IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 8, 2020, accepted March 27, 2020, date of publication April 3, 2020, date of current version April 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2985659

HBLP: A Privacy Protection Framework for TIP Attributes in NTTP-Based LBS Systems

KHALID ALSUBHI[1], **M. USMAN ASHRAF**[2], **AND IQRA ILYAS**[3]
[1]Department of Computer Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2]Department of Computer Science, University of Management and Technology at Sialkot, Sialkot 53310, Pakistan
[3]Department of Computer Science, GC Women University, Sialkot 51310, Pakistan

Corresponding author: M. Usman Ashraf (usman.ashraf@skt.umt.edu.pk)

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. (D-648-611-1441). The authors, therefore, acknowledge with thanks DSR technical and financial support.

ABSTRACT Nowadays, location-based services are being widely popularized due to their massive usage in current and emerging technologies. These services are based on searching out areas of interest which are likely to be accessed by users. Despite helping users worldwide, Location Based Services (LBSs) Systems endanger users' privacy because a user must provide personal information in order to use the services. Users thus become easy prey for assailants to access their social and personal lives. This problem is a giant issue for contemporary technologies because they are increasingly being used with the passage of time. Many existing solutions have attempted to resolve the challenges, but they face some serious dilemmas regarding the preservation of privacy. In order to address the privacy challenges in LBS systems, in this paper we have introduced a new Hierarchy Based Location Privacy (HBLP) model that protects the user's privacy, including the user's query time and identity and location information. The proposed model protects the user's privacy by using pseudo identity exchange, an aggregation protocol, and the concepts of Forest User (FU), Tree User (TU), and Child Users (CU) with k-anonymity and t-closeness, which is a reasonable combination for privacy provision for a user's query time, identity, and location. In order to evaluate the privacy protection level, we implemented the HBLP model in a Riverbed (Opnet) simulation and compared the results with existing state-of-the-art privacy-provisioning methods. The results showed that HBLP protected all the privacy attributes when a user interacts with an LBS system.

INDEX TERMS Location based services, user privacy, NTTP, point of interest.

I. INTRODUCTION

Today, internet technology is speedily expanding, and people can explore areas and associate and make friends with others who are geographically far away [1]. When accessing individuals or areas or when retrieving information based upon Location Based Services (LBSs), protecting one's own location information is extremely important LBSs are beneficial in that they allow the discovery of multiple places like [2] educational organizations, hotels, parks, shopping malls, and nonprofit organizations, and also delivers several types of services like publicizing services, vending services, and transportation services, etc. However, they also reveal a user's location, identity, and temporal information, and we have to secure these three attributes from unsanctioned access. Some key types of LBS are used nowadays [3], such as location aware services, location tracking services, and map navigation services.

In spite of providing great convenience, like discovering tourism locations, enjoying online games with anonymous people in faraway locations, and social networking, companies like Instagram, Facebook, and Twitter collect users' topics of interest by retaining their critical information and personal data [4]. For example, Google Maps uses the Global Positioning System (GPS), through which everyone can detect their location from anywhere, but users' private information can be used by unauthorized persons without a user being informed of what their information is being used for and also who is using it [5]. All these services collect our private information, and due to this, our privacy is compromised. This privacy problem means that sensitive information given to an LBS is not fully safe because it can still be damaged by attackers [6], [7]. There may be occasions where we can provide a dummy

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

position and identity for the purpose of protecting our privacy, but if a consumer orders fast food from a restaurant, for example, then they will have to provide their actual location, and similarly, if someone wants to use Amazon, they must provide accurate information to create an account. These scenarios require users to provide real information, and there arises the problem of protecting users' sensitive information.

LBSs utilize two main methods to try to ensure privacy; i.e., by using Trusted Third Party (TTP) and Non-Trusted Third Party (NTTP) protocols, where TTP means there is a node or server owned by some third party which is assisting the LBS to guard its users [8]. According to emerging Block chain technology, the TTP based model can be review in [51]. LBS using TTP depends fully on the third party, but it is not always possible to determine whether the third party is always trustworthy in protecting the private information of the user. There are several techniques which deal with privacy protection in the context of TTP in LBS, and the existing literature provides a huge variety of approaches to solve the privacy problem [5], [9].

However, all approaches have some serious drawbacks regarding the privacy and security of LBS-users, and it is hard to obtain a perfect approach. Due to these reasons, NTTP protocols are being increasingly focused on for preserving privacy, which is beneficial because no trusted third party tool is used while processing query in LBS system. There are many proposed approaches for using NTTP in LBS, and these are discussed in detail in Section III. These techniques help an LBS to protect a user's personal information from being accessed by unauthorized persons. The primary problem to solve in the current study is to protect three attributes, which are users' identity, temporal information, and spatial information, and LBS privacy is mainly concerned with these three attributes. Because inadequate privacy can lead to problems like misusing or attacking a user's personal information, this is a very serious issue for users, and if users lose their trust in an LBS, this would have serious consequences for its future. So in order for users to have a high satisfaction level in an LBS, we need to maintain their confidence in their privacy [10] with regard to the users' identity and temporal and spatial information by using NTTP.

The rest of this paper is organized as follows. Section I provides the introduction of the topic, and then we specify the motivations for the research. Section II encompasses a detailed view of the goals of the research, and Section III provides a review of the literature with details regarding the background and related research. Section IV consists of the proposed model description, flowchart, algorithm, and architecture of the proposed approach. Section V provides the details of the experiment and the results, as well as experiments related to implementing the proposed approach, and results are described. Section VI provides a discussion of the research and the relevant details.

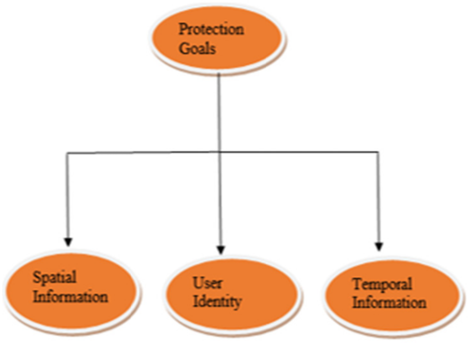


FIGURE 1. Three attributes of users.

II. PROTECTION GOALS

This research work addresses the most vulnerable LBS attributes with regard to user privacy, which are Time, Identity, and Position (TIP), and the study's goal is to provide a way to protect these three attributes. Three fundamental privacy attributes mentioned in figure 1 are the most sensitive and critical for mobile user, as he does not agree to compromise their privacy.

A. SPATIAL INFORMATION

Spatial information specifies the information related to a user's geographical position when they access a Location Based Service (LBS) system to request information about a Point of Interest (PoI) [11]. It identifies the position of the user through the effect of creating a bottleneck to trace the user's exact location. A primary objective of the research is to maintain the protection of the spatial information of users, as follows.

- A user should be able to enquire about an organization of interest where they wish to visit, for example, a food court, bank, or educational institution, without unveiling their location.
- A user should be able to use an advanced navigation system such as the Global Positioning System (GPS) [12] for predicting traffic jams.
- A user may not want to publicize that they are enjoying a meetup with friends by instead appearing to be in a meeting with their boss at their workplace, just for example.

B. USER IDENTITY

User Identity is a major characteristic when dealing with geography-driven applications, as it includes very confidential information related to the user. The related need is to camouflage a user's identity when they interact with an LBS. User identity can be a name, a unique value related to the user, or a combination of central labels that uniquely identify the user. If a user makes their confidential information available to the LBS, the information may be intercepted by an unapproved entity who may be an attacker or adversary [5].

C. TEMPORAL INFORMATIO

Temporal information comprises the instants of time in which a user has interacted with or passed a request to an LBS. A Point in Time (PiT) is a sensitive factor to protect because an adversary can keep track of a user's times of use and infer information about them through it. It includes time or the PiT when the location of the user is accurate. In some cases, location information is considered to be significant if it builds a strong association with a user's temporal information [13]. For example, a user's PiT record may disclose critical time information while travelling, thereby disclosing their speed of travel and other data. Therefore, a mobile user should always beware of any of his/her data being fed into any computing system.

III. REVIEW OF LITERATURE

To address the three main areas of concern in Location Based Services (LBSs) with regard to privacy, i.e., Time, Identity, and Location, several privacy provisioning methods are proposed as presented in this section.

A. BACKGROUND

Location Based Services (LBS) today are a part of everything from control systems to smart weapons. The vision for this was created in the mid-1990s by Todd Glasey and others working inside the American Bar Associations Information Security Committee [14]. In 1993 [15], International Teletrac Systems (later PacTel Teletrac), founded in Los Angeles, California, introduced the world's first dynamic real-time stolen vehicle recovery services. As an adjunct to this, they began developing an LBS that could transmit information about location-based goods and services. Further the US Federal Communication Commission (FCC) issued rules requiring all US mobile operators to provide emergency callers with location services [16]. In 1997, Christopher Kingdon of the Ericsson corporation submitted a Location Services (LCS) plan to the joint GSM group of the European Telecommunications Standards Institute (ETSI) and the American National Standards Institute (ANSI) [17]. As a result, the LCS sub-working group was created under ANSI. This group went on to select positioning methods and to standardize Location Services (LCS), later known as LBS [18]. As a result of these efforts, in 1999 the first Digital Location Based Service (DLBS) patent was filed in the US [19]. In 2000, after approval from the world's 12 largest telecom operators, Ericsson, Motorola, and Nokia jointly formed and launched the Location Interoperability Forum Ltd (LIF), which first specified the Mobile Location Protocol (MLP) [20]. Later on, LIF was merged with the Open Mobile Association (OMA), and an LBS work group was formed within the OMA [21]. Marex.com in Miami Florida designed the world's first marine asset telemetry device for commercial sale. The device, designed by Marex and engineered by its partner firms in telecom and hardware, was capable of transmitting location data and retrieving location-based service data via both cellular- and satellite-based communication channels. The first consumer LBS-capable mobile web device was the Palm VII, released in 1999 [22]. Therefore, the first LBSs were launched in 2001 by TeliaSonera in Sweden (Friend Finder, house position, emergency call location, etc.), [23].

