UNIVERSITY OF AUCKLAND
DEPARTMENT OF COMPUTER SCIENCE

Thesis

A FIFTH GENERATION MESSAGING SYSTEM

By

JIHONG LI
PGDipSci, The University of Auckland 2000

Submitted in partial fulfilment of the
requirements for the degree of
Master of Science
2001

A FIFTH GENERATION MESSAGING SYSTEM

By

JIHONG LI

Department of Computer Science, The university of Auckland, 2001

Abstract

This thesis is about delivering electronic messages. We propose a multi-services network – a fifth generation messaging system, a software system, designed to make delivery of electronic messages easier, more secure and efficient.

Our goals are to describe an "anytime, anywhere, any-persona and from any-device" multi-services system, which refers to the ability to send and receive electronic messages at any particular time using different kinds of personal identities and through a variety of devices wherever you are. These multi-services include various kinds of information such as voice, data, images and multi-media, any of which can be transferred on the wired and wireless computer networks such as LAN, WAN, and telecommunication networks such as telephone, fax and mobile etc. We will also specify what the most important characteristic features in this multi-services system are.

Today, there are a multitude of communication devices and corresponding means available to exchange electronic information. However, each of these devices and means has different capabilities. For a user wishing to transfer messages, they may have several different identities, such as several phone numbers or many E-mail addresses. In this thesis, we study how a fifth generation messaging system manages their identities, and maintains their privacy and security. Additionally, the location of a user and their preferred device may change at any time. Current information delivery integration systems, which send a message in a heterogeneous communication environment, are incomplete, insecure and inefficient. This fifth generation messaging system we define here offers improved efficiency, security and completeness.

Acknowledgements

I met Professor Clark Thomborson in the middle of 2000. His first lecture of Computer Security convinced me that the adventure of this area was something I wanted to pursue. Prof. Clark taught me many things during this year that I worked for him; the most important being how to write academic documents and complete scientific research. He has been a marvellous mentor and I thank him from my heart for his constant support throughout my project.

Special thanks also go to Paul G Barrett of Telecom NZ, and Alex Skeet of Esolutions. Their inspiration for this project was what got me started and I thank them for paving the way.

There have been a number of folks in the department of computer Science who have helped me on the technical support, to whom I want to give special thanks. I would also like to thank Mark for his help during this year.

My parents: XiuHua and Zijun, I guess I was never able to express my thanks for their love and support throughout my whole life, but I really thank you for being there for me.

Table of Contents

Table of Figures

Table of Tables

1 Introduction:

1.1 Messaging System

Speaking broadly, messaging (also called *electronic messaging*) systems are used for the creation, storage, exchange, and management of text, images, voice, telex, fax and E-mail over a communications network [TechTarget 2002].

We will introduce a fifth generation messaging system in this thesis. In order to understand what the fifth generation messaging system will be, we will first look at the problems associated with current messaging systems, followed by a brief review of the evolution of messaging systems.

Summarized below are the main problems with messaging systems, including the problems of communication, translation, redirection and persona. The requirement of solving these problems is the motivation of messaging system development.

1.2 Problems associated with messaging systems

There has always been a need for people to communicate and share information with each other. It is interesting and useful to see how people have dealt with the problems of long-distance communication throughout history:

In ancient times the communication was based upon signals of sound and light, e.g. drums and horns, smoke signals and beacon fires. Then people started to use tools like pigeons to send message. Throughout the ages groups of people have communicated with one another by making use of different kinds of signaling systems.

As early as the 18th century, attempts had been made to use electricity for the transmission of messages.

Since then, the market and users' demand for communication has grown rapidly. People not only want the message be delivered to the recipient, but may also like to transfer different kinds of information, such as their voice, picture etc. When a person feels that they cannot communicate using a specific information type, we say that they meet the “communication problem”.

In order to satisfy people’s communication needs, different kinds of networks and services have been created. There has been a rapid increase in the variety and absolute number of devices that are used to transfer personal information, such as landline telephones, faxes, cellular phones, PCs, PDAs (Personal Digital Assistant) etc. Figure 1 shows a multitude of communication devices that a person may use today.

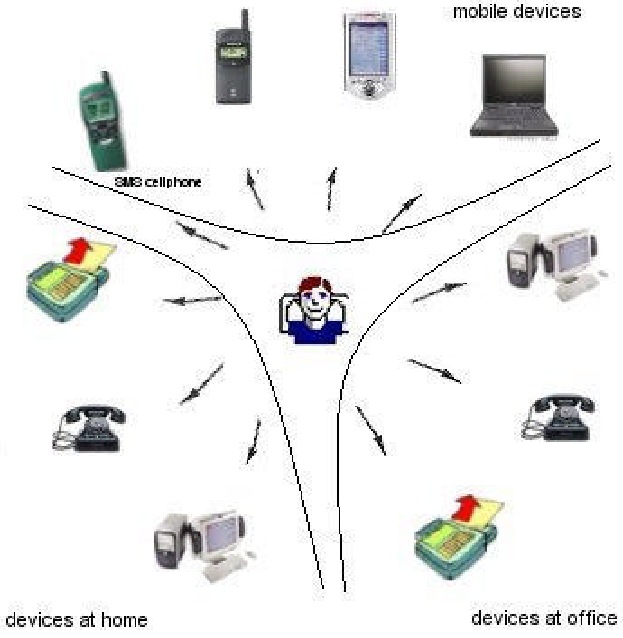

Figure 1: A multitude of communication devices

It seems unlikely that these heterogeneous devices will converge into a single device anytime soon, due to “feature clashes” among portability, power consumption, economy, backwards compatibility, and input/output devices (keyboard, mice, video, etc.).

Some devices are unable to communicate directly with some other devices, unless a “translation service” is available.

When a person is unable to quickly find and use an appropriate translation service, they face what we have identified as a “translation problem”.

The increasing mobility of individuals and their need to be reachable has led to an increased demand for services to access these users' devices so that they can be used conveniently. Message reach to the recipient is not just talking about the must-have cell phones, personal digital assistants, and other wireless devices that more and more people carry every day. But for now the race is on to get as connected as possible. So far we can take and make calls, browse the Web, and even read and send e-mail on our phones, PDAs, etc.

When a communication system is unable to let a kind of high priority and time-critical information reach the recipient, and let the sender get the received feedback on time, we will say that this system has a "redirection problem".

Finally, from psychologist's view, a well-developed individual may have several personae appropriate to business and social situations. One of Sigmund Freud's followers and students, Carl Gustav Jung, who was the best-known member of the group that formed the core of the early psychoanalytic movement saw "the persona as a vital sector of the personality which provides the individual with a container, a protective covering for his or her inner self" [Hopcke, R. H. 1989]. One's persona reveals certain selected aspects of the individual and hides others [Geist, M 1998]. People may need to "hide" the information related to his or her one persona from the communication partner who related with his or her other persona.

When people feel a need for help in managing the information belonging to their different persona, we say that they face a "persona problem".

In the following four subsections, let us see those four problems' details one by one.

1.2.1 Communication problem:

In recent years, people have been building up different kinds of networks and services to satisfy the need for communication. The solving of the "communication problem" has caused the existence of the two independent and parallel networks currently operating. They are the voice network that we use for telephone calls and fax, and an Internet that we use for IP based data communications, such as E-mail and images etc.

People have access to a growing number of networks (e.g., Internet, cellular,) on a growing number of devices (e.g., personal digital assistants, cell phones, smart cards) at a growing number of locations (e.g., work, home, on the road). It looks as if people are easy to reach now, but in fact it is just opposite. A sender may find it even more difficult to catch the recipient.

1.2.2 Redirection problem:

Network devices, applications, and accessible locations are growing, it becomes less likely that other people (*information sender*) can get in touch with a mobile person at any particular time. People are limited in their reach ability by the devices they can use at a certain location. For example, a sender might not have the traveling person's hotel phone number, or the correspondent's E-mail application might not interoperate with the mobile person's phone. People are becoming more difficult to keep track of now.

For high priority and time-critical information, the recipient may want to receive on time, and sender may want to get the feedback of the information as soon as possible.

When the message cannot be received by the recipient on time, we say this messaging system has a “redirection problem”.

A growing need for people to instantly reach others, and the difficulty of keeping track of people makes redirection important in a messaging system.

Stefan Arbanowski and Dr. Thomas Magedanz mentioned this function in their upcoming fourth generation of messaging system, by using a location-awareness application (automated, manually, or scheduled) to recognize the recipient’s position, to know the addresses of the terminals, and for sending information [Meer, S. Arbanowski, S. Magedanz, T. 1999]. Some existing integration systems have provided a partial solution to this “redirection problem”. For instance Active Messenger [Marti, S. J. W. 1999], and some product’s “follow me” feature.

Besides the aim of sending the information to where the users can easily receive it, we expand the “redirection problem” as:

- *Person-to-person reachability:*

  First, we need a system that can provide person-to-person reachability. The system should direct the sender's communications to the mobile person, regardless of whether the sender and recipient have direct access to the same kind of network, device, or application.

  Let’s suppose Alice and Bob are two sales people in the process of closing an important new deal. Alice is travelling, when a critical, last minute issue arises. Bob can send an urgent message from his office laptop to Alice, without knowing exactly where and how to reach her. Through our messaging system, Alice has identified her mobile phone as her “urgent” device for that specific time. Under the help of our general translation function, the system can automatically route information to Alice’s mobile phone. The feedback, which shows that Alice had received and read the message, can be sent back to Bob.

- *Sequentially redirecting information over time:*

  Second, message redirection includes not only rerouting a message to the recipient’s appropriate device, but also using several devices sequentially over time.

  While Alice is on vacation, she can receive a message on her cell phone alerting her of possible credit card fraud. By pressing “1,” she confirms that the charges are hers. Several days later, she receives an alert on her PDA indicating that she is nearing her credit limit. By responding with a message saying, “transfer,” Alice pays off part of her credit card bill by transferring funds from her checking account. When she returns home, there is a fax waiting for her summarizing her monthly checking and credit card account activity.

- *Mobile person's privacy protection:*

  Third, lack of control over redirection routing and device specificity can result in a user's personal information, such as his current location, to be exposed. We need a system that can provide the mobile person's privacy protection.

  To redirect the information to a mobile person, the system must track the devices and applications through which the person is currently reachable, and should not reveal this tracking information, whether current or historical, because it could be used to deduce the person's location and therefore compromise his privacy. In addition, receiving unwanted messages is also an invasion of privacy.

- *Redirect according to the information's priority:*

  Lastly, some of the voice network services can cut the delivery of a low priority message when a higher priority message arrives. However many applications, such as IP systems, have no way to deliver high priority communications intrusively while delivering low priority communications. So we also need a function to evaluate messages to let users be able to have all their incoming communications prioritised and filtered according to their preferences, then sending information according to the information's priority.

The earliest attempts of solving the "redirection problem" were systems with one address receiving all of a user's messages. The system stores the messages in a centralized location, waiting for the recipient to check them. Several third generation messaging products use this kind of method. For example, Unified Messaging System stores the voice mail, fax mail and E-mail in a unified mail box; the user can then use any telephone, PC or mobile phone to retrieve these messages.

More sophisticated systems were later developed which filter text messages and attempt to prioritize them by looking at the user's recent communication history, calendar, and address book entries.

We will introduce those systems in Chapter 3. However, they are either not effective in deciding where to send a message according to its importance and the available receiving device, or they just provide a partial solution to the problems we mention above.

The fifth generation messaging system we describe, will define an “anytime anywhere” software system that integrates mobile delivery systems like PDA and cell phone.

It filters the incoming information by using the sender’s priority request and recipient’s persona profile, then forwards the information to the available portable and stationary device. It also uses several devices sequentially over time.

Depending on the sender’s request, the system should be able to give information back to the sender about whether the information has been received or read.

Using the identity management function, the system can protect the recipient’s location privacy.

Identity Management is a main function that the fifth generation messaging systems have compared with the early generation messaging systems. It is also this function, which solves our fourth problem - the “persona problem”.

Before examining the “persona problem”, let us look at the “translation problem”.

1.2.3 Translation problem:

Today, many people have adopted a wide range of communication devices for efficient and timely information delivery: telephones, cellular phones, PCs, PDAs, etc. They own multiple devices for communication over diverse networks. Such as: PSTN (Public Switched Telephone Network), the interconnected voice-oriented public telephone networks. GSM (Global System for Mobile communication), a digital mobile telephone system that is widely used in Europe and CDMA (Code-Division Multiple Access), which is popular in North American. *

Most of those sending and receiving devices are capable for only single information transferring service, using a single protocol and information type.

When using a landline phone as a sending and receiving device, we need the PSTN protocol; information type is voice. PCs can send and receive voice by using VoIP (Voice over IP - that is, voice delivered using the Internet Protocol). GSM and CDMA are used as the protocol in the mobile phone voice transferring service. SMS (Short Message Service) is a protocol for sending text messages of up to 160 characters to mobile phones. Etc.

It might be *inconvenient* for non-IT users to find an efficient method from so many integrated products to transfer their information using their specific sending and receiving device.

Figure 2 and Figure 3 show the existing transfer possibility between devices. Here we just use the voice and text as the example of information type, more details will be mentioned in Chapter 2.

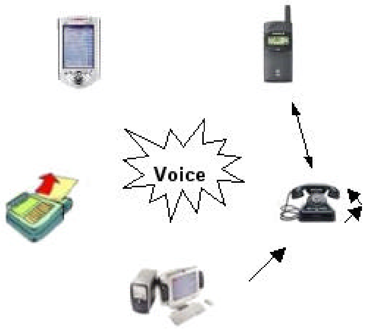

Figure 2: Voice transferred between devices

* Because of the many acronyms in this thesis, we do not explain each of them. Please check the appendix A for the acronyms list for a detailed description.

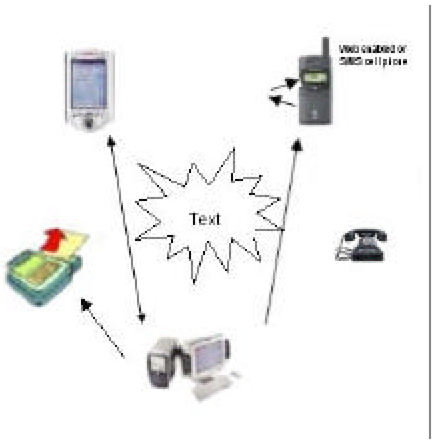

Figure 3: Text transferred between devices

From Figure 2 and Figure 3, we can see that: *Not all the devices can be used to transfer the information direct*ly. Such as there is no possibility to use fax as sending device to send text message to be received by a mobile phone.

The attempts of trying to solve the "translation problem" lead the appearance of second and third generation messaging system where they are discussed as "conversion of messages". [Meer, S. Arbanowski, S. Magedanz, T. 1999]

Some of the third generation messaging integration systems, such as Unified Messaging [UMS 2002] and Canard community messaging [Chesnais, P. R. 1997] [Chesnais, P. R. 1999] provide an information format translation function appropriately chosen from sending and receiving devices. The details of those integration systems will be discussed in Chapter 3.

But almost all the existing integration methods only provide *one-step translation*. By using voice mail, a user could speak out an E-mail, then send it to any E-mail address in the world. But if the recipient's E-mail is not reachable, most people lack a desired service in further retranslation and redirection, such as resending this message to their fax.

Those existing information delivery services only pay attention to the "translation problem" within an IP-based network, not including the translation between the voice network and the IP-based network. When they do consider voice, they treat the voice message as a voice mail, and attach the file to an e-mail message. No existing services to our knowledge provide translation between these two parallel services.

A general translation function is required to converge these two kinds of networks together. The future messaging systems, the fourth and fifth generation systems we will mention in section 1.3, aim to solve this problem.

The fifth generation messaging system we describe in this thesis will provide a full range of message reformatting for different information types and languages between differing networks and devices.

Although we said that the system contains a full range of message reformatting this does not mean it has actual "any to any" traffic type reformatting, as some translations are infeasible, being either too expensive or impossible to achieve with the current technical knowledge. For example, text image can be translated into voice, but the picture images cannot. The translation, which bridges a real time quality of service (QoS) guaranteed network (such as ATM) with a network that has no quality of service guarantee (such as some "best effort" delivery without error control network), will not be considered in this thesis.

We now turn to our fourth problem in message delivery, the "persona problem".

1.2.4 Persona problem:

From the perspective of psychology, people possess many sectors within their personality, and play numerous roles in their life – such as children, parents, students, employees, neighbors, and friends [Suler, J. 2000]. A person may have several personas.

The original meaning of persona is an actor's portrayal of someone in a play [WordNet 2002]. In this thesis we cite it as a portrayal of someone in a "social constellation" – groups of colleagues, friends and family. A persona is a personal facade one presents to one of their "social constellation". It is the role that person is currently acting in, but may vary depending on the respective relationship to the communication partner.

Therefore, a person uses different persona when they are at home, in the office, with friends, going to see a doctor, exercising in a recreation center etc. Sometimes this goes so far that a person use different personal identities such as name, with correspondingly different message receiving devices.

Two kinds of personal needs about the persona's information will be:

Non-interaction between different persona's information

People might not want one of their persona's information to get involved into the other persona. This common requirement is the inspiration for solving the "persona problem".

Below is an example, to illustrate some of the issues involved in the "persona problem".

Alice is a person who has a formal work and a normal family. So she has at least two personas. One is the persona in office, dealing with many colleagues and business. Another is with the family, dealing with her husband and two kids and some of her private information, such as her health information.

The government is trying to protect a person's privacy as a patient persona by passing such laws as the Health Insurance Portability and Accountability Act, which requires health care organizations to protect the confidentiality of patient information. But consider that Alice may give permission to those organizations to send her health related information to her E-mail address or mobile phone. One of her colleagues, who is responsible to help her for a project in the office, may need to check E-mail for Alice, thus he may accidentally get her health problems message from the health center.

Similarly, Alice's work related information, such as the sensitive details of a commercial contract, should be kept confidential from her family numbers, even though they can also check her E-mail.

Self-handling the path for different persona's information

Alice might decide that only the information related with her family persona can reach her whe rever she is. Upon receiving such information our fifth generation messaging system would try to find Alice and redirect the information. She may also decide that information sent to her recreation center persona could be routed to a special in-box.

Despite discussions about the role of the government in protecting privacy, the importance of building choice into IT has emerged as an equally important issue, Franklin S. Reeder, chairman of the Computer System Security and Privacy Advisory Board, which advises the US Congress and Federal agencies, says "As people want more convenience and are willing to accept greater levels of intrusion to get that convenience, we have to be able to let them choose that. At the same time, we need the option to preserve anonymity." [Lais, S. 2001]

The conventional concept of privacy -- of simply making sure information isn't disclosed -- is much too narrow, Reeder says. Privacy is also "about making sure information is properly authenticated. It's about protecting the accuracy of information even though it may be public."

So we need a message delivery system containing an identity management function which can let Alice make the decision of which anonymity level she wants, and who can get involved to the information that bebngs to her work persona, and who can get involved with her family persona information.

Persona is also the criteria for judging the information's priority, so that the system does the redirection according to the priority.

No existing services delivery system considers their users' persona factor. The fifth messaging system we describe here will define an "any-persona" system.

"Persona problem" is a kind of privacy protection. Besides the "persona problem", there are some general security issues in the fifth generation messaging system we also need to discuss. We will do this discussion when we design the Security Control Server in the Chapter 5.

In our system, the user will have many device identities, such as office phone number, office fax number, home phone number, home fax number, E-mail addresses, cell phone number, etc; and personal identities, such as PIN number, password and different certificates. A user's device identity and personal identity can be used to determine their persona. For details please see Chapter 6.

Systems will use those identities to authenticate each user. But by using a more stringent authentication process, the sender or recipient's persona can be authenticated sufficiently and strongly. Some however are not, such as when using fax as a sending or receiving device.

Now we understand that messaging systems originate as a solution to the demand for increased communication between people. Two main kinds of networks appeared from solving the "communication problem", they are the voice networks that we do telephone calls on, and an Internet that we do e-mail data communications on. There are many services provided on these two kinds of networks. Following the increase of services and devices, we currently face the "translation problem" and "redirection problem". In order to protect the user's security, "persona problem" is also an issue.

Following the attempts of people trying to solve those problems, messaging systems developed. In the next section, we will see the five main stages of the messaging system's development.

1.3 Evolution of messaging systems

1.3.1 Past and Present messaging systems

From Sven van der Meer, Stefan Arbanowski, and Dr. Thomas Magedanz's perspective, [Meer, S. Arbanowski, S. Magedanz, T. 1999] traditional messaging systems support the process of incoming, asynchronous messages. This means that the involved users do not communicate directly with each other. The calling party sends information as a message, which will be stored where the addressed party can access this information at any time. Specifically, four major messaging technologies are in parallel use: voice-mail, fax, E-mail, and paging. They also identified four different stages of messaging system (1st 2nd 3rd, and 4th generation messaging system).

First generation of messaging systems

In the first generation messaging systems, all messaging services are processed by special facilities. Users had to use different particular types of devices to check for incoming messages, e.g. an automatic answering machine for voice messages, a fax machine for fax message, and a workstation for reading Emails. [Meer, S. Arbanowski, S. Magedanz, T. 1999]

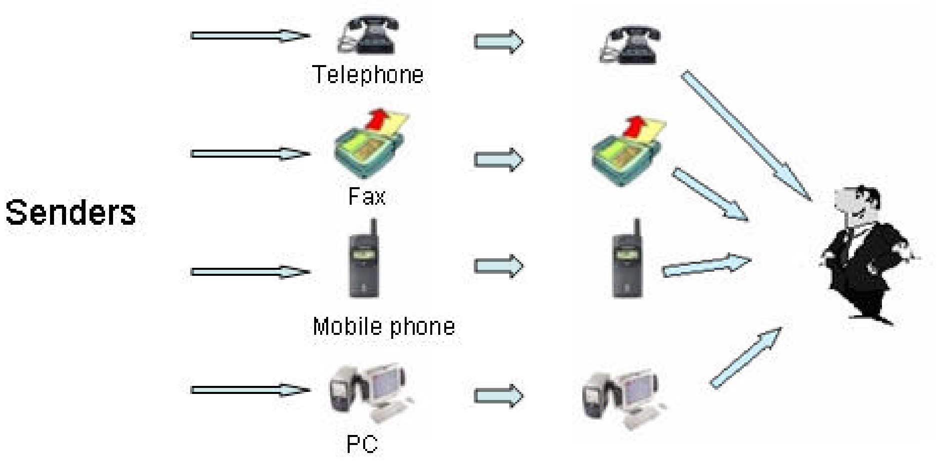

Figure 4: Four kinds of 1st generation messaging systems

In Figure 4, we show four kind of first generation messaging system. They are a telephone system, a fax system, a mobile system and a E-mail system. Each system supports a single traffic type such as voice, image, text etc. The arrow shows the direction of the information flow.

First generation messaging system solved "communication problem" we defined.

Second generation of messaging systems

The second generation messaging system, which is also call integrated messaging, provides access to all messages via a universal inbox.

The basic technology for these systems is E-mail, which is able to integrate all kind of multimedia objects, e.g. MIME attachment. All kinds of messages can be retrieved by E-mail client. [Meer, S. Arbanowski, S. Magedanz, T. 1999]

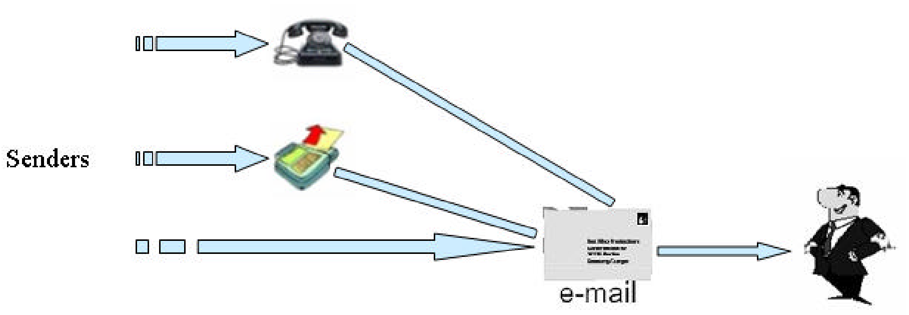

Figure 5: 2nd generation messaging system

Figure 5 gives us the main concept of the second generation messaging system. The arrows in the figure show the information flow, and the line without arrow means the redirection of the information. Here the voice and fax is attached to E-mail.

This second generation messaging systems attempted to satisfy the user's communication need and also part of the "redirection problem" for it redirected the voice mail and fax mail to E-mail.

