**Paper Title: Agent-based Location Aware Services in Wireless Mobile Networks** [1]

*Authors: A. V. Sutagundar, S. S. Manvi, Selvin, M. N. Birje*
*Conference: AICT’07*

This paper proposes an agency based location aware service scheme. In case of any service breakdown, node and link failure the agency can manage service. Their proposed system model divides a wireless network into several clusters. Each cluster is actually a local wired network and has a fixed active node, which comprises of the agency. The agency consists of several agents and a knowledge base. The knowledge base is updated by manager agent. They suggest that agent based location discovery services offer flexibility in terms of the learning capabilities of the agents, scalability as the proposed model is scalable to any network, efficiency, adaptability as the nodes adapt to changing network conditions such as node movement, service break-down, node failure and link failures and maintainability as the agent components can be easily debugged and replaced.

**Paper Title: LORE An infrastructure to support location-aware services** [2]

*Authors: Y. Chen, X. Y. Chen, F. Y. Rao, X. L. Yu, Y. Li, D. Liu*
*Conference: IBM Journal of Research and Development 2004*

This paper presents an infrastructure that supports location aware services. This infrastructure is based on a proposed location operating reference model, which addresses many major aspects of building location aware services. Three key components of the infrastructure are: the location server, a moving object database and a spatial publish/subscribe engine. Different components of this infrastructure are built to meet different layers of and expose APIs to developers who can then build other components that can plug into the model. In short the composition of the components facilitates the development of various location aware services.

In this infrastructure the location server provides flexible location APIs, extensible service management frameworks and scalable common adapter framework. The common adapter framework provides standard APIs to fetch the location information of the target object. The service management framework addresses the issues of privacy and security. The moving database object stores historical and current location information of mobile users. It is composed of several components such as location listener, query engine, location filter, trigger handler, data server etc. that can be physically distributed in different network nodes, which communicate with each other using standard protocol service such as HTTP, TCP/IP. The spatial sub/pub manager manages subscription or publishing events, example of subscription is: a service request “If I am around this (location) sent me this (service)“.

**Paper Title: MobiEyes: A Distributed Location Monitoring Service Using Moving Location Queries** [3]

*Authors: Bugra Gedik, Ling Liu*
*Conference: IEEE Transactions on Mobile Computing, 2006*

This paper issues one important research challenge for location information management, which is, the capability to handle large and rapidly growing number of mobile objects and processing complex queries over mobile object positions. It represents the design and development of MobiEyes, a distributed real-time location monitoring service for moving location queries over a large and growing number of mobile objects.
Moving location queries are defined as, a mobile object seeking other relevant mobile objects around. E.g. “Give me the positions of those customers who are looking for taxi and are within 5 miles (of my location, at an interval of every minute) during the next 20 minutes” can be posted by a taxi driver moving on the road. Motivated by the fact that mobile users are typically interested in other mobile object nearby, the proposed distributed architecture lets determine each mobile object by itself whether or not it should be included in the result of a location query nearby, without requiring global knowledge regarding the moving location queries and the object positions of interest.

The server first installs the query by saving the relevant information, calculates the grid cell for the query and sends installation notification to the object requesting the query. Then the server forwards this query to all objects that reside in the query’s monitoring region.

Upon receiving a broadcast message, a mobile object examines each moving query in the broadcast message using its local state and determines whether this moving query is nearby and whether it should be registered locally. The decision is primarily based on whether the mobile object itself is within the monitoring region of the moving query and whether the query’s filter is also satisfied by the mobile object. If the answer to both of these questions is yes, the mobile object registers the query into its local query table.

**Paper Title: Person Wide Web: Active Location based WebService Architecture using Wireless Infrastructure** [4]

Authors: Seungjae Shin, Pyung Kim, Yeojeong Yoon, Seongbea Eun, Hyunsoo Yoon.
Conference: TENCON 2010 - 2010 IEEE Region 10 Conference

In this paper a new type of location based web service architecture is proposed which is named as ‘Person Wide Web (PWW)’. Based on the geographical location of the mobile user PWW effectively recognized the location specific web resources. Among so-many resources in the WWW, only the things closely located to the user, make up his PWW. It is stated first that the most widely used LBS such as map search, navigation search have different system architecture from each other and also users have to use different client software for each of them. On the contrary web based LBS does not require any specific client software. For web based LBS, all the LBS providers need to establish their own web site. PWW will automatically recognize geographically effective web resources and will notify them to the users in a periodic manner.

In contrast to the existing web service technologies passively waiting until the user requests the service, PWW tries to trigger intended requests of service from users by actively delivering PUSH messages that includes abbreviated information for location-specific web resources. User then connects to the push server to get service.

**Paper Title: A Layered Architecture for Location-based Services in Wireless Ad Hoc Networks** [5]

Authors: Jonathan Agre, Adedji Akhyemi, Lusheng Ji, Ryusuke Masuoka and Pankaj Thakkar

In this paper the design of a location service module is presented with an example. A location service middleware layer is presented that hides the location determination technology from application. One example TULIP is presented here.
The Time-User-Location Information Processing (TULIP) System represents an initial design of a location-aware service system consisting of one or more servers that provides location-context sensitive world wide web (WWW) pages to clients with standard web-browsers and some additional software. In the proposed system a client with a wired or wireless connection to the Internet uses its browser to log onto a TULIP server, available on the web. The login procedure will also generate a special user profile that is sent to the server. After login, the server will initiate a separate side-channel socket connection to the client and will request the client location, as determined through its LSM. Once the server has received the requested location data, it will generate web pages that contain hyperlinks based on that location. These pages are derived from a spatial database with geographic information and knowledge from the user profile.