In term of LBS systems, the Location Privacy Protection Act of 2012 was introduced by Senator Al Franken in order to regulate the transmission and sharing of user location data in the United States [24]. After observing that users' needs were not being satisfied by Trusted Third Party (TTP) protocols, an approach to use Non-Trusted Third Party (NTTP) protocols in LBSs was proposed, but which further work and research is still required to provide sufficient privacy using this method. TTP protocols are based on the involvement of a trusted third party, which is a threat for users' privacy because third parties may actually be adversaries, resulting in the leakage of personal information. This was the main reason for moving towards NTTP protocols, because they do not fully involve a trusted third party. In the case of NTTP, a third party is not considered trustworthy by users; regardless, NTTP still preserves users' privacy better compared to TTP. NTTP is mainly focused for the future work to provide privacy in an LBS by protecting the three crucial attributes of users, which are temporal information, user identity, and spatial information [5], [25].

B. RELATED WORK

To solve the privacy issues in LBS systems, three attributes are used which are: Time, Identity, and Position (TIP). A number of solutions have been presented by different scientists, and some of them are given below. There are several privacy challenges which need to be addressed. In the Location Label-Based Approach (L2P2) [26], the LBS system consists of three key components: User Requests (USER), Pseudonym Identity Server (PIDS), and Location Provider (LP). The LP operates in accordance with the relevant regulations and agreements in an LBS system, but it does not rule out that the LP has curious and hope to deduce the user's location, preferences, and trajectory privacy. L2P2 used in Location & trajectory privacy. This scheme is based on agreements so that by following the agreements, a user's personal information is not collided and also LP. Its drawback is that the LP is honest-but-curious, so it is not fully trusted. LP can intervene privacy of user in some certain conditions if there is any opportunity.

In the Cloud-Based model [27], there are three important factors, which include an LBS provider, a group of LBS users, and a cloud server. An LP registers its users on a cloud server, and in the cloud system, a secret key is provided to an LBS user to prevent unofficial access to individual user data. The LBS user sends their confidential information to a Service Provider (SP), and then the SP uploads the encrypted information to the main (cloud) server. Further, cloud server answered to the query of the user and expires the user's credentials. In future, if user again want to connect the server, system revokes user to the network. In such way, a user's privacy is protected from malicious users. In contrast, many attackers know how to perform decryption by applying the most frequently used decryption keys, which can compromise the user's privacy.

Another cache-based data privacy provisioning model [28] saves a user's information in a cache (temporary memory), which is helpful in keeping attackers from unauthorized access because after using the data it is lost and the server does not give permission to any other entity to use the data. On other hand, the case-based model couldn't deal with server, which is not feasible if the user later queries the server to obtain the data.

A Content Concealed Bottle mechanism has also been proposed to maintain privacy in LBS systems [29], and this has three main categories, i.e., (1) a secure matching stage, (2) a Euclidean distance computation, and (3) a private point of interest (POI) retrieval stage. The user generates a vector attribute query which is compared with existing saved vectors in the database server, and the protocol of the Euclidean distance computation finds the difference between the two parameters. The secure matching stage is meant to search for the correct match of attribute vectors related to the user's query. An approach the Garbled Circuit with optimized circuit modules for this phase to ominously condense the cost of whole construction of circuits. In the third step, a Quadratic Residuosity Assumption (QRA)-based private information retrieval protocol securely fetches the needed points of interest for the user. In this model, clients are semi-honest and server, it means both follow the defined protocols but still they are eager to know each other. However, in this model, only the user knows the results of the final query, while on the other hand, the server is responsible providing the relevant results and following the protocols. In actually user hides its query and 4 server hides its database. However, as the query is encrypted thus user is concerned with accurate results and server does not know about its content. A disadvantage of this approach is that an adversary/server can easily search out the content of the query.

In the Context-Aware Privacy Protection technique [30], users are ranked according to their exact distance from a queried location; a ranking function is used, and most importantly, an LBS query is viewed as a top-k query. After receiving a query, the server processes it against a spatial database and sends a reply to the user. Location unsettled element disturbs the Query-Based Location (QBL) reorganizes data for retrieval of actual location. Anonymous routing element leathers user ID through relaying nodes routing. This is a very economical approach, but a problem is that Quality of Service (QoS) is not given as much attention in anonymous networks.

Spatial Bloom Filtering [31] is a famous method used to examine the temporal and location information of a user. This method uses an SP-based protocol and communicates directly with the user, but both entities distrust each other, and consequently, neither entity will want to expose the private information to a third party. Here, the LBS only knows the Area of Interest (AoI) of the user, but not the exact location. An issue with the bloom filtering model was that the provider can only estimate the user's distance from the central area to a certain extent, and the relative location is only exposed when the user is within a determined area. Distributing the area around the POI in a different manner may reveal the direction but conceal the distance.

Homomorphism is another method [33] that aims to manage a guaranty level that centroid has been gain in the absence of actual user's position. A strategic public key homomorphism is composed to attain location privacy. Homomorphism is a TTP-free mechanism that helps to generate a public key; the user's location can be encrypted, and information is decrypted through LBS involvement and then sent to every user involved in order to determine /assess centroid. However, a drawback of this approach is location's decryption used by the attacker to cause violation. Micro Aggregation-Based Approach [34] the big quality of this method is zero-mean Gaussian noise is added and convey directly to the LBS database server and which is difficult to search out the centroid of K upset/ unsettled user location. Due to zero-mean there is no estimation of location find out and also Gaussian noise which is created by weak illustration and high point temperature but primary issue in this method was that if user belongs to a fixed (same location for a long time) position then Gaussian noise can be repeatedly applied to getting the real location of the user.

Private Information Retrieval (PIR) [35] is another way to protect a user's location, where an LP uses a protocol for the interaction of user in efficient way and best manner. It prevents the defined method to work in real environment, where LP just answers the query of the users without care of privacy. By addressing the massive utilization of resources, PIR can be considered as one of the leading models for privacy provisioning in LBS systems. Persona [36] is another privacy provision model wherein a user generates an asymmetric key pair and shares its public key with other users to whom the sender wishes to send information. The sender defines the levels of trust for other users, and those users can be assigned a particular relationship with the sender. The user can create groups and add participants accordingly, and the user's information can be protected through encryption. Users are highly advised to choose their friends carefully, like university fellows, friends, and colleagues. There are some drawbacks to Persona, and one of these is that the LBS server decrypts all coordinates of the position, which makes it very tough for the LBS server to even work on nearest-position queries.

Obfuscation is a process of degrading the quality of information about a user's location with the aim to protect that user's privacy when using location services [37]. It is used less precision by using graph though different vertices. A disadvantage of this approach is that users and providers must share the graph modelling the space for a comprehensive approach to imprecision in location systems. Space Twist is a technique which generates an anchor (i.e., a fake point) that is used to retrieve information on the k nearest points of interest from the LP in location services. This method hides a user's real identity from k values, which makes it difficult for an adversary to trace the right person due to multiple fake points. However, due to the lack of collaboration, Space Twist is unable to achieve k-anonymity.

The Path Confusion technique [38] depends upon giving bogus locations by camouflaging a user's actual location using anonymized pseudonyms. In path confusion, user sends one or more bogus locations which are related to the actual position and protect user's privacy. The algorithm for checking the unpredictability of higher or lower privacy is:

$$\mathrm{H} = -\sum \mathrm{p_i} \log \mathrm{p_i} \tag{1}$$

In Equation (1), 'p' is the probability of a location and 'i' is the target vehicle. However, if a user is using path confusion but is still sending information affiliated to an adjacent location, they can be traced easily.

In the Silent Period approach [39], a particular interval of time converted into a silent state in order to prevent communication because of not being attacked by contender. When system's this silent mode is terminated location is upgraded to novel one but downside of this approach is, if vehicle's speed is lower than desired then silent period will go long and location will not be upgraded and will keep former which is vulnerable to attack. In the swing and swap method [40], a node can interchange its Identities with imminent and corresponding vehicle to obfuscate the attacker about vehicles but where user is on the less-crowded road or on motorway then this approach is not efficient. In another coordinate transformation technique [41], [42], the user executes some geometric options such as shifting and rotating their location before getting a service from the LBS. In order to get the original location, an inverse transformation of these functions is used. This technique uses mathematical operations such as enlarging the radius, shifting the center, increasing the radius, or applying double obfuscation (i.e., mixing shifting center with any of remainders). The disadvantage of this approach is that inverse transformation can be used to find the user's actual information of. A privacy-supported LBS server directly exchanges information with the user. The server originates notifications about the privacy level of the user, but it depends on the user whether the user will maintain these notifications or not. A downside of this method is that the user depends totally on the server, and if the server is inoperable then it can send incorrect notifications to the user, which can mislead the user about their privacy.

Leading to privacy provisioning in LBS systems, geo-indistinguishability, a conventional thought of privacy that ensures the user's actual location, while permitting estimated data normally expected to acquire a certain desired service to be released. In any case, geo-indistinctness entails that an informed adversary who definitely realizes that the mobile user is situated inside a little region N, can't improve his underlying learning and find the user with higher precision [43]. Further Geo Indistinguishably was also explored by [44] and emphasized on differential privacy which means to safeguard user's information in a worldwide manner by some mathematical clamor or noise and differential privacy intends to supply means to rise the correctness of queries from statistical databases while reduces the possibility of identifying its record and erroneous information is given to the system like if the user is in Canada but it will act as to be in America. But the issue is that user produces inessential Clamor like if he is at the lake then it's nugatory to make noise. Blind filtering [45] involves a semi-trusted party called a proxy, for the percolating of our supplementary POI audits in a blind manner. Semi server is not fully trusted that's why user is consistently prepare to face an inauspicious state. It includes a semi trusted server that's why we have to depend on it. If an SP behaves as a user, then the semi-trusted server will send information to it rather than the actual user.

A L4NE protocol [46] is a privacy protocol which describes the privacy affairs of LBS in non-discriminating testing by giving appropriate privacy and performance and it depends on a composition of functions. In this protocol, we used n-self composition of functions. Self-composition functions are as reliable as the discrete logarithm technique as long as the non-linear function is chosen carefully. This validates the L4NE protocol as being as reliable as most of the aforementioned protocols, and possibly more safe than some. Computation of self-compositions is much accelerated than power functions. The L4NE protocol does not escape information of user to anyone else. The L4NE protocol uses the capricious property of the composite function. But weakness of this method is, if the nodes who are sharing information with each other are found to be at the constant location then it will divulge or disclose their information.