Third generation of messaging systems

The third generation messaging system use open architecture to incorporate E-mail, fax, and voice mail from most sources, systems, and platforms. [Meer, S. Arbanowski, S. Magedanz, T. 1999]

Following the traffic flow (arrow lines) in the Figure 6, we can see that information from senders are stored at the third generation messaging system. The recipient will access the system to retrieve information.

Access to the centralized stored and managed information resource, is provided for all major communication services, e.g. touch-tone phone, fax polling, or E-mail retrieval (see Figure 6:)

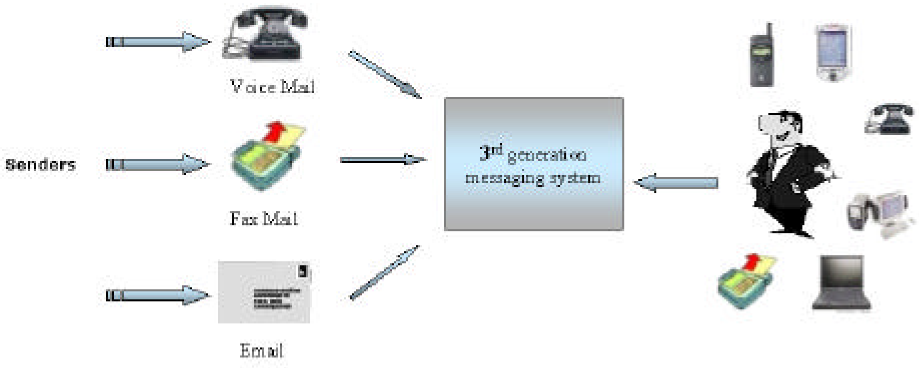

Figure 6: 3rd generation messaging system [Meer, S. Arbanowski, S. Magedanz, T. 1999]

In third generation messaging system, the first solution of "translation problem" appeared. E.g. a text to speech (TTS) function is used to read a fax or an E-mail to users who access to their messages by phone.

Most of the integration messaging systems introduced in Chapter 3 belong to this generation, or are an intermediate step towards the next generation, as they provide a partial solution to the "redirection problem".

The second and third generation messaging system are all considering the services integration of the Internet network, not including the voice. The future messaging system will integrate both of the voice and Internet network.

1.3.2 Future messaging systems

Fourth generation of messaging system

The upcoming fourth generation of messaging systems has to take in account new technologies such as distributed processing, intelligent mobile agents, and location-aware applications. [Meer, S. Arbanowski, S. Magedanz, T. 1999]

The main interest of the users is no longer the ubiquitous access to their messages but the control of their reachability. (See Figure 7:)

In Figure 7, the traffic flow between the recipient and the system is bi-direction, which means that the fouth generation system will actively send the recipient's message to the device they specified, and the recipient can also access the system to retrieve their messages.

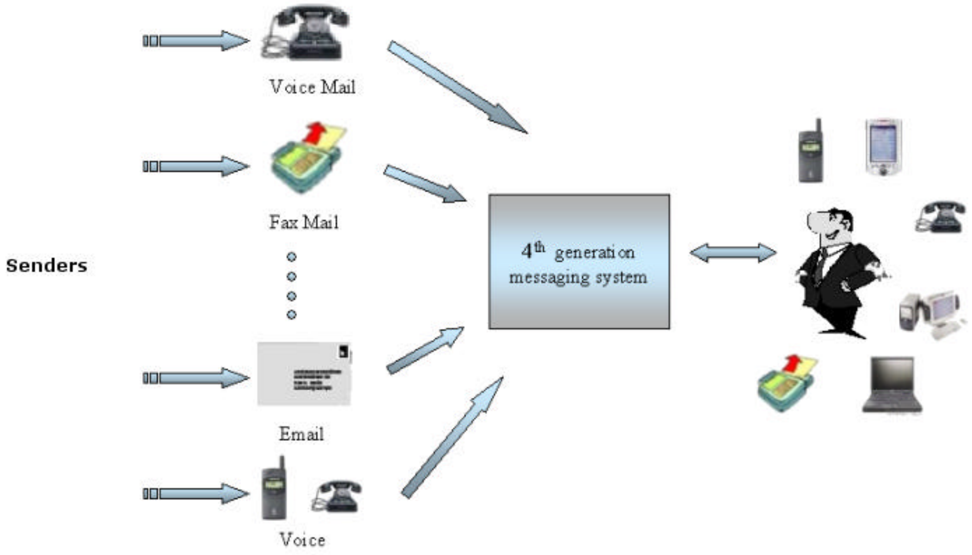

Figure 7: 4th generation messaging system

The fourth generation messaging system purports to completely solve the "translation problem" and part of the "redirection problem" by letting users define where to forward their messages. No *sequential redirection, mobile person's privacy protection*, *redirection according to the information's priority* and "persona problem" was mentioned in this generation.

Fifth generation of messaging system: Our solution to the four problems

Once the major opportunities for using IT to improve industrial and business processes have been exhausted, "the main driver for the adoption of an advanced technology will be the degree to which it satisfies the higher human needs," Nick Jones, a London-based research director at Stamford, Conn.-based Gartner Group Inc, says [Lais, S. 2001].

The "anytime, anywhere, any-persona and from any-device" message delivery system we describe in the later chapter, will correspond with people's needs: transferring information conveniently and secretly.

The fifth generation messaging system will:

- Support multi-services to satisfy the user's communication needs. Solving the "communication problem" we previously defined.

- Provide full information translation, to implement message transferal "from any device".
  This is a solution for the "translation problem" allowing us to support seamless and personalized integration of services across heterogeneous networks.

- Support user definition of when, where, and for whom he is reachable. Also providing negotiation for senders and recipients to decide how to do *Sequential redirection*.

  This solution to the "redirection problem" accomplishes the "anytime anywhere" information delivery.

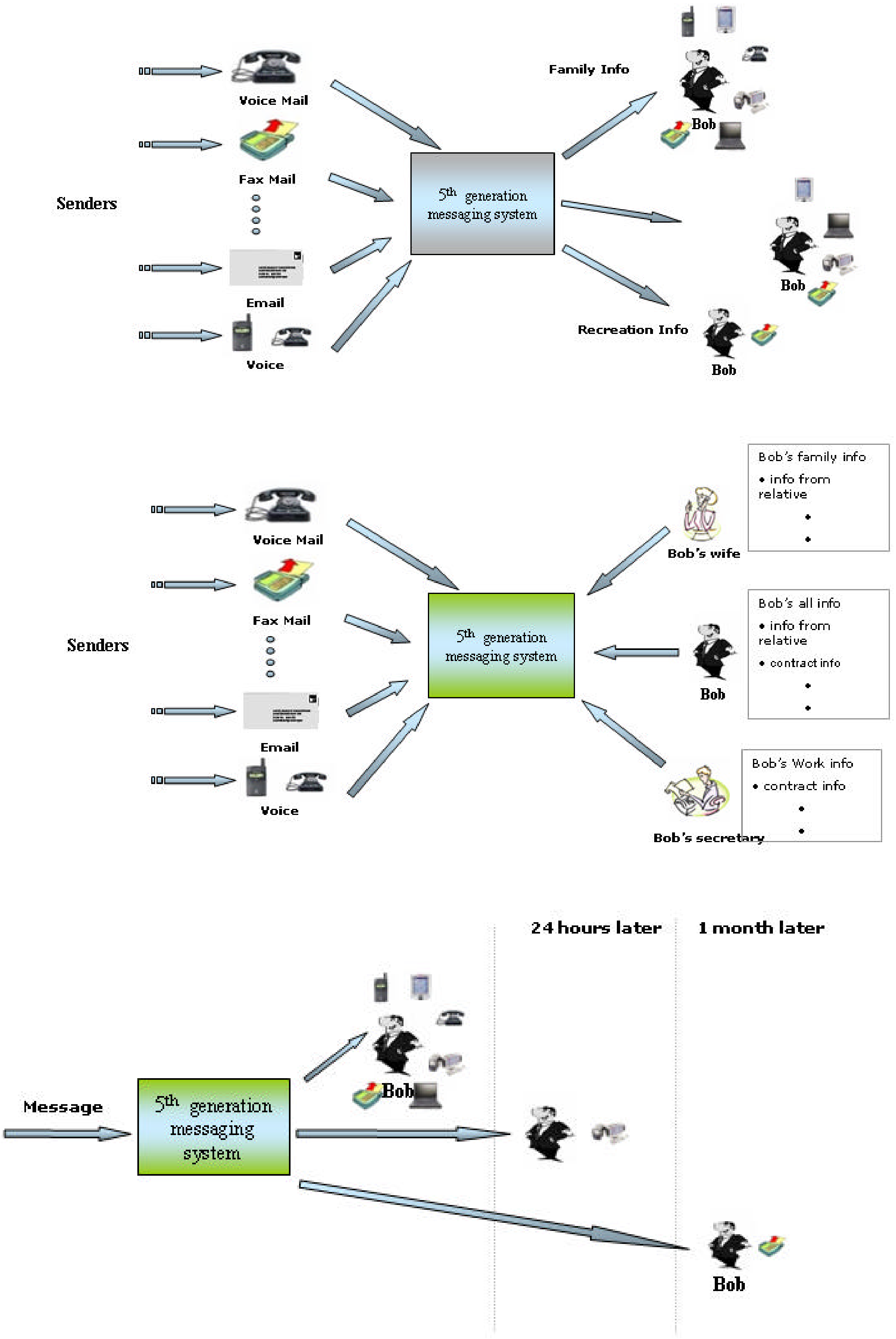

Figure 8: 5th generation messaging system

- Provide security functions and a persona profile, to let the user self-control their use of personas for sending or receiving messages.

We try to use the fifth generation messaging system to converge the voice and IP networks as a solution to the problems and unnecessary costs caused by these two networks not talking to each other.

Leverage both networks to their fullest potential in terms of consumer convenience and security.

As a user of a fifth generation messaging system, they would be able to call anyone even if they only have a recipient's e-mail address, or email anyone if they know the recipient's phone number.

In this thesis, we will consider these four messaging system problems to describe a fifth generation messaging system.

1.4 Summary

In Figure 9, we summarize the relationship between the four problems we described and the different stages of the messaging system:

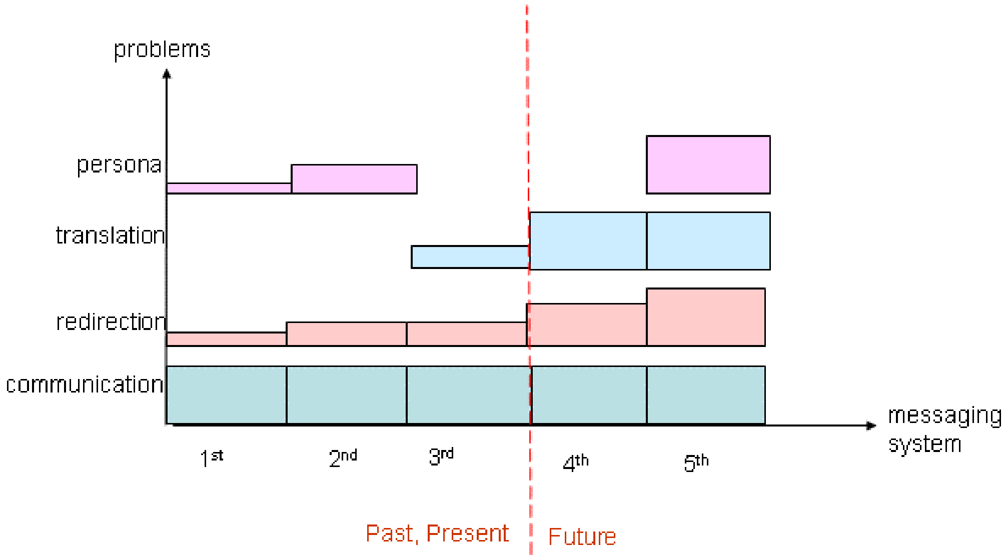

Figure 9: Relationship between problems and stages of messaging system

From the first generation to the fifth generation messaging system, they are trying to solve the user's "communication problem", to satisfy their need of message exchange.

Some services that belong to first generation of messaging have features related to the redirection. Such as the PSTN's call forward feature, which can redirect a call to the other landline phones.

The second and fourth generation messaging systems provide a partial solution to the "redirection problem". The second generation messaging systems only redirect voice mail and fax mail to E-mail. In the fourth generation messaging systems mention is made of the person-to-person reachability, but they do not look at the other issues in the "redirection problem", such as *sequentially redirecting information over time*.

Partial solutions to the "translation problem" appeared in the third generation messaging system, for they only have the text to speech translation. Upcoming fourth and fifth generations will fully solve this problem by providing a general translation function. Here we call it a complete solution just from the technical perspective as we explained before.

Features such as Caller ID in PSTN or GSM, which belong to the first generation systems, help the recipient to refuse messages belonging to one of the recipient's persona, but the decision on whether or not to refuse is up to the recipient, not the system.

In the second generation messaging system, by using several E-mail addresses, recipients can partially solve the "persona problem". The third generation messaging system centrally stores the recipient's messages, and there is no persona concept in the fourth generation messaging system, so we say there is no "persona problem" solution in the third and fourth generation messaging systems.

A full solution to the redirection and persona problems will appear in the fifth generation messaging system.

1.5 Contents of the Thesis

This thesis consists of 7 Chapters:

Chapter 1 contains an introduction intended to help the reader to understand what the problems with messaging systems are, and the different stages of evolution of the messaging systems.

Details of an electronic message, the services that the fifth generation messaging systems will interact with, and the characteristics of those services are described in Chapter 2.

In Chapter 3, we will give a survey of existing approaches designed to solve the four messaging system problems. Chapter 4 describes the feature framework of the messaging system, followed by a high-level structural view of our system in Chapter 5.

Chapter 6 discusses our solution to the "persona problem". The last part, Chapter 7, will include future works and conclusion.

2 Description of the multi-services

As a result of solving the “communication problem” many services such as PSTN and GSM appeared. The integration of these existing and future services is one of the reasons behind the development of this fifth generation messaging system.

In this chapter, we will introduce the electronic information and services, which our fifth generation messaging system will interact with, and present the characteristics of these services.

We first need to understand the meaning behind the word *services*.

2.1 Definition of services:

The term services, is used here to describe all the telecommunication means and facilities provides to users by telecommunication carriers for communication over public and private networks [Bocker, P. 1988]. Examples are telephony, telefax, teletex, etc.

2.2 Communication related characteristics of the services:

2.2.1 Service traffic types

Also referred to as information types in this thesis, can be:

- *Text*: a human-readable sequence of characters and the words they form that can be encoded into computer-readable formats such as ASCII.
- *Image*: a picture that has been created or copied and stored in electronic form
- *Voice*: sound uttered by the mouth, especially that uttered by human beings in speech or song
- *Multimedia*: the combination of text, sound, and/or motion video

Service terminals (sometimes referred to as "sending and receiving devices") and their supported information type is shown in Table 1.

	Text	Voice	Image	Multimedia
PSTN* phone	N	Y	N	N
Mobile phone	Limited	Y	Limited	Limited
PDA*	Y	Limited	Limited	Limited
Fax Machine	N	N	Y	N
PC*	Y	Y	Y	Y

Table 1: Services terminals and their supported information types

"Y" in this table means that the specific device can support the corresponding traffic type. So a PC with the required software (e.g. E-mail client) and hardware (e.g. sound card) installed can, with support connectivity (e.g. Internet), be used to exchange these four types of information (text, voice, image and multimedia).

"Limited," means that with the original design, a specific device cannot support that specific traffic, but with an add-on function, it can. For example mobile phones can currently be used to send and receive text information, but only when the mobile phone has an SMS service enabled on it.

"N" means that a specific device cannot support that specific traffic type.

We will discuss most of the services interacting with the fifth generation messaging system in the later subsection.

* **PSTN:** Public Switched Telephone Network
* **PDA**: Personal Digital Assistant
* **PC:** Personal Computer

2.2.2 Service classes:

Services' technical function and protocol can be classified according to the hierarchical structure of the seven layers of the OSI (Open System Interconnection) reference model. [Bocker, P. 1988]

From the services' operation perspective, we can classify services into the three types listed below.

- *Conversational services*: Allows bi-directional dialog communication between users. It represents a considerable advance in voice communication.

  This synchronous real-time service refers to the need for a bi-directional connection between sender and recipient. This kind of service is always two-way transmission, with no information buffering.

  Buffering means that the information will always reach the user eventually, even if the device is temporarily out of range or switched off. Conversational services, such as two users wanting to talk on the phone, use voice information, which will not be stored anywhere if the recipient does not pick up the phone.

- *Messaging services:* Offers communication between users via the storage units of information. From this kind of asynchronous store-and-forward services, information such as E-mail, fax, or voice message, can be sent to the recipient even he is unavailable by depositing information in his personal electronic mailbox. This kind of service is one-way transmission and the information must be buffered before recipient gets it.

  The information of this kind of services is stored at the recipient's side.

- *Retrieval services:* Allows the user to access information stored in an information center that is generally provided to public users. It is a kind of on-demand service, especially suitable for multimedia information, which is a mixture of text, sound and image. This can be in the form of two-way services such as video conferencing, or one-way like news on demand.

We suggest that this kind of services' information be buffered at the sender side, waiting for the recipient to retrieve it. The reason behind this suggestion is to decrease the traffic load of the system.

This is a kind of "pull" service. The system sends the abstract of the information to the recipient at first, the recipient can then pull that information from where it stored if they really want it.

Relationship between services and traffic type is in Table 2:

Service classes	Traffic (information) type	Example services
Conversational	Voice, text, image	PSTN, GSM, CDMA, Instant Messenger, etc
Messaging	Voice, Text, image	E-mail, voice mail, fax mail, Ftp, SMS, etc
Retrieval	Voice, Text, Image, Multimedia	Video conference, online TV, news on demand, etc

Table 2: Service classes and the type of information they support

2.3 Translation related characteristics of the services

The services we are discussing here belong to the first generation messaging system. Therefore there is no solution to the "translation problem" at this stage, and no translation related characteristics in those services.

2.4 Redirection related characteristics of the services

There is no "redirection problem" solution in those services. But some of the characteristics of the device or service are related to the "redirection problem". They are listed as following.

- *Buffering:* depends on whether the information of that service will be buffered before being sent to the recipient.

  For those services that will buffer the information, it is easy to redirect the information. But for the services that do not buffer the information, like the PSTN voice, we should consider buffering the message before trying to redirect them.

- *In range indication:* depends on the services system getting information about whether the device is in service range before the system tries to deliver a message.

  For example, PSTN phones will not give feedback indicating whether the recipient is reachable at this device. But the mobile phones can send feedback to the GSM or CDMA saying if the device is on or off. Suppose that the recipient always has his mobile phone with him, the system will then know when that recipient is reachable on this device.

- *Arriving indication:* depends on the whether the service can get information about the message's arrival at the recipient's device.

- *Reading indication:* depends on the device's ability to get the information about whether recipient has read the message.

  This indication is useful for our fifth messaging system to handle high priority message delivery. For those messages that must be delivered to the recipient and receive confirmation from the recipient, if there is no reading indication received after delivery to the recipient's device our system will still try to deliver them to other possible devices.

  And this characteristic is also related to the "non-intercepting" system feature we discuss in Chapter 6.

2.5 Persona related characteristics of the services

There is no “persona problem” solution in those services. But some of the characteristics of the device or service are related to the “persona problem”. They are listed as following.

- *Authen ticating:* depends on whether the service provides a stringent authentication process.

  If the service itself does not provide an authentication process, our fifth generation messaging system should have an authentication function to identify the user’s persona.

Now that we have examined the characteristics for the services, we will continue in the next section looking at each service.

2.6 Services that the 5th generation of messaging can interact with

These services are:

Belong to Voice network:

- PSTN
- GSM and CDMA
- SMS
- Fax

Belong to Internet network:

- WAP
- WWW (HTTP)
- E-mail
- Instant Messenger
- PDA

This heterogeneous communication environment has different characteristics, shown in Table 3:

	Communication related		Redirection related				Persona related
	Traffic type	Service Classes	Buffering	In range indication	Arriving indication	Reading indication	Authenticating
PSTN	Voice	Conversational	No	No	Yes	Yes	Limited
GSM	Voice	Conversational	No	Yes	Yes	Yes	Yes
CDMA	Voice	Conversational	No	Yes	Yes	Yes	Yes
SMS	Text	Messaging	Yes	Yes	Yes		Yes
FAX	Image	Messaging	Yes	Yes	Yes	No	Limited
WAP	All	Retrieval	Yes	Yes	Yes	Yes	Yes
WWW	All	Retrieval	Yes	No	No	No	Limited
E-mail	All	Messaging	Yes	Yes	Yes	Yes	Yes
IM	Text voice	Conversational	Limited	Yes	Yes	No	Depends on the program
PDA	Limited	Conversational	Yes	No	Yes	Yes	Limited

Table 3: Characteristics of some communication services

These information services all belong to the first generation of messaging systems; which means that all the information services are processed by special facilities. Users had to use different specific equipment to check for incoming messages, e.g. an automatic answering machine for voice message, a fax machine for fax message, and a PC for reading E-mails.

So there is no solution to the “translation problem” in this section.

Now let us first look at the voice network.

2.6.1 Public Switched Telephone Network:

PSTN (Public Switched Telephone Network) is a worldwide collection of interconnected voice-oriented public telephone networks.

Today, it is almost entirely digital in technology except for the final link from the central (local) telephone office to the user.

In relation to the message delivery, the PSTN actually furnishes much of the Internet's long-distance infrastructure.

Communication related:

Traditional telephone services carried by the PSTN are often called Plain Old Telephone Service (POTS). Using PSTN for voicemail support will be discussed in the E-mail services.

PSTN is a typical *conversational* service, and its "three-way-call" feature can let the information sender setup a conference call between many recipients.

Redirection related:

A customer can use the telephone service's features such as call divert to configure how an incoming call should be handled (forwarding to another phone or voice recorder) on different conditions (line busy, no answer after a period of time or permanent forward). It is sort of *person-to-person* information redirection.

When two messages arrive, the "POTS' call waiting feature can let recipients make the decision on which message to receive. It is a kind of *Delivery according to the information's priority,* but the decision on the priority of the information is based on the user's mind at that moment.

As a conversational service, PSTN will not buffer information so there is no recipient in range indication. The ringing of the phone is the arriving indication, and the recipient pick up the phone indicate that the message be read.

There are no features to help the *Sequentially delivery information over time* and *Mobile person's privacy protection.*

Characteristics		PSTN
Communication related	Traffic type Service Classes	Voice Conversational
Redirection Related	Buffering	No
	In range indication	No
	Arriving indication	Yes
	Reading indication	Yes
Persona Related	Authenticating	Limited

Table 4: Characteristics of the PSTN service

Persona problem related:

Caller ID lets recipients know the likely identity of a sender, and where the information comes from. They can then decide if they would like to receive it or not, solving that part of the “persona problem”.

Toll bars can help to identify or authenticate a sender. But there is no security protection on the actual voice message.

PSTN services have several features related to our communication, redirection, and persona problems. Refer to Table 4 Characteristics of the PSTN service.

2.6.2 Global System for Mobile communication and CDMA

GSM (Global System for Mobile communication) is a digital mobile telephone system that was first introduced in 1991. As of the end of 1997, GSM service was available in more than 100 countries and has become the de facto standard in Europe and Asia.

A competing system, CDMA (Code-Division Multiple Access), is based on a military technology first used during World War II by the English allies to foil German attempts at jamming transmissions. The allies decided to transmit over several frequencies, instead of one, making it difficult for the Germans to pick up the complete signal. Finally, this digital cellular technology uses spread-spectrum techniques, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth.

The CDMA technology is used in ultra-high-frequency (UHF) cellular telephone systems. And is common in the U.S

Communication related:

Here we just talk about using the original concept of GSM or CDMA, which is to use devices in order to receive voice information. Using those mobile phone devices able to receive text message or multimedia message will be mentioned in the SMS and WAP services.

GSM and CDMA here are conversational services, and because of the their basic mechanism, its devices will contact with the nearest Base Station periodically, so it is easy for our system to know whether the device is available.

Redirection and Persona related:

GSM and CDMA's redirection and persona related features are almost the same as PSTN. See Table 5.

They use TMSI (Temporal Mobile Subscriber Identity) to authenticate a legal user after the call setup, so it is possible to have *Mobile person's privacy protection*.

GSM and CDMA have a pretty powerful two-step authentication method. The first step is that the hardware (handset here) uses a PIN (Personal Identity Number) to authenticate the user. The second step is for the GSM system to use IMSI (International Mobile Subscriber Identity) and a Private Key that is stored in the SIM (Subscriber Identity Module) to authenticate a legal user. CDMA system use MIN (Mobile Identification Number) and ESN (Electronic Serial Number) that are stored in the handset to authenticate legal user.

