology were formulated in this simulation. Figures 5 (a), (b) and (c) present the configuration of each node and data carrier bus.

In the experiments, the size of the CR over different scenarios and the number of queried objects concerning changes in the fixed clients (Kf) using the cloaked region were observed, in which a single grid cell was considered to have a length of 1 meter (m), and time in seconds (t). The size of the CR determined the privacy of users concerning the shielding of all privacy aspects. The most significant part of the ADPA was maintaining user privacy to efficiently guard user personal, temporal, and spatial information simultaneously. The correlation between the size of the cloaked region (CR) and the time of the fixed anonymous clients (kf) is shown in Figure. 6.

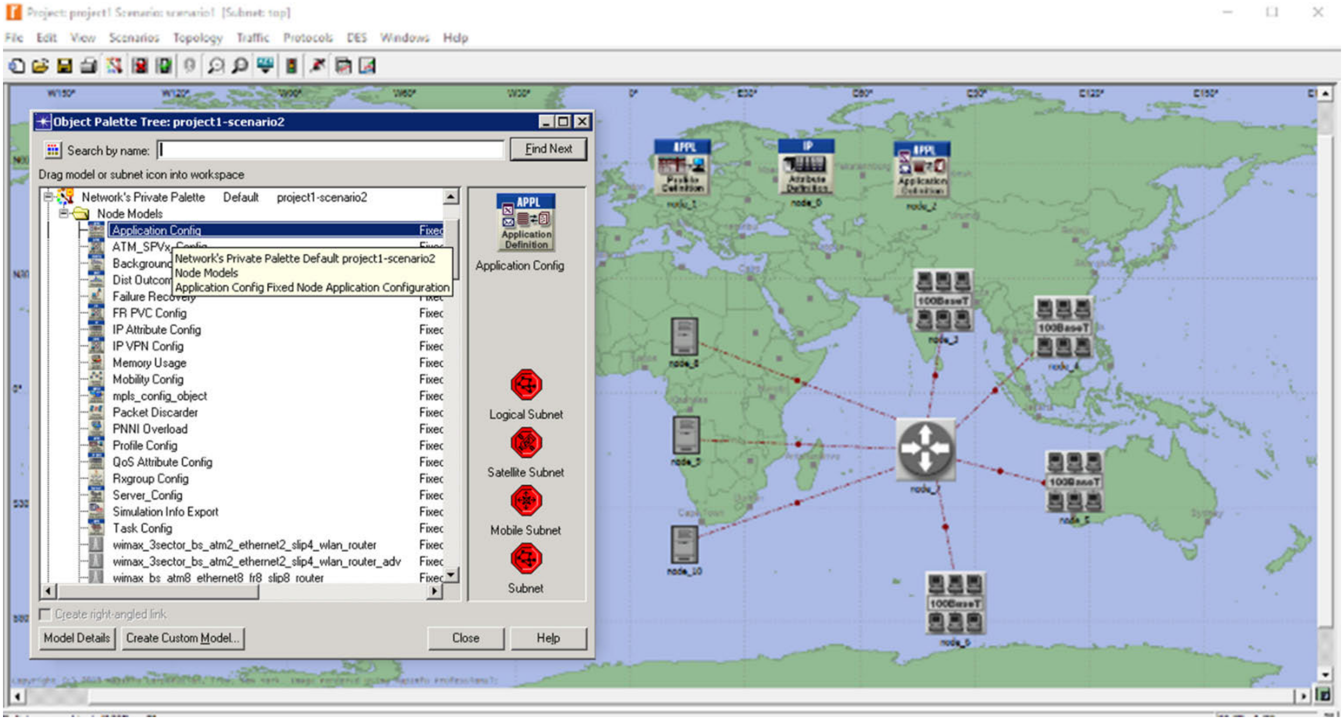

Project: project1 Scenario: scenario1 [Subnet: top]
File Edit View Scenarios Topology Traffic Protocols DES Windows Help
Object Palette Tree: project1-scenario2
Search by name:
Find Next
Drag model or subnet icon into workspace
Network's Private Palette Default project1-scenario2
Node Models
Application Config Fixed
ATM_SPVx_Config
Background
Dist Outcom
Failure Recovery
FR PVC Config Fixed
IP Attribute Config Fixed
IP VPN Config Fixed
Memory Usage Fixed
Mobility Config Fixed
mpls_config_object Fixed
Packet Discarder Fixed
PNNI Overload Fixed
Profile Config Fixed
QoS Attribute Config Fixed
Rxgroup Config Fixed
Server_Config Fixed
Simulation Info Export Fixed
Task Config Fixed
wimax_3sector_bs_atm2_ethernet2_slip4_wlan_router Fixed
wimax_3sector_bs_atm2_ethernet2_slip4_wlan_router_adv Fixed
wimax_bs_atm8_ethernet8_fr8_slip8_router Fixed
Network's Private Palette Default project1-scenario2
Node Models
Application Config Fixed Node Application Configuration
APPL
Application Definition
Application Config
Logical Subnet
Satellite Subnet
Mobile Subnet
Subnet
Create right-angled link
Model Details
Create Custom Model...
Close
Help
APPL
IP
100BaseT
node_0
node_1
node_2
node_3
node_4
node_5
node_6
node_7
node_8
node_9
node_10

FIGURE 4. Implementation of the proposed model in Riverbed Opnet.

