Wireless Location Privacy Protection

Bill Schilit, Intel Research
Jason Hong, University of California, Berkeley
Marco Gruteser, University of Colorado at Boulder

After more than two decades of hype, computing and communication technologies are finally converging. Java-enabled cell phones run a host of powerful applications including mobile Internet access, while many notebook computers offer high-speed wireless connectivity as a standard feature. The big decision when purchasing a PDA this holiday season is whether to get integrated cellular service or Wi-Fi capability.

Location-based services are emerging as the next killer app in personal wireless devices, but there are few safeguards on location privacy. In fact, the demand for improved public safety is pushing regulation in the opposite direction.

Today, when a person reports an emergency from a landline phone by dialing 911 in the United States or 112 in Europe, the system displays the caller's phone number and address to the dispatcher. The US Federal Communications Commission has mandated that, by December 2005, all cellular carriers be able to identify the location of emergency callers using mobile phones to within 50 to 100 meters (www.fcc.gov/911/enhanced/). In July 2003, the European Commission recommended rapid deployment of a similar location-enhanced 112 service.

However, how cellular carriers and other businesses will use this capability remains open to question. The Wireless Privacy Protection Act of 2003 (www.theorator.com/bills108/hr71.html), currently under consideration by the US Congress, proposes to amend the Communications Act of 1934 "to require customer consent to the provision of wireless call location information." However, commercial entities are adept at concealing questionable practices with fine print in a service contract or click-wrap agreement.

Positioning technologies have the potential to intrude on personal privacy.

PRIVACY RISKS

In practice, privacy is a malleable concept based on societal perceptions of risk and benefit. For example, people routinely use a credit card to buy goods and services on the Internet because they believe that the convenience of online purchases outweighs the potential cost of such transaction data being misused.

The challenge with wireless location privacy is making it easy to share the right information with the right people or service at the right time and, conversely, being able to opt out at will. Exchanging location information with friends and family or knowing whether a nearby store is having a sale on a product you want can be helpful. However, wireless location-based technologies also present several risks to privacy.

Economic damages

Information about a person's movements or activities can result in financial losses. In one highly publicized case two years ago, a Connecticut rental car company that equipped its vehicles with Global Positioning System devices fined a customer $450 for speeding on three occasions after tracking his van (http://news.com.com/2100-1040-268747.html). Although the rental contract included a warning that speeding would result in additional fees, the driver successfully sued the company for failing to adequately explain how it used the location-tracking system.

Some losses, however, are far more difficult to substantiate in court. For example, it would be hard to prove that a company failed to promote, fired, or discriminated against an employee because it had used some location-based technology to determine that the person visited a drug rehabilitation clinic.

Location-based spam

In addition, the corporate world can discover and match a person's location trail to create unwelcome spam. For example, cybermarketers could bombard a mobile device with customized voice and data ads for stores, restau-

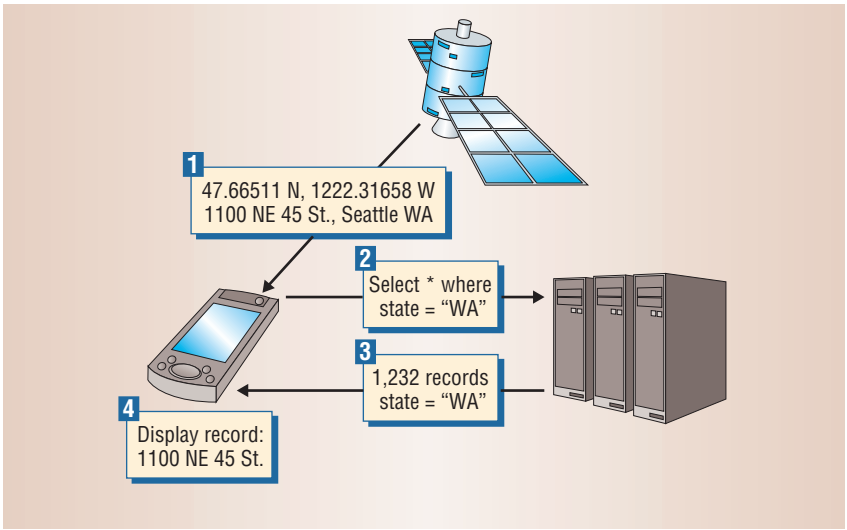

Figure 1. Intermittent connectivity for privacy. To avoid revealing precise location information to network services, mobile devices retrieve geographically coded records one set at a time rather than individually through separate queries.

rants, and other businesses as an individual strolls through a mall. It is reasonable to imagine that companies that buy and sell mailing and telephone lists may also trade in location traces.

Harm to a reputation

Finally, disclosure of location information may cause personal embarrassment or humiliation—for example, by exposing a diet doctor's tendency to frequent fast-food restaurants or a family-values politician's regular visits to an adult video rental business. In some cases, such revelations can lead to tragic consequences including resignation, ostracism, or even suicide.

If taken out of context, location information could also lead others to make incorrect inferences that unjustly tarnish a person's reputation. For example, imagine a husband who, at his boss's insistence, had a few drinks at a nightclub and then tries to explain his whereabouts—revealed through cell phone activity—to his spouse.

