

A Virtual Learning Environment for Mobile IP

Laura Bergström, Kaj J. Grahn, and Göran Pulkkis
Arcada Polytechnic, 00550 Helsinki, Finland

laura.bergstrom@arcada.fi kaj.grahn@arcada.fi
goran.pulkkis@arcada.fi

Abstract

This paper presents a virtual learning environment for Mobile IP (Internet Protocol). The learning environment has been produced in a production circle of Virtual Polytechnic of Finland. Protocols and mechanisms for secure mobility in the Internet are surveyed. A detailed description of the development of the learning environment and the content of the Mobile IP animation is given. The chosen didactical approach and the graphical design of the learning platform are presented and motivated. The IT technology and the IT infrastructure needed to implement and use the learning platform are also described and assessed.

Keywords: animation, didactical, learning environment, Mobile IP, security

Introduction

Today, the number of wireless and mobile devices connected to the Internet is strongly growing. Wireless links and networks, mobile users and mobility-related services form an increasing part of the Internet infrastructure. These wireless and mobile parts are normally connected to larger, wired networks. Mastering the key concepts in mobile, wireless and wired technology areas are therefore of increasing importance in the society of today.

There is a distinction between wireless and mobility. You can find many networked environments in which the network nodes are wireless but not mobile. Such examples are wireless home and office networks with stationary workstations. A limited form of mobility that does not require wireless links is the use of a wired laptop at home and in the office. A both wireless and mobile example is the scenario where a mobile user is maintaining a voice-over-IP call while racing down the autobahn. The various degrees of mobility, from the network layer's point of view, can therefore be presented as a user moving only within the same wireless access network, as a user moving between access networks shutting down while moving between network and as a user moving between access networks maintaining ongoing connections (Kurose & Ross, 2005).

Mobile Internet Protocol (IP) is an extension to the standard IP for use in mobile applications.

Material published as part of this publication, either on-line or in print, is copyrighted by the Informing Science Institute. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation on the first page. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission and payment of a fee. Contact Publisher@InformingScience.org to request redistribution permission.

The standard allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to a network with a different IP address. According to the ISP Glossary 2005:

A common analogy to explain Mobile IP is when someone moves his residence from one location to another. Person moves from Boston to New York. Per-

son drops off new mailing address to New York post office. New York post office notifies Boston post office of new mailing address. When Boston post office receives mail for person it knows to forward mail to person's New York address.

Mobility management skills are needed by practically any user of a mobile device connected to a wireless network. Presently, there is a growing demand for wireless network professionals. Typical areas of interest include mobility management principles, development of wireless network technologies, methodologies and standards, and delivery of support and training to mobile users and professionals in wireless network related issues

A virtual, survey oriented Mobile IP environment, developed for students, will give highly needed, specialized, and also custom designed network education.

The Mobile Internet Protocol

The Mobile Internet Protocol (Mobile IP) was developed for the network layer to support mobility. The Internet architecture and protocols for supporting mobility are defined primarily in the standard RFC 3344 (Perkins, 2002). Objectives related to the development of Mobile IP include (Schiller, 2000):

- *Compatibility.* Mobile IP does not require changes to end-systems, routers, applications and network protocols already in use. Data link layer protocols as IP are also supported. Furthermore, Mobile IP has to ensure that mobile end-systems can communicate with fixed systems.
- *Transparency.* Higher protocols, like TCP (Transport Control Protocol), continue to work even if the mobile unit changes its network attachment point. This implies that mobility remains 'invisible' for higher level protocols and applications.
- *Scalability and efficiency.* Mobile IP has to be scalable over a large number of participants of the Internet. Enhancing mobility must not degrade the efficiency of the network.
- *Security.* Minimum requirements are message replay prevention and authentication of all registration messages.

The Mobile IP standard consists of three main areas (Kurose & Ross, 2005). *Agent discovery* is a procedure where a home or foreign agent advertises its services to be used by the mobile node. When care-of-addresses (COAs) are registered and deregistered with the mobile node's home agent and COA defines the current location of the mobile node from an IP point of view, the procedure is called *registration*. The third main area is *indirect routing of datagrams*, i.e. datagrams (packets) are forwarded to mobile nodes by the home agent. This includes rules for handling error conditions and different forms of encapsulation.

Packet Delivery

Data transfer to/from a mobile node in a typical example network is illustrated in Figure 1. The used terminology is defined below (Schiller, 2000):

- *Mobile node (MN).* A mobile node is a host or router that changes its point of attachment from one network or subnetwork to another. The mobile node may communicate with other Internet nodes without changing its IP address.
- *Correspondent node (CN).* A correspondent node is a mobile or stationary peer communicating with a mobile node.

- *Home network.* The network to which the mobile node is normally attached with respect to its IP address.
- *Foreign network.* The network in which the mobile node is currently residing and which is not the home network.
- *Home agent (HA).* The home agent is implemented on a router connected to a mobile node's home network. HA maintains information about the device's current location.
- *Foreign agent (FA).* The foreign agent provides services to the mobile node during its visit in the foreign network. Typically, the foreign agent is implemented on a router connected to the foreign network.
- *Care-of-address (COA).* The care-of-address defines the current position of the mobile node. Packets sent to the mobile node are delivered to the care-of-address using tunnelling, i.e. the care-of-address marks the tunnel endpoint. There are two types of COA:
 - *Foreign agent COA.* The COA is the IP address of the FA
 - *Co-located COA.* An additional IP address which acts as COA is given to the MN
- *Binding cache (BC).* A cache of mobility bindings of mobile nodes, maintained by a node for use in tunneling datagrams to those mobile nodes.

In Figure 1, a CN is connected via a router to the Internet. The HA and the FA are implemented on corresponding routers connected to respective networks. The MN is currently in the foreign

