



Location-Based Services: Back to the Future

Paolo Bellavista, Axel Küpper, and Sumi Helal

Gainesville, Florida, 10 March 2012. Today, the Mobile Location-Based Services Summit hosted a panel entitled “What Was Wrong with First-Generation Location-Based Services?” The panel chair, Sumi Helal of the University of Florida, invited two world-class experts in LBS history and technology to discuss the topic: Paolo Bellavista of the University of Bologna and Axel Küpper of the University of Munich. The panel discussed the popularity of today’s LBSs and analyzed their distinguishing aspects in comparison with first-generation LBSs.

The panel was anything but controversial, with all panelists in total agreement on what initially went wrong and why today’s LBSs work. They analyzed how the failure unfolded to set the stage for a major paradigm shift in LBS business and technology and noted the milestones that shaped today’s LBSs.

HISTORICAL PERSPECTIVE

The panel opened with a historical overview of LBS evolution, which we quickly review here (see figure 1).

The main origin of LBS was the E911 (Enhanced 911) mandate, which the US government passed in 1996. The mandate was for mobile-network operators to locate emergency callers with prescribed accuracy, so that the operators could deliver a caller’s location to Public Safety Answering Points. Cellular technology couldn’t fulfill these accuracy demands back then, so operators

started enormous efforts to introduce advanced positioning methods.

To gain returns on the E911 investments, operators launched a series of commercial LBSs. In most cases, these consisted of finder services that, on request, delivered to users a list of nearby points of interest, such as restaurants or gas stations. However, most users weren’t interested in this kind of LBS, so many operators quickly phased

**Several significant
developments and
favorable conditions
came together in 2005
to resurrect LBSs.**

out their LBS offerings and stopped related development efforts.

It was 2005 before the LBS wind started blowing again—this time in the right direction. Several significant developments and favorable conditions came together at that time to resurrect LBSs. The emergence of GPS-capable mobile devices, the advent of the Web 2.0 paradigm, and the introduction of 3G broadband wireless services were among the enabling developments. In the meantime, small software and hardware companies realized a broad range of LBS capabilities for both mass and niche markets and laid down the foundation for a new generation of LBSs.

After the quick overview, the panel

identified and extensively analyzed the five primary factors that collectively changed a commercial flop into a pervasive on-the-go service for consumers.

THE EVOLUTION OF LBS FEATURES

Early LBS was reactive, self-referencing, single-target, and content-oriented. This started to change with the maturation of low-power positioning technology (such as assisted GPS), LBS middleware technology, and 3G mobile networks.

In 2004, operators and other providers started offering services for fleet management and for tracking children and pets—these were the first examples of cross-referencing LBSs. Initial versions of these services were based on cell-ID positioning using triangulation techniques, which suffered from low accuracy and were soon replaced by GPS.

With the emergence of GPS-capable mobiles, users started to write small applications passing location data to a central server to make their location available to other users. Soon, these early initiatives turned into professional businesses that created a broad range of proactive and multitarget services—such as for mobile gaming, marketing, and health. These developments were accompanied by Web 2.0: location became another context item exchanged between the members of a social network, which was the origin

