A Testbed for Ubiquitous Computing using Next Generation Mobile Networks

Michael Hecker, Peter Leijdekkers, Valerie Gay

University of Technology, Sydney
P.O. Box 123 Broadway, NSW 2007, Australia
{Mhecker, Peterl, Valerie}@it.uts.edu.au

Abstract: Ubiquitous Computing becomes feasible in an environment where the user is always and everywhere surrounded by an environment that is able to determine the location and plans of the user. It is therefore able to provide services that are tailored to the user’s preferences. This paper describes work in progress to develop a testbed consisting of various mobile networks (WiFi, GPRS, and Bluetooth) and Motes. The objective of this testbed is to provide a ubiquitous computing environment where location-based, context-aware and tailored services can be implemented and tested. We focus on seamless-roaming, security and privacy that are important aspects in a ubiquitous environment.

Keywords: Ubiquitous Computing, Motes, WiFi, Mobile IP, Seamless roaming, security, privacy, mobile services, location-based services, context awareness.

1 Introduction

With the emergence of 4th generation networks such as UMTS and wireless LAN (WiFi), and an increase of devices (PDAs, notebooks, intelligent fridges) supporting these networks, everyone has almost permanent access to his/her preferred online services. A new technology called ‘smart dust’ or Motes [13] is in a trial stage which can be used as a sensing technology. Motes are able to sense the presence of objects (humans, vehicles etc) in its neighbourhood. They are mini computers with a size of a 50 cents coin and equipped with a radio transmitter that send signals to other Motes. A Mote collects and communicates small amounts of data such as temperature, vibration or light intensity readings and sends it to a host computer which converts it into meaningful information [14].

This combination of mobile networks with new technologies such as Motes open the way to ubiquitous computing where users can access services tailored to their personal preferences. Ubiquitous computing is a widely used term and in this paper we restrict ourselves to the following characteristics:

- **Context awareness** which is divided in three components [1]. Firstly, the environment where the person is situated in. The environment can be the location of the user but also the physical properties such as brightness and noise levels around the person. Secondly, the person itself which can be characterised by personal properties such as age, gender and education but also the mental state or physical health. Thirdly, the activities the person is involved in. Activities relate to the tasks and goals of that person or events that occur such as a sudden change in weather.

- **Personalisation**: an important aspect of ubiquitous computing in 4G is personalisation. This means that tailored (mobile) services are offered according to the context of the person. A user has a certain profile or preferences, and services are offered taking this into account. We regard location awareness as an important aspect of ubiquitous computing in 4G since knowing the location of a person facilitates the offering of personalised services.

A ubiquitous service would be for example a lecturer entering a lab equipped with audiovisual equipment, WiFi and Motes. Upon entering the lecturer’s PDA roams from a GPRS network to the Lab’s WiFi network and is offered a web based application which allows the lecturer to control the audiovisual equipment. The motes in the lab sensed the presence of the person and based on the user profile of the lecturer it allows only him/her to control the equipment.

To realize ubiquitous computing in 4G we need an infrastructure that supports seamless roaming, security and privacy mechanisms. **Seamless roaming** allows the user to switch network without interruption of the voice and data connection. Seamless roaming is already realized within a single mobile network (e.g. GSM) but not between different network technologies. **Security mechanisms** need to be in place to guarantee secure transfer of user sensitive information such as user profiles and location information.
information. **Privacy mechanisms** need to be in place to protect the user from malicious usage of information.

Currently, the various network technologies operate independently from each other. To achieve true ubiquitous computing experience, these networks need to interoperate and allow the user to seamlessly roam from one to another without losing the connection and without signing on for each access network. Current solutions such as public WiFi hotspots force the user to sign on each time it enters or leaves a public hotspot. Additionally context aware services do not exist based on the user profile and preferences. Motes are a new technology and integration with WiFi technology is an unexplored area. A challenge is to combine information sensed by a mote to provide localised context aware services.

This paper describes work in progress of a testbed integrating some of the ubiquitous characteristics, i.e. seamless roaming and (location-based) context awareness. The testbed is being developed at UTS, Faculty of IT. It incorporates several wireless network technologies (WiFi, Bluetooth and Motes) and its aim is to provide a platform to test, implement and research ubiquitous services for 4G networks.

Based on an end-user scenario we identify several major requirements for ubiquitous computing in a heterogeneous mobile network. We then present our testbed and discuss open issues and future work.