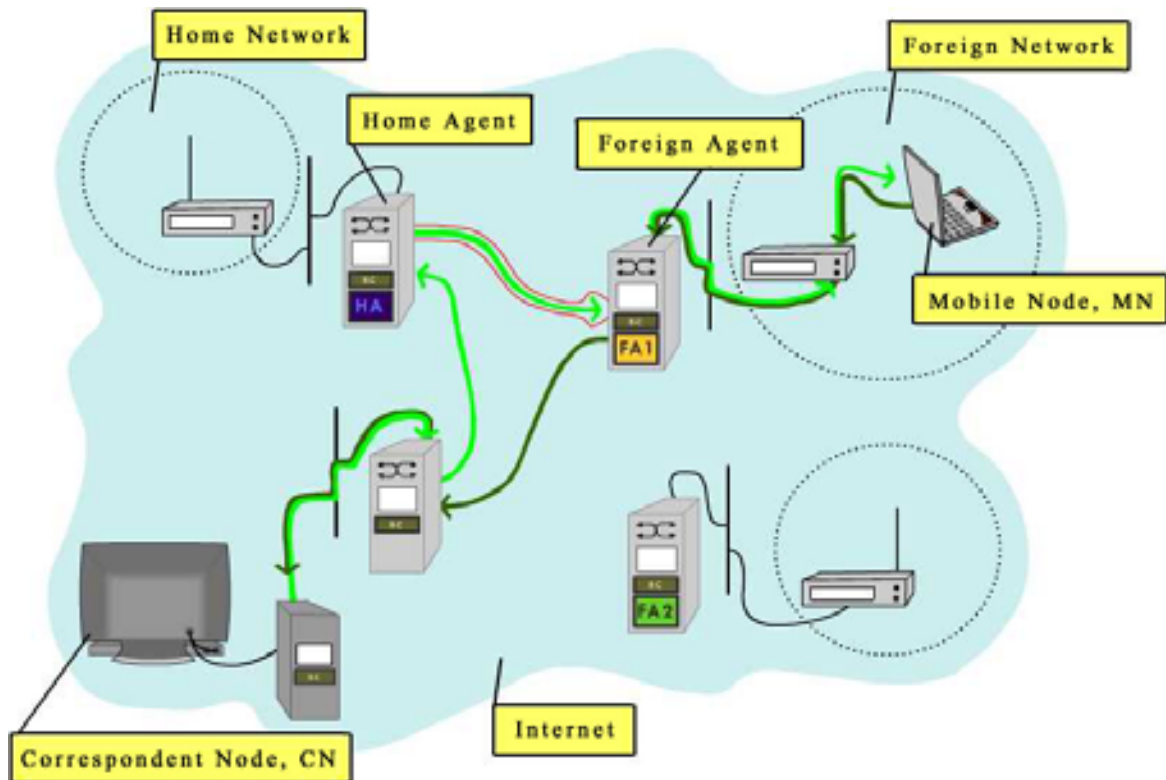


Figure 1: Data transfer to/from the mobile node in an example network.

network. The correspondent node wants to send an IP packet to the mobile node. The ordinary IP address can be used although the current position of the mobile node may not be known. The packet delivery process starts by CN sending the packet to the IP address of the MN. The HA knows that the MN is not in its home network and intercepts the packet. The packet is now encapsulated and tunnelled to the COA in FA. The FA forwards the packet to the MN.

Agent Discovery

After moving the mobile node has to find a foreign agent. The discovery of a new foreign agent and a new network address tells the mobile node that it has moved into a new foreign network. This is called *agent discovery*. This procedure can be accomplished by *agent advertisement* or by *agent solicitation*. In agent advertisement available services are advertised by the foreign or home agent. These beacon broadcast messages are handled by the Internet Control Message Protocol (ICMP) including some mobility extensions. When a mobile node doesn't want to wait for a receiving agent advertisement it can broadcast an agent solicitation message. The agent will then directly unicast an agent advertisement to the mobile node.

Registration

Registration is performed in order to inform the HA of the current location of MN. One role of the foreign agent is to create the COA for the MN. Registration takes part after MN has received the COA. Two addresses are then associated with the MN, its permanent address and its COA (care-of-address, foreign address). The registration procedures depend on the location of the COA (Schiller, 2000). When the COA is at the FA, the MN sends the registration request with the COA included to the FA, which forwards the registration to the HA. In this case the procedure is accomplished by *registration of a MN via the FA*. When the COA is co-located, the MN sends the request directly to the HA and the HA sends its registration reply back to the MN. This is *direct registration of a MN with the HA*.

Tunneling and Encapsulation

Forwarding of packets between the HA and the COA in FA1 is illustrated in Figure 1. A virtual pipe, a *tunnel*, has been established between the two endpoints. Data packets are forwarded unchanged inside the tunnel. This mechanism is achieved by *encapsulation*, i.e. the packet header and data are put into the data part of a new packet. The encapsulated packet is then routed to the COA. There are different types of encapsulation:

- *IP-in-IP encapsulation*. This type of encapsulation follows the standard specification of the IP protocol. Several fields in the inner (original) and the outer (new) IP header are redundant.
- *Minimal encapsulation*. In this optional method the number of fields of the inner header is reduced due to the redundancy. The minimal encapsulation scheme works only for IP.
- *Generic routing encapsulation (GRE)*. Generally, the system has a packet that needs to be encapsulated and delivered to some destination. The packet (payload) is first encapsulated in a GRE packet, then encapsulated in some other protocol and finally forwarded. This outer protocol is called the delivery protocol.

Optimization of Packet Forwarding

In the basic Mobile IP protocol, packets to the MN go through the HA. In some cases this will cause additional and unnecessary overhead for the network. The packet route is made of three segments, CN to HA, HA to COA/MN, and MN back to CN. This is called *triangular routing* (Schiller, 2000).

The route can be optimized by informing the CN of the current MN location. The update is given by HA. CN makes use of a BC. This cache is a part of the local routing table for the CN. Optimization of the original Mobile IP protocol includes four additional binding messages: request, update, acknowledgement and warning (Schiller, 2000).

Reverse Tunneling

In the solution illustrated in Figure 1, the MN sends directly its packets to the CN according to the standard IP. This solution has some severe problems (Schiller, 2000). A *firewall* can cause problems because it can be set up to filter out malicious addresses. The MN sends packets with a fixed IP address as source which may not be allowed in a foreign network. *Multicast* packets cannot be transmitted by the MN located in a foreign network, a reverse tunnel is needed. When the MN moves to a foreign network, the *TTL (Time To Live)* field may be too low for the packets to reach the destination nodes. Also in this case reverse tunnelling is needed.

Reverse tunnelling can briefly be described by a sequence where the MN is transmitting to the FA, the FA tunnels packets to the HA by encapsulation and finally the HA forwards the packets to the receiver CN in a standard way.

Reverse tunnelling as an extension to Mobile IP is described in RFC 2344 (Montenegro, 1998).

Roaming

Roaming refers to the ability of the MN to move from one access point coverage area to another without interruption in service or loss in connectivity (Webopedia, 2005). This is the case when the MN changes its location from an old FA and registers with a new FA. The HA and the old FA will then receive binding update messages from the new FA/MN. If the CN is sending to the old FA, the FA now notices that the packets have the destination MN and forwards these packets to the COA in the new FA. This procedure provides *smooth handover*. Smooth handover is a kind of handover operation that minimizes data loss during the time that the mobile node is establishing its link to the new access point.

Mobile IP Security

A MN uses wireless data communication. Physical access control to the communication media can only be implemented for wired data communication. Network security issues are therefore especially important for Mobile IP. Security goals and requirements must be defined. Risks, attack possibilities, and vulnerabilities must be thoroughly assessed. Solutions for secure authentication and protected data communication are needed.