STANDARDS & EMERGING TECHNOLOGIES

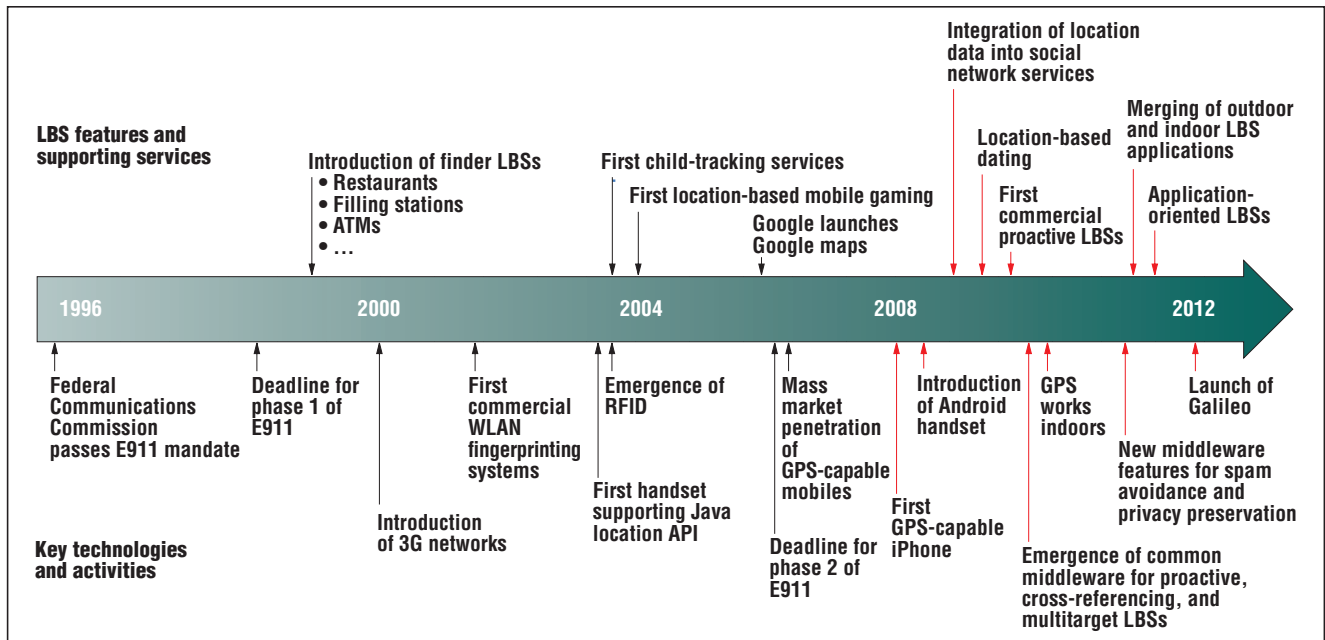


Figure 1. The evolution of location-based services. A timeline from the E911 mandate to current LBSs (the red arrows represent predictions).

for location sharing, a basic function of many of today's multitarget LBSs.

In analyzing rudimentary LBSs compared to today's sophisticated LBSs, the panel identified four major changes that made it so today's LBSs aren't restricted to a few fixed services but instead appear as a broad set of different, dynamic, and feature-rich services that are both exciting and helpful to consumers.

From reactive to proactive

Reactive LBSs are explicitly invoked by the user—for example, a user might request a list of nearby points of interest. Proactive LBSs, instead, are automatically initiated when a predefined event occurs—for example, if the user or a target (another designated person) approaches or leaves a certain point of interest or another target.

Proactive LBSs demand much less user attention and interaction. However, designing and implementing proactive LBSs is more difficult, because the services must continuously track their target and evaluate location events.

From self- to cross-referencing

It's important to distinguish between

the user, who requests and consumes an LBS, and a target, whose location is requested for LBS provisioning. Self-referencing LBSs are services in which the user and target coincide, while cross-referencing LBSs exploit the target location for service-provisioning of another user, thus requiring stronger privacy protection. In particular, targets should be able to restrict access to their location data to a limited and well-defined group of users.

From single- to multitarget

Another relevant classification concerns the number of targets participating in an LBS session. In single-target LBSs, the major focus is on tracking one target's position, which is usually displayed on a map or in relation to nearby points of interest. In multitarget LBSs, the focus is more on interrelating the positions of several targets among each other. Nowadays, LBSs detect the proximity of multiple targets.¹

From content- to application-oriented

Content orientation occurs when LBSs aim to deliver relevant information

depending on users' locations. Examples are a list of points of interest, maps, or information about nearby sightseeing. These LBSs are usually part of applications specialized in content delivery, such as a web browser or a front end for SMS messages.

Today's LBSs offer applications tailored to the user and delivered dynamically on the basis of current location and execution context. Unlike over-the-air downloadable applications, which tend to take time and effort to install and uninstall, the delivery of such dynamic applications is impromptu. In contrast to content-oriented LBSs, application-oriented LBSs provide a more powerful and richer interaction model, with autonomic installation and removal of dynamically needed components. This undoubtedly improves the overall user experience.²

