MoRaR: A Pattern Language

for Mobility and Radio Resource Management [1]

Rossana Andrade
Department of Computer Science (DC),
Federal University of Ceará (UFC),
Ceará, Brazil
E-mail: rossana@ufc.br

Luigi Logrippo
Université du Québec en Outaouais
Département d'informatique et ingénierie
Québec, Canada
Email : luigi@uqo.ca

Abstract. In mobile wireless communication environments, different systems adopt common solutions for recurring problems associated with similar architectural elements. This paper extracts and documents patterns that identify such common problems and solutions among second and third generation mobile systems, in the area of mobility and radio resource management. . These patterns are grouped into a pattern language that shows how they interact. At a high level of abstraction, the pattern language makes it possible to generate different scenarios of the mobile system behavior. These patterns are suitable to be reused at the requirements and analysis stages during the development and evolution of mobile systems.

Keywords: Mobile wireless systems, mobility management, radio resource management, patterns, pattern language.

1 Introduction

Mobile users are able to roam with a large variety of mobile wireless communication systems. For instance, the Global System for Mobile communications 900 (GSM-900) is a European-based technology that is the foundation for the digital cellular system 1800 (GSM-1800) [30][33] and the Personal Communication System 1900 (PCS-1900) [23]. General Packet Radio Services (GPRS) [22] and Universal Mobile Telecommunications System (UMTS) [31] are evolutions of GSM. Furthermore, the Digital Advanced Mobile Phone System (D-AMPS) (also known as Interim Standard 54-B) [10], which is a North American technology, defines a hybrid air interface that allows mobile stations to operate in a dual mode fashion (analog and digital). These cellular systems provide basic and supplementary telecommunication services [23]. The D-AMPS air interface is supported by the **A**merican **N**ational **S**tandards **I**nstitute – 41 (ANSI-41) [9][18]. ANSI-41 provides registration, roaming, call features, and other mobile application protocol features on the network side.

These systems have substantial differences related to their architecture, protocols, and services [23]. Interfaces among components, cryptography algorithms, and types of handoff are proprietary solutions. However, these systems adopt common solutions for dealing with recurring mobility, communication, and radio resource management problems as already discussed in [4], [7] and [8].

Third generation standards such as the International Mobile Telecommunications 2000 (IMT-2000) Systems [25][26][27] have been developed to overcome the incompatibilities among the second generation systems mentioned earlier and to integrate

[1] This paper will appear in: Pattern Languages of Program Design 5. Addison-Wesley, 2006.

standardization activities. Meanwhile, other solutions such as signaling protocols for Wireless mobile Asynchronous Transfer Mode (WmATM) systems have been proposed to provide mobility and radio resource management functions for high-speed Local Area Networks (LANs) and Wide-Area Networks (WANs) [11][15][37]. IMT-2000 systems and WmATM networks present commonalities with second generation systems regarding the architectural elements and the functional behaviors involved in mobility and radio resource management.

This paper investigates the commonalities among mobile wireless communication systems as presented in [7] in order to identify, to capture, and to document patterns. We identify and capture commonalities related to mobility and radio resource management functions among the following second and third generation mobile systems: Global System for Mobile Communications (GSM) and General Packet Radio Services (GPRS) [10][22][30][33], American National Standard Institute 41 (ANSI-41) [9][18], Wireless Intelligent Network (WIN) [3], Universal Mobile Telecommunications System (UMTS) [10][31], International Mobile Telecommunication Systems 2000 (IMT-2000) [25][26][27], and Wireless mobile ATM (WmATM) [11][15][37].

These patterns are grouped into a pattern language for mobility and radio resource management (MoRaR) that shows possible relationships among them. Several alternative scenarios can be derived from these relationships. Furthermore, this set of patterns allows designers to recognize similarities among legacy systems at the early stages of the system development process and evolution, and to re-use good solutions independent of implementation.

This paper is organized as follows. The next sub-section gives an overview of mobile wireless systems, which are the pattern language context. Section 3 introduces the MoRaR pattern language that shows the relationship between the patterns related to mobility management introduced in [4] and the radio resource management patterns presented in [8]. These patterns are detailed in Section 4 and Section 5, respectively. Finally, Section 6 addresses our main contributions and potential future work. A table with a summary and an index of all patterns presented in this paper is provided in the Appendix.

2 Mobile Wireless Systems: Architectural Concepts

The geographical area covered by a mobile system is divided in *cells* that are grouped in location areas. Typically, a *location area* is a group of cells that constitute the domain of an operator, although an operator can have several location areas. A mobile station needs to *register* when it enters a new location area, and remains registered as long as it remains in it. A mobile station has a *home location area* where it is initially registered (this area typically includes the principal address of the user) and it is said to be *roaming* when it goes to other location areas (*visited area*). Roaming must occur without interruption of service. Mobility management operations are responsible for keeping a record of the mobile user's location (location registration function) as well as for finding the correct location of a mobile station in a group of cells (paging function). Mobile user's privileges are also checked during mobility management in order to minimize the possibility of fraud (ciphering and authentication functions).

When a powered-on mobile station crosses certain boundaries or detects a better channel in another location area, it requests a location update to the network. The network is in charge of the databases that keep information about the user. If a call is coming to the mobile user, the network requests a paging operation to locate the mobile station and establish the connection.

Authentication is applied to validate the user’s identity and ciphering is used to protect the information exchanged between the mobile station and the network. Authentication and ciphering operations give the mobile user privacy and security. At a high-level of abstraction, these solutions are the same for GSM/GPRS/UMTS, ANSI-41/WIN, IMT-2000, and WmATM systems. However, implementations differ. Differences may exist in the ciphering and authentication algorithms and the sequences of exchanged messages or parameters between the network entities during this process.

Figure 1 illustrates a typical mobile wireless environment (a PLMN or Public Land Mobile Network), which is an example of the common architectural elements among the systems under consideration. The mobile system functions mentioned earlier in this section involve mobile stations (MSs), home database (commonly called home location register), visitor database (also called visitor location register or VLR), security database (called authentication center), and mobile switching centers (MSCs). This scenario depicts a mobile station (represented by a car) that is roaming from its home location area to a visited area. The mobile station movement is represented by gray (previous locations) and black (current location) colors.

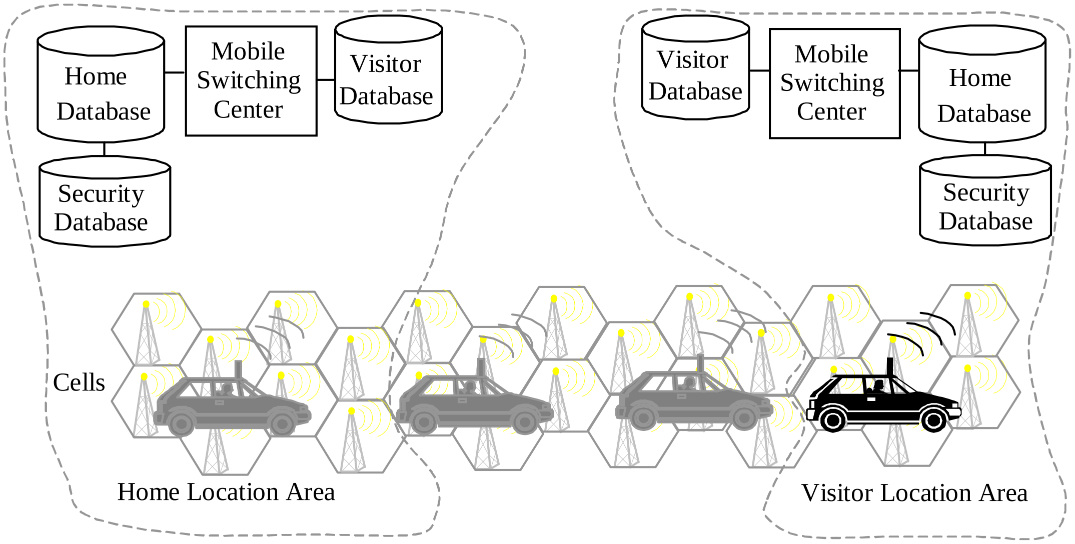

Figure 1. Typical Components of a Mobile Wireless Communication System

The MS is the equipment used to terminate the radio path at the user side. At the network side, base station controllers (BSCs) and mobile switching centers (MSCs) are also involved.

The mobile switching center is the interface between the base station controller (BSC), which is not shown in the figure, and the home database as well as the visitor database. Each mobile switching center is responsible for one or more location areas and for the exchange of messages between the network side and the mobile stations through common or dedicated radio channels. The MSC also constitutes the interface for user traffic between the cellular network and other public switched networks, or other MSCs in the same or other cellular networks. Typically there is an MSC and one location area for each operator. However standards leave considerable freedom to different implementations. Operators responsible for large geographical entities can have several MSCs and location areas. A mobile user is registered with her mobile station with the MSC which is in her *home* location area.

The home database permanently keeps information about the mobile user profile while the visitor database temporarily keeps part of the mobile user profile, the part that is needed to perform the current call. The security database is responsible for the sensitive data related to authentication and ciphering functions. In short, these databases are responsible for keeping information about mobile users' location, services, and equipment.

As depicted in Figure 2, a cell is the region covered by the radio signal of a base station transceiver. A BSC is responsible for monitoring a certain number of cells grouped in a location area. The set of BST and BSC is often called a base station (BS).