Security Goals and Requirements

Two fundamental goals of Mobile IP security have been defined. When the MN visits a foreign network

1. it has the same connectivity and safety as in its home network

2. both the home network and the visited foreign network are protected from active and passive attacks.

To achieve these security goals the following security measures have been considered to be necessary:

1. Mobile IP registration and location update messages must have
 - *data integrity protection*
 - *data origin authentication*
 - *anti-replay protection*
2. *Access control* of resources in foreign networks used by visiting Mobile Nodes
3. IP packet redirecting tunnels must provide
 - *data integrity protection*
 - *data origin authentication*
 - *data confidentiality*

Moreover, MNs should have *location privacy* and *anonymity* (Zao et al., 1999).

Risks, Attacks and Vulnerabilities

Risks of, attacks on and vulnerabilities of Mobile IP are surveyed in Islam (2005) and listed below:

- *Denial-of-Service (DOS)*. This attack has two forms, TCP SYN packet flooding or redirection of data packet flow. Strong authentication of all registration messages prevent some DOS attack patterns.
- *Replay Attack*. In this attack a valid Registration Request is tapped and replayed by a malicious node. Use of time stamps or nonces in combination with strong authentication of registration messages give protection against replay attacks.
- *Passive Eavesdropping*. In this attack a malicious node listens to the data communication from a mobile nod. Encrypted data communication gives protection.
- *Session Hijacking*. In this attack an intruder node sends a false registration message to a CN. This message claims that the legal MN has moved to the care-of-address of the intruder node. Encryption of end-to-end or Link Layer data communication gives protection.
- *Malicious Mobile Node Flooding*. In this attack a malicious node is a valid mobile node, which with legal registration request messages redirects data traffic from the CN to a victim node.
- *Other Intrusion Attack*. A malicious node may get physical access to a network socket or use the air interface for intrusion attempts. To prevent this type of attack
 - a visiting MN must be fully registered to the FA before any data packets are routed
 - Link Layer data communication encryption is required from every MN trying to connect to a FA.

Security Solutions

Replay prevention with timestamps or nonces for all messages exchanged within the base Mobile IP protocol is specified in Perkins and Calhoun (2000). Other Mobile IP security solutions specify authentication schemes and protection of data communication.

Secure Mobile IP Authentication with AAA Servers

The base Mobile IP protocol specifies a Mobility Security Association (MSA) between a MN and the HA. This MSA is used to authenticate the Registration Request sent from the MN to the HA. The base Mobile IP protocol also supports an optional MSA between the MN and the FA as well as an optional MSA between a FA and a HA. These two MSAs are used for authenticating of registration messages when a MN connects to a foreign network (Perkins, 2002).

The Authentication, Authorization, and Accounting (AAA) requirements for the base Mobile IP protocol are specified in Glass, Hiller, Jacobs, and Perkins (2000). In Calhoun, Johansson, Perkins, Hiller, & McCann (2005) is specified how these requirement can be fulfilled by the Diameter AAA protocol. Secure Mobile IP registration in a foreign network requires that

- the Foreign Agent is a client of an AAA server of the foreign network of the Mobile Node
- the Home Agent is a client of an AAA server of the home network of the Mobile Node
- both AAA servers have a trust relationship.

Figure 2 shows the request/reply handshake message exchange in the AAA infrastructure, when a MN is registered in a foreign network. AAAF is the foreign network AAA server and AAAH is the home network AAA server.

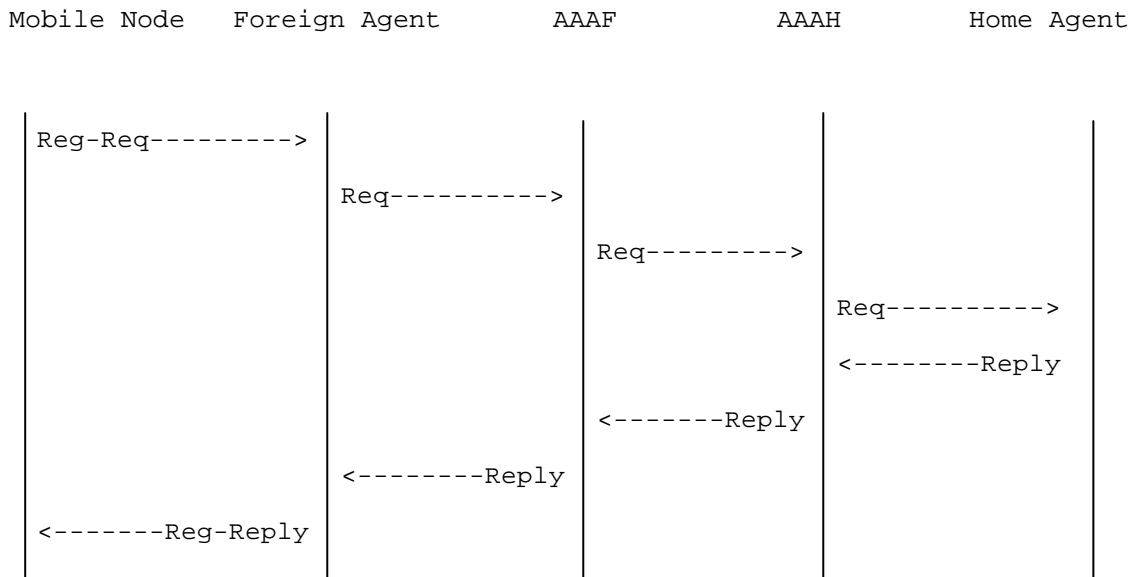


Figure 2: Mobile IP/Diameter Message Exchange (Calhoun & al, 2005).

Secure Mobile IP Authentication with Public Key Cryptography

A Mobile IP authentication extension using a X.509 certificate based PKI has been proposed in an expired Internet Draft (Jabobs & Belgard, 2000). In this scheme all nodes participating in MN registration have a X.509 certified public/private key pair.

Also Mobile IP authentication extensions using an identity based public key cryptosystem, which was first introduced in 1984 (Shamir, 1984), have been proposed (Hwu, Chen, & Lin, in press; Lee, Choi, Kim, Sohn, & Park, 2003). In an identity based public key cryptosystem the public key is derived from public information that uniquely identifies a network user or a network node, for example the email address or telephone number of a network user and `node_name@dns_domain_name` for an Internet connected node. The corresponding private key is obtained from a trusted Private Key Generator.

An extension of the base Mobile IP protocol specifies authentication based on MN identities and other network host identities in the form of Network Access Identifiers (NAIs). A NAI is derived from `hostname.realm`, the Fully Qualified Domain Name of a network host, as `hostname@realm` (Johansson & Johansson, 2004).

