Ubiquitous Computing: Making It a Reality

Ken Sakamura

Professor, University of Tokyo / Director, YRP Ubiquitous Networking Laboratory

1. Background to Ubiquitous Computing

Application of the RFID (Radio Frequency IDentifier) chip has expanded rapidly since its practical application 20 years ago. Advances in technology have increased chip memory capacity to several hundreds of bits, significantly reduced antenna size and lowered cost. This development in microchip technology has brought us to the threshold of a development in new computer technology that enables tiny microchips to be implanted in physical objects and from there perceive conditions in the real world. Perceiving conditions in the real world refers to the ability to detect a diverse range of real world information, including current location, temperature and humidity levels, the identity of a person, when a product was made and by whom it was made.

The example shown in Fig. 1 shows that it is now becoming possible to implant a microchip loaded with information into clothing, then use a small terminal (Note 1) to read and send the number stored in the microchip to a server computer to obtain detailed information about that object.

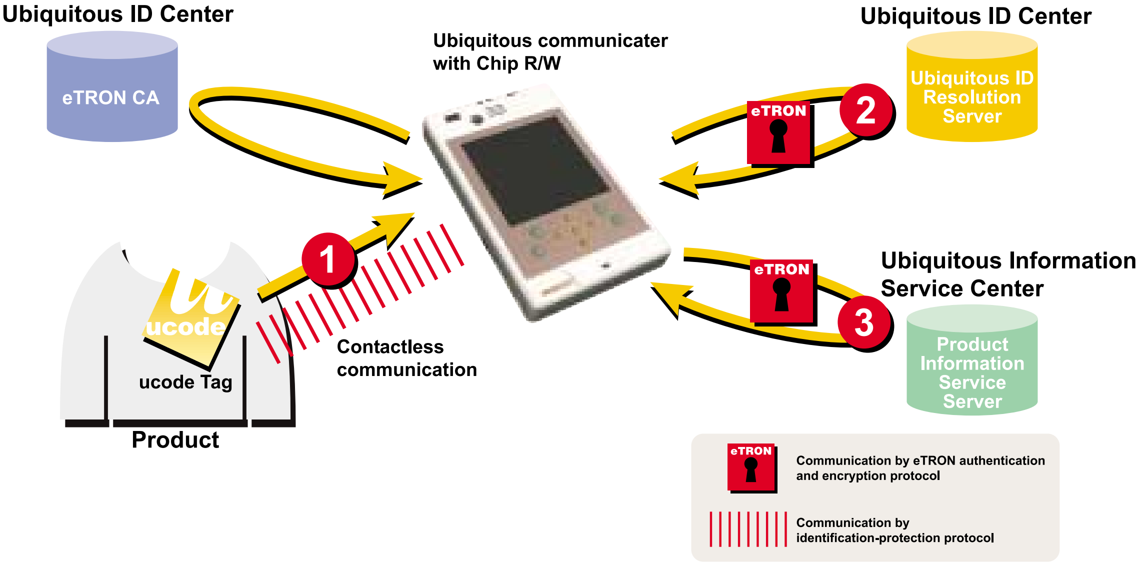
Ubiquitous ID Center
eTRON CA
Ubiquitous communicater with Chip R/W
Ubiquitous ID Center
Ubiquitous ID Resolution Server
eTRON
2
1
ucode
ucode Tag
Product
Contactless communication
eTRON
3
Ubiquitous Information Service Center
Product Information Service Server
eTRON
Communication by eTRON authentication and encryption protocol
Communication by identification-protection protocol

Fig. 1: Using ucode to search for product information

It is now becoming possible to make practical application of sensor networks that support people’s daily lives. This is done by a vast array of groups of devices containing computers that are placed at various locations in the environment where they automatically sense conditions in the real world, exchange the information gathered over networks from where it is channeled to other sensor/computers operating in coordination. Such systems and models are referred to as “ubiquitous computing” and “pervasive computing."

Existing computer networks, as typified by web sites on the Internet, are designed so that "we are not even conscious of where the connected computers are." That is why these networks have come to be referred to as "virtual worlds" that are apart from the real world. In contrast, ubiquitous computing offers a model in which computing is an integral part of the real world where the concept of the physical location, "the location of the computer" is one of the key "conditions." It is precisely the difference in strength of emphasis on this physical location that sets the two models apart.

Note 1: The all important, small handheld terminal (see Photo. 1) used to read the information contained in the tiny microchips implanted in the various physical objects that make up the ubiquitous computing environment are referred to as "Ubiquitous Communicators." One terminal can become a mobile phone, act as a wireless LAN terminal at other times, and has a special antenna device designed to read radio waves emitted by microchips. The information read from the microchips contained in physical objects can then be transmitted outside the premises using a wireless LAN function. Conversely, it is also possible to transmit information on the person carrying the handheld terminal (when permissible and only the permitted information) to the surrounding environment. Ubiquitous communicators specialize in communication not only between people, but also between people and things.

