Ubiquitous Networking and Security Parameters

[1]Mayur Dabhade, [2]Wrushal Kirnapure, [3]Jayendra Khandare, [4]Pooja Dange, [5]Swapnil Dabhade
[1]Leelavati Awhad Institute of Technology MS & R, Kanore (Thane), Maharashtra, India
[2,3,4,5]Dr. Babasaheb Ambedkar Technological University, Lonere (Raigad), Maharashtra, India

Abstract

The paper discusses about the future generation of networking based the current scenario in the form of omnipotent network. But still something is lacking, which could be "Exotic Networks". The central idea is 'connectivity' that is available everywhere and in any form. Also, this paper explains the concept of ubiquitous network implementation, along with the intermediate state i.e. ubiquitous computing and then the obstacles to this idea.

Keywords

Ubiquitous Computing, Pervasive Computing, Piezoelectric Speaker, Exotic Networks

I. Introduction

Today Internetworking has become an integral part of our life because of widespread Internet. 'The network' is just a booming thing, since the developments in the fields of social networking, rapid growth of sites like Facebook.com, Twitter.com, etc. But this revolution is not over yet. The next step in the development can be termed as 'ubiquitous computing'. Ubiquity means which are present anywhere, anytime. This concept includes networking where you can access all of your data whenever and where-ever you require, provided that you should be near to any kind of computing device connected in the network. It includes any kind of data, from office documents and files to movies, music and just anything. In short, one won't be needed to carry anything with him, just the transceiver. In case of virtual reality, we enter in a computerized world. By means of ubiquitous networks, computers come out of its casing to interact with us.

But this ubiquity demands to consider some other issues that we are going to explain in next sections. Section 2 focuses on recent networks and problems with that; section 3 defines the working parameters and Section 4 enlists requirements for ubiquity; section 5 details security issues that need to be considered for development of ubiquitous networks; Section 6 specifies applications of ubiquitous networking in workplace; finally, the conclusion is outlined.

II. Recent Networks

The networks available now are definitely not sufficient for ubiquity that we are expecting in future. For connecting the whole environment of a person in a network technique has to be developed to provide necessary bandwidths that will be required; also we'll need high computing power, so that the networking devices work in synchronization. We'll also need a new generation of radio transceivers.

The recent networks are not capable enough to provide the necessary bandwidth with required precision; they must be modified keeping the cost factor in consideration. As there will be many devices connected to network, protocols needed to be modified. Constant Internet access will be needed at relatively low cost. Also, government will have to play an important role, like the policies used by Japan government for its project 'u-Japan'.

III. Working Parameters

Instead of taking the hardware with you, we'll design a system that allows your program applications to follow you wherever you go. Following is just a single way that could be used to implement the Ubiquitous networking:

A. Send Out the Bat Signal

In order for a computer program to track its user, researchers had to develop a system that could locate both people and devices. The AT&T researchers came up with the ultrasonic location system. This location tracking system has three basic parts:

- Bats - small ultrasonic transceivers worn by users.
- Receivers - ultrasonic signal detectors embedded in ceiling.
- Central unit - coordinates the bats and receiver chains.

Users within the system will wear a bat, a small device that transmits a 48-bit code to the receivers in the ceiling. Bats also have an imbedded transmitter, which allows it to communicate with the central unit using a bi-directional 433-MHz radio link. Bats are about the size of a pager. These small devices are powered by a single 3.6-volt lithium battery. The devices also contain two buttons, two light-emitting diodes (LEDs) and a piezoelectric speaker, allowing them to be used as ubiquitous input and output devices.

A bat will transmit an ultrasonic signal, which will be detected by receivers located in the ceiling approximately feet (1.2 m) apart in a square grid. There are about 720 of these receivers in the 10,000-square-foot building at the AT&T Labs in Cambridge. An object's location is found using trilateration, a position-finding technique that measures the object's distance in relation to three reference points.