Leading to privacy protection in LBS system another approach Location Labelling Based (LLB) model was introduced in [52]. LLB not deal only the single query processing but for continues query as well. In LLB, the users are labels either he/she belongs to similar or different location and then posted to the server along with query. This mechanism ensures the protection of location as well as user's identity. In contrast, authors in [49] introduced Local-Area Mobile social networks (PLAM) protocol where t-closeness and k-anonymity are used to preserve the privacy of the user's identity as well as spatial information. These techniques assist in providing satisfactory user privacy.

IV. PROPOSED MODEL (HIERARCHY BASED LOCATION PRIVACY)

In order to address the privacy challenges in a Non-Trusted Third Part (NTTP) LBS system, we have proposed a new model named the Hierarchy Based Location Privacy (HBLP) model. The primary purpose of the proposed architecture is to provide users with privacy (l-diversity, t-closeness) at an acceptable level, and improve query success rate as well as response time than earlier approaches. The proposed model comprises four fundamental components: a request aggregation protocol, a sensitive service category / an ordinary service category, a Location Provider (LP) for requests for services and to get responses. There can be two possibilities,

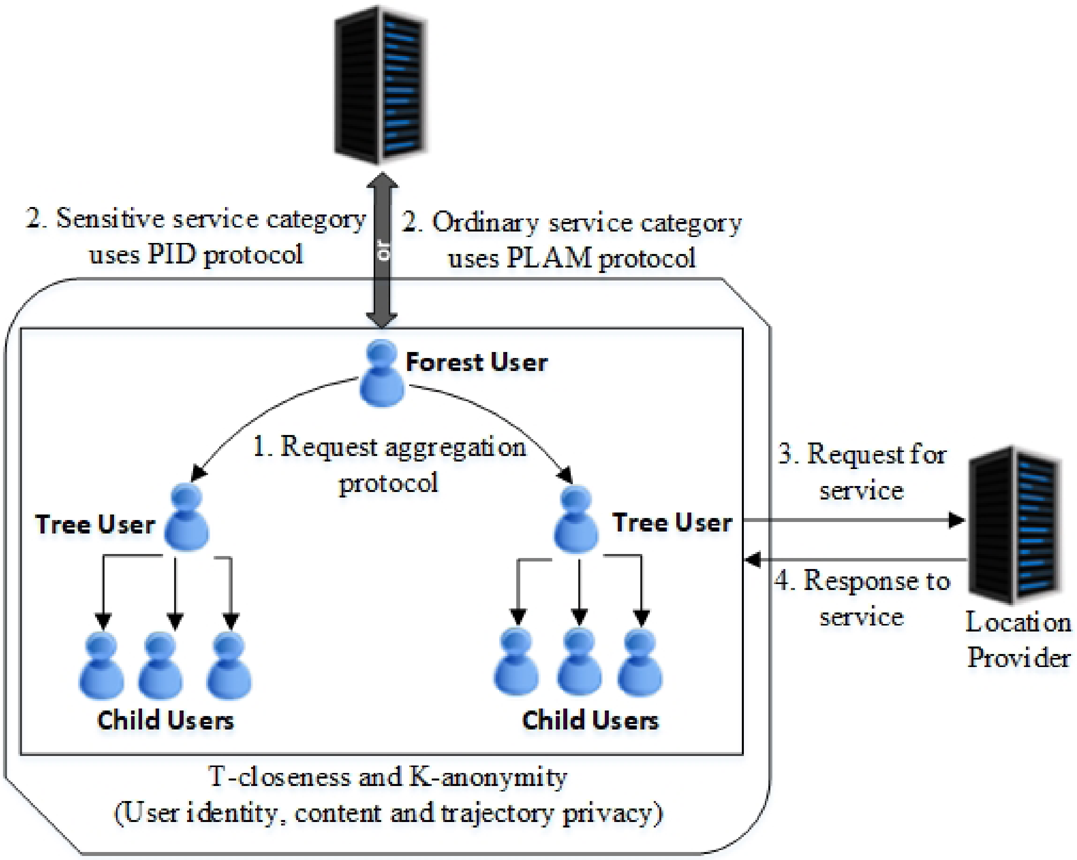

2. Sensitive service category uses PID protocol
or
2. Ordinary service category uses PLAM protocol
Forest User
1. Request aggregation protocol
Tree User
Tree User
Child Users
Child Users
3. Request for service
4. Response to service
Location Provider
T-closeness and K-anonymity
(User identity, content and trajectory privacy)

FIGURE 2. Architecture of Hierarchy based model.

either the user is located at sensitive location among other users who are at same place or non-sensitive and different locations. In case, the user is located in a sensitive location and all labeled users are also at similar place, the model invokes Pseudo Identity (PID) Protocol [13], that protect a user's spatial information efficiently. In contrast, if a user is in a non-sensitive location, then a privacy-preserving framework for Local-Area Mobile social networks (PLAM) protocol will be invoked that can protect the location and preference privacy when the users' locations are different [49]. In PLAM framework, t-closeness and k-anonymity are used to preserve the privacy of the user's identity as well as spatial information. These techniques assist in providing satisfactory user privacy. The model involves a hierarchy-based structure wherein a Forest User (FU) also known as root user requests Tree Users (TU) (child users of root parent) to aggregate and furthermore Tree users inherit Child Users (CU) as shown in figure 2.

Therefore, FU appears to be the leading user which is supervising the TU and TU to CU 't' also anonymizes the identity of real users who are requesting for services from LP. The FU interacts directly with an LP in this approach to provide privacy for the user. By applying t-closeness and k-anonymity [47], it becomes very strenuous for an adversary to reveal the attributes of users driven from user input for query processing. Other tools like the PID protocol and improved PLAM are used to safeguard the user's identity and location, and in that way, this technique provides a great deal of privacy to users. Identity disclosure can lead to attribute disclosure, but t-closeness in combination with l-diversity prevents both identity and attribute disclosure. Every attribute is assigned a global distribution, which means the extent to which an attribute can go on. If this distribution is narrow in scope, then it is very easy to infer a user's information, but if it has a broader scope, the probability of vulnerability of information goes down, but it is possible to intercept a user's critical information. t-closeness involves a main entity 't', which means threshold. t-closeness basically relies on the idea of maintaining distributions for a user's identity and attributes in such a way that rounds about threshold 't' by expounding the global background observation. Figure1 shows the details of the proposed model.

A. FRAMEWORK WORKFLOW

The workflow of the approach involves each component of the entire system. Firstly, it goes through the Identity Exchange Server (IDES) initialization step; this step performs initialization of server according to the given parameters in input which are 't' threshold for attribute distribution and 'l' location category based on l-diversity having characteristics of well-represented attributes. After the server initialization,

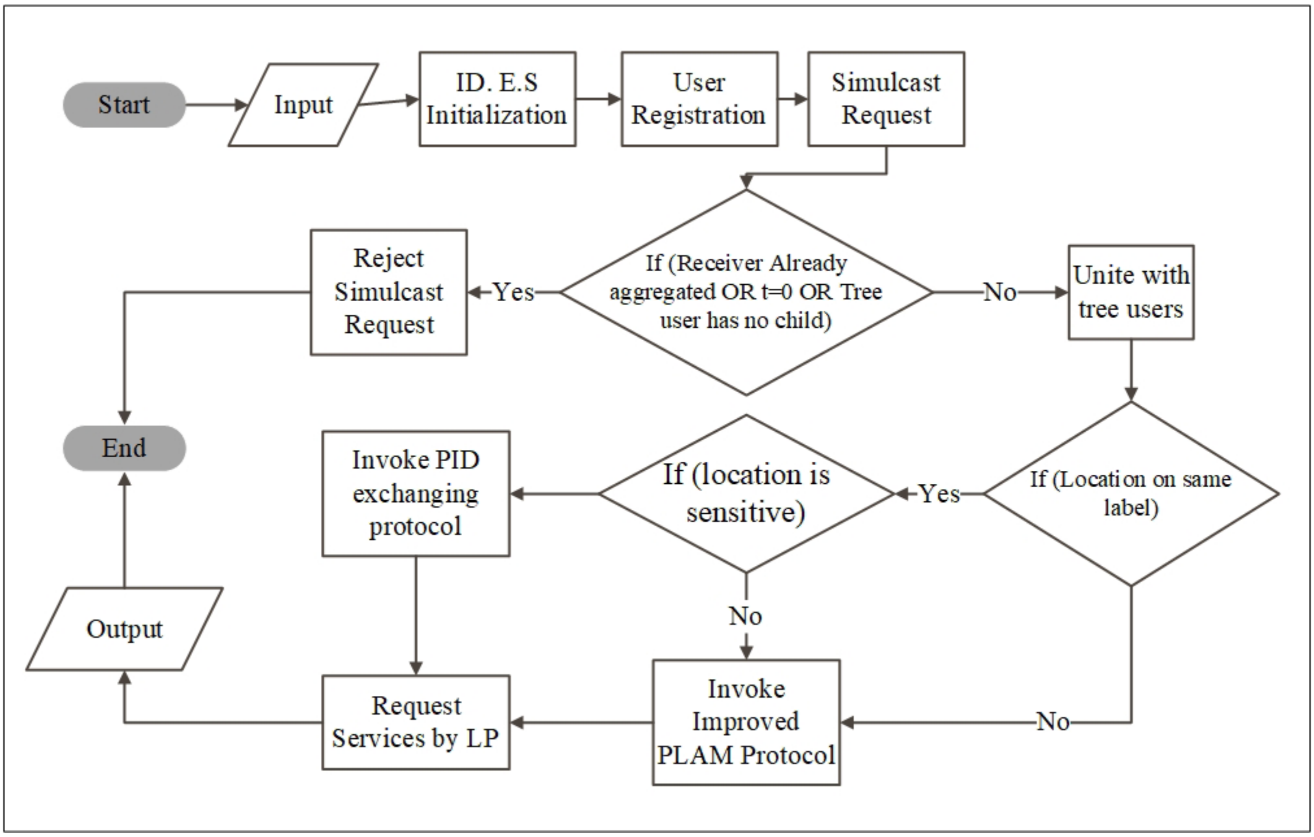

Start
Input
ID. E.S Initialization
User Registration
Simulcast Request
If (Receiver Already aggregated OR t=0 OR Tree user has no child)
Yes
No
Reject Simulcast Request
Unite with tree users
End
Invoke PID exchanging protocol
If (location is sensitive)
Yes
If (Location on same label)
No
No
Output
Request Services by LP
Invoke Improved PLAM Protocol

FIGURE 3. Workflow of proposed model.

a user must be registered in order to proceed further, and this also ensures the authenticity of the Location Based Server. Once a user is registered, then they will come up with simulcasting of request with tree user by using a request aggregation protocol which will enable the FU to communicate with the LP. FU will first check conditions if the TU have already aggregated with another one or request timeout has been elapsed or TU inherit no CU which are actual users requesting services, then the simulcast request will fall in rejection state and process will be terminated but in other case FU would confederate with TU.

