An Infrastructure for Location Aware Computing

Albert Huang ALBERT@CSAIL.MIT.EDU
Larry Rudolph RUDOLPH@CSAIL.MIT.EDU
MIT Computer Science and Artificial Intelligence Laboratory, 200 Technology Square, Cambridge MA, 02139 USA

1. Introduction

We present a low cost and easily deployed infrastructure for location aware computing that is built using standard bluetooth® technologies and personal computers. Mobile devices are able to determine their location to room-level granularity with existing bluetooth technology, and to even greater resolution with the use of the recently adopted bluetooth 1.2 specification, all while maintaining complete anonymity. The system is trivial to implement on a large scale - our network covering 5,000 square meters was deployed by a single student over the course of a few days at a cost of less than US$1,000.

Location aware computing provides applications with knowledge of the physical location where the computation is taking place. This allows applications to operate in a more context-sensitive fashion. Fundamental to location aware computing is the task of determining the location of the computational device. In outdoor environments with unobstructed views, GPS(Getting, 1993) is widely used for this purpose. Indoors, and in crowded city streets, however, the effectiveness of GPS is greatly diminished. A number of approaches have been made towards indoor localization, with varying features and measures of success. We present a system that provides an infrastructure for location aware computing that emphasizes the following key features.

Cost The system must not be prohibitively expensive, and its costs should scale well with its size.

Privacy Previous studies(Barkhuus & Dey, 2003) find that privacy is a significant concern in ubiquitous computing. A location aware system should preserve the privacy of its users. Users should be able to choose whether or not to reveal their location and identity to others, and should not be actively tracked without explicit consent. It should not be *possible* for the system to track users without permission.

Deployment Our system relies on technology that is already widely available and in use today. The hardware is multi-purpose and can be used for a variety of other computing tasks when not being used for localization purposes. Many potential users of our system would not need a significant investment in capital or other resources to take advantage of our infrastructure. Additionally, the system is simple and almost trivial to deploy on a large scale.

2. Motivation

The ability to automatically determine the physical location of a computation device makes possible a host of new applications. We describe a few such conceptual applications here.

Visitors to a large complex who are unfamiliar with the local area can be given a handheld navigational unit that guides them about the area. The navigational units display their location in real time, providing turn-by-turn instructions on how to reach their destination. Such a system could easily be used in tourist attractions, museums, hospitals, and industrial complexes. Visitors equipped with bluetooth cell phones or PDAs would not even require additional hardware, and could simply download a software client.

A software agent running on an individual's cell phone or PDA periodically determines its location. As the user moves about during the day, the agent can alert the user to perform certain tasks in certain places (e.g. buy a screwdriver at the hardware store or make some photocopies at the office). While the user would have to input these tasks, he would no longer be required to actively check and see if anything needs to be done in a particular location. Instead, he is simply notified when action is required.

A network of information kiosks(Van Kleek, 2003), which provide context sensitive information, could leverage a location-aware infrastructure to automatically configure its components, thus lowering the cost and complexity of deployment. The kiosks display information relevant to their particular location (e.g. weather, talks, movies, unannounced fire alarm testings), all without any manual configuration.

All of these examples share the common attribute of a computational device that is aware of its current location. In order for this to happen, an infrastructure must be in place that assists the device in this purpose. It is the infrastructure that makes all of the applications possible.

3. Related Work

A variety of systems have been developed for use in location aware computing. The Active Bat System(Harter et al., 2002) uses a combination of ultrasound and radio transmissions to actively track its users. Cricket(Priyantha et al., 2000) also uses ultrasound and RF, but allows its users to hide their location, preventing the system from tracking them. Both Cricket and Active Bat have the advantage of sub-meter level granularity, and the drawback of being prohibitively expensive to deploy on a large scale. 802.11 based systems have also been developed, one of which(Ladd et al., 2002) uses bayesian inference techniques to estimate location. This system suffers from the need for intensive training of the bayesian network, however, and does not scale well. Anastasi et al(Anastasi et al., 2003) have experimented with an indoor bluetooth system that uses a central database to track its users. We believe a privacy-respecting system should not track its users, as there is great potential for abuse when it does.

4. System Overview

Thirty D-Link DBT-120 USB Bluetooth Adapters (firmware version 1.4.2.10) were purchased for US$30 each, to be used as beacons. Research groups in our building were asked to spare a single USB port in their computers. Our beacons were then placed in computers approximately every 10 meters on six different floors. The only software installed on the hosting machines were the device drivers. On average, configuring a machine to host one of our beacons took less than three minutes. The most time consuming part of the deployment was actually tracking down the administrators of the machines we wanted to use, and obtaining their permission[1].

By taking advantage of an existing computational infrastructure, we were able to deploy our system on a building-wide scale with a minimal investment of capital and labor. We did not need to mount any hardware in special places, run cables, or displace any existing equipment or furniture. The only physical change to the environment needed was the addition of 30 small USB devices. While our system was tailored for an environment densely populated with personal computers, it could also be deployed in other areas such as sports arenas and shopping centers as long as suitable bluetooth devices are used[2]

Client software must be loaded onto a device before it is able to take advantage of our network. We wrote a linux client, and a Nokia Series 60 client. The linux client was used on laptops, desktops, and HP iPAQ 5550 Pocket PCs running the Familiar distribution of linux. The Nokia Series 60 client was used on Nokia 3650 and Nokia 6600 cellular phones. The client software was a simple demonstration program that determined its physical location, and displayed a map of the surrounding area, highlighting the predicted location of the mobile device.