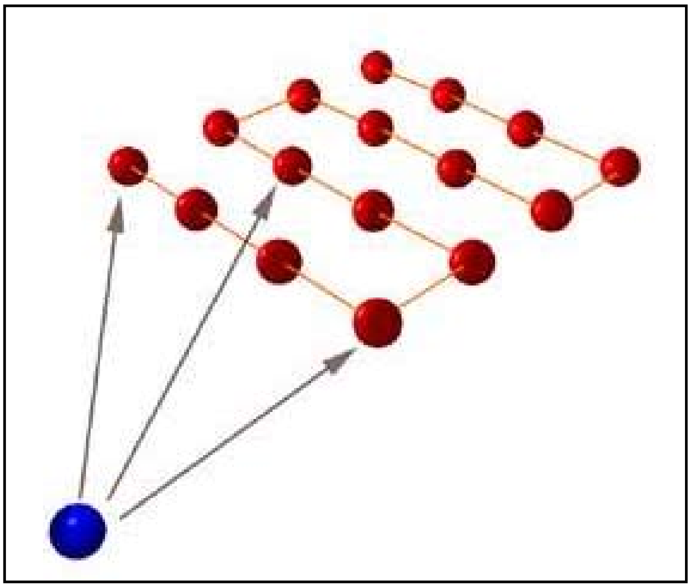

Fig. 1: Sketch of Trilateration Method Where Blue Dot Represents a Bat and Red Dots Represent Sensors Fitted in the Ceiling

Trilateration works by measuring the distance from the bat worn by the user to three sensors in the ceiling. Researchers can locate a user's position with up to accuracy of 3 cm.

If a bat needs to be located, the central unit sends the bat's ID over a radio link to the bat. The bat will detect its ID and send out an ultrasonic pulse. The central unit measures time it took for pulse to reach the receiver. Since the speed of sound through air is known, the position of the bat is found by measuring the speed at which the ultrasonic pulse reached three other sensors.

By finding the position of two or more bats, the system can determine the orientation of a bat. The central unit can also determine which way a person is facing by analyzing the pattern of receivers that detected the ultrasonic signal and the strength of the signal.

B. In the Zone

The central unit creates a zone around every person and object within the location system. When all the sensors and bats are in place, they are included in a virtual map of the building. The computer uses a spatial monitor to detect if a user's zone overlaps with the zone of a device. If the zones do overlap, then the user can become the temporary owner of the device. Computer desktops can be created that actually follow their owners anywhere within the system. Just by approaching any display in the building, the bat can enable the VNC (virtual network computing) desktop to appear on that display.

C. Information Hoppers and Smart Posters

The system will help us store and retrieve data in an "information hopper." This is a timeline of information that keeps track of when data is created. The hopper knows who created it, where they were and whom they were with.

By using a digital camera that is connected to the network, a user's photographs are immediately stored in his or her timeline. Tape recorders or bats could also send audio memos to the information hopper. Another application that will come out of this ultrasonic location system is the smart poster. In this new system, a button can be placed anywhere in your workplace. Smart posters will be used to control any device that is plugged into the network. The poster will know where to send a file and a user's preferences. The system automatically knows who is pressing the poster's button by means of bats. This new ubiquitous network will enable all computers in a building to transfer ownership and store all of our files in a central timeline.

IV. Requirements

Following are the requirements that must be satisfied to achieve ubiquitous networking:

A. Multi-modal

Ubiquitous networks should be broadband and multi-modal. The goal should be to make data transfer at 6 Mbps not only over cable and fixed-point networks but also with portable terminals that work even from automobiles. In other words, ubiquitous networks are multi-modal networks that can switch between fixed point and mobile locations, cable and wireless, and telecommunication and broadcast network modes without undue difficulty.

B. Protocols for Multi-modal

The IP protocol for this multi-modal network should naturally be IPv6 or advanced. As an IP address is required for each information appliance or automobile in ubiquitous-network configuration, we cannot rely upon IPv6 only.

Users can also take advantage of services using ADSL with the powerful broadband services now in place. Satellite Internet has begun high speed Internet services for consumers.

C. Other Upgrades

In wireless systems, NTT DoCoMo's I-mode has started a cellular telephone Internet boom. This would become an ideal ubiquitous network and terminal if NTT DoCoMo upgrades the service in the future to the Mbps level at a moderate price.

Another development is Bluetooth technology, which can connect all devices within ten-meter radius at speeds up to maximum of 1Mbps.Another alternative is electric power distribution networks that directly use electric power lines instead of telephone or cable lines to form a network that connects information appliances. Of these, however, the most likely candidate for broadband service for household ubiquitous network is an optical fiber FTTH (fiber-to-the-home) network. The potential for FTTH, which appeared to have been forgotten for a period, continues to increase. While FTTH has various problems, it undoubtedly holds the key to realizing ubiquitous networks.

