IT Education Topics for Future Networking

Göran Pulkkis, Kaj Grahn, and Jonny Karlsson
Arcada University of Applied Sciences, Helsinki, Finland

goran.pulkkis@arcada.fi kaj.grahn@arcada.fi
jonny.karlsson@arcada.fi

Abstract

In this paper, we discuss how information society and the global data network infrastructure are evolving. Global integration of networked information processing capabilities is a main issue. One of the many important building blocks in the ongoing process is the choice of network architectures. Another basic issue is Internet mobility support. Basic requirements for mobile networking are presented. Issues like network security architectures and quality of service (QoS) architectures are outlined. Trust in cryptographic identities including public key infrastructure and identity based encryption is described. In the network protocols section wireless communication, mobility management, routing and network security protocols are presented. Essential network programming skills are summarized. The impact from the described requirements on future networking on education and research in Arcada University of Applied Sciences is outlined.

Keywords: networking, communication, mobility, security, QoS, protocol, architecture, wireless

Introduction

Three fundamental views of a data network are the user view, the infrastructure view, and the functional view.

In the user view a network is a platform for a set of services accessible through the user interface of a computing device. Such services are web pages, net banks, email, net shops, navigations assistants for cars and boats, etc.

In the infrastructure view the network is, as the Internet, a set of interconnected devices, which are end user devices (computing devices, sensors, and actuators) and middleboxes (hubs, switches, routers, gateways, firewalls, base stations, base station controllers, etc.). Interconnections are wired or wireless. In mobile networking the network infrastructure is partly dynamic (mobile end user devices and mobile networks with dynamically changing attachments to a static network infrastructure) or fully dynamic (a Mobile Ad-hoc NETwork – a MANET in which all interconnections are wireless and each network device can serve both as an end user device and as a middlebox for other network devices). A network architecture is an implementation of a network infrastructure.

In the functional view a network is a stack of layers for protocols, which implement functionality. This protocol stack has been standardized as the OSI model consisting of the following layers (ISO/IEC 7498-1, 1994):

- Application layer
- Presentation layer
- Session layer

- Transport layer
- Network layer
- Link layer
- Physical layer.

A network protocol on a layer communicates only with the layers immediately above and below in the protocol stack. Propagation of physical signals occurs on the bottom layer, the physical layer. The top layer, the application layer, provides the user interface to the network services in the user view.

Fundamental requirements on data networks are security, and Quality of Service (QoS). A security architecture is an implementation of network security requirements. QoS is based on network bandwidth management, on management of available processing power of computing devices in a network, and on reliability issues such as Mean-Time-Between-Failures (MTBF) of network devices and their interconnections as well as fault tolerance features like acceptable bit-error-rates (BER).

The number of devices connected to the Internet has grown rapidly during the last years. At the same time more and more computers have become portable and mobile. Information processing capabilities are embedded in vehicles, in houses, in home equipment devices, in watches, and in many other objects in our everyday environment. The emerging need to interconnect and manage objects with information processing capabilities has lead to an increased need for unique IP addresses as well as for the ability to move between different network attachments while still maintaining the network connection. A transition to IPv6 with a practically unlimited IP address space for all Internet communication is a necessity. Global support for mobility management network protocols like Mobile IPv6 is also important. For secure network mobility there is a need for network protocols like the Host Identity Protocol, in which device identities can be cryptographic and IP addresses are used only for localization of devices and for routing of data communication.

The current evolution trends in ICT technologies put requirements on the education of data networking professionals. More and more social services in the current Information Society are electronic, network based and even ubiquitous - available anywhere and anytime. Network professionals should be able design and maintain a broad spectrum of ubiquitous network services as well as the underlying network infrastructure. Topics like

- design of ubiquitous network services
- architecture of mobile data networks,
- security architecture of mobile data networks
- network protocols with emphasis on IPv6, wireless communication protocols, mobility management protocols and network security protocols
- network programming with emphasis on mobile operating systems, mobile programming methodology, object oriented programming, socket programming, and application development tools

are highly essential in the education of data networking professionals. These topics are outlined in this paper. (Abbreviations for many terms are listed in the Appendix.)

Networks and Information Society

In the last century, the industrial society has evolved into an information society. Traditional society structures and functions based on the principles of the industrial era cannot effectively face the complex demands and problems arising from citizens who live immersed in a new paradigm of this information society. The technological platform of the information society is a global data network infrastructure for information processing devices. This infrastructure is based on the

Internet, interconnected mobile cellular networks, satellite communication, and connected mobile ad hoc networks (MANETs).

The global integration of networked information processing capabilities everywhere in objects and in everyday activities is initially called ***ubiquitous computing*** and currently also ***pervasive computing***. Related concepts are "***the Internet of Things***", which proposes a shift from the current global network of interconnected computers to a future global network of interconnected smart objects, and ***ambient intelligence*** referring to smart electronic environments which are sensitive and responsive to human presence. An information processing device or a smart object is

- a computer or an object with an embedded computer,
- a sensor, which is an input device for registration of environmental events and human behaviour, or
- an actuator, which is an output device for control of environmental properties like temperature and/or for delivering information.

(Pervasive, 2006; Poslad, 2009)

The human user interface to pervasive information processing environments can provide network services, which are

- ***embedded***. This means that the environment can be saturated with integrated networked devices.
- ***context aware***. This means that services delivered by networked devices may depend on time, place, environment type, and situational events. Outdoor localization can be based on the Global Positioning System (GPS) and on the global infrastructure of cellular mobile network base stations. Indoor localization can be based on an suitable infrastructure of embedded wireless networking devices.
- ***personalized***. This means that services delivered by networked devices can be tailored to personal needs and requirements
- ***adaptive***. This means that services delivered by networked devices can be changed in response to service users
- ***anticipatory.*** This means services delivered by networked devices anticipate needs and behaviour of service users.

(Aarts et al., 2001)

Network services in

- public administration
- net based education
- multimedia

are presented in this section.

Network Services in Public Administration

Many IT companies are presently developing network service solutions for public administration. Following network service solutions have been developed by maatG (Business, 2010)**:**

- Self-management of Pages, Components, Services Self-designed and Third Party Applications
- Mash-ups Configuration, On-the-fly integration, Drag&Drop, Data model, Interoperability, Client Presentation Layer.
- Citizen Folder (access of the contributor to different transactions such as: Document Input/Output Register, Initiating In-Person transactions, download of documentation, transactions, Citizen mailbox and Telematic Payment of taxes and using various means of payment approved by the municipality).

- Back office of municipal management (Governmental Accounting, Tax Management and Collection, Personnel and Payroll Management, Input/Output Register).
- File Manager, Workflow Manager.
- Middleware.

Siemens IT Solutions and Services has developed following network service solutions for public administration (eAdministration, 2010):

- Multi-channel access via mail, telephone, Internet portal and e-mail
- Core administration activities, such as:
  - Forms management
  - Document management
  - Workflow management
  - Content management
  - Secure archiving
- IT security solutions such as single sign-on, PKI, digital signature, biometrics.

Network Based Education

The global data network infrastructure offers many powerful resources for implementing distance education. Net based education can take many forms, including: (1) tutorial, (2) virtual classroom, (3) correspondence course, (4) project-based education, and (5) event-based education. Net based education can also provide a valuable supplement to traditional class room and laboratory education. As network technologies develop, more possibilities emerge. (McLellan, 2004)

A fundamental issue is the difference between **synchronous** and **asynchronous** communication. Synchronous refers to instantaneous real time communication. A telephone call is an example of synchronous communication. Asynchronous communication must not take place in real time and can be delayed at the receiver's end. For example, the communication with a telephone answering machine is asynchronous. Also electronic mail communication is asynchronous. Proper utilization of synchronous and asynchronous communication is an important issue in network based education since many communication patterns are possible. (McLellan, 2004)

Network based education requires educators to recognize and utilize the vast resource set, which is now available on the global data network infrastructure, especially the World Wide Web. In addition to selecting a textbook, a teacher should now consider to include in a study course a Web navigation guide tailored to the course subject. Awareness of these network resources and skills in navigating them is an essential component of information literacy and a basic technological competence for today and tomorrow. (McLellan, 2004)

Multimedia Services

IP Multimedia Subsystem (IMS) is an important standard for design of multimedia services in current TCP/IP networks and in such current mobile cellular networks like UMTS which have sufficient bandwidth resources. Examples of multimedia services are

- PoC (Push to Talk Over Cellular)
- Push to See
- Interactive Gaming
- File Sharing
- Instant Messaging
- Voice Messaging
- Voice Telephony over IMS
- Video Conferencing
- Content Streaming Services.

IMS features are

- Multimedia Session Management
- Mobility Management and Roaming
- QoS
- Service Execution
- Third Party Service Support.

Multimedia services usually require high end-to-end data communication bandwidth and rich user interface. New ubiquitous multimedia services can be designed when the bandwidth of wireless network attachment networks increases. (IMS, 2010)

Network Architecture Issues

Important architectural issues of pervasive networks are implementation of wireless interconnection between network devices, mobile networking, and evolving networking infrastructures.