In the fixed k-method, Kf = 2 from K= 5. The adaptive fixed k-anonymization (A-kf) generated a CR for the querier when Cn=10 and Kf=2, whereas the ADPA method generated a CR for the querier when Kf=5 and Cn=10. This signified that the size of the CR in the ADPA rather than in the A-kf method decreased gradually by changing the Kf clients.

To evaluate the cloaked region with different time intervals (sec) over the scale of CRs, which shifted with Cn, it was concluded that the scale of the CRs shifted with the Cn, where Cn=40 in the proposed ADPA, as shown in Figure. 7. At t=0 to t=2, the size of the CR was smaller compared to A-kf, and from t=4, the size of the CR began to increase due to an increase in the number of clients (Cn). Figure 9 depicts the size of the CR following the modification in KF (Fixed Anonymous Clients).

In the ADPA method, the size of the CR at t=1 began to decrease, and at t=4 to t=7, the size of the CR became smaller compared to the A-kf method. This implied that in the ADPA method when the fixed clients (kf) were modified, the size of the CR decreased. The size of the CR with regard to a change in the velocity is shown in Figure. 9. The size of the CR was proportional to the velocity of the clients. The size of the CR decreases as the client velocity decreases. At V=5, the size of the CR in the proposed ADPA was smaller than the A-kf method. The size of the CR when V=2 was smaller when V=3 or V=4. The number of queried objects having an expected number of objects and time intervals indicated that the search region for the querier increased with fixed anonymous clients (kf) presented in Figure 10. In the ADPA, the size of the CR was larger than the size of the CR in the A-kf method, which showed a wide search region for the querier, indicating that the size of the CR increased as the Kf increased. LBS clients are also concerned with the size of the CR with different numbers of objects. Figure 11 shows that when the objects = 1000, the size of the CR produced in the ADPA method was comparatively smaller than with the fixed-k and adoptive fixed methods. Similarly, when the objects=2000 and 4000, the CR's size decreased compared to the A-kf and fixed k-methods, thereby indicating that the size of the CR decreased as the client numbers increased.