TOWARD USER CENTRICITY

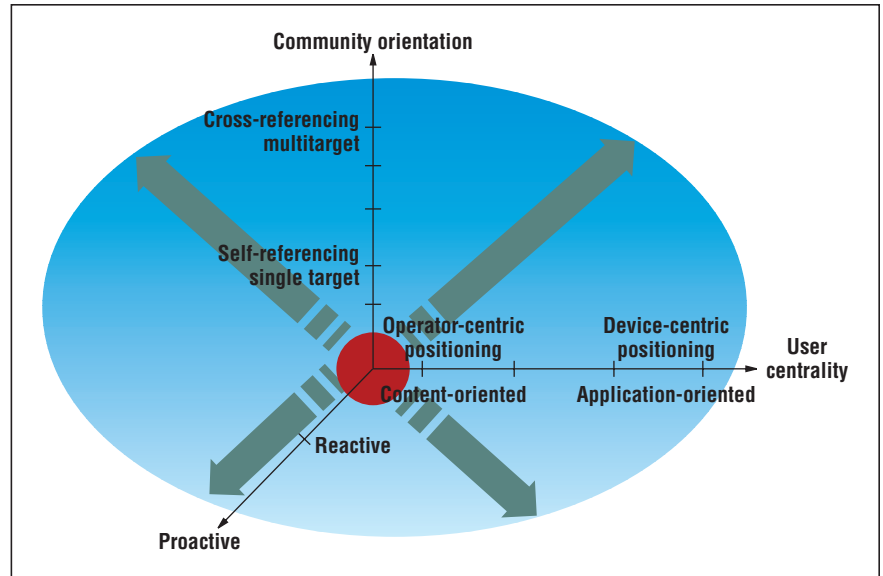
By analyzing a posteriori the history of LBSs, the panel recognized that a primary factor that slowed LBS acceptance and diffusion was the network operator-centric management of location data. On the one hand, initial

Figure 2. The “Big Bang” of LBS. The LBS explosion occurred through proactivity, community orientation, and user centrality.

localization solutions for LBSs adopted the idea that telecom operators were the primary actor for positioning their clients (infrastructure-centric localization) and for owning and privately handling that valuable information. On the other hand, and partially as a consequence of that approach, LBS provisioning was considered an exclusive property of telecom operators. In other words, the overall LBS management process (both location-data extraction and LBS content provisioning) was operator centric. End users and their client devices were expected to be unaware passive entities in the processes of localization and LBS provisioning. A major factor in LBS's success was the shift of both ownership and management of location data from being operator centric to user centric.

The demand for user-centric LBSs, driven by the users themselves to enable the effective exchange of user-generated content among peers, called for terminal-based localization estimation and user-centric management of location data. Such demands led to innovations in terminal-based localization techniques that can exploit different positioning systems or techniques provided by other nearby terminals, in a completely decentralized and unplanned fashion.

The cost reduction in external positioning systems (such as GPS) and heterogeneous wireless interfaces (such as Wi-Fi, Bluetooth, infrared, and the Universal Mobile Telecommunications System) provided mobile devices with several ways to gather location data. This has required novel middleware solutions to properly and autonomously integrate and switch between different localization solutions—even those that are simultaneously available—such as from GPS to terminal-based position estimation via Wi-Fi fingerprinting.³ However, this has enabled cheap, anytime anywhere positioning in both



outdoor and indoor environments. Research efforts to specify standardized APIs for heterogeneous positioning-system management, such as the JSR-179 Location API for J2ME, positively contributed to this evolution.⁴

At the same time, the effectiveness of terminal-based localization techniques has favored the wave of user-owned localization data. Letting clients determine the visibility of their positioning data indirectly increased users' confidence in LBSs. Users became less reluctant to let other selected users trace their movements by activating local positioning. They felt comfortable with the idea of personally deciding to which (types of) services to reveal their position, on a case-by-case basis and with variable levels of details. Empowering users over the operator has reduced privacy concerns, compared to letting operators determine and export (even sell) user locations in first-generation LBSs.

Terminal-based positioning has also led to the widening of the LBS market to a new breed of service providers that aren't telecom operators, thus leveraging the rapid development of a critical mass of differentiated LBSs. This crucial change opened the arena to a variety of companies, including those with more agile business models.

Figure 2 concisely depicts the most

relevant evolutionary directions that have determined the explosion of current LBSs in terms of market relevance and users' acceptance.

MIDDLEWARE FOR OPENING LBS PARTICIPATION

The emergence of service discovery and delivery middleware as well as open mobile platforms—such as Google's Android (code.google.com/android) and the Linux Openmoko project (www.openmoko.org)—have completely changed the LBS equation. Today, the vast majority of LBS providers are businesses and industries that aren't telecom operators. The middleware and open platforms have shifted LBS ownership, letting any business use simple tools and commodity-hosting services to author, publish, and self-manage their own notions of LBS. This yawning participation by the masses of businesses around the world has bolstered the business model and the profitability of LBSs for all.