Both GSM and CDMA have algorithms to protect a voice message during its transmission.

Characteristics		GSM	CDMA
Communication related	Traffic type	Voice	Voice
	Service Classes	Conversational	Conversational
Redirection Related	Buffering	No	No
	In range indication	Yes	Yes
	Arriving indication	Yes	Yes
	Reading indication	Yes	Yes
Persona Related	Authenticating	Yes	Yes

Table 5: Characteristics of the GSM and CDMA services

2.6.3 Short Message Service

The SMS, as defined originally within the GSM digital mobile phone standard, has several features:

Communication related:

- SMS is a service for sending messages of up to 160 characters to mobile phones that use GSM communication. GSM and SMS service is primarily available in Europe.

- The Short Message Service is a store and forward service, in other words, SMS messages do not require the mobile phone to be active and within range. Short messages are not sent directly from sender to recipient, but always via an SMS Center instead. Each mobile telephone network that supports SMS has one or more messaging centers to handle and manage the short messages. And message will be held for a number of days until the phone is active and within range.

- Short messages can be sent and received simultaneously with GSM voice, This is possible because whereas voice takes over a dedicated radio channel for the duration of the call, short messages travel over and above the radio channel using the signaling path. Recipients receive messages automatically even if they are currently talking on the phone.

Redirection related:

- The Short Message Service features confirmation of message delivery. Users do not simply send a short message and trust and hope that it gets delivered. Instead the sender of the short message can receive a notification about whether the short message has been delivered or not.

- Ways of sending multiple short messages are available. SMS concatenation (stringing several short messages together) and SMS compression (getting more than 160 characters of information within a single short message) have been defined and incorporated in the GSM SMS standards.

SMS message can also be sent to digital mobile phones from a Web site equipped with PC Link or from one digital mobile phone to another.

Persona problem related:

Authentication on the SMS service is same as GSM and CDMA.

Since its inclusion in the GSM standard, SMS has also been incorporated into many other mobile phone network standards, including Nordic Mobile Telephone (NMT), Code Division Multiple Access (CDMA) and Personal Digital Cellular (PDC) in Japan.

In 1999, the standard: Short Message Service for Spread Spectrum Systems [TIA/EIA 1999] was published. This standard allows the exchange of short messages between a mobile station and the CDMA wireless system; between the wireless system and an external device that the capability of transmitting and optionally receiving short messages. The external device may be a voice telephone, a data terminal or a short message entry system.

Characteristics		SMS
Communication related	Traffic type	Text
	Service Classes	Messaging
Redirection Related	Buffering	Yes
	In range indication	Yes
	Arriving indication	Yes
	Reading indication	?
Persona Related	Authenticating	Yes

Table 6: Characteristics of the SMS service

Each of these standards (GSM, CDMA, NMT, PDC etc) implements SMS in slightly different ways and message lengths do vary. For example CDMA supports SMS services only with a message length of 120 characters.

Lack of translation between SMS on CDMA and SMS on GSM means those two systems cannot exchange message with each other.

A drawback for SMS is that a user who has received a SMS message, can modify it and resend it again, which will cause a security risk: replay attack. Replay attack will be discussed in the Chapter 6.

2.6.4 Fax:

Although fax machines seem to be a somehow antique technology, they are still very popular, especially since many machines combine phone, answering machine, and fax in one desktop device.

Communication related:

Traditional Fax services, sometimes called "telecopying", are very similar to telephony services, the same transmission network and the same logic.

The original document is scanned with a fax machine, which treats the contents (text or images) as a single fixed graphic image, converting it into a bitmap. In this digital form, the information is transmitted as electrical signals through the telephone system. The receiving fax machine reconverts the coded image and prints a paper copy of the document.

The Internet now provides a new and cheaper way to send faxes: Fax over IP (FoIP) rather than using the public telephone system for most or part of the path to the fax point.

Faxes are transmitted from the sender's desktop fax software to the special server. The server routes faxes via an Internet connection to a remote server located in the geographical proximity to the destination fax machine. From this remote server, the fax is sent to its target address using the local telephone system. If the recipient wants only to read the message, they can receive faxes directly to the PC. However, if the document requires editing, it must be converted into text by an OCR (Optical Character Recognition) program, or it must be retyped manually into the computer.

Some services also provide the ability to broadcast a fax to multiple addresses.

Redirection and Persona problem related:

The Fax's redirection and persona related features are almost same as PSTN. See Table 7

Although we know if a fax was sent successfully and has arrived, there is no way to know if the user has read it.

Characteristics		FAX
Communication related	Traffic type	Image
	Service Classes	Messaging
Redirection Related	Buffering	Yes
	In range indication	No
	Arriving indication	Yes
	Reading indication	NO
Persona Related	Authenticating	Limited

Table 7: Characteristics of the FAX service

From next subsection, we will start to introduce Internet network services:

2.6.5 World-Wide Web

A technical definition of the World Wide Web (WWW) is all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP). [TechTarget 2002]

A broader definition comes from the organization that Web inventor Tim Berners-Lee helped found, the World Wide Web Consortium (W3C). [W3C]

> *"The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge."*

Communication related:

Text, Image, Voice and multimedia information can all be transferred on the WWW.

The web is an Internet client-server hypertext distributed information *retrieval* system, which originated from the **CERN** High-Energy Physics laboratories in Geneva, Switzerland.

On the WWW everything is represented to the user as a hypertext object in HTML format. Hypertext links refer to other documents by their URLs (Uniform Resource Locator) These can refer to local or remote resources accessible via FTP, Gopher, Telnet or news, as well as those available via the http protocol used to transfer hypertext documents.

The client program (known as a browser) runs on the user's computer and provides two basic navigation operations: to follow a link or to send a query to a server.

Redirection related:

The web system will not know the client is connected and ready to receive messages unless the client sends a request. That is why we say there is no "In range" indication on WWW service.

And after the web server sends out the message, even if the client receives it, there is no “arriving” and “reading” indication feedback to web server.

Persona problem related:

WWW service will not ask users to authenticate themselves, unless some application requires it. So the authenticating characteristic of the WWW is dependant on the application.

Characteristics		WWW
Communication related	Traffic type	All
	Service Classes	Retrieval
Redirection Related	Buffering	Yes
	In range indication	No
	Arriving indication	No
	Reading indication	No
Persona Related	Authenticating	Limited

Table 8: Characteristics of the WWW service

2.6.6 Wireless Application Protocol

The idea of WAP comes from the wireless industry, from companies such as Phone.com, Nokia and Ericsson. The point of this standard is to serve Internet contents and Internet services to wireless clients.

Communication related:

WAP is not a single entity, but a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access. This includes e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC). IRC allows the users to download the client applet with homepage from their web server for chatting. [TechTarget]

Wireless devices act as a simple web browser, which are called microbrowsers – browsers with small file sizes that can accommodate the low memory constraints of handheld devices, and the low bandwidth constraints of a wireless-handheld network.

WAP optimizes the markup language, scripting language, and the transmission protocols for wireless use. WML (Wireless Markup Language), language (an XML application) is specifically devised for small screens and one-hand navigation without a keyboard. WMLScript is similar to JavaScript, but as it makes minimal demands on memory and CPU power usage it does not contain many of the unnecessary functions found in other scripting languages.

The optimized protocols are translated to plain old HTTP by a WAP gateway.

Messages to be retrieved can be cached in the WAP gateway.

Redirection related:

WAP is based on wireless devices, so its redirection related characteristics are the same as GSM and CDMA. See Table 9.

Characteristics		WAP
Communication related	Traffic type	All
	Service Classes	Retrieval
Redirection Related	Buffering	Yes
	In range indication	Yes
	Arriving indication	Yes
	Reading indication	Yes
Persona Related	Authenticating	Yes

Table 9: Characteristics of the WAP service

Persona related:

The Wireless Application Protocol is a secure specification, has a powerful authentication method and the message can be encrypted during the transmission.

WAP supports most wireless networks. These include CDPD, CDMA, GSM, PDC, etc.

WAP user can be authenticated using the traditional wireless network authentication plus the X.509 mini-certification.

2.6.7 Electronic mail

E-mail (electronic mail) is the exchange of computer-stored messages through telecommunication. It was one of the first services used on the Internet and is still the most popular. A large percentage of the total traffic over the Internet is due to E-mail.

Communication related:

E-mail messages were usually encoded in ASCII text before MIME (Multipurpose Internet Mail Extensions) was created. User can send non-text files, such as graphic images (Fax mail) and sound files (voicemail), as attachments sent in binary streams. MIME's purpose was to facilitate the inclusion of 8-bit word-oriented data into a transport mechanism that is only capable of transporting 7-bit ASCII characters [RFC 1521, 1522]. Therefore multimedia content can be transferred in E-mail.

E-mail can be distributed to lists of people as well as to individuals.

Some mailing lists allow you to subscribe by sending a request to the mailing list administrator.

E-mail is a *messaging* service. A popular protocol for sending E-mail is Simple Mail Transfer Protocol (SMTP) [RFC 821] and a popular protocol for receiving it is Post Office Protocol (POP). [RFC 1939]

When a user sends an E-mail message, his MUA (Mail User Agents), which is a mail client, first establishes a connection with default mail server or MTA (Mail Transfer Agent) and sends a sequence of commands to it. Once the MTA has received a message, it then acts on it based on the destination address or addresses within the message. If a destination address is local to the MTA, the MTA will store the message and wait for an MUA to retrieve it. If a destination address is not local to the MTA, the MTA will either forward the mail message to the destination MTA if it is known, or relay it to another MTA server that may be closer to the final destination. When the mail message finally arrives at the destination MTA, the message is again stored until the MUA of the destination host retrieves it.

Characteristics		E-mail
Communication related	Traffic type	All
	Service Classes	Messaging
Redirection Related	Buffering	Yes
	In range indication	Yes
	Arriving indication	Yes
	Reading indication	Yes
Persona Related	Authenticating	Yes

Table 10: Characteristics of the E-mail service

Redirection problem related:

E-mail has the ability to forward information, which means to redirect messages to other recipients. It is different to the *person-to-person* information redirection we defined in Chapter 1.

A lot of mail clients have provided the sender with the ability to change the priority for the message. It can then be *delivered according to the information's priority*.

There are no features to help the *Sequential delivery of information over time* and *Mobile person's privacy protection*.

A drawback for E-mail is that a user who has received an E-mail message, can modify it and resend it again, which will cause a security risk: replay attack. Replay attack will be discussed in the Chapter 6.

Persona problem related:

An E-mail user can manage his persona by using different E-mail addresses for different persona.

E-mail message can be encrypted using PGP and add digital signatures for authentication.

2.6.8 Instant Messaging

Instant messaging sometimes called IM or IMing, is the ability to easily see whether a chosen friend or co-worker is connected to the Internet and, if they are, to exchange messages with them.

Communication related:

Instant messaging differs from ordinary E-mail in the immediacy of the message exchange, and also a continued exchange is simpler than sending E-mail back and forth. Most exchanges are text-only. However, some services allow attachments.

Instant messaging differs from the Internet Relay Chat (IRC) that belongs to WWW. IRC uses an ordinary browser, but using Iming requests both parties must have downloaded the program. For example, ICQ (“I Seek You”) [ICQ] and AIM® (AOL's Instant Messenger), [AOL 2002] etc.

AOL (America Online) first popularized instant messaging. AOL's Instant Messenger can only be used by AOL members, but here is no requirement to be connected to the Internet through AOL [AOL 2002]

A person might receive an IM from someone while already engaged in a chat with someone else, and decide to carry on IM chats with both people independently and concurrently, or chat with both of them at the same room, like a conference.

Redirection related:

Buffering depends on the IM application. Some of them such as ICQ will buffer the chat record for users, whereas others do not use buffering

In order for IMing to work, both users must be online at the same time, and the intended recipient must be willing to accept instant messages. It is possible to set your software to reject messages. It can alert the recipient to new messages with a distinctive sound, a window indicates that an IM has arrived and allows the recipient to accept or reject it.

Persona related:

Authenticating in IM is depends on the program.

Characteristics		IM
Communication related	Traffic type Service Classes	Text, voice on IP Conversational
Redirection Related	Buffering	Limited
	In range indication	Yes
	Arriving indication	Yes
	Reading indication	No
Persona Related	Authenticating	Depends on the program

Table 11: Characteristics of the Instant Messaging service

2.6.9 Personal Digital Assistant

PDA (Personal Digital Assistant) is a term for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy. [PDA].

Because of that not all readers use PDA very often, we will explain the concept in more detail:

In 1993, Apple Computers vowed to reinvent portable computing. The company promised an "all-being, all-knowing, all-doing" electronic device. It would serve as an address book, Day planner, Notepad, Fax machine, Pager. All electronic, easy to use, fits in the palm of a human hand. The name for this miracle machine is Personal Digital Assistant.

Finally, at MacWorld, Apple released the first PDA, the Newton. Its specifications were impressive. LCD touch screen. Pen input. Handwriting recognition. Suite of productivity applications. Wide hardware expandability options. Open architecture for add-on software. Bundled neatly into a one pound, sleek, black casing.

But many people complained about its inaccurate handwriting recognition, fragile hardware components, excessive weight and uncomfortable ergonomics.

Then other companies attempted to take advantage of Apple's failure. Each one of them released their own version of the perfect PDA

The styles of PDA in the market now can be classified as:

Simple PDA: are just electronic organizers. They simply assist in organizing users' lives, leaving handling bloated spreadsheets, databases, or text documents to a desktop computer or laptop.

Their main function is to make information highly accessible to users. Hardware should be small, fast, and cheap.

They can handle third-party software and hardware. But, these add-ons should not be complex. U.S. Robotics Pilot is an example of this kind of PDA.

Complex PDA: can function as a standard PC computer.

This is the ultimate purpose of PDAs - to replace notebook computers. The IBM PC110 is this kind of PDA.

Middle PDA: have the potential to be used for any and all purposes.

The majority of PDAs in the current market are middle PDAs. It is the one that between simple and complex PDA.

Communication related:

The input method of information to a PDA is either by using a small keyboard or an electronically sensitive pad on which handwriting can be received.

Most of the connectivity for PDA to perform local information exchange is in a resting cradle. Users place the PDA into this cradle that is connected to the host computer. Then, with a touch of a single button, all the information between the PDA and the host is synchronized and updated. As well as facilitating connection to the desktop device, many cradles also provide a source of power, recharging the PDA's battery whilst the device is docked. However, two wireless technologies – the one with us now being the "Infrared Data Association (IrDA)", and the other, known as **"**Bluetooth"**,** due to become available in the near future, are likely to play an increasing role in the synchronization tasks of PDA's in the future.

Connectivity for PDA's to perform data transfer through the Internet is a PDA with a suite of Internet software and a built-in modem. Some of Internet PDA are running on a Java-based operating system. This allows users to connect to the Internet and work with downloaded Java applications.

With wireless modems, PDAs can provide users with more portable connectivity than a cellular phone (WAP) ever could. However, there are vast problems with merging the Internet and PDAs. These include formatting HTML to comfortably fit pages into small, low resolution displays. Contents and navigation would also need to be condensed because of screen size and speed limitations. In addition, wireless technology needs to be made faster, cheaper, and more secure before it gains mainstream acceptance.

Characteristics		PDA
Communication related	Traffic type	Limited
	Service Classes	Messaging
Redirection Related	Buffering	Yes
	In range indication	No
	Arriving indication	Yes
	Reading indication	Yes
Persona Related	Authenticating	Limited

Table 12: Characteristics of the PDA service

PDA's hot synchronization is the text messaging service. The information can be buffed in the PDA.

Redirection related:

Messages can be buffered in PDA. There is no signal to indicate to the system that the PDA is in range of service until the message start been transferred.

Hot synchronisation function in PDA allows the system to know that the message has arrived to the recipient and been read (updated).

Persona related:

PDA uses a password to authenticate the user; however, this is typically not the powerful authentication. The security of the message depends on the application.

3 A survey of existing integration approach

In this section, we will discuss six existing electronic information delivery integration technologies, which attempt to solve the communication, redirection, translation and persona problems we mentioned above.

These six integration messaging system are either notable, such as *UMS* (Unified Messaging System) and *MPA* (Mobile People Architecture), or a commercial proprietary system representing the different trends of the messaging system market, such as iPulse™ that is directed more toward service providers. Some of them focus on solving one particular problem, for example, *Canard* focuses on the "translation problem" we defined, but *Active Messenger* focuses on the "redirection problem". Amongst them are the earliest integration messaging systems, which I found, such as Phoneshell which was developed in 1993. However, none of these systems solve the problems completely and efficiently.

We will describe each of the messaging systems by focusing on their solutions to these four problems.

3.1 Unified messaging:

Unified Messaging (sometimes referred to as the *Unified Messaging System* or *UMS*) is the handling of voice, fax, and regular text messages as objects in a single mailbox that a user can access either with a regular e-mail client or by telephone .

3.1.1 Communication problem issues:

Information types:

- E-mail
- Voice mail
- Fax mail

Services integrated:

- PSTN (only employed for voicemail support)
- FAX

- VoIP
- E-mail

All of the services are messaging services.

3.1.2 Unified messaging features:

We will use “Remark! Unified MessagingAssistant®” (see Figure 10) [Bigskytech 2002] as an example to examine the Unified Messaging System’s features:

- Single Message Store: Regardless of the type of the information, all messages are stored in one unified message box and can be retrieved using communication media.
- Multiple access methods: Computer desktop, telephone, mobile phone and other mobile devices (Palm, Windows CE and WAP Enabled PDA) can all be used to access the message box to retrieve information.

  The computer desktop user can view e-mail and fax messages, can open and play back voice messages, assuming that their computer hardware/software has multimedia capabilities. All e-mail tools (reply, forward, etc.) are available for processing messages.

  Telephone or mobile phone users can listen to voice messages and/or listen to e-mail messages. In this case, ordinary email notes in text are converted into audio files and played back. All normal voice mail tools (reply, forward, etc.) are available to process messages

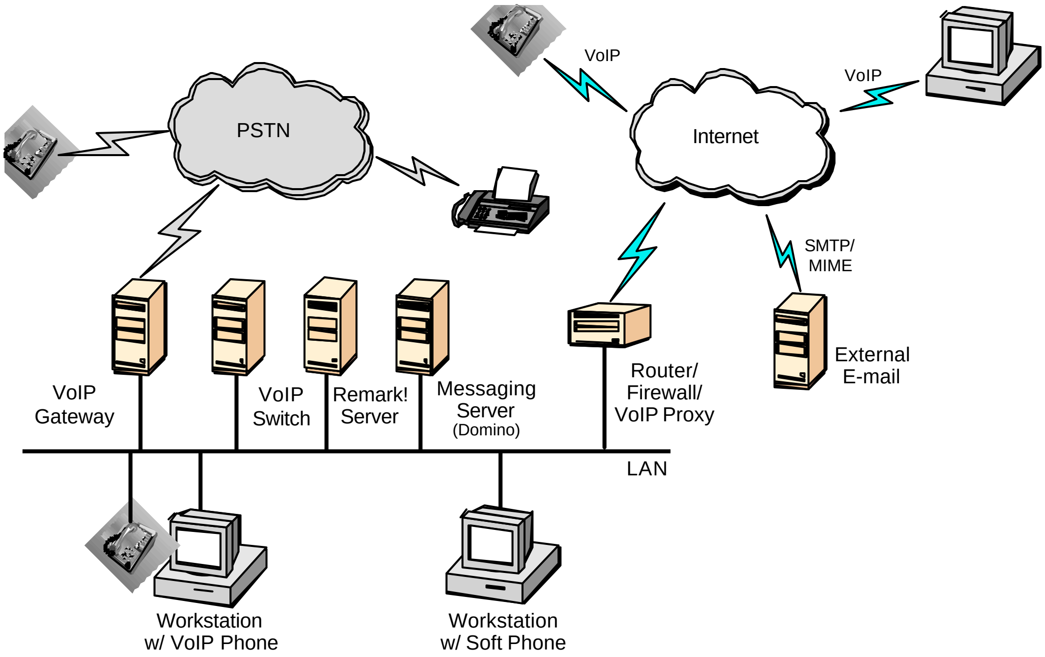

Figure 10: Unified Messaging Diagram [Bigskytech 2002]

In Table 13, we describe the features of several UMS products, using the acronyms defined in Table 14.

Those products come from the first two pages after using the "google" search engine, with the keywords – "unified messaging product": [UMS 2000]

Product	Vendor	Operation system	Functions
PhoneSoft®	Active Voice	NT, Netware	MAPI, TAPI, TTS, Web access
WIN Series®	Digital Speech System	NT	TAPI, PBX feature
Unified Messenger®	Lucent, Octel messaging	Unix	VPIM, TTS, Web access
CallPilot®	Nortel	Unix	Only for Meridian ™ PBX
CommWorks 8250®	CommWorks Corporation	Unix	VPIM, TTS, Web access

Table 13: Function comparison of five UMS products

Acronyms	Explanations
MAPI (Messaging Application Program Interface)	A Microsoft Windows program interface that enables you to send e-mail from within a Windows application and attach the document you are working on to the e-mail note
TAPI (Telephony Application Program Interface)	A standard program interface developed and promoted by Microsoft that lets a user and their computer "talk" over telephones or videophones to people or phone-connected resources elsewhere in the world. Allows the user to dial from the personal information manager (PIM) for Windows or any desktop application; See who they are talking to individually or at a conference call; Add a voice note to an e-mail note they send; Listen to a voice note attached to an e-mail note they received; Program their computer to automatically receive phone calls from certain numbers (but not from others); etc.
VPIM (Voice Profile for Internet Mail)	Allows inter exchange of Voice and fax messages between Voice messaging systems over IP networks. This standard is intended to facilitate server-to-server message exchange, especially between voice message systems from different vendors, and will make it possible deliver store-and-forward messages at low cost.
TTS (Text-to-Speech)	A type of speech synthesis application that is used to create a spoken sound version of the text in a computer document. Allows user to access E-mail (sometimes also fax) via the phone
Web Access	Show that user can access their messages via a standard browser.
PBX Feature	PBX extensions, such as Phone message waiting lights control, Connects to loop start trunks, DID (Direct Inward Dialling)

Table 14: Definition of acronyms

3.1.3 Translation problem issues:

Media conversion is an integral component of Unified Messaging Systems, as it provides “multiple access”. For example, messages sent as faxes can often be accessed and received as E-mails, or vice versa. E-mails can be read to users who access them from telephones using TTS technology.

We say Unified Messaging Systems provides a partial solution to the “translation problem”, because UMS have not integrated the conversational and retrieval services. There is no analog voice message translation to a Fax image, or SMS text format. It is not a “full translation” in which a system will integrate all three kinds of services.

Many of the UMS solutions do NOT include the inclusion of SMS messages as a type of information WITHIN the unified mailbox itself. SMS is used only for message arriving notifications and alerts.

3.1.4 Redirection problem issues:

Unified messaging provides a single inbox, accessed via different devices; central stored the user’s information. Basically, it cannot actively redirect the information to follow the recipient.

But now some of UMS products, such as Active Voice’s PhoneSoft® provide “follow me” capability, allowing recipients to receive a short message notifying them that they have a new message in their unified messaging box. The short message often also includes an indication of the type of new message that has been deposited, such as fax, E-mail or voice mail. This notification message can be send to the recipient according to his predefined set of devices where he might be reachable according to the time of day. Then recipient accesses his information box to get the information.

It actually is a message arrival alerting function, not the real message redirection we mentioned in Chapter 1. So we could not say that Unified Messaging System has a solution of “Redirection Problem”

3.1.5 Persona problem issues:

The unified messaging system assigns users a single phone number and an E-mail address that allows them to send and receive phone calls, faxes, voice-mail and E-mail services through the web. So that one user can only have one persona.

In Table 15, we summarize the UMS's on the four problems in message delivery"

Problem		Solution Quality
Communication (Services integrated)		E-mail, voice mail, fax mail
Translation		Partial
Redirection	Person to person reach ability	None
	Sequentially redirecting	None
	Mobile person's privacy protection	None
	Redirect according to the information's priority	None
Persona		Only one persona

Table 15: Analysis of four problems in Unified Messaging System

Unified messaging have partially implemented the "anytime anywhere" multi-services, but limits the user's persona, and redirection of information.

From the simplest unified messaging product to till now, Unified messaging covered the second and third generation messaging system stages. It is developing towards to the fourth generation.

3.2 Phoneshell:

Phoneshell is a telephone-based system providing remote voice access to personal desktop databases such as voice mail, e-mail, calendar and rolodex. [Schmandt, C. 1993]

It was developed at the MIT Media Lab in 1993.