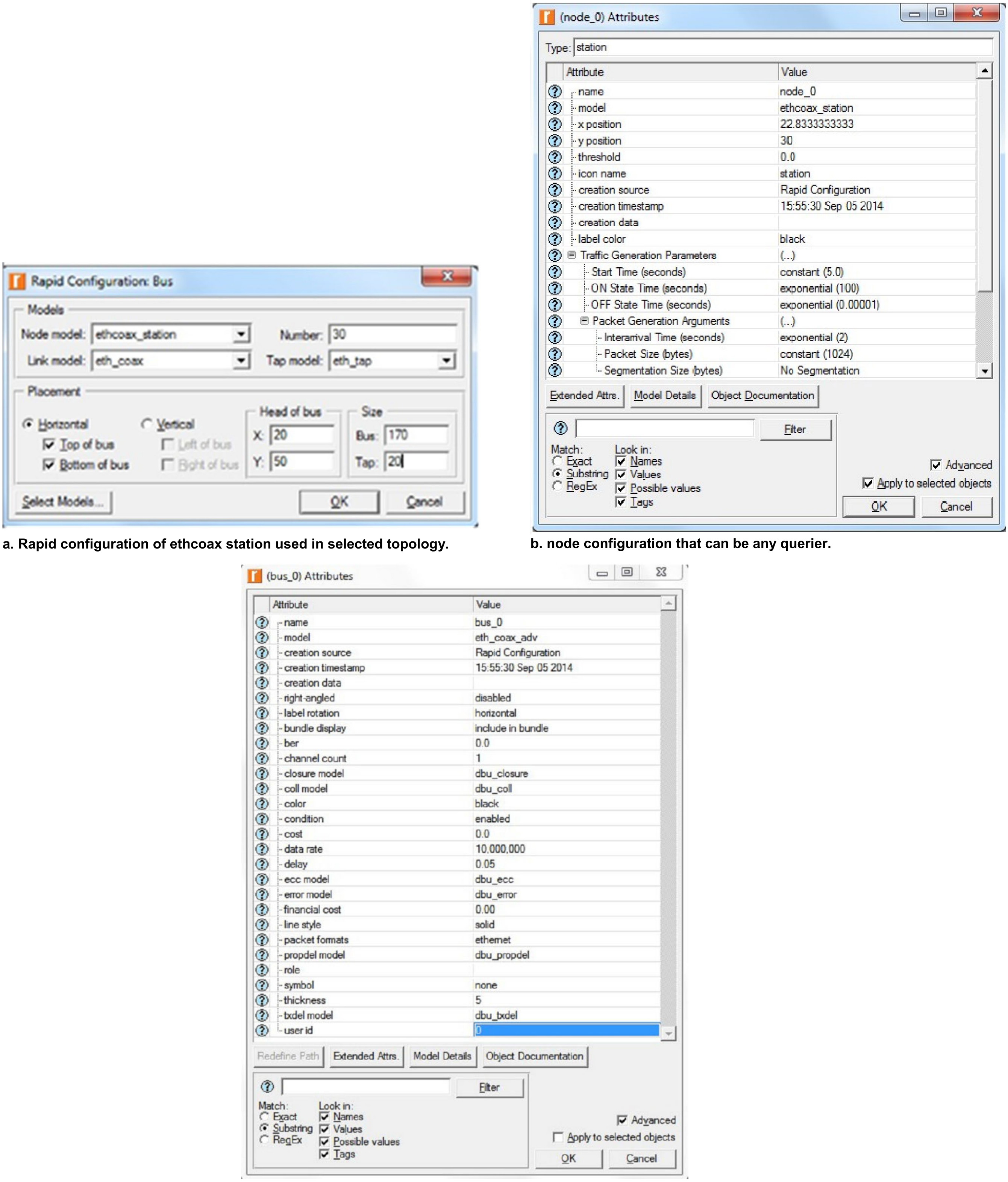
ANONYMOUS ENTROPY

According to [38], anonymous entropy is a primary parameter to measure privacy in LBS systems. It can quantify the uncertainty of the desired POI from set of locations. Therefore, considering the anonymity factor in our proposed PDAS model, we use anonymous entropy measurement to determine the extent of anonymity.

Assuming a set G of k number of locations $\{(x_0,\ y_0),\ (x_1,\ y_1),(x_2,\ y_2),.\ .\ .(x_{k-1},\ y_{k-1})\}$ containing the POI probability as q_i at location (x_i,y_i) whereas the neighbour probability is P_i. The anonymous entropy can be defined as:

$$E = \sum\nolimits_{i=0}^{k-1} pilog2pi \qquad (4)$$

To determine the privacy level, we have evaluated the anonymous entropy and compared the proposed PDAS with three existing different dummy position-based approaches, including E-DLS algorithm [35], random dummy position-based



Rapid Configuration: Bus

Models

Node model: ethcoax_station

Number: 30

Link model: eth_coax

Tap model: eth_tap

Placement

● Horizontal ○ Vertical

☑ Top of bus □ Left of bus

☑ Bottom of bus □ Right of bus

Head of bus X: 20 Y: 50

Size Bus: 170 Tap: 20

a. Rapid configuration of ethcoax station used in selected topology.