Wireless Communication

Wireless communication protocols have general characteristics and goals that they try to achieve. Some of these general guidelines are (Overview, 2010): **Unlimited roaming and range** (the location of the user is irrelevant), **Guarantee of delivery** (messages and data are guaranteed to be delivered), **Dependability of delivery**. (accurate and full transmission of messages is guaranteed), **Notification** (the user is aware that data has been sent and needs to be looked at), **Connectivity options** (a wide range of options in hardware and type of connection are given), **Millions of users** (engages millions of users), **Priority alerts** (able to control high-priority data traffic), **Communication** (able to communicate through devices that hold reliable and user-friendly applications), **Host reconfiguration** (the ability to reconfigure when changing environments), **Host mobility** (flexible mobility allows the host to move as it pleases) and **Dynamic encapsulation** (the need to register a mobile host with its base agent).

Typical wireless communication networks are Mobile Cellular Networks (GSM->GPRS->3G(UMTS)->4G), WWAN (Satellite Communication), WMAN (WiMAX), WLAN (Wi-Fi), WPAN (Bluetooth), NFC (Near Field Communication) and WMN (Wireless Mesh Network). Here, we shortly describe WMN, because WMNs can be implemented with various wireless technology like IEEE 802.11, IEEE 802.16, cellular technologies or combinations of these.

A WMN network is made up of radio nodes organized in a mesh topology and most often consists of mesh clients, mesh routers and gateways. The clients are laptops, cell phones and other wireless devices. The routers forward traffic through the gateways which may be connected to the Internet. A mesh network is reliable and offers redundancy. A WMN can be seen as a special type of wireless ad-hoc network and it offers dynamic and cost effective connectivity over a certain geographic area. It's built of peer radio devices that don't have to be cabled to a wired port like in traditional WLAN. The topology of a WMN is reliable because every node is connected to several other nodes. The principle of operation in WMN is similar to the way packets travel in the wired Internet. Dynamic routing algorithms implemented in each device make this possible.

Mobile Networking

In order to provide Internet mobility support, i.e. when an IP-based device moves to different networks and changes its topological point of attachment, a number of fundamental issues arise. We summarize the following basic requirements for Internet mobility support (Fu et al., 2006):

- **Handover management**. When a mobile node moves and changes its point of attachment to the Internet the communication must continue. Handover management minimizes service disruption during handover.

- **Location management**. This technique identifies the current location of the mobile node and keeps track of the location changes to other nodes that need this information.
- **Multi-homing**. Future mobile environments are characterized by diverse wireless access networks. This requires multi-homing support by the mobile node, i.e. simultaneous access through multiple links and selection and switching of dynamic links.
- **Applications**. The mobility management mechanism must be transparent without requiring changes to current services and applications.
    - GPS applications and other location based mobile services
    - Context sensitive mobile services
- **Security**. Any mobility solution must protect itself against misuses of the mobility features and mechanisms.
- **Performance requirements**. Performance metrics include handover latency, packet loss, signalling overhead and throughput.

The traditional TCP/IP was designed for fixed computer networks. In (Le et al., 2004), some limitations of traditional TCP/IP for Internet mobility are mentioned:

- **Limitation of the link layer**. Mobility across heterogeneous networks requires mobility support functions provided at layers above the link layer. Providing mobility of homogeneous networks at the link layer is not appropriate.
- **Limitation of the IP address**. The IP address is used both as locator and identifier. In a mobile environment, when the mobile node moves from one network to another the IP address has to be changed according to point of attachment. Even if the mobile node obtains a new IP address dynamically, the transport connection in the previous network will be broken after the change of IP address.
- **Lack of the cross-layer awareness and cooperation**. Traditional transport layer protocols rely on services provided by the network layer. Further, the congestion control of TCP does not distinguish the packet loss by handover of mobility from the normal packet loss in wired networks. Besides, the congestion control relies on the assumption that the end-to-end connection is stable which may be violated in a mobile environment.
- **Limitation of applications**. Applications based on traditional TCP/IP may be limited in use in the mobile environment. For example, the binding between the Fully Qualified Domain Name (FQDN) in DNS and the IP address will be invalid.

4G Networks

Frameworks for future 4G networks, which seamlessly integrate heterogeneous mobile technologies in order to provide enhanced service integration, QoS, flexibility, scalability, mobility, and security, are currently being developed. However, these frameworks raise security vulnerabilities. An international consortium presents requirements and recommendations for the evolving 4G mobile networking technology (Choi et al., 2007). The 4G technology, which is at its infancy, is supposed to allow data transfer up to 100 Mbps outdoor and 1 Gbps indoor. The International Telecommunications Union (ITU) defines 4G as downlink throughput of 100 Mbps or more, and corresponding uplink speeds of at least 50 Mbps.

The 4G technology will support roaming for interactive services such as Video Conferencing. The cost of the data transfer will be comparatively low and global mobility will be possible. The networks will be all IPv6 networks. WLAN, 2.5G, 3G and other networks such as SATCOM, WiMAX and Bluetooth will be integrated in 4G networks. The two main candidates for 4G wireless technologies are currently WiMAX based on IEEE802.16 and Long Term Evolution (LTE) Advanced (Ghosh et al., 2010). Older technologies such as WLAN, 2.5G, and 3G will also be supported. The antennas will be much smarter and improved access technologies like OFDM and

MC-CDMA will be used. More efficient algorithms at the physical layer will reduce the inter-channel interference and co-channel interference.

Security Architecture

The security architecture standard outlined in 1989 in the OSI (Open Systems Interconnection) model of layered networks (ISO 7498-2, 1989) does not take specific security requirements of mobile networking in consideration and for this reason there is a clear need to update this standard. Recent security architecture proposals are published in (Eschenbrücher et al., 2004; Ghalwash et al, 2007; Hashim et al., 2007; Zheng et al., 2005b).

Network access security, network area security, user area security, and application security is implemented for Mobile Equipment devices (MEs) in a mobile infrastructure network by the security architecture described in (Zheng et al, 2005b). A ME ought to be a Trusted Mobile Platform according to the specification in (Trusted, 2004). All mobile network entities, the users, the home environment (HE) of each user, the MEs, the manufacturer of each ME, the cellular wireless access network (AN), the service provider, and each base station (BS) in the AN should have trusted cryptographic identities implemented by public key certificates in the same public key infrastructure (PKI). The user HE issues a USIM card to be installed in the user ME. The cryptographic user identity is stored in the USIM card of the user. Legacy base stations broadcast both own public security parameters and also public security parameters of all neighbour base stations in order to prevent user MEs to be attached to malicious base stations. The cryptographic identities of network entities are used for mutual authentication between a user USIM and the host ME as well as between the user, the AN, and the HE of the user. These cryptographic identities are also used to create a shared session key between each user and the AN. For identification purposes each user also needs a password and a stored fingerprint pattern. A user ME should be provided with a trusted fingerprint reader. Information stored in a database maintained by the user HE is used to verify the password and fingerprint of a user.

In Eschenbrücher et al. (2004) a reference model for a security architecture in a typical 3G cellular mobile network is outlined. In this reference model, security services are implemented on three separate security planes, the End User Security Plane, the Signalling-and-Control Security Plane, and the O&M (Operations and Management) Security Plane. These security services are based on given security policies and principles. Subscriber access and the use of the service provider's network is managed in the End User Security Plane, which also represents actual end-user data flows. The Signalling-and-Control Security Plane provides protection to activities which enable efficient delivery of information, services and applications across the network. The O&M security plane protects O&M functions of the network elements such as charging functions, transmission facilities, data centres, and back-office systems (operations support systems, business support systems, customer care systems) are protected by the Q&M Security Plane, which also supports fault-, configuration-, accounting-, performance-, and security management functions. There are three layers in each security plane, the Application Security Layer, the Network Services Security Layer, and the Infrastructure Security Layer. Security services are implemented by security functions and mechanisms. Every security service must be evaluated on every security plane in terms of authentication, authorization, accountability, availability, confidentiality, integrity, non-repudiation, and privacy. On the Application Security Layer are implemented security services like virus protection, system access control, certificates, application layer gateway, deep inspection firewall, Secure Shell (SSH), and Simple Network Management Protocol version 3 (SNMPv3) as countermeasures to security threats like virus infections, false data, malicious programs, unauthorized users, and file corruption. On the Network Services Security Layer are implemented security services like IPSec Virtual Private Network (VPN), Secure Socket Layer/Transport Layer Security (SSL/TLS), and stateful inspection firewall as countermeasures

to security threats like corrupted router tables, Denial-of-Service attacks, and interception of data. On the Infrastructure Security Layer security services like secure perimeters, limited administrators, role based access control, Layer 2 VPN/Virtual Local Area Network (L2 VPN/VLAN), and Media Access Control (MAC) filtering are implemented as countermeasures to security threats like electronic attacks and destroyed relays.

In (Hashim et al., 2007) is described a security architecture for a mobile infrastructure network with mobile end user devices for protection against two severe security threats in mobile networking, Denial-of-Service and worm. Such a mobile infrastructure network, called Next Generation Mobile Networks (NGMN) (Kibria & Jamalipour, 2007), has a network topology similar to the hierarchical topology of present 3G wireless cellular networks. However, an important extension is that a mobile end user device can use different wireless access network types such as cellular network, WLAN, Bluetooth, Worldwide Interoperability for Microwave Access (WiMAX), and emerging network access technologies.