Protected Data Communication

A MN often uses a WLAN connection in the home network and in a foreign network. WLAN Link Layer protection is provided by the security protocol WPA or IEEE 802.11i. For protected end-to-end Mobile IP data communication, several IPSec based solutions have been presented (Barun & Danzeisen, 2001; Islam, 2005; Zao & Condell, 1997). Also SSL or SSH encryption or an identity based public key cryptosystem (Hwu et al., 2005) provides protection for end-to-end Mobile IP data communication.

Learning Environment Design

The importance of a well-planned learning environment grows especially in products aimed for learning, as the use of the product must fall into a secondary place and be almost an unnoticeable action. The interface should support the content of the product and lead the user in his/her learning process. A learning environment should not be the cause of any unnecessary frustration and should instead permit an easier interpretation of the study material. In fact, the interface of the product should support direct interaction, in other words, it should let users be able to spend their full cognitive resources on the task, not on the interface. As a result, the interface becomes invisible to users and on the contrary the task becomes transparent. This is achieved by minimization of the *gulfs of execution* and *gulfs of evaluation*, which are created when executing any particular task. More in specific, according to Norman's seven stages of action any activity is composed of many cycles of the following stages of activities: establishing the goal, forming the intention, specifying the action, executing the action, perceiving the system state, interpreting the state and evaluating the system state with respect to the goals and intentions. The gulf of execution in this cycle is the gap between intention and action, and the gulf of evaluation is instead the gap between perception and evaluation (Norman, 1988; as cited in Griffiths, n.d.).

This model brings to evidence the importance of considering principals like

- visibility
- presentation of operations and results in a coherent, consistent system image
- efficient relationships between elements and their effects
- feedback

when designing elements for an interface (Norman, 1988; as cited in Griffiths, n.d.).

The best way to achieve these objectives is to divide the design of the interface, or the learning environment, to two dimensions: to a communicating dimension, *the interface*, which describes the interaction between the user and the learning environment and to an esthetical dimension, *the layout*, which describes the visual style of the product. As communication goals are more easily achieved with a strong esthetical structure (Mullet & Sano, 1995), these two dimensions are very much dependent of each other and only together can they make a learning environment a place where the interface supports the execution of tasks and therefore supports learning.

The functionality of the learning environment can be divided in usability and comprehensibility. The aims of its functions are described in the communicating dimension of the design. In the esthetical dimension topics like the problem of space, harmony of colors, and right font type are confronted.

Didactical Objectives

The “Mobile IP animation” is a learning object, which can be integrated in virtual network courses as well as in traditional network courses.

The chosen didactical approach is a structured animated network environment in which the communication between a CN and a MN can be studied. The communication logistics for all options of the Mobile IP can be studied on the highest level. Communication details, like the data packet header fields, can be interactively studied on lower levels of the animated environment.

Mobile IP Implementation

The learning environment should be a static and scalable framework for the dynamic features of Mobile IP. The underlying visualization model of the Mobile IP animation includes following features:

- communication architecture
- Home Network with HA Router
- two Foreign Networks with FA Router
- a Corresponding Node, CN
- data communication paths
- fundamental data structures
- flow of data packets
- structure of data packets.

Integration of additional Mobile IP features is supported.

The animation is implemented in an environment where a big part of the elements are symbols, in other words they are elements that have a conventional relationship to their referent. This means that the referents, the technical objects, are typically described with these more easily comprehended symbols or graphical elements. Internet is described with the help of a cloud, networks by an area in this cloud, and routers are computers that are labeled with the symbol of a router (☐). Data packets in data communication are described with rectangular boxes that are similar to packets. Nevertheless there are also elements that are described through their imaginable physical appearance. These elements are the information flow that is described with a packet flow and the radio signals that are described with a flow of waves. Moreover, the correspondent node is an actual person responding to the mobile node that is described through an owl. An owl was chosen as a mobile node as it has the capability to fly, which makes it easy to resolve the problem of the constant moving of the receiver between the networks, and is considered likable, wise and re-

spectable. Animals also often inspire sympathy and therefore give the learning environment, and the very technical contents of it, a humanitarian tone.

All these elements are designed to help the study process and to establish a connection between theory and reality as all the levels of communication are brought to the highest level of abstraction through a physical appearance. The implemented Mobile IP becomes comprehensible for everybody as it is in a recognizable and imaginable environment.

The animation is structured through a division of the learning material into eleven scenes and seven detail scenes. Besides helping the comprehension of the animation and its contents, this division contributes also to reducing the consequences of errors that a user might commit when navigating in the product, and renders the use of the product easier as the search times for particular events is less than in an animation without scenes. A possible future development is an index with a table of contents.

To play all the scenes in the animation with the respective detail scenes takes about 40 minutes. This estimation does not include the additional time of a learning process, which is a difficult variable to count, as it is subjective.

Communicating Dimension – The Interface

The learning environment is designed after an old television with a screen with round edges and on it's left channel, or here scene, buttons and other control buttons. The motivation of the design is to render the control of the animation familiar and to wake attention and interest combining old and new, traditional media and new media.

For a good usability and comprehensibility of the product the interface has to present clearly the

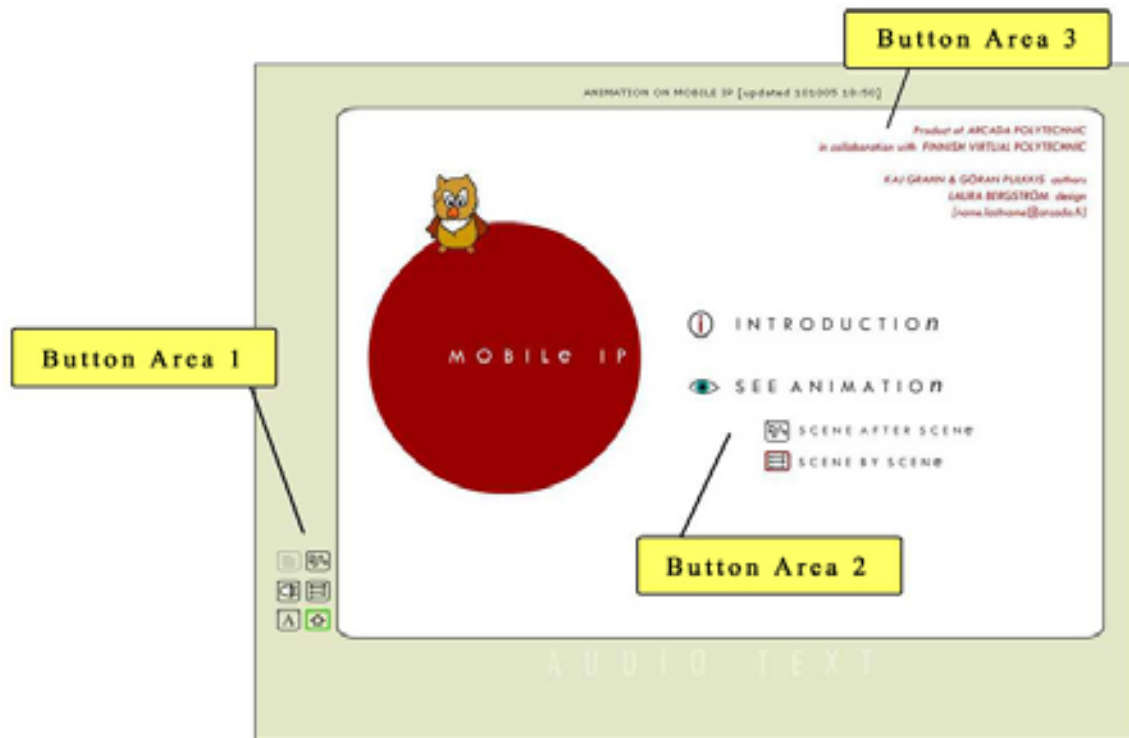


Figure 3: The start composition of the animation. The mouse is over the ‘scene-by-scene’ option in ‘see animation’.