Furthermore, location labels of the TU are gone under checking whether location labels are sensitive or ordinary that's a very crucial stage because users are served by LP on the basis of their type of position. If a user is requesting from a sensitive location, then PID Exchanging protocol will be entreated but if locations are same and ordinary, ultimately improved PLAM will be invoked and after accurate completion of this step the forest user would finally request the LP to serve the required services. The LP will process the packaged query sent over by the FU, and then, after generating a meaningful and precise output, it will send it back to the FU, who will get its inherited members TU entertained with the requested services. Figure 3 shows the workflow of the proposed model.

As we see words and their abbreviation that are being used in algorithms are mentioned in the variables so it need not be discussed again we will only explain the flow or working of algorithms 1, 2, 3 and 4.

The Request aggregation protocol algorithm is based on the protocol that assists in handling a user's aggregation problems. This algorithm is used for the smooth aggregation of FU with the TU, so first of all the FU sends the Request aggregation message (Ram) to the TU, but for the TU to accept the message, some conditions need to be met. One condition is aggregation will be accomplished successfully if TU's are not already aggregated with the other party or third party or in simple words if third party aggregation is not true second is the value of time is not zero means aggregation time not out and third is if the TU's has some CU means value of CU is not zero otherwise aggregation suspended and requires the completion of these conditions. Also, if the number of TUs is equal to the number of Aggregation Users (AUs), means if all the TU's successfully aggregated with the FU then Aggregation Package (Ag) will be generated for acknowledgement of problem free aggregation but for maintaining the privacy of users t-closeness requirements checking is important for that FU fully aggregated with TU's in that case if Ag meets the t-closeness requirements otherwise aggregation will have aborted.

Algorithm 1 Request Aggregation Protocol

```
Declarations:
    Request aggregating message ➔ Ram,
    Tree Users ➔ TU,
    Forest User ➔ FU,
    Child User ➔ CU,
    Aggregated User ➔ AU
    Representative User ➔ RU
    Aggregated Package ➔ Ag
Input: Ram, All Users (TU, FU, CU), k
Output: Ag, RU
Simulcast Ram (FU); // FU want to be served by LBS System, however, he will firstly unite with other k-1 users by using the Ram.
Receive the simulcast message (TU); // TU receive broadcast request from FU, then CU from TU.
if (TU aggregated with others || t=0 || number > k/2) // t = 0 (if the time t is zero in request package), if number (other users joined with receivers) of users more than k/2 are agree to join FU and TU
Ignore the simulcast message;
else
Agree to aggregate with the FU;
end if
if (FU aggregation with other number of users = k)
Generate Ag; // output
end if
if (Ag meets the t-closeness requirements)
make FU as RU // the sender will become the representative user
else
Terminate aggregation process unsuccessfully.
end if
```

Algorithm 2 Pseudo-ID Exchanging

```
Declarations:
    Location in Aggregated Package ➔ LAg,
    Number of Users ➔ nu,
    Counter Variable ➔ i,
    Hash functions ➔ H1, H2
    Pseudo-ID ➔ $Pid_i$
    Public Key ➔ $PK_{pids}$
    Private Key ➔ $Sk_i$
    Unique identity ➔ Uid
Input: Ag, $\rho$, system parameters (q, g, G, GT, e, $PK_{pids}$, f, H1, H2, $Pid_i$, enc())
Output: Uid for each user
if (LAg==identical && LAg==sensitive)
    Exchange IDs with probability $\rho$;
    while (i=0 to nu)
        Receive Pidi and Ski for each user
    end while
        if(e(H2($Pid_i$), $PK_{pids}$) = e(Ski, g)); // in case of hashed key pseudo-id encrypted with public key is equal to encrypted 'g' with private key
        Replace user's original identity by $Pid_i$;
        else
        Exchanging pseudo-ID is not successful;
        end if
    update the Ag and send it to the LP;
end if
```

This algorithm is designed for the Pseudo ID Exchanging Protocol, which is used to exchange the IDs of users from the ID Exchange Server belonging to sensitive locations. Key exchange method can also be followed from [50]. This algorithm also uses some encryption schemes, hash functions, and bilinear pairing methods to protect users' identities or characteristics. In the first step, PID Exchanging and other services will be provided if the aggregation of the FU and TU is completed successfully, and after that, if the Location in aggregation Package (LAg) is identical or sensitive, then the PID Exchanging Protocol will be executed and the IDs of the users will be exchanged. If the users are identical or in sensitive locations, then users who want to exchange their IDs will be protected by the encryption schemes, and after that, the ability and accuracy of the encryption methods is checked to determine whether the data is encrypted properly or not. If all these phases are completed correctly, then the users' identities will be exchanged with the help of the PID exchanging protocol; otherwise, the identities will not be exchanged.

The PID Exchanging protocol is used for sensitive locations, but if a user is in an ordinary location, then another protocol is used which is called the improved PLAM Protocol. So if the location is identical AND ordinary OR different services in Aggregation Package will be checked if the number of services categories (services that user requires from the LP) are greater than or equal to the 't' here 't' is the value of t-closeness then the location information of child users will be compared, k/n represents the child users k represents total number of users and n represents number of TU and by dividing k with n only CU remains so if number of TU are in identical locations or ordinary locations then PLAM protocol will be executed for Exchanging IDs from the ID.E.S or for securing user's information. If there is no need in order to exchange IDs, then the Ag is sent to the LP to obtain the services. However, if the number of Service Category (nsc)

Algorithm 3 The Improved PLAM Protocol

```
Declarations:
    Representative User ➔ RU
    Unique identity ➔ Uid
    Location in Aggregated Package ➔ LAg,
    Number of Service Category ➔ NSC,
    Users at same Location ➔ USL
Input: LAg, k, $l$, RU
Output: Uid for each user
if (LAg == identical && LAg == ordinary) || LAg == different);
    Check the services in LAg;
    if (NSC $\geq l$)
        Compare the location (x, y) of k users;
        if (USL > k/2)
        Call Algorithm-II (PID exchanging protocol);
        else
        Send the LAg to LP;
        end if
    else
    Request is failed, terminate the LAg;
    end if
end if
```

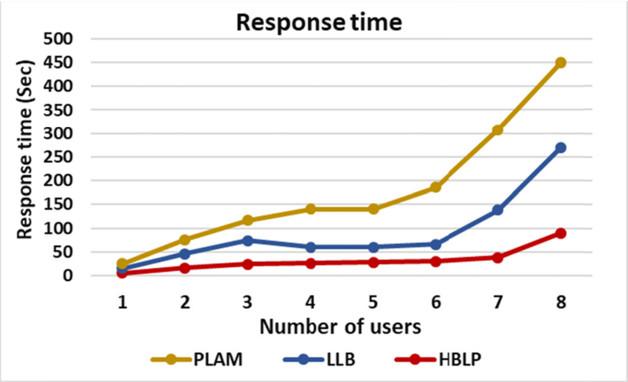


FIGURE 4. Measuring response time.

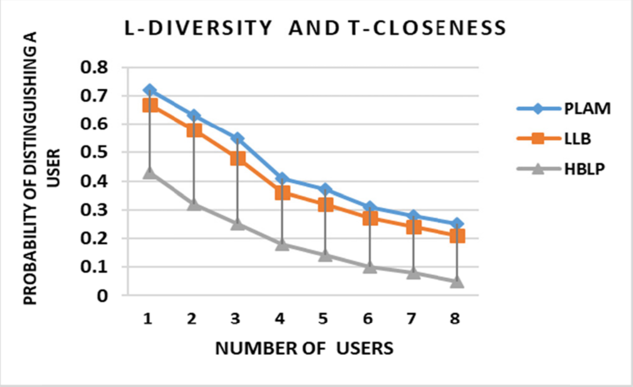


FIGURE 5. Measuring l-diversity and t-closeness.

is not greater than or equal to 't', then the request for services will fail or be aborted.

The Location Category Based Algorithm specifies the overall working or callings of different functions. First of all, the Ram is sent by the FU to the TU by using the Request aggregation protocol (Rap), and after this, the location labels of the TU are compared to determine whether the labels are sensitive or ordinary. If the location labels are identical and sensitive, then the PID Exchanging Protocol is executed, and if the labels are identical and ordinary or even if location labels are different, then the PLAM Protocol is executed.

B. TIME COMPLEXITY CALCULATION

Appropriate division of k users and allocation of the division to the TU can reduce the time complexity of the communication process among the users, the LP, and the PID Exchange server. The below equations are formulated to calculate the complexity of the time elapsed for the FU and TU. If the total number of users is divided by the total number of TUs and the resulting value is then differentiated from the total number of TUs but excluding the FU, then we can determine the time complexity for the FU. If the total number of users is divided by the total number of TUs and eliminating the total number of TU in next step and FU itself, then we can determine the time complexity for the TU by following equation 2 and 3 respectively. In a hierarchy-based model, the time complexity goes towards reduction when a huge number of users are handed over to TU acting as managers and FU just administrates the TU and has no burden of handling CU who are actual users.