Key components of the security architecture described in (Hashim et al., 2007) are Detection Units (DU), Decision Maker Units (DMU), and Security Database Units (SDU). A DU can be integrated in any network node. A DU transmits an alarm message to a DMU on the next network level, whenever an anomaly like a DoS attack or a worm attack is detected. DMU functionality can be integrated in all network nodes above the network level of end user devices. A DMU stops DoS attacks and prevents the spread of a worm in a network domain by isolating infected end user devices and preventing them from contacting other network domains. A DMU is a client to the server function of a SDU, which maintains a database with

- security solutions,
- an Attacker Blacklist, and
- a list of worm signatures.

On receiving an alarm message, a DMU requests a security solution from the SDU. The SDU updates the database with the DMU request information and sends security solution proposal in a reply. A SDU is hosted in a Mobility Anchor Point (MAP) node in the NGMN hierarchy. A MAP has a similar functionality in the NGMN hierarchy as a Serving GPRS Support Node (SGSN) has in a present 3G wireless cellular network (Kibria & Jamalipour, 2007).

Seamless convergence of heterogeneous wireless networks provides new security challenges for the network security research community. There is a need for global authentication architectures, which can operate independently of the wireless physical layer protocols. Moreover, specifications are needed to maintain the confidentiality and the integrity of the communication data, whilst the user terminal is in a hand-off state. A forum of mobile operators called Fixed Mobile Convergence Alliance (FMCA) is developing specifications for the convergence of heterogeneous networks in the context of all IP 4G wireless systems.

Security policy issues such as the use of lightweight and flexible AAAA (Authentication, Authorization, Account, Audit) schemes, the use of Trusted Computing (Zheng, 2005b), and the use of different security polices for different services are recommended for 4G systems (Zheng et al., 2005a). Integration of the SSL security protocol and a Public Key Infrastructure is outlined and evaluated in (Kambourakis et al., 2004).

In Ghalwash et al. (2007) is proposed for MANETS a security architecture, in which a MANET is divided into clusters. Data communication between nodes in different cluster uses gateway nodes in the clusters. A Cluster Head node (CH) is responsible for establishing and organizing a cluster. The CHs in a MANET represent a CH network. Every network node generates an own key pair in public key cryptography. Public keys are certified by a distributed Certificate Authority (CA) consisting of the CHs in the MANET. Each CH holds a share of the private CA key, which is

used for signing network node certificates with a threshold technique based on Lagrange interpolation. A sufficient subset of all CH nodes must collaborate in creating valid signatures on certificates. The CH network composition changes dynamically as CHs join and leave the MANET. The secret private CA key shares must therefore be renewed regularly. The public CA key must of course be known by all MANET nodes. Trust relations between the network nodes in a cluster are created by signing public keys of network nodes with a method similar to the public key signing method in Pretty Good Privacy (PGP). The key pairs of network nodes are used to provide authentication, integrity and confidentiality. A cluster CH maintains a cluster key and distributes it to cluster nodes using the public node keys. Confidentiality of intra-cluster communication is provided by encryption with the shared secret cluster key.

Distribution of Session Keys

Session keys are shared secrets needed in confidential data communication between network nodes, since confidentiality is implemented by symmetric encryption. An import network security architecture feature is secure distribution of session keys. In a local network domain with few network nodes needed session keys can be manually installed and changed. However, practically always network nodes get needed session key by a key distribution protocol or from a network node functioning as a Key Distribution Centre (KDC). A key distribution protocol is based on key agreement or key transport. Key transport means that one of two communicating parties creates a session key and sends it to the other party encrypted with the public key of the other party. Then decryption is possible only with the corresponding private key, which is a private secret of the receiving party. Common key agreement protocols are Diffie-Hellman (DH), which is based on secure modular exponentiation in publicly known finite integer field, and Elliptic Curve Diffie-Hellman (ECDH), which is based on secure duplication of discrete points on a publicly known elliptic curve. Emerging key agreement protocols use Identity Based Encryption and Quantum Cryptography. In this sub-section is outlined session key distribution with a KDC and session key agreement based on Quantum Cryptography.

Key distribution centre (KDC)

For secure pairwise communication between network nodes and/or network users when the number of network nodes or users is large, key distribution usually relies on a Key Distribution Server, which is called a Key Distribution Centre (KDC). In secure data communication based on the services of a trusted KDC, the following cryptograhpical information hierarchy is defined:

- *bottom level:* **user data** cryptographically protected using session keys
- *middle level:* **session keys** cryptographically protected using master keys
- *top level:* **master keys** non-cryptographically protected for example by manual key delivery.

Every network node or user shares a unique secret master key with the KDC, which on demand delivers secret session keys to pairs of network nodes or users who want to communicate securely. (Stallings, 2011)

Quantum key distribution (QKD)

The observation, that the stochastic parallelism of quantum states cannot be simulated efficiently on a classical computer (Feynman, 1982) started research on using quantum physics for efficient information processing. In 1984 a quantum protocol, called the BB84 Protocol, for information transfer with perfect secrecy was proposed (Bennett & Brassard, 1984). This protocol is a Quantum Key Distribution (QKD) protocol, which uses quantum states implemented by randomly polarized photons for secure distribution of symmetric encryption/decryption keys (Elliot, 2004; Quellette, 2004). For some years also commercial QKD technology has been available (id Quantique, 2011; MAGIQ, 2007).

The communication architecture and the phases of the BB84 Protocol are shown in Figure 1.

1. Alice sends over an optical channel a sequence of polarized photons to Bob. Each photon is randomly polarized to a state in the set {|horis>, |vert>, |+45°>, |-45°>}. Bob guesses the polarization base (horisontal/vertical or diagonal) of each photon and measures the polarization in the guessed base. Polarization is correctly measured only for a correctly guessed polarization base, since measurement outcome is with equal probability one of the two orthogonal states of a wrongly guessed polarization base.
2. Bob sends over a classical network channel the sequence of polarization base guesses to Alice.
3. Alice returns to Bob the sequence of correct guesses.

Now Alice and Bob can use Bob's correctly measured polarizations as a shared secret (key), which consists of the polarization states of about 50% of the photons sent by Alice.

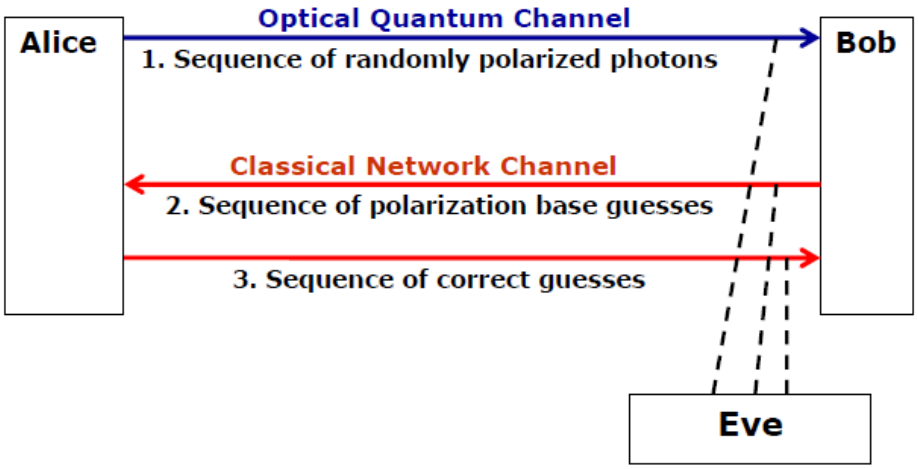

Figure 1: Principle of the BB84 QKD protocol.

Assume that Eve (eavesdropper) measures the polarization of each photon in Alice's sequence in a guessed basis and forwards the measured photons to Bob. This means that a random choice of 0 or 1 is forwarded when Eve's polarization basis guess is incorrect. Since the probability of an incorrect guess is 50 %, about half of the bits are randomized in the bit sequence, which Alice and Bob think is a shared secret.

The original BB84 Protocol is however only a "Sifting Phase" of a QKD Protocol for agreement on a raw shared secret key by Alice and Bob. Sifting means that emitted photons not reaching the receiver are never included in the raw keys. In the use of the BB84 Protocol a "Key Distillation" process consisting of "Error Correction" and "Privacy Amplification" is a necessity. A shared secret key consists of the bits remaining in a raw key after "Key Distillation". In "Error correction" the bits which are different in the raw keys of Alice and Bob are detected and removed. In "Privacy Amplification" as many as possible of the correct bits known by a possible eavesdropper are removed from both raw keys. The probability that a possible eavesdropper has correctly guessed the polarization basis of all photons corresponding to the raw key bits is 2^{-N}, where N is the raw key length. (Elliott, Pearson, & Troxel, 2003)

The BB84 Protocol is a 4-state QKD protocol since it is based on random choice from four different polarization states. However, only 2 non-orthogonal polarization states are in fact needed in implementation of a perfectly secret QKD protocol (Bennett, 1992). Perfectly secret 6-state QKD protocols have also been proposed and analyzed (Bruss, 1998).

Trust in Cryptographic Identities

A cryptographic identity can be defined as ownership of a key pair in public key cryptography. Presently common public key cryptography is based on secure modular exponentiation (RSA, DSA, DH) and on Elliptic Curve Cryptography (ECDH, ECDSA). A cryptographic identity is trusted of the binding between a public key cryptography key pair and identity information of the key pair owner is genuine and unambiguous. A structure for providing trust in cryptographic identities is an important feature in a network security architecture. The usual trust structure is a Public Key Infrastructure (PKI) in which the binding between the owned public key cryptography key pair and identity information of the key pair owner is certified with a trusted digital signature. An emerging trust structure is a network of trusted Private Key Generation authorities in Identity Based Encryption (IBE). Both trust structures are outlined in this sub-section.