2 Scenario

We are in 2006 and John and Lisa, just like almost everyone of their generation have subscribed to a MeetMe service which is a very popular location-based service that helps them to meet people with similar interests/profile. The MeetMe service is used for example to find a tennis partner, or someone to go shopping with but also to catch up with friends when they are in the neighbourhood.

Upon her arrival at the Adelaide airport, Lisa sets her profile to ‘catch up with local friends’ and she is curious to see how efficient the MeetMe service is. The MeetMe service starts immediately looking for her friends located in Adelaide and notifies John that his old friend Lisa is currently in town.

At that time, John is on his way to his office and is running late. Looking forward to meet Lisa after work, he quickly adds Lisa to his MeetMe ‘friends contacts’ list. He also authorizes the MeetMe service to notify her that he is in the neighbourhood. When John enters his office his profile is automatically set to ‘business’ which makes him invisible to his non-business contact list (context awareness).

Lisa is on the bus from the airport to the city, watching the news on the Internet from her PDA (seamless roaming), when she receives the notification from John via the MeetMe service. She tries to locate him but John stays invisible (privacy/security). She adds him to her MeetMe ‘private contacts’ list and authorizes him to contact and locate her.

When John leaves the office, he contacts the MeetMe service to locate Lisa (pull service). A map on his PDA shows that she is in a park only a few kilometres away. He contacts her via the MeetMe service and they agree to have dinner together and meet at a Greek restaurant not far from Lisa’s current location. The Greek restaurant was a suggestion made by the MeetMe service since both indicated in their profile that they like Greek food (profile info). The MeetMe service also evaluates the time John and Lisa need to reach the destination. Lisa is just 5mn walk away and John needs to take the bus in 10mn at the bus stop one block from his current location. When he reaches the bus station, John reads on the information board that his bus is delayed and will arrive 30mn later (motes detection) and he decides to catch a cab instead. On his way to the restaurant, while passing a movie theatre, a pop-up shows up on his screen advertising for a new thriller movie (push service), his preferred movie type (user preferences). Maybe an idea for after the diner? But he promises himself to deactivate those pop-ups which can be sometimes annoying (privacy).

3 Issues to be solved

This section discusses several important issues that need to be solved to realize the scenario as described above and that we will address in our research. They are seamless roaming, IP connectivity, Authentication, Security, Privacy and Context Awareness (which includes user location and user profile).
Seamless roaming

For Lisa to be able to watch the news while being on the bus, we need seamless roaming for voice and data. Normally when roaming between different networks the data connection is terminated and has to be re-established. This results in an interruption of all services, which rely upon that connection. When a new connection is made, the user usually gets a new IP address and all previous TCP/IP sessions need to be re-established, which takes time and can be interruptive for the end user.

Seamless roaming is not just maintaining the data connection but also all related issues involved in this process like keeping the context of the application and automatic sign-on upon authentication in the new network. Lisa should neither be concerned about the different access network technologies involved, nor about the different operators of those networks and their authentication process. For example she should not have to sign up manually with an access network provider when she roams from one network to another. This should be done automatically.

IP connectivity

We will use IP connectivity to realise the scenario in section 2 since IPv4 is the most commonly used protocol nowadays. However, IPv4 will run out of unique addresses when a vast amount of mobile devices hit the market each requiring a unique IP address. A Network Address Translation (NAT) solution or IPv6 will be required. NAT is possible but it does not allow the device to be globally contactable by other parties. This is an essential requirement for mobile devices, since it must be contactable when messages are sent to the mobile device. Therefore IPv6 is the most appropriate solution and in order to support seamless roaming we need to use Mobile IPv6 [2]. This technology allows the device to maintain one IP address, the so-called Home address. Other users will use this address to contact and send data to the device which is then forwarded to the network where the mobile device is currently residing. Mobile IPv6 is available nowadays but several problems exist. One issue is the handover process which can be fairly long, resulting in possible packet losses and high latency. Furthermore, the intermediate systems have a higher processing load which might affect the availability when many handover processes occur. To minimize the latency and packet loss two solutions are proposed in [3] and [4] which are ‘Fast Handover Protocol’ and ‘Hierarchical Mobile IPv6’

Authentication

An important element in ubiquitous computing is for the service to know who the person is using the networks and services. This info will be essential for getting the right user profile and context information and also to be able to bill the use of the network and of the service.

