

# Network Access and Security Issues in Ubiquitous Computing

Upkar Varshney  
CIS Department  
Georgia State University, Atlanta  
E-mail: uvarshney@gsu.edu  
Phone: 404-463-9139, Fax: 404-651-3842

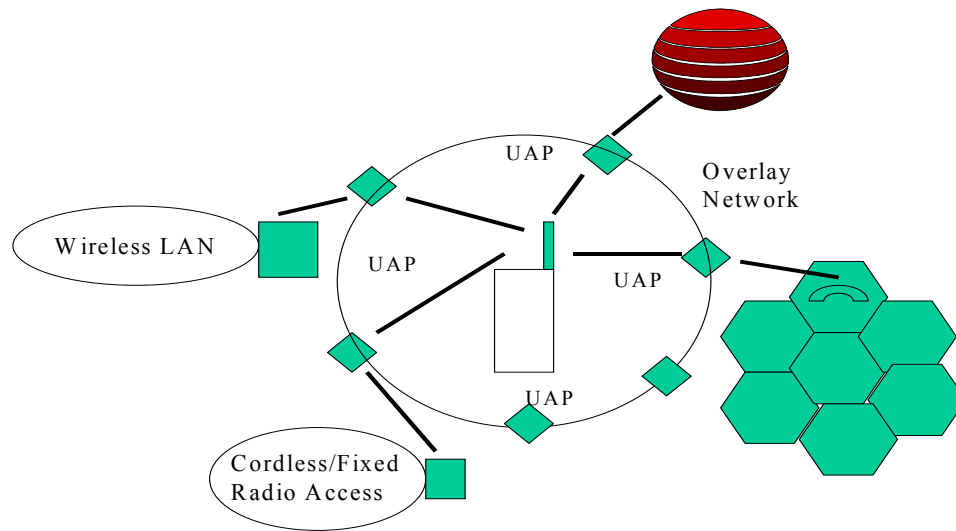
Here are several topics that we would like to discuss and explore at the workshop. These are wireless and mobile infrastructure, security, applications and services, and mobile payments. Due to our current expertise and interest, we would like to focus on infrastructure and security issues and how problems of access, coverage, roaming, end-to-end security, reliability, location management and multicast communications could be addressed in the pervasive and ubiquitous environment.

## 1. Wireless and Mobile Infrastructure

There are many major issues related to wireless and mobile infrastructure in the ubiquitous and pervasive computing environment. Since this infrastructure is likely to play a major role in how users are able to interact with ubiquitous applications and services, we believe that more research is necessary in deriving the specific role and requirements of wireless infrastructure. In general terms, the requirements could include an integrated or universal access to different wireless and mobile networks, support for group communications (multicast), reliable communications (dependable infrastructure), and interworking of these technologies. Many of these issues have not been addressed and we believe that these must be covered before the vision of ubiquitous computing is realized.

Currently, there are several different types of wireless and mobile networks available today and among each type there are multiple standards. For Cellular and Personal Communications Systems, the US standards include analog cellular, digital cellular, two versions of PCS based on time and code division multiple access, and GSM, the common European standard for wide area cellular service. One attraction behind GSM is General Packet Radio Service (GPRS), a packet data service for up to 160 Kbps. This is currently being deployed in many US cities as some major carriers are introducing GSM/GPRS for high-speed data transmission. Another technology is Enhanced Data rate for GSM Evolution, a 2.5G technology due to its usage as a transition technology to the emerging 3<sup>rd</sup> generation wireless systems. It can support up to 384 Kbps by using the link quality control, which adapts the error control technique to the current channel quality. Multiple standards also exist among CDMA, including the one used by DoCoMo for its iMode service. Additionally there are multiple proprietary wireless networks such as wireless WANs (28.8-128 Kbps), Satellites (9.6-400 Kbps, possibly higher), Wireless Local Loops (1-10 Mbps or even higher). Multiple standards also exist for wireless LANs, multiple IEEE 802.11 standards in 1 to 54 Mbps range and HIPERLAN2 at 54 Mbps. These multiple standards also differ in coverage and access protocols. The multiple standards in wireless and mobile networks make interoperability much more difficult and also limit the roaming between networks and slow down the development of new features. There have been many proposed solutions such as a worldwide common standard for terrestrial wireless services, however it remains a distant dream.

We will propose several possible architectures that would allow users to seamlessly roam across heterogeneous wireless networks. One of these architectures is based on a virtual overlay network with universal access points and these points translate the network protocols into a generic protocol for a user device (Figure 1). This architecture supports highly dependable wireless operation where the existence of multiple heterogeneous wireless networks is also very transparent to users. These UAPs will also translate frequency and QoS schemes used in a wireless network that is currently being accessed by users. Another architecture is by having an intelligent network card that can switch among two or more different wireless networks. These architectures are likely to increase coverage, provide dependable access and will offer an integrated access to mobile and wireless networks with some probability of quality of service to users.