Public key infrastructure (PKI)

An IT infrastructure for creation, distribution and utilization of certificates with trustworthy signatures is called a **Public Key Infrastructure** (**PKI**). In (Vacca, 2004) a PKI is described as "a set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke Public Key Certificates based on public-key cryptography". Trust in the public key of a certificate is cancelled on revocation. Openly accessible Certificate Revocation Lists (CRL) are thus necessary data structures of a PKI. A PKI consists of five types of components:

1. **Certification Authorities (CAs)** - to issue and revoke Public-Key Certificates (PKCs)
2. **Organizational Registration Authorities (ORAs)** - to vouch for the binding between keys and certificate holder identities and other attributes
3. **Certificate holders** - to sign and encrypt digital documents
4. **Clients** - to validate digital signatures and their certification path from a known public key of a trusted CA
5. **Repositories** - to store and make available certificates and Certificate Revocation Lists (CRLs)

A Registration Authority (RA) is an optional component of a PKI. A RA is a service controlled by a CA. This means that a RA is "an optional entity given responsibility for performing some of the administrative tasks necessary in the registration of subjects, such as: confirming the subject's identity; validating that the subject is entitled to have the values requested in a PKC; and verifying that the subject has possession of the private key associated with the public key requested for a PKC" (Vacca, 2004). For repositories of issued certificates and CRLs directory services based on the Lightweight Directory Access Protocol (LDAP) (Sermersheim, 2006) are recommended.

Identity based encryption (IBE)

The traditional Public Key Infrastructure (PKI) provides strong security but has turned out to be difficult to use for an average user. Furthermore, PKI causes, especially in mobile devices, a high load on the computational power and the bandwidth. Identity Based Encryption (IBE) is a public key cryptosystem where an arbitrary identity string is a valid public key. Public key certificates and certificate revocation lists (CRLs) are therefore not needed. Computationally costly certificate and CRL management is avoided.

IBE concept was first introduced in (Shamir, 1984). The first practical IBE scheme proposed in (Boneh & Franklin 2001) was followed by vast research on IBE. A security flaw in the Boneh & Franklin scheme has been removed (Galindo, 2005), several variants of these schemes have been proposed (Al-Riyami & Paterson 2003; Boneh & Boyen 2004; Gentry, 2006; Sahai & Waters, 2007), IBE signature schemes have been proposed (Cha & Cheon, 2002; IBE, 2007), a different practical IBE scheme has been proposed (Cocks, 2001), IETF standardization of IBE has started

(Appenzeller et al. 2007), and IBE based security services have been integrated in commercial security products (Voltage, 2011).

Authentication, protected data communication, stored data protection, and non-repudiation signatures are examples of security services, which can be implemented with IBE. Requirements for authentication services are IBE based signing, signature verification, encryption and decryption. Requirements for protected data communication and stored data protection are IBE based encryption and decryption. Requirements for non-repudiation signatures are generation and distribution of private user keys without key escrow, IBE based signing, and IBE based signature verification.

An IBE scheme consists of four algorithms (Boneh & Franklin 2001):

- **Setup** – A master private key and public IBE parameters are generated by a Private Key Generation Authority (PKG)
- **Extract** – The private user key associated with an arbitrary public key string is generated with the master private key
- **Encrypt** with the public user key
- **Decrypt** with the associated private user key.

An IBE scheme can be based on an operation called pairing defined for a pair of discrete elliptic curve points or on quadratic residuosity. Elliptic Curve Public Key Cryptosystems are described in detail for example in Menezes (1994).

Software and/or hardware for IBE and a PKG are required for security service implementations. Two open source software libraries for pairing implementations are presently available (Identity, 2007; PBC, 2011). Software implementations of quadratic residuosity are supported by number theoretic functions in the GMP library (GMP, 2010).

Secure private user key generation and distribution requires

- authentication of legitimate PKG users
- protected data communication between the PKG and authenticated users.

Three methods have hitherto been used to preserve some benefit of IBE cryptosystems without introducing full key escrow by default:

- Threshold techniques to distribute the secret master key
- Embedment of a user generated component in a private key issued by a PKG
- Use of an Accountable Authority Identity based Encryption (A-IBE) scheme for which the existence of multiple private keys for the same identity string can be proved and detected.

QoS Architecture

Quality of service (QoS) means that different applications, data flows, and users in a computer network can be given different priorities and that certain service levels for data flows are guaranteed. Service levels are specified by bounds on performance parameters like bandwidth, latency (delay), jitter (delay variation), dropping probability of data packets, and bit error rate (BER). QoS should provide necessary performance, reliability, and usability of a network service even if the network is overloaded and/or faulty.

Network applications which cannot function without a lower bound on the available bandwidth and an upper bound of the latency are inelastic applications. Other network applications are elastic applications, which can utilize any available bandwidth and function for any latency. Examples of inelastic network applications are

- safety-critical applications such as remote surgery and remote real-time control of machinery in industrial systems
- streaming media and specifically Internet protocol television (IPTV)

- Voice over IP (VoIP)
- Videoconferencing
- Online games.

Future IP based networks are heterogeneous, composed of different portions managed by different service providers, and use different technologies and transmission means. Each single network portion may implement a different QoS solution. A Service Level Agreements (SLA) between a network user and a network service provider specifies QoS levels for network applications and network services to the network user. A QoS solution in a heterogeneous network consists of the following network structures, activities and algorithms:

- QoS architecture
- QoS signalling
- QoS classes
- Data packet marking
- Flow identification
- Data traffic shaping
- Scheduling
- Flow Control
- Queue management
- Routing
- Call admission control
- Network resource reservation
- Network resource allocation
- Network traffic engineering
- Overprovisioning.
  (Marchese, 2007)

Two basic QoS architectures, Integrated Services (IntServ) in RFC 1693 and Differentiated Services (DiffServ) in RFC 2475, have been standardized for IP network by the Internet Engineering Task Force (IETF). IETF has also outlined an evolution of the IP QoS Architecture in RFC 2990. The Technical Specification ETSI TS 185 001 V1.1.1 (2005-11) from the European Telecommunications Standards Institute (ETSI) defines following requirements for a Next Generation Network (NGN) QoS Architecture:

1. Support functions for QoS resource reservation, admission control service based on local policy, network policy control and gate control.
2. Provide a mechanism to Application Functions in different multimedia service subsystems to reserve resources in the access transport and the core transport.
3. Support resource and admission control across multiple administrative domains.
4. Support the three QoS scenarios defined in clause 9, namely "Proxied QoS with policy-push", "User-requested QoS with policy-push" and "User-requested QoS with policy-pull".
5. Support both guaranteed QoS control and relative QoS control.
6. Support different access transport technologies, including xDSL, UMTS, Cable, LAN, WLAN, Ethernet, MPLS, IP, ATM, etc.
7. Support different core transport technologies.
8. Be able to export charging information and session metrics.

QoS architectures for future network are proposed in research papers from several research projects (for example in Chen et al., 2009; de Castro Monteiro & de Lira Gordim, 2010; Dugeon et al., 2007; Gozdecki et al., 2003; Jun et al., 2010; Sargento et al., 2005; Sargento et al., 2007; Sulthani & Rao, 2009).

Two QoS signalling protocols, Resource Reservation Protocol (RSVP) in RFC2295 and Next Steps in Signalling (NSIS) in RFC 4080, have been standardized by IETF. QoS Signalling Requirements in NGN are specified in the Technical Specification ETSI TS 185 001 V1.1.1 (2005-11).

NGN QoS classes are defined for example by the Telecommunication Standardization sector of the International Telecommunication Union ITU-T in the Recommendation Y.1541 (02/2006), see Tables 1 and 2. In Table 3 are shown the bandwidth allocation methods, which are specified in the ETSI Recommendation Y.1221 for the proposed QoS Classes 5 … 0.

Table 1: IP QoS Classes in ITU-T Y.1541 (U = unspecified).

Network Performance Parameter	Nature of Network Performance Objective	Class 0	Class 1	Class 2	Class 3	Class 4	Class 5
IP Packet Transfer Delay (IPTD)	Upper bound on the mean IPTD	100 ms	400 ms	100 ms	400 ms	1 s	U
IPTD Variation	Upper bound on the $1\text{-}10^{-3}$ quartile of IPTD minus the minimum IPTD	50 ms	50 ms	U	U	U	U
IP Packet Loss Ratio	Upper bound on the packet loss probability	$1*10^{-3}$	$1*10^{-3}$	$1*10^{-3}$	$1*10^{-3}$	$1*10^{-3}$	U
IP Packet Error Ratio	Upper bound	$1*10^{-4}$					U

Table 2: Guidance for QoS Classes in ETSI Y.1541 (VTC = Video Teleconference).

QoS Class	Applications (Examples)	Node Mechanisms	Network Techniques
0	Real-Time, Jitter Sensitive, High Interaction (VoIP, VTC)	Separate Queue with Preferential Servicing, Traffic Grooming	Constrained Routing/Distance
1	Real-Time, Jitter Sensitive, Interactive (VoIP, VTC)		Less Constrained Routing/ Distance
2	Transaction Data, Highly Interactive (Signalling)	Separate Queue, Drop Priority	Constrained Routing/Distance
3	Transaction Data, Interactive		Less Constrained Routing/ Distance
4	Low Loss Only (Short Transactions, Bulk Data, Video Streaming)	Long Queue, Drop Priority	Any Route/Path
5	Traditional Applications of Default IP Networks	Separate Queue (Lowest Priority)	Any Route/Path

Table 3: Recommendations in ITU-T Y.1221 (PHB = Per Hop Behaviour).