(node_0) Attributes

Type: station

Attribute	Value
name	node_0
model	ethcoax_station
x position	22.8333333333
y position	30
threshold	0.0
icon name	station
creation source	Rapid Configuration
creation timestamp	15:55:30 Sep 05 2014
creation data	
label color	black
⊟ Traffic Generation Parameters	(...)
Start Time (seconds)	constant (5.0)
ON State Time (seconds)	exponential (100)
OFF State Time (seconds)	exponential (0.00001)
⊟ Packet Generation Arguments	(...)
Interarrival Time (seconds)	exponential (2)
Packet Size (bytes)	constant (1024)
Segmentation Size (bytes)	No Segmentation

b. node configuration that can be any querier.

(bus_0) Attributes

Attribute	Value
name	bus_0
model	eth_coax_adv
creation source	Rapid Configuration
creation timestamp	15:55:30 Sep 05 2014
creation data	
right-angled	disabled
label rotation	horizontal
bundle display	include in bundle
ber	0.0
channel count	1
closure model	dbu_closure
coll model	dbu_coll
color	black
condition	enabled
cost	0.0
data rate	10,000,000
delay	0.05
ecc model	dbu_ecc
error model	dbu_error
financial cost	0.00
line style	solid
packet formats	ethernet
propdel model	dbu_propdel
role	
symbol	none
thickness	5
txdel model	dbu_txdel
user id	0

c. Attributes of used bus topology.

FIGURE 5. (a), (b), and (c) selected configurations of each node and topology used during implementation.

algorithm, Dest-ex method [36], and HBLP [37]. In Figure. 12, we noticed that ADPA attained the maximum entropy level and reached up to 3.68 when the number of dummy positions (K) is 10.

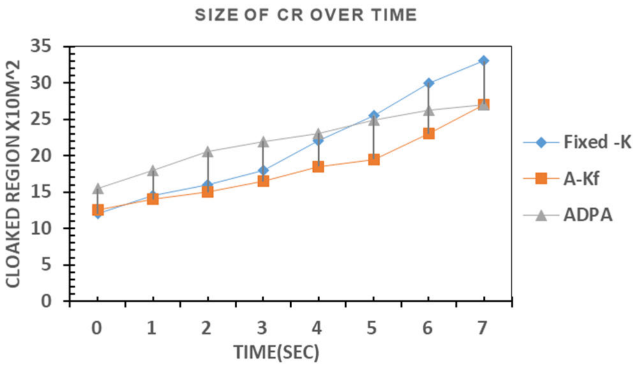


FIGURE 6. Size of CR over time.

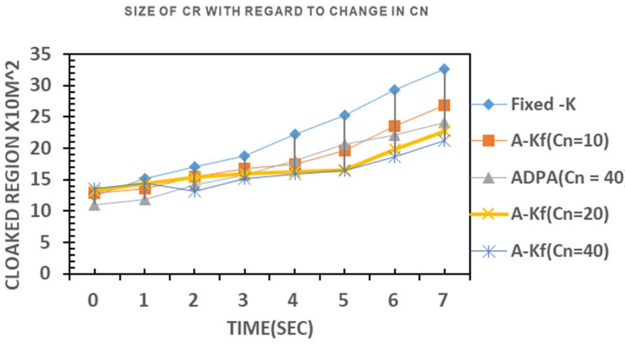


FIGURE 7. Size of CRs w.r.t modification in C_N.

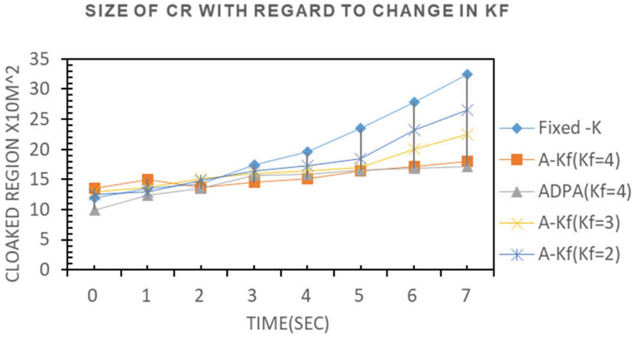


FIGURE 8. Size of CR with modification in Kf.