UAP: Universal Access Point

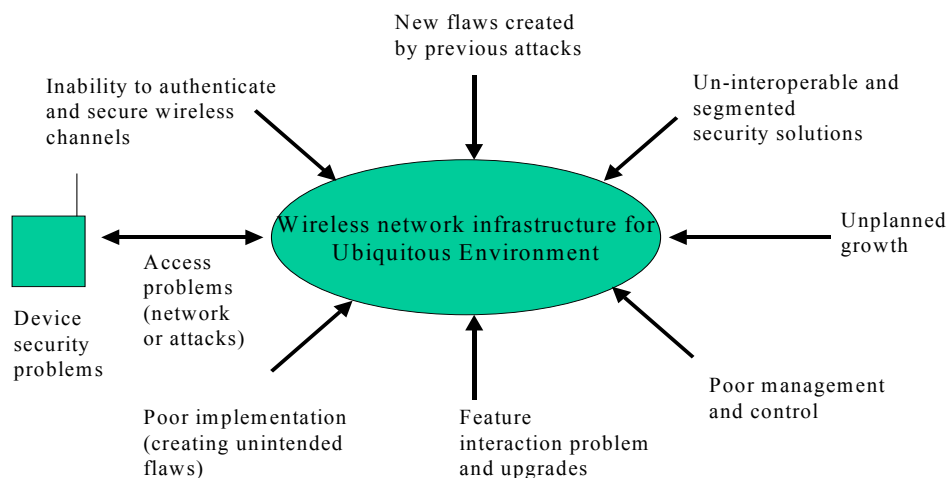
**Figure 1. Supporting Integrated Access to Wireless Networks in the Ubiquitous Environment**

In ubiquitous environment, most users do not need to know what networks they are currently accessing. We believe that focus is on personalisation and services and not so much on the infrastructure. The devices, applications and software must move across multiple heterogeneous wireless networks seamlessly without making these transitions apparent to users. Other infrastructure issues in the ubiquitous environment are ease of use (easy registration at hot-spots, easier setup etc.), new network management tools for enhanced performance (access, interference, and security management functions), creation of a localized attractive environment for customers, creating personalized and localized environment (like games for kids while parent shop, local maps, areas of interest, location-sensitive advertising, coupons for nearby restaurants and shops, etc.), support for push and pull applications, multicast and broadcast of information (such as advertisements or game score information), and support for transactions even when the user is going through brief disconnectivity or intermittent connectivity.

## 2. Security Issues

The security in ubiquitous and pervasive computing would be a major issue as individual, groups, and organizations are unlikely to put personal, important, and mission-critical information over an infrastructure that is either not secure or is not perceived to be secure. The security weaknesses of wireless and mobile infrastructure stems from both the use of multiple “incompatible” security schemes and due to “inherent” weaknesses in certain wireless security algorithm (such as wireless LANs). It should be noted that security issues are quite different in wireless networks and for variety of reasons strong security has not been implemented in wireless infrastructure.

There are many security issues in the ubiquitous environment, including confidentiality, authentication, integrity, authorization, non-repudiation, and accessibility. Other issues would include convenience, speed, ease-of-use, and standardization. Depending on the type of data and the cost of possible loss, modification, and stolen data, a security strategy must be devised and implemented. In addition to security and privacy risks, new vulnerabilities arise due to the use of wireless devices. Use of wireless infrastructure may involve multiple wireless networks with different levels of security. These could lead to possible change/deletion of information, and denial of service. In addition to these, many more security issues arise due to poor implementation, feature interactions, unplanned growth and new flaws that are created due to prior attacks (Figure 2).