FU = Forest User; TU = Tree User; k = Total number of users; τ = time; n = Total number of tree users

$$\text{Time of FU} = \tau^{*}(\text{k/n} - \text{m}) \tag{2}$$

Let m=k/n-n

$$\text{Time of TU} = \tau^{*}(\text{k/n} - \text{n}) - 1 \tag{3}$$

V. EXPERIMENTS AND RESULTS

A. EXPERIMENTAL ENVIRONMENT

All the experiments were performed on OPNET Riverbed Modeler simulation tool [48]. OPNET Riverbed provides a virtual environment for simulating large and complicated networks involving routers, switches, servers, internet connection, protocols, and applications. This tool effectively evaluates the performance of a proposed model before implementing it in a real environment. We have also implemented this tool, and our very first step was to clearly identify the network needed for users and servers to communicate. Here we created four scenarios based on different categories and conditions, and then generated graphs according to the created scenarios.

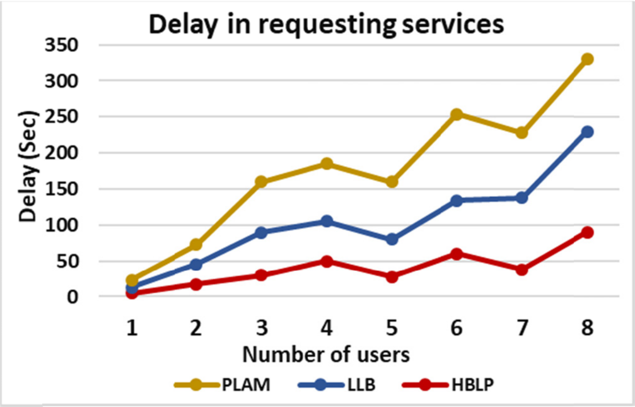


FIGURE 6. Measuring delay rate.

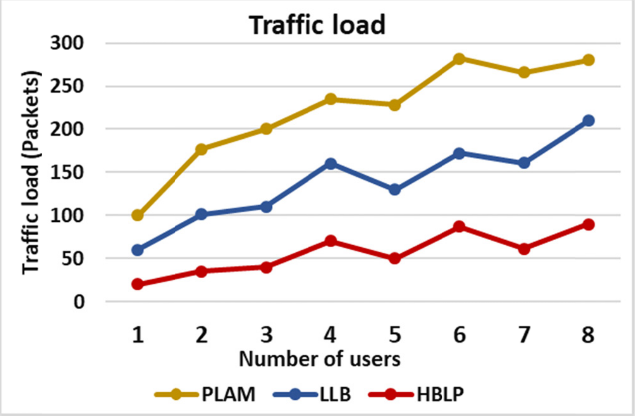


FIGURE 7. Measuring traffic load.

Scenario1: In Figure 9, as shown in Scenario 1 in Appendix, there is a user-defined application configuration in which we created an application protocol for the Location Provider (LP) services and a profile configuration which stores a profile used for a user's registration with the LP. Moreover, it has two subnets, named the server subnet and the user subnet, wherein the server subnet contains an LP server and the user subnet contains the Forest User (FU), and there is also an internet link through which the server and user communicate with each other. In this network scenario, only the FU requests user services from the LP, and this connection takes place through the internet linkage. The internet connection routers are then connected with the server and the FU.

Scenario2: Figure 10 is shown in Appendix. Scenario2 has a star topology created with 1 × 9 nodes, where some nodes are assigned with a name such as Tree User1 (TU), one as FU, and so on. Every node is connected to a central hub, and hubs are further connected with a router. TU are aggregating with FU who is handling and managing all requests and services of TU and acting as representative. The FU packages all the requests into a single package, and after that it sends this aggregated request to the LP, as mentioned above. The Request aggregation protocol is implemented in this scenario.

Scenario3: Figure 11 is presented in Appendix. Scenario3 also has a star topology created with 1×9 nodes, where some nodes are assigned with a name as such Child User1 (CU), some are TU1, and so on. Every tree and child node is connected with a central hub, and hubs are further connected with a router. CU are aggregating with TU who is responsible for managing requests and services of CU.

Scenario4: Figure 12, as shown in Appendix, involves four subnets, city1, city2, city3, and city 4, and a server subnet with a Pseudo Identity (PID) Exchange server. the All cities have a maximum of 10 nodes categorized as sensitive and ordinary locations. This scenario uses the PID Exchange protocol as an application, and the PID Server registers all nodes within the specified cities; this network is established through routers and switches. All routers are bound to an internet connection, and every node communicates to get an exchange identity from the PID server.

Algorithm 4 Location-Category Based Algorithm

```
Declarations:
    Request Aggregation message ➔ Ram,
    Request Aggregation Protocol ➔ Rap,
    Aggregated Package ➔ Ag,
    Locations ➔ loc,
    Forest User ➔ FU,
    Tree User ➔ TU
Simulcast Ram;
Ag by using Rap;
 if (FU has TU)
     Compare the tree users' location labels;
     if(loc=identical && loc=sensitive)
     Call Algorithm-II (pseudo-ID exchanging protocol);
   else if ((loc=identical && loc = ordinary) || loc =
   different)
Call Algorithm-III (improved-PLAM protocol);
end if
end if
```

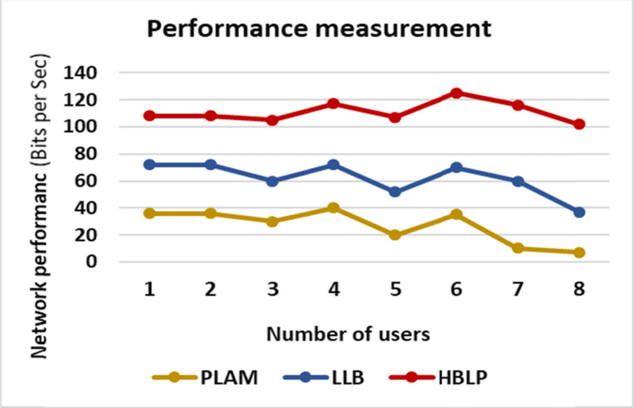


FIGURE 8. Measuring network performance.

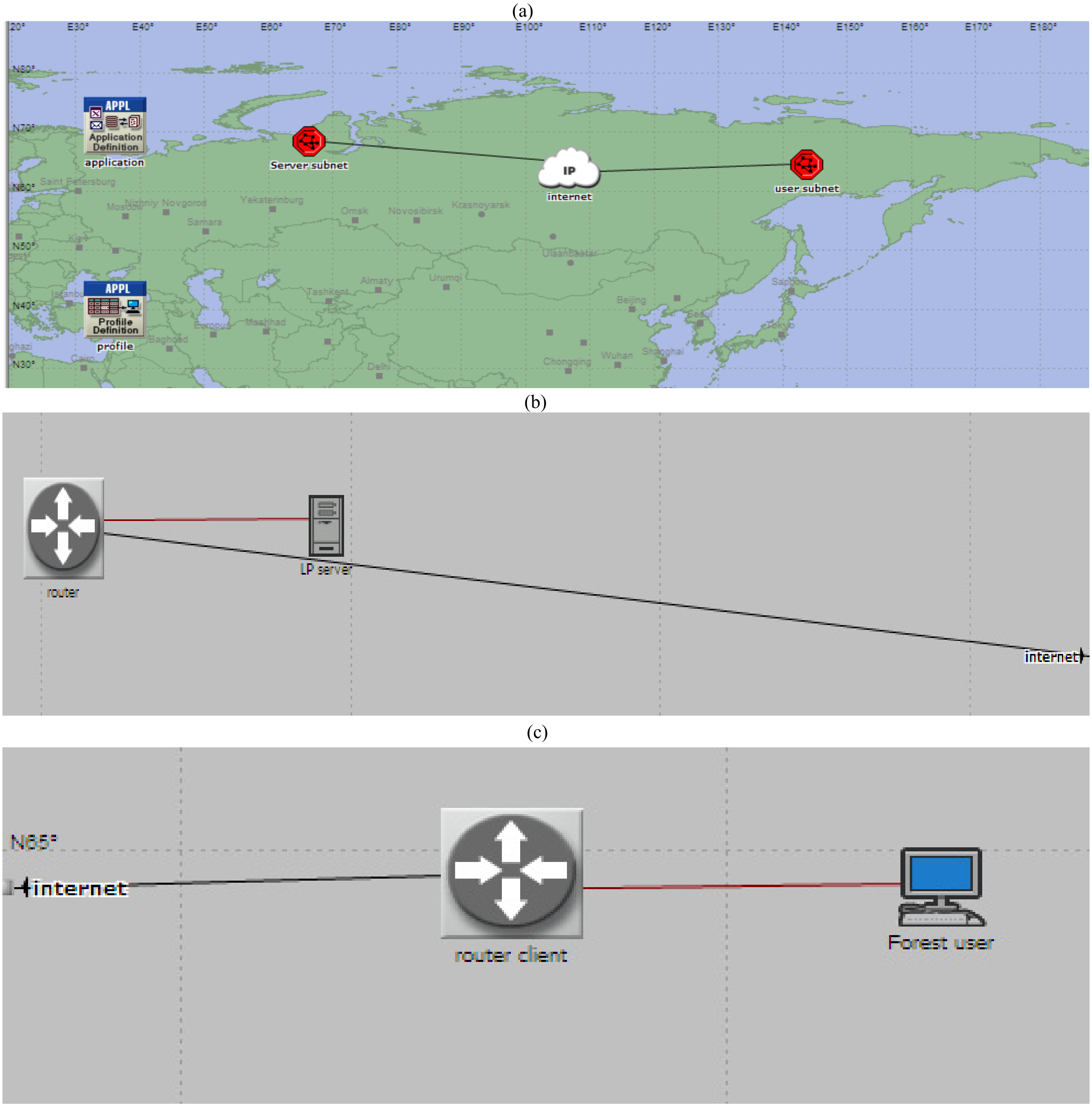

(a)
(b)
(c)

FIGURE 9. Scenario1.

