The Locust Swarm: An environmentally-powered, networkless location and messaging system

D. Kirsch and T. Starner
Room E15-383, The Media Laboratory
Massachusetts Institute of Technology
20 Ames Street, Cambridge MA 02139
zuul,thad@media.mit.edu

Abstract

The Locust infared system provides location information and messaging without batteries and without its own network. The system is "privacy aware" in that it supplies information to the wearable computer user who can then control how much of this information is shared with others or the installed infrastructure. By combining the abilities of Locusts with an appropriately equipped wearable computer, the user can interact with web-like hyperlinks, graphics, and sounds virtually associated with objects in the physical world. In addition the user can annotate and change these links as desired.

1 The Need for an Indoor Location System

The U.S. military's satellite-based Global Positioning System (GPS) can provide meter precision position information anywhere on the planet. Unfortunately, the radio frequencies used prevent the system from being effective indoors. However, many applications need indoor position information. For example, an indoor paging system might use position information to determine if someone is available for a last-minute meeting. Monitoring systems for high security areas can use position information to track employees and visitors. User and interaction modeling systems [Want and Hopper, 1992, Schmandt, 1994, Lamming and Flynn, 1994, Orwant, 1996] might use position information to reroute resources (e.g. an incoming call to the nearest telephone), predict the next action of the user, or provide automatic annotation of a meeting (e.g. to answer queries such as "who was I talking with in the stairs on Friday?").

2 Privacy Concerns

As observed by Mann [Mann, 1995], technological infrastructure can easily be used to violate privacy if it is not taken into account in the design of the system. Most current indoor location systems work through "active badges." In these systems, the badges continually announce their presence to the environment which then, through a wired network, report the location of the badge to a central system. Such systems raise several privacy concerns.

Active badge systems suffer from a possible user perception that the infrastructure is used for "spying." While the badge system may be very useful for opening locked doors automatically, might it not also be used to time how long a trip to the restroom takes? While a concerned badge wearer can certainly take off the badge at any given instance, the aggregate information collected over several days or months can still reveal patterns of behavior.

Technically, active badges can be made secure. A badge system can use current encryption technology such that only a master operator/security guard has access to the descrambled signature from a given badge. However, this master operator might be bribeable or might be manipulated to reveal information without realizing it. [Rothfeder, 1992] shows repeatedly how such "social engineering" can be used to gain sensitive information. In addition, any such central database is vulnerable to subpoenas.

Suppose that the above concerns are addressed through technology and policy. Yet another attack can be performed on an active badge system. This attack simply monitors the amount of traffic from the various badge receiving stations. While specific user information might not be obtained, data on how many people are in a given area or the path of some person through the building might be determined.

This section has provided a glimpse at some of the issues of an active badge systems. The reader is encouraged to examine the literature for more detailed information on privacy attacks and general privacy issues [Schneier, 1994, Westin, 1970, McCarthy, 1987, Smith, 1980, Miller, 1970]. The Locust system presented below has tried to take into account some of these issues by giving the user sole control of the location information and its release to the network.

3 Implementation

Each Locust consists of a 4Mhz PIC 16C84 microcontroller, a RS232 line voltage converter, infared receiver, infared LED, 6"x6" 9V solar cell, and a voltage regulator. Instructions, parts lists, and code are available from the web site listed in the references [Poor, 1996]. The resulting board is approximately 1" by 3".

Figure 1: By using solar cells placed in overhead lights, the Locust can run without batteries and service 20 foot diameter areas.

The Locust is dependent solely on its solar cell to provide it power. In order to get enough light for power and to cover a significant area with the infrared LED transmitter, Locusts are generally placed in the grills beneath overhead fluorescent lights (Figure 1) Depending on the height of the light, a 20 foot diameter circle under the light can be covered by a Locust.

A Locust's PIC contains 2KBytes of EEPROM. The Locust program and location information is loaded into the PIC before deployment. Upon power-up the Locust begins broadcasting its location information as specified. A user's system can listen to this broadcast without detection and decide whether or not to announce the user's location. The Locust also monitors the area with its infrared receiver to determine if a user is trying to upload an annotation about the area.