Contrast this accomplishment with the early LBS business model, in which telecom operators and large content providers teamed up to offer LBSs. For example, Microsoft MSN and Verizon Wireless joined forces in 2002 to create a “groundbreaking” alliance to offer LBS to Verizon Wireless subscribers.

STANDARDS & EMERGING TECHNOLOGIES

The alliance was heavily advertised but failed to result in a killer application or serious profits.

Looking back, it makes perfect sense that LBS, by nature, can't be owned, managed, or envisioned by a few participants, no matter how large they are. Opening up the participation has clearly proliferated the concept itself and easily and quietly created millions of LBSs that are distributed, autonomous, and well maintained by their individual owners, including numerous small companies.

MIDDLEWARE FOR AVOIDING LBS SPAM

LBSs are inherently proactive and advertising oriented, which has helped their success. To ensure that users receive only location-dependent messages of genuine interest, researchers developed effective context-aware middleware to automatically filter out the LBS content that end users perceived as spam. Using such middleware has contributed to maintaining and even improving users' confidence in both disclosing location data and subscribing to a growing number of LBSs.

From a technical viewpoint, middleware for LBS spam avoidance required advanced and effective solutions to

- handle a large range of heterogeneous user contexts (for example, preference profiles and session history),
- allow interoperability with statically unknown LBS providers, and
- efficiently enable simple forms of semantic-based matching between contexts and service characteristics.

So, it was crucial to adopt middleware design guidelines based on dynamically deployable proxies, running on the infrastructure side and in client vicinity. Proxies act on behalf of their possibly limited client devices and maintain and process groups of user contexts in a scalable way. The proxies achieve scalability by exploiting the dynamic structuring of client groups in

hierarchical clusters based on locality. In addition, advanced techniques for predicting client movements and network handoffs enabled the middleware solutions to anticipate the dissemination of user contexts to next-visited wireless domains.

Open networking with LBSs was enabled by the wide adoption of standard XML-based descriptions for representing user preferences, device characteristics, local resource availability, and service properties and requirements. Standardization efforts—such as W3C CC/PP (World Wide Web Consortium Composite Capabilities/

Looking back, it makes perfect sense that LBSs, by nature, can't be owned, managed, or envisioned by a few participants, no matter how large they are.

Preference Profiles), Session Initiation, and Context Transfer Protocols—were central to inducing LBS providers to standardize their ways of maintaining and exchanging context.⁵ In addition, the availability of standard APIs for context access and manipulation, such as in Google Android, facilitated a uniform approach for different LBS providers, thus increasing cost effectiveness and reducing time to market.

Finally, semantic-based techniques enabled real interworking with statically unknown LBSs. For example, simple reasoning on context descriptions let the middleware identify content of interest—for example, by matching user interests and LBS properties even when the two were expressed with different terms. Shared ontologies, which associate terms through semantic relationships, made this possible.

MIDDLEWARE FOR PRIVACY PRESERVATION

A target's current location (or the locations a user has visited in the past) is

sensitive data that other actors in the LBS value chain could misuse—for criminal intent or to analyze target behaviors to personalize special offers and advertisements. When LBSs first appeared, there was basically no public discussion about potential misuse scenarios. At that time, LBSs represented only a small niche market, and many users viewed the mobile-network operators, which controlled the entire value chain, as trusted entities. However, the situation rapidly changed after the widespread diffusion of LBSs. Suddenly, there was a broad discussion about LBS privacy risks: many countries adapted their privacy laws accordingly or passed new ones, while LBS providers adopted novel technical solutions to enforce privacy protection.

One technical solution was *dynamic trust management*—the development of novel, effective, and lightweight mechanisms to dynamically establish trust relationships with not only centralized but also peer-to-peer entities (to which clients disclose their location at runtime). In traditional LBSs, the need for centralized authentication authorities significantly reduced the potential of “anytime, anywhere” service provisioning; it was always necessary to use Internet connectivity to reach a trusted and wired authentication authority for the relatively long process of LBS provider credential checking. Autonomous and disconnection-robust trust management based on peer-to-peer dynamic trust chains (credential-based, reputation-based, and social-network-based) have been a good fit for user-centric LBS-provisioning scenarios.