B. PERFORMANCE ANALYSIS

This part encompasses all generated results of the above-mentioned scenarios which are created in a simulation environment. All the figures shown above are graphs for use in evaluating the proposed model Hierarchy based privacy provision (HBLP) model with the existing model L2P2. Five different parameters are tested, with varying conditions and values.

According to Figure 4, the LLB and PLAM algorithms used in existing papers require more response time compared to the HBLP model, because the LLB and PLAM algorithms involve multiple users which individually aggregate and request servers through a representative user. These all users demand the same resource allocation and privacy simultaneously, which causes server overhead while in Hierarchy based approach a Forest User (FU) is handling Tree Users (TU) and TU are handling Child Users (CU).

The whole work is distributed among all and only one FU is communication with the server which reduces server overhead of processing a lot of queries simultaneously but

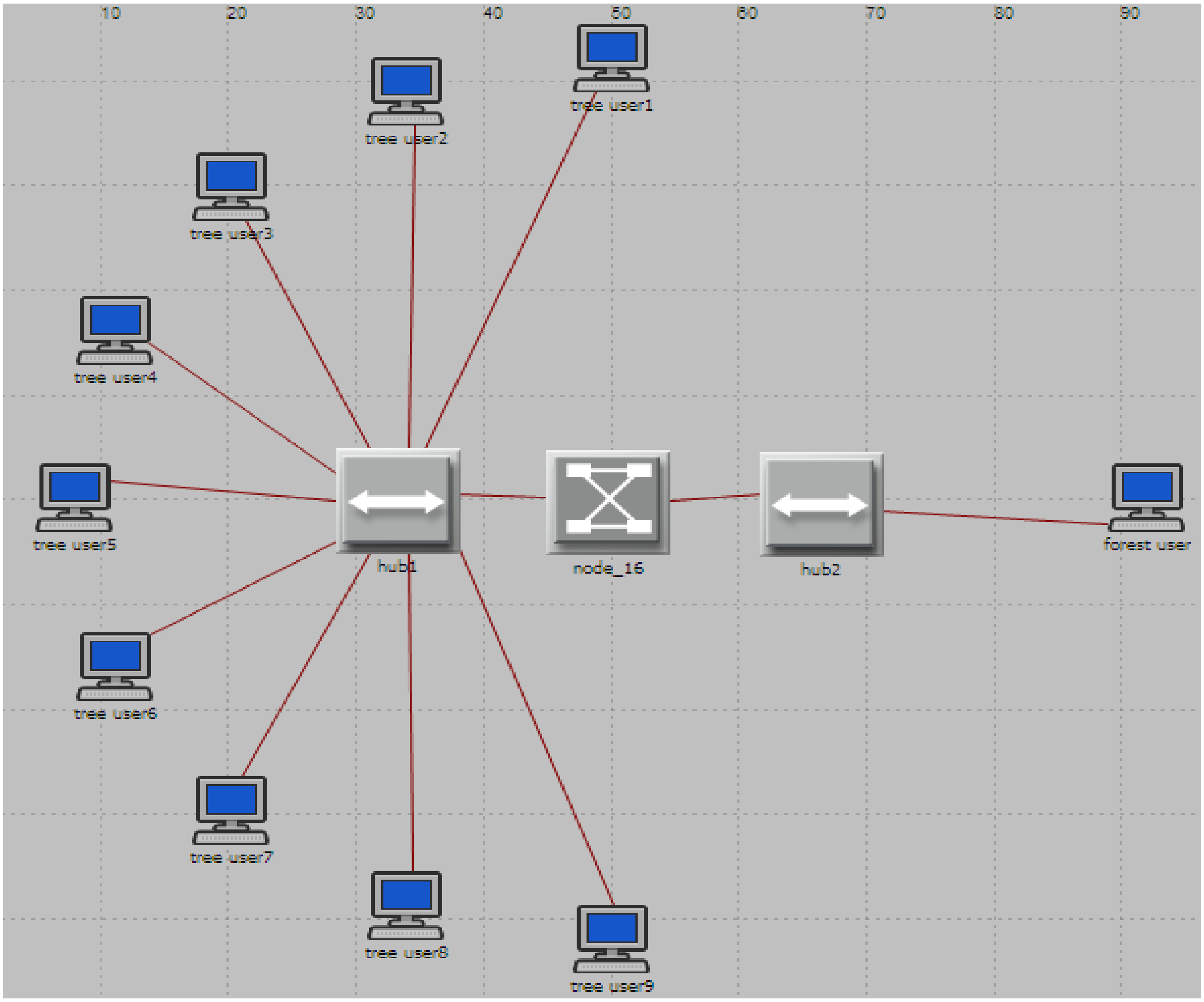


FIGURE 10. Scenario2.

instead server is now less-burdened because it just has to process sent by only a single FU. Figure 5 shows the effectiveness of t-closeness and l-diversity. The LLB and PLAM algorithms that were used in the earlier technique use a combination of k-anonymity and l-diversity, and this combination suffers from many shortcomings. k-anonymity and l-diversity gives a close probability of keeping track of the attribute and identity information because its global distribution value is closely related to the actual stored values, while on other hand t-closeness and l-diversity comes as a solution to this problem because global distribution value of t-closeness is not closely related to real value instead it defines as many as possible values in it just hinting as less or greater. For instance, if t threshold is <9.0, it means all the values below 9.0 which can go much longer even approaching negative infinity. However, it's very hard to trace out the probability of getting even closely related figure about the stored information.

In figure 6, Delay rate in requesting services is analyzed existing approach's algorithms LLB and PLAM has high value of delay in requesting aggregation with other user because only a representative user broadcast the aggregation request 9 to all other users which increases the delay rate as the number of users goes up, the delay rate goes up. In the LLB and PLAM algorithms, the number of users and the delay rate are directly proportional to each other, while in HBLP, the numbers of user and the delay rate are inversely proportional because not only are all aggregation requests sent by the FU, but also the FU inherits its own clients to manage further aggregation requests by the CU. So, in both algorithms of existing technique only representative is broadcasting aggregation request which takes more time but in HBLP model FU and TU are broadcasting aggregation requests which divides the delay time. Figure 7 shows a comparison of the traffic loads on the network, which increase if the number of users increases.

