Migration / Evolution of security towards wireless ATM

D Patiyoot
Royal Thai Naval Academy
Department of Engineering
Sukhumvit Road, Tumbon Paknam
Ampher Muang, Samutprakran, 10270
THAILAND
Tel. + 66 2 4753992
E-mail : taharnmoo@yahoo.com

Abstract

This proposal aims to outline possibilities for the migration[1], evolution[2] path from second-generation systems (GSM) to wireless ATM regarding security aspect.

Some of the factors and parameters of security affecting the migration path towards wireless ATM are identified. Also expected, planned security features for wireless ATM is explained and compared to second generation cellular systems.

This work is done following the work of ASPeCT (Advanced Security for Personal Communications Technologies) in a similar manner.

1. Introduction

The need for security features in wireless ATM has led to the definition of specific objectives. These objectives have been translated into security requirements, resulting in a classification of security features. However, it is envisaged that the network-based migration process will be affected by introduction of B-ISDN.

The fundamental of migration/evolution path towards wireless ATM security is based on gradual enhancements and exploitation of the GSM infrastructure, thus maximising the use of existing network investments.Evolution (improvement or upgrade) of the GSM security features is done by implementing new, advanced security features into wireless ATM security one. In Section two, explained why migration is happened, Section three, parameter concerning of security migration were investigated. Section four, expected security features both in second generation and wireless ATM is detailed. Section five described with the objective of of security in wireless ATM. Finally, conclusions deduced from this paper are given in Section 6.

---

[1] Migration: Movement of users and/or service delivery from existing telecommunications systems to wireless ATM.

[2] Evolution: A process of change and development of a telecommunications system towards the capabilities and functionalities of wireless ATM.

2. Migration Scenario

2.1 Factors for Migration

Migration scenarios can be defined based on:

2.1.1 Use of B-ISDN in the core network.

2.1.2 The introduction of the wireless ATM radio interface.

2.1.3 In order to facilitate the transition towards wireless ATM deployment, it should be possible to provide wireless ATM services which contains components of fixed networks and second-generation cellular system, forming an integrated system infrastructure. This means that the various services and (security-related) features which are to be supported within wireless ATM must allow for both forwards compatibility and backwards between wireless ATM and second-generation cellular system and fixed ATM.

2.2 Process of migration

The security migration aspects can be looked at in various stages of process.

2.2.1 Additional security features that could be supported the system.

2.2.2 Appropriate security mechanisms for those security features.

2.2.3 Identify interfaces and protocols for relevant security.

3. Security Migration Related Aspects

This section is to identify the parameter that could affect the GSM network-based migration path towards wireless ATM also provide a framework for the migration of security offered by second generation towards wireless ATM security.

3.1 Involved Entities

The entities involved in the migration process are (see Figure 1):

- SIM
- Mobile terminal equipment
- Access system[3]
- Core network, comprise of backbone network[4] and service network[5].

[3] Access system: provides the radio functions i.e. basic transmission and local switching functionality enabling access of mobile terminals to the fixed network resources via the radio interface.

[4] Backbone network: provides the basic fixed network switching infrastructure and network resource i.e., call and connection control

[5] Service network: provides for data storage, data handling and processing of service requests from mobile users.

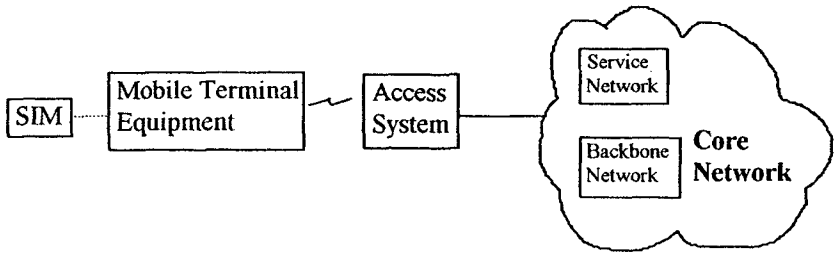

Figure 1 The Entities involved in the migration process

SIM TYPE	TERMINAL TYPE	ACCESS SYSTEM	SWITCHING NETWORK	SERVICE NETWORK
GSM	GSM MS	BTS ⊕ BSC (GSM)	MSC/VLR	HLR (GSM)
Wireless ATM	Wireless ATM MT	BS	ATM switching /VLR	HLR

Table 1: Possible evolution of entities involved in the migration process

⊕ : means connected to
/ : means and/or

Table 1 depicts the possible evolution of entities depicts in Figure 1. The characteristics of those are described below:

A. SIM

The SIM evolution considers the development of GSM SIM to meet the requirements of new wireless ATM users. SIM might also be used in fixed terminals to allow for personal mobility.