Photo. 1: Ubiquitous Communicator

2. The New Possibilities Ubiquitous Computing Brings

Implanting microchips into physical objects and then reading that information using computers built into household electronics and other devices makes it possible to configure a sensor network capable of understanding surrounding conditions with greater accuracy. This in turn makes it possible to perform optimal control of various types of processes. Using the energy conservation problem as an example, implanting a tiny sensor chip in a person's shirt makes it possible to know both current body surface temperature and the person's history of temperature conditions. Sending the information directly to an air-conditioning system makes it possible to regulate temperature to optimum levels for each individual. The result is a much more finely tuned temperature control than could be possible with the average remote control unit. For example, a person who has just come from hot weather outside can be quickly cooled and his or her thermal history is update to reflect this latest condition. Then the person will quickly become and stay comfortable without the need for continued excessive cooling. And if the chip is capable of detecting the degree of perspiration from the person wearing it the chip can pass information, for example, to a washing machine. If the clothing is not very soiled from perspiration a simple water wash would be sufficient. This sort of finely tuned individualized control can be used to maintain optimum levels of comfort while avoiding any excessive expenditure of energy. Used on a larger scale such optimally controlled process could contribute to energy conservation at the society level.

Eventually many different computers will be installed in the floors and walls of houses. The trend will probably be extended to household electrical devices, household furnishings, clothing and food packages. Wearing ubiquitous communicators makes it possible to have air-conditioning and lighting instantly adjusted to the personal tastes and requirements other person entering the room. Simply entering a rented car can ensure that the driving position is automatically adjusted to personal needs. It will instruct street billboards to change letter size and color to improve visibility, if necessary, to suit the individual who has come to read. Automatic translation processes could also be used to display messages in various different languages. In other words, the surrounding environment could be adjusted to suit the physical needs and limitations of all individuals, including the elderly and the handicapped.

Ubiquitous computing would make it possible to keep up-to-date information on the foodstuffs currently available in refrigerators and storage pantries and their consume-by dates. The system can be configured so that items are ordered whenever they become low or so that the information kept on one’s person could be used to advise automatically when the person is in the vicinity of a product that you are short of at home during a store visit. A person carrying a ubiquitous communicator would not have to bother paying at the cash register because the payment would be automatically deducted when a person leaves the store carrying the products. Since electronic tags are present on waste discarded into intelligent waste boxes, it can be sorted and the materials recycled and reused much more efficiently than by human hand.

In the field of medical care, errors in administering or prescribing medicine at medical facilities could be significantly reduced by designing a system in which the IC chips on medicine bottles can communicate with the IC chips being worn by the patients on fingernails. At home, ubiquitous communicators could also be designed to warn individuals when two different drugs must not be taken together. Using voice warnings could free blind people from the worry of fumbling about for the correct medicine. A refrigerator would read the information from the food stuff inside and could warn someone with an allergy about its ingredients.

Ubiquitous computing has many applications in the distribution process as well. Not only does being able to identify each individual product make the distribution process runs smother, it would be possible to recall only the affected lots whenever problems occur with a product. If applied to items sensitive to storage temperature, such as wines and virus vaccines, for example, tiny microchips with temperature sensors as in the example of the shirt described above can be designed to notify the warehouse air-conditioning system when temperatures are too high or to notify customers at the time of purchase if product quality has deteriorated.

Long after the store sales, as long as the purchaser’s refrigerator is connected to the ubiquitous network, it can immediately receive public food warnings and conduct automatic checks for food products that might be included in the dangerous items list. A warning that “this product is included in the dangers items list” can be issued before the product is consumed and the individual product lot in question can be tracked down and recalled just before consumption as a way to minimize any danger or damage. This traceability advantage would be particularly great for those commodities that are linked directly to people's health, such as medicines and food. While not a pleasant subject, traceability can also be used to prevent stolen goods from entering the distribution system as a way of preventing crime. The issue of consumption of stolen medicines that have passed their expiry dates is a problem in Third World countries where it sometimes results in death. Prevention of such accidents is another useful application for this technology.

3. Checking on Security

Ubiquitous computing can be seen as a form of dream technology capable of triggering significant social changes and opening up new business opportunities. Here in Japan, companies ranging from major trading firms right down to companies with any sort of link to electrical and electronic devices have established their own ubiquitous computing departments in the last year or two. For someone such as myself who has been promoting the potential of ubiquitous computing as the “ability to have computers everywhere” for the past 15 years [1] [2], it now seems like such a different world. (Being Japanese, however, I was not able to use the more sophisticated and accurate “ubiquitous” as the name. I had to settle for the more simple equivalent of “Computing Everywhere” which did serve its purpose in informing people of an advanced new field of technology. Thus, though I am recognized to have been ahead of my time, it was the Americans' terminology ubiquitous [3] and pervasive [4], that have been adopted worldwide.)