Radio resource management functions handle the connection, which is done through radio access ports (known as air interface), between base station transceivers (BSTs) and mobile stations (MSs). The handoff (also known as handover in Europe) procedure guarantees the quality of the connection (i.e., the dedicated radio channel between the MS and the network) that allows each mobile user to roam. We capture and document patterns related to handoffs, which constitute the main issues for radio resource management, on the basis of the architectural elements involved and their functional behavior.

Handoff is a critical functionality for mobile systems since all communication services should be maintained while the user is roaming. Without handoffs, calls would be dropped as soon as the user moves from the home location area. As depicted in Figure 2, handoffs can occur in three different ways depending on the network equipment involved [23][25][30].

Inter-base station transceiver handoff involves modifications only in the radio channel between BSTs and the MS (position 1 in the figure). Inter-base station controller (or intra-MSC) handoff includes also changes in the BST (position 2). These types of handoffs are also known as intra-system handoff. Finally, the inter-mobile switching center handoff (also known as inter-system handoff) involves different MSCs (position 3).

As illustrated in the figure, BSTs and BSCs are important components of the handoff process; however, this work considers only the so-called intersystem handoffs, which involve different MSCs. At the upper layers, inter-system handoffs are managed by MSs and MSCs. BSTs and BSCs act as complex transmission systems and can be ignored. This handoff requires specialized signaling protocols between the current and the candidate MSCs that are involved in the process.

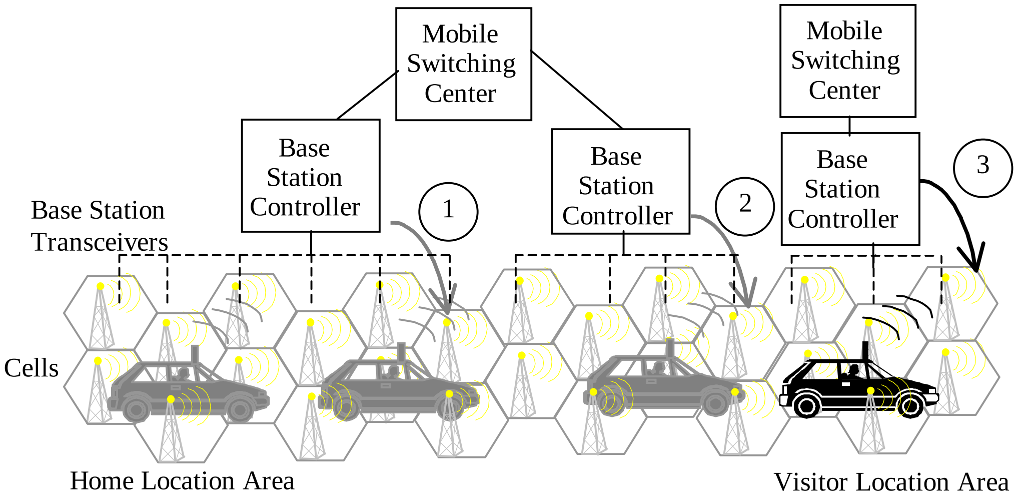

Figure 2. Type of Handoffs

It is worth to mention that mobile wireless systems´ architectural models distinguish among functional entities, network entities and physical entities. The highest level of abstraction is described in terms of functional entities, and these are incorporated into network entities at a lower level of abstraction. Network entities are then mapped to real physical entities at the implementation level. In this paper, we use the term architectural (or structural) element as a synonym for functional or network entity. As mentioned earlier, common architectural (or structural) elements are identified among these systems [7][10][23]. Thus, the next sections take into consideration the following common architectural elements: MS, MSC, BST, BSC, and databases such as the Home Location Register (HLR) and the Visitor Location Register (VLR).

3 The MoRaR Pattern Language

The common functional behaviors among the mobile wireless systems mentioned previously are presented in [7] using a notation called Use Case Maps (UCMs) [3][5][6][14]. These commonalities are analyzed and when it is appropriate, a pattern is captured and documented. The patterns based on the functional behavior are called behavioral patterns. Furthermore, common architectural elements among the chosen systems are also identified in [7], where each system architecture is described with UCM components and the common elements are extracted. Accordingly, when the pattern concept can be applied [2][16][29][34], these network or functional entities are translated to the pattern template and they constitute the structural patterns.

After identifying behavioral and structural patterns from the commonalities presented in [7], the motivation for designing a pattern language arises from the need of showing interactions among them. The pattern language for mobility and radio resource management (MoRaR), which is illustrated in Figure 3, gives designers the possibility of generating different scenarios related to mobile systems. Designers are then able to find the patterns that are relevant for what they intend to do at the requirements and analysis stages. It should be mentioned that the pattern language shows alternative ways to combine patterns.

Figure 3 depicts the pattern language with the behavioral (ovals) and architectural (plain rectangles) patterns classified into two categories (dashed rectangles) as follows: mobility management and radio resource management. In short, these two categories describe the functional layers discussed in [7] that are often used in the literature when discussing protocols for mobile communication systems. In addition to a name, each pattern has a number that identifies the sub-section in which it is discussed. The dashed and plain black arrows illustrate the relationship among the patterns. The gray arrows with outgoing call, incoming call, and roaming labels depict three possible start points for scenarios derived from the pattern language.

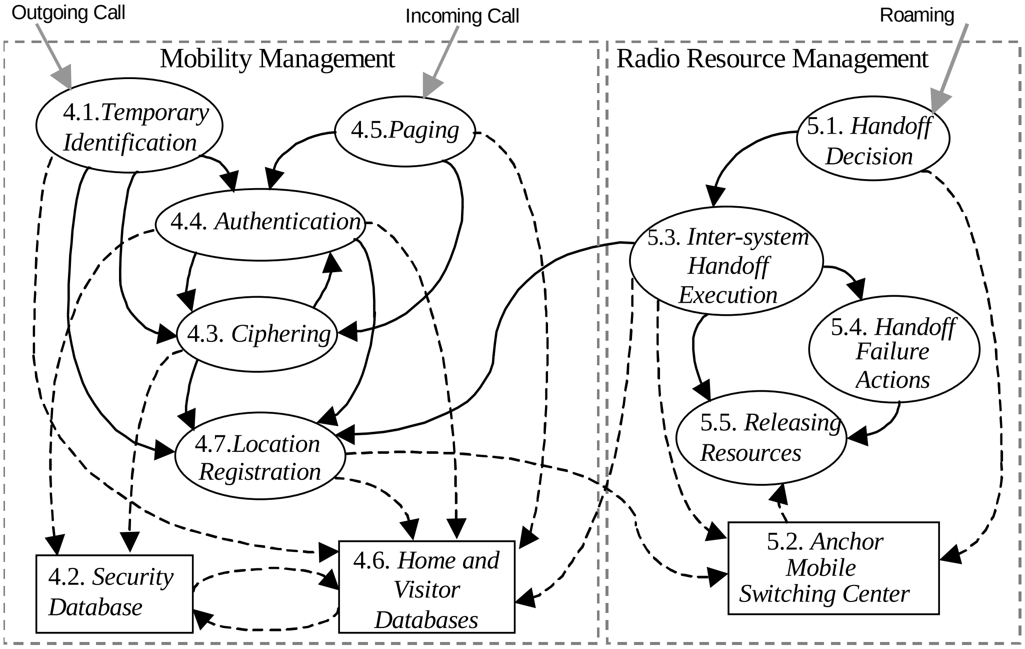
Outgoing Call
Incoming Call
Roaming
Mobility Management
Radio Resource Management
4.1.Temporary Identification
4.5.Paging
4.4. Authentication
4.3. Ciphering
4.7.Location Registration
4.2. Security Database
4.6. Home and Visitor Databases
5.1. Handoff Decision
5.3. Inter-system Handoff Execution
5.4. Handoff Failure Actions
5.5. Releasing Resources
5.2. Anchor Mobile Switching Center

Figure 3. Relationship among the Patterns within the MoRaR Pattern Language

Dashed arrows represent the exchange of the following information requests between the behavioral and the structural patterns: a request for data items, a request for operations on data items, or a request for control or release of resources. For instance, *location registration* requests the *home and visitor databases* to store, update, and delete data items related to the mobile users' location. On the other hand, *paging, temporary identification* assignment, *authentication*, and *inter-system handoff execution* request data items that are stored in the databases. In addition, the *home database* requests data items that are stored in the *security database* and vice-versa. The *anchor mobile switching center*, which controls the resources (e.g., *releasing resources*) for the *inter-system handoff execution*, is triggered by a request from the *handoff decision* or from the *location registration*.

Plain arrows represent the order in which the patterns occur. A designer chooses either a set of patterns or an individual pattern that best suit the system needs. In other words, the first pattern in a sequence or a single pattern is chosen according to the specific scenario that the designer wants to generate (e.g., outgoing call, incoming call, or roaming). The context of each pattern in a specific sequence is related to the resulting context of the previous pattern. As mentioned earlier, the following systems have been using these patterns: GSM/GPRS/UMTS, ANSI-41/WIN, and IMT-2000 based systems as well as WmATM networks.

For instance, a scenario with the sequence of patterns that describe what happens when a user powers on the mobile station and tries to make a call starts with an outgoing call request, as shown in Figure 3. First, the network queries the mobile station for its *temporary identification*, then, *authentication* and *ciphering* provide a secure environment for the communication. The *security database* separates the user's authentication information from the user's profile and it is accessed during the previous two steps. After this, a new *temporary identification* is assigned to the mobile station and the *location registration* updates the *home and visitor databases* that keep track of the mobile user's current location information whenever the user roams.