possible operations that may be done in the product and their results. In the start composition of the animation the user has three possibilities of interaction with the product, in other words in this state there are three different button areas on which the user can focus his attention (see Figure 3). Button area 1 is a part of the animations' control panel and will be visible all the time during the use of the product. This property of persistence is described with the fact that it is located outside the television screen, e.g. outside the dynamic animation area, and is therefore available also after changing the contents on the screen. On the contrary, button areas 2 and 3 are located inside the animation area, and are in fact only visible for the user in this particular state of the animation (home page). Button area 3 contains information about the authors of the product and can therefore be easily understood as non-relevant information for the use of the product. Button area 2 initially contains two options, introduction and see animation, and their functionalities as main options are described through a big font and an additional graphical symbol. When bringing the mouse over these options a further description of the user's possibilities is introduced. An observant user can also notice that the same two possibilities for seeing the animation are offered in the control panel on the left. These above mentioned actions are all the possible actions that the user can at this point initialise. Once selected one of the playing modes (see animation) there will appear a list of scenes above the control panel buttons in button area 1 (see Figure 4), which will expand the users possibilities for action.

The learning platform can be divided in three parts, where every part has a particular role (see Figure 4). The screen where the animation is played is the dynamic area of the learning platform, and the text area underneath it is synchronized with the events in it. The control panel on the left of the screen implements the control and comprehension of the platform.

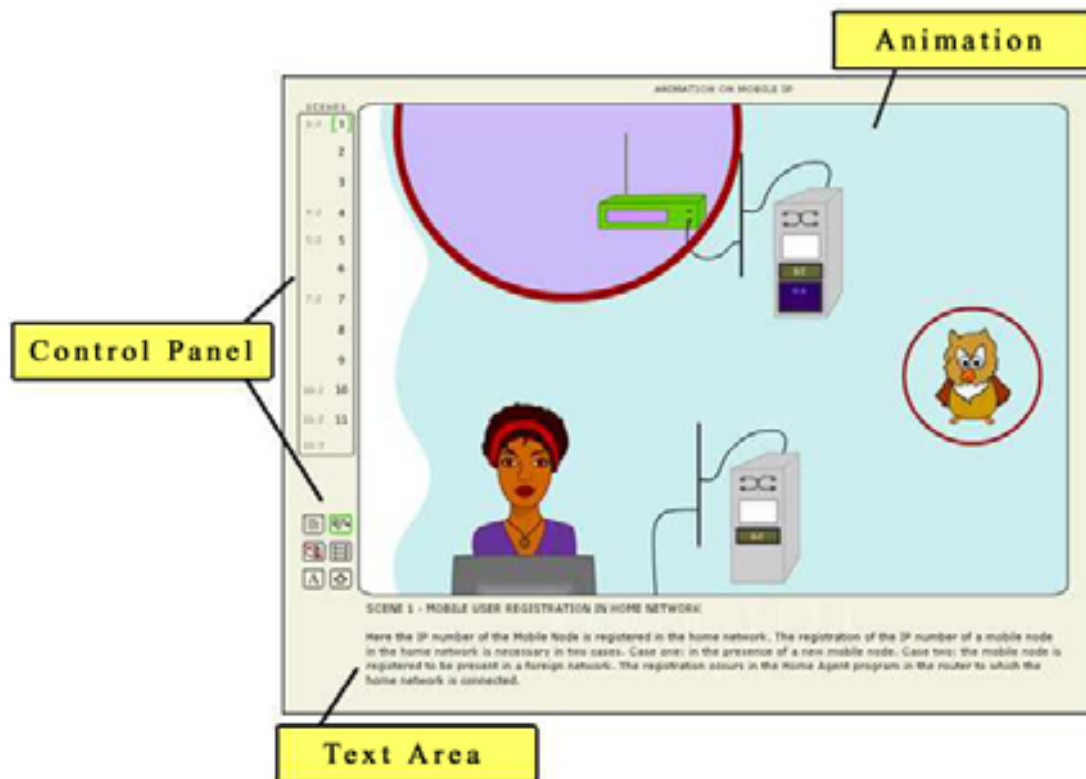


Figure 4: The beginning explanation of scene 1 is playing. The control panel is on the left of the animation meanwhile the text area is below it.

Usability

There are two different animation modes;

1. the main scenes, which are eleven, can be played all in a row with the play mode scene-after-scene and
2. the detail scenes, which are details of a particular event in a determinate scene, can be played only on request.

The study material has been divided in events, or scenes, to render it easier to comprehend, handle and play. This means also that the user is not obliged to see the whole animation when he/she wants to play or replay just a particular event. All scenes, main and detail scenes, start with a beginning explanation that however can be jumped over in the main scenes. This feature allows frequent or material acquainted users to avoid the, for others important, explanations that could for them become elements of frustration. The explanations describe the context, the actions and other necessary information of the scene that is to be played. To render this otherwise difficult listening part, where the user has a passive role, easier to follow, it has been animated in synchronization with the audio and highlighting elements of interest in the environment (see Figure 4).

The main scenes are not interactive, with the exception of the prompt windows that ask the user if he wants to see details, and can therefore only be watched. The detail scenes are on the contrary interactive and divided in multiple steps that the user has to choose between for the animation to play (see Figure 5). Also the introduction to the Mobile IP Environment, which can be accessed from the home page of the learning environment, is interactive (see Figure 6). The introduction permits the user to get acquainted to the all the elements in the animation by bringing the mouse over them and then read (listen) about their significance to the Mobile IP. In the main scenes a constant flow of information was chosen over the activeness of the user as it in this situation helps to establish a connection between small events and the context. Furthermore, this causes less frustration in a frequent user than obligated interventions from his part. On the contrary, it was thought suitable to leave the possibility for an interaction between the product and the user in the detail scenes, where studying chosen features demands its own time.