While I am delighted to see that people are interested in this promising new technology, there are inherent dangers that must also be considered. A company in the United States is planning to insert microchips into the hundreds of millions of razor blades it distributes and manages. In addition to the technical aspects, I believe it is important to first in gain social consensus for such mass application of this new technology. Civic organizations [5] in the United States have begun opposing the rapid application of RFID chip technology to consumer products which they see as an invasion of privacy.

The important issue is that the field of ubiquitous computing is too vast and potentially too pervasive to simply sit back and deal with problems when they arise. Security and privacy are issues that must be dealt with from the outset. There is also the issue of what sort of frequency bandwidth to use for the radio waves emitted by the microchips, as each country has its own rules and regulations concerning radio waves. The effect that radio waves can have on the human body must also be considered. In contrast with the Internet that applies uniform standards throughout the world, national customs and cultural traditions, local characteristics and legislation already in place in each country come into play when physical objects are involved. Because it is such an important new technology, it must be developed carefully and any wrong turns must be avoided or the situation can quickly get out of control.

Attempts to apply ubiquitous computing technology will require careful consideration of the implications with regard to information security technology. Being able to use computers to detect real world “conditions” opens up the possibility of illegal use of information. Bad things will happen. The ability to stalk individuals without even having to lift a finger would become possible. False information can be sent to refrigerators, for example, that can result in consumers drinking spoiled milk.

By virtue of the fact that ubiquitous computing will bring RFID chips and computers into our daily lives it is crucial to consider the worst-case scenario in which a criminal element could take over the system. Even the common user can be a member of the criminal element. In other words, there is a limit to what software protection can do when even the owner cannot be trusted. Effective security measures will entail the development of special types of hardware. We are currently conducting work on developing such hardware. “eTRON” is a special encryption hardware system that prevents electronic data from being copied or counterfeited. eTRON offers a distributed system framework for secure distribution of data (see Photo. 2) [6].

Photo. 2: eTRON Chip (SIM type)

Rather than as a simple replacement for the bar code, we are working towards developing the ideal approach to building a society that incorporates ubiquitous computing. We were well aware of the privacy issue since the outset and have focused efforts on developing the means to protect that privacy. We have succeeded in developing a communication protocol that protects the attribute information in the RFID chip including its id by randomly varying the response so that individual identification is very difficult. We have also developed a very strong security chip that utilizes a shared encryption key scheme.

4. When Will the System Be Completed?

In addition to the issue of security, the hurdles that ubiquitous computing companies must overcome before they can succeed include reducing the cost of the microchips themselves. Implanting microchips on everything would require the production of a variety of different types of microchips (see Photo. 3) to meet the needs of various objects and we will need to produce hundreds of millions of such chips. The development of affordable and safe microchips will require the great leaps in production technology for which much research and development has yet to be done.

Photo. 3: different types of microchips

Just to give you an idea of where we are at now, it should be possible to supply lots of hundreds of millions of microchips that offer a simple number reading capability at five cents per chip within two or three years time. At that point chips containing microprocessors or sensors will still cost several tens of cents. But it will likely be 10 years or so before distributors will be ready to replace their bar-code systems with the new microchips.

Taking these cost consideration into account, I foresee that the initial application will likely be in the area of traceability for products such as medicines and food where safety is a concern and very expensive products for which the merit of traceability exceeds cost considerations. The fields of application for ubiquitous computing will expand in a gradual process as the various challenges, which include cost considerations and production techniques, are overcome. I would not be surprised if it takes 10 years before ubiquitous computing begins to take shape in the way that we visualize it now. In fact, I feel it is important to take the time to do things right especially with regard to achieving the necessary social consensus on privacy and security issues.

5. Framework Required for Implementing Ubiquitous Computing

In closing my presentation I would like to discuss the various activities we have conducted in our efforts to bring about the implementation of ubiquitous computing.

In the area of foundation technology, the key players in its development on our side include the YRP Ubiquitous Networking Laboratory and my research lab at Tokyo University.

Because the embedded computers for ubiquitous computing will be overwhelmingly more numerous than personal computers, a development framework will be required that can safely develop high quality, large volume embedded computer systems. Unlike semi-finished products, such as personal computers of today, where the user will put up with them even if bugs shut them down, errors of this magnitude in ubiquitous computing, which involves equipment and devices that support our daily lives, could very well result in the loss of assets and even human life.