Another solution was *user-controlled privacy policies*. The shift toward a user-centric approach simplified, to some extent, the issue of location privacy preservation, by letting users directly manage their location data and decide whether and with what granularity level (city, street, building, or room number) to disclose them to LBSs. User-controlled privacy policies can be suitably defined depending on

runtime context evaluation and LBS permissions, possibly defined after negotiation with the user.

Pseudonymization is another technique that LBS providers used for a while. Instead of disclosing a user's location with his or her true identity, a pseudonym was attached to the user's location. However, LBS providers quickly realized that this approach was risky if an attacker (such as a non-trusted LBS) has some background information, like the target's residence and working place: comparing these locations with the collected stock of pseudonymized data would make depseudonymization easily possible.

To counteract depseudonymization, researchers have proposed many mechanisms, from mix zones to data obfuscation. Unfortunately, all of them are difficult to implement effectively. In addition, to enable authority-driven lawful interception, several countries recently prohibited pseudonymization. In fact, pseudonymization remained a theoretical approach and never achieved any practical significance for LBSs, where trust management and user-controlled policies were considered sufficient for privacy protection.

Notably, legitimate users of a cross-referencing or multitarget LBS could also violate a target's privacy. The situation is similar to the emergence of mobile handsets in the 1990s, when many people were suddenly confronted with the reality of always being available to their spouses, relatives, colleagues, and so forth. LBSs go one step further by providing your location, and denying location requests is like turning off your cell phone—there's a kind of social pressure to always be available.

Because this pressure endangered the success of LBSs, the majority of LBS providers released a voluntary agreement in 2011 that contains rules for designing privacy-compliant LBSs. Apart from trust management and policy frameworks, the agreement recommends implementing *plausible*

deniability and *reciprocal exchange of location data*.⁶ Plausible deniability means that location attempts must be deniable without reporting the reason of failure; hence, the requesting user doesn't know whether the target denied his or her request or a technical error occurred. Reciprocal exchange of location data means that LBSs must be designed symmetrically. For example, a user requesting a target location must disclose his or her location to the target with an analogous granularity level.

You can't look back at how the concept of LBS evolved and not be impressed with the power of ubiquity and pervasiveness. The people and businesses were a missing infrastructure that had to be added to the telecom operators; it was a big mistake limiting their participation to only target customers and service payees. ■

REFERENCES

1. A. Küpper, G. Treu, and C. Linnhoff-Popien, "TraX: A Device-Centric Middleware Framework for Location-Based Services," *IEEE Comm. Magazine*, vol. 44, no. 9, 2006, pp. 114–120.
2. C. Lee, A. Helal, and D. Nordstedt, "The µJini Proxy Architecture for Impromptu Mobile Service Access," *Proc. 2006 Int'l Symp. Applications and the Internet Workshops (SAINT 2006 Workshops)*, IEEE CS Press, 2006, pp. 113–117.
3. P. Bellavista, A. Corradi, and C. Giannelli, "Coupling Transparency and Visibility: A Translucent Middleware Approach for Positioning System Integration and Management (PoSIM)," *Proc. Int'l Symp. Wireless Communication Systems (ISWCS 06)*, IEEE Press, 2006, pp. 179–184.
4. Java Community Process, *JSR179 Location API for J2ME*, <http://jcp.org/aboutJava/communityprocess/final/jsr179>.
5. K. Rehman, F. Stajano, and G. Courlouris, "An Architecture for Interactive Context-Aware Applications," *IEEE Pervasive Computing*, vol. 6, no. 1, 2007, pp. 73–80.
6. G. Treu, F. Fuchs, and C. Dargatz, "Implicit Authorization for Social Location Disclosure," *J. Software*, vol. 3, no. 1, 2008, pp. 18–26.

Paolo Bellavista is an associate professor at the University of Bologna. Contact him at pbellavista@deis.unibo.it.




Axel Küpper is a research assistant in the Mobile and Distributed Systems Group at the Ludwig Maximilian University Munich. Contact him at axel.kuepper@ifi.lmu.de.




Sumi Helal is a professor in the Computer and Information Science and Engineering department at the University of Florida. Contact him at helal@cise.ufl.edu.

Visit



on the Web



www.computer.org/pervasive