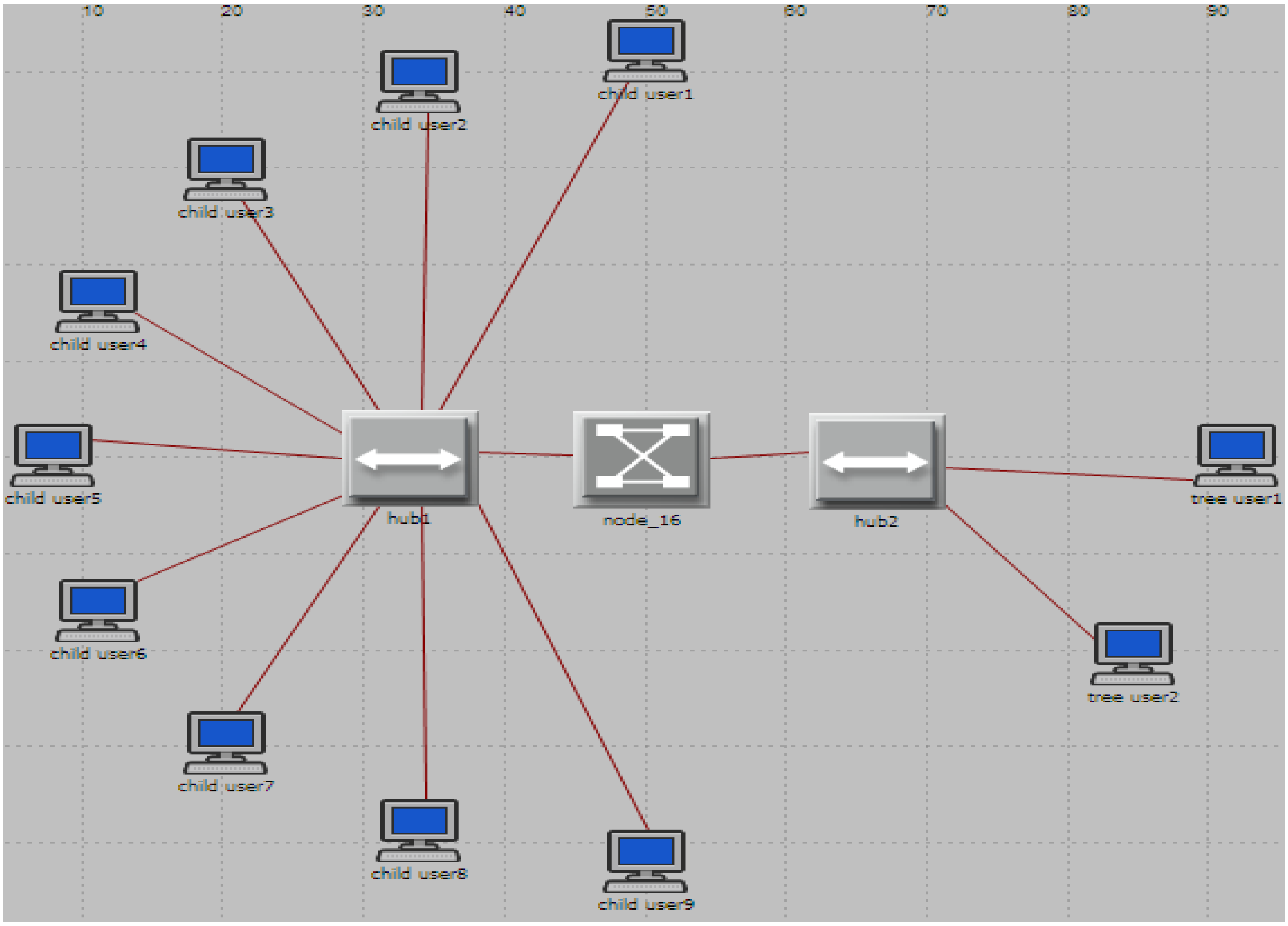


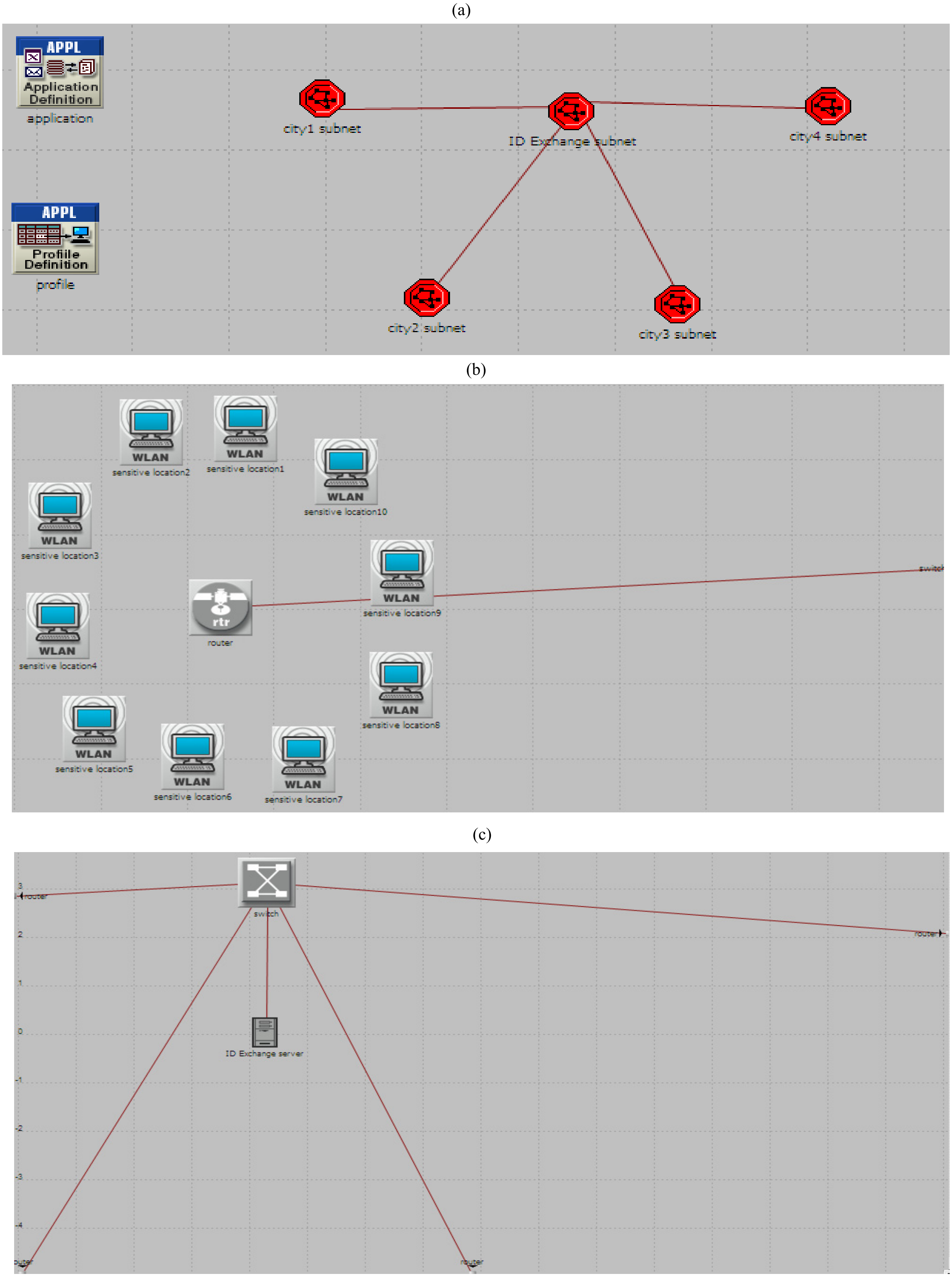
FIGURE 11. Scenario3.

The LLB and PLAM algorithms process all outgoing and incoming traffic, involving different protocols and applications since these protocols frustrate the channel through heavy traffic load because of low-administration nodes but in case of Hierarchy based it all depends on FU and TU to equally manages the traffic load where FU has to administer TU and TU have to administer CU but at the back end both are responsible for in-time availability of resources and query generation for all the nodes.

Figure 8 shows the collective performance based on response time, delay time, traffic load, and the effectiveness of t-closeness and l-diversity. All these parameters prove the improved performance of HBLP as compared to the approaches of existing algorithms in terms of resources, throughput, incoming requests, outgoing aggregation requests, and server processing timeouts when a node fails to aggregate within a given time. With the definite evidence of all these performance-measuring parameters, the HBLP model is quite reasonable in providing of privacy to users with regard to their three sensitive metrics, i.e., spatial, position, and temporal information.

VI. DISCUSSION

As we have seen, the day-to-day progress of Location Based Services (LBSs) involves users encountering privacy issues. Privacy has been treated as a serious concern by many researchers who have sought breakthroughs in order to guarantee users' privacy. Although their creations have reflected a tremendous success rate, there still exists no full-fledged flawless system, because if a system targets one specific issue, another one will surely arise. Therefore, more advances are always required, and the challenge of protecting users' privacy in a technological world will remain. A user can be threatened through three main attributes, which are spatial, identity, and temporal information, which can be compromised by ascertaining a user's Point of Interest (PoI). Users' critical information may be misused or misinterpreted by an adversary, and this can include spoiling the image of a renowned business or harming people at an individual level, which can be devastating for people's social, political, and personal lives. Our proposed approach enables improvements in the privacy provision of previous approaches as well. For conducting a lucrative research we surfed different websites


(a)

(b)

(c)

FIGURE 12. Scenario4.

and gone through vast number of recently written research papers so that we can figure out the recently raised complications related to the privacy of LBS Systems because recently written research papers are the removal of drawbacks in the old techniques and the advance approach always proves better than the previous so as our objective is to introduce a new approach which provides privacy in LBS systems at users satisfactory level by eliminating the shortcomings in the earlier approaches. Thus, we thoroughly studied recently proposed approaches, and through comparing them, we found the best ones among them. After that, we analyzed these approaches with regard to their implementations, results, and the devices used for the development of these approaches, and by doing a comprehensive analysis, we developed a new framework which fulfils our main objective by creating a scenario which includes different encryption schemes, servers, and the devices used at the user's end. Our proposed model is grounded in the Internet of Things (IOT), which is an emerging technology that modern research aims to use for further advancements in computer science. The proposed model is named the Hierarchy Based Location Privacy (HBLP) model, and it includes many technical aspects, like pseudo ID exchanging, request aggregation, and Location Providers (LPs). Mainly it involves Forest Users (FUs), Tree Users (TUs), and Child Users (CUs) for accessing services. Because of its hierarchical structure, it is termed a hierarchy-based model, wherein an FU commands a TU, and the TU rules out CUs in an ad-hoc fashion. Through this hierarchy, HBLP model controls resources, response times, traffic, and delay rates. In contrast the base paper technique focused only on having all the users at the same level without the division of FU, TU and CU where all the burdens and overheads are to be carried out by only a representative user and others only enjoys the status of being served and in such a way this technique suffered from time complexity. The proposed framework handles the time complexity issue at a very ample level. In order to protect the said privacy metrics (User's identity, spatial information and temporal information), the HBLP uses t-closeness and l-diversity, with CUs being the entities actually demanding services from the TU, which in turn demands them from the FU. This chain automatically hides the identity of real users, and the requirement for thorough privacy is fulfilled through a combination of encryption schemes like bilinear pairing, hash functions, and specified protocols in order to have checks and balances on the conditions. These conditions are the bases for further processing in the proposed model, which differentiates between the nature of locations, i.e., ordinary and sensitive location. However, as discussed above, the proposed approach is designed to cope with the existing challenges and drawbacks and is very helpful in providing privacy due to its attributes.

VII. CONCLUSION

The accessibility of mobile devices with incorporated position sensors and LBS systems is now extremely prevalent. However, since these services access personal information (location, identity, and query time) when a user interact with an LBS system, measures to maintain a user's privacy are necessary when they are making queries. The literature portrays a wide range of ideas and concepts to protect location privacy which vary in terms of the secured data and their adequacy against different type of attacks. Regarding these privacy challenges, we have proposed a new model, the HBLP, which protect a mobile user's privacy attributes (User Query Time, Identity, Location) for Non-Trusted Third Party (NTTP) LBS systems. Furthermore, we implemented the proposed model using the Riverbed OpNet++ simulation tool. During the implementation, we evaluated different privacy-related factors, such as l-diversity, t-closeness, query success rate, response time, and delay in query response, and compared the results with existing state-of-the-art privacy provision mechanisms. It was observed that the proposed HBLP model outperformed all existing strategies in all aspects of protecting a user's privacy.

APPENDIXES

APPENDIX A

See Scenario1 in Fig. 9(a)–(c).

APPENDIX B

See Scenario2 in Fig. 10.

APPENDIX C

See Scenario3 in Fig. 11.

APPENDIX D

See Scenario4 in Fig. 12(a)–(c).

ACKNOWLEDGEMENT

The authors would like to acknowledge with thanks DSR technical and financial support.

REFERENCES

[1] V. Primault, A. Boutet, S. B. Mokhtar, and L. Brunie, "The long road to computational location privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2772–2793, 3rd Quart., 2019.

[2] K. P. N. Puttaswamy, S. Wang, T. Steinbauer, D. Agrawal, A. E. Abbadi, C. Kruegel, and B. Y. Zhao, "Preserving location privacy in geosocial applications," *IEEE Trans. Mobile Comput.*, vol. 13, no. 1, pp. 159–173, Jan. 2014.

[3] R. Gupta and U. P. Rao, "An exploration to location based service and its privacy preserving techniques: A survey," *Wireless Pers. Commun.*, vol. 96, no. 2, pp. 1973–2007, Sep. 2017.

[4] M. Yamin and A. A. A. Sen, "Improving privacy and security of user data in location based services," *Int. J. Ambient Comput. Intell.*, vol. 9, no. 1, pp. 19–42, Jan. 2018.

[5] 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.

[6] Barnes, "Location-based services: The state of the art," *e-Service J.*, vol. 2, no. 3, p. 59, 2003.