Transfer capability	Associated DiffServ PHB	IP QoS class	Remarks
Best Effort (BE)	**Default**	**QoS Class 5 (Unspecified)**	A legacy IP service, when operated on a lightly loaded network, may achieve a good level of IP QoS.
Statistical Bandwidth (Modified to Limit Delay)	**Assured Forwarding**	**QoS Classes 2,3,4**	The IP Packet Loss Ratio objective applies only to the IP packets in the higher priority levels of each AF class; the IPTD objective applies to all packets.
Dedicated Bandwidth (DBW)	**Expedited Forwarding**	**QoS Classes 0 and 1**	–

Network Protocols

IPv6 and following network protocols and network protocol types are especially important in future pervasive networks:

- Wireless Communication Protocols
- Mobility Management Protocols
- Routing Protocol
- Network Security Protocols.

IPv6 and these network protocols are described in this section.

IPv6

IPv6 is designed to be an improved version of the current IPv4 protocol. The current public specifications are available at (IETF, 2007). The main improvement made in IPv6 is the increased number of addresses available for network devices. IPv6 has 128 bits available for addressing, meaning that the available addresses are 2^{128} which is 10^{28} more than in IPv4. Thus Network Address Translation (NAT), or other devices breaking the end-to-end Internet traffic nature, is no longer needed in IPv6 networks. An IPv6 address is usually written as eight groups of four hexadecimal digits, e.g. *2001:0ba8:85a3:08d3:1319:8a2e:0170:7221*. The IPv6 addresses are divided into three categories:

- *Unicast Addresses*. Defines a single network interface. A packet sent to a unicast address is delivered to one specific computer.
- *Multicast Addresses.* Are used to define a set of network interfaces that belong to several computers. A packet sent to a multicast address is delivered to all network interfaces identified by that address.
- *Anycast Addresses.* Several network interfaces share the same anycast address. By sending a message to an anycast address, a message from a network node can be sent to several hosts with the idea that the nearest host receives the message and then distributes it to the others with the same anycast address. This feature is usable i.e. when updating routing tables.

An IPv6 packet consists of two main parts: a header and a payload. The first 320 bits of the packet is reserved for the header, see Figure 2. It contains a source and a destination address of which both are 128 bits. Other parts of the header are:

- IP version (4 bits)

- Traffic class (4 bits, packet priority)
- Flow label (20 bits, QoS management)
- Payload length (16 bits, payload length in bytes)
- Next header (8 bits, specifies the transport layer protocol used by a packet's payload)
- Hop limit (8 bits, time to live).

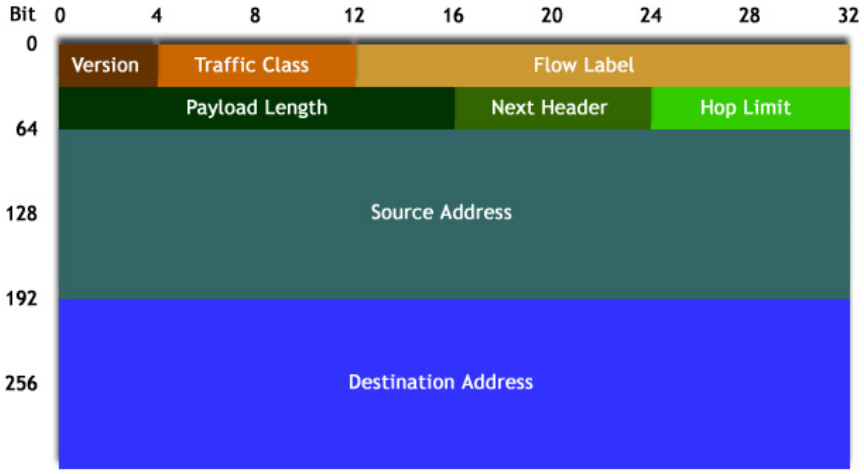

Figure 2: The structure of an IPv6 packet header.

The rest of the IP packet (after the header) is allocated for the payload (the essential data of the IP packet). The size of the payload can be maximum 64 kB in standard mode, or as large as 4GB "jumbo payload" option is used.

Wireless Communication Protocols

An often used data network taxonomy is based on the data communication range. Data networks with global range are called Wide Area Networks (WAN), data networks with a range of 10-100 km are called Metropolitan Area Networks (MAN), data networks with a range of 100-1000 m are called Local Area Network (LAN), and data networks with a range of 10-100 m are called Personal Area Networks (PAN). In ubiquitous networking wireless communication protocols are needed for all these network categories. Current wireless communication protocols are

- Satellite Communication for Wireless WANs (WWAN)
- WiMAX for Wireless MANs (WMAN)
- Wi-Fi for Wireless LANs (WLAN)
- Bluetooth for Wireless PANs (WPAN).

Mobile cellular networks of type GSM, GPRS, and UMTS use own communication protocols for the wireless data communication between mobile devices and the base station of the cell in which they are located. For data communication with a very short range of 1-2 m the Near Field Communication (NFC) protocol can be used.

Mobility Management Protocols

A link layer mobility protocol is included in the IEEE 802.11 specifications for WLANs. On network layer Mobile IP (MIP) is the most well known protocol for network host mobility. Network Mobility (NEMO) is a protocol based on MIPv6 for mobility of networks. Other network layer mobility protocols are MOBIKE, a mobility and multi-homing extension to Internet Key Exchange Version 2 (IKEv2), and Location Independent Network Architecture (LINA). The first

transport layer mobility management proposals were TCP-R, MSOCKS, and Multi-homed TCP, also known as Extended Transport Control Protocol (ETCP). Current transport layer mobility scheme proposals are Mobile Stream Control Transport Protocol (mSCTP), Migrate TCP, and Datagram Congestion Control Protocol (DCCP). At the session layer, Migrate is a proposed protocol to cope with mobility events. Other session layer mobility protocols are Session Layer Mobility Management (SLMM) and Distributed Home Agent for Robust Mobile Access (DHARMA). Session Initiation Protocol (SIP) is a mobile application layer protocol for establishing interactive multimedia sessions. SIP can handle terminal, session, personal and service mobility. Hybrid mobility management schemes have been proposed in order to combine advantages of mobility management on the transport and the network layers of the network protocol stack. Proposals of hybrid mobility management schemes are Host Identity Protocol (HIP) and Homeless Mobile IP.

Network layer mobility

Mobility IPv4 (MIPv4), Mobility IPv6 (MIPv6) and Location Independent Network Architecture for IPv6 (LIN6) are protocols that apply proxy, tunnelling and security techniques in the network layer to deal with mobility.

Mobility IPv4 (MIPv4). The protocol defines a home network, a home agent (HA), a home address of the mobile node (MN), a foreign network and a foreign agent (FA). HA and FA relay data packets between the MN and a corresponding node (CN), se Figure 3. When MN accesses a foreign network it obtains a care of address (CoA) through DHCP (Dynamic Host Configuration Protocol) and informs it´s HA by sending a Register Request message. For further information details about architecture and operation, see (Le, Fu & Hogrefe, 2006). In MIPv4, the security in enhanced by using reverse tunnelling to avoid ingress filtering problems, by authentication of registration messages and by adding time steps to the mentioned messages in order to check validity.

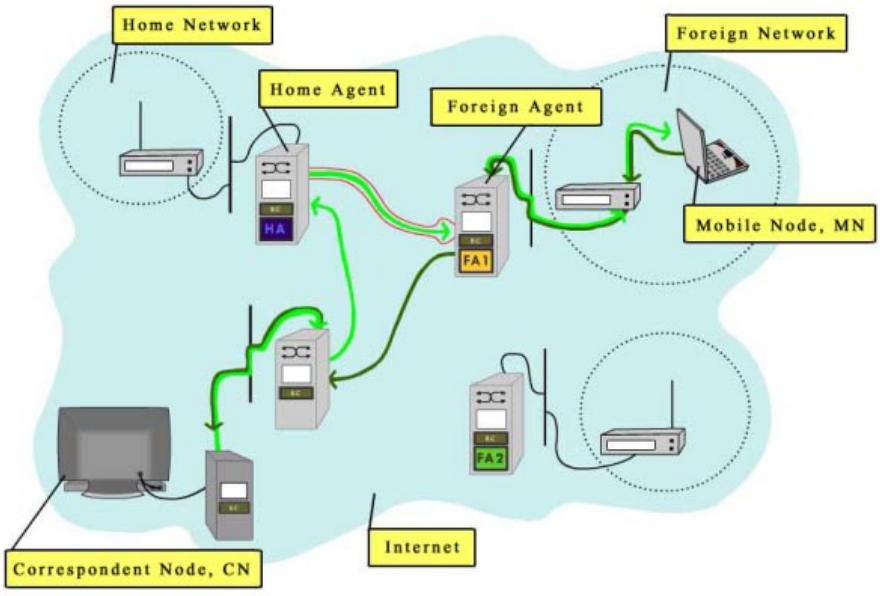

Figure 3: Data communication to/from a Mobil Node for Mobile IPv4 in an example network.