When an incoming call (see gray arrow in Figure 3) arrives to a mobile station that is powered on, *paging* is performed to reach the mobile station before *authentication* and *ciphering* that guarantee security and privacy for the establishment of the connection between the users. A *temporary identification* is assigned to the mobile user to avoid sending the real user's identity through the air interface.

Meanwhile, a handoff decision monitors the quality of the link between the mobile station and the network whenever a user moves from one location to another (see the roaming gray arrow in Figure 3). The *inter-system handoff execution* guarantees the communication when the roaming occurs. However, unsuccessful handoff outcomes also occur in this case and handoff failure actions handle them. The ability to release resources (i.e., *releasing resources*) after a handoff is also supported by the network. As presented earlier, an anchor mobile switching center maintains the control of the resources (e.g., transmission links) during the call processing.

The patterns gathered in the MoRaR pattern language are general and abstract enough to allow freedom with respect to future implementation decisions and to be re-used at the early stages of the system development process and evolution of mobile systems. Table 1 presents an overview of the MoRaR pattern language in terms of its reusable software units and their correlation to the software development stages. These units can be reused at the requirements and analysis stages of a mobile system development process. [6] presents an approach that adds rigor to the pattern reuse and validation. It validates requirements, analysis, and design models against validation test cases that are derived from the pattern solutions.

Reusable Software	**Development Stage**
Behavioral Patterns	Requirements
Structural Patterns	Analysis

Table 1 Reusable Units of the MoRaR Pattern Language

The next sections introduce the mobility and radio resource patterns, which are used in different second and third generation systems as stated earlier. Pattern names are given in sub-section headings. When we reference patterns that are included in the MoRaR pattern language, we identify them within the context or the resulting context sub-sections. However, a separate sub-section describes other patterns related to *ciphering*, *authentication* and *location registration*.

4 Patterns Related to Mobility Management Functions

Mobility management functions solve problems related to the user's security and location. For instance, mobile communication systems use wireless technologies, such as the Time Division Multiple Access (TDMA) technique, that are by nature more prone to eavesdropping and fraud on the radio interfaces than fixed networks. Furthermore, in such systems, other facilities are required to manage location aspects related to users that roam from cell to cell and to reach a user that is being called. This contrasts with the situation in fixed systems where the location of the user (or the user's terminal) is always known since it is associated to the subscriber's number.

The next sub-sections present patterns that solve mobility management problems such as: guaranteeing security and privacy (*temporary identification*, *security database*, *ciphering*, and *authentication*); reaching a mobile user that receives an incoming call (*paging*); keeping a record of the subscriber's location information that enables the establishment of calls efficiently (*home and visitor databases*); and keeping up to date the location information of the mobile station (*location registration*).

4.1 Temporary Identification

Context

A user has just powered on the mobile station, traveled to a new location area, or an incoming call has just arrived to a mobile user. In all these cases, common control channels are used for network management messages before the establishment of a dedicated control channel between the mobile station and the network [33]. At this time, privacy and security operations are the main concerns of the network in order to protect the communication over the air interface against illegal scanning of these control channels [18].

Problem

How does one ensure privacy of the subscriber's identity when sending it on the radio path?

Forces

- All the information exchanges in clear on the radio path are vulnerable to a third party listening to the control channels. As a result, the subscriber's identity can be easily captured on the air interface. Then, a fraudulent mobile station can be programmed with this valid identification and make calls at the original mobile station's expense (known as mobile cloning fraud);

- Although encryption is very efficient for confidentiality, it is not possible to protect every single information exchange on the radio path, for example:

  - when common channels are used simultaneously by all mobile stations in the cell and in the neighboring cells, *ciphering* (Section 4.3) is not applied since a key known to all mobile stations has a low level of security;

  - when a mobile user moves to a dedicated channel, there is a period during which the subscriber's real identity is unknown to the network and ciphering methods are not applied.

Solution

Assign a temporary identification to the mobile station in order to avoid exchanging the subscriber's real identity and the electronic serial number of the mobile station over a non-*ciphering* (Section 4.3) radio path.

Each mobile station has a unique temporary identification that is composed of a location area identity and a digit string. The temporary identification, which is dynamically allocated by the network when the mobile user registers in the location area, is stored in the mobile station and in the *visitor database* (Section 4.6). When a mobile user powers off the mobile station or changes to another location area, this identification is released in the old *visitor database*. The network reduces signaling messages and resources by storing the temporary identification in the *visitor database*.

Figure 4 illustrates two scenarios that represent, respectively, a *temporary identification* inquiry and a *temporary identification* assignment. The former is used by GSM, ANSI-41-C, and IMT-2000 based systems when a mobile station powers on or tries to make a call. The latter can be performed by these systems when a mobile station receives a call or changes location area. When the mobile station changes location, in addition to the temporary identification assignment, the old temporary identification is released from the old *visitor database*.

Rationale

Temporary identification adds an extra level of protection in mobile wireless environment. It is used instead of the real subscriber's identity when the user powers on a mobile station or tries to make a call and it has been previously assigned by the network. The advantage of the use of this identity is observed when *ciphering* (Section 4.3) is not applied to the traffic. In this case, even if someone is listening to the radio path, this identity does not have any meaning outside the serving network (e.g., an illegal mobile station cannot be programmed with this number).

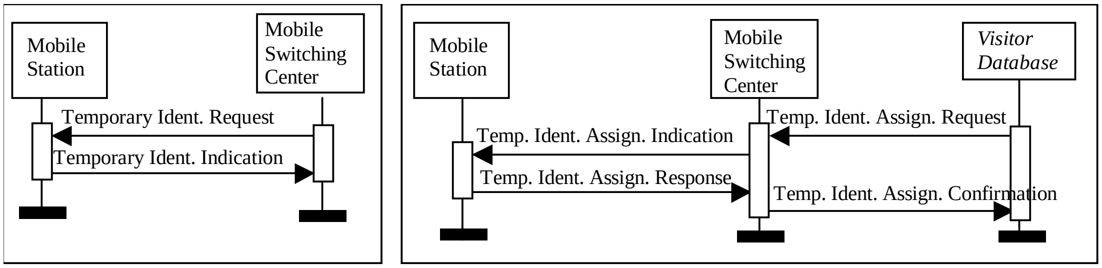
Mobile Station
Mobile Switching Center
Temporary Ident. Request
Temporary Ident. Indication
Mobile Station
Mobile Switching Center
Visitor Database
Temp. Ident. Assign. Indication
Temp. Ident. Assign. Request
Temp. Ident. Assign. Response
Temp. Ident. Assign. Confirmation

Figure 4. Temporary identification Inquiry and Assignment

Resulting Context

The *temporary identification* protects the mobile user and the network from third parties that could otherwise get information about the subscriber's real identity by listening on the radio path. Once the temporary identification has been assigned to the mobile station, the user identity can be validated through *authentication* (Section 4.4) and the exchanged information over the dedicated channel can be secured through *ciphering* (Section 4.3).

Known Uses

Temporary identification is called Temporary Mobile Subscriber Identity (TMSI) in GSM/GPRS and ANSI-41 Specifications and Temporary Mobile User Identity (TMUI) in IMT-2000 Systems and UMTS.

4.2 Security Database

Context

Security and privacy management functions handle information such as authentication keys and security-related parameters. Furthermore, they check the validity of received authenticated data, and perform confidentiality controls.

On the other hand, location management functions manage mobile users' location information as well as their identification and profile that are relevant to the provision of telecommunication services. This information is stored in the *home and visitor databases* (Section 4.6).

Problem

How does one handle the mobile user's sensitive information while assuring its protection on the network side?

Forces

- All the security mechanisms including keys and algorithms should be a concern for operators and manufacturers of mobile systems. For example, *ciphering* (Section 4.3) and *authentication* (Section 4.4) not only rely on the secrecy of the information that are provided by them, but they also rely on the secrecy of their keys and algorithms;

- Even though security management functions involve the same protocols and architectural elements as location management functions, the location information and user profile are often accessed by the network while performing *paging* (Section 4.4) and *location registration* (Section 4.6). Consequently, the information in the *home and visitor databases* is vulnerable to attacks and failures due to this frequent access;

- It is also not possible to store the security-related information only in the *visitor database* since this database is in charge of storing temporarily information related to subscribers who are currently in its location area.

Solution

Create a repository of the user's sensitive information that is only accessed by functions involved in the security management process. This database does not transmit any sensitive information (e.g., secret keys and algorithms) but performs the *ciphering* and the *authentication* computations itself.

The authentication center is the security database for ANSI-41 and GSM based systems. The same secret keys and algorithms are permanently stored in the internal memory of the mobile station when its activation occurs. In GSM, the Subscriber Interface Module (SIM) stores this information.

The *home and visitor databases* (Section 4.6) have small roles during the security management process. For example, they store complementary information that is necessary to perform the authentication and ciphering computations.

Rationale

The amount of security information in a wireless environment such as keys and algorithms that are used to perform ciphering and authentication calculations justifies their separation from the user profile information stored permanently in the home database. Any problem that home databases face will not affect the *authentication* or *ciphering* procedures. This decision gives an extra level of security to any mobile system.

Resulting Context

Sensitive data has been stored in the *security database*, which provides an additional layer of protection around this information. Consequently, the *ciphering* (Section 4.3) and the *authentication* (Section 4.4) functions use this information in order to guarantee privacy and security to the mobile user.