3.2.1 Information types and services integration:

Phoneshell is used to prioritise E-mail messages. It attempts to identify “timely” messages by analysing the information found on a user's desktop computer and the message transaction history, but can also handle voice messages based on caller identification, as well as fax messages based on the fax header information.

3.2.2 Phoneshell features:

A Phoneshell user can hear new or older messages; record messages for other voice mail subscribers, or change the voice mail greeting.

E-mail applications inside Phoneshell will sort the mail, present it with text-to-speech synthesis, deliver the higher priority messages first, and generate voice replies.

E-mail sorting is based on the filtering and prioritization system, known as CLUES and developed by Matt Marx at the Media Lab [Marx, M. 1996]

Calendar applications under Phoneshell allow users to review and add entries to their personal calendars.

CLUES

CLUES uses the users' personal information on their desktop computers to prioritize messages for mobile access. By relying on information sources, such as a calendar or mail log that change along with the user's plans and activities, CLUES creates dynamic filters in order to identify timely messages.

Unlike most mail filtering systems, CLUES contrasts short-term, timely information from long-term information that reflects stable user interests or social relationships. CLUES divides the work of filtering, using both dynamic filters to capture short-term interests and a small number of user-authored rules to capture long-term interests, which are not dependent on time or place.

Information is first extracted from temporally organized data sources. Calendar entries are indexed by date and time, and a user-defined window of interest determines the granularity used in the analysis. Users often maintain to-do lists, and CLUES assumes that such lists are, by nature, up-to-date and therefore relevant. Sent-mail logs supply the names of frequent correspondents and subjects of interest, and thus are relevant as well, within a user-defined window of interest. Computer telephony applications supply data on outgoing calls, which may be associated with e-mail addresses via the address book.

3.2.3 Solutions to messaging system problems:

We classify Phoneshell as a third generation messaging system. It provides a partial solution to the "translation problem", for it can transfer text into voice. No "redirection problem" and "persona problem" solution exists in this integration system.

Problem		Solution Quality
Communication (Services integrated)		E-mail, voice mail, fax mail
Translation		Partial
Redirection	Person to person reach ability	None
	Sequentially redirecting	None
	Mobile person's privacy protection	None
	Redirect according to the information's priority	None
Persona		Only one persona

Table 16: Analysis of four problems in Phoneshell

User studies have shown [Marx, M. 1996] that Phoneshell, which is based on CLUES, is especially useful for subscribers with high message traffic who often access their messages from mobile devices or via the phone. Nevertheless, the user still has to decide what to do (delete or achieve) with a message of a certain category. Active Messenger makes this process automatic on behalf of the user by modifying the filtering rules according to the importance of the message.

3.3 Active Messenger

3.3.1 Information types and services integration:

The main service handled by Active Messenger is E-mail, with the information type as text.

3.3.2 Active Messenger features:

Active Messenger (AM) is a server-based agent process that monitors a user's incoming e-mail messages, prioritizes them using CLUES (described earlier), and forwards them to the available communication channels, e.g., pagers, fax machines, and phones. [Marti, S. 1999]

When a message arrives in the user’s inbox, Active Messenger decides if the message is important by looking at the user's recent communication history, user-specified rules, and other resources. Depending on the importance of the message and the inferred location of the user, the Active Messenger decides where to send the message.

The basic forwarding rules are specified in a user preference file, but can be modified by the agent to adjust to the user's current situation.

The Active Messenger is an agent that is capable of taking several steps over time to guarantee the delivery of a message, trying multiple channels and awaiting possible user reactions. It infers the location of the user by looking at her communication history and communication behaviour. For example, if a reply comes back shortly after a message is sent to a two-way capable device, the Active Messenger assumes that the user has read the message. If the primary communication device used provides no back-channel information, the Active Messenger tries to infer whether the message has been read by monitoring other channels shortly thereafter.

After having sent a message to the first channel, it checks the status of each message and channel, and waits for possible user reactions. If the user has not read the message after a certain time, the agent sends it to the next appropriate channel that is available, and so forth. An example is shown in Figure 11.

Depending on the user-defined status of a sender, Active Messenger may also give feedback to the sender of a message about the location and communication behaviour of the user.

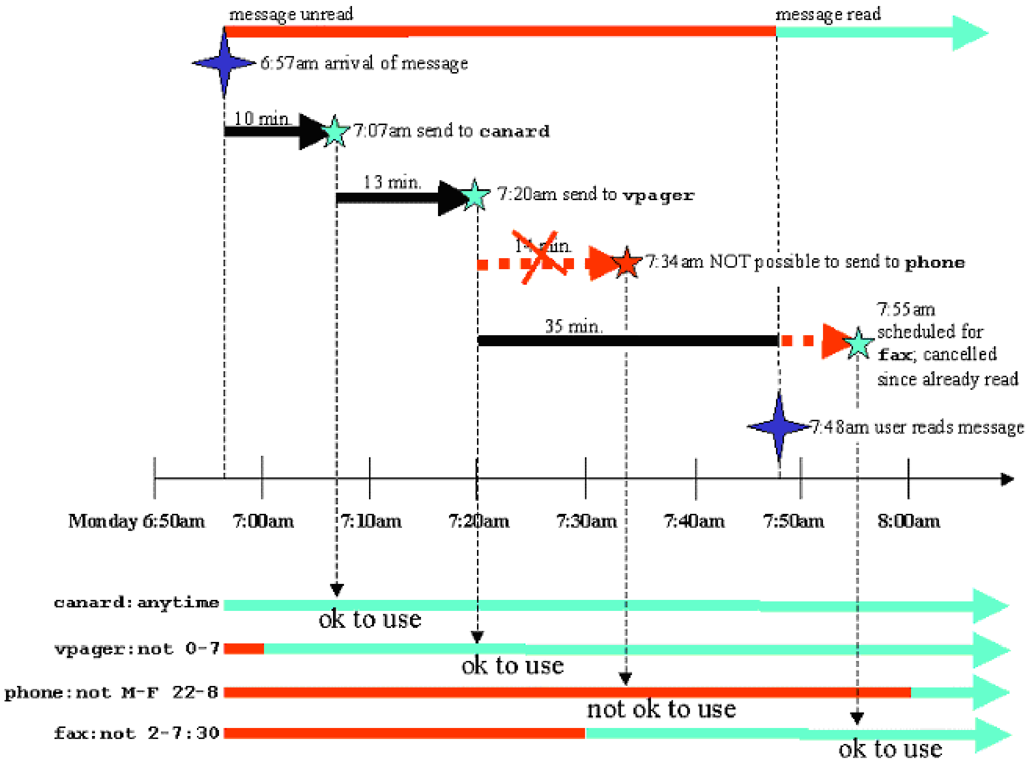

Figure 11: AM message redirection [Marti, S. 1999]

3.3.3 Solutions to messaging system problems:

Active Messenger belongs to the third and fourth generation messaging system. It does translation from text to voice or image, but no translation from voice to text, etc; we say it provides partial translation.

Active Messenger has a very powerful solution to the “redirection problem”, but offer no protection to the recipient’s location privacy.

Active messenger does not mention the “persona problem” we defined previously.

Problem Communication (Services integrated)		Solution Quality E-mail
Translation		Partial
Redirection	Person to person reach ability Sequentially redirecting	Yes Yes
	Mobile person's privacy protection	None
	Redirect according to the information’s priority	Yes
Persona		Only one persona

Table 17: Analysis of four problems in Active Messenger

3.4 Canard community messaging

3.4.1 Information types and services integration:

Canard [Chesnais, P. R. 1997] [Chesnais, P. R. 1999] is a Media Lab project that uses two-way pagers, a touch-tone based telephone interface with synthesized speech, a WWW interface, and electronic whiteboards.

3.4.2 Canard features:

These communications devices and protocols are converted into a uniform message representation. Using personal databases, the relevancy of a message is evaluated and appropriate delivery channels selected (see Figure 12).

The Canard messaging model is a three-layered approach: representation, evaluation, and transport. First, source material is analyzed and converted into a uniform representation. Next, at the evaluation layer, one or more programs can be used to analyze the message using personal databases to evaluate its importance, and ultimately, its delivery mechanism. Finally, at the transport layer, a message is transcoded for delivery on a particular channel - stripping the message of unusable material (i.e., stripping video data to a text only device and instead sending a textual description, if available, of the footage).

The user only needs to know the person she is communicating with, and not the method of transport. By using filters similar to Procmail, Canard selects the most economic channel for the message as a function of the sender/recipient relationship and message urgency.

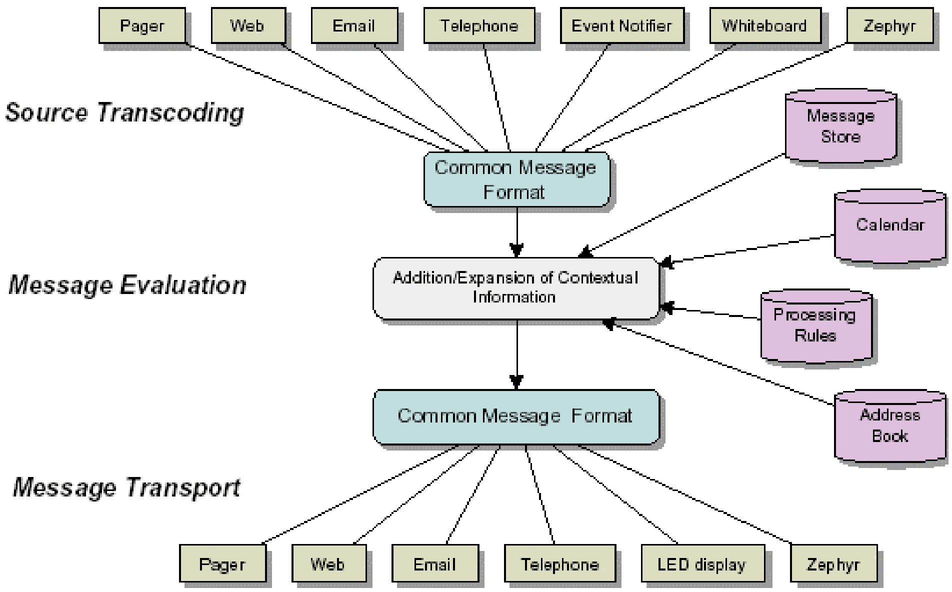

Figure 12: Canard message translation [Chesnais, P. R. 1997]

3.4.3 Solutions to messaging system problems:

Canard belongs to the fourth generation messaging system. It has the most powerful solution to the "translation problem" among the approaches described. Within it's scalability, we might say that it can provide full translation for the heterogeneous communication environment.

Canard attempts to solve the problem of differing communication channels, it provides the person-to-person level redirection but does not have the ability to using several devices sequentially over time, and the ability to protect recipient's location privacy.

No solution to the "persona problem" was mentioned in the Canard

Problem		Solution Quality
Communication (Services integrated)		All
Translation		Full
Redirection	Person to person reach ability	Yes
	Sequentially redirecting	None
	Mobile person's privacy protection	None
	Redirect according to the information's priority	Yes
Persona		Only one persona

Table 18: Analysis of four problems in Canard

3.5 iPulse™ by Ericsson and Oz.com™

iPulse™ by Ericsson and Oz.com™. [OZ] is another system that mediates between two subscribers by finding a way to get a text message or audio stream through, according to the preferences of the recipient.

3.5.1 Information types and services integration:

The voice and text information types are used by iPulse™. The services are voice mail, VoIP, instant messaging, and WWW.

3.5.2 iPulse™ features:

The manufacturer claims that iPulse™ can instantly and easily connect users to each other by computer, phone, pager or mobile phone through a simple point-and-click contact menu (see Figure 13: iPulse™ screen shot). Pushing the *Contact Menu* button triggers pop up menus to let user select contact recipient with Page, Voice Chat, Text Conference, Web Conference and Dial Pad (default communication items).

It also allows users to customize their communications by setting up individual profiles that indicate when, by whom and how they want to be reached. It is supposed to alleviate the contacting person from the burden of finding the right channel. It supports paging, voice chat, text chat, web conference (text chat with the control of a common web browser), and IP telephony. The user also can keep a contact list and set her online status very similar to the Instant Messaging product.

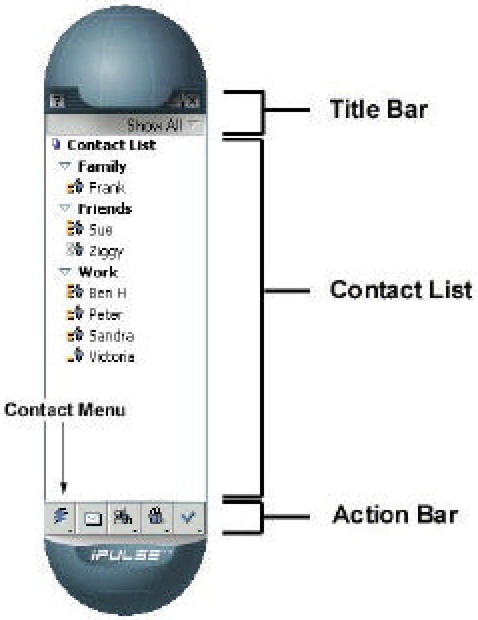

Figure 13: iPulse™ screen shot[OZ]

The iPulse™ framework consists of a client application and a back-end server system. The main function of the framework is to provide users with a simple and secure way of establishing communication sessions with other users or services, running either on IP or other networks like PSTN. Basically, iPulse™ acts as a mediator. It mediates communication services between two or more people and regulates access to value added services.

3.5.3 Solutions to messaging system problems:

Problem		Solution Quality
Communication (Services integrated)		Voice mail, VoIP, instant messaging, WWW
Translation		Partial
Redirection	Person to person reach ability	None
	Sequentially redirecting	None
	Mobile person's privacy protection	None
	Redirect according to the information's priority	Yes
Persona		Only one persona

Table 19: Analysis of four problems in iPulse™

iPulse™ is a kind of the third generation messaging system, but contains some fourth generation messaging system features. It does one-step translation during the message delivery. It uses "categories" to let users organize their contacts. The categories can be: *VIP*, *Regular*, and *Blocked*, according to how users want their contacts to reach them.

Users can use the "Configure My Reachability" window to define how they want each contact category to reach them.

Although iPulse™ can use the 'Status button" to show the user's online status as At Home, At Work, and Busy, it does not have a "persona" concept.

3.6 The Mobile People Architecture

The *Mobile People Architecture* (MPA) [Appenzeller, G., Lai, K., Maniatis, P., Roussopoulos, M., Swierk, E., Zhao, X., Baker, M. 1999] is an advanced and promising framework for connecting people instead of their devices.

3.6.1 Information types and services integration:

Currently, the MPA prototype interoperates the telephony, E-mail, and ICQ™ services. Information types can be text or voice.

3.6.2 MPA features:

The researchers focus on routing between people. The key challenge today is to find people and communicate with them personally, as opposed to communicating only with their possibly inaccessible machines such as cellular phones and pagers that are turned off.

They define the Personal Proxy (see Figure 14) as a dual role: As a Tracking Agent, where the proxy maintains the list of devices or applications through which a person is currently accessible. And as a Dispatcher, with the proxy directing communications and using Application Drivers to convert the messages into a format that the recipient can see immediately.

Because no one wants to be receiving messages constantly, an important function of the Personal Proxy is to protect the user's privacy by blocking unwanted messages and hiding the true location of the user.

3.6.3 Solutions to messaging system problems:

The framework of the MPA includes also Stream-to-Message conversion. For example, if the recipient receives a phone call and is currently reachable through E-mail only, the Personal Proxy converts the voice mail to an E-mail and sends it to the recipient's computer.

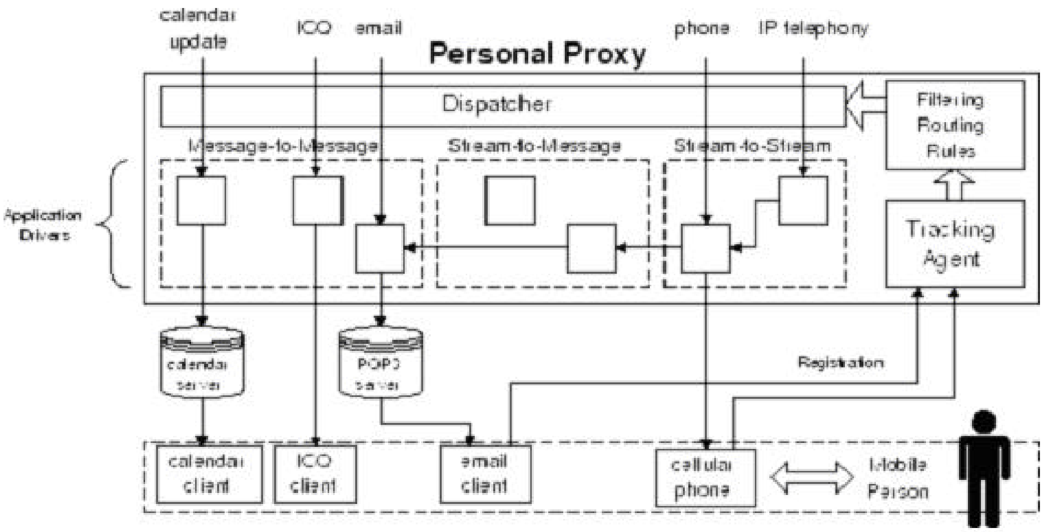

Figure 14: MPA's Personal Proxy [Appenzeller, G., Lai, K., Maniatis, P., Roussopoulos, M., Swierk, E., Zhao, X., Baker, M. 1999]

MPA does not take several steps over time to guarantee the delivery of a message, which the Active Messenger product does by trying multiple channels and awaiting possible recipient's reactions.

Similar to Canard, MPA also belongs to the fourth generation messaging systems.

Problem		Solution Quality
Communication (Services integrated)		PSTN, E-mail, instant messaging,
Translation		Partial
Redirection	Person to person reach ability	Yes
	Sequentially redirecting	None
	Mobile person's privacy protection	Yes
	Redirect according to the information's priority	Yes
Persona		Only one persona

Table 20: Analysis of four problems in MPA

3.7 Summary:

In this chapter we described six messaging systems. Some of them belong to the second and third generation messaging systems, such as Unified Messaging. While the others belong to the third generation toward fourth generation, such as MPA.

An analysis of these existing message systems' solutions for the four messaging system problems is shown in Table 21.

	Communication Problem	Translation Problem	Redirection Problem	Persona Problem	Generation classification
UMS	Partial	Partial	None	None	2nd , 3rd
Phoneshell	Partial	Partial	None	None	3rd
Active Messenger	Partial	Partial	Partial	None	3rd , 4th
Canard	Partial	Full	Partial	None	4th
IPulse™	Partial	Partial	Partial	None	3rd , 4th
MPA	Partial	Full	Partial	None	4th

Table 21: Analysis of four problems in existing approach

In Figure 15, we show their relation with messaging system evolution.

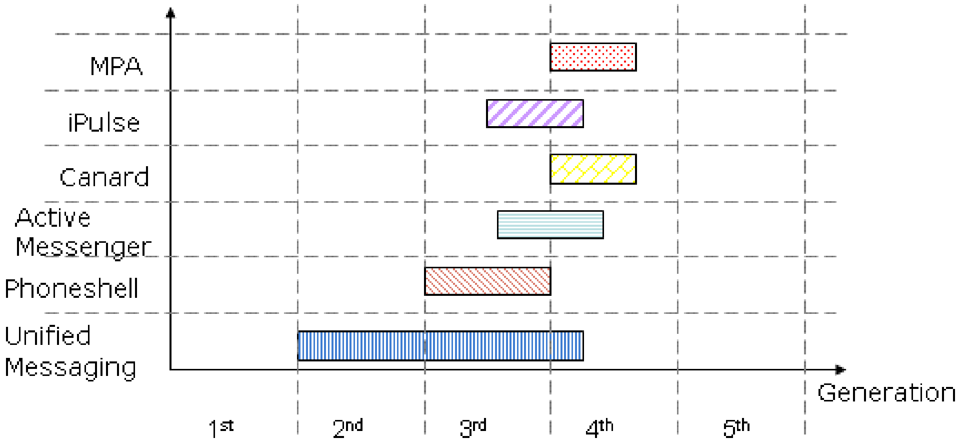

Figure 15: Some messaging system road map on evolution history

From the summary Table 21, we can see that none of the integration systems solve all four of the messaging system problems comple tely and efficiently.

With the fifth generation messaging system, which we introduce the structure of in the later chapter, a full solution for the four messaging system problems is possible.

4 Features Classification Framework:

We have discussed four main problems in the messaging system, current solutions within the existing messaging systems, and the relationship between these four problems, existing messaging systems and the messaging system generations.

In this section we will present the features dassification framework, which helps us to understand and discuss the messaging system and its features.

The framework is organized into four catalogues: the message delivery catalogue, message processing catalogue, message security catalogue, and the message failure catalogue.

In the message delivery catalogue, we define the fundamental properties of message delivery. The message processing catalogue extends the delivery catalogue with properties in addition to the message processing. Security properties of the system are defined in the message security catalogue. Finally, we define properties of message failure, with respect to message delivery, processing or message security in the message failure catalogue.

Message delivery catalogue	Message Failure catalogue
Message processing catalogue Message security catalogue	

Table 22: Features Classification Framework

The framework is quite comprehensive, and we deliberately address a wide variety of system aspects. We define a number of features in each catalogue, and for each feature describe the possible values. Combinations of such values characterise the system architecture. Not all combinations of values for the features can be implemented using currently existing message delivery products, and some combinations may not be feasible at all.

The features we defined in each catalogue represent those aspects of the system that are important for capturing the main functions of the system. The classification framework aims to establish a common language to better describe the messaging system. We selected the features based on the users of the messaging system, including:

4.1 Message delivery catalogue

The message delivery catalogue includes the features related to exchanging (sending and receiving) messages between the message sender and the recipient of the message. It is not concerned with the processing of messages, i.e., the messages are reformatted according to the type of receiving devices. The message delivery catalogue is essentially concerned with the occurrence of the messages state transition.

The message delivery catalogue comprises of the following features:

4.1.1 Initiating

Initiating defines who causes a message delivery to happen. Refer to Table 23, the delivery can either be initiated by a sender who sends a message, known as pushing, [TechTarget] or by a receiver who queries for a message, known as pulling [TechTarget]. Mixed initiating refers to the case where the same message is both pushed and pulle d by different users.

	Initiating
1.	By sender (push)
2.	By recipient (pull)
3.	Combination of 1 and 2

Table 23: Initiating feature

In the push technology, like opt-in versus opt-out debate in E-mail marketing [Kinnard, S. 1999], we also have two different approaches to gathering and using the recipient's address. In general opt-in refers to a message address-gathering technique in which a person gives another explicit permission to send them messages. Opt-out involves the gathering of addresses without explaining how they will be used and sending messages to those addresses unless asked to stop.

Pull technology means the recipient has declared an interest in receiving messages by subscribing according to some subscription mechanism. Recipients may subscribe to our system or to sender directly.

The fifth generation messaging system we define will be a system that combines push and pull opt-in system.

4.1.2 Distributing

Distributing defines the number of the final recipients of the sent message. If there is only one such recipient, the message delivery is unicast, or point-to-point. The message delivery is multicast or point-to-multipoint if there are multiple ultimate recipients. Broadcast is a special case of multicast delivery, where the message is sent to all the customers of the system.

Distributing	
1.	Broadcast
2.	Multicast
3.	Unicast
4.	Combination of 1,2,3

Table 24: Distributing feature

Suppose our fifth generation messaging system sends a notice to all the users, this is known as *broadcast* distributing.

When a user tries to send message to a group of recipients, a multicast distributing is needed. For instance, a user sends a message to a group of his family members.

Unicast distributing will be the main traffic in our system.

The fifth generation messaging system will be a system that supports all three kinds of distributing methods

4.1.3 Redirecting

Redirecting defines how a message is rerouted so that the message arrives at recipient. There may be none, by sender's intention, by recipient's intention, or a combination of sender and recipient's intention for a message rerouting.

Rerouting here means not only to reroute the message within a recipient's available devices, but also to reroute the message to another recipient.

Redirecting	
1.	None
2.	By sender
3.	By recipient
4.	Combination of 2 and 3

Table 25: Redirecting feature

The fifth generation messaging system will redirect a message combining the sender and the recipient's intention. Beside the user's intention, our system will also examine the system's status such as the traffic load to decide the path of the message delivery.

When there is a conflict between sender and recipient's intention, a policy, defined in the Operation Administration and Maintenance server, will be applied. More detailed explanation will be given in Chapter 5, the fifth generation messaging system structure.