D. Balancing Proactivity and Transparency

Proactivity is a double-edged sword. Unless carefully designed, a proactive system can annoy a user and thus defeat the goal of invisibility. How does one design a system that strikes the proper-balance at all times? Self-tuning can be an important tool in this effort. A user's need and tolerance for proactivity are likely to be closely related to his level of expertise on a task and his familiarity with his environment. A system that can infer these factors by observing user behavior and context is better positioned to strike the right balance.

Historically, the ideal in system design has been transparency. For example, caching is attractive in distributed file systems because it is completely transparent. Unfortunately, servicing apache miss on a large file over a low-bandwidth wireless network takes so long that most users would rather be asked first whether they really need the file. However, a flurry of such interactions can overwhelm the user. Coda suggests a way to resolve this dilemma. On a cache miss, the system consults an internally maintained user patience model to predict whether the user will respond positively to a fetch request. If this appears likely, the user interaction is suppressed and the fetch is handled transparently.

Many subtle problems arise in designing a system that walks the fine line between annoying proactivity and inscrutable transparency. For example: "How are individual user preferences and tolerances specified and taken into account? Are these static or do they change dynamically?

"What cues can such a system use to determine if it is veering too far from balance? Is explicit interaction with the user to obtain this information acceptable? Or, would it be an annoyance too?

"Can one provide systematic design guidelines to application designers to help in this task? Can one retrofit balancing mechanism into existing applications?

E. Privacy and Trust

Privacy, already a thorny problem in distributed systems and mobile computing, is greatly complicated by ubiquitous computing. Mechanisms such as location tracking, smart spaces, and use of surrogates monitor user actions on an almost continuous basis. As a user becomes more dependent on a ubiquitous computing system, it becomes more knowledgeable about that user's movements, behavior patterns and habits. Exploiting this information is critical to successful proactivity and self-tuning. At the same time, unless use of this information is strictly controlled, it can be put to a variety of unsavory uses ranging from targeted spam to blackmail. Indeed, the potential for serious loss of privacy may deter knowledgeable users from using a pervasive computing system Greater reliance on infrastructure means that a user must trust that infrastructure to a considerable extent. Conversely, the infrastructure needs to be confident of the user's identity and authorization level before responding to his requests. It is a difficult challenge to establish this mutual trust in a manner that is minimally intrusive and thus preserves invisibility. Privacy and trust are likely to be enduring problems in pervasive computing. Many research questions follow. For example: "How does one strike the right balance between seamless system behavior and the need to alert users to potential loss of privacy? What are the mechanisms, techniques and design principles relevant to this problem? How often should the system remind a user that his actions are being recorded? When and how can a user turn off monitoring in a smart space?

"What are the authentication techniques best suited to ubiquitous computing? Are password-based challenge response protocols such as Kerberos adequate or are more exotic techniques such as biometric authentication necessary? What role, if any, can smart cards play? "How does one express generic identities in access control? For example, how does one express security constraints such as ''Only the person currently using the projector in this room can set its lighting level?'' Or, ''Only employees of our partner companies can negotiate QoS properties in this smart space?''

F. Impact on Layering

A recurring theme in the earlier sections of this paper has been the merging of information from diverse layers of a system to produce an effective response. Proactivity and adaptation based on corrective actions seem to imply exposure of much more information across layers than is typical in systems today. Layering cleanly separates abstraction from implementation and is thus consistent with sound software engineering. Layering is also conducive to standardization since it encourages the creation of modular software components. Deciding how to decompose a complex system into layers or modules is nontrivial, and remains very much an art rather than a science. The two most widely-used guidelines for layering are Parnas' principle of information hiding and end-to-end principle of Saltzer et. al. However, these dates back to the early 1970's and early 1980 are respectively, long before pervasive computing was conceived. Many research questions follow: "How can the benefits of layering be preserved while accommodating the needs of pervasive computing? What is the impact of these accommodations on efficiency and maintainability? "Are existing layers best extended for pervasive computing by broadening their primary interfaces or by creating secondary interfaces (such as the SNMP network management interface)?" When creating a new layer, are there systematic guidelines we can offer to ensure compatibility with the needs of ubiquitous computing? How much harder is it to design and implement such a layer?

G. Context Aware Computing

Context-aware systems are a component of a ubiquitous computing or pervasive computing environment. Three important aspects of context are:

1. where you are;
2. who you are with; and
3. what resources are nearby.

Although location is a primary capability, location-aware does not necessarily capture things of interest that are mobile or changing. Context-aware in contrast is used more generally to include nearby people, devices, lighting, noise level, network availability, and even the social situation, e.g., whether you are with your family or a friend from school.