We propose use of the “T-Engine” platform as the framework for development [7] [8] [9]. The T-Engine offers an open hardware platform (see Photo. 4) for developing embedded systems. We believe that setting the necessary rules in advance provides an efficient means for developing high-quality embedded computer systems. We have also established an NPO referred also to as the T-Engine Forum as a means for further developing the platform. The NPO included 22 companies at the time it was launched. As of September 2003, the NPO membership stood at over 240 companies, which now serve to make up very strong platform indeed.

Photo. 4: different types of T-Engine board

I would like to conclude this discussion with an overview of the operational and management issues that must be overcome in implementing this framework. One key issue is that of how to distinguish between the various computers and chip tags that we implant into physical objects. Another important issue is that of how to effectively maintain security

Of particular importance is the implementation of the ucode number system required for distinguishing between objects. The ucode numbering system must be standardized and a system effective in maintaining the uniqueness of ID numbers must be devised. This is because being able to identify “what each object is” is the key to recognizing real world conditions. It will also be important to standardize the specifications used for transmitting information between the chip tags and ubiquitous communicators, and for maintaining security. Standardizing the data read protocol will make it possible to use mobile phone, which everyone has, as a standard UC. For it is only when each user possesses a standardized reading device that it will be possible to create the ideal ubiquitous computing society.

With regard to the framework for implementing the ucode management system, rather than aiming for a “virtual world,” as personified by the Internet, it will be important to refrain from using “global standards” for a system so closely tied to the real world. Even though many technical aspects will be standardized and shared across regions, it would be a mistake to attempt to standardize the actual implementation of the framework. This is because it will be necessary to accommodate the many national differences in cultural and legal traditions and regional characteristics. We think that a regional management is a preferred solution.

We believe it is important to establish system management centers in each country and as such have established our own Ubiquitous ID Center together with the T-Engine Forum. Our center is engaged in allocating IDs, coordinating operation with existing ID systems, establishing mandatory common security policies for ucode implementation for all participants and conducting verification and certification of the various technologies required.

With regard to security policies pursuant to the implementation of the ucode, we have established a total of seven standard tag classes, including the bar code, for each level of security in order to accommodate the various implementation and cost conditions. The security procedures are stipulated [10] according to these terms and classes. For example, a rule would read "for the tags attached to clothing that the user constantly wears, an RFID chip (class 2 or above) that supports the identification preventing ubiquitous networking protocol is used. Steps also have been taken to inform users of the attachment methods and locations in the event they decide they no longer wish to use the system and are willing to accept responsibility for removing the chips themselves." One of the principal aims of the Ubiquitous ID Center, in addition to developing technology, is to establish the infrastructure for ensuring that consumers feel secure in using the RFID chip tags and accompanying security policy by disclosing information, including that regarding administrative aspects of the operation details, to enable consumers to manage their own personal information under their own control.

6. Conclusion

As described in the foregoing sections, we are dedicated to taking strong initiative in working toward establishing a ubiquitous computing world using our three-pillar framework comprised of the YRP Ubiquitous Networking Laboratory, T-Engine Forum and Ubiquitous ID Center. We are also dedicated to actively sharing our technology with the rest of the world based on the principle of open architecture. This is because we believe that helping the establishment of regional ubiquitous ID centers in every country and region will be a valuable addition to the future contribution that Japan must make worldwide.

7. Documents and Web Sites Used As Reference

[1] K. Sakamura, "The TRON Project," IEEE Micro, vol. 7, no. 2, Apr. 1987, pp. 8-14.

[2] TRON Project Home Page, http://www.tron.org/

[3] Mark Weiser, "The Computer for the 21st Century," Scientific American Volume 265, Number 3, September 1991.

[4] Gene F. Hoffnagle, "Preface," Special Issue on Pervasive Computing, IBM System Journal Volume 38, Number 4, 1999.

[5] http://www.stoprfid.org

[6] K. Sakamura and N. Koshizuka, "The eTRON Wide-Area Distributed-System Architecture for E-Commerce," IEEE Micro, vol. 21, no. 6, Dec. 2001, pp. 7-13.

[7] K. Sakamura and N. Koshizuka, "T-Engine: The Open Realtime Embedded Systems Platform", IEEE MICRO, vol. 22, no. 6, Dec. 2002.

[8] K. Sakamura and N. Koshizuka, "T-Engine: The Open, Real-Time Embedded-Systems Platform for Ubiquitous Computing", in Proc. VLSI Circuit Symposium, June 2003.

[9] T-Engine Forum Home Page, http://www.t-engine.org/

[10] Ubiquitous ID Center Home Page, http://www.uidcenter.org/

Contact Details for Ubiquitous ID Center

Ubiquitous ID Center (In the YRP Ubiquitous Networking Laboratory)
The 28th Kowa Building, 2-20-1 Nishigotanda, Shinagawa-ku Tokyo 141-0031, Japan
E-mail: uid-office@uidcenter.org / TEL: +81-3-5437-2338 / FAX: +81-3-5437-2271