4.1.4 Alerting

Alerting defines whether or not the system will give arrival notification to the recipient when a message has arrived, outcall notification before system sends scheduled message for sender.

Alerting messages such as a beep or a shining light could be generated by the access network. Or as our fifth generation messaging system will do, an alerting message is generated by our system, which means that our system will generate a notice and setup a call sending it to recipient.

Altering
1. None
2. Alterable

Table 26: Altering feature

4.1.5 Certifying

Certifying defines whether or not the system will provide the sender with feedback composed of the message receipt.

Certifying
1. None
2. Certifiable

Table 27: Certifying feature

The information sender, as the customer of the system, asks our system to execute the service they want, and may need a message receipt to avoid our system denying that they received the message from the sender.

The sender's bill is based on every message they pass through our system. Our system also needs evidence to avoid arguments about non-payments.

At both of the customers and systems request, the message receipt should be used and kept by each as evidence of the sender's message.

The message receipt can either be a certifying receipt, which is generated by the system when the system receives the message, an arriving receipt, which is generated by our system after the delivery has been accomplished, or the reading receipt, which indicates to the sender that the message has been read by the recipient.

4.2 Message processing catalogue

The message processing catalogue defines the properties that characterize message translating, storing, ordering and filtering.

4.2.1 Message Translating

Translating defines whether the system will perform the traffic type (information type) translation, caused by sender and recipient using different services and devices to send and receive message.

The "None" value shows that the sender and receiver might use the same services and devices, or the services they are using can support the same traffic type. Such as a sender sending an E-mail and the recipient using SMS to receive messages. As the Traffic type for both of them is text, no translating is needed.

Message Translating
1. None
2. One step
3. Multiple step

Table 28: Message translating feature

"One step" shows that before the message can be delivered successfully, it must be translated only once.

"Multiple step" means the system need to do more than one step translation in order to deliver the message to a recipient's device. It can either be multiple step translation with one service, such as by using OCR to translate image to text, then using TTS to translate text to voice so that the sender can send a fax to recipient’s phone, or it may be multiple step translation within multiple calls, For example, in order to deliver message sequentially over time, system might translate a Email message to voice at one time and deliver it to recipient’s landline phone, then few days later, this E-mail message will be translated in to image to send to recipient’s fax.

Traffic type translation can be voice to text translation or the reverse, image to text translating or the reverse etc. All the translating will be executed in the Message Sever in our fifth generation messaging system.

4.2.2 Message Ordering

The ordering property defines the sequence in which the message is queued before being delivered. The message ordering at the system can be implemented as “none”, which actually means random ordering, temporal based ordering, such as first-in-first-out (FIFO) or Last-in-first-out (LIFO), or as a priority and persona based ordering.

Message Ordering	
1.	Random
2.	FIFO or LIFO
3.	By priority and persona

Table 29: Message ordering feature

The fifth generation messaging system will queue the messages according to message’s priority, determined by the sender, and according to the message’s persona, determined by the recipient.

4.2.3 Message Storing

Message storing defines where the messaging system stores the messages.

For the conversation services messages, they will be delivered to the recipients’ device directly, and stored in the message log in the database.

The messaging service message, which is a type of store-and-forward service, can be saved in the *message storage* at the recipient's side.

Message Storing
1. Sender's side
2. Recipient's side
3. Combination of 2 and 3

Table 30: Message storing feature

For the *retrieval services* and high volume *messaging services* message s, it is better to save the message at the sender's side, and our system will send a brief description to the recipient in order to let the recipient decide whether to retrieve the message.

4.2.4 Message Filtering

Filtering defines whether a message is subject to a selection mechanism in order to be further distributed to the recipient.

Filtering can be based on the message itself (timestamps, message size, or message content etc), based on the system, such as anti-virus protection, or a combination of them, which is the method adopted by our system.

Message Filtering
1. None
2. Message
3. System
4. Combination of 2 and 3

Table 31: Message filtering feature

4.3 Message security catalogue

The message security catalogue defines the properties related to the security issues of the messaging system.

4.3.1 Non-intercepting

Non-intercepting defines whether the system can make sure that no one but only the intended recipient can get the message from the sender. Only the sender and receiver should be able to interpret the contents of the message.

Non-intercepting
1. Non-confidential
2. Confidential

Table 32: Non-intercepting feature

The persona management and some of the security services such as authentication and access control can support non-intercepting in our fifth generation messaging system.

4.3.2 Non-repudiation

Non-repudiation defines whether the system users can deny their actions. This may be set to be either *repudiative* or *non-repudiative*

Non-repudiation includes: *non-repudiation of the origin*, the sender can not deny having send the message and *non-repudiation of the receipt*, where the receiver cannot deny having received the message.

This feature may be performed by a trusted third party through which the parties to a message agree to monitor their messages. This provides independent historic proof that the transmission took place at a specific time and on specific time. Non-repudiation can also be achieved by using the Public Key Infrastructure.

Non-repudiation
1. Repudiative
2. Non-repudiative

Table 33: Non-repudiation feature

The fifth generation messaging system uses full authentication to achieve *non-reputable* for non-repudiation feature, and *confidential* for non-intercepting feature. For the device that cannot be fully authenticated, our system can use a sufficiently secure way based upon the use of a communication device that both parties agree on; such as sending a Fax to a particular Fax machine locked in the private office, and using a PIN number to identify the sender.

4.3.3 Non-replaying

Defines whether our system can protect messages from a "replay attack", an attempt to copy messages, even if encrypted, and then to resend them.

Replay attack is an attack against the authentication and key distribution. It is based on recording messages or their parts, and replaying them in another context. The message can be redirected to recipients other than those originally intended, or they can be repeated in different transmission step. [Syverson, P. 1994] [Aura, T 1997]

Non-replaying
1. Replayable
2. Non-replayable

Table 34: Non-replaying feature

The system can be classified as *replayable* or *non-replayable*. In the fifth generation messaging system, senders can issue a credit memo or nonce value included in the message to protect from this type of attack. Nonce value defines how many times the message can be played, deduced by one for each usage.

4.3.4 Non-tracing

Defines whether the system can protect the sender or recipient's location privacy, which we will discuss a in Chapter 6

Non-tracing
1. Traceable
2. Non- traceable

Table 35: Non-tracing feature

By using the persona management function, which means that it is the user's *temporary identity to* be transmitted during the message delivery, the fifth generation messaging system can protect the users' location privacy.

The protection for message log, which records the message delivery information and stores it in the database, can also help our system to be Non-traceable.

4.4 Message Failure catalogue

The message failure catalogue defines the properties that characterize a *failure range*, *failure level*, and how system *handles* the failure. The message failure model is of primary importance for integrating messaging system.

4.4.1 Failure range

Defines whether the success of a message delivery is based on a defined number or range of any recipients' devices (for example, exactly one, at least one, or 2-5 recipients), or all ultimate recipients' all devices.

Failure range describes how the message delivery property *Distributing* relates to message failure definition. The "Any recipient, any devices" value of the range means: if any of the devices of any of the recipients receive the message, we will define the message delivery as successful. "All recipients all device" means that only when all of the devices of the recipients receive the message, we define the delivery successful.

Failure range	
1.	Any recipients; any devices
2.	All recipients; all devices

Table 36: Failure range feature

4.4.2 Failure level

Failure level defines whether a message's success is either based on only its successful delivery (*delivery level*), based on successful delivery and successfully getting the right response (*processing level*), or based on successful delivery and successfully getting the right response plus satisfied security request (*security level*).

Failure level
1. Delivery level
2. Processing level
3. Security level

Table 37: Failure level feature

4.4.3 Failure handling

Failure handling finally defines how the messaging system handles the failure. *Best-effort* is the lowest level for failure handling, with no guarantee for the message delivery. *Retry for soft bounce* means that the system will try several times if the recipient is temporary unreachable. Or *remove for hard bounce*, such as there being no such recipient.

Failure handling
1. Best-effort
2. Retry for soft bounce
3. Remove for hard bounce
4. Combination of 2 and 3

Table 38: Failure handling feature

The fifth generation messaging system could be implemented with any value of failure catalogue feature.

4.5 Summary

In this chapter, we defined a comprehensive framework for classifying messaging systems.

We summarize all of the features and their values in Table 39. Values with an asterisk (∗) in front are the ones our system described in Chapter 5 is designed to achieve.

Message delivery catalogue:

Initiating	Distributing	Rerouting	Alerting	Certifying
Sender (push)	Broadcast	None	None	None
Receiver (pull)	Multicast	Sender’s request	∗Alterable	∗Certifiable
∗Combined 1 and 2	Unicast	Receiver’s request		
	∗ Combined 1,2 3	∗Combined 2 and 3		

Message Processing catalogue

Translating	Ordering	Storing	Filtering
None	None	Sender’s side	None
One step	By sender	Recipient’s side	Message
∗Multiple step	By recipient	∗Combined 2 and 3	System
	∗By priority		∗Combined 2 and 3

Message security catalogue

Non-intercepting	Non-repudiation	Non-replaying	Non-tracing
Non-confidential	Repudiable	Replayable	Traceable
∗Confidential	∗Non-repudiable	∗Non-replayable	∗Non- traceable

Message failure catalogue

Range	Failure level	Handling
Any recipients’ any devices	Delivery level	Best-effort
∗All recipients’ all devices	Processing level	Retry for soft bounce
	∗Security level	Remove for hard bounce
		∗Combined 2 and 3

Table 39: Messaging system feature framework

5 The fifth generation messaging system structure

The fifth generation messaging system we describe here is a future integration of the existing and future messaging systems.

The first and second generations of messaging systems belong to the past, with details of their structures easily available. However due to commercial reasons, structural details of the third generation system introduced in Chapter 3 are not disclosed to the public. Published descriptions for the fourth generation messaging systems have specified only the main components of the system, without describing the details. [Meer, S. Arbanowski, S. Magedanz, T. 1999]

In this chapter, we provide a structure that can be implemented. We start by describing the fifth generation messaging system's high level architecture and explaining the main functional parts. Several scenarios are used in order to illustrate how the overall system works.

5.1 General definitions and design decisions:

5.1.1 Internet-based

The fifth generation messaging system will converge the voice network and Internet network. The question is whether we design it based on a circuit-switched Signaling System No. 7 architecture as a telephony-based system, or based on a packet switch such as an Internet-based integration system?

Our decision is to design an IP-based system, for the following reason. Compared with the other possible solutions, such as ATM, Internet Protocol (IP) provides a simple services model of packet delivery, and we believe it to be the easiest and lowest cost deployment option of the network-based services using the client-server model.

We treat the different communication networks (i.e. PSTN, GSM etc) as *access networks*. Once our system receives a services request from those access networks it will build up a connection on top of the Internet, integrating different services from heterogeneous networks.

5.1.2 Client-server Model

In the client-server model, the fifth generation messaging system consists of three logical parts: server, network and client.

A server provides the service, and the service communicates through a network to a client’s device. The network provides a connection between the server and client. The client is a multipurpose device that is used to access the service, and the same client’s device is able to access multiple services.

5.1.3 Recipient control

In most current message delivery systems, a sender chooses how and when to reach the recipient. In our system, we shift the control from sender to recipient.

To achieve this, the fifth generation messaging system must provide functions for the recipient to personalize their delivery services such as call redirection, call waiting etc.

5.1.4 Call model:

Here we introduce a variation of the Call Model of Sven van der Meer [Meer, S. Arbanowski, S. Magedanz, T. 1999]. Which means a service requests to our system will be processed according to our Call Model, Shown in Figure 16.

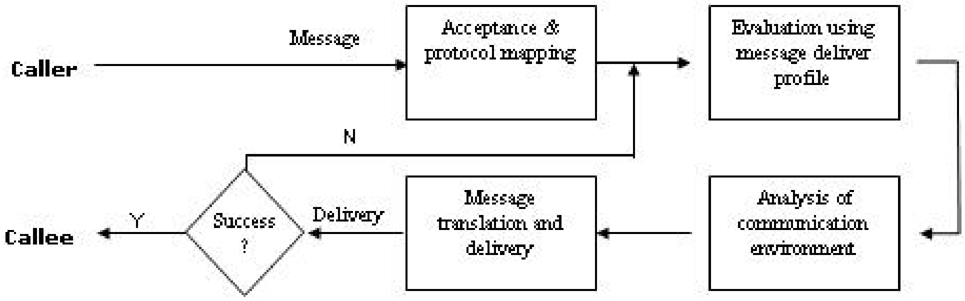
Caller
Message
Acceptance & protocol mapping
Evaluation using message deliver profile
N
Callee
Y
Success ?
Delivery
Message translation and delivery
Analysis of communication environment

Figure 16: Call model

Caller and Callee

Caller in our model means the one who start up the call request. The caller can be the message sender, message recipient and or system itself. When the message recipient wants a pull service, the caller at this moment is the message recipient. The caller will be the system if our system needs to send a notice to the user, for example, the system will require a call setup when it needs to the send a message arrival alert notification to the recipient of the message.

Callee is the destination of a call. It can be message sender during the pull services, or the message recipient.

Evaluation using message delivery profile

If a call request is detected by the system and the protocol has been mapped from the access network to the protocol used in our system, then our system will evaluate information by using the message delivery profile. This message delivery profile combines the message sender, message recipient and system's delivery intentions. The result of this evaluation determines if this message belongs to which persona of the recipient and the path for the message to be delivered to the recipient.

For the conversational service, the feedback call path will be setup automatically.

Analysis of communication environment

An analysis of the actual communication environment of the system and the recipient selected devices should also be taken into account before the service is delivered. This analysis includes detecting if the delivery can be successful. Especially when the call path was determined by scheduled location registration, for sometimes the device may be not in range.

Message translation and delivery

If necessary, the message may have to be translated prior to its delivery of the message to the recipient's device.

The message delivery may fail, for example, if the message requires a guaranteed reading by the recipient with a certain time, but the recipient's device is not available, or the message is not be read within a certain time. When the call delivery has failed another evaluation should be performed to decide how the call should be handled. Either another call path must be setup or the failure handling feature defined in Chapter 4 should be applied.

Some procedures of the call model may be repeated until the service can be completed.

In order to accomplish a service, several call paths may be required. For instance, Alice sends a message to Bob, and Bob requires an alerting service, then to accomplish these services, at least two calls will be setup. One is with Alice as the caller and Bob as callee to transfer message. Another one is our system as caller and Bob as callee to send message arriving notification.

Our call model covers almost all the features in our *message delivery catalogue*, and some of the features in the *processing catalogue* and *failure catalogue* as defined in Chapter 4.

- *Initiating*: A call, can be initiated by message senders or recipients. The case of recipient initiated messaging is sometimes referred to as "pull" technology (see section 4.1.1).

  During the "pull" services, it is the message recipient who starts up the call model. After a recipient requests a message, our system setups a call path for the recipient to deliver the request to the information sender, a feedback call path, which used for deliver the requested message from the information sender to recipient, will be setup by the system automatically.

- *Distributing:* For *multicast* or *broadcast,* our system will setup a separate call for each recipient.

- *Rerouting:* Evaluation using the message delivery profile and analysis of the communication environment procedures in the call model will support message be rerouting according to the sender and the recipient's intention.

- *Alerting:* An alerting message path is setup by our system if the recipient requests the alerting service.
- *Certifying:* A message receipt delivery path is setup by our system to the information sender if the sender requests the certifying service.
- *Translating:* Message translation is an essential procedure in our call model.
- *Ordering:* The value of the call's ordering attribute decides the execution priority of the call.
- *Filtering:* The filtering feature indicates whether or not the system should accept a call request.
- *Failure handling:* This feature defines what the system should do when call delivery fails.

5.2 Architecture and function requirements:

This fifth generation message delivering system should support the customers using legacy messaging services and future communication services. So the main requirements of this system are that it should consider the constantly changing demand of the markets and the customers, the scalability of the system architecture, and the completeness of its functionality.

We list our requirements below:

- Our system should accommodate a wide variety of services: conversational, messaging and retrieval services.
- Our system should work with existing applications without the need for application programming interface changes or host software modifications.
- Our system should minimize the costs of the adaptation of future access network, services, and applications.
- Our system should support high availability and fault tolerance. Communication may happen at anytime so our system should be able to handle failures seamlessly, hiding any indication of failure from the users.
- Our system should protect the user with high-level privacy and security.
- Our system should have a high level of personalization, to let users have greater control over their messaging environment.
- Our system should support all the functions of fourth generation messaging systems: call redirection, service management, message translation, remote access, service delivery, multimedia message storage, authentication, and user interface.

5.3 High level architecture overview

Our system will have 6 main components, listed below and shown in Figure 17.

- Media Gateways are the interface between our system and the *access networks*. They also allow our system to provide various services, such as the IVR (Interactive Voice Response) function.
- Application Servers control the call logic.
- Message Servers accomplish the main work on message translation, message management etc.
- The Security Control Server: deals with the response for user authentication and other security issues.
- The Database Server stores the customer and system data.
- The Operation Administration and Maintenance (OAM) Server handles the user interface, system management, network management, billing, auditing and fault tolerance.

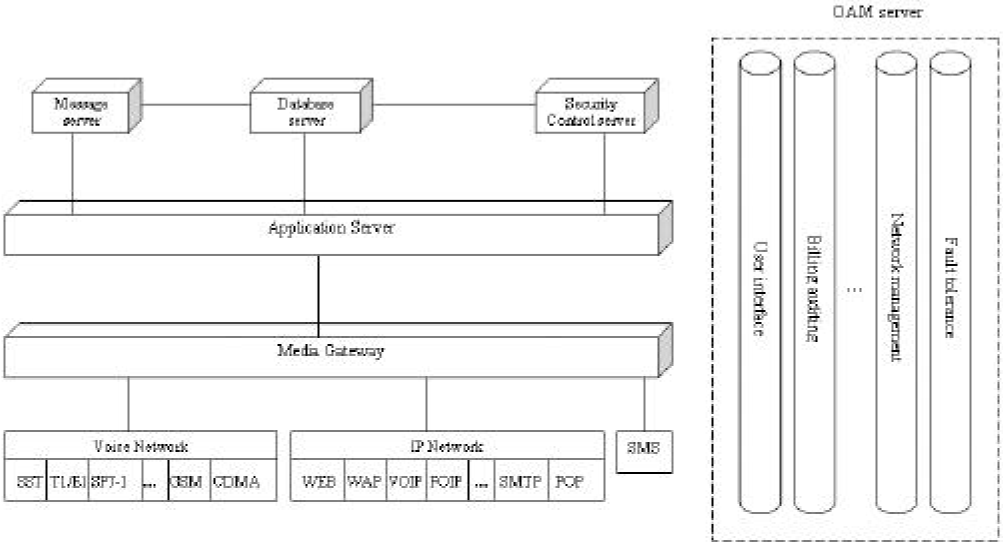

Figure 17: High -level architecture of the 5th generation messaging system

In the following sections, we will examine each component's main function and their requirements.

5.4 Media Gateway (MG)

A Media Gateway can interconnect an *access network* with the remaining components of our system. It enables users to access integrated services over their choice of client devices and *access networks.*

A Media Gateway integrates multiple traffic types across multiple access networks like telephony, wireless data, and wire data access.

By using a Media Gateway, the fifth generation messaging system can be designed as a network and device independent system, which allows new networks and devices to be plugged into our architecture without modifying any other components of the system.

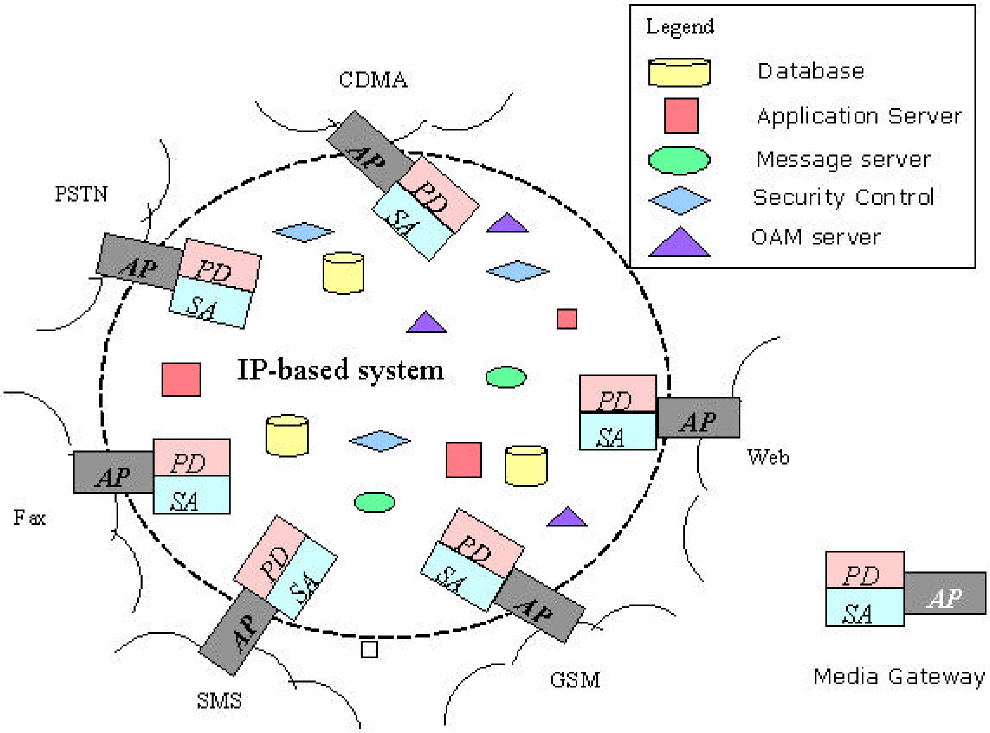

Figure 18: Media Gateway

Our Media Gateway consists of hardware and software for transcoding between the signaling protocol and data format used by the *access network* and those used by our system. It should interface with the Application Server, Security Control Server, Database Message server and Operation Administration Maintenance.

We identify three components within the Media Gateway: Access Point (AP), Protocol Driver (PD) and Service Assistant (SA). These components are shown in Figure 18 and discussed in separate setting below.

5.4.1 Access Point (AP)

Access Point is the connection of the fifth generation messaging delivery system to any kind of legacy or future telecommunication services. It connects all of the communication services and provides desktop and mobile client access to our system.

Functionalities:

- Hardware interconnects between messaging system and access networks.
- Accepts a call establishment from the access network on behalf of our system.
- Setup calls from our system to the access network.
- Reports alarm to the OAM server. Abnormal events such as overload or traffic congestion should be reported to system administrator.

Requirements:

- Quality: AP should provide low data loss and low delay.
- Connectivity: AP should provide good connectivity between our system and the access network, since it is located at the boundary of both of these networks. It should support the different network's physical features. For example support Fax tone detection, support PSTN connection such as E1, T1, STM-1 etc, and the double stage

dialling feature in PSTN, which means that sender first dials the number of the recipient to the AP, the AP send back a tone, then sender inputs the digits to identify himself.

This double stage dialling feature in PSTN enables the user to input their PIN for authentication in our system.

- Reliability: Since AP is the network interface, its reliability is much more important. AP should support redundancy in order provide carrier grade reliability. When an AP fails, another AP should take over for the failed one and continue serving the ongoing call.

5.4.2 Protocol Driver (PD)

Functionalities:

- Signaling conversion between different types of access network and our system IP based standard protocol. Like convert incoming PSTN signals from TDM to IP.

  It bridges different signaling and control protocols with our system and access networks.

- Message log generation: such as message arrival time etc

Requirements:

- Openness: The key requirement of the standard protocol is openness. It should accept all the existing application type of access network, e.g. SMTP, VPIM, POPS/IMAP4, GSM, SMS, Instant messaging.

  It should handle any kind of legacy or future telecommunication signal, allowing new protocols to be introduced.

- Scalability: The implementation of PD should mean that it can be plugged into the system at runtime and be immediately operational.

- Security: non-authorized users must not have access to the system. So PD must support the authentication protocols used by the *access network* .

5.4.3 Service Assistant (SA):

Provide function in order to deliver messages more efficiently. Such as:

- Interactive Voice Response (IVR): offers voice prompts in different languages to the caller, accepts a combination of voice telephone input and touch-tone keypad selection and provides appropriate responses.

  Allow users to record personal greeting.

- Computer Telephony Integration (CTI): improves the management and message processing for customer. Activities such as automated computer dial out, automatic redialing on a busy signal, assigned time-to-call intervals, call scheduling and speech recognition etc.

5.5 Application Server (APS)

An Application Server is the main part of the system. It will provide service control according to the call model (Call Server), monitor the recipient's connectivity state (Tracking Agent), and help the services to be more efficient (Call Assistant).