In an ideal implementation, each Locust would possess enough memory to contain any annotation the user would like to make. This would make the system completely self-contained and self-sufficient. In this first implementation, memory external to the PIC's 38 bytes of RAM was not included in the design. To emulate a full memory system with the current design, an annotation currently consists of an infrared upload request to the local Locust (to indicate the annotation's presence) and a registration request through the user's personal network connection (generally a digital cellular connection) to an annotation database maintained on the Internet. The Locust upload request consists of a command byte and a data byte. The command byte specifies adding or deleting a message and the data byte contains the message number. When a message is added, the Locust interleaves broadcasting its location information with the message number. The registration request to the annotation database consists of the Locust location ID, the message ID, and the annotation data. Thus, a Locust's message ID currently acts as a location-based hash table. In this way, an arbitrary amount of memory can be associated with the Locust.

When a user "hears" a message ID from a Locust, he has the option to ignore it. However, if he wants to decypher the message, his system sends a message to the annotation database with the Locust ID and message ID. The annotation database then returns the annotation data to the user.

Note that limiting message ID's to one byte allows only 256 different states. However, the combination of the Locust's unique position ID, the annotation byte, a user's unique (PGP signature) ID, and some sensing allows for considerable functionality as will be shown below.

4 Analysis and Future of the Locust Swarm

The Locust hardware described above is inexpensive to make, easy to install, and require little maintenance. Currently, 300 units are being deployed throughout the lab after a successful trial of 10 systems. A densely populated area can be saturated with Locusts to provide many uniquely identified regions. Less interesting areas may have Locusts only above each doorway. By using solar cells, costs and installation time for wall power adapters were eliminated. In addition, this method removed the constraint of having the Locusts near a power source, which is often in an inconvenient location for a line-of-sight broadcasting scheme. Of course, batteries were another option. However, if each unit's battery lasts a month and 300 units are installed, the maintenance time and costs for the system becomes prohibitive.

A valid criticism of the Locust swarm is that the same functionality can be obtained by installing only the location system and having the user's 2-way network directly inform the user of any annotations in the area. In many cases, however, the 2-way network may not be available. For example, current 2-way networks (Wavelan, Richochet, digital cellular) require expensive, and in some cases heavy, modems that the user must carry along with his wearable computer. In addition, many of these systems require repeaters that are wired into a buildings computer network and power systems. In areas such as public schools this infrastructure would not be economically feasible. However, the user's 2-way network is not necessary to get the desired functionality. The entire annotation database for a building might be downloaded from a master Locust when the user first walks in. Updates to the annotation database might be limited to one or two commonly used areas (i.e. elevators). Of course, another method of eliminating the 2-way network is to have each Locust contain its local annotation database. Given the cheap price, low power, and small size of modern serially addressed memory chips, this method will probably be adopted in the next revision of the system.

The obvious lack of networking hardware and the broadcast nature of the current Locusts assuages users' fears that the devices can be used for "Big Brother" activities. However, traffic analysis of the users' 2-way networks can still lead to privacy violations in the current system. A secondary benefit to making the annotation database local to each Locust is that it puts up a physical barrier to such attacks. Attacking the Locust system would involve the installation of a second system as extensive as the first and would still only yield traffic information (provided that users encrypt their annotations).

The location information the Locusts provide allows many of the uses mentioned in the introduction. Position information can be used for personal navigational assistants (a GPS implementation can be found in [Smailagic and Siewiorek, 1994]). If a user allows his wearable computer to broadcast his current location, co-workers can better schedule last-minute meetings and re-route telephone calls. Position information can be used for indexing other data on personal events such as lectures, hallway conversations, and deliveries [Rhodes and Starner, 1996]. Using predictive models on position information, software agents might ready physical resources, such as a calling an elevator while the user is still 50 feet away. In addition, software agents may use the positional data of several people to increase "physical serendipity." For example, a user's agent can alert him when a friend or co-worker from another building is nearby.

Figure 2: Multiple graphical overlays aligned through visual tag tracking. Such techniques can provide a dynamic, physically-realized extension to the World Wide Web.

Position information may be combined with additional sensors on a wearable computer to identify what objects are in the room. Once an object is uniquely identified, the annotation system of the Locusts may be used to add "physically based hyperlinks" to that object. For example, [Starner et al., 1996] present a wearable computer vision system for recognizing tagged objects and overlaying text, graphics, or video on those objects (Figure 2). Unfortunately, the tags had a limited number of bits for identification. However, when combined with position information, the same tags can be reused in different areas without ambiguity. From this point is not difficult to speculate about vision techniques that would eliminate such tags and allow identification of objects simply by their location, size, color, and structure. Then, if a user would like to leave a virtual "post-it" note on an object, he would simply look at the object and upload its visual "signature" and his message to the local Locust. Thus, the next user to enter the area would download the visual signature and associated message and, when he looks at the appropriate object, the note appears overlaid on it. Even if such vision systems are not feasible in the immediate future, other methods of tagging physical objects are quickly advancing. Two dimensional bar codes and radio frequency identification (RFID) tags are beginning to appear on the market. As these methods drop in price, they may be used as a matter of course in the manufacturing process. Already it is difficult to find objects in a grocery store without a UPC code.