Known Uses

Security Database is called Authentication Center (AC) in ANSI-41 Specifications, IMT-2000 Systems, and GSM/GPRS/UMTS.

4.3 Ciphering

Context

In the idle mode, common control channels are used for all mobile stations that are in a particular cell as well as for the ones in the neighboring cells. Once a mobile station sends its *temporary identification* (Section 4.1) to the network, a dedicated control channel and a traffic channel, which is reserved for user information, are allocated. As a result, the mobile user changes from idle mode to dedicated mode.

After this, the type of information transmitted through the radio path belongs to different categories, such as: user information (voice or data), user-related signaling (messages carrying user's identity numbers), and system-related signaling (messages carrying radio results measurement).

Problem

How does one protect the privacy of the communication over an insecure wireless communication channel?

Forces

- If the information is sent in clear text on the radio path, third parties are able to eavesdrop the communication;

- A good protection against unauthorized listening is not easy with analog transmission, which is used by first generation systems such as AMPS. For instance, analog mobile systems have to apply more than one mechanism to encrypt selected parameters in the signaling messages or to encrypt the user traffic. However, digital transmission, which is used by second generation systems such as GSM, provides privacy and security to mobile subscribers by protecting all the transmitted information (e.g., voice, data, and signaling);

- Encryption of the same data must not generate the same encrypted sequence on the network each time to prevent replication fraud (e.g., play back of the encrypted sequence from a previously intercepted sequence).

Solution

Apply encryption mechanisms to the digital information that is transmitted through control and traffic channels when the mobile station is in dedicated mode. These mechanisms are independent of the exchanged information type.

Figure 5 depicts two scenarios that involve the setup of the ciphering mode and the transmission of the ciphering information in IMT-2000 systems. In Figure 5a, the network instructs the mobile station that the *ciphering* mode should be employed during the transmission process. Figure 5b illustrates the mobile station sending an encrypted data stream on the radio interface.

Before setting up the encryption mechanisms as shown in Figure 5a, the mobile station and the network have already agreed on the inputs that allow the ciphering and deciphering methods, which are the following ones: a frame number, an encryption algorithm, a ciphering key. The frame number, which is provided by the network for each ciphering sequence, prevents the replication fraud. The encryption algorithm, which is specified for use in several countries, generates the ciphering sequence. The ciphering key is calculated for each communication according to a random number, a computation algorithm, and a secret key. The mobile station, the home and visitor databases (Section 4.6), and the security database (Section 4.2) are responsible for storing the inputs and calculating the operations mentioned previously.

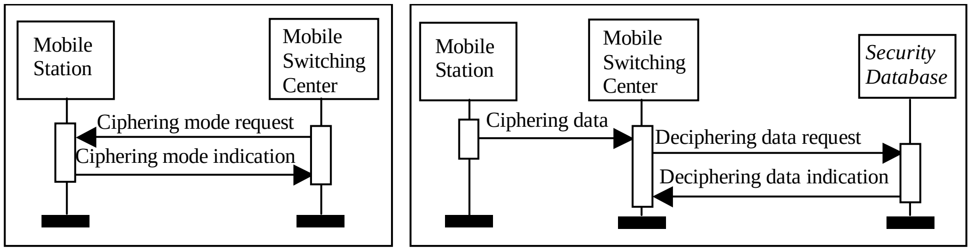

Figure 5. (a) Ciphering Mode Setup and (b) Ciphering Data Exchange

In order to ensure that the ciphered data from the mobile user's side can be deciphered on the network side, the encryption algorithm should be reversible. For instance, if the encryption algorithm is used to cipher a data stream, the same algorithm is used twice to decipher this data and get back to the original stream.

Rationale

The wireless environment does not protect against eavesdropping. Hence the need of ciphering the traffic in the air interface. Ciphering provides algorithms to encrypt signaling messages and data that are exchanged in the air interface.

Resulting Context

In dedicated mode, encryption mechanisms provide an enhanced degree of privacy over the radio channel by preventing unauthorized access to the information exchanges. For instance, when an incoming call has been requested through *paging* (Section 4.3), *ciphering* is applied to assure privacy of the information exchanges between the network and the user who is being called. In addition to ciphering, mobile user's authentication (Section 4.4) should be performed to prevent fraudulent access.

Known Uses
Ciphering is used in ANSI-41 Specifications, IMT-2000 Systems, GSM/GPRS/UMTS, and WmATM networks.

Related Patterns
Secure-channel communication, *information secrecy*, *secrecy with sender authentication*, and *secrecy with signature* are presented in [12] within a pattern language for cryptographic software.

Information secrecy has the same purpose as *ciphering*. In other words, both patterns support encryption and decryption of data. However, *ciphering* documents specific characteristics of mobile systems and concentrates on the requirements and analysis stages while *information secrecy* focuses on the design stage of cryptographic software, which are used in different domains. *Secrecy with sender authentication* and *secrecy with signature* are modifications of the *information secrecy* with the addition of *sender authentication* (see related patterns of Section 4.4) and *signature*, which guarantees the authorship of the message (non-repudiation objective of the cryptographic process).

4.4 Authentication

Context
A *temporary identification* (Section 4.1) has been requested from a mobile user that has powered on the mobile station, or entered a new location area. Once the network has provided a dedicated channel, *ciphering* (Section 4.3) prevents the eavesdropping of communications through the radio path. Nevertheless, transmissions could have been intercepted before using the temporary identification or enabling the ciphering methods whenever a *location registration* (Section 4.6) has occurred or when a mobile user has received an incoming call request through *paging* (Section 4.5). As a result, the stolen identification codes could have been used to obtain airtime fraudulently.

Problem
How does one prevent unauthorized or fraudulent access to cellular networks by mobile stations illegally programmed with counterfeit identification and electronic serial number?

Forces

- If the subscriber’s identity is transmitted without encryption over the air interface and special radio scanners capture this information, the valid user’s identity (and the user’s account) can be illegally used by someone else;

- If the identity of the mobile station cannot be verified, any fraudulent mobile station programmed with a valid subscriber’s identification can make calls, which leads to the possibility of incorrect billing to the legitimate user, or the possibility of receiving calls with false identification (impersonation);

- Passwords can limit physical access to the mobile station, but are of little value when sent over an open channel on the air interface;
- A robust method of validating the true identity of a subscriber in a wireless environment requires no subscriber intervention and no exchange of keys or algorithms through the air interface.

Solution

Perform an authentication operation in both the mobile station and the network sides based on an encryption algorithm and a secret key number. These values are stored in the legitimate mobile station and in the *security database* (Section 4.2) at the initiation of the service (e.g., at the time of mobile station activation). Furthermore, they are neither displayable nor retrievable and never transmitted over the air or passed between systems.

The operation consists of applying the encryption algorithm with the following inputs: a random value dynamically provided by the network, the secret key number, an electronic serial number, which identifies the mobile station, and the user's identification number. According to the comparison of both authentication results, the mobile station is either authorized or denied access to the network. The user's identification number is sent over a *ciphering* (Section 4.3) radio path and the electronic serial number has been previously stored in the *home database* (Section 4.6).

Figure 6 illustrates a typical mobile wireless communication environment with a scenario that shows the authentication operations performed by a mobile station and its home network provider. The architectural elements shown in the figure are related to the following scenario: a mobile user powers on the mobile station inside the home location area and an *authentication* is requested.

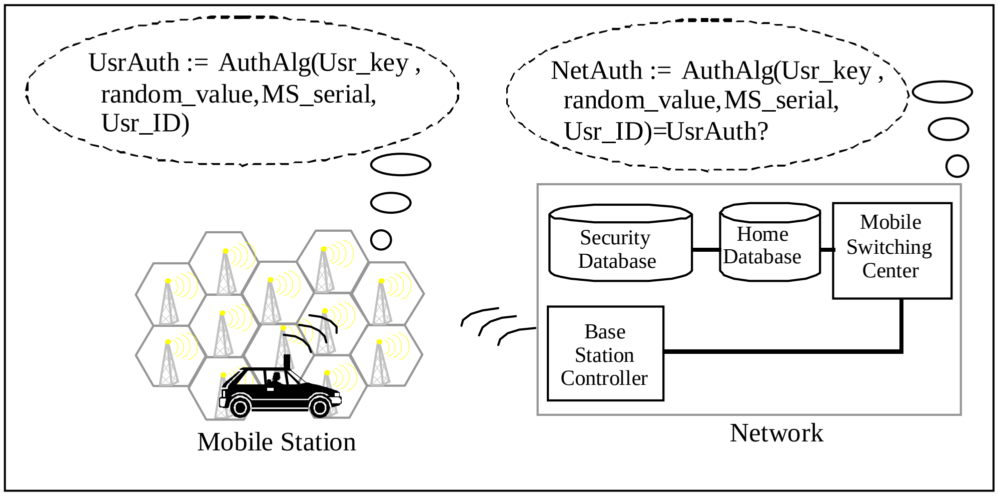
UsrAuth := AuthAlg(Usr_key , random_value,MS_serial, Usr_ID)
NetAuth := AuthAlg(Usr_key , random_value,MS_serial, Usr_ID)=UsrAuth?
Security Database
Home Database
Mobile Switching Center
Base Station Controller
Mobile Station
Network

Figure 6. Authentication Operations

First, the network sends to the mobile station a random value from a pool of free numbers. The mobile station performs the authentication operation based on the encryption algorithm with this random value and the inputs assigned previously. The operation result is sent to the network. The comparison between these results (respectively, UsrAuth and NetAuth) is made at the network side with the following network entities involved: mobile switching center, *home database* (Section 4.6), and *security database* (Section 4.2). The mobile user is successfully authenticated and able to access communication services in case of identical results. Otherwise, the access is denied.