[7] L. Chen, S. Thombre, K. Jarvinen, E. S. Lohan, A. Alen-Savikko, H. Leppakoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[8] R. Gupta and U. P. Rao, "Achieving location privacy through CAST in location based services," *J. Commun. Netw.*, vol. 19, no. 3, pp. 239–249, 2017.

[9] A. Aloudat, K. Michael, and J. Yan, "Location-based services in emergency management-from government to citizens: Global case studies," Univ. Wollongong, Wollongong, NSW, Australia, Tech. Rep. 21602, 2007.

[10] F. Tang, J. Li, I. You, and M. Guo, "Long-term location privacy protection for location-based services in mobile cloud computing," *Soft Comput.*, vol. 20, no. 5, pp. 1735–1747, May 2016.

[11] *Teletrac Navman: GPS Fleet Management Solution*. Accessed: May 8, 2019. [Online]. Available: https://www.teletracnavman.com.au/

[12] G. Sun, D. Liao, H. Li, H. Yu, and V. Chang, "L2P2: A location-label based approach for privacy preserving in LBS," *Future Gener. Comput. Syst.*, vol. 74, pp. 375–384, Sep. 2017.

[13] *Digital Signature Guidelines Tutorial*, Amer. Bar Assoc., Chicago, IL, USA, Mar. 2010 pp. 1–8.

[14] M. Licht, "Delivering IVHS to the marketplace: A provider's perspective," in *Proc. Vehicle Navigat. Inf. Syst. Conf. (VNIS)*, 1993, pp. 330–333.

[15] N. Gandal, D. Salant, and L. Waverman, "Standards in wireless telephone networks," *Telecommun. Policy*, vol. 27, nos. 5–6, pp. 325–332, Jun. 2003.

[16] T. Havinis and D. Boltz, "System and method for downloading network information to mobile stations for location calculation," U.S. Patent 6 671 377, Dec. 30, 2003.

[17] S. Wang, J. Min, and B. K. Yi, "Location based services for mobiles: Technologies and standards," in *Proc. IEEE Int. Conf. Commun. (ICC)*. vol. 19, 2008.

[18] J. D. Busch, "Systems and methods to deliver digital location-based content to a visitor at a physical business location," U.S. Patent 8 447 331, May 21, 2013.

[19] P. Vlacil and R. Bestak, "Implementing mobile location protocol," in *Proc. 32nd Int. Conf. Telecommun. Signal Process.*, 2009, pp. 1–4.

[20] D. Seo and R. Bekkers, "The importance of and a comparison of standards development organizations in the ubiquitous society," in *Proc. Korean Soc. Manage. Inf. Sci.*, 2008, pp. 23–28.

[21] O. M. Murali, "Unit-2 recent trends in geoinformatics," IGNOU, New Delhi, India, Annu. Rep. 2017-2018, 2017.

[22] G. R. Hendrey, "Managing and querying moving point data," U.S. Patent 7 010 308, Mar. 7, 2006.

[23] J. Brookman, "Protecting privacy in an era of weakening regulation," *Harvard Law Policy Rev.* vol. 9, p. 355, Summer 2015.

[24] M. L. Damiani, E. Bertino, and C. Silvestri, "Protecting location privacy against spatial inferences: The PROBE approach," in *Proc. 2nd SIGSPATIAL ACM GIS Int. Workshop Secur. Privacy GIS LBS (SPRINGL)*. New York, NY, USA: Association for Computing Machinery, 2009, pp. 32–41.

[25] Y. Wang, D. Xu, X. He, C. Zhang, F. Li, and B. Xu, "L2P2: Location-aware location privacy protection for location-based services," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1996–2004, doi: 10.1109/INFCOM.2012.6195577.

[26] L. Ou, H. Yin, Z. Qin, S. Xiao, G. Yang, and Y. Hu, "An efficient and privacy-preserving multiuser cloud-based LBS query scheme," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Mar. 2018, doi: 10.1155/2018/4724815.

[27] H. Huang, G. Gartner, J. M. Krisp, M. Raubal, and N. Van de Weghe, "Location based services: Ongoing evolution and research agenda," *J. Location Based Services*, vol. 12, no. 2, pp. 1–31, 2018, 10.1080/17489725.2018.1508763.

[28] Q. Hu, S. Wang, C. Hu, J. Huang, W. Li, and X. Cheng, "Messages in a concealed bottle: Achieving query content privacy with accurate location-based services," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7698–7711, Aug. 2018.

[29] J. Qu, G. Zhang, and Z. Fang, "Prophet: A context-aware location privacy-preserving scheme in location sharing service," *Discrete Dyn. Nature Soc.*, vol. 2017, May 2017, Art. no. 6814832.

[30] P. Palmieri, L. Calderoni, and D. Maio, "Spatial Bloom filters: Enabling privacy in location-aware applications," in *Information Security and Cryptology* (Lecture Notes in Computer Science), vol. 8957, D. Lin, M. Yung, and J. Zhou, Eds. Cham, Switzerland: Springer, 2015.

[31] A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, "Location privacy in location-based services: Beyond TTP-based schemes," in *Proc. CEUR Workshop*, 2008, p. 397.

[32] M. Ashouri-Talouki and A. Baraani-Dastjerdi, "Homomorphic encryption to preserve location privacy," *Int. J. Secur. Appl.*, vol. 6, no. 4, pp. 183–189, 2012.

[33] S. A. Bukhari, 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.

[34] K. Nikolopoulos, S. Bakiras, A. U. Tansel, and S. Zachos, "Efficient private information retrieval," Tech. Rep., 2019.

[35] J. Krisp, *Progress in Location-Based Services*. Berlin, Germany: Springer, 2013, doi: 10.1007/978-3-642-34203-5.

[36] F. Li, S. Wan, B. Niu, H. Li, and Y. He, "Time obfuscation-based privacy-preserving scheme for location-based services," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2016, pp. 465–470.

[37] A. Banihani, "Evaluating trajectory privacy in autonomous vehicular communications," SAE Tech. Paper 2019-01-0487, 2019.

[38] Q. A. Arain, I. Memon, Z. Deng, M. H. Memon, F. A. Mangi, and A. Zubedi, "Location monitoring approach: Multiple mix-zones with location privacy protection based on traffic flow over road networks," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 5563–5607, Mar. 2018.

[39] S. Wang, N. Yao, N. Gong, and Z. Gao, "A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs," *Peer-Peer Netw. Appl.*, vol. 11, no. 3, pp. 548–560, May 2018.

[40] M. Shady, M. Usman, A. Abesen, and S. Arif, "AES-route server model for location based services in road networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 8, pp. 361–368, 2017.

[41] A. K. Tyagi and N. Sreenath, "Location privacy preserving techniques for location based services over road networks," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2015, pp. 1319–1326.

[42] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2014, pp. 251–262.

[43] E. Chou, "Location data and geo-indistinguishable privacy preserving protocols," Univ. Illinois Urbana-Champaign, Champaign, IL, USA, Tech. Rep. ECE499-Sp2017, 2017.

[44] J. Chen, K. He, Q. Yuan, M. Chen, R. Du, and Y. Xiang, "Blind filtering at third parties: An efficient privacy-preserving framework for location-based services," *IEEE Trans. Mobile Comput.*, vol. 17, no. 11, pp. 2524–2535, Nov. 2018.

[45] L. Ertaul, "Privacy in location based services (LBS) via composite functions: The L4NE protocol," *Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. 3, p. 117, 2017.

[46] D. Roy and S. Jena, "Determining t in t-closeness using multiple sensitive attributes," *Int. J. Comput. Appl.*, vol. 70, pp. 47–51, May 2013, doi: 10.5120/12179-8291.

[47] *OPNET Technologies—Network Simulator | Riverbed*. Accessed: May 9, 2019. [Online]. Available: https://www.riverbed.com/products/steelcentral/opnet.html

[48] R. Lu, X. Lin, Z. Shi, and J. Shao, "PLAM: A privacy-preserving framework for local-area mobile social networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2014, pp. 763–771.

[49] C. Ting, L. Xinghua, and C. Qingfeng, "An enhanced key exchange protocol exhibiting key compromise impersonation attacks resistance in mobile commerce environment," *Sci. China Inf. Sci.*, vol. 63, no. 5, 2020.

[50] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2034–2048, Feb. 2020.

[51] D. Liao, H. Li, V. Anand, V. Chang, G. Sun, and H.-F. Yu, "Using location-labeling for privacy protection in location-based services," in *Proc. Int. Conf. Internet Things Big Data*, 2016, pp. 299–306.

KHALID ALSUBHI received the B.Sc. degree in computer science from King Abdulaziz University (KAU), Jeddah, Saudi Arabia, in 2003, and the M.Math. and Ph.D. degrees in computer science from the University of Waterloo, Waterloo, ON, Canada, in 2009 and 2016, respectively. He is currently an Assistant Professor of computer science with KAU. His research interests are focused on network security and management, cloud computing, and the security and privacy of healthcare applications.

M. USMAN ASHRAF was born in Sialkot, Pakistan, in 1988. He received the B.Sc. degree in mathematics from The University of Punjab, Lahore, Pakistan, in 2007, the M.S. degree in computer science from the University of Lahore, Lahore, in 2014, and the Ph.D. degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia. He was a Senior Software Engineer (SSE) with Coeus Solutions GmbH. He is currently an Assistant Professor with the Department of Computer Science, University of Management and Technology, Lahore Sialkot campus, Pakistan. His research interests include high-performance computing (HPC), parallel computing, exascale computing, ubiquitous computing, software engineering, location-based service systems, and recommender systems.

IQRA ILYAS was born in Sialkot, Pakistan. She received the bachelor's degree from the University of Punjab, Lahore, Pakistan, in 2010, the M.Sc. degree in IT from the University of Gujrat, Gujrat, Pakistan, in 2012, and the M.S. degree in IT from the University of Lahore, Lahore, Pakistan, in 2016. She is currently pursuing the Ph.D. degree in computer science with Superior University, Lahore. She was a Lecturer with GC Women University, Sialkot, Pakistan, from 2013 to 2017, where she is also serving as a Network Administrator. Her research interests include software engineering, data mining, cloud computing and artificial intelligence, and the Internet of Things.