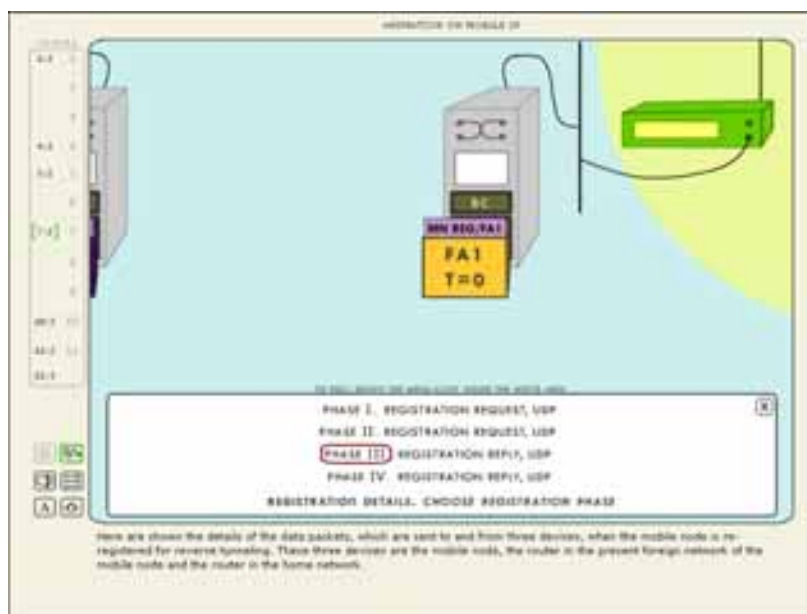


Figure 5: The detail scene of scene 7 is playing. The mouse is over the third option of this detail scene.

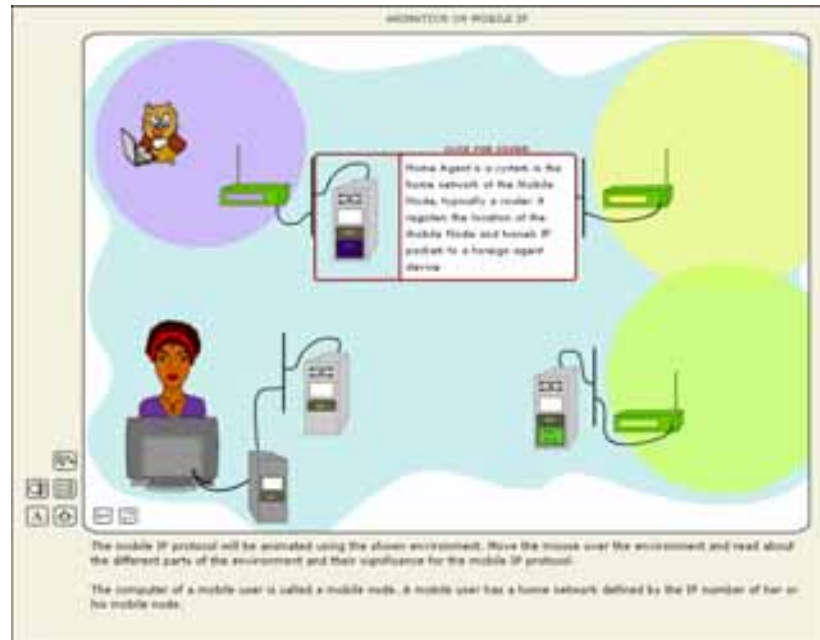


Figure 6: The introduction to the Mobile IP Environment is playing. The mouse is over the Home Agent Router.

The control panel allows the user to navigate inside the learning environment and to control the flow of the animation. In play mode it is composed of a scene area and six control buttons (see Figure 4). In the scene area the numbered scenes are placed in numeric order (see Figure 7). The main scenes are whole numbers meanwhile the detail scenes are composed of two numbers where the first number indicates the main scene it derives from and the second number indicates it being second (or third) part of the particular scene. For example 1:2 is a detail scene of an event in scene 1 (see Figure 8). The six control buttons are placed below the scenes area. These control buttons are home, scene-after-scene, scene-by-scene, sound, authors, and skip explanation (see Figure 9). The last mentioned is active just in the beginning of every scene as it lets the user to jump over the beginning explanation of a scene and to see only the animation without detailed explanations of the material.

The home button brings the user to the home page of the animation, in other words to the start of the animation (see Figure 3). The protagonist of the animation, the flying owl, is introduced directly in the beginning by letting him fly into a scene otherwise non-animated. In this way the user's interest is waked up immediately and he is invited to explore the product. To continue the user has to choose between introduction to the animation or playing the animation. The access to the introduction of the animations environment is only from this home page as it is considered information that the user studies before playing the animation. There are two different modes to play the animation, scene-after-scene and scene-by-scene mode, which can be chosen either from this beginning picture or from the control panel. If the scene-after-scene mode is chosen the animation will automatically continue to the next scene after one scene has ended. In scene-by-scene mode the animation on the contrary will stop at every fully played scene. It was chosen to have these both options because a user who is already familiar with the product or a user who wants to study the animation more slowly than programmed may be motivated to see just a specific part of the animation at a time.

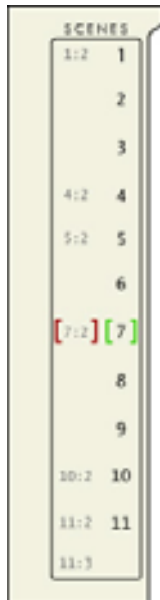


Figure 7: The scenes area in normal mode. Here scene 7 is playing and the mouse is over its detail scene.

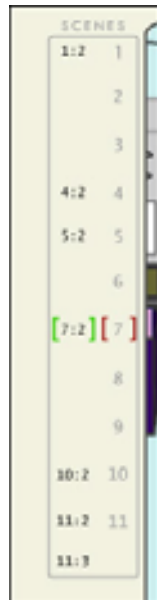


Figure 8: The scenes area when a detail scene is open. Here a detail scene from scene 7 is playing. The mouse is over scene 7.



Figure 9: The control buttons. The significance of the buttons beginning from the top left; skip explanation, scene-after-scene, audio, scene-by-scene, authors and home. Here the scene-after-scene mode is playing and the mouse is over the author's button.

The sound button switches off or on the audio of the animation. The role of this button becomes important at the point where the user wants to switch off the sound of this product without muting his computer. The last element in the control panel, the authors button, opens or closes a small window containing the necessary information of the authors of the product.

The third element of the learning environment is the text area, which is located under the animation, and where all the played audio will appear in the form of text (see Figure 4). This is an important part of the learning environment as all the students have different ways of learning, and it is relevant to include both audio stimulation and text support.