The message sequence chart shown in Figure 7 illustrates the architectural elements of an ANSI-41-C based system that are involved in the authentication of the mobile station shown in Figure 6.

Rationale

There is a need for verifying the authenticity of every mobile station that tries to access a network to avoid problems such as mobile cloning. Different from the fixed networks, in a wireless environment, extra protection is also necessary to avoid exchanging security information over the air interface when ciphering is not available. *Authentication* combines the verification of the mobile station's identity in the network side with the exchange of random numbers through the radio ports instead of the mobile user's identity.

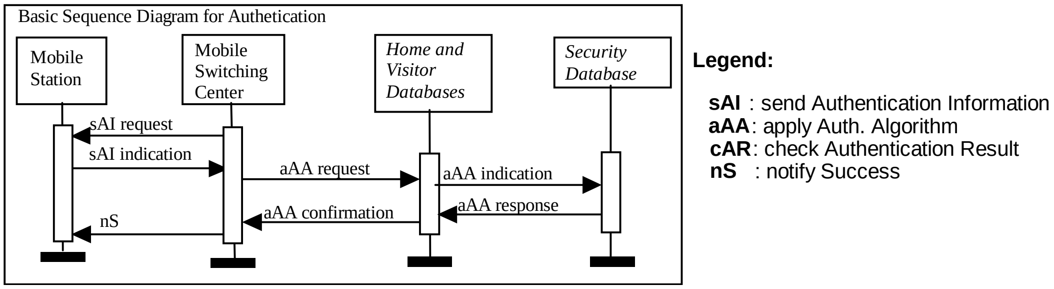
Basic Sequence Diagram for Authetication
Mobile Station
Mobile Switching Center
Home and Visitor Databases
Security Database
sAI request
sAI indication
aAA request
aAA indication
aAA response
aAA confirmation
nS
Legend:
sAI : send Authentication Information
aAA: apply Auth. Algorithm
cAR: check Authentication Result
nS : notify Success

Figure 7. Authentication: ANSI-41 Message Sequence Diagram

Resulting Context

The *authentication* operation protects the network against unauthorized access and the mobile user from fraudulent impersonation by certifying her identity. As a result, a secure mobile communication environment is offered to the subscribers before the user's *location registration* (Section 4.6), before an attempt to make a call, or when a mobile user has received an incoming call request through *paging* (Section 4.5).

Known Uses

On the basis of the air interface protocol (e.g., IS-95 or IS-136), which is used to access mobile systems, or of a roaming agreement between the home and the serving systems, it is possible to determine whether the MS is authentication-capable or not. The ANSI-41-C mobile application part (MAP) contains operations and algorithms that are responsible for the authentication tasks [18]. The authentication operations are done by a set of algorithms called **C**ellular **A**uthentication and **V**oice **E**ncryption (CAVE) and two secret keys: A-key and SSD.

Related Patterns

Secure-channel communication, *sender authentication*, and *secrecy with sender authentication* are presented in [12] within a pattern language for cryptographic software. *Sender authentication* has the same purpose as *authentication*. In other words, both patterns guarantee that the sender is genuine and authentic. However, *authentication* documents specific characteristics of mobile systems and concentrates on the requirements and analysis stages while *sender authentication* focuses on the design stage of cryptographic software, which is a different domain. *Secrecy with sender authentication* is a design pattern that combines *information secrecy* (*ciphering*) and *sender authentication* (*authentication*).

The *authenticator pattern* is presented in [13] to describe identification and authentication mechanisms for distributed object systems. This design pattern uses a login-and-authenticate protocol to grant or deny access to individual requestors. Although the authenticator and the authentication intents are related, these patterns have differences regarding their problems, solutions, resulting context, and applicability.

4.5 Paging

Context

A network has received an incoming call request that is addressed to a mobile user whose current location area is kept by the *home and visitor databases* (Section 4.6). This request contains the mobile user's identity (dialed number). The network refers to the user as the terminating or called party.

Problem

How does one reach the terminating mobile user and route the call to the actual location of the mobile station?

Forces

- The precise location of a terminating mobile station needs to be known in order to establish the communication;

- In a fixed telecommunication environment, the user's location is always known since it is associated to the subscriber's number. On the contrary, in a mobile network, the dialed number has no information about the terminating user's current location, since it changes with the user's wanderings;

- The mobile environment is split into cells and each location area includes several cells managed by a single mobile switching center. When a user roams within a location area, this user eventually changes cells;

- When an incoming call request is sent to the network, *home and visitor databases* (Section 4.6) are queried about the terminating user's current location area. However, each location area is composed of several cells and the current cell where the mobile station is camped on needs to be found by the network;

- The amount of information transmitted and processed by the network increases considerably if smaller cells are used. For instance, when a large number of mobile users are transmitting information about their location through every cell, both base stations and the spectrum in use by them are overloaded.

Solution

Send a paging message to reach the terminating mobile user in a set of cells where the user is expected to be (for example, several dozen cells). The location area information is retrieved from the *home and visitor databases* (Section 4.6), which are kept updated by the *location registration* (Section 4.7). Based on the mobile station reply, the network precisely knows the cell where the terminating user is currently located.

Figure 8 shows a successful *paging* scenario after the network receives an incoming call request.

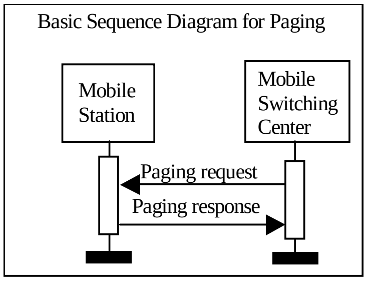

Figure 8. Paging Message Sequence Diagram

Rationale

When there is an incoming call for a mobile user, it is not possible to locate the user on the basis of the dialed number. The location of the terminating user is not included in the number since it is not fixed. *Paging* solves the problem of locating the terminating user with the information provided in the user profile of the home database.

Resulting Context

Once the network has found the terminating mobile user and allocated a dedicated channel, the call establishment proceeds. The terminating user's *authentication* (Section 4.4) and *ciphering* (Section 4.3), which is used to protect the information on the radio path, can also follow *paging* depending on implementation decisions.

In large networks, this solution provides a balance between the amount of location information to be exchanged among architectural elements and the number of necessary *paging* messages to be sent on the radio path. Besides locating the user, the paging procedure minimizes resource consumption regarding both the signaling load on the radio path and the processing load on the network.

Known Uses

Paging is used in ANSI-41 Specifications, IMT-2000 Systems, GSM/GPRS/UMTS, and WmATM networks.

4.6 Home and Visitor Databases

Context

In the mobile wireless network world, the fact that a user moves from one location area, which groups a set of cells, to another is called "roaming". Roaming occurs when a user moves to a location area other than her own home area. In practice, this usually means that a user is changing from one provider's domain to another provider's domain, although it is possible for a provider to have several domains.

Problem

How does one enable a user's mobility between location areas of the same provider or between location areas of different providers?

Forces

- Different from fixed users' identification, a mobile user's identification includes no information about the subscriber's current location;
- Mobile communication providers are responsible for keeping information about the users permanently registered in their networks as well as about the ones currently visiting them;
- Information about mobile users' home, previous, and current locations are essential to enable telecommunication services when one or several providers are involved in the roaming;
- Telecommunication services are only obtained from a current visiting location area if a mobile station is registered in this particular area. This registration relies on the home and previous location area in order to get information about the mobile user.

Solution

Create two types of repositories to handle the mobile user's information. One is the home database, which is a primary repository for information (such as current location) about a set of users permanently registered in a location area. The other repository is the visitor database, which temporarily stores part of the information (e.g., home location) about the users that are currently visiting a particular location area. The visitor database reduces the signaling messages to the home database when the user is roaming.

Every time a mobile user registers in a new location area, the *location registration* (Section 4.6) procedure updates the home, previous, and current location information.

Rationale

Databases are used in fixed networks to keep information about their subscribers such as billing information and features. In mobile systems, these databases are still necessary and they also have to keep information about user's current location area, *temporary identification,* and security information, among others. Some of this information is kept permanently in databases, other is kept temporarily. The permanent information is stored in the user's home network that can be far form the current user's location. The temporary information is often accessed by the network and should be close to the current user's location. *Home and visitor databases* are used for this purpose.

Known Uses

GSM, ANSI-41, and IMT-2000 based systems maintain a home database that is called Home Location Register (HLR) and a visitor database that is called Visitor Location Register (VLR). The GSM-900 VLR is physically integrated with the Mobile Switching Center (MSC).

ANSI-41's specifications describe the *visitor database* as the VLR functional entity. The ANSI-41 serving system is described as a single entity composed of the MSC and VLR functional entities. Most of the ANSI-41 implementations currently available in service also describe a single MSC/VLR; however, there is potential for their separation at the implementation level.

Resulting Context

Home and visitor databases keep track of users' information through *location registration* (Section 4.6). As a result of having these databases, the roaming capability is guaranteed and the restriction of offering services only in a specific area within a particular network is removed. In addition, the *visitor database* stores the *temporary* identification (Section 4.1) as well as part of the user's profile information.