Paper Title: Enabling Location-Based Services on Wireless LANs [6]
Authors: Yen-Cheng Chen, Yao-Jung Chan, and Cheung-Wo She

In this paper location determination technique by means of the SNMP supported in (Access Points) Aps is proposed. By this approach, no any particular hardware and software is required in mobile devices. In the wired network, only a location server is needed to receive SNMP traps from APs and to perform location detection.

This paper also aims to enable WLAN location-based services in WWW environments. If a location-based service can be implemented as a web application, the web browser in a mobile device will be the only required software to access location dependent information. Previous location determination approaches use particular hardware or software in mobile devices to perform location detection. These approaches were not appropriate for use in WWW environments. Since they assume that the web browser is the only software used in a mobile client, what it can use for location determination will be only the IP address of the mobile device, which can be retrieved from HTTP requests.

Although Java applets can be embedded in most web browsers, it is not allowed to retrieve the MAC address or other identification information of the mobile client via Java applets due to security and privacy concern. On the other hand, most APs use MAC addresses to identify mobile devices. Therefore, as it can obtain the IP address of a mobile device, it still needs to get the MAC address corresponding to the IP address. To support location-based services in WWW environments, this location determination approach will also involve the mapping between IP addresses and MAC addresses.

Paper Title: Safeguarding location privacy in wireless ad-hoc networks [7]
Author: Tanzima Hashem and Lars Kulik
Conference: 9th International Conference on Ubiquitous Computing (UbiComp 2007).

This paper proposes a new approach regarding the location privacy issue of LBS. Their proposed solution states that a query initiator can select itself or one of the k-1 agent in its ad-hoc network as a query requestor, the query initiator remains k-anonymous. In addition, the location revealed to the location service provider is a rectangle instead of an exact coordinate. This can ensure a level of safety regarding location privacy, but still this also considers the traditional server to client based approach for LBS.

Paper Title: Caching as Privacy Enhancing Mechanism in Location-Based Services [8]
Author: Himanshu Pagey, Kien Hua and Chow-Sing Lin
This paper proposes a new caching technique preserving the privacy of user. Their proposed approach tells about an anonymizer, this will be a trusted third party that will perform query blurring to produce a set of different LBS request objects. This trusted third party will also be another server where the user will actually submit his request. The anonymizer performs spatial or temporal cloaking (blurring) to convert a single point into a spatial region. This spatial region along with the set of multiple request object types is submitted to the LBS. Thus, the exact location and query type of the user is shielded from the LBS. The LBS returns a set of candidate results instead of the exact result. Caching is used at the anonymizer in LBS to save communication and computation cost and to preserve privacy for snapshot and continuous queries.

Here they compare their work with other K-anonymity models and proposes their caching model is much more cost effective than other proposed solutions. Their proposed model divides the cache hit events into several parts to improve the computation and communication cost and to preserve user privacy more efficiently. Yet the trusted third party proposed here is another server which processes request over the net.

Paper Title: Cache Management Techniques for Privacy Preserving Location-based Services [9]
Authors: Yu Chen, Jie Bao, Wei-Shinn Ku and Jiun-Long Huang

This paper proposes a cache management technique for improving user privacy protection, saving computation power and decreasing communication cost. This paper also proposes the cache management technique for location based service using trusted server. The fundamental idea behind their methodology is to leverage the cached results from prior spatial queries for answering future queries at the location cloaker. The location cloaker is an intermediate agent which can be trusted by mobile users. The location cloaker receives continuous location updates from mobile users and stores their locations with an index structure. In addition, the location cloaker also anonymizes the location of any query requesting mobile user to a cloaked region before forwarding the query to related location-based service providers. Any user identity related information in the query is also removed by the location cloaker during the cloaking process. They propose if the location cloaker can cache the received query results from service providers, the cached results can be utilized to fulfill new spatial queries from mobile users. By applying this cache based solution, mobile users’ privacy protection can be further improved. Since the location cloaker can solve a certain number of queries without forwarding them to service providers, it would be much more difficult for adversaries to launch correlation attacks.

Paper Title: De-centralized Location Management: Minimizing Privacy Concerns for Location Based Services [10]
Author: Maximilian Zundt, Girija Dee, Mirko Naumann and Dr. Marhs Ludwig

This paper proposes a de-centralized system where location information is directly exchanged and completely controlled by participating peers. Concerning privacy in a decentralized system, the user has full control over his location information: if and when positioning is done, the location data
is generated and controlled at user mobile device and can be provided to a trusted known peer or application service provider of user’s choice.

**Paper Title:** Protection of Location Privacy using Dummies for Location-based Services [11]  
**Author:** Hidetoshi Kido, Yutaka Yanagisawa and Tetsuji Satoh  
**Conference:** 21st International Conference on Data Engineering Workshops, 2005.

This paper proposed to use ‘Dummies’ to protect the location privacy in LBSs. In the proposed technique, a user sends the true location data with dummies, i.e., false location data, to a service provider that will reply with a message for each received location data. The user only extracts the necessary information from the reply messages. In this manner, the service provider cannot tell the true position data, thus leading to the protection of user’s location privacy.

**Paper Title:** A Lightweight Approach to Managing Privacy in Location-Based Services [12]  
**Author:** Tom Rodden, Adrian Friday, Henk Muller and Alan Dix

In this paper, they proposed an approach in which users are allowed to use randomly generated pseudonyms in the control to the access to their location information. The location information, a time stamp and an associated pseudonym is stored at a location server and only the service providers that possess the correct pseudonym can access the location information. Users can change who can access the location information by simply changing the respective pseudonyms associated with the location information.

**References**


p. 372-390.