While most of the applications in this paper have concentrated on wearable computing, the last use for the Locust swarm is by creatures that are themselves computers. Autonomous robots, such as described by [Martin, 1994] can use these position beacons to help navigate while performing their tasks. The annotation facility of the Locusts might be used by such a robot to leave messages or "bread crumbs trails" for cooperating robots. In such a way, many small robots might perform tasks such as have been explored by artificial life researchers [Travers, 1988].

5 Conclusion

The Locust swarm provides an inexpensive and low-maintenance alternative for providing indoor position information and messaging. While limited in functionality, this system demonstrates a wide spectrum of applications including dynamic routing of resources for a mobile user, user modeling, physically-based hypertext systems, and robot guidance. Privacy is inherently built into the system's architecture, encouraging user trust. Hopefully, positioning systems such as the Locusts will be used to help computer systems migrate from the desktop to the physical world.

Acknowledgements

Many thanks to Rob Poor for his IRX design, without which this project might not have happened. Also, thanks to Lenny Foner for his insistance on using solar cells instead of batteries. Finally, thanks to Fred Martin and Steve Mann for initial brainstorming and prototyping and to Brygg Ullmer whose late night discussions have inspired a new mindset on this research.

References

[Lamming and Flynn, 1994] Lamming, M. and Flynn, M. (1994). Forget-me-not: Intimate computing in support of human memory. In *FRIEND21: Inter. Symp. on Next Generation Human Interface*, pages 125–128, Meguro Gajoen, Japan.

[Mann, 1995] Mann, S. (1995). Personal web page. *http://wearcam.org/.*

[Martin, 1994] Martin, F. (1994). *Circuits to Control: Learning Engineering by Designing LEGO Robots.* PhD thesis, MIT Media Laboratory, Cambridge, MA.

[McCarthy, 1987] McCarthy, J. T. (1987). *The Rights of Publicity and Privacy.* Boardman, New York.

[Miller, 1970] Miller, A. (1970). *The Assault on Privacy: Computers, Data Banks, and Dossiers.* Univ. of Michigan Press, Ann Arbor.

[Orwant, 1996] Orwant, J. (1996). For want of a bit the user was lost: Cheap user modeling. *IBM Systems Journal*, 35(3).

[Poor, 1996] Poor, R. (1996). iRX 2.0. *http:// ttt.www.media.mit.edu/ pia/ Research/ iRX2/ index.html.*

[Rhodes and Starner, 1996] Rhodes, B. and Starner, T. (1996). Remembrance agent: A continuously running automated information retreival system. In *Proc. of Pract. App. of Intelligent Agents and Multi-Agent Tech. (PAAM)*, London.

[Rothfeder, 1992] Rothfeder, J. (1992). *Privacy for Sale: How Computerization Has Made Everyone's Private Live an Open Secret.* Simon and Schuester.

[Schmandt, 1994] Schmandt, C. (1994). *Voice Communication with Computers.* Van Nostrand Reinhold, New York.

[Schneier, 1994] Schneier, B. (1994). *Applied Cryptography.* John Wiley & Sons.

[Smailagic and Siewiorek, 1994] Smailagic, A. and Siewiorek, D. (1994). The cmu mobile comptuers: A new generation of computer systems. In *COMPCON '94.* IEEE Computer Society Press.

[Smith, 1980] Smith, R. E. (1980). *Our Vanishing Right to Privacy.* Loompanics Unlimited, Port Townsend, WA.

[Starner et al., 1996] Starner, T., Mann, S., Rhodes, B., Levine, J., Healey, J., Kirsch, D., Picard, R., and Pentland, A. (1996). Augmented reality through wearable computing. Technical Report 397, MIT Media Lab, Perceptual Computing Group. To appear Presence 6(4); Submitted Oct. 1995.

[Travers, 1988] Travers, M. (1988). Agar: An animal construction kit. Master's thesis, MIT, Media Laboratory.

[Want and Hopper, 1992] Want, R. and Hopper, A. (1992). Active badges and personal interactive computing objects. *IEEE Trans. on Consumer Electronics*, 38(1):10–20.

[Westin, 1970] Westin, A. (1970). *Privacy and Freedom*. Bodley Head.