PROTECTING PRIVACY

Positioning systems fall into one of three categories. In the *network-based* approach, infrastructure receivers such as cell towers track cellular handsets or other mobile transmitting units. In the *networked-assisted* approach, location determination occurs in the network with the mobile device's active participation—for example, Qualcomm's Enhanced 911 solution uses handsets to receive raw GPS satellite data that it sends to network processors for calculation. In the *client-based* approach, mobile devices autonomously compute their own position, as is the case with a GPS unit.

In terms of privacy, client-based positioning is fundamentally better than network-based or network-assisted tracking because it does not reveal any location information to the network unless the user decides to communicate. Along with other researchers, we are exploring how computationally powerful clients with positioning capabilities can be the foundation for location privacy. For example, preloading a mobile device with the Zagat's restaurant guide or an airline schedule would enable users to access the cached local information without revealing their location.

Intermittent connectivity

Ideally there is a middle ground between operating while disconnected from the communications network and potentially revealing location information with each query to a network service. In this area, we are exploring ways to apply previous distributed systems research on intermittently connected databases to privacy rather than availability.

For example, Figure 1 shows a model in which mobile devices avoid revealing precise location information by retrieving geographically coded records one set at a time rather than individually through separate queries. *Intermittent connectivity* is a powerful mechanism, but it is only useful for specific kinds of services in which data changes relatively slowly.

User interfaces

Another area of research is the design of user interfaces to support location queries on mobile devices. For example, a GUI widget for a location-based tour guide service could show end users whether they are currently sharing location information for a particular city, neighborhood, or street and what services they are receiving in return—for example, nearby interesting shops or real-time maps.

Such interfaces should include mechanisms that require clients to provide greater feedback about who is requesting location data. In many cases, simple notifications are sufficient to prevent abuses. For example, Alice is less likely to repeatedly query Bob's location if she knows that Bob can see each of her requests.

Network privacy

Managing privacy in the network is one of the more challenging aspects of wireless location privacy. Although major network providers such as cellular phone carriers may be trustworthy, Wi-Fi wireless networks and hot spots are based on the Internet protocol, for which TraceRoute and other tools can expose packet routes and therefore source location.

The mobile IP community recognizes this vulnerability and has enumerated

a number of solutions including using fixed home agents through which clients communicate with all services. Such agents hide location just as Internet services such as Anonymizer.com hide identity.

A project at the University of Colorado at Boulder used a *trusted location cloaking proxy* to hide precise location information from network services (http://systems.cs.colorado.edu/Papers/Generated/2003anonymousLbs.html). This approach provides anonymity by adjusting the resolution reported to such services based on the density of users in a region.

Figure 2 shows an automotive application in which the proxy provides *k*-anonymity by revealing a wireless device's location to a resolution that includes $k - 1$ other users. The yellow dot represents a vehicle with a wireless device connected to an untrusted service through the cloaking proxy, while the black dots represent other vehicles in the area.

The proxy runs a cloaking algorithm that selects the smallest of a set of regions that includes the vehicle equipped with the device and at least $k - 1$ other vehicles and reports this to the service. In this way, the untrusted service cannot easily map the reported location back to an individual vehicle.

A number of organizations, including the Internet Engineering Task Force, recognize the need for location privacy standards. Geopriv (www.ietf.org/html.charters/geopriv-charter.html), an IETF working group examining some of the risks associated with location-based services, has proposed several requirements for location privacy, including limited identifiability and customizable rules for controlling how data flows. A separate threat analysis considers how hackers and companies might subvert the system and ways to manage these threats.

Technological means alone cannot manage location privacy; legislation, corporate policy, and social norms will eventually dictate the use of wireless location information. In the meantime, researchers must provide strong and secure models to ensure that privacy is both a feasible and desirable component of future location-capable personal wireless devices. ■

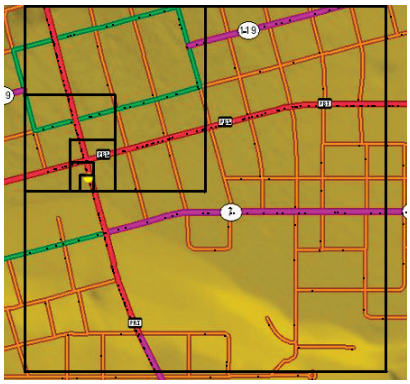

Figure 2. Trusted network cloaking proxy. The proxy runs a cloaking algorithm that selects the smallest of a set of regions (black squares) that includes the vehicle equipped with the wireless device (yellow dot) and at least k – 1 other vehicles (black dots).

Bill Schilit *is codirector of Intel Research Seattle. Contact him at bill.schilit@intel.com.*

Jason Hong *is a PhD candidate in the Computer Science Division at the University of California, Berkeley. Contact him at jasonh@cs.berkeley.edu.*

Marco Gruteser *is a PhD candidate in the Department of Computer Science at the University of Colorado at Boulder. Contact him at gruteser@colorado.edu.*

Editor: Bill N. Schilit, Intel Research Seattle; bill.schilit@intel.com