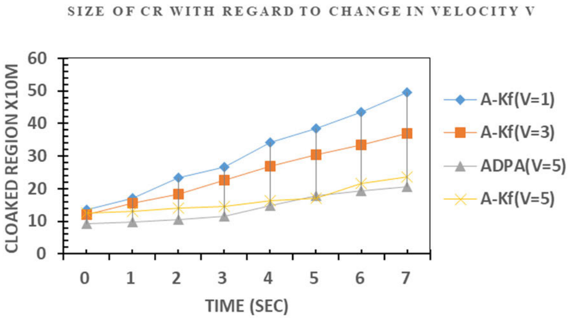


FIGURE 9. Size of CR w.r.t change in velocity.

Since anonymous entropy in E-DLS and Dest-ex is smaller than the proposed ADPA method because existing methods select the dummy positions according to the service request probability that can be filtered out using accessory knowledge. Similarly, the random dummy position algorithm also chooses the dummy locations randomly, resulting in the lowest anonymous entropy.

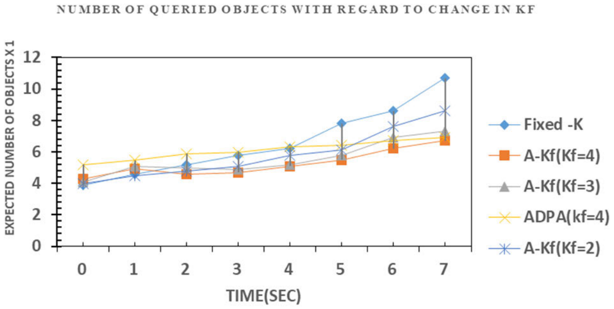


FIGURE 10. Number of queried objects w.r.t change in Kf.

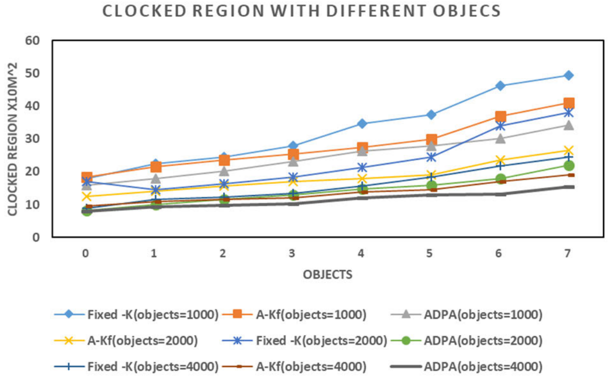


FIGURE 11. Size of the CR w.r.t changes in LBS clients.

The results show the size of the CR using the ADPA approach was 15 percent larger in contrast to the A-Kf method. By increasing the time factor in this evaluation to t=4, it was determined that the proposed solution achieved a CR value of up to 23%, but on the other hand, it was also observed that the existing solution could achieve a CR value of up to 18%, which indicated a lower CR size. By shifting the time factor to t=7, it was observed that the suggested approach achieved a maximum value of 27%, as shown in Figure. 7. The size of the CR also varied with changes to the number of clients (Cn) over different periods. The size of the CR at Cn=40 was different between the A-kf method and the ADPA method, as demonstrated in Figure. 8. At the beginning, the size of the CR in the ADPA method was lower, but as the time increased to t=4, it was at 18%, in contrast with the A-Kf method, where it was observed that the CR value was 15%. Similarly, at t=7, the size of the CR in the ADPA method achieved an optimal value of 24%. Modifications to the fixed anonymous clients (Kf) can also alter the size of the CR. Different Kf clients can generate different CR sizes. At Kf=4, the CR size in the ADPA method was 10% as compared to the A-kf method, which was 13%. The size of the CR created by the ADPA method was smaller compared

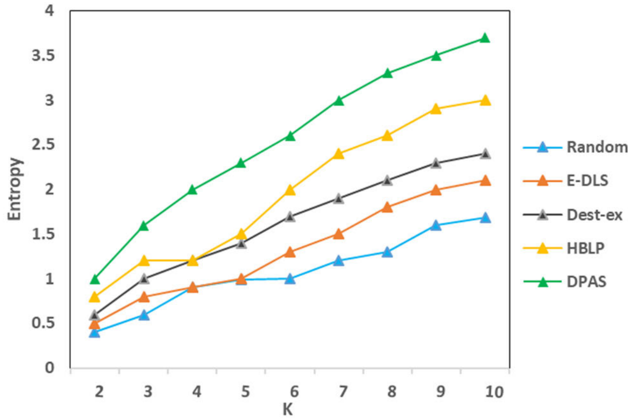


FIGURE 12. Anonymous entropy in dummy position based methods.