Mobility IPv6 (MIPv6). In MIPv6, the same basic principles as in MIPv4 are followed. Route optimization has been added but on the other hand, the foreign agent (FA) is missing. Security

features are integrated and included as an extension to the headers by the use of the IPSec protocol.

LIN6. In LIN6, the identifier and the locator in the IPv6 address are separated. A LIN6 ID is introduced for each node as the node identifier. Further, two types of network addresses, the LIN6 generalized ID and the LIN6 address, are defined. The generalized ID is used to identify the connection in the transport layer and the LIN6 address is used to route packets over the network layer. Both values are formed by concatenating the LIN6 ID to corresponding prefixes. Location registration is authenticated by IPSec or by exchanged cookies. This gives a security level of the same order as in MIPv6. (Le, Fu and Hogrefe, 2006)

MOBIKE. In a mobile environment during IPSec communication, the existing IKE Security Association (SA) and IPSec SA become invalid. Rekeying the SAs for user interaction and authentication has shown to be slow. Therefore an extension called MOBIKE has been added to IKEv2. The established SAs are kept alive and no rerun of the initial IKEv2 exchange is needed. Connectivity check of dead peers and updating of the IP addresses is an included mechanism. In addition, MOBIKE supports multihoming and has the possibility to inform a node whether its peer support MOBIKE or not. However, the rendezvous problem is not dealt with in MOBIKE. All MOBIKE messages are authenticated by the IKEv2 thus preventing modification of the contents of the packets although the IP addresses in the IP header are authenticated. This might cause remote redirection vulnerabilities.

Mobility technique in an additional layer

Host Identity Protocol (HIP). HIP separates location from identity by an identity layer that operates between the network and transport layers, see Figure 4. Connection to the transport layer is bound to a host identifier (HI) namespace which actually is a public key. The HI, presented by a host identifier tag (HIT), is mapped to one or more IP addresses in the HIP layer. By "hashing" the HI and truncation the output to the IPv6 address size the HIT is obtained. A rendezvous server (RVS) is used to provide location management. Communications are bound to the public keys of the HI and are encrypted with ESP. Correspondingly, the REA message (update packet with readdress parameter) is signed with the sender´s public key. Additionally, DoS attacks are prevented by a four step connection establishment procedure.

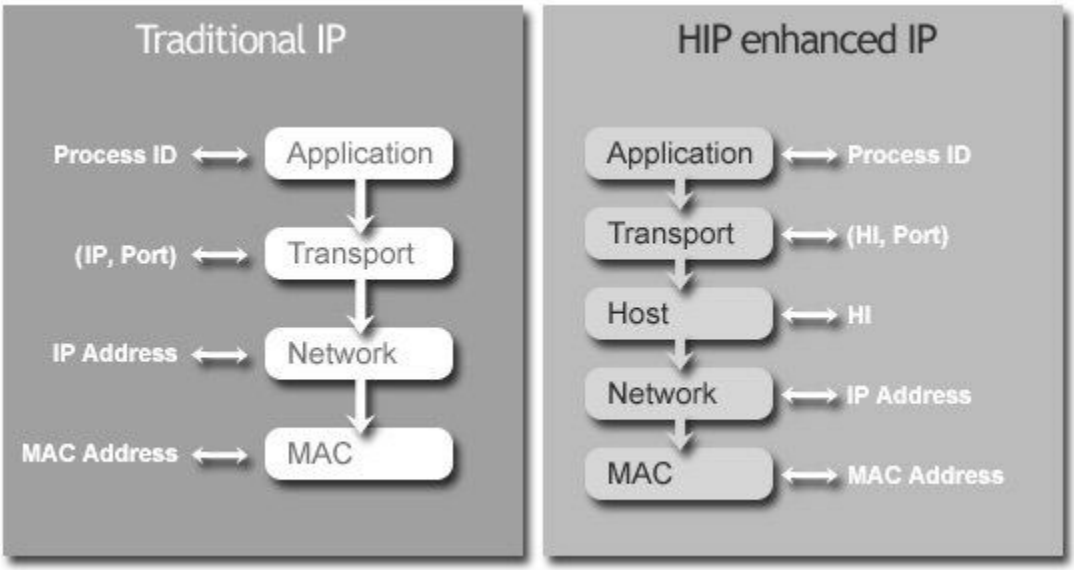

Figure 4: Traditional IP (left) and HIP enhanced IP protocol stacks.

Multiple Address Service for Transport (MAST). MAST defines a layer between the network and transport layers. No new namespace or addressing structure is created. As a consequence no additional packet header overhead and minimal additional packet processing overhead is created. Mobility is provided by mapping different IP addresses to the single initial IP address. The initial IP address is used for the identifier of the MN and other IP addresses are added dynamically while moving and are used as the locator of the MN. A mechanism that supports multiple IP address association is used. MAST uses association-specific weak authentication to resist hijacking attacks. This ensures that later packets come from the same source as the initial packet. IPSec and TLS are suggested for protection against spoofing and redirection.

Transport layer mobility

Mobile Stream Control Transmission Protocol (mSCTP). Stream Control Transmission Protocol (SCTP) is a transport layer protocol that supports mobility due to its multi-homing feature. An SCTP session is established over multiple interfaces identified by multiple addresses, i.e. the MN initiates a negotiation process to initiate an SCTP association with the CN by negotiating a list of IP addresses. One address is chosen as the primary part and the other addresses are active IP addresses. Using the ADDIP extension (RFC5061) it is possible to add or delete an IP address and change the primary address. SCTP with ADDIP extension is known as Mobile SCTP (mSCTP). The four step negotiation process prevents DoS attacks and further, IPSec is used to secure the communication. The IP address addition/deleting process provides an opportunity in which an existing association can be hijacked. SCTP needs a link level/upper layer mechanism, e.g. SIP, to detect mobility and handover.

Datagram Congestion Control Protocol (DCCP). DCCP provides integrated mobility and multi-homing support. A generalized connection in DCCP combines so-called component connections into a single application level entity. When a host attaches a new connection component and deletes the old one, mobility is achieved. Mobility support is optional. When multiple component connections with different endpoint addresses are maintained multi-homing is implemented. Cryptographic security guarantees are not provided by DCCP but sequence validity checks protect against hijacking of DCCP connections.

Mobile TCP (M-TCP). Various solutions have been developed to extend TCP to support mobility. Indirect TCP (I-TCP) and Mobile TCP (M-TCP) address the bit error rate (BER) problem of wireless links. A Lightweight Mobility Detection and Response (LMDR) TCP option has also been implemented. This option allows proper congestion control. The proposals optimize the TCP performance over wireless links but they cannot support real mobile networking. TCP Redirection (TCP-R) and TCP Migrate are extensions that maintain active TCP connection through secure redirection and migrate options.

Mobile UDP (M-UDP). A Mobile UDP (M-UDP) has been proposed aiming at reducing packet losses in wireless links. Like in I-TCP and M-TCP, the idea is to split UDP connections in two at some node close to the mobile user. This node will use any free bandwidth to retransmit lost packets. This approach does not consider security.

Application layer mobility

Session Initiation Protocol (SIP). SIP is an application layer protocol for establishing interactive multimedia sessions. Two types of terminal mobility, pre-call and mid-call mobility, can be established. Pre-call mobility establishes a session at the start of a new connection when a MN has moved to a new location. The new IP address is registered by the MN with a redirect server at the MN's home network. When the MN requires a new IP address in the middle of a session, CN and also the redirect server have to be informed. Delays involved in the application layer processing

and the need for support from lower layers to detect network changes are disadvantages. SIP supports both authentication and encryption of messages by using challenge response or private/public key cryptography.

Routing Protocols

In mobile infrastructure networks, end user devices communicating with wireless access points (APs). APs operate as routers between wireless nodes connected to that AP as well as between the wireless network and the wired network infrastructure behind the AP. A network node, connected to a wireless router, receives all data packets sent from the wireless router, even though a data packet was not meant for that particular node. Therefore it is essential, that all wireless links use secure wireless protocols.

In a mobile network, where nodes are dynamically changing their locations and network attachment points, mobility features must be provided, such as smooth handover and reach ability. There are several security risks related to mobility. For instance, a network session can be hijacked when a mobile node moves and changes IP-address.

In MANETs, where no network infrastructure such as APs or dedicated routers exists, designing secure routing protocols is a very challenging task. Routing protocols are expected to work securely in a network where the network topology changes dynamically. Due to the lack of infrastructure in MANETs, every node must participate in the routing process. Most MANET nodes are small portable devices with limited processor, power, bandwidth, and storage capacity. This must be taken into account routing protocol design.

Network Security Protocols

Relevant network security protocols in ubiquitous networking are

- **SSL/TLS** – for secure www browsing, for secure email communication, for Virtual Private Networking (VPN) and for secure implementations of any network application
- **PGP, S/MIME** – for secure email content
- **IPSec, IKEv2, MOBIKE** – for secure network layer data communication and for mobile VPN
- **HIP** – for secure network layer communication and for secure mobility.