Comprehensibility

A good comprehensibility of a product is achieved when the elements of the interface have an efficient relationships between the interpretation of them and their effects, and when the users actions towards the interface have a feedback from the part of the last mentioned. Here the comprehensibility of the elements in the interface, regarding the signs that they are described through and the feedback that they give to the users actions, is discussed.

A green color indicates to the user where he finds himself in the material, for example when the user is located in the first scene and playing the animation in scene-after-scene mode. Both scene 1 and scene-after-scene buttons are highlighted with a bright green color (see Figure 4). This kind of path indication supports the navigation and makes it clearer. However, an easy comprehensibility is achieved only by combining path indication and action feedback. Action feedback means that when the user brings his mouse over a button or hyperlink this should indicate him its task or its activeness. Here all feedback is given with a dark red color. The same red is used for highlighting the elements of interest during the beginning explanation of the scenes, as its aim is to support the audio and in this way give feedback for thoughts.

The control panel buttons are designed to demonstrate their functions as efficiently as possible (see Figure 9). The signs on the home and audio buttons are symbols, in other words signs that have a conventional relationship to their referent. These kinds of signs are more often easily recognizable as the user is used to the symbols and know their meaning. Therefore, if it is possible, signs as symbols are strongly recommended, especially for learning environment interfaces. The signs on the buttons scene-after-scene, scene-by-scene and skip explanation are icons meaning that the design reflects their referent by appearance. The user is probably able to interpret the meaning of the signs if he applies them to the situation, but it could take him a longer time to interpret an icon compared to a symbol that is familiar to him from advance. However, if the functions of the buttons are not clear to the user, an explanation of what it will do appears on its side when the mouse is brought over the button. This is in fact the only way to understand the signification of the authors button as it is represented with a sign 'A' that stands for 'Authors'. This was considered to be the best option for a referent that doesn't have a conventional sign or is not easily presentable by appearance.

On the home page we can find two buttons, the information and play animation buttons (see Figure 3). The first one is represented with the symbol 'I' that refers to 'Information'. This sign is very commonly used for the referent and can therefore be considered the symbol of 'Information'. Also the second button that is an image of an eye, which refers to the action 'to see', clearly states the function of it.

The scenes area in the control panel has two modes; a main mode for the main scenes and a detail mode for the detail scenes. The second mentioned differs from the main mode for its lower color intensity (see Figure 7 and 8). These two modes are designed to support and enhance the different purposes of the contents in main mode animations and detail mode animations.

Esthetical Dimension – The Layout

The secrets of an elegant and harmonic interface are unity of its elements, contrast that creates tension and interest, and space that helps separate elements earn more attention and/or be grouped (Mullet & Sano, 1995). In other words contrast and space create visibility and unity creates coherence; these are two of the principals that are to keep in mind when designing an interface so that a direct interaction between the user and the product can be achieved (see section *Learning Environment Design*).

All the buttons and also the scenes area, authors window and the screen where the animation is played have rounded corners, which is the unifying element of the learning environment. Another unifying factor is the use of a limited amount of colors in the interface, which are dark gray, red and green. The contrast between elements is created with

1. closure, the element that describes the function of the button is closed inside an defined area (square),
2. colors, the path indication color, the feedback color and the buttons normal color are all easily distinctive, and
3. size, the small size of the control panel buttons compared to the big size of the screen.

Space is used in the control panel between the six buttons and the scenes area to enhance their different functionalities; almost all of the six buttons are for an overall control of the product, while the scenes buttons permits to control the flow of the animation. Also the text area is separated from these elements by a vertical space underneath the buttons that almost seems an explicit and concrete graphical barrier although it is not.

The background color of the learning platform is light gray, which enhances and lifts up the animation that is built on a white background. This is because white, which derives from the unity of

red, green and blue (according to the additive color system RGB), has a higher value of light than gray, which is a tint, or a pure color to which has been added white and has therefore a lower value of light than white (Götz, 1998; Larmann, 1995). This causes an effect that pushes the gray on the background and brings the white on top.

All buttons are dark gray and highlighted with a clear green to indicate the path and with dark red to give feedback for users actions. These colors are chosen because green indicates among other things permission or 'go!' and given the situation of its use, an element being used or played, the color corresponds to its function. On the contrary red often stands for stop, alert or attention and is here used as feedback color for user's actions. Often choosing another option means interrupting the one that is playing and therefore the user has to pay attention to his choice as the one playing will stop and/or disappear. These two colors are also the two colors less used in the animation, which makes their use easy as they are not associated to another element in the learning environment.

The font type used in the animation and in the rest of the learning environment is Tw Cen MT. The written audio text is dark gray of the size 11 (points). This is a font without serifs, in other words without end curves in the letters, and because of that it has a better legibility on the computer screen than a font with serifs, like for example Times New Roman.

IT Infrastructure Requirements

Offering the product requires an Apache www server with installed Secure Socket Layer (SSL) support for secure authentication of learning environment users. User authentication to a virtual course, into which the Mobile IP learning environment has been integrated, is necessary. Email address, mobile phone number and Skype address of the user are needed for communication with course teachers.

Requisites for using the product are a high bandwidth Internet connection, a Flash Player that can be downloaded from the website of Macromedia (<http://www.macromedia.com>), and loudspeakers or headphones. Nevertheless, the animation can be seen without sound as it contains all the audio also as text. A relatively high screen resolution is another important hardware characteristic that is needed for playing the animation properly. In a 800 x 600 pixel resolution screen not even the whole animation area is fully visualized and the user has the scroll both vertically and horizontally to see all corners of the learning platform. With a 1024 x 768 pixel resolution all except the text area is fully visualized. In all screens with 1280 x 1024 pixels and more the learning platform is fully visualized. Therefore a computer screen with at least 1024 x 768 pixel resolution is recommended. In other words at least a laptop is needed for optimal using of this product. A PDA is not sufficient.

The product works with browsers Mozilla Firefox, Netscape 7 and Internet Explorer.

User feedback

A team from the Finnish Virtual Polytechnic (Finnish Virtual Polytechnic, 2006a) has evaluated the learning platform both from a pedagogic and heuristic point of view. The evaluation, which is in Finnish, is available online but requires authentication, e.g. a user account for Finnish Virtual Polytechnic (Finnish Virtual Polytechnic, 2006b).

According to the team the strength of the product, from the pedagogical point of view, is in its context and problem formulation, which are authentic. Also the fact that the user can focus on some details of the Mobile IP is considered particularly good. But on the contrary improvements regarding support for thinking and problem resolving processes of the user could be made. In fact

tasks could be associated to the animation in the way that the user has to find answers to them navigating in the animation.

The positive feedback regarding the heuristic evaluation of the platform is its simple navigation that together with an efficient and flexible interface offers the user an easy and, from his part, controlled use of the platform. However some persons from the evaluation team would have wanted more instructions for use before starting the animation. The visualization of the contents in the animation is according to the team expressive and clear, although to fully understand all the elements in it requires having seen the introduction. The introduction is the element that received most critics, as it is not clear and interactive enough. A positive factor is also the fact that the platform is uploaded fast and that it works in many environments.