to the A-Kf method, as shown in Figure. 9. As the time was changed to t=4, the size of the CR with the ADPA method decreased and was lower than that obtained with the A-Kf method, which was 16% in contrast to 14% in the existing solution. Furthermore, at t=7, the size of the CR with the proposed ADPA method was lower than with the A-Kf method, reaching 17% without sacrificing user privacy. Changing the velocity of clients can also alter the CR size, as depicted in Figure. 10. The size of the CR decreased gradually with increasing velocity. At V=5, the size of the CR with the proposed technique was different from the existing technique. At t=4, the size of the CR with the ADPA technique was 15%, which was lower than that of the existing technique, which was 16%. By increasing the time in this evaluation, it was found that the size of the CR in the suggested methodology decreased to 20%, while the A-Kf method achieved a CR size of 23%. The number of queried objects often varied with changes to the Kf. The proposed technique beat the fixed-k, and A-Kf approaches to achieve a greater CR at Kf=4, as shown in Figure. 11. At t=4, the ADPA method had 6% of the queried objects relative to the A-Kf method, which had 5%. The suggested methodology became more effective over time to achieve an optimum value of 7%. The size of the CR about changes in the LBS clients is shown in Figure. 12. The size of the CR varied with different numbers of clients. The CR created by the ADPA method was smaller compared to the fixed-k and A-Kf methods. The size of the CR using the ADPA technique was smaller when the number of objects was 1000, 20000, and 4000. When the objects=1000, the size of the CR with the proposed technique was 16% compared to 18% in the previous strategies. Meanwhile, at t=4 and having objects=2000, the size of the CR with the ADPA method was 14% compared to 18% and 21% in the previous strategies. Furthermore, at t=7 and having objects=4000, the proposed technique outplayed the fixed-K and A-Kf methods.

The suggested approach ADPA comprises an anonymizer server and LBS server processing. The distribution of dummies in the grid partition prevents an attacker from knowing which one is the actual user. The anonymizer server provides the user with numerous, effective services. For example, if the user wants to know the route log (L), road network (G), or point of interest (POI), then the anonymizer server provides all these services to users without interacting with the LBS server, thereby increasing the efficiency of the proposed technique. The AS not only provides all these services, but also identifies the queriers' cloaked regions (CRs) to protect their privacy. The AS only interacts with the LBS server when the required POI is not available in the AS, for which the AS sends the user requests along with the identified cloaked region to achieve the POI. The LBS server provides an AS with the POI, which is returned to the querier. All querier requests to the AS are authenticated and temporally protected so that no hacker will be able to destroy the details of users, thereby proving that users are protected when using the LBS. Finally, the ADPA is recommended as the best solution for achieving privacy while a user is interacting in the LBS system because CRs and dummies are implemented to protect users' privacy. The decrease in the size of the CR does not mean that user privacy has been compromised. Privacy (spatial, temporal, personal) is provided to users even within these CRs.

VI. CONCLUSION

Location-based systems have shown immense advantages for individuals and communities, and the growing disclosure of user details poses major privacy issues. In this research, the preservation of the privacy of users while interacting with LBS system was studied. To protect users' spatial, personal, and temporal information during interactions with an LBS system, we propose a dummy position-based anonymizer server, which is an enhancement of the active fixed K-anonymization (A-Kf) method that shields all these privacy aspects. However, the suggested approach ADPA used dummy positions and an encryption mechanism to enhance the efficiency of the model by raising the service speed and computing intensity of the model. The cloaked regions (CRs) provided by the anonymizer server made the credentials of the user more authenticated and protected by rendering them inaccessible to intruders, who might use them for wrongful purposes. Extensive simulations were performed to analyse the performance of the model. A comparison with the A-K_f and K_f methods revealed that the ADPA technique outperformed the existing method and ensure that the users' information could not be tampered with. Thus, the proposed approach can be used to ensure the privacy of LBS users. In future, the privacy level can be enhanced even more by upgrading the proposed solution.