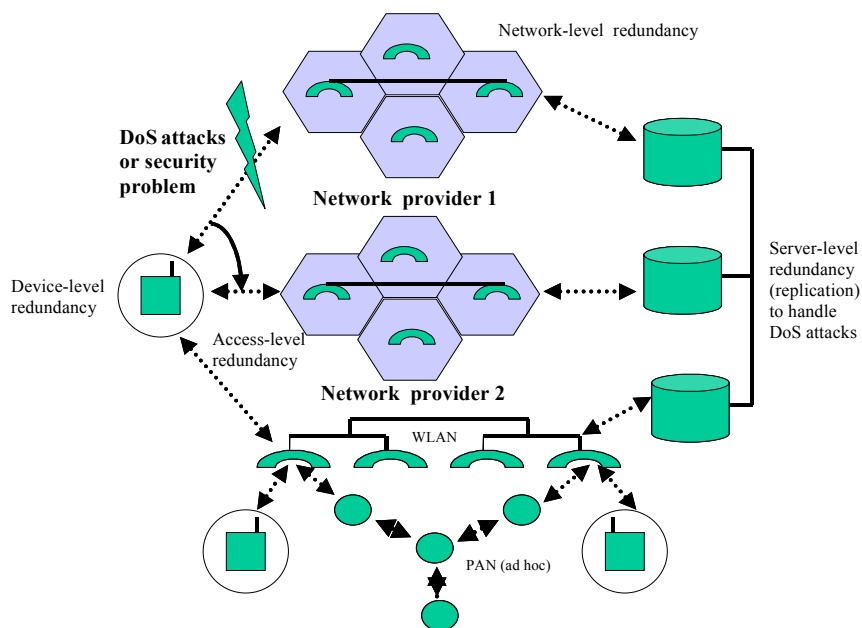


**Figure 2. Security Issues in the Ubiquitous and Pervasive Environment**

The end-to-end security issues are important in ubiquitous environment as multiple networks, devices, applications and software will exist and inter-operate. The security issues can be addressed by mobile middleware. For example, WAP provides security using Wireless Transport Security Layer (WTLS), but it does not always result in the end-to-end security (only between device and WAP gateway) [4]. It is possible to add some security feature for financial services as GSM supports both user (PIN) and device authentication (SSL). Finnish wireless provider Sonera is offering PKI on a SIM card. Another possibility is wireless PKI, a system to manage keys and certificates and requires the user to enter 2 PINs (authentication and digital signature). The WPKI is used in WTLS to support 2-way authentication (anonymous: class 1, server: class 2, user: class 3).

It has been shown that wireless security used in IEEE 802.11 has been compromised and several weaknesses have been exposed including breaking of key in few minutes by eavesdropping and analyzing the wireless network traffic. WEP is based on the use of single shared key (common to all users and kept in a software-accessible location) and no key management protocol defined so it is hard to re-key if a device is stolen or key becomes public.

We believe that secure and dependable wireless solutions must be designed and implemented before mission-critical data can be put on wireless infrastructure. The dependability problems arise due to component failures or caused by attacks. Both of these require very careful attention as far as enterprise environment is concerned. We also believe that techniques used for wireless dependability could also lead to increased security. To support dependable, secure, and integrated wireless access in the ubiquitous and pervasive environment, we propose a design solution as shown in Figure 3. The increased dependability is achieved by fault-tolerance or “added” redundancy in the wireless infrastructure. This fault-tolerance allows business transactions to be executed even when there are one or more failures in the infrastructure. This redundancy would also allow overcoming or at least alleviating denial of service attacks. If an attack occurs at device, access, network, or server levels, the redundancy would allow switching to another network, server, or device interface. The proposed solution is also scalable in terms of number of users, transactions, and the network size.



**Figure 3. A Dependable, Secure and Scalable Solution for Wireless Enterprise**

## Other Issues

### 1. Applications and Services

One of the major issues in ubiquitous computing is identifying applications and services for users. This has been a difficult task as service providers and applications developers attempt to figure out what services are needed. While some potential users wait for some new applications and services to be offered and tested, before attempting to use. A lack of killer applications has

always been a problem with many technologies, where applications and services are designed sometimes without considering user requirements, interests, and expertise. In addition to what is needed by users, other requirements are how to adapt applications and services to limited and varying amount of resources caused by user mobility, network and device constraints. It is known that personalisation and user empowerment along with context and location-awareness must be added in applications and services. We would like to explore different constraints and design parameters of new applications and services in the ubiquitous and pervasive computing environment. These could include adding location and context awareness, increased personalisation, location-dependent services and discovery and other factors in applications and services. As applications and services ubiquitous and pervasive environment could include mobile financial applications, location-aware services, mobile games and entertainment services, mobile auctions, we believe that much more work is necessary in identifying the requirements of these applications before offering an advanced version of these services.

## **2. Mobile payments**

Some of the applications would require movement of money in the ubiquitous and pervasive environment involving multiple networks and entities. Support for mobile payments will be important as the increasingly mobile workforce and individuals would use mobile financial applications and location and user specific shopping. The support for both macro and micro payments would be required. One important area of research is to look into the different roles various players could play in mobile payments. The wireless service providers could be more interested in micro payments (<\$10), while financial institutions could support macro payments (>\$10) well.

## **3. Business and Pricing Issues**

We believe that business models involving pricing and new ways of charging, revenue generation and division among carriers and operators would be an important research issue.

## **REFERENCES**

1. Varshney, U., Vetter, R. and Kalakota, R. "Mobile commerce: A New Frontier", IEEE Computer: Special Issue on E-commerce, October 2000.
2. Varshney, U. and R. Vetter, "Mobile Commerce: Framework, Applications, and Networking Support", ACM/Kluwer Journal on Mobile Networks and Applications (MONET), vol. 7, no. 3, June 2002 (pp. 185-198)
3. CTIA, Background on CTIA's Semi-Annual Wireless Industry Survey, [http://www.wow-com.com/pdf/wireless\\_survey\\_2000.pdf](http://www.wow-com.com/pdf/wireless_survey_2000.pdf)
4. Ghosh and Swaminatha, "M-commerce Security", Communications of the ACM, Feb 2001