The user needs to be authenticated to use the different Access Networks. This can be done via a roaming provider (RP) [10]. Its role is to maintain the relations with the network access providers (NAP). The user obtains the authentication credentials from the roaming provider, which can be used for network access authentication. These credentials can either be a username/password or a certificate. A username/password combination is not as secure as a certificate but it does not need a Public Key Infrastructure to make it work. This makes username/password combination easier to use for ‘not too sensitive’ information exchange. However, the user will need to provide his credentials to the network access provider in a secure way. The Extensible Authentication Protocol (EAP) [15] is a standard solution which can be used for this purpose. When a network access provider receives a request from a user that wants to use its network, it needs to verify the validity of the request. In our case, the network access provider will not maintain a database of users that roam into its network but will verify the credentials against the roaming provider that has issued the credentials. The RADIUS protocol [12] offers a standard solution for this problem and a detailed description of network authentication is described in [11].

Service Providers also need to verify the identity of a user that wants to use a particular service such as the MeetMe service. Verification can be done as described above using a Roaming Provider. The user will send his credentials to the service provider, which will verify the information against the roaming provider. However, this raises some additional authentication issues, as everyone can be a service provider. Does the user really want to give this information to a service provider s/he might not necessarily trust, which might use the information for other purposes like getting access to a network with the user’s credentials? One solution can be that a roaming provider has to verify the truth worthiness of a service provider. While this is a convenient solution for the user, it is not really a secure one. The roaming provider should therefore issue a second kind of credential, which can only be used with service providers or even tokens which can be used only once. While this reduces the risk of misuse, as the credentials are not valid for the actual network access, abuse is still possible. Additionally, a service provider could fake being a particular service provider and obtain the credentials from the user. To overcome this, service providers should also be verified towards the user and not just the user towards the service provider. Finally, service providers should also have a means to authenticate themselves against each other to avoid misuse.
Security

Security plays an important role when the user transmits data over a network, which cannot be trusted or is insecure due to the lack of security/encryption mechanisms. Nowadays, data is sent over a secure connection (SSL) when the content is confidential like a money transfer or online ordering over the Internet. In some wireless networks such as GSM, the data between the mobile device and base station is encrypted. Security for public WiFi networks is in its early stages. A promising solution for public WiFi networks is the use of a standard security framework as defined by IEEE 802.1x [9]. Even if the wireless link is secure, other parts of the network can be still insecure. A solution could be the use of SSL, IPSec [7] or VPN. However the signalling between the home agent and the mobile device is still vulnerable using mobile IPv6. Therefore, signalling data must also be secured, which can be achieved using IPSec as described in [5]. Other approaches exist but incur more complexity such as ‘Tiny SESAME’ [6]. This is a lightweight reconfigurable security mechanism for 3G/4G mobile devices based on Kerberos [8] and protects both voice and data connections.

Privacy

Privacy is an issue in a networked environment and it is important to know where and which data is stored and who has access to it. When people are connected to a network most of the time it is possible to locate them whenever the device is switched on. The party (Roaming Provider in our case) that provides the authentication of the user has the information about the network the user is accessing. The network access provider has the information about the location of the user but does not necessarily know who the real person behind the device is. It is the roaming provider that has the overall view which implies that strict privacy policies must be implemented to meet regulatory privacy laws. For example how long can the Roaming Provider store location information about a user and which service providers may use location information to offer their services?

Apart from location based information, other personal information such as profiles and preferences will be stored by the different providers. It is important that parties only store the information they need to offer their services. For example, it is not relevant for a network access provider to know the user’s restaurant preferences used by the MeetMe service. This is information that should be only known to the MeetMe service provider.

Context Awareness

The user in a 4G network will be able to use various services depending on the context of his environment. Different technologies can be used to obtain the context of a user such as measuring the physical condition of a user (body temperature/heart rate etc) or by determining the location of the user (John entering his office). We focus on user location information for context awareness in this paper.

User location information can be provided by the terminal using a GPS receiver or by sensors such as Motes. It is also possible that the network determines the location of a user [10]. In this case the network access provider sends the location data to the roaming provider. Based on the location, a service can adapt its content. For example when Jack passed by the cinema a popup is shown advertising for the latest movie shown in that theatre which also takes into account his movie preferences.

4 Testbed

This section focuses on the testbed which allows us to demonstrate and evaluate the scenarios of section 2 by creating an environment for ubiquitous computing.