REFERENCES

[1] S. Stefan, M. Neun, and A. Edwardes, "Foundations of location based services," in *CartouCHe* (Lecture Notes on LBS), vol. 272, 1st ed. Zurich, Switzerland: University of Zurich, 2006, ch. 1, pp. 1–28.

[2] M. K. Tefera and X. Yang, "A game-theoretic framework to preserve location information privacy in location-based service applications," *Sensors*, vol. 19, no. 7, p. 1581, Apr. 2019.

[3] Y. Li and M. L. Yiu, "Route-saver: Leveraging route APIs for accurate and efficient query processing at location-based services," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 1, pp. 235–249, Jan. 2015.

[4] M. Xin, M. Lu, and W. Li, "An adaptive collaboration evaluation model and its algorithm oriented to multi-domain location-based services," *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2798–2807, Apr. 2015.

[5] D. Chen, P. Zhang, C. Hu, H. Wang, S. Wu, and N. Xing, "PAPERS: Private and precise range search for location based services," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 7347–7352.

[6] G. Zhuo, Q. Jia, L. Guo, M. Li, and Y. Fang, "Privacy-preserving verifiable proximity test for location-based services," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[7] X. Chen, A. Mizera, and J. Pang, "Activity tracking: A new attack on location privacy," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Florence, Italy, Sep. 2015, pp. 22–30.

[8] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Kowloon, Hong Kong, Apr. 2015, pp. 1017–1025.

[9] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 972–980.

[10] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Pers. Ubiquitous Comput.*, vol. 18, no. 1, pp. 163–175, Jan. 2014.

[11] B. S. Aniqa, W. Zainab, and M. U. Ashraf, "Privacy provision for tip attributes in NTTP based LBS systems," *Int. J. Adv. Res. Comput. Sci.*, vol. 10, no. 2, pp. 84–90, 2019.

[12] D. Yang, X. Fang, and G. Xue, "Truthful incentive mechanisms for k-anonymity location privacy," in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013, pp. 2994–3002.

[13] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *Proc. IEEE Conf. Comput. Commun.*, Vancouver, BC, Canada, Apr. /May 2014, pp. 754–762.

[14] X. Zhu, H. Chi, B. Niu, W. Zhang, Z. Li, and H. Li, "MobiCache: When k-anonymity meets cache," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Atlanta, GA, USA, Dec. 2013, pp. 820–825.

[15] J. Shao, R. Lu, and X. Lin, "FINE: A fine-grained privacy-preserving location-based service framework for mobile devices," in *Proc. IEEE Conf. Comput. Commun.*, Toronto, ON, Canada, Apr. 2014, pp. 244–252.

[16] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. Mobile Syst., Appl. Services*, San Francisco, CA, USA, May 2003, pp. 31–42.

[17] B. Claudio, X. S. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in *Proc. 2nd VLDB Workshop Secure Data Manag. SDM*, Trondheim, Norway, 2005, pp. 185–199.

[18] R. Everett and T. W. Valente, "A history of information theory in communication research," in *Between Communication and Information*. Evanston, IL, USA: Routledge, 2017, pp. 35–56.

[19] K. Hyeong, Y. K. Kim, and J. W. Chang, "A grid-based cloaking area creation scheme for continuous LBS queries in distributed systems," *JoC*, vol. 4, no. 1, pp. 23–30, 2013.

[20] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, Chicago, IL, USA, 2009, pp. 348–357.

[21] D. Song, J. Sim, K. Park, and M. Song, "A privacy-preserving continuous location monitoring system for location-based services," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, Aug. 2015, Art. no. 815613.

[22] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in *Proc. 15th Annu. ACM Int. Symp. Adv. Geographic Inf. Syst.*, Seattle, WA, USA, Nov. 2007, pp. 1–8.

[23] V. K. Yadav, S. Verma, and S. Venkatesan, "Linkable privacy-preserving scheme for location-based services," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 7998–8012, Jul. 2022.

[24] L. Dan, H. Li, V. Anand, V. Chang, G. Sun, and H. F. Yu, "Using location-labeling for privacy protection in location-based services," in *Proc. IoTBD*, Pegue, Czech Republic, 2016, pp. 299–306.