An Application Server should interface with the other components in the system, shown in Figure 19.

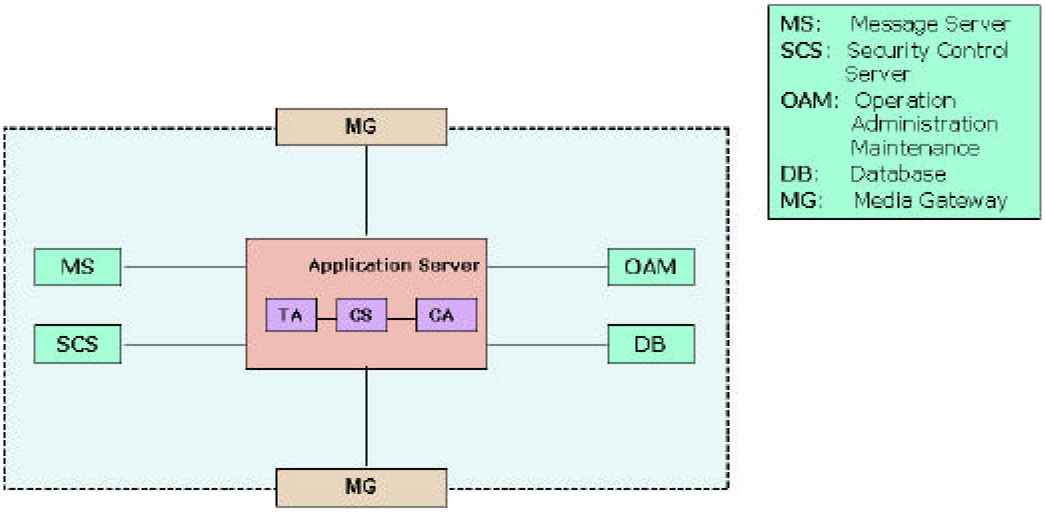

Figure 19: Application Server

Application Servers must provide functions to handle multiple services.

5.5.1 Call Server (CS)

The main task of the Call Server is to help the call control to deliver the message.

- Name mapping: Mapping the incoming information with the recipient's persona.
- Path creation (Message evaluation): according to the message delivery profile, generated by the Database Server, and Tracking Agent to determine call path.

  If it is a conversational service, the feedback call path will be setup automatically.
- Media Gateway communication: providing service assistants such as the Interactive Voice Response (IVR) function.
- Call Delivery: Auto start up a call to recipient, and send the message to Media Gateway.

5.5.2 Tracking Agent (TA)

Tracking Agents will monitor the recipient's connectivity state. Helping the Call Server to setup the call route.

It should support three kinds of Location registration methods: *automatic, manual, or scheduled.*

- *Automatic*

  For the automatic registration, as we mentioned in Chapter 2, some devices can provide feedback information about whether the device is within range, a user using this kind of device can automatically register their location.

- *Manual*

  The manual registration can be done by using a registration interface, which is in OAM parts, to send registration message to our system. For example, filling a web form, call our system's registration number, or sending a registration E-mail.

- *Scheduled*

  The scheduled registration means that system assumes a change in the user's location according to a schedule. It enables registration for regular events like " for the next week, every morning from 9am to 10am, I have a meeting in room 249".

Whatever what kind of the registration method, all the registration must be authenticated and encrypted to preserve the user's location privacy.

5.5.3 Call Assistant (CA)

CA will help system to deliver the message efficiently:

- Message notification generation:

  It could be message waiting indication such as using audible or visible signal to notify the recipient about newly arrived messages. If the user does not reject the message, it will ask the user to authenticate himself to guarantee that the message is delivered to the recipient at the right persona, then start the call delivery.

And also could be an Outcall notification for sender. If a sender defines a scheduled message delivery, the system can send this outcall notification to the sender asking him confirm the sending of the message.

If it is a retrieval services, or according to user's preference, system can generates a short notice message. This short notice can be a short SMS text message, or a voice notice. After the recipient receives the notice, they can make the decision to use which device to retrieve it.

- Message log generation: generates the call details and record it in the message storage.
- Message delivery error control: retry for non-permanent errors like device being temporary unavailable. Or let the Message Server generate error message.

  The number of retry times will be defined in OAM policy control.
- Service management: such as auditing, quality of service (QoS) handling
- Network and system management: Like alarm management, performance monitoring, faulty recovery etc.

The Application Server will handle the call control. It is the main components to solve the messaging system "redirection problem".

By using our *Call Model*, our system can support person-to-person reachability, sequentially redirecting information over time, and redirecting according to the information's priority.

Tracking Agent in APS track the recipient's available devices, so that the service can be delivered to the recipient.

If users request the sequentially redirecting information over time service, at a particular time, our system can setup a call to deliver information to the recipient, or send requests to the information sender asking for the information for the recipient.

The procedure of evaluation using the message delivery profile can support the messages to be delivered according to their priority.

Another feature in the “redirecting problem”: Mobile person’s privacy protection will be discussed in Chapter 6.

5.6 Message Server (MS)

The main task for Message Server is to translate the message format. It will also provide functions enabling users' communication with the messages composed by different access network, and messages stored in the Message Storage inside Database.

Message server must provide a database independent function to store, retrieve and modify messages.

It should have interface toward Media gateway, Application Server, Security Control Server, OAM Server and Database Server.

5.6.1 Message Translator (MT)

The heart of Message Server is the Message Translator, which transforms incoming communication from the sender into a traffic type understandable by recipient's services and devices. We list some important translation services below.

- Text-to-speech (TTS) translation can let system read E-mails to recipient over the phone.
- Text message can be produced from speech through speech synthesis, Speech-to-text (STT).
- Text message can be translated between different languages.
- Voice messages can be translated and delivered as WAV files attached to E-mails.
- Faxes image can be translated and delivered as TIF files attached to E-mails.
- Optical Character Recognition (OCR) can convert faxes to editable text.

By using one step translation or many step translations (such as image being transferred to text by using OCR, then using STT, text transferred into voice) our system can accomplish the full translation we defined in Chapter 1.

Message Translator is the main component in our system to solve the messaging system "translation problem". Under the control of Application Server, it can do "one step" or "multiple step" translation.

5.6.2 Message Manager (MM)

The Message Manager helps the system to manage messages.

- Message folder management: allow users to create, rename, delete and retrieve message folders according to their persona, defined when the user logs in.

- Message Input: allow users to directly store a new message in a folder by not using the Application Server. Which means this message is not from a call, but from the user himself.

  This function will could be used to send the user himself a warning message. User could save a message saying, "will have meeting at 9am", and define that to send this message to himself at 8.55am to his mobile phone.

- Stored message management: allow users to delete, move, save, archive, copy message which stored in the Message Storage.

- Message filtering: allow system to filter the incoming and outgoing message for security reasons, such as anti-virus scanning or based on user preference.

- Message query: provide the message query information to user.

- Error message generation: During the message delivery, if there is a permanent error such as the incoming message could not be mapped with the recipient's persona, or after trying the several times that are defined by OAM, a bounce message – A notification message returned to the sender indicating that the message could not be delivered will be generated. Bounce message should indicate what went wrong.

5.7 Security Control Server (SCS)

In this section, we show how a Security Control Server can handle the security issues arising in our system.

Security is important in the messaging system. Before we start the SCS's function, let's see the system security goals at first.

5.7.1 Security goals for messaging system

The goals we list below are from the system's perspective, goals from users' perspective will be examined in Chapter 6

As Charles P. Pfleeger mentioned in his book, Computer security consists of three characteristics: *confidentiality, integrity, and availability*. These are also the security goals for messaging system. [Pfleeger, C. P. 1997]

Confidentiality means that the assets of the messaging system are accessible only by authorized parties. Confidentiality is sometimes called privacy.

Integrity means that assets can be modified only by authorized parties or only in authorized ways.

Availability means that assets are accessible to authorized parities.

Those are three traditional areas of the computer security. They all deal with different aspects of access control and put their emphasis on the prevention of unwelcome events to against unauthorized use. In the messaging system, the assets available are not just the software, but also the hardware and data. Messaging system is not just a simple computer system, but a lot of user messages and user personal data is involved, so we may add two new security requirements: *Accountability and reliability*

Accountability mean that audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.

To be able to do so, our system has to identify and authenticate users. It has to keep an audit trail of security events. If a security violation has occurred, information from the audit trail may help to identify the perpetrator and the steps that were taken to compromise the system.

Reliability relates to failure and safety, to the impact of system failure on their environment.

To be able to do so, we have the Network Management (NM), Fault Tolerance (FT) and Policy Management (PM) components in the Operation Administration and Maintenance (OAM) Server.

5.7.2 Security services in the fifth generation messaging system

To achieve the goals we list, five classes of security services should be provided in our fifth generation messaging system. They are: authentication, access control, data confidentiality, data integrity, and non-repudiation.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what they declared to be. [TechTarget]

Authentication is the essence of the messaging system security. It is required for achieving all system security purposes: *Confidentiality, Integrity, Availability, and Accountability*. It also supports privacy protection for users, which we describe in Chapter 6.

Access control

Access control services provide the protection of system resources against unauthorized use. Access control services are closely tired to authentication services. A user must be authenticated before an access control services can effectively mediate access to the system resources.

Access control is the service that is required to accomplish the *Confidential*, *Integrity* and *Availability*

Data confidentiality

Data confidentiality services provide protection of the data from unauthorized disclosure. Three kinds of confidentiality could be:

- *Connection confidentiality services:* is to provide confidentiality of all data transmitted in the system.
- *Connectionless confidentiality services:* is to provide confidentiality of all database units.
- Traffic flow *confidentiality services:* is to provide protection of information that may be compromised or in directly derived from a traffic analysis.

Data integrity

Data integrity services are to provide for the protection of message data against unauthorised modifications. It includes:

- *Connection integrity services:* is to provide integrity of message data in a call connection.
- *Connectionless integrity services:* is to provide integrity of database.

Non-repudiation

Non-repudiation services give protection against the originator of a message or action from denying that he or she has originated the message or the action, as well as against the recipient of message denying that the receiver received the message. Consequently, there are two kinds of *Non-repudiation* to be distinguished:

- *Non-repudiation with proof of origin* is to provide the recipient of a message with a proof of origin

- *Non-repudiation with proof of delivery* is to provide the sender of a message with a proof of delivery.

Non-repudiation services are based on the authentication services. Non-repudiation is becoming increasingly important in the context of electronic messaging system now, and also in e-commerce application on the Internet. It is required to achieve accountability purpose.

The confidentiality services and integrity services of software and hardware are not the points in this thesis.

5.7.3 Security Control Server functionality and requirements

Security Control Server should have interface with the other components of the system.

Functionalities:

- User authentication: verify user's password, digital signature
- User access control: grants access based on the user's access right.
- Encryption and decryption: encrypt and decrypt date transferred in our system.
- Certificates manage: is to issue revoke and verify digital certificate.
- Key generation: generate public private key pair for user's certificate and symmetric key for cryptography.
- Key distribution: distribute symmetric key secretly to the user.
- Certificate revocation list (CRL) maintaining: A user can revoke his/her certificate. Server will add the revoked certificate to the CRL, and provide retrieve for any application.
- Activities log maintaining: record users' activities such as login
- Certificate and password storage: store users' certificate and password.

Requirements:

- It can issue certificates to wireless devices such as PDA or mobile phone and wire devices such as PC.

- SCS should support different authentication mechanism and cryptography method.

- Any application can retrieve the CRL.

- IT should support high faulty tolerate: SCS should be available 24 hours a day and 7 days a week, should tolerant failure gracefully.

- SCS should separate the private data like system user applying revoking certificate, and public data and operation like anybody search and download user's certification and obtain CRL.

- Certificate should support multi language.

- SCS should have user activity auditing and error recording.

5.8 Database (DB)

Database is designed in a way that data can be used by all other parts of the system. It provide centralized place to store all the data.

Main sets of information are: available service and device registration, routing rules, and message information, and persona management information.

5.8.1 Database elements

Database should include the following elements shown in Figure 20.

- User information: stores information related to users, e.g. user's real name, address, and relation to devices.
- Available services and devices information: stores information of user's location and available services and devices.
- Terminal information: stores the information related to a device. Such as the model of the devices and their supported traffic types.

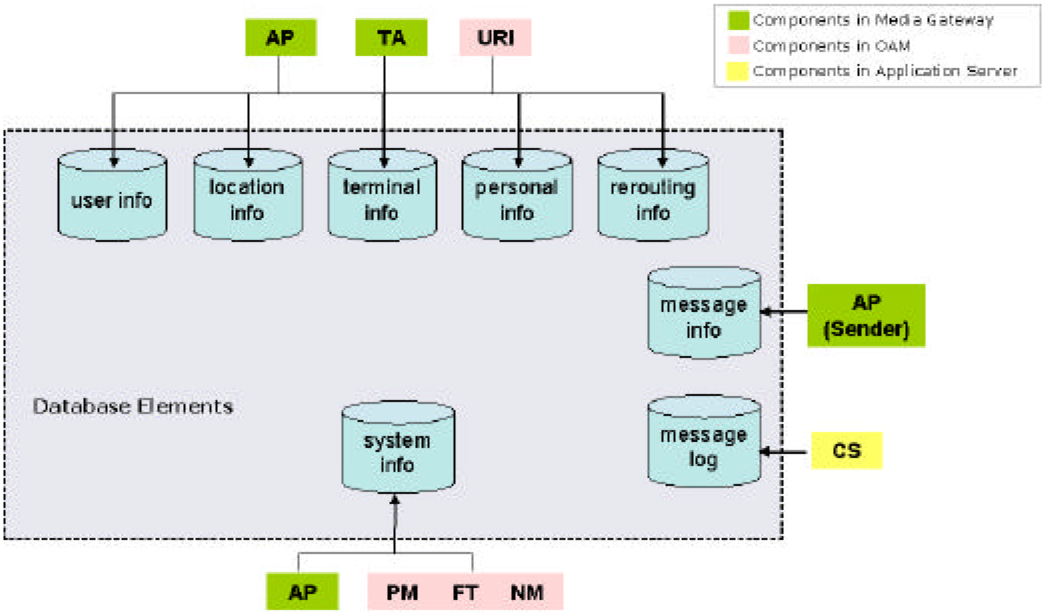

Figure 20: Database elements

- Persona management information: stores the information of user's different identities (user's UID, PID and DID[*] defined in Chapter 6), and the relation of user's persona to identities, for example, one of Alice's PID and her DID determine Alice's persona as family.

- Routing rules information: stores the rules that user defined for services control. For example, at what time, forward all user's message to a specific device, or the message belonging to a specific persona be reroute to which address, and how to do the *Sequentially redirecting information over time*, which is one of the feature in the "redirecting problem".

- Message delivery log: stores the information about the message, like "from" "to" and message status like arrived, rejected, and deleted.

- Message information: stores the information related to the message itself such as the message priority.

- System information: store the information related to the system such as the access networks traffic load.

5.8.2 Profile Generator (PG):

To generate the message delivery profile from user persona profile, system profile and message profile shown in Figure 21.

[*] UID: Universal identity
PID: Personal identity
DID: Device identity

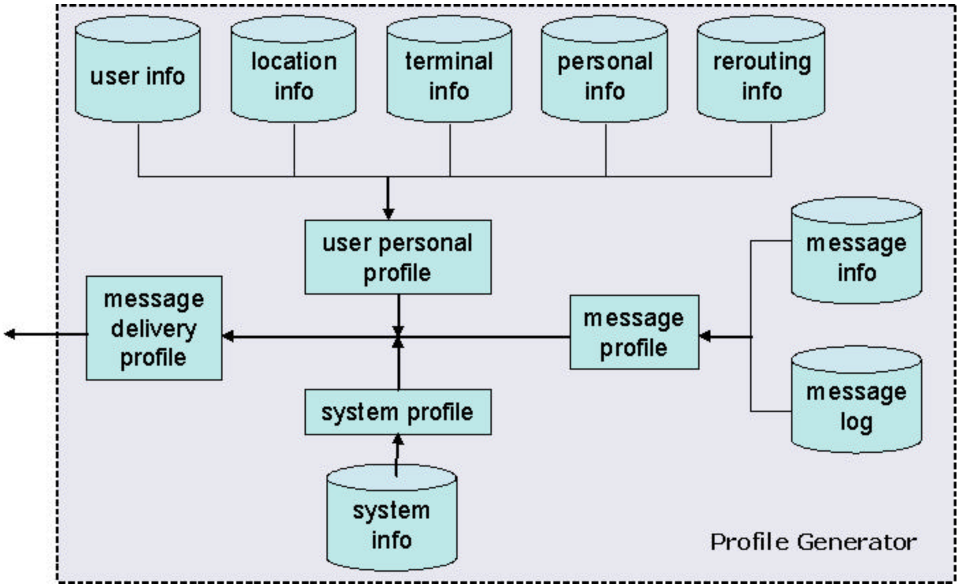

Figure 21: Message delivery profile

Profiles consist of a set of rules, which follow the form as:

***IF** condition **THEN** action*

Conditions here define on which circumstances a specific communication behavior is demanded by the user, such as time equal to “9.00am”, persona equal to “family”, or message priority equal to “high”.

Action can be: *Rerouting* which changes the path that the message is delivered by, *Content translating* which means use Message Server’s Message Translator to modify or convert the format of the message, or *Service portraying* which show if the message must be delivered to recipient.

User persona profile:

Define the preferred delivery path from the recipient’s perspective. Such as at a specific time, the recipient like to receive message using mobile phone, if failed, then use a specific landline phone.

For instance it could be described as:

IF time is 9:00am THEN forwarding to phone (09) 3737599.

IF persona is family THEN must be delivered

System profile:

Define the preferred delivery path from the system's perspective. Such as define when there is network congestion, high-level message will be delivered first.

For instance it could be described as:

IF PSTN load is great than 80% THEN forwarding to E-mail

Message profile:

Define the preferred delivery path from the sender's perspective. Such as the message's priority

IF priority is urgent THEN must be delivered

Message delivery profile:

Message delivery profile is the interface to be used by other parts of the system, to show how to deliver message. It based on the matrix of user persona profile, system profile and message profile to determine delivery rules.

When there is conflict in the generation of message delivery profile, the policy defined in OAM's Policy Management will be applied.

For instance, from System profile, message will be reroute to E-mail, but from User persona profile, it should be delivered to mobile, then profile should applied.

5.8.3 Message Storage (MSt)

Message Storage is used to store the message for recipient to retrieve.

As we described in the Chapter 2, the fifth generation messaging system will support multi-services. The message for *conversational services* will be delivered to the recipient's device directly without storing. For the *messaging* *services and retrieval services,* Message Storage is used to store the messages for recipient to retrieve.

As we discussed in the *Message Storing* feature in Chapter 4, for the *retrieval services* and high volume *messaging services* messages, it is better to save the message at the sender's side, and our system will send a brief description to recipient to let recipient decide whether to retrieve the message.

Messages of low volume messaging services could be stored at the recipient's side.

The reason to store high volume messages and retrieval services at the sender's side is to decrease the system's traffic flow.

5.9 Operation Administration and Maintenance (OAM):

OAM is a system management tool that provides a comprehensive suite of management capabilities and a friendly user interface.

User Registration Interface provides the tools that let user maintain their personal date, services requirement etc. Management tools enable system configuration, preventive fault management, performance monitoring, real-time reporting, image management etc. Billing generate bill and control the bill distribution. Elements within an OAM server are shown in Figure 22.

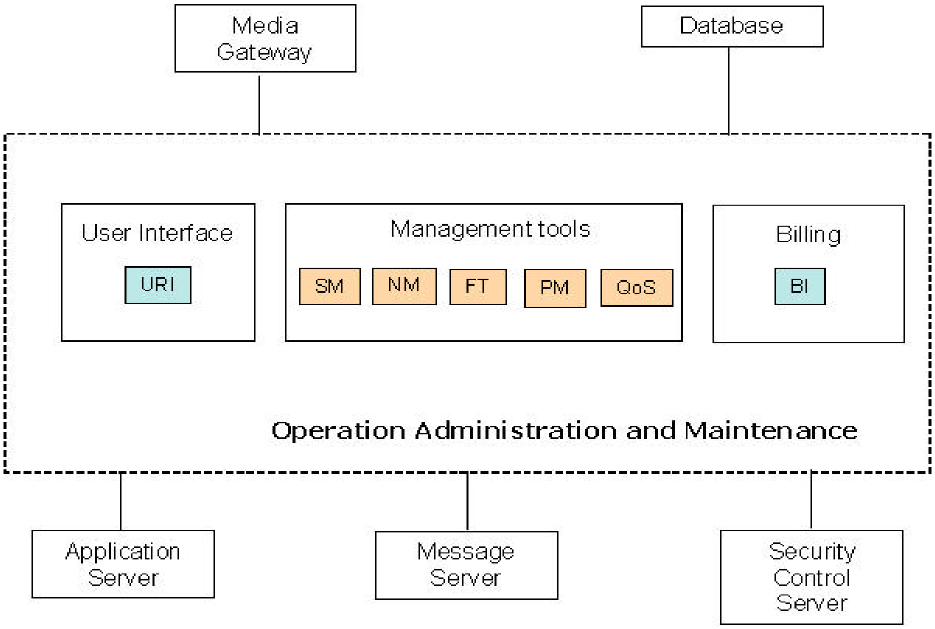

Figure 22: Operation Administration and Maintenance

5.9.1 User Registration Interface (URI)

The fifth messaging system is a recipient control system, which means that the recipient controls when and how the message delivered. It must be configured with personal information.

Four sets of information, which we discussed in above subsection, are provided from URI: user information, available service and device registration, routing rules, and persona management information.

Functionalities:

- Provide user registration: In our system, user could register their personal information, such as name address, and register their location, terminals, etc.

- Provide user location registration.

  Let user register their location, terminals manually or scheduled.

  Inform Call Server what kind of protocol (PSTN, SMTP, etc) and traffic types (TIFF image, voice etc), should be use.

- Allow user to configure their routing rules. Such as: IF Alice is not reachable from her landline phone, THEN send to her mobile phone.

  Enable user to define when, where, for whom, and using which device they can receive message.

  Let user determine how to handle the message according to the message's priority.

- Provide persona management interface.

  Let user select which of their persona's location information should be protected.

  Let user determine the relationship between persona and identity.

  Let user define the different process for message of different persona.

- Provide user interface to let them define their message filtering rules.

- Provide user login interface.

- Provide message query interface to user: let user can retrieve the message they send or received according to their persona. And query a specific message's status.
- Distribute the data collected to database.

Requirements:

- Supporting different interface

  Provide a web-based interface to let user input basic information that system required.

  Provide service based tool to let use register location, modify the information at any time. Such as use touch-tones telephone to navigate through a menu to change the preferred receiving device, routing rules, or persona message information.

- Message compose interface: Our system should keep on using access network's original interface. Such as

  For PC, a graphical user interface (GUI) can be used. Depending on the particular service, other options may also be available. For instance, allows users to record a message with a PC microphone.

  For landline phone and mobile phone, a Telephone user interface (TUI) can be used. From a user perspective, accessing and manipulating messages via phone is no different between the methods used for Public Switched Telephone Network (PSTN, the type in most of our homes) phones and those used in cellular phones.

5.9.2 System Management (SM)

Handle the alarm report that from the other component, and provide the correspond procedure. For example, after the Access Point reports the traffic congestion, OAM will ask Call server to initiate filtering to let the high priority message delivery at first and set a "call gapping".

Provide systems administration tools, like system back up

5.9.3 Network Management (NM)

Network Management provides administration interface, let administrator manage the whole system; maintain system policy.

Network management function will assist human network managers in monitoring and maintaining networks, network devices and their functions.

It will auto-poll the network devices, and use workstations to generate real-time graphical views of network topology changes and traffic.

It should support standard network management protocol, such as SNMP, CORBA in order to use widely used management tools.

5.9.4 Fault Tolerance (FT)

When a system component fails, fault tolerance will handle using a backup component or procedure that can immediately take its place with no loss of service.

Fault tolerance can be provided with software, or embedded in hardware, or provided by some combination.

5.9.5 Policy Management (PM)

Policy control: such as define how many times the system will try when there is a non-permanent error occurred during the delivery. Define how long the CRL (certificate Revocation List) should be refreshed.

When there are conflicts within the user persona profile, system profile and message, define what policy will apply.

5.9.6 Billing (BI):

OAM server should generate bill from the relevant information stored in the message log, such as call duration, message send volume, message retrieved volume, etc

The price of the services will be customer oriented

It should also provide mechanisms for pre-paid billing system.

5.9.7 Quality of Service (QoS):

An application-based Quality of Service mechanism will be needed to guarantee that the system is capable to meet the customer’s preference control, And to ensure quality of voice and data transmission

This is a measure of the system’s efficiency.