The Roaming Provider (RP) is the party with whom the end-user has a contract. It issues the credentials for the user which can be stored on the mobile device (PDA, Laptop) of the user. The RP software is hosted on a Linux machine which also consists of a router and hosting the Home Agent (HA) for mobile IPv6. The RADIUS server used for authentication as well as an application server and database are located in the RP domain. The application server is used for subscription matters as well as responding to user location requests based on Parlay X as described in [10] made by third party service providers. The database hosts the credentials and relevant user profile information.

Third party services are hosted in the service provider domain, which is represented in the testbed as a set of computers each implementing a particular third party service. Typical software would be an application server (J2EE, .Net), a web-server (Apache, IIS) and a database (Oracle, MySQL), but can easily be adapted to the particular needs of a third party service provider.
The testbed consists of three access networks, to demonstrate different roaming scenarios such as inter-domain and inter technology roaming. The access networks use different subnets to reflect a commercial environment.

- The first wireless network supports IPv6 with mobility support. It consists of a gateway computer, which runs the Foreign Agent for Mobile IPv6. The network consists of two IEEE 802.11b compliant access points to demonstrate roaming between access points and also to retrieve information to which access point the user is connected. Furthermore, the network has a Mote base station and motes. The motes in this network communicate with the mote base station as well as with mote-enabled mobile devices. The access points are connected to a hub, which is connected to the gateway. The mobile devices consist of a laptop and a PDA with mobile IP.

- The second network also runs IPv6 and has a gateway supporting a foreign agent for mobile IP. The network has an IEEE 802.11b base station and a wireless Bluetooth base station. It will enable us to demonstrate seamless roaming between these two technologies. The gateway can be queried for the location of users that are accessing this network.

- The third network runs IPv4 and has one wireless access point. This type of network is added to show scenarios where the target network only supports IPv4 which is the case for most mobile and fixed networks of today. A different technique will be used to support mobility in these types of networks.

The gateway computer of each access network runs a RADIUS proxy, which forwards authentication requests to the RADIUS server of the Roaming Provider. The central router is only used to route traffic between the different subnets and will be used to monitor data traffic. The router has a connection to the public Internet to simulate scenarios with external third party service providers and other roaming providers.
5 Conclusion

This paper described work in progress and we are currently in the process of setting up the testbed. We encountered several issues that need to be solved:

- **When will mobile IPv6 be widely supported?** The mobile devices need to support mobile IP. As far as we know, neither Windows CE, nor any other Windows operating system has stable support for mobile IP. While IPv6 is supported in the most recent versions of Microsoft Windows (XP), Windows CE (.NET 4.2) and Windows XPE, there is no enhancement with mobility so far. The only implementation for mobile IPv6 can be found in Windows 2000 SP1, which was a research project and is not maintained any more. We decided to use a Linux version with mobile IP support for both the laptops and PDAs.

- **How to express contracts (or Service Level Agreements) between the end users and the providers?** Additionally, is policy-based networking the best alternative to switch from one network to another? Who decides which policies are applied when? A challenge will be to determine when a handover should occur between two different networks. We need to develop an application on the mobile device that is able to obtain the information from the access networks that are currently accessible and is able to switch to another network according to certain policies. Switching can be based, for example, on the signal strength (QoS related), security rules or cost related (switch to the cheapest access network). To achieve seamless roaming, most of these policies should be defined beforehand in a contract between the end-user, the network access provider and the third party service provider. Also the access network can exercise policies whether or not allowing a mobile device to access the network depending on current traffic load.

- **How to optimize the handover to achieve seamless roaming?** As identified before, the handover process is not seamless yet. We need to look into solutions to achieve handover as fast as possible without loosing data. Optimizations for mobile IP exist but most of them are still experimental.

- **What will be the role of the Motes for location based information?** Motes are a new technology and not yet as evolved as required for the scenarios described in this paper. Whereas we are convinced they will play an important role in the testbed, we do not know yet to which extend they can be used in our testbed for obtaining the user location.

We expect the testbed to be operational within two months. We will then focus on how the different providers interoperate and how service level agreements are established and realized.

Acknowledgement

We would like to acknowledge Elaine Lawrence and Josep Riudavets for their discussion on Motes as well as former colleagues from Lucent Bell Labs, the Netherlands for their expert advice on the testbed.
6 References


