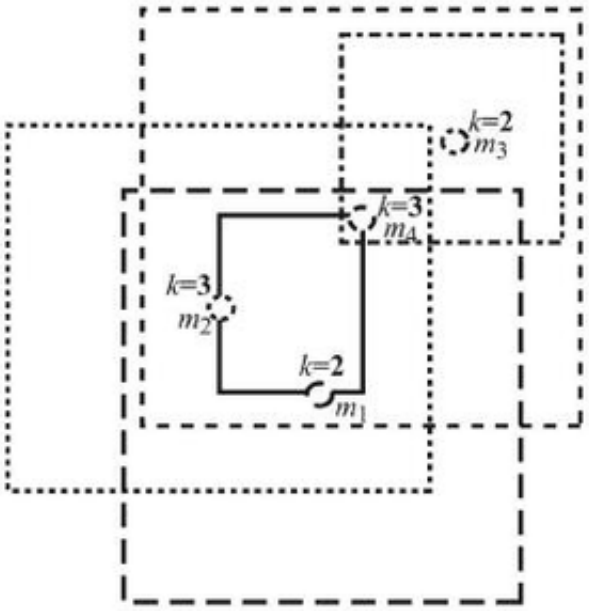
New Technology Combines GPS Benefits with Privacy Protection

December 11 2007, By Lisa Zyga



This spatial layout shows how four messages relate to each other, with messages 1, 2, and 4 included in the same cloaking box (solid rectangle) in order to blur the identities of the users. Credit: Bugra Gedik and Ling Liu. ©2007 IEEE.

As GPS and other wireless location-based technologies are becoming prevalent on cell phones and other everyday devices, two researchers are thinking about the social reaction to constant surveillance. As George Orwell envisioned, a world in which everyone is being watched opens the doors for privacy abuse and totalitarian control.

Computer scientists Bugra Gedik and Ling Liu explain that, while an Orwellian society is not right around the corner, location-based technologies have already raised major personal privacy issues. One case in point is DARPA's LifeLog project, "a massive electronic database of every activity and relationship a person engages in," which was recently scrapped due to privacy concerns.

Gedik, a researcher at the IBM T.J. Watson Research Center, and Liu, an associate professor at the Georgia Institute of Technology, have recently developed a new technology that could protect cell phone and mobile device users from privacy abuse, while still enabling them to enjoy the benefits that location-based technologies have to offer.

"We need to devise a location anonymization architecture that is both scalable in terms of achieving high anonymization success rate and high accuracy, and robust in terms of protecting users from vulnerabilities and threats of misuse and abuse of their location information," Liu told *PhysOrg.com*, explaining one of the major challenges of developing a location privacy protection system.

While previous attempts at location privacy applications have been made, Gedik and Liu's system is the first to enable individuals to choose the level of anonymity for different applications, while still providing nearly optimal performance. For example, a cell phone user could send a request for a local gas station offering the most inexpensive gas to a "location-based services" (LBS) provider, and receive an accurate answer even without the provider knowing exactly where the user is located.

Without knowing a user's location, it would also be impossible for an LBS provider to determine with certainty a user's identity when using the protective system. This protection is important since, using only location information, curious or malicious providers could conceivably determine

information such as a user's political affiliations, alternative lifestyles, medical problems or the private businesses of an organization such as new business initiatives and partnerships, the researchers explained.

The new system uses an anonymity-based approach called "location k-anonymity." A user is considered to be location k-anonymous if their location information sent to the LBS provider is indistinguishable from the location information of at least k – 1 other users. In tests, the researchers experimented with k values from 2 to 12, with higher values meaning increased privacy, but also longer search times. In real life, different users could choose different k values for different applications based on their personalized privacy requirements, but the researchers predicted that even the most privacy-conscious users would be satisfied with a k value of 5.

"Most of the privacy-preserving algorithms today work with a system-defined fixed k for all users, and we argue that 'one-size-fits-all' k-anonymization approaches are not efficient," Gedik explained. "Our system is the first one to develop a personalized location anonymization model for a wide range of users with context-sensitive privacy requirements, while maintaining high accuracy through optimal location anonymization."

Whenever the system receives a message, an algorithm searches for other messages coming from the same general area, and then groups together k or more messages in a geographical rectangle encompassing all the messages. For tuning the system level parameters to obtain close-to-optimal accuracy in practice, the system uses a "trace generator," which simulates cars moving on roads based on real-world road data.

After the messages are anonymized in this way, the system forwards them to the external LBS providers. In tests, the system processed 50% of messages in less than five seconds, and 75% in less than 10 seconds.

Further, the personalized location k-anonymity model had a high success rate, with only about 10% of messages being dropped due to algorithm shortcomings, such as the inability to find other messages sent within the same location.

The scientists will continue working on improving the algorithm, and also studying the quality of location-based services when used under the privacy algorithm in real-world situations.

“Our location privacy project is progressing along three dimensions,” Liu explained. “First, we are working on ways to combine policy-based privacy specification and enforcement with anonymous usage of location information for protecting the location privacy of users and organizations. Second, we are interested in developing a privacy-conscious mobile community for different classes of applications. Third, we are interested in studying different location anonymization techniques in terms of both their ability to balance the level of privacy guarantees and the quality of service, and their resilience to various location-based inference attacks.“

This location privacy project is currently funded by the NSF Cybertrust program.

More information: Gedik, Bugra, and Liu, Ling. “Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. *IEEE Transactions on Mobile Computing*, Vol. 7, No. 1, January 2008.