Till now, we introduced each component in our fifth generation system. In the following section, we will use two scenarios to see how these components work together to provide the service.

5.10 Typical usage scenarios

We will provide some typical usage scenario to show how the fifth generation messaging system components work together to implement a message delivery:

5.10.1 Scenario 1:

Bob wants to initiate communication using his cell phone to connect to Alice's cell phone. Alice defines that the entire message sent to her at this time will be rerouted to her E-mail. Then system feeds information back to Bob by voice menu as to whether he still would like to send the message. After Bob replys saying that he will send the message, our system redirects it to Alice's E-mail.

In Figure 23 we show the call setup sequence diagram. The explanations according to the four procedures in the call model and two extra step which are outside our call model are listed below. The indicated numbers in the procedure correspond to the Figure 23.

Acceptance and protocol mapping: (1, 2, 3) (shown in red in Figure 23)

Access Point, connected with PSTN, will accept the call if Bob is the legal user of our system (1). Protocol Driver parses the protocol to IP pocket based protocol (2). Finally, the call control request is passed to the Application Server (3).

Evaluation: (5,6,7 8 9) (shown in green in Figure 23)

The Call Server will evaluate the message by using a delivery profile; find that the message should actually belong with Alice's family persona, and should reroute the message to Alice's E-mail address (5, 6)

Then CS in the Application Server will ask Media Gateway using the IVR function to provide a voice menu to Bob, asking him to confirm the sending of the message (7,8).

Bob confirms to our system that he wants to send that message (9).

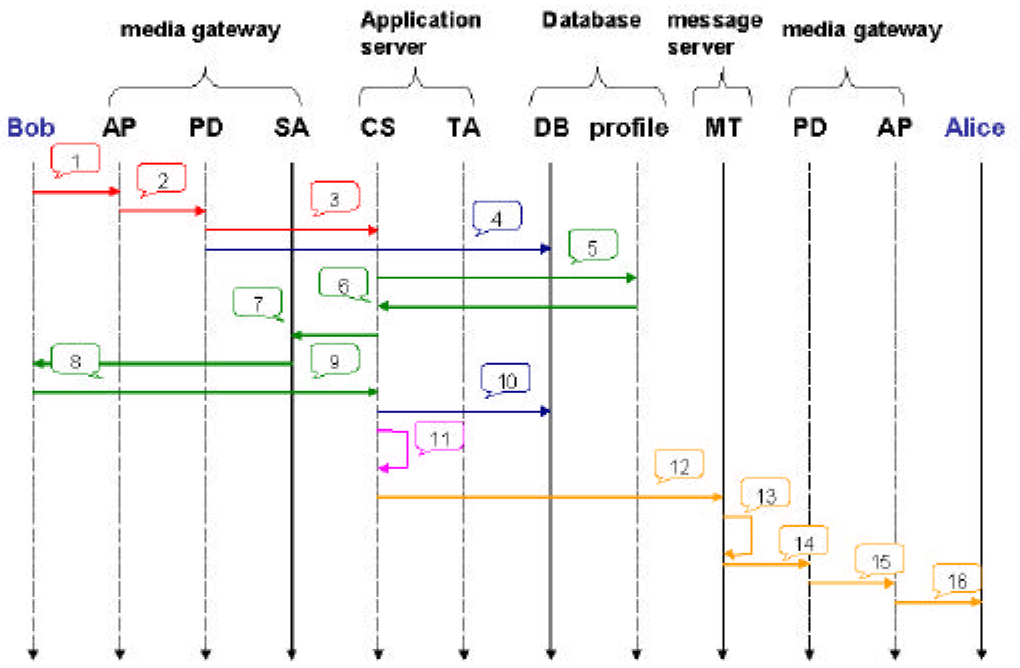

Figure 23: Delivery diagram for scenario 1

Analysis of communication environment: (11) (shown in pink in Figure 23)

Since E-mail is a Messaging Service, it can be delivered even the device is not in range. So the call path can be determined.

Message translation and delivery: (12, 13, 14, 15,16) (shown in yellow in Figure 23)

The Message Server's Translator will translate the voice message into text after receiving the request from CS.

Media Gateway will do the protocol mapping and deliver text message to the access network connected to the recipient.

Two extra steps: (4,10) (shown in blue in Figure 23)

Step 4 is to store the message to the Database (4).

Step 10 is to generate a message log and store it.

5.10.2 Scenario 2:

Alice wants to send her colleague Bob an urgent E-mail. Bob currently is at the company's out branch, which is in another city for a week. So he registers that he prefers all the messages of his working persona be delivered to his office phone in this branch. Bob might also define that any message that marked as urgent should try his mobile phone too, but he should have a chance to decide if he wants to receive it.

Alice's marks her E-mail as highest priority, which means that message must be delivered on time.

When this message arrives, Bob is unfortunately out for dinner but has his mobile phone on him.

Acceptance and protocol mapping:

After authenticating Alice is a legal user of our system, Access Point will accept the E-mail message from her. Then mapping the access point signal with the system standard.

Evaluation:

The Application Server maps this E-mail to Bob's office persona, evaluates the message delivery profile generated by the Message Server to create the delivery path, which means that the message will be delivered to a landline phone.

Analysis of communication environment:

Because the landline phone does not provide the in range indication to our system, the application server will setup the call from our system to an AP which is connected to a PSTN access network to dial Bob's office phone number. This phone is not in range (no one will answer the phone after it rings). So the system will try the same call path for several times (the number is defined in the OAM server). If it still fails, it will generate a bounce message in the message log.

But because this message must be delivered, the system will try to re-evaluate the profiles and get the new path.

Re-evaluation and re-analysis:

System will re-evaluate the message, this time setting up the call to Bob's mobile phone. The mobile phone is a kind of device that can provide feedback to our system if it is within range, so after re-analysis of the communication environment, it will know that mobile phone is ready for receive message.

Message translation and delivery:

Bob is asked to decide whether he will receive the message on his mobile, so a SMS message which is a message arrival notification will be sent to Bob's mobile phone. This SMS should include the subject of the message so that Bob can make the decision to receive the information.

After Bob gets this notification, he can give feedback to our system by pressing button "1" which means "get the message by using SMS message", pressing button "2" to "get the message by mobile voice", or pressing button "3" to "save the message in the message box", waiting for him to receive it later.

After Bob makes his choice, Message Server will perform message translation, either translates the E-mail to SMS message or under the help of the Assistant Server's TTS function, translates the E-mail to voice. It then delivers them to Bob's mobile phone.

If Bob press "3", the Message Server will save Alice's message to the Message Storage, waiting for Bob to retrieve it. Bob could use any kind of kind of device to retrieve that message sometime later.

6 Persona management

From the introduction of high level system structure and the scenarios we illustrated in last chapter, we have shown how our fifth generation messaging system solves the "translation problem" and "redirection problem".

Another important problem our fifth generation messaging system was attempting to solve was the "persona problem".

Solving the "persona problem" is a kind of privacy protection. Privacy has long been considered a fundamental human right in society. With the rapid advancement and globalisation of messaging system, the right to privacy is becoming an increasingly difficult concept to sustain. The nature of the messaging system, where personal information can be digitally transferred has lead to the situation where privacy issues are being threatened on a large and systematic scale.

In this chapter, personal data privacy within messaging systems is highlighted. We will discuss how the fifth generation messaging system solves those issues by using a "persona management model".

6.1 User privacy and privacy risks

6.1.1 User privacy

Users want their privacy to be protected in a messaging system. Roger Clarke defined privacy as:

> *Privacy is the interest that individuals have in sustaining a "person space", free from interference by other people and organisations. [Clarke, R. 2001]*

Drilling down to a deeper level, he said, privacy turns out not to be a single interest, but rather has several dimensions**:**

- *privacy of the person***,** sometimes referred to as "bodily privacy" This is concerned with the integrity of the individual's body. Issues include compulsory immunization, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilization;

- *privacy of personal behaviour***.** This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as “media privacy”;

- *privacy of personal communications*. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organizations. This includes what is sometimes referred to as “interception privacy”;

- *privacy of personal data***.** Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy'.

Except for the *privacy of the person,* which means the “bodily privacy” here, the “Persona problem” defined in Chapter 1 is associated with all the other three privacies.

6.1.2 Privacy risks

Privacy risks in a messaging system can be:

- *Profiling* means building the preferences, activities and characteristics of users by data-mining message log files.

  For example, by analysis of the logs known by the messaging systems message log, a user’s record can be collected without the user’s knowledge. The record might be reading, shopping, and entertainment habits, where they always go, what they always do, etc.

This risk can be avoided by improved database security, which we will not discuss in this thesis.

- *Tracking* is the building of the preferences, activities and characteristics of the users by monitoring the system traffic.

  A system that keeps track of how a person is reachable and distributes that information without limits could be used to deduce the person's location and compromise his privacy. Ideally, people should be able to receive messages anywhere, without revealing their whereabouts to the entire world. The trend of eavesdropping is making use of such information now.

  For instance, data on who sends a message to whom, and when, and tracing information with each message that sender ask for, are increasing by being collected and maintained by systems. If eavesdroppers, or even recipients get such information, the pattern of the user’s relationships is laid bare, and the customer’s business secrets may be obtained by analysis of the messages. Also, by monitoring an opponent’s traffic in order to find out where they are at a particular time, may give away commercial secrets.

  Tracking risks can be avoided by applying our persona management model.

  The goal of profiling and tracking is to have the most complete picture of the user.

- Spamming means receiving unwanted messages, it is another type of invasion of privacy. Many messaging services have no way to deliver messages unintrusively. For example, most telephones can either ring or not ring when a call arrives, instead of ringing for some callers and taking a message for others, or ringing during the day and taking a message at night. Users should be able to have all their incoming communications prioritized and filtered on their behalf.

6.2 Persona management model

Persona management is something we do in normal conversation everyday when we decide on what to tell one another about ourself. Each person considers the conversation context and the persona s/he is currently acting in as well as the respective relationship to the communication partners.

In this section we will describe how our fifth generation messaging system performs the persona management. First, let's see the different identities in our persona management model. Second, we will examine what the definition of persona is.

6.2.1 Identities in persona management:

The Webster English Dictionary describes the word identity as: [Webster 1988]

1) *the condition or fact of being the same or exactly alike (sameness, oneness);*

2 a) *the condition or fact of being a specific person or thing (individuality);*

b) *the condition of being the same as a persona or thing described or Claimed*

In the messaging system, the aspect of identity as proving to be a specific person is more important that the aspect of identity defined by all the information that describes a specific person in the real word.

We define four kinds of identities in our persona management model.

- UID (Universal identity): It is unique to each customer and has long duration. System routinely uses it essentially for identifying data such as the user's name, PID repositories, and mail list etc.
- PID (Personal identity): System uses this to verify customers. Each customer might have several PIDs. For example, using E-mail, the PID can be X.509 certificated. For the telephone service, maybe PIN.

- DID (Device identity): System uses the DID to verify the transport devices that the customer may be using. E.g. using Fax to send message, the DID can be the telephone number of that Fax line; using E-mail, the DID can be E-mail address.

- TID (Temporary identity): it is "one- time -use" pseudonym. It will be used within the system to verify messages used by validated customers.

6.2.2 Digital persona

In Jungian psychology [Jung, C. 2002], the *anima* or *animus* is the inner personality, turned towards the unconscious, and the *persona* is the public personality that is presented to the world. The persona that Jung knew was that based on the physical appearance and behaviour.

With the increased data-intensity in the second half of the twentieth century, we supplement Jung's persona, to some extent even replaced in this thesis, by the summation of the data available about an individual.

Definition

The digital persona is a construct, i.e. a rich cluster of inter-related concepts and implications. As a working definition, in this thesis we adopt the following meaning:

> *the digital persona is a model of an indiv idual's public personality based on data created and maintained by the individua , and intended for use as a proxy for the individual.*

Which means that the information sent to a recipient is actually sent to his persona. The ability to create a persona may be mainly vested in the recipient.

Representation

The User's PID plus their DID determines their persona. Recipients can define their messages to belong to which of their persona's by using any combination of the message sender's and recipient's PID and DID. Shown in Figure 24

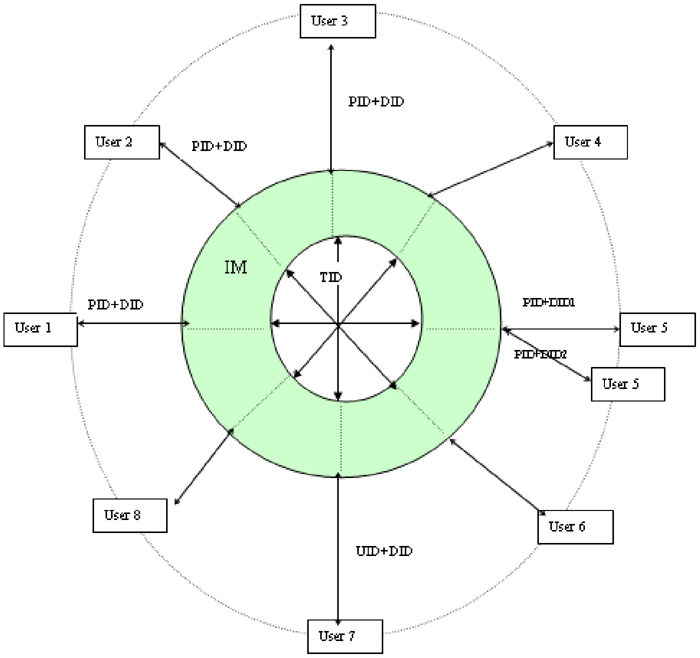

Figure 24: Identities in the 5th generation messaging system

For example, Alice can classify an E-mail message from the PID belonging to the company as her work persona, and a voice message from the sender who have a special PIN number as belonging to her family persona.

Alice may select two PINs, assigning PIN-A to her family number, PIN-B to her colleague. She can define that the messages coming from PIN-A (a person who hold this number) to her telephone (with DID) to belong to her family persona; but the message from PIN-B to Alice's same telephone to belong to her work persona.

A recipient will define several persona belong to himself, the meaning of a digital persona is determined by the recipient based on their own processing rules, and likely to gather different set of data about him.

6.2.3 Three major functions in persona management model:

- Identity administration: is the provisioning and maintenance of individual identities. Combats misuse of identities. E.g. issues certificate for the customer.

- Identity integration: focuses on the connection and cooperation of multiple identity repositories. E.g. the relationship between the PID and UID (Universal identity).

- Community management: addresses the connection and security relationships between identities e.g. convert PID (pseudo identity), UID, DID into TID (temporary identity), and vice versa as desired. Keep the records for the relationship between TID and PID, UID and DID.

6.3 Privacy protective services in our messaging system

6.3.1 Authentication

Authentication "is the most essential of all the security services because reliable authentication is needed to enforce access control, to determine who is authorised to receive or modify information, to enforce accountability, and to achieve non-repudiation" [Ford W. Baum M S. 1997].

In his book Rolf Oppliger said:

> *In general, authentication refers to the process of verifying the claimed identity of principal. Authentication results in authenticity, meaning that the verifying principal (verifier) can be sure that the verified principal (claimant) is the one he or she claims to be. [Oppliger, R. 1996]*

Oppliger divides the techniques that are used for authentication into three categories, depending on whether a technique is based on:

- Something the claimer knows (proof by knowledge)
- Something the claimer possesses (proof by possession)
- Some biometric characteristics of the claimer (proof by property)

Examples for the first category are personal identification numbers (PIN), passwords, whereas examples for the second category are keys, identification cards, and other physical devices or personal tokens. Biometric characteristics that were used for authentication can be fingerprints, facial images, and voice patterns.

6.3.1.1 Something the claimer knows

Password-based authentication

Passwords (in combination with user names) have been the mainstay of identity authentication systems since multi-user information systems came into being.

Unfortunately, password-based authentication systems have several drawbacks. They are one of the least secure techniques available. Some of the threats to password-based authentication are:

- External disclosure
- Guessing
- Communications eavesdropping
- Replay attacks

Password authentication systems are so notoriously insecure that they are nearly always combined with other methods of identity authentication.

Password-based authentication is a kind of Challenge-response authentication, which also known as CHAP (Challenge-Handshake Authentication Protocol) [TechTarget]. So that after a connection is made, the verifier sends a challenging message to the connection claimer, the claimer responds with what he knows, what he owns and what is, the verifier checks the response by comparing it with the information he has, if they match, the authentication is acknowledged; otherwise the connection is usually terminated.

Beside the password-based authentication schemes, in our fifth generation messaging system, we have another kind of authentication method, which is when both the calling parties are in agreement. We classify this kind of scheme belongs to something the claimer knows.

Rendezvous

This authentication method is not based on the techniques, but on the agreement between the two parties on the message delivery. Which means that the two parties agree to setup the call at a particular place and time.

For services that could not provide the authentication to support non-intercepting and non-repudiation, this is a supplement to perform security. For example, using Fax as the sending and receiving devices, the sender and receiver can negotiate the sending time.

6.3.1.2 Something the claimer possesses

Symmetric cryptographic-based authentication

The basic idea of a symmetric cryptographic- based authentication is that a claimant A proves his or her identity to a verifier B by performing a cryptogram operation of a quantity that either both know or B supplies. [Oppliger, R. 1996]

The cryptographic operation performed by A and B is based on a symmetric key. Such as the DES- or RSA-based authentication mechanisms.

Symmetric cryptographic-based authentication can be made more secure than password-based authentication. But problems can occur during the key distribution.

Physical tokens based authentication

Physical tokens are frequently used to enhance the security of identity authentication systems. For example, a physical storage token is used by banks to corroborate an account number (held on a magnetic stripe card) with a password (PIN).

Since IC (Intelligent Card), sometimes called "smart card", was born nearly twenty years ago, it has led a major role in use of physical tokens.

Password-based authentication, Symmetric cryptographic-based authentication and Physical tokens based authentication are all belong to Challenge-response authentication.

We say that the challenge-response authentication is a repudiative authentication scheme, for the knowledge about the secret to the verifier will be transferred. User can deny the services by complaining that someone pretended to be him.

Compared with the challenge-response authentication, Trust Third Party schemes authentication will be a non-repudiative authentication.

Trust Third Party authentication

Trust Third Party schemes authentication may provide even more powerful authentication mechanism. This techniques demand rather intensive mathematical computations, but present attractive features for the authentication. Such as non-repudiation.

Trusting third party is based on asymmetric cryptographic, which we also call it as PKI (public key infrastructure).

Strong asymmetric cryptography combined with secure hash functions allow the creation of a digital signature. Digital signatures verify that the sender of a message is in possession of a unique 'private' key and also verifies that the message has not been altered in transit.

We will not examine the technical details of this procedure in this thesis. For an excellent primer on every aspect of modern cryptographic techniques see the book "Applied Cryptography" [Schneier, B 1995].

As stated above, digital signatures verify that the sender of a message is in possession of a unique private key. In order to verify a message signed with a digital signature, the recipient needs a copy of the sender's public key. If the recipient knows the sender personally and can meet with them to exchange public keys, then a secure identity authentication system can be established.

But in our messaging system, messages between people or organizations in close physical proximity, with prior identity-trust relationships, are in the minority. It is therefore necessary to trust someone to provide recipients with public keys and to guarantee the association of the public key with some "chosen attribute".

This function is performed by a Certification Authority (CA), which issues digital certificates attesting to the connection between attribute and public key. In our fifth generation messaging system structure, the *Security control Server (SCS)* will do the CA's job. A standard X.509 Version 3 Digital Certification can be found in Appendix C.

Thus, a public key here is a proxy presence in cyberspace for some entity in physical space. It acts directly in cyberspace, just as the associated entity can act in physical space. Assuming that the person wishing to authenticate a cyberspace identity trusts his CA and assuming that the CA is operating securely and correctly, the only problem with public key infrastructure (PKI) based systems arises when the private key of a certified private-public key-pair becomes compromised. Private keys must be generated randomly, and stored and transmitted securely in order for the trust placed in the associated digital certificate to be deserved.

6.3.1.3 Biometric based authentication

Biometric techniques include fingerprint recognition, retinal scanning, hand-geometry scanning, and handwriting or voice recognition. These techniques are all, currently, extremely expensive to implement effectively and are therefore only worth considering in big-budget, high-security applications. As the drawbacks (including high cost, poor ergonomics, reliability, speed, and data storage requirements) are mitigated by improvements in technology, biometric techniques could emerge as the most secure method of automated identity authentication. [Kim H 1995]

6.3.2 Authentication services used in our system

In Table 40, we summarize the authentication services in the fifth generation messaging system. Descriptions of the services are in section 2.6.

	Something the claimer knows		Something the claimer possesses			Biometrics
	Password-based	Rendezvous	Symmetric cryptographic	Physical token	Trust third party	
PSTN	*	*				
GSM & CDMA		*	*	*		
SMS		*	*	*		
FAX	*	*				
WWW	*	*	*		*	
WAP		*	*		*	
E-mail	*	*			*	
IM	*	*				
PDA	*	*			*	

Table 40: Authentication services in the fifth generation messaging system

Biometrics authentication scheme will not be used in our fifth generation messaging system. However, rendezvous can be used in any kind of services in our system.

As discussed in section 6.2, a user's persona is determined by the PID, DID or PID plus DID in the fifth generation messaging system, so in order to analyze user's persona, sometimes we may need to authenticate both the PID and DID.

6.3.3 Anonymity

As discussed in [Pfitzmann and Waidner 1987], there are three types of anonymous communication properties that can be provided: sender anonymity, receiver anonymity, and unlinkability of sender and receiver.

- Sender anonymity means that the identity of the party who sent a message is hidden, while its receiver (and the message itself) might not be.

- Receiver anonymity similarly means that the identity of the receiver is hidden.

- Unlinkability of sender and receiver means that although the sender and receiver can each be identified as participating in some communication, they cannot be identified as communication with each other.

They are all being applied in the fifth generation messaging system. The other aspect of the anonymous communication is the *degree* of the anonymous. [Rubin A, Retiter M. 1998]

As shown in Figure 25 by Michael K. Reiter and Aviel D. Rubin, the degree of anonymity can be viewed as an informal continuum.

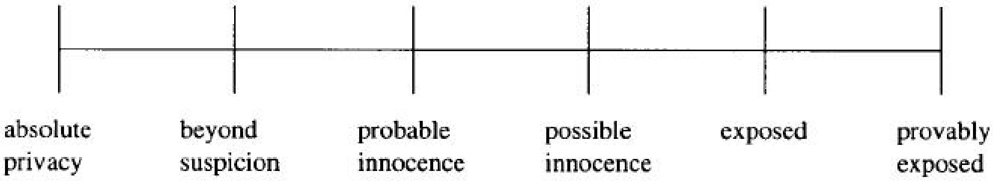

Figure 25: Degrees of anonymity [Rubin A, Retiter M. 1998]

For simplicity, we just describe this continuum with respect to sender anonymity, but it can naturally be extended to receiver anonymity and unlinkability as well.

Degrees range from absolute privacy to provably exposed. On one end of the spectrum is absolute privacy: absolute sender privacy against an attacker means that the attacker can in no way distinguish the situations in which a potential sender actually sent communication and those in which it did not. That is, sending a message results in no observable effects for the attacker. On the other end of the spectrum is provably exposed: the identity of a sender is provably exposed if the attacker cannot only identify the sender of a message, but can also prove the identity of the sender to others.

Michael K Reiter also described the beyond suspicion, probable innocence and possible innocence in his paper. But in out fifth generation messaging system, we will just use the absolute privacy, where the attacker cannot perceive the presence of communication, or provably exposed, where the attacker can prove the sender, receiver, or their relationship to others.

When user selects the absolute privacy, after the *authentication*, our system will use the TID to instead of the user's real identity during the communication, otherwise, user's real identity still applied.

6.4 Privacy protection by using persona management model

By using persona management, a user may decide whom to give the information to, when to act anonymously.

Persona management enables the user to chose the degree of anonymity, either being provably exposed or being absolute privacy.

Either the sender or the recipient selects that to have absolute privacy, After the successful authentication for the user and the recipient, our persona management in fifth generation messaging system will replace user's real PID and DID with a TID. During the transmission of the message, it will be the TID that is used to identify the user.

So by using the TID, the fifth generation messaging system can protect the user's location privacy and relationship privacy between the sender and recipient.

For the provably exposed anonymous degree, our system will not apply TID.

6.5 A solution to the Persona problem

The “persona problem” we defined in Chapter 1 has two aspects: *Non-interaction between different persona’s information* and *Self-handling the path for different persona’s information*

How our fifth generation messaging system solves the “persona problem”: by using the persona management model is shown as follows:

Non-interaction between different persona’s information

A recipient might not want one of his persona’s information to get involved into the other persona. He can define that the people who use one of his digital persona to login to the system can only check messages belong to that persona.