H. Home Automation

Home automation is the residential extension of "building automation". It is automation of the home, housework or household activity. Home automation may include centralized control of lighting, HVAC (heating, ventilation and air conditioning), appliances, and other systems, to provide improved convenience, comfort, energy efficiency and security. Home automation for the elderly and disabled can provide increased quality of life for persons who might otherwise require caregivers or institutional care.

A home automation system integrates electrical devices in a house with each other. The techniques employed in home automation include those in building automation as well as the control of domestic activities, such as home entertainment systems, houseplant and yard watering, pet feeding, changing the ambiance "scenes" for different events (such as dinners or parties), and the use of domestic robots. Devices may be connected through a computer network to allow control by a personal computer, and may allow remote access from the internet. Through the integration of information technologies with the home environment, systems and appliances are able to communicate in an integrated manner which results in convenience, energy efficiency, and safety benefits.

Although automated homes of the future have been staple exhibits for World's Fairs and popular backgrounds in science fiction, complexity, competition between vendors, multiple incompatible standards and the resulting expense have limited the penetration of home automation to homes of the wealthy or ambitious hobbyists. Possibly the first "home computer" was an experimental home automation system in 1966.

An ubiquitous learning environment is any setting in which students can become totally immersed in the learning process. So, a ubiquitous learning environment (ULE) is a situation or setting of pervasive or omnipresent education or learning. Education is happening all around the student but the student may not even be conscious of the learning process. Source data is present in the embedded objects and students do not have to DO anything in order to learn. They just have to be there.

V. Security Issues

The security related issues of such a vast network are even more complicated. Ubiquitous computing works on the premise that computers can collect enough data to monitor your behavior, assess your needs and then adjust in response. However, anything that aims to understand that much about you can be misused. So ubiquitous computing for your home has great potential, but there are dangers as well.

One obvious issue is privacy and how the information collected by your house can be abused, which also raises security concerns. At the end of the day, ubiquitous computing is just a smart computer network - and computer networks can be hacked. Another concern is that you might get used to being monitored, which brings up ethical concerns about the technology.

Hence, the central controller unit should be protected carefully. The signals sent and received by bats must be implemented by using concept of frequency-hopping. Though connectivity is important central unit shouldn't be connected directly to the Internet as it becomes more insecure and the private data or behavioral patterns of the user can be leaked out. So we can use an alternative method, in here for net access a terminal should be used which will be accessed by central unit as an individual user not as a system. 'PGP' idea will prove useful in this field, since it can provide various levels of encryption as per the user requirements.

VI. Applications in Workplace

The elements of ubiquitous computing nanotechnology, wireless computing, context-awareness, and natural interaction offer a powerful set of tools to achieve the promise of ubiquitous computing. To provide a better sense of what this future holds, let's take a look at how ubiquitous computing might play out in the workplace. e.g. It's the beginning of the day and Elaine has a major presentation to work on for a sales call. Two weeks ago, when the meeting was set up, she instructed her calendar to schedule two additional meetings with her team to4 April 2002 to prepare for the presentation. It is about time for the second meeting, and she walks into the conference room that her calendar had reserved. The display on the conference room door lists the title of the meeting and checks off attendees as they enter. The giant "work board" on one wall of the room has preloaded all of the documents related to the presentation and is waiting for input. When everybody has arrived for the meeting, the display on the conference room door lists the meeting as "in progress" and dims the window to minimize distraction from the busy hallway outside.

As the team reviews the presentation, Elaine spots a section that flows poorly. After discussing it with the team, she calls to the work board and tells it to move the section on product features to just before the section on optional services. The meeting covers several additional topics and then disbands 10 minutes early. The work board automatically saves the updated files as the attendees exit the room.