The mobile user's location information is needed for *authentication* (Section 4.4) purposes and for *paging* (Section 4.5) the terminating mobile user. Furthermore, the *security database* (Section 4.2) requests information from the *home and visitor databases* in order to perform the *authentication* and *ciphering* calculations, whose results are requested by the *home and visitor databases*.

4.7 Location Registration

Context

A user has changed location area in a mobile wireless environment that contains *home and visitor databases* (Section 4.6). The user's location has changed as a consequence of a power-on event[2], an outgoing call, or an incoming call. Optionally, an *authentication* operation (Section 4.4) has been successfully performed.

Problem

How does one keep up-to-date information about a mobile user's location every time the user changes location area?

Forces

- A visitor database has limited storage capacity that is easily overloaded with a large number of mobile users roaming in its location area;
- The accuracy of the location information is necessary in order to offer telecommunication services such as information exchange between users;

[2] A mobile user changes location area before powering on the mobile station.

- The location information in the previous *visitor database* is no longer up-to-date or useful when the mobile user moves to a new location area.

Solution

Perform a location registration procedure that consists of updating and inserting the mobile user's location, respectively, in the *home and* current *visitor databases* (Section 4.6) every time the mobile user changes location area. This registration operation also includes a request message to the previous *visitor database* in order to delete the mobile user's temporary location record.

Figure 9 illustrates a location registration in ANSI-41-C networks. This scenario considers that the mobile user's home network is different from the previous location area (old network). The user is registered in a new network (new location area).

A location registration failure occurs in two cases: the mobile user's previous location information is not reachable or the mobile station does not support the new area for technical reasons, such as network failure. As a result, the location information is not updated and the network notifies the mobile user.

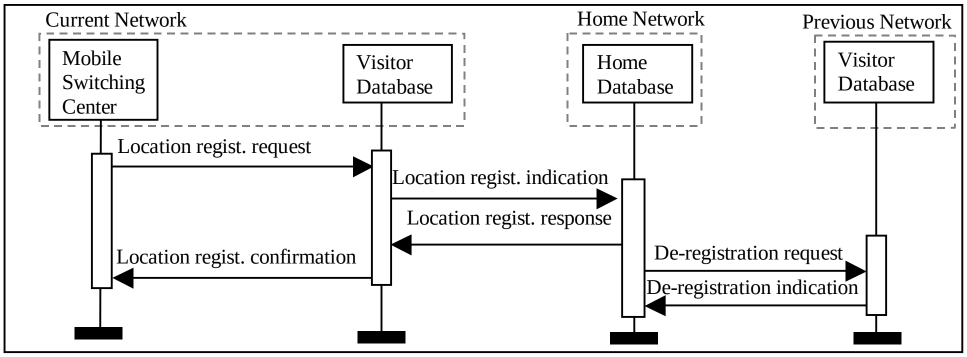

Figure 9. Location Registration Message Sequence Diagram

Rationale

In order to handle the user's mobility, there is a need for updating the *home and visitor databases* every time a user enters in a new location area. This must be done constantly in order to make it possible to complete calls or offer services to mobile users. *Location registration* not only takes care of this problem but also maintains the *visitor database* with temporary information about the users that are currently roaming its respective location area.

Resulting Context

When the current mobile switching center has successfully registered the mobile station in the new location area, the mobile station is allowed to operate in this area, as well as to request services, to establish, and to receive calls. In addition, the temporary record containing out-of-date location information has been deleted from the previous *visitor database*. As a result, storage resources have been released.

On the other hand, information about user location does not change in case of location registration failure.

Known Uses

The triggering events for location registrations are dependent on the protocol used for the air interface and on internal algorithms implemented in the serving systems [18]. However, the air interfaces standards for AMPS, CDMA, and TDMA registrations support the following common registration events: mobile station power-on, timer-based (i.e., registration occurs at periodic intervals while the mobile station is powered on), transition to another system, and call origination. At a high level of abstraction, the actions involved in the location registration are common to ANSI-41 and GSM based systems, and WmATM networks.

Related Patterns

The *Parameter Database* [36] that is described within a *Pattern Language of Feature Interaction* solves the problem of two or more features accessing and modifying the same database parameter. This pattern language handles similar feature interactions occurring in telecommunication services (for fixed and mobile users).

5 Patterns for Radio Resource Management

After investigating the radio resource management concerns of the mobile systems that we have considered in our study, we identify the following patterns detailed in the next sub-sections: *handoff decision* (Section 5.1), *anchor entity* (Section 5.2), *inter-system handoff execution* (Section 5.3), *handoff failure actions* (Section 5.4), and *releasing resources* (Section 5.5).

A decision of doing handoff is taken every time it is appropriate to change a radio communication link. The execution of an inter-system handoff maintains the stability of the dedicated radio channel despite the user’s move to a different location area. An anchor MSC handles the resources for information exchange during the inter-system handoff process. The network is also responsible for handling unsuccessful outcomes during the inter-system handoff execution. The use of radio resources is minimized by releasing circuits that are no longer necessary when a user roams.

5.1 Handoff Decision

Context

A dedicated radio communication channel has been assigned between a mobile station, which has changed from idle to dedicated mode, and a mobile switching center for transmitting signaling and data. The mobile user is moving from one place to another. This possibility of changing cells (and possibly location area) is called handoff and it is one of the major sources of complexity for mobile networks [18][30].

Problem

How do you monitor the quality of the radio communication link between the mobile station and the network to decide whether to trigger a handoff or not?

Forces

- Radio communication is interrupted as soon as the user leaves the radio coverage area of the current cell whether a call is in progress or not;

- When a call is in progress, the radio communication cut-off has an important weight in the overall perception of voice quality from the user's point of view;

- When comparing the capabilities of two cells, the load of each base station transceiver and the overall interference level in each cell affect the radio link quality;

- Local geographic peaks can occur in events such as sport competitions, concerts, and festivals. It is possible in these situations that a cell is congested in the peak area while its neighbor cells are not.

Solution

The decision whether a handoff should be triggered or not is based on the signal measurements of the transmission quality for ongoing dedicated radio connections. These measurements are best taken by the current base station or by both the current base station and the mobile station, with parameters such as: transmission error rate, propagation path loss, propagation delay, traffic considerations, as well as the cell capacity and load.

Mobile stations provide measurements of the received base station signal strength to the current mobile switching center. Although the signal measurements normally concern the allocated radio resources of the current cell, when it is necessary, adjacent base stations (in the neighbor cells) also provide measurements to the current mobile switching center while the mobile station moves towards their coverage areas.

The handoff decision can be taken by the mobile station (mobile station-controlled handoff), the serving mobile switching center (network-controlled handoff) or both (mobile station-assisted handoff called MAHO) depending on implementation issues. When the handoff involves two radio channels that are controlled by the same mobile switching center (intra-system handoff), the base station controller can also take the handoff decision.

Figure 10 shows a handoff decision involving two or more mobile switching centers (inter-system handoff).

The current mobile switching center queries adjacent mobile switching centers to determine whether the mobile station should be assigned to another mobile switching center. The adjacent mobile switching centers send the collected handoff measurements, which contain radio signal strength that is being received on the specific channel. The current mobile switching center examines each measurement to determine whether a handoff is appropriate or not. In this figure, the handoff is successfully done with the allocation of a dedicated channel to the mobile station.

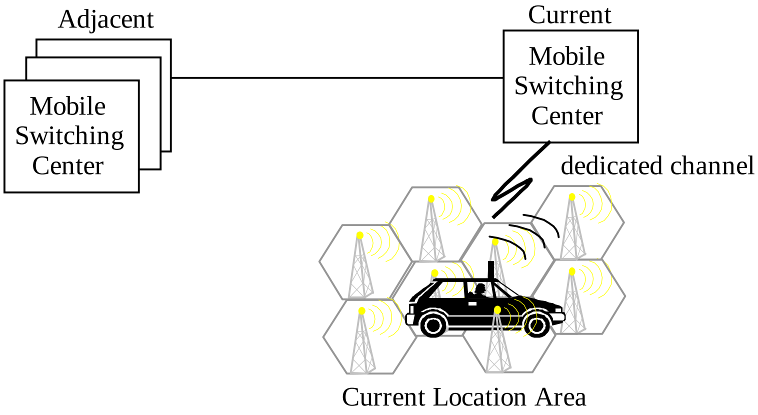

Figure 10. *Handoff Decision* with different MSCs

Figure 11 depicts a possible scenario for applying an inter-system handoff decision. The diagram starts when the mobile station moves near the border of a location area. In this scenario, a mobile switching center receives the measurements from the mobile station and decides whether the handoff is necessary or not. These measurements can be also taken by the base station or both mobile station and base station.

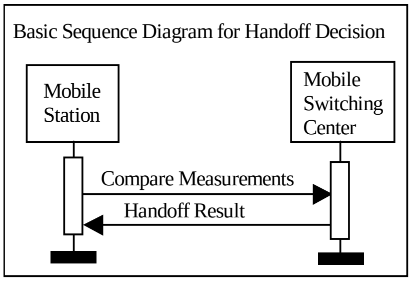

Figure 11. A Scenario for the *Handoff Decision*

Known Uses

The handoff decisions taken by the signaling alternatives for WmATM presented in [11], the ANSI-41 Handoff Measurement Request scenario presented in [18], and GSM based systems such as GSM-900 and GSM-1800 [10][30] follow this pattern.