Conclusions

Mobile IP is – compared to other network protocols – a complex protocol with many options and extensions. The creation of a network learning environment is therefore a demanding challenge. Experts, like graphical designers, have to be included in the production team. Prototypes have to be tested and feedback from students is needed before the learning environment is in its final form. A proper choice of computer software and IT technology is necessary. Furthermore, a sufficient and realistic budget is essential.

The Mobile IP learning environment has proven to be of major importance for the students. In general, the levels of acceptance and satisfaction have been high. The work done during the project has given the authors valuable experience for further work on similar issues.

A future extension of the implemented learning environment will be integration of security schemes in the Mobile IP animation. An example is animation of ‘redirection of data packet’ DOS attacks with and without strong authentication. The animation should show how the DOS attack succeeds without strong authentication and how it fails with strong authentication. Request/reply messaging to/from AAA servers will be included. Also training exercises should be implemented. A user of the learning environment should have possibilities to trigger DOS attack patterns and study how the attack patterns are handled by different Mobile IP extensions.

References

- Barun, T. & Danzeisen, M. (2001). Secure mobile IP communication. *Proceedings of IEE 26th Annual Conference on Local Computer Networks*, 586-593.
- Calhoun, P., Johansson, T., Perkins, C., Hiller, T., & McCann, E. P. (2005). Diameter mobile IPv4 application. IETF, RFC 4004. Retrieved March 8, 2006, from <http://www.ietf.org/rfc/rfc4004.txt?number=4004>
- Finnish Virtual Polytechnic (2006a). Portal of Finnish virtual polytechnic. Retrieved March 3, 2006, from <http://www.virtuaaliyamk.fi/channels/www/eng/etusivu.html>
- Finnish Virtual Polytechnic (2006b). Production team evaluation page (internal). Retrieved March 3, 2006, from <https://www.virtuaaliyamk.fi/opintojaksot/041005/1092991850017/1099044944687/1113319626141/1113319658781.html.stx>
- Glass, S., Hiller, T., Jacobs, S., & Perkins, C. (2000). Mobile IP authentication, authorization, and accounting requirements. IETF, RFC 2977. Retrieved March 8, 2006, from <http://www.ietf.org/rfc/rfc2977.txt?number=2977>
- Griffiths, R. (n.d.) Norman's gulfs of execution and evaluation. Retrieved February 27, 2006, from <http://www.it.bton.ac.uk/staff/rng/teaching/notes/NormanGulfs.html>

- Götz, V. (1998). *Color & type for the screen*. Crans: RotoVision SA.
- Hwu, J.-S., Chen, R.-J. & Lin, Y.-B. (in press). An efficient identity-based cryptosystem for end-to-end mobile security. *IEEE Transactions on Wireless Communication*.
- Islam, R. (2005). *Enhanced security in Mobile IP communication*. MSc Thesis, Department of Computer and Systems Sciences, Royal Institute of Technology, Stockholm, Sweden.
- ISP Glossary (2005). Mobile IP. Retrieved January 20, 2005 from, http://isp.webopedia.com/TERM/M/Mobile_IP.html
- Jacobs, S. & Belgard, S. (2001, July). Mobile IP public key based authentication. IETF, Internet Draft (expired). Retrieved November 27, 2005, from <http://mirrors.isc.org/pub/www.watersprings.org/pub/id/draft-jacobs-mobileip-pki-auth-03.txt>
- Johansson, F. & Johansson, T. (2004). Mobile IPv4 extension for carrying network access identifiers. IETF, RFC 3846. Retrieved March 8, 2006, from <http://www.ietf.org/rfc/rfc3846.txt?number=3846>
- Kurose, J. & Ross, K.W. (2005). *Computer networking* (3rd ed.). USA: Pearson.
- Larmann, R. M. (1995). *Color saturation and intensity*. University of Evansville, Art Department. Retrieved November 26, 2005, from <http://www2.evansville.edu/studiochalkboard/c-saturate.html>
- Lee, B-G., Choi, D-H., Kim, H-G., Sohn, S-W., & Park, K-H. (2003). Mobile IP and WLAN with AAA authentication protocol using identity-based cryptography. *10th International Conference on Telecommunications ICT 2003, 1*, 597 - 603
- Montenegro, G. (1998). *RFC 2344 -Reverse tunnelling for Mobile IP*. Retrieved November 29, 2005, from <http://www.faqs.org/rfcs/rfc2344.html>
- Mullet, K. & Sano, D. (1995). *Designing visual interfaces*. Mountain View, CA: Sun Microsystems.
- Perkins, C. (2002). IP mobility support for IPv4, IETF, RFC 3344. Retrieved March 8, 2006, from <http://www.ietf.org/rfc/rfc3344.txt?number=3344>
- Perkins, C. & Calhoun, P. (2000). Mobile IPv4 challenge/response extensions, IETF, RFC 3012. Retrieved March 8, 2006, from <http://www.ietf.org/rfc/rfc3012.txt?number=3012>
- Shamir, A. (1984). Identity-based cryptosystems and signature schemes. *Advances in Cryptology-CRYPTO'84*, 47-53.
- Schiller, J. (2000). *Mobile communications*. Great Britain: Addison-Wesley.
- Webopedia (2005). The #1 online encyclopedia dedicated to computer technology. Retrieved November 29, 2005, from <http://www.webopedia.com/TERM/r/roaming.html>
- Zao, J. K. & Condell, M. (1997, November). Use of IPsec in mobile IP. IETF, Internet Draft (expired). Retrieved November 28, 2005, from <http://mirrors.isc.org/pub/www.watersprings.org/pub/id/draft-ietf-mobileip-ipsec-use-00.txt>
- Zao, J., Kent, S., Gahm, J., Troxel, G., Condell, M., Helinek, P., Yuan, N. & Castineyra, I. (1999). A public-key based secure mobile IP. *Wireless Networks*, 5(5), 393-390.

Biographies



Laura Bergström has a BSc in Media Culture from Arcada Polytechnic, Espoo Finland. Since March 2002 she works for Arcada Polytechnic as graphical designer in virtual education development.



Kaj J. Grahn, Dr. Tech., is presently senior lecturer in Telecommunications at the Department of Business Administration, Media, and Technology of Arcada Polytechnic, Helsinki, Finland. He is also Program Manager of the Electrical Engineering Programme. His current research interests include Wireless and Mobile Network Security.



Göran Pulkkis, Dr. Tech., is presently senior lecturer in Computer Science and Engineering at the Department of Business Administration, Media, and Technology of Arcada Polytechnic, Helsinki, Finland. His current research interests include Network Security and Applied Cryptography