Network Programming

In development of network applications and in design of network services for ubiquitous networks the following knowledge patterns and skills are needed:

- Familiarity with mobile operating systems. Current relevant mobile operating systems are Symbian, Windows Mobile, Linux based MeeGo and Android, and Blackberry OS
- Use of mobile programming methodology
- Procedural and object oriented programming skills in programming languages like
    - C,
    - C++,
    - Java, and
    - C#
- Socket Programming Skills
- Use of development tools like
    - QT in Symbian, MeeGo, and Windows environments,
    - Windows Mobile SDK,
    - Android SDK, and
    - Blackberry SDK.

Impact on Education and Research in Arcada

Arcada is a university of applied sciences in Helsinki, Finland. Arcada offers 16 BSc and MSc degree programmes, three of which are in English. Arcada also offers specialization studies, professionally orientated supplemental training and open courses within the frames of Arcada Further Education. Arcada offer education within Sports, Health Care, Social Services, Business Administration, Media and Technology. Arcada provides an international learning environment. About 10% of the students are of foreign origin and represent more than 40 nationalities. Education and research areas are integrated. Information technology research areas are data communication security software, applied cryptography, security in wireless and mobile data communication, education concepts, and IT in business processes.

Data communication security software. The research is focused on development, testing, and verification of mobile security software for wireless data networks such as MIP (Mobile Internet Protocol), HIP (Host Identity protocol) and VPN (Virtual Private Network).

Applied cryptography. In this area authentication methods (certificate, identity based) are studied. Confidential and certified health information, and security based on quantum cryptography are examples.

Security in wireless and mobile data communication. Included topics are security testing of standardized mobile and wireless networks, security of MANET networks, security software testing based on HIP, and application security of smart cell phones.

Education concepts. Flash animations are being developed. Network courses like ”Network Security” and ”Communication Platforms for Mobile Services” are in use.

IT in business processes. In this area mobile digital services are commercialized.

As a result the following courses are for the moment included in the ICT (35 cr), Network Master (25 cr) and Mobile systems (15 cr) modules of the Arcada BSc Degree Programme in Information Technology:

Introduction to programming with Java, 5 cr
Internet technology, 5 cr
Operating systems and working with Linux
Network protocols, 5 cr
Databases and SQL, 5 cr
Project management, 5 cr
Telecommunication and DSP, 5 cr

Computers, computer architecture and network, 5 cr
Network installation and administration, 5 cr
Security of computer systems and networks, 5 cr
Network programming, 5 cr
Advanced course in computer networks, 5 cr

Mobile systems, 5 cr
Radio frequency technology, 5 cr
Wireless networks, 5 cr

The current education modules will be updated. Education areas of importance are listed below and some typical education topics mentioned:

- **Cryptography and data security**. Typical subareas are distribution of session keys (KDC, QKD) and identity trust (PKI, IBE).

- **Network protocols and programming**. Most used protocols such as IPv6, MIP, MOBIKE, HIP and SIP are included. Programming languages like C, C++, C# and Java will be used in the programming.
- **Network architectures**. (W)LAN, WMAN, WPAN, WMN, NFC and Mobile Cellular Networks are the most typical ones. Ubiqutous and sensor networks are also included. Mobile ecosystem platforms in education will be Android, Windows Phone and MeeGo/Symbian.
- **Next generation wireless technologies**. Most typical technologies like LTE, 4G, Wi-Fi, WiMAX, Bluetooth and ZigBee
- **Quality of service architecture**. Bandwidth, power, reliability and fault tolerance for different QoS architectures are handled.
- **Network services**. Services being developed are in the areas of public administration, network based education, multimedia and business.

In exercises and laboratory works emphasis will be on installation of different networks, architectures and services. Integration of different technologies and performance optimization are crucial.

Conclusions

The final stage of the information society is not here yet. Ubiquitous computing and the Internet of Things are still in the future. There are still many obstacles although the IT development goes fast in the right direction. Mobility, security, and quality of service (QoS) related problems seem to be the most common. In order to cope with these questions many steps in different areas have to be taken. Network architectures, security architectures, QoS architectures, cryptographic identities, wireless communication protocols, and mobility management protocols are of major importance for the development. This trend will of course also affect university studies and education.

References

Aarts, E., Harwig, R., & Schuurmans, M. (2001). Ambient intelligence. In P. Denning (Ed.), *The invisible future: The seamless integration of technology into everyday life*. New York, NY, USA: McGraw-Hill.

Al-Riyami, S., & Paterson, K. (2003). Certificateless public key cryptography. In *Advances in Cryptology - Asiacrypt'03, LNCS 2894*, Berlin: Springer-Verlag. 452-473.

Appenzeller, G., Martin, L., & Schertler, M. (2007). *Identity-based encryption architecture*. IETF Internet Draft.

Bennett, C. H., & Brassard G. (1984). Quantum cryptography: Public key distribution and coin tossing. *International Conference on Computers, Systems & Signal Processing, Bagalore, India*, December 10-12, 1984, 175 - 179

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett. 68*, 3121-3124.

Boneh, D., & Boyen, X. (2004) Efficient selective-ID secure identity based encryption without random oracles. In *Advances in Cryptology - Eurocrypt'04, LNCS 3027*, Berlin: Springer-Verlag, 223-238

Boneh, D., & Franklin M. (2001). Identity-based encryption from the weil pairing. *Proceedings of Crypto 2001*, *LNCS* 2139, Berlin: Springer-Verlag, 213-29

Bruss, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett. 81*, 3018-3021.

Business Lines > e-Administration Solutions. (2010). maatG, Retrieved December 13th, 2010 from http://maatg.knowleer.org/ptr/vista/tpl/maatg/eadministration.html

Cha, J. C., & Cheon, J. H. (2002). *An identity-based signature from gap Diffie-Hellman groups.* Cryptology ePrint Archive. Retrieved March 20th, 2011, from http://eprint.iacr.org/2002/018

Chen, J.-L., Chen, M.-C., Liu, S.-W., & Jhuo, J.-Y. (2009). Cross-layer QoS architecture for 4G heterogeneous network services. *Proceedings of the 11th international conference on Advanced Communication Technology - Volume 1.* Piscataway, NJ, USA: IEEE Press.

Choi, Y.-J., Lee, K., & Bahk, S., (2007). All-IP 4G network architecture for efficient solutions mobility and resource management. *Wireless Communications, 14*(2), 42-46.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. *Eight IMA International Conference on Cryptography and Coding*, Royal Agricultural College, Cirencester, UK

De Castro Monteiro, C., & de Lira Gondim, P. (2010). An alternative QoS architecture for integrating WLAN/3G networks. *Proceedings of the Sixth International Conference on Wireless and Mobile Communications.*

Dugeon, O., Morris, D., Monteiro, E., Burakowski, W., & Diaz, M. (2007). End to end quality of service over heterogeneous networks EuQoS. In D. Gaiti (Ed.), *Network control and engineering for QoS, security and mobility, IV*. Berlin: Springer-Verlag.

eAdministration More innovation and efficiency, (2010). Siemens IT and Services GmbH, Retrieved December 13, 2010 from http://www.it-solutions.siemens.com/b2b/it/en/global/industries/public-sector/national-regional-administrations/e-administration/Pages/e-administration.aspx

Elliot, C. (2004). Quantum cryptography. *IEEE Security & Privacy*, *2*(4), 57-61.

Elliott, C., Pearson, D., & Troxel, G., (2003). Quantum cryptography in practice. *Proceedings of ACM SIGCOMM 2003*, USA: ACM Press, 227–238.

Eschenbrücher, D., Mellberg, J., Niklander, S., Näslund, M., Palm, P., & Sahlin, B. (2004). Security architectures for mobile networks. *Ericsson Review, 2*, 68 – 81.

Feynman, R. (1982). Simulating physics with computers. *International Journal of Theoretical Physics 21*(6&7), 467–488.

Galindo, D. (2005). Boneh-Franklin identity based encryption revisited. *Automata, Languages and Programming, LNCS 3580*, Berlin: Springer-Verlag, 791-802.

Ghalwash, A. Z., Youssif, A. A. A., Hashad, S. M., & Doss, R. (2007). Self adjusted security architecture for mobile ad hoc networks (MANETs). *Proceedings of 6th IEEE/ACIS International Conference on Computer and Information Science ICIS 2007*. 682 – 687

Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N. & Thomas, T. (2010). LTE-Advanced: next-generation wireless broadband technology. *IEEE Wireless Communications, 17*(3), 10-22.

GMP web pages. (2010). Retrieved March 20th, 2011, from http://gmplib.org/

Gozdecki, J., Pacyna, P., Marques, V., Aguilar, R., Garcia, C., Moreno, J., Beaujean, C., Melin, E. & Liebsch, M. (2003). An IP QoS architecture for 4G networks. *Proceedings of the 2003 international conference on Architectures for quality of service in the Internet.*

Hashim, F., Kibria, R., Magoni, D., & Jamalipour, A. (2007). Hierarchical security architecture for next generation mobile networks. *ICSPCS'07 - 1st International Conference on Signal Processing and Communication Systems*.

id Quantique Portal. (2011). Retrieved March 20th, 2011, from http://www.idquantique.com

Identity Based Encryption JCE Provider. (2007). National University of Ireland. Retrieved March 11th, 2008 from http://www.crypto.cs.nuim.ie/software/eyebee/

ISO 7498-2. (1989). *Information processing systems -- Open systems interconnection -- Basic reference model -- Part 2: Security architecture.*

ISO/IEC 7498-1. (1994). *Information technology -- Open systems interconnection -- Basic reference model: The basic model*.