Resulting Context

After the decision about the need of a handoff, an intra-system or an *inter-system handoff* (Section 5.3) can occur. Otherwise, there is no need for handing off. An *anchor entity* (Section 5.2) handles the network resources without being perceived by the mobile user.

5.2 Anchor Entity

Context

A *handoff decision* (Section 5.1) has been taken and an inter-system handoff, which involves the modification of a dedicated transmission path between a mobile station and a mobile switching center, must be performed [10][30].

Problem

How do you manage the network resources involved in information exchanges during an inter-system handoff?

Forces

- The physical transmission path, which includes both the dedicated radio channel between the mobile station and the network and the fixed transmission path within the network, is constantly modified by handoffs;
- If the transmission path is released as soon as an inter-system handoff decision is taken, all call information that should be transmitted to the new mobile switching center is lost. This can happen regardless of whether a new channel is allocated successfully or not;
- Charging is complicated since more than one mobile switching center is responsible for a call.

Solution

The mobile switching center that has first established the dedicated channel with the mobile station will be in charge of the call. This mobile switching center, called anchor, keeps control of the call processing information including the billing record during the inter-system handoff. Figure 12 depicts an example of an anchor MSC.

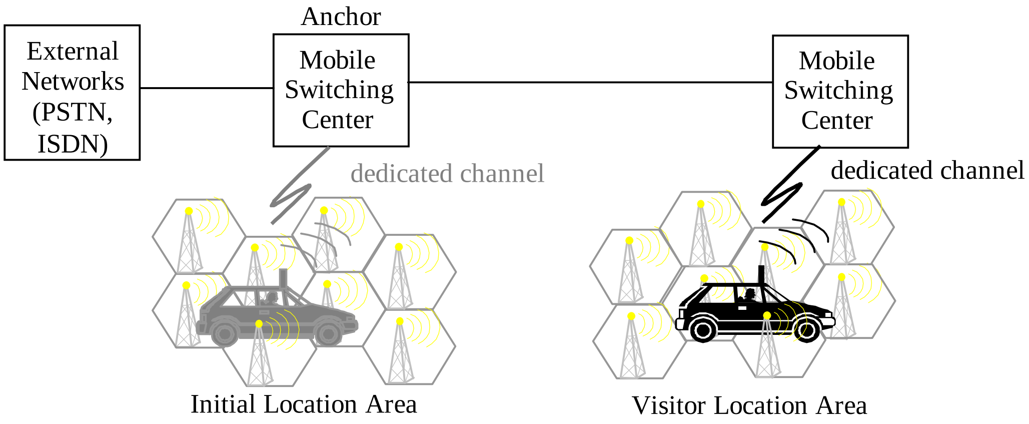

Figure 12. ANSI-41 Successful Handoff-Forward with *Anchor entity* [8]

When an inter-system handoff occurs, the network configuration changes and other mobile switching centers become involved. The anchor remains the same and the other

MSCs become just relays. As an example of anchor use when the anchor mobile switching center is different from the previous mobile switching center, consider the case where the quality of the new channel is worse than the quality of the previous one. The anchor requests the previous base station controller to re-direct the transmission to the previous mobile switching center.

Figure 13 illustrates a scenario that contains an *anchor entity mobile switching center* as a component. This scenario describes *inter-system handoff execution.* Furthermore, *anchor entity* also participates in the *handoff failure actions* and *releasing resources*.

Resulting Context

The *anchor entity* is responsible for controlling the resources that guarantee the signaling and data information exchanges during inter-system handoffs. The handoff process includes *inter-system handoff execution* (Section 5.3) and eventually *handoff failure actions* (Section 5.4)

When a *location registration* (see [4]) occurs as a consequence of a handoff, the *anchor entity* mobile switching center is also in charge of the resources for the information exchanges.

Known Uses

Anchor Entity Mobile Switching Center is used in ANSI-41 Specifications (see Figure 12), IMT-2000 Systems (called MSC), and GSM/GPRS/UMTS (called anchor MSC).

5.3 Inter-system Handoff Execution

Context

A *handoff decision* (Section 5.1) has been taken and it is necessary to perform a handoff that involves different mobile switching centers. The *anchor entity* (Section 5.2) controls the resources for the information exchanges.

Problem

How do you guarantee continuous communication service for mobile users, even if they change location area?

Forces

- The current service can be cut off as a result of one of the following:
  - the candidate mobile switching center (MSC) does not support the requested radio channel characteristics. For example, a TDMA digital channel is required but not available;
  - the signal quality of the candidate MSC is below an acceptable threshold;
  - the current traffic conditions on the candidate MSC do not allow handoff traffic;

- Users' expectations are not met by the candidate MSC concerning the reliability and consistency of the signaling and data transmission.

- A similar situation could hold for security requirements.

Solution

Identify the candidate MSC, which is being considered for handoff purposes, and evaluate its characteristics before executing the handoff. If the evaluation is successful, the candidate mobile switching center is selected to handle the communication. After this, the mobile switching center detects and accepts the mobile station in its location area and the mobile station tunes to the new channel.

Figure 13 depicts a possible scenario for performing an inter-system handoff. The scenario starts with a request triggering event, which represents the positive handoff decision (see Figure 11). After this, a new channel is allocated. The mobile station tunes to the new channel, and according to the communication status (whether a communication between the two users is occurring or not), the call is also rerouted. The new channel is verified to guarantee that the new link has better quality of transmission than the previous one. Successful or unsuccessful sub-paths can be generated as a result of this action.

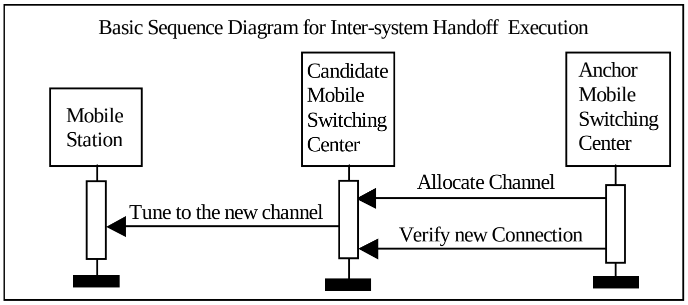
Basic Sequence Diagram for Inter-system Handoff Execution
Mobile Station
Candidate Mobile Switching Center
Anchor Mobile Switching Center
Allocate Channel
Tune to the new channel
Verify new Connection

Figure 13. A scenario for the *Inter-System Handoff Execution*

Resulting Context

If successful, the *inter-system handoff execution* is completed and the mobile station characteristics become stable. The *anchor entity* (Section 5.2) is then able to release the resources that are no longer needed (*releasing resources* in Section 5.5). Meanwhile, *home and visitor databases* (see [4]) update mobile user's location information. This successful outcome is transparent to the user.

On the other hand, when a handoff failure occurs during this process, the network takes *handoff failure actions* (Section 5.4) and notifies the user.

Known Uses

Inter-System Handoff Execution is used in ANSI-41 Specifications, IMT-2000 Systems, GSM/GPRS/UMTS, and WmATM networks. For instance, the handoff is performed through previous or candidate ports in case of WmATM. ANSI-41 documents also present different scenarios for handoff back and forward.

5.4 Handoff Failure Actions

Context

A failure has occurred during the *inter-system handoff execution* (Section 5.3) due to the lack of radio or terrestrial resources or propagation loss (for example, obstacles such as bridges or tunnels). As mentioned earlier, an *anchor entity* (Section 5.2) controls the allocated resources during inter-system handoffs when the mobile station is in dedicated mode.

Problem

How does the network handle an inter-system handoff failure?

Forces

- The *handoff decision* (Section 5.1) and the *inter-system handoff execution* reduce the chances of handoff failure. However, the possibility of failure is not eliminated completely and the communication with the current cell can be effectively lost;

- The current communication service is cut off with possible loss of information. This failure can be perceived by the user;

- Before the failure occurred, several communication resources were allocated including the transmission path;

Solution

Choose one of the following alternatives: a new handoff attempt towards the same cell, a new handoff attempt towards another cell, or tuning to the previous channel (see Figure 1). Then, request the release of all the previously allocated resources (*releasing resources* in Section 5.5) along the path in which the failure has occurred. One alternative that should be avoided is to lose the communication between the users or the ability to access network services. The *anchor entity* (Section 5.2) chooses one of the previous alternatives. When the alternative is to tune to the previous channel, it also includes the proper actions to de-allocate the candidate channel that is performed by the *Releasing resources*.

Resulting Context

Either a handoff has been re-initiated (first and second alternatives described in the pattern solution) or the mobile station has tuned to the previous channel (the last alternative). Furthermore, all the resources in use during the failed handoff have been de-allocated (see *releasing resources*).

Known Uses

Handoff Failure Actions is used in ANSI-41 Specifications, GSM/GPRS, and WmATM networks. Third generation systems such as IMT-2000 Systems and UMTS also use this solution.

5.5 Releasing Resources

Context

An *inter-system handoff execution* (Sections 5.3) has successfully occurred or *handoff failure actions* (Section 5.4) have been performed. Meanwhile, the *anchor entity* (Section 5.2) is controlling the allocated resources despite handoffs.

Problem

How does the network minimize the use of resources that are no longer needed, such as the circuits between the mobile switching centers?