B. Mobile Terminal

From single-mode GSM terminal to single-mode wireless ATM terminal, the migration has to be done.

C. Access System

Prior to the introduction of the wireless ATM BS access system, GSM system must be declared and met. Access to the GSM services is supported via BTS and BSC. New wireless ATM BS have to be investigated in order to support the use of ATM.

D. Core Network

The GSM core network functionality will be gradually upgraded so as to meet the wireless ATM requirements. The enchantments involve both the GSM MSC/VLR and the GSM HLR/EIR. ATM switching might replace GSM MSC.

E. Service and Features

The set of services and features offered nowadays by the existing GSM systems will be further developed into serving ATM service such as videotelephony, multimedia, broadband data service,etc.

3.2 Framework for the security migration

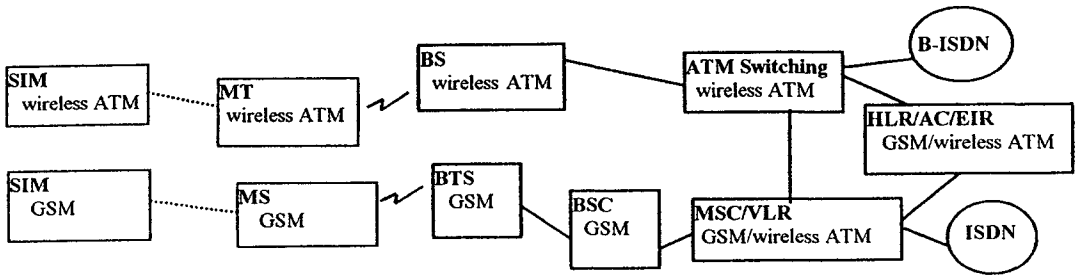

Figure 2 *Framework for the security migration*

In figure 2, framework of security migration is shown. It fulfils the wireless ATM requirements. SIM card for wireless ATM MT (Mobile Terminal) is produced. Wireless ATM radio interface was introduced by using BS (Base Station) which also connected to new switching system. The MSC is replaced by ATM switching, to support B-ISDN, but still using the VLR facility. HLr/AC/EIR still using the one that GSM used.

4. Expected Security Features

4.1 GSM

GSM security features are standardised in GSM 02.09[2]. It consists of

- **Subscriber identity confidentiality**
- **Subscriber identity authentication**
- **User data confidentiality on physical connections**
- **Connectionless user data confidentiality**
- **Signalling information element confidentiality**

4.2 Wireless ATM

Wireless ATM features are expected as follow:

- **Features mentioned in GSM**
- **Service providers/Network operators identity authentication**
- **Non- Repudiation of data**
- **Access control at the mobile terminal**
- **Data Integrity**
- **Key agreement**
- **Certificate**
- **Supplementary security features**

4.3 Selection of the Security Features

Table 2 presents an indicative, comparative list of the security features offered by the second generation mobile systems (GSM) and the expected for wireless ATM systems.

Security Features	GSM	Wireless ATM
Confidentiality		
User Traffic Confidentiality	y	y
User Identity Confidentiality	y	y
User Location confidentiality		y
Signalling Data confidentiality	y	y
Confidentially of Stored Data		y
Integrity		
User Traffic Integrity		y
User Location Integrity		y
Terminal Location Integrity		y
Signalling data Integrity		y
Integrity of stored data		y
Authentication		
Authentication of SP to User		y
Authentication of User to SP		y
User Identity Authentication	y	y
Authentication of terminal to terminal manager	y	y
Authentication of providers		y
Authentication of NO to User (Terminal)		y
Authentication of User (Terminal) to NO	y	y
Re-Authentication of users	y	y
Re-Authentication of Terminals		y
Non-Repudiation		
Non-repudiation of origin of signalling and Control data		y
Non-repudiation of Delivery of Signalling and Control Data		y
Non-repudiation of Access to Stored Data		y
Access Control		
Access Control to SIM	y	y
Access Control to terminal Equipment		y
Access control to service Profile		y
Access Control to Subscription data		y
Access Control to Telecommunication Service		y

***Table 2** comparison of second and Expect Wireless ATM security features*

5. Objective of wireless ATM security features

5.1 Access Control

Unauthorised attempts to access information and resources of a system should be prevented.Resources in wireless ATM should be protected because serious complications may

arise in case of unrestricted access. The access control security mechanisms should provide for protection of entities by means of verification of access rights.