On the way back to her desk, Elaine stops by her friend Roger's desk task him a question. Sensing her approach, Roger's computer works in the background to load documents that the two of them have worked on together in the past 2 weeks, should any of them be required. Elaine is greeted excitedly by Roger, who is rushing to a meeting of his own. "We really need your input on pricing for this service," says Roger. "Can you join us? "Elaine can spare some time, so she elects to participate in the meeting. When Elaine enters the conference room, her calendar automatically updates to include the new meeting. After Roger introduces the topic, Elaine says, "My team came up with a template to determine pricing for a slightly different service. Maybe we can use it as a starting point." Elaine approaches the work board, and a list of her public files appears. The files are sorted in alphabetical order, with the files whose contents are related to the topic of the meeting highlighted. Elaine touches the template file, and the document opens. After some discussion, the template is modified and is ready for testing. Meeting attendees pitch different "what-if" scenarios, which are automatically entered into the template and processed, with the final price displayed. Once everyone is satisfied with the revised template, the meeting breaks up. To thank Elaine for her help, Roger offers to buy her lunch at the cafeteria. Elaine accepts the invitation, saying that she'll be ready as soon as she checks her video mail. As she approaches a nearby public communications portal, the screen shows the four new video mails waiting for her. One video mail is from a longstanding client. She touches the message and watches as the client recounts a story of superior service received from one of Elaine's direct reports, Dave. Elaine tells the video mail system to add the message to her file on Dave, and records a thank-you message to the client. Business done, Elaine and Roger take the elevator down to the cafeteria.

VII. Conclusion

Ubiquitous computing has the ability to simplify, minimize, or altogether reduce human interventions currently required of computer system architectures. If the implementation is done cautiously and the privacy issues are handled appropriately, it can be used as an alternative to recent technologies.

But before that level, first of all, telecom giants have to provide higher data access at low price rates. Research is going on everywhere for the same cause. If all goes in the right direction, one day the final dream of 'Exotic Networks' can be realized with 'ubiquitous networks' as an intermediate stage.

References

[1] Michael R. Heim,"The Metaphysics of Virtual Reality".

[2] Masayoshi Ohashi, KDDI R&D Laboratories, "Ubiquitous Networks".

[3] James Weather all et al.,"Applications of Ubiquitous Networks".

[4] Kistler, J.J., Satyanarayanan, M.,"Disconnected Operation in the Coda File System", ACM Transactions on Computer Systems , February, 1992.

[5] Steiner, J.G., Neuman, G., Schiller, J.I.,"Kerberos: An Authentication Service for Open Network Systems", In Proceedings of the Winter 1988 USENIX Technical Conference. Dallas, TX, February, 1988.

[6] Jain, A., Hong, L., Pankanti, S.,"Biometric Identification", Communications of the ACM 43(2), February, 2000.

[7] Itoi, N., Honeyman, P.,"Practical Security Systems with Smartcards", In The 7th IEEE Workshop on Hot Topics in Operating Systems,Rio Rico, AZ, March, 1999.

[8] Parnas, D.L.,"On the Criteria to be Used in Decomposing Systems into Modules", Communications of the ACM 15(12), December,1972.

[9] Saltzer, J.H., Reed, D.P., Clark, D.D.,"End-to-End Arguments in System Design", ACM Transactions on Computer Systems 2(4), November, 1984.

[10] M. Satyanarayanan,"Pervasive Computing: Vision and Challenges", School of Computer Science, Carnegie Mellon University.

[11] Case, J., Fedor, M., Schoffstall, M., Davin, J.,"A Simple Network management Protocol", Internet Engineering Task Force (RFC 1157), 1990.

[12] John Byrne, Byrne Robotics,"The John Byrne Forum", 1966 : Prediction of the Home Computer.

[13] Phil Zimmermann,"An Introduction to Cryptography"

[14] Andrew S. Tatenbaum,"Computer Networks".

[15] Behrouz Forozan,"Data Communication and Networking".

Mr. Mayur Sanjay Dabhade is a final year student at Leelavati Awhad Institute of Technology MS & R, Kanore (Thane)- India pursuing his B.E. in Computer Engineering. He has published a paper in an International conference. Web-mining and networking are area of interest.

Mr. Wrushal Kewalram Kirnapure has completed B.Tech. in Computer Engineering at Dr. B. A. Technological University, Lonere (Raigad)- India. Software testing and Computer networks are area of interest.

Mr. Jayendra Narendra Khandare, has completed B.Tech. in Computer Engineering at Dr. B. A. Technological University, Lonere-India. Artificial Intelligence and Software testing are area of interest.

Ms. Pooja Vivekrao Dange, has completed B.Tech. in Information Technology at Dr. B. A. Technological University, Lonere (Raigad)- India. She has published 3 national and 3 International papers. Neural networks and Data mining are area of interest.

Mr. Swapnil Sanjay Dabhade, has completed B.Tech. in Information Technology at Dr. B. A. Technological University, Lonere (Raigad)- India. He has published 4 national and 3 International papers. Data mining, computer networks and information Security are the area of interest.