Once the beacons are in place, there are three steps that a mobile device (locator) must take to determine its own location.

1. The locator scans for beacons by performing a bluetooth device inquiry. This involves repeatedly broadcasting a predefined sequence of bits while hopping frequencies pseudorandomly. The broadcast contains no content which can be used to identify the locator. Beacons that detect the broadcast will reply with their own identities.

2. The locator determines the location of detected beacons. A cache is maintained, mapping beacon identities to their locations. If a beacon is not present in the cache, then the locator can query the beacon directly at the cost of anonymity.

3. The locator determines its location relative to the detected beacons. If only one beacon is detected, the locator can conclude it is within 10 meters of the beacon. With multiple beacons, simple geometry can be used to refine the estimate. If privacy is not a concern, then a connection to the beacons can be established, and the locator can use link quality measurements to obtain more precise positioning data. In the newer bluetooth 1.2 standard, the locator can obtain signal strength measurements without establishing a connection to the beacons, allowing it to retain its anonymity.

5. Optimizations

Some bluetooth devices support the ability to report signal strength and link quality of a connection with another device. These attributes degrade with distance, and statistical inference techniques can be used to determine the distance to a beacon with greater precision.

We have experimented with the use of multiple co-located

[1] Ironically, despite being a hub of research in computer science, many lab members had no idea what bluetooth is and does, or how it would affect their computer. One researcher whose computer was not hosting a beacon expressed sincere concern that nearby bluetooth devices would introduce security vulnerabilities on his workstation.

[2] To date, we have not found a low-cost, widely available commercial bluetooth device that is suitable for this purpose. However, we believe that current manufacturing processes could easily and inexpensively mass produce such a device if interest arose.

bluetooth devices to form a single beacon. When the locator performs a device inquiry, it is more likely to receive a response in a shorter amount of time when two bluetooth devices are present instead of only one, and thus is able to determine its position more quickly. Similarly, we can also increase the density of the bluetooth devices in an area to provide more precise positioning estimates.

We also introduce an algorithm for rapidly determining the position of the locator in the presence of unknown bluetooth devices, one of which is a beacon. This algorithm is described in detail in (Huang & Rudolph, 2004)

6. Discussion

Effectiveness The locators are much more effective in areas densely populated with beacons. Applying simple geometry, the resolution of the locator is directly related to the number of beacons it can detect. When more than a couple beacons are detected, the locator can determine which room it is in with a high level of accuracy. In areas with few beacons, however, the locator is only not able to achieve this resolution. While high resolution is a desirable feature, room-level resolution is sufficient for all of the applications mentioned earlier.

Maintenance The most significant problem with our infrastructure so far has been maintenance. The most common problems are machines being moved, taken offline, or upgraded and reformatted with a new operating system. Since each research area administers its own computer systems, it is difficult to keep track of every single bluetooth device we install. We attribute this difficulty to the lack of a central point of administration in our computer systems, and believe maintenance would be significantly easier in an environment where more machines are administered by fewer people, as is usually the case in industrial organizations and smaller institutions. After three months of deployment, eight out of the original 30 beacons in our network were rendered ineffective due to one of these reasons. If a suitable bluetooth device were found that could as a standalone unit, maintenance would also be easier, as the beacons would not be dependent on the surrounding computers.

Security Currently, the infrastructure is susceptible to a simple spoofing attack, whereby a rogue bluetooth device could simply be given a name that matches our naming scheme. If the locator operates entirely out of its cache, however, then spoofing a beacon becomes more difficult, as the spoofing device would need to spoof its bluetooth address. We currently do not address this concern, as spoofing a beacon requires the physical presence of a device and once detected, could be easily removed.

7. Future Work

At the time of this writing, there are no bluetooth 1.2 compliant devices commercially available on the market. Once devices are available, we plan on investigating the usefulness of the additional signal strength features.

Application of noisy inference techniques to the localization problem in our system is also an area that merits further investigation. There are a number of users for whom privacy concerns are not an issue that would benefit from the use of these methods.

We have plans to increase the coverage and density of our network, and deploy more precise client software. Integration with other location aware applications is also planned.

References

Anastasi, G., Bandelloni, R., Conti, M., Demastro, F., Gregori, E., & Mainetto, G. (2003). Experimenting an indoor bluetooth-based positioning service. *Proceedings of the International Conference on Distributed Computing Systems Workshops* (pp. 480–483).

Barkhuus, L., & Dey, A. (2003). Location-based services for mobile telephony: a study of users' privacy concerns. *Proceedings of Interact 2003* (pp. 709–712). Zurich, Switzerland.

Getting, I. A. (1993). The global positioning system. *IEEE Spectrum*, *30*, 36–47.

Harter, A., Hopper, A., Steggles, P., Ward, A., & Webster, P. (2002). The anatomy of a context-aware application. *Wirel. Netw.*, *8*, 187–197.

Huang, A., & Rudolph, L. (2004). A privacy conscious bluetooth infrastructure for location aware computing. Unpublished.

Ladd, A. M., Bekris, K. E., Rudys, A., Kavraki, L. E., Wallach, D. S., & Marceau, G. (2002). Robotics-based location sensing using wireless ethernet. *Proceedings of the 8th annual international conference on Mobile computing and networking* (pp. 227–238).

Priyantha, N. B., Chakraborty, A., & Balakrishnan, H. (2000). The cricket location-support system. *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 32–43).

Van Kleek, M. (2003). Intelligent environments for informal public spaces: the Ki/o Kiosk Platform. M.Eng. Thesis, Massachusetts Institute of Technology, Cambridge, MA.