[25] B. Niu, X. Zhu, W. Li, H. Li, Y. Wang, and Z. Lu, "A personalized two-tier cloaking scheme for privacy-aware location-based services," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Anaheim, CA, USA, Feb. 2015, pp. 94–98.

[26] D. Song and K. Park, "A privacy-preserving location-based system for continuous spatial queries," *Mobile Inf. Syst.*, vol. 2016, pp. 1–9, Oct. 2016.

[27] S. Bennati and A. Kovacevic, "Modelling imperfect knowledge via location semantics for realistic privacy risks estimation in trajectory data," 2020, *arXiv:2011.09218*.

[28] R. Gupta and U. P. Rao, "VIC-PRO: Vicinity protection by concealing location coordinates using geometrical transformations in location based services," *Wireless Pers. Commun.*, vol. 107, no. 2, pp. 1041–1059, Jul. 2019.

[29] R. Gupta and U. P. Rao, "A hybrid location privacy solution for mobile LBS," *Mobile Inf. Syst.*, vol. 2017, pp. 1–11, Jun. 2017.

[30] A. Moro and B. Garbinato, "ResPred: A privacy preserving location prediction system ensuring location-based service utility," in *Proc. 4th Int. Conf. Geographical Inf. Syst. Theory, Appl. Manage.*, 2018, pp. 107–118.

[31] G. Kaur, "Implementation of secure authentication mechanism for LBS using best encryption technique on the bases of performance analysis of cryptographic algorithms," *Int. J. Secur., Privacy Trust Manage.*, vol. 1, no. 6, pp. 11–27, Dec. 2012.

[32] X. Xu, L. Xiong, V. Sunderam, and Y. Xiao, "A Markov chain based pruning method for predictive range queries," in *Proc. 24th ACM SIGSPATIAL Int. Conf. Adv. Geographic Inf. Syst.*, Burlingame, CA, USA, Oct. 2016, pp. 1–10.

[33] G. Sun, S. Cai, H. Yu, S. Maharjan, V. Chang, X. Du, and M. Guizani, "Location privacy preservation for mobile users in location-based services," *IEEE Access*, vol. 7, pp. 87425–87438, 2019.

[34] R. Jiang, R. Lu, and K.-K.-R. Choo, "Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data," *Future Gener. Comput. Syst.*, vol. 78, pp. 392–401, Jan. 2018.

[35] *Riverbed*. Accessed: Mar. 2023. [Online]. Available: https://www.riverbed.com/sg/

[36] T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, "Dummy-based user location anonymization under real-world constraints," *IEEE Access*, vol. 4, pp. 673–687, 2016.

[37] K. Alsubhi, M. U. Ashraf, and I. Ilyas, "HBLP: A privacy protection framework for TIP attributes in NTTP-based LBS systems," *IEEE Access*, vol. 8, pp. 67718–67734, 2020.

[38] M. U. Ashraf, K. M. Jamb, R. Qayyum, H. Ejaz, and I. Ilyas, "IDP: A privacy provisioning framework for TIP attributes in trusted third party-based location-based services systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 7, pp. 604–617, 2020.

M. USMAN ASHRAF received the Ph.D. degree in computer science from King Abdulaziz University, Saudi Arabia, in 2018. He is an Associate Professor and the Head of the Department of Computer Science, GC Women University, Sialkot, Pakistan. He was a HPC Scientist with the HPC Centre, King Abdulaziz University. His research on exascale computing systems, high performance computing (HPC) systems, parallel computing, HPC for deep learning, and location based services systems, which have appeared in IEEE Access, *IET Software*, *International Journal of Advanced Research in Computer Science*, *International Journal of Advanced Computer Science and Applications*, *International Journal of Information Technology and Computer Science*, and *International Journal of Computer Science and Security*; and several international IEEE/ACM/Springer conferences.

KHALID ALI ALMARHABI received the B.Sc. degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2009, the M.Sc. degree in information technology from the Queensland University of Technology, Brisbane, Australia, in 2014, and the Ph.D. degree in computer science from King Abdulaziz University and the Queensland University of Technology. He is an Associate Professor with the Computer Science Department, College of Computing in Al-Qunfudah, Umm Al-Qura University, Saudi Arabia. His research interests include information security, BYODs research, access control policies, information system management, and cloud computing.