*IMS Architectur*e. (2010). Metaswitch Networks. Retrieved December 13th, 2010 from http://www.metaswitch.com/sbc-session-border-controller/ims-architecture.aspx

Jun, L., Ning, Y., Lichun. Z., & Yi, S. (2010). Research on QoS architecture of mobile ad hoc networks. *Proceedings of Computational Intelligence and Software Engineering (CISE)*. USA: IEEE Press.

Kambourakis, G., Rouskas, A., & Gritzalis, S. (2004). Experimental analysis of an SSL-based AKA mechanism in 3G-and-beyond wireless networks. *Journal of Wireless Personal Communications, 29*(3-4).

Kibria, M. R., & Jamalipour, A. (2007). On designing issues of the next generation mobile network. *IEEE Network, 21*(1), 6–13.

Le, D., Fu, X., & Hogrefe, D., (2006). A review of mobility support paradigms for the Internet. *IEEE Communications Survey, 8*(1). 38-50.

Overview of wireless architectures and products. (2010), Retrieved December 13th, 2010 from http://www.cs.purdue.edu/homes/fahmy/reports/leynawap.htm

Marchese, M. (2007). *QoS over heterogeneous networks*. West Sussex, England: John Wiley & Sons

MAGIQ QPN 8505 Uncompromising VPN security. (2007). Retrieved March 20th, 2011, from http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf

McLellan, H. (2004). *Internet-based education: Some guidelines*. McLellan Wyatt Digital, Retrieved December 13th, 2010 from http://tech-head.com/i-ed.htm

Menezes, A. J. (1994) *Elliptic curve public key cryptosystems.* USA: Kluwer Academic Publishers. ISBN: 0-792-39368-6.

PBC library. (2011). Stanford University, Department of Computer Science, Retrieved March 20, 2011, from http://crypto.stanford.edu/pbc/

Pervasive Computing. (2006). Postnote Number 263, Parliamentary Office of Science and Technology, Retrieved December 11th, 2010 from http://www.parliament.uk/documents/post/postpn263.pdf

Poslad, S. (2009). *Ubiquitous computing: Smart devices, environments and interactions.* USA: Wiley. ISBN 978-0-470-03560-3.

Quellette, J. (2004). Quantum key distribution. *The Industrial Physicist*, December 2004/January 2005, 22-25.

Sahai, A., & Waters, B. (2007). *Fuzzy identity-based encryption.* E-print 2004/086, Retrieved March 20th, 2011, from http://eprint.iacr.org/2004/086.pdf

Sargento, S., Almeida, M., Corujo, D., Jesus, V., Aguiar, R., Carneiro, G., Godzecki, J., Banchs, A., & Yáñez-Mingot, P. (2007). Integration of mobility and quality-of-service in 4G networks. *Proceedings of 3rd ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2007).* New York: ACM Press

Sargento, S., Prior, R., Goncalves, P., Gozdecki, J., Gomes, D., Guainella, E., Cuevas, A., Dziunikowski, W., & Fontes, F. (2005). End-to-end QoS architecture for 4G scenarios. *IST Mobile & Wireless Communications Summit,* 19- 22-Jun 2005, Dresden, Germany

Sermersheim, J. (2006). *Lightweight directory access protocol (LDAP): The protocol***,** IETF RFC 4511, Retrieved November 19th , 2010 from http://tools.ietf.org/html/rfc4511

Stallings, W. (2011). C*ryptography and network security principles and practice* (5th ed.). USA: Prentice Hall. ISBN 978-0-13-705632-3.

Sulthani, R., & Rao, D. (2009). Design of an efficient QoS architecture (DEQA) for mobile ad hoc networks. *ICGST-CNIR Journal, 8*(2), 49-57

Trusted mobile platform specifications released for industry review. (2004). Retrieved March 20th , 2011, from http://xml.coverpages.org/ni2004-10-27-a.html

Vacca, J. R. (2004). *Public key infrastructure building trusted applications and web services.* USA: Auerbach Publications. Print ISBN 978-0-8493-0822-2, eBook ISBN 978-0-203-49815-6.

Voltage encryption and key management. (2011). Retrieved March 20th, 2011, from http://www.voltage.com/products/kmserver.htm

Zheng, Y., He, D., Xu, L., & Tang, X. (2005a) Security scheme for 4G wireless systems. *Proceedings of the International Conference Communications, Circuits and Systems, Vol 1*. USA: IEEE Press. 397-401

Zheng, Y., He, D., Yu, W., & Tang, X. (2005b). Trusted computing-based security architecture for 4G mobile networks. *Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies PDCAT*. 251–255.

Appendix: List of Abbreviations

2.5G	2.5th Generation
3G	3rd Generation
4G	4th Generation
A-IBE	Accountable Authority Identity based Encryption
AAAA	Authentication, Authorization, Account, Audit
AN	Access Network
AP	Access Point
ATM	Asynchronous Transfer Mode
BE	Best Effort
BS	Base Station
BSc	Bachelor of Science
CA	Certificate Authority
CH	Cluster Head node
CoA	Care-of-Address
CRL	Certificate Revocation List
CN	Correspondent Node
DBW	Dedicated Bandwidth
DCCP	Datagram Congestion Control Protocol
DMU	Decision Maker Unit
DH	Diffie Hellman
DHARMA	Distributed Home Agent for Robust Mobile Access
DHCP	Dynamic Host Configuration Protocol
DSA	Digital Signature Algorithm
DNS	Domain Name System
DoS	Denial-of-Service
DU	Detection Unit
ECDH	Elliptic Curve DH
ECDSA	Elliptic Curve DSA
ESP	Encapsulating Security Payload
ETCP	Extended TCP
ETSI	European Telecommunications Standards Institute
FMCA	Fixed Mobile Convergence Alliance
FQDN	Fully Qualified Domain Name
GB	Gigabyte
Gbps	Gigabit per second

GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HA	Home Agent
HE	Home Environment
HI	Host Identity
HIP	Host Identity Protocol
HIT	Host Identity Tag
I-TCP	Indirect TCP
IBE	Identity-based Encryption
ICT	Information and Communications Technology
ID	Identity
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv2	IKE version 2
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	IP Security
IPTD	IP Packet Transfer Delay
IPTV	IP Television
IPv4	IP version 4
IPv6	IP version 6
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization sector of ITU
kB	kilobyte
KDC	Key Distribution Centre
L2	Layer 2
LAN	Local Area Network
LIN6	Location Independent Networking for IPv6
LINA	Location Independent Network Architecture
LMDR	Lightweight Mobility Detection and Response
LTE	Long Term Evolution
M-TCP	Mobile TCP
M-UDP	Mobile UDP
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MAP	Mobility Anchor Point
MANET	Mobile Ad-Hoc Network
MAST	Multiple Address Service for Transport
Mbps	Megabit per second
MC-CDMA	Multi Carrier Code Division Multiple Access
ME	Mobile Equipment device
MIP	Mobile IP
MIPv4	Mobile IP version 4
MIPv6	Mobile IP version 6
MOBIKE	Mobile IKE
MAP	Mobility Anchor Point

MN	Mobile Node
MPLS	Multiprotocol Label Switching
mSCTP	Mobile SCTP
MTBF	Mean Time Between Failures
NAT	Network Address Translation
NEMO	Network Mobility
NFC	Near Field Communication
NGMN	Next Generation Mobile Network
NGN	Next Generation Network
NSIS	Next Steps in Signalling
O&M	Operations and Management
OFDM	Orthogonal Frequency Division Multiplexing
ORA	Organizational Registration Authority
OS	Operating System
PAN	Personal Area Network
PGP	Pretty Good Privacy
PHB	Per Hop Behaviour
PKC	Public Key Certificate
PKG	Private Key Generation Authority
PKI	Public Key Infrastructure
PoC	Push to talk over Cellular
QKD	Quantum Key Distribution
QoS	Quality of Service
Qt	a cross-platform application and user interface framework
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest, Shamir, & Adleman
RSVP	Resource Reservation Protocol
RVS	Rendezvous Server
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	Security Association
SCTP	Stream Control Transmission Protocol
SDK	Software Development Kit
SDU	Security Database Unit
SIP	Session Initiation Protocol
SLMM	Session Layer Mobility Management
SNMPv3	Simple Network Management Protocol version 3
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TCP-R	TCP Redirection
TLS	Transport Layer Security
TS	Technical Specification
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USIM	User Services Identity Module
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network

Wi-Fi	trademark of the Wi-Fi Alliance
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless MAN
WMN	Wireless Mesh Network
WPAN	Wireless PAN
WWAN	Wireless WAN
xDSL	Digital Subscriber Line

Biographies

Göran Pulkkis received in 1983 his doctoral degree at Helsinki University of Technology and is presently senior lecturer and researcher in computer science and engineering at Arcada University of Applied Sciences, Helsinki, Finland. His current research interests include network security and applied cryptography.

Kaj J. Grahn received his doctoral degree at Helsinki University of Technology and is presently senior lecturer in telecommunications at Arcada University of Applied Sciences, Helsinki, Finland. His current research interests include security of wireless and mobile networks.

Jonny Karlsson received his Bachelor of Science degree in Information Technology and is since May 2002 research assistant and teacher at Arcada University of Applied Sciences, Helsinki, Finland. In January 2009 he started PhD studies in security of future networks at the Open University, Milton Keynes, UK. His current research interests include security of wireless and mobile networks.