Look back to the examples we gave in Chapter 1. Alice has two personas, family and work persona. She do not want her colleagues to get involved with the family persona’s information, and also may not want her family members get involved with her work persona’s information.

Alice can define that the people who login to our system using a special PID can check only the information belonging to her work persona. Then distribute this PID to her colleagues.

Alice can also define that the people who login from the specific DID with a specific PID can check her family persona’s information.

Using Alice’s UID login to the system can modify her personal data, modify persona definition, and check the messages belonging to her all personas, etc.

Self-handling the path for different persona’s information

A recipient can self define a message from whom, where or to where, belongs to which of his persona. He can manage how to handle these messages (delete, redirect, must reach him etc).

Alice may define that the messages to one of her devices (with DID) and from whom (with PID) belong to her family persona, and must be delivered to her.

The “Persona problem” solution and the persona management model we represented here, is the new part in the fifth generation messaging system on top of the fourth generation.

We have introduced the solution of the four messaging system problems. But inside the fifth generation messaging system, there are still many issues that need consideration. The list of possible future works is detailed in Chapter 7.

7 Future works and conclusion:

7.1 Future works

In this thesis, we have presented our design for a fifth generation messaging system. There are still issues that we have not been discussed in this thesis. They are listed below.

Service Mobility: this refers to the seamless mobility across different devices in the middle of a service session. For example, shift from Instant Messaging to a telephone call during the same communication session.

Billing integration: "Enhanced services are not worth doing unless there is a way to bill for them" [Hua, C. Faggion, N. 1998]. In the future, we plan to look at billing issues that will alow us to build up a unique billing system integrating the fifth generation messaging system billing with the existing services network billing.

Full range of anonymity: in this thesis, we just discussed how persona management handles *absolute privacy* and *provably exposed* degree in anonymity. In the future, we plan to give the user full selection of the degree of anonymity.

Implementation: refers to the discussion of the scale of the tasks required to implement the system we specified. The fifth generation messaging system is a huge network that has numerous items not considered, mainly the method of implementing.

User interface: this refers to the various items to be defined by the user. Especially, for the persona management, the user needs to self manage a lot of PIDs and DIDs, for the redirection, the user needs to define numerous rules. We need to find easy ways to help users do this kind of self management.

Performance Evaluation: this refers to the performance and usability evaluation of the design. Especially with respect to scaling, latency, ease of new service development, and user satisfaction.

We expect that the results of considering above issues will drive the next iteration of the fifth generation messaging system designs, and will enlarge and complement our structure. A discussion of this system will never be completed so long as new technical devices are being introduced.

7.2 Conclusion

The fifth generation messaging system is a people-centric system that will make it convenient for users to deliver messages. Based on the state-of-the-art communication, computing and messaging technologies, we directed our system to achieve the target vision of an “anytime, anywhere, any-persona and from any-device” multi-services system.

In addition to proposing a fifth generation messaging system, we have presented four main problems to be addressed by any messaging system. We give an overview of the history and future of messaging systems, and a survey of existing messaging systems.

The fifth generation messaging system attempts to solve those four main problems –

- By solving the “Communication problem”, we satisfy users’ communication needs.
- By solving “redirection problem”, our system allows users to send and receive message “at anytime anywhere”.
- By solving the “translation problem”, we guarantee users can send and receive messages on “any device” without worrying about the other party’s device.
- By solving the “persona problem”, the fifth generation messaging system can protect user privacy.

We defined the feature framework in the messaging system, and also have identified the key components within this messaging system, and their corresponding functionality.

From our experiences with proposing and defining the fifth generation messaging system, we have come to believe that it is possible to build this system, but that a number of problems remain to be solved, and the implement effort will be large. We hope the road of developing a future fifth generation messaging system from the existing third generation is smooth.

Appendix A: Acronyms

ATM (asynchronous transfer mode) - is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. See § 1.1.3.

AOL (America Online) – is a company's name. See § 2.6.8.

CA (Certificate Authority) - is an authority in a network that issues and manages security credentials and public keys for message encryption. See § 6.3.2.

CDMA (Code-Division Multiple Access) - is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimising the use of available bandwidth. See § 1.2.3.

CDPD (Cellular Digital Packet Data) - is a specification for supporting wireless access to the Internet and other public packet-switched networks. See § 2.6.6.

CRL (Certificate revocation list) - Certificate Revocation List (CRL) is one of two common methods when using a public key infrastructure for maintaining access to servers in a network. See § 5.7.3.

CTI (Computer Telephone Integration) – is a mechanism to allow an application to control the operation of the telephone network (e.g. for call setup from a directory, or automatic routing to an available agent, or "screen popping" to tell the recipient of a call information about the caller). Typically this is performed either via over a serial cable connecting the server to the PBX, or via a board in the server that connects to a digital port on the PBX. See § 5.4.3.

DID (Direct Inward Dialling) - is a service of a local phone company that provides a block of telephone numbers for calling into a company's PBX (private branch exchange) system. Using DID, a company can offer its customers individual phone numbers for each person or workstation within the company without requiring a physical line into the PBX for each possible connection. See § 3.1.2.

E-mail (Electronic Mail) – is an application of messaging which moves text messages (plan or with some associated formatting) and file attachments between two users, or an application and a user. See § 2.6.7.

ESN (Electronic Serial Number) - is a 32-bit number assigned by the mobile station manufacturer which uniquely identifies the mobile station equipment. See § 2.6.2.

FoIP (Fax over IP) - is fax delivered using the Internet Protocol. See § 2.6.4.

FTP (File Transfer Protocol) - a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. See § 2.6.5.

GSM (Global System for Mobile Communications) - GSM is one of the leading cellular phone systems and the de facto standard in Europe and Asia. See § 2.6.2.

GUI (Graphical User Interface) - A GUI is a program interface that takes advantage of computer graphics to make the program easier to use. Characteristics of many GUIs under the Microsoft Windows platform are pointers, icons, windows, and menus. See § 5.9.1.

HTML (Hypertext Markup Language) - is the basic language used to create Web pages for access from a Web browser. HTML can represent content (such as text to be displayed), hold links to other content (hyperlinks) and act as a container for other objects (e.g. JavaScript and other active programs). See § 2.6.5.

HTTP (Hypertext Transfer Protocol) - is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. See § 2.6.5.

IM, IMing (Instant messaging) – is a mechanism for sending short text messages immediately between two Instant Messaging clients. The use of real time communications between the two clients means that the message is displayed as soon as the sender has finished typing it. See § 2.6.8.

IMAP (Internet Message Access Protocol) - IMAP is a protocol for retrieving email messages. Similar to POP, but having additional features, IMAP uses SMTP to communicate between the e-mail client and server. See § 5.4.2.

IMSI (International Mobile Subscriber Identity) - is a decimal number used to uniquely identify personal mobile stations. See § 2.6.2.

IP (Internet Protocol) - is the method or protocol by which data is sent from one computer to another on the Internet. See § 1.2.1.

IRC (Internet Relay Chat) - is a system for chatting that involves a set of rules and conventions and client/server software. See § 2.6.6.

IrDA (Infrared Data Association) - is an industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. See § 2.6.9.

IVR (Interactive Voice Response) - is a traditional CTI application which allows users on the telephone to enter DTMF tones to retrieve information, which might then be read to them, faxed to them, etc. Most unified messaging solutions for the telephone network have associated toolkits to allow you to extend the facilities offered to callers to include most traditional IVR functions. See § 5.4.3.

LAN (Local Area Network) - is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). See § Abstract.

MIME (Multipurpose Internet Mail Extensions) - MIME is a specification for formatting non-ASCII messages so they can be sent over the Internet. See § 2.6.7.

MIN (Mobile Identification Number) - is a 34-bit number that is derived from the 10-digit directory telephone number assigned to a mobile station. See § 2.6.2.

MPA (Mobile People Architecture) - The MPA is a research project at Stanford University. Their system, Calliope, is a UCS that is being developed. See § 3.6.

MUA (Mail User Agents) - is the software that allows a user to access and manage e-mail, including reading, composing, disposing, printing and displaying e-mail messages. See § 2.6.7.

MTA (Mail Transfer Agent) – is the program responsible for receiving incoming e-mails and delivering the messages to individual users. See § 2.6.7.

NMT (Nordic Mobile Telephone) – is the first to introduce cellular services for commercial use in 1981. See § 2.6.3.

OCR (Optical Character Recognition) - is the recognition of printed or written text characters by a computer. See § 2.6.4.

OSI (Open Systems Interconnection) - is a standard description or “reference model” for how messages should be transmitted between any two points in a telecommunication network. See § 2.2.2.

PBX (Private Branch eXchange) - is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of externa l phone lines. See § 3.1.

PC (Personal Computer) - is a computer designed for use by one person at a time. See § 1.2.

PDA (Personal Digital Assistant) - Also known as a palmtop, a PDA is a small computer that literally fits in a palm. The last couple years have seen palm PDA's that support colour, sound, and an Internet connection. See § 2.6.9.

PDC (Personal Digital Cellular) – is a second-generation wireless service which uses a packet-switching technology. Messages are split into packets of data for transmission, then reassembled at their destination. PDC is widely used in Japan. See § 2.6.3.

PIM (Personal Information Manger) – is a type of software application designed to help users organize random bits of information. See § 3.1.2

PIN (Personal Identity Number) - is a personal identification number. See § 1.2.4.

PKI (public key infrastructure) - enables users of a basically insecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. See § 6.3.

POP (Post Office Protocol) - POP is a protocol used to retrieve e-mail and is similar to the newer IMAP, and also requires SMTP when sending messages. See § 2.6.7.

POTS (Plain Old Telephone Service) - is a term sometimes used in discussion of new telephone technologies in which the question of whether and how existing voice transmission for ordinary phone communication can be accommodated. See § 2.6.1.

PSTN (Public Switched Telephone Network) - PSTN refers to the international telephone system based on copper wired carrying analog voice data. Most household phones are linked to a PSTN. See § 2.6.1.

QoS (Quality of Service) - is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance on the Internet and in other networks. See § 5.9.

SIM (Subscriber Identity Module) - When you purchase your GSM phone from your provider, a SIM card is installed in your phone. The SIM card contains a computer memory chip that keeps track of your phone number, the services you have ordered from your network provider, your phone book information, and other network security related information. See § 2.6.2.

SMTP (Simple Mail Transfer Protocol) - SMTP is a protocol for sending e-mail messages between servers. Most e-mail systems use SMTP over the Internet when sending messages from one server to another. Both IMAP and POP use SMTP. See § 2.6.7.

SMS (Short Message Service) - is a service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (**GSM**) communication. See § 2.6.3.

TMSI (Temporal Mobile Subscriber Identity) - In a GSM system, the TMSI is used by the VLR to protect the user's identity. See § 2.6.2.

TTS (Text To Speech) - The conversion of a piece of text, such as an E-mail, into an audible form which can be played down the telephone to the caller. Advanced TTS applications should automatically recognize the language used (when it is not explicitly indicated) and identify the use of acronyms (such as IBM) versus words (such as Lotus). A TTS process for use with e-mail should also strip the e-mail headers which the user does not wish to hear, understand the structure of messages (e.g. a reply with the original message attached, or embedded as a quote, or a meeting notice within an e-mail) and support common E-mail “emoticons” (such as “:-)”) and abbreviations (such as IMHO for “in my humble opinion”). See § 3.1.

TUI (Telephony User Interface) – is a server application which connects through a telephony board to a PBX or the PSTN to receive telephone calls, interact with the user, and implement voicemail on top of the messaging infrastructure. Three basic applications are provided by a TUI: The Auto Attendant, which takes voicemail messages from external callers, the Voicemail Application, which allows users to interact with their electronic mailbox via the telephone, and Call Control, which allows PC users to control their physical telephone via a PC interface (e.g. requesting that a voice message in the e-mail client is played to them via the telephone). See § 5.9.1.

UHF (Ultra-High-Frequency) - range of the radio spectrum is the band extending from 300 MHz to 3 GHz. See § 2.6.2.

UMS (Unified Messaging System) - UMS is the handling of voice, fax, and regular text messages as objects in a single mailbox that a user can access either with a regular e-mail client or by telephone. See § 3.1.

URL (Uniform Resource Locator) - is the address of a file (resource) accessible on the Internet. See § 2.6.5.

VoIP (Voice over IP) - is voice delivered using the Internet Protocol is a term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). See § 1.2.3.

VPIM (Voice Profile for Internet Messaging) – is a standard protocol allowing one voicemail server to forward voicemail messages to another over the Internet or a corporate intranet. The current standard is version 2 (v2). See § 3.1.

W3C (World Wide Web Consortium) – is an international consortium of companies involved with the Internet and the Web. See § 2.6.5.

WAP (Wireless Application Protocol) - is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC). See § 2.6.6.

WAN (Wide Area Network) - is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network. See § Abstract.

WML (Wireless Markup Language) - formerly called HDML (Handheld Devices Markup Languages), is a language that allows the text portions of Web pages to be presented on cellular telephones and personal digital assistants (PDAs) via wireless access. See §2.6.6.

WWW (World Wide Web) - is all the resour ces and users on the Internet that are using the Hypertext Transfer Protocol. See § 2.6.5.

XML (Extensible Markup Language) is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere. See §2.6.6.

Appendix B: Trademark

PhoneSoft® is trademark of Active Voice

WIN Series® is trademark of Digital Speech Systems, Inc.

Interchange ® is trademark of Key Voice Technologies

CallPilot® and Meridian® are trademarks of Nortel Networks

CommWorks 8250® is the trademark of CommWorks Corporation

iPulse® is a trademark of LM Ericsson AB

AnyPath® is a trademark of Lucent, Octel messaging

AIM® is a trademark of America Online

Appendix C: X.509 Version 3 Digital Certificate

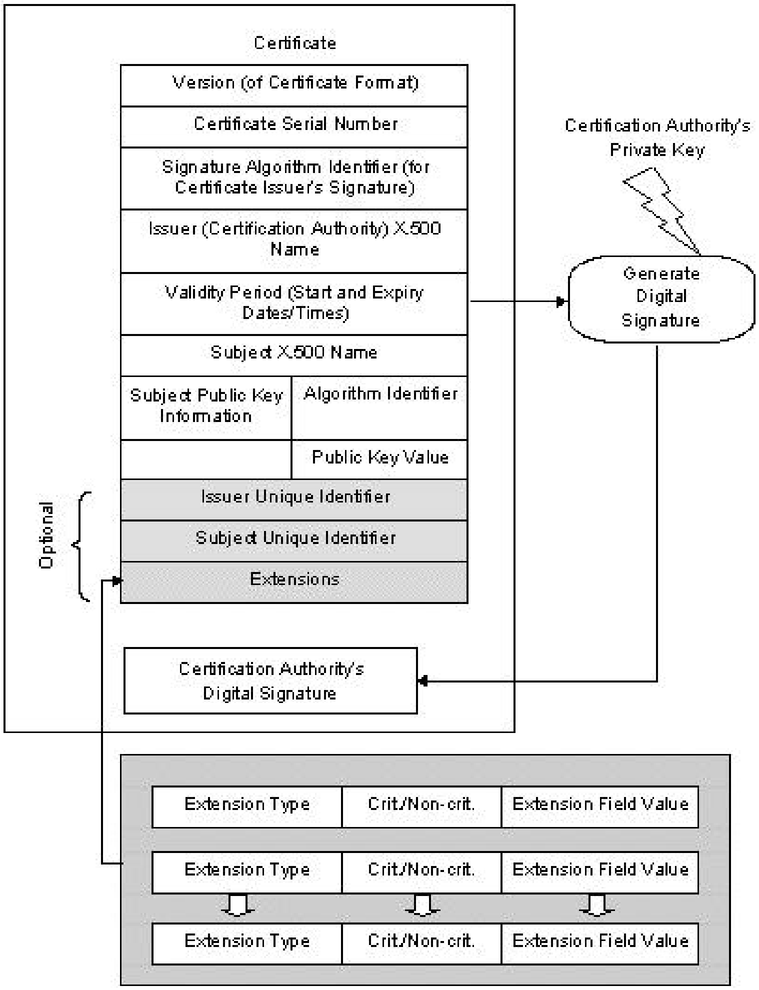
Certificate
Version (of Certificate Format)
Certificate Serial Number
Signature Algorithm Identifier (for Certificate Issuer's Signature)
Issuer (Certification Authority) X.500 Name
Validity Period (Start and Expiry Dates/Times)
Subject X.500 Name
Subject Public Key Information
Algorithm Identifier
Public Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Optional
Certification Authority's Private Key
Generate Digital Signature
Certification Authority's Digital Signature
Extension Type
Crit./Non-crit.
Extension Field Value
Extension Type
Crit./Non-crit.
Extension Field Value
Extension Type
Crit./Non-crit.
Extension Field Value

Figure 26: X.509 Version 3 Digital Certificate

Bibliography:

[AOL 2002] *AOL Instant Messenger.* [WWW Document] URL http://www.aim.com/index.adp (visited 2002, 16 Feb).

[Aura, T 1997] *Strategies Against Replay Attacks.* Proceedings of the 10th IEEE Computer Security Foundations Workshop, pages 59--68, 1997. URL http://citeseer.nj.nec.com/aura97strategies.html

[Bigskytech 2002] *Remark UM Data Sheet.* [WWW Document] URL http://www.bigskytech.com/d_RemarkUMDataSheet.pdf (visited 2002, 16 Feb).

[Appenzeller, G., Lai, K., Maniatis, P., Roussopoulos, M., Swierk, E., Zhao, X., Baker, M. 1999]

The Mobile People Architecture. Technical Report CSL-TR-99-777, Computer Systems Laboratory, Stanford University, January 1999. Online at URL http://mosquitonet.stanford.edu/publications/CSL-TR-99-777.ps (visited 2002, 16 Feb).

[Berthold, O. Kohntopp, M 2000] *Identity Management Based on P3P.* Anonymity 2000, Lecture Note of Computer Science, LNCS 2009,pages 141-160, 2001.

[Bocker, P. 1988] *ISDN: The Integrated Services Digital Network.* Berlin, Springer-Verlag.

[Chaum, D 1985] *Security Without Identification: Card Computer to Make Big Brother Obsolete,* Communications of the ACM, Vol. 28 No. 10, pages 1030-1044.

[Chesnais, P. R. 1997] *Canard: A framework for community messaging.* Proceedings of the First International Symposium on Wearable Computers, Cambridge, MA, IEEE, New York, October 1997, pages 108-115.

[Chesnais, P. R. 1999] *A Framework for Designing Constructionist Approaches to Community-Centered Messaging.* Ph.D. thesis, Massachusetts Institute of Technology.

[Clarke, R. 2001] *Roger Clarke's Privacy introduce and definitions*. [WWW Document] URL http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (visited 2002, 16 Feb).

[Geist, M 1998] *A Brief Introduction to C. G. Jung and Analytical Psychology* [WWW Document] URL http://www.cgjungpage.org/articles/geist1.html (visited 2002, 16 Feb).

[Hopcke, R. H. 1989] *A guided tour of The Collected Works of C. G. Jung.* Boston and London, Shambala.

[Hua, C. Faggion, N. 1998] *Personal communication services through the evolution of fixed and mobile communication and the intelligent network concept.* IEEE Network (Jul/Aug).

[ICQ] *ICQ - World's Largest Internet Online Communication Network* [WWW Document] URL http://www.mirabilis.com/ (visited 2002, 16 Feb).

[Information and Privacy Commissioner, Registratiekamer 1995] *Privacy-Enhancing Technologies: The path to Anonymity;* By Information and Privacy Commissioner/Ontario Canada, and Registratiekamer The Netherlands, Augest 1995, URL http://zedz.net/mirror/privacy/p2.index.html (visited 2001, 16 Apr)

[Kim H 1995] *Biometrics – Is it a viable proposition for identity authentication and access-control.* Computers & Security Vol. 14, No. 3: pages 205-214.

[Jung, C. 2002] [WWW Document] URL http://oldsci.eiu.edu/psychology/Spencer/Jung.html (visited 2002, 16 Feb).

[Kinnard, S. 1999] *Marketing With E-Mail: A Spam-Free Guide to Increasing Awareness, Building Loyalty, and Increasing Sales*, Maximum Press.

[Lais, S. 2001] *Analysis: Will wireless tech erode privacy?* [WWW Document] URL http://www8.cnn.com/2001/TECH/internet/02/21/future.privacy.idg/index.html (visited 2002, 16 Feb).

[Mobile Streams Ltd, 2002] *Introduction to Unified Messaging*. [WWW Document] URL http://www.unifiedmobile.com/whatis.asp (visited 2002, 16 Feb).

[Marti, S. 1999] *Active Messenger: E-mail Filtering and Mobile Delivery*, Master thesis, Massachusetts Institute of Technology.

[Marx, M. 1996] *CLUES: Dynamic Personalized Message Filtering.* Proceedings of Computer Supported Cooperative Work, ACM, New York, 1996, pages 113-121.

[Oppliger, R. 1996] *Authentication System for Secure Networks*, Artech House, INC.

[OZ] *iPulse homepage* [WWW Document] URL http://www.oz.com/ipulse/help/mainwnd.html (visited 2002, 16 Feb).

[PDA] [WWW Document] URL
Plam Inc, http://www.palm.com/support/ (visited 2002, 16 Feb).
Hewlett-Packard company, http://www.hp.com/country/us/eng/support.htm (visited 2002, 16 Feb).

Handspring,
http://support.handspring.com/esupport/start/hsWelcome.jsp
(visited 2002, 16 Feb).

[Pfleeger, C. P. 1997] *Security in Computing,* Prentice Hall PTR.

[RFC 821] *SMTP (Simple Mail Transfer Protocol) RFC 821,* Information Sciences Institute University of Southern California

[RFC 1939] Post Office Protocol - Version 3 *RFC 1939,* Network Working Group

[RFC 1521, 1522] *MIME RFCs 1521 and 1522* URL
http://www.oac.uci.edu/indiv/ehood/MIME/MIME.html
(visited 2002, 16 Feb)

[Rubin A, Retiter M. 1998] *Crowds: anonymity for Web transactions.* ACM Transactions on Information and System Security Volume 1 Issue 1: Pages 66-92.

[Ford W. Baum M S. 1997] *Secure Electronic Commerce: Building the infrastructure for digital signatures and encryption*. Prentice Hall, Inc. New Jersey.

[Schmandt, C. 1993] *Phoneshell: The Telephone as Computer Terminal.* Proceedings of the ACM Multimedia Conference, Anaheim CA, ACM New York, pages 373-382.

[Schneier, B 1995] *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition.* John Wiley & Sons.

[Suler, J. 2000] *In The Psychology of Cyberspace.* [WWW Document] URL
http://www.rider.edu/users/suler/psycyber/identitymanage.html
(visited 2002, 16 Feb).

[Syverson, P. 1994] A *Taxonomy of Replay Attacks.* Proceedings of the Computer Security Foundations Workshop VII, pages 131-136.

[TechTarget] [WWW Document] URL http://www.whatis.com (visited 2002, 16 Feb).

[TIA/EIA 1999] *Short Message Service for Spread Spectrum Systems*. TIA/EIA-637-A-99.

[UMS 2002] [WWW Document] URL
Active Voice,
http://www.activevoice.com/products/phonesoft/index.html
(visited 2002, 16 Feb).
Key Voice, http://www.keyvoice.com/platforms/index.html
(visited 2002, 16 Feb).
Digital Speech, http://www.digitalspeech.com/index1.htm
(visited 2002, 16 Feb).
Nortel Networks,
http://www.nortelnetworks.com/products/01/callpilot/index.html (visited 2002, 16 Feb).
3Com Corporation,
http://www.commworks.com/Enhanced_Services/IP_Messaging/CommWorks_8250/ (visited 2002, 16 Feb).

[Meer, S. Arbanowski, S. Magedanz, T. 1999] *An Approach for 4th Generation Messaging System*. IEEE, Autonomous Decentralized Systems, 1999. Integration of Heterogeneous System proceedings, The Fourth International Symposium, pages 158-167.

[W3C] *About The World Wide Web.* [WWW Document] URL http://www.w3.org/WWW/ (visited 2002, 16 Feb)

[Webster 1988] *Webster's New World Dictionary of American English.* Third College Edition, Cleveland : Webster's New World, 1988.

[WordNet 2002] *WordNet Online* [WWW Document]. URL http://www.cogsci.princeton.edu/cgi-bin/webwn1.7.1?stage=1&word=persona (visited 2002, 16 Feb).