5.1.1 Access Control to SIM

This element ensures that a SIM can only be used by an authorised party.

5.1.2 Access Control to Terminal Equipment

This element ensures that terminal equipment can only be utilised by authorised parties.

5.1.3 Access Control to Service Profile

This element ensures that only authorised parties can access a service profile.

5.1.4 Access Control Subscription Data

An element by which there are restrictions in the access to the personal data of a user or subscriber stored in the network.

5.1.5 Access Control to Telecommunication Services

This element ensures that only authorised parties can access a telecommunication service.

5.2 Data Integrity

The wireless ATM should ensure that the integrity of signalling information is guaranteed. it will require to ensure that data,transfered data[6] and stored data[7], will not be altered or destroyed on the transfer path or location of storage. It also includes that location management procedures be performed in a secure manner, and that the integrity of signalling information is unaffected by handovers. The appropriate security mechanisms will be applied continuously during any transfer or storage of data.

5.2.1 User Traffic Integrity

This element protects against manipulation (modification,insertion and/or replay) by unauthorised parties of user data on the radio path.

5.2.2 User Location Integrity

An element by which the service provider and/or network operator can have some assurance that the user location related information cannot be modified by the intruders.

5.2.3 Terminal Location Integrity

An element by which the service provider and/or the network operator can have some assurance that the mobile terminal location related information cannot be modified by the intruders.

5.2.4 Integrity of Stored Data

This element offers protection for stored data against unauthorised writing and modifying.

5.2.5 Signalling Data Integrity

This element provides protection against manipulation (modification, insertion or replay) by unauthorised parties of signalling data.

5.3 Non-Repudiation

---

[6] Transferred data: It includes speech, user(fax,files,etc), signalling and management (identifiers location, charging/billing, etc) data that is transferred over the radio interface or a signalling channel.

[7] Stored data: It includes signalling and management data, data stored in the SIM and mobile terminal as well as charging and billing data.

It will be necessary for the need to be able to prove that a entity at a particular instance will involved in an action related to the network. This will allow to solve possible disputes with the involved party who will try to deny involvement in the certain action.

5.3.1 Non-repudiation of Origin of Signalling and Control Data

This element provides proof to a third party that a message was sent by a certain entity.

5.3.2 Non-repudiation of Delivery of Signalling and Control Data

This element provides proof to a third party that a message was received by a certain entity.

5.3.3 Non-repudiation of Access to Stored Data

This element provides protection against an entity denying attempted to access stored data.

5.4 Confidentiality

5.4.1 User Traffic Confidentiality

This element protects against unauthorised eavesdropping on user traffic.

5.4.2 User Identity Confidentiality

An Element by which the identity of a user is protected against disclosure over a radio interface.

5.4.3 User Location Confidentiality

An element by which the physical location of a user is prote3cted against disclosure over a radio interface.

5.4.4 Signalling Data Confidentiality

This element ensures that the signalling data is not made available or disclosed to unauthorised parties.

5.4.5 Confidentiality of Stored Data

This element ensures that stored data is not made available or disclosed to unauthorised parties.

5.5 Authentication

5.5.1 Authentication of SP to User

This element provides corroboration of the identity of a service provider to a user.

5.5.2 Authentication of User to SP

This element provides corroboration of the claimed identity of a user to a service provider.

5.5.3 User Identity Authentication

An element by which the identity of a user is verified to be the one claimed.

5.5.4 Authentication of Terminal to terminal manager

This element provides corroboration of the identity of a terminal to a terminal manager.

5.5.5 Authentication of Providers

This element provides corroboration of the identity of one network operator or service provider to another.

5.5.6 Authentication of NO to User (Terminal)

This element provides corroboration of the identity of a network operator to a user.

5.5.7 Authentication of user (Terminal) to No

This element provides corroboration of the claimed identity of a user to a network operator.

5.5.8 Re-authentication of Users

An element by which the identity of a user is re-verified to be the one claimed. This feature may be invoked repeated or at any appropriate instant.

5.5.9 Re-authentication of Terminals

An element by which the identity of a terminal is re-verified to be the one claimed. This feature may be invoked repeatedly or at any appropriate instant.

6. Conclusion

In this paper, issues related to the migration of security from second generation cellular systems to wireless ATM have been addressed. It explained the factors, parameters that affecting the migration. Also expected security features in wireless ATM were described and compared to existing second generation one.

References

1. AC095 ASPECT (Advanced Security for personal Communications Technologies), Available at http://east.kuleuven.ac.be/cosic/PMN018.htm
2. European digital cellular telecommunications system (Phase2); Security aspects (GSM02.09).