Forces

- The circuits between mobile switching centers are limited, and also resources may be required by other users for handoff execution or for location registration;

- If the user is out of coverage, or has powered off the mobile station in the middle of a call, the network infrastructure has to detect that the resources are no longer needed and make sure that the mobile station is back to the idle mode;

- Before a mobile station is back to idle mode (after finishing a call or due to a network failure), a frame loss can occur since the mobile station can still transmit on its dedicated channel while the network is allocating the same channel to another mobile station.

Solution

Release the unnecessary inter-mobile switching center circuits using a request from the *anchor entity* (Section 5.2) to mobile switching centers previously involved in the handoff. In order to avoid conflict on the allocation of channels, the mobile station goes back to idle mode (in case of *handoff failure actions*) or stand by mode (in case of *inter-system handoff execution*) and stops using the channels before the network releases the resources.

Resulting Context

Once the inter-mobile switching center circuits have been released, they are available for allocation to other purposes.

Known Uses

Resources are released by the signaling alternatives for WmATM networks. This pattern can be found also in the ANSI-41 Handoff scenarios and in the GSM Handoff scenarios. *Releasing Resources* is also used in IMT-2000 Systems and UMTS.

6 Conclusion

This paper presents the MoRaR pattern language to describe mobility and radio resource management functions at a high level abstraction. In practice, the pattern problems and their respective solutions are recognized by investigating different mobile systems and by capturing their commonalities. MoRaR captures common functional behaviors and architectural elements used in various mobile systems while looking for similarities and the solution of specific design problems associated with the commonalities. GSM/GPRS/UMTS [20][30][31], ANSI-41/WIN [3][9](D-AMPS [10] is an ANSI-41 based system), IMT-2000 [25][26][27], and WmATM [11][37] are the systems investigated in this work. In [4], we have published the patterns related to mobility management functions and in [8] those related to radio resource management. The MoRaR pattern language presents the patterns in their context.

After commonalities among existing systems are recognized, it is easier to iron out differences and enable them to inter-work. Furthermore, these solutions become more accessible and better understood to novices and experts when documented as patterns. Whether designers are maintaining existing systems or building new ones, they can identify similarities and differences with respect to actual or future systems using MoRaR. The MoRaR patterns are general and abstract enough to allow freedom with respect to implementation decisions and can be re-used at the early stages of system development and in the evolution of systems.

This work does not intend to cover all common functional behaviors and architectural elements among mobile systems. We believe that common functionalities for communication management can be further investigated and other patterns can be extracted from these commonalities. These new patterns can be included in the MoRaR language within new categories (e.g. communication management) if they are not directly related to mobility or radio resource management.

A case study of pattern language reuse and validation in a WmATM environment is presented in [6]. Furthermore, the MoRaR language is applied in [1] to design a hybrid network [32] that aims to integrate cellular and IP networks. Other wireless systems, such as IEEE.802.11 [20] and Bluetooth [21], can also reuse MoRaR. As future case studies, the mobility and radio resource management functions used by the IS-95 systems (i.e., CDMA systems) [18] can be investigated in order to find out which of the radio resource management patterns are suitable for them.

A framework that graphically describes the MoRaR pattern language with UCMs is presented in [5]. This framework includes not only mobility and radio resource management functions (i.e. commonalities) but also variabilities such as communication management functions and the network reference model presented in [3].

It is worth to mention that even though the MoRaR patterns are not presented in the object-oriented paradigm, designers should be able to apply object-oriented approaches [28][17] to implement them.

In addition, we believe that a more complete identification of the intersection between the software patterns presented in the literature [19][35] and the requirements and analysis patterns documented in this work should be done to point out more *related patterns*. This was attempted in some of the behavioral patterns presented earlier in this paper. This identification can help to migrate from requirements and analysis models to object-oriented design and implementation.

7 Acknowledgments

We would like to thank our PLoP 2000 shepherd, Todd Coram, and the participants of the workshop for their insightful and valuable comments as well as our PLoP 2001 shepherd, Dennis DeBruler, and the participants of the MensorePLoP 2001 workshop for their encouraging suggestions. John Visser motivated us to investigate this area and gave us much valuable information. We are also thankful to Jim Coplien for encouraging us to be involved in the PLoP conferences. Finally, we acknowledge CAPES, CITO, Mitel and NortelNetworks for their financial support during our research.

8 References

[1] Albano, W.; Sales, W.; Andrade, R.; Cavalcanti, R.; Souza, J. N., SiGMA: Uma entidade para localização e autenticação de dispositivos móveis entre áreas de micromobilidade. *22^o Brazilian Symposium on Computer Networks (SBRC 2004)*, Gramado (RS), Brazil, May, 2004. (in Portuguese)

[2] Alexander, C., Ishikawa, S., Silverstein, M. *A Pattern Language: Town, Buildings, Constructions*, Volume 2, Oxford University Press, New York, 1977.

[3] Amyot, D., Andrade, R. Description of Wireless Intelligent Networks with Use Case Maps, *Proc. 18^o Brazilian Symposium on Computer Networks (SBRC 99)*, 418-433, Salvador (BA), Brazil, May, 1999.

[4] Andrade, R., Bottomley, M., Logrippo, L., Coram, T. A Pattern Language for Mobility Management. In: *Proc. of the 7th Conference on the Pattern Languages of Programs* (PLoP 2000), Monticello, Illinois, August 2000.

[5] Andrade, R., and Logrippo, L. Reusability at the Early Development Stages of the Mobile Wireless Communication Systems. In: *Proc. of the 4th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2000*), Orlando, Florida, July 2000.

[6] Andrade, R. Applying Use Case Maps and Formal Methods to the Development of Wireless Mobile ATM Networks. In: *Proc. of the Fifth NASA Langley Formal Methods Workshop*, Williamsburg, Virginia, June 2000.

[7] Andrade, R. M. C., *Capture, Reuse, and Validation of Requirements and Analysis Patterns for Mobile Systems*. 2001. 226 f. Thesis (Doctor of Philosophy in Computer Science)-School of Information Technology and Engineering (SITE), University of Ottawa-Carleton Institute of Computer Science, Ottawa, Ontario, Canada, 2001.

[8] Andrade, R., Logrippo, L. A Pattern Language for Radio Resource Management. Submitted and Discussed in the Shepherding Process of the 8th *Conference on the Pattern Languages of Programs* (PLoP 2001). Workshopped in *the 1st Japan Conference on the Pattern Languages of Programs* (MensorePLoP 2001), Okinawa, Japan, November 2001.

[9] ANSI/TIA/EIA. ANSI-41-D. Cellular Radiotelecommunications Intersystem Operations, 1997.

[10] Black, U. *Second Generation Mobile & Wireless Networks*. Prentice Hall Series in Advanced Communication Technologies, Prentice-Hall, Inc., 1999.

[11] Bora, A. Signaling Alternatives in a Wireless ATM Network. *IEEE Journal on Selected Areas in Communications*, Vol. 15, No. 1, January 1997

[12] Braga, A. M., Rubira, C. M. F., Dahab, R. Tropyc: A Pattern Language for Cryptographic Software. *Pattern Languages of Program Design* 4 (PLoPD4), N.D. Harrison, B. Foote, H. Rohnert (eds.), Addison-Wesley, 337-371, 2000.

[13] Brown, F. L. Jr., DiVietri, J., Villegas, G. D., Fernandez, E. D. The Authenticator Pattern. In: *Proceedings of Pattern Language of Programs* (PloP'99), August 15-18, 1999.

[14] Buhr, R. J. A. Use Case Maps as Architectural Entities for Complex Systems. In: *IEEE Transactions on Software Engineering, Special Issue on Scenario Management*, Vol. 24, No. 12, December 1998.

[15] Cheng, F.C., Holtzman, J.M. Wireless Intelligent ATM Network and Protocol Design for Future Personal Communication Systems. *IEEE Journal on Selected Areas in Communications*, Vol. 15, No. 7, September 1997.

[16] Coplien, J. O. *Software Patterns.* SIGS books and Multimedia, June 1996.

[17] Fowler, M., Scott, K. *UML Distilled: a brief guide to the standard object modeling language.* Second Edition, Addison-Wesley, 2000.

[18] Gallagher, M. D., Snyder, R. A. *Mobile Telecommunications Networking with IS-41*. McGraw-Hill, 1997.

[19] Gamma, E., Helm, R., Johnson, R., Vlissides, J. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley, 1995.

[20] Gast, Matheus S. *802.11 Wireless Network The Definitive Guide*. O´Reilly & Associates, Inc. 2002. ISBN 0-596-00183-5.

[21] Gratton, Dean A. *Bluetooth Profiles The Definitive Guide*. Pearson Education, Inc. 2003. ISBN 0-13-009221-5.

[22] Ghribi, B.; Logrippo, L. Understanding GPRS: The GSM Packet Radio Service, *Computer Networks*, 2000.

[23] Grinberg, A. *Seamless Networks: Interoperating wireless and wireline networks*. Addison-Wesley, 1996.

[24] International Telecommunications Union. Recommendation Z. 120: Message Sequence Chart (MSC). Geneva, 1996.

[25] International Telecommunications Union. Recommendation Q.1701: Framework for IMT-2000 Systems. Geneva 1999.

[26] International Telecommunications Union. Recommendation Q.1711: Network Functional Model for IMT-2000. Geneva 1999.

[27] International Telecommunications Union. Recommendation Q.1721: Information Flows for IMT-2000 (in preparation).

[28] Jacobson, I., Christerson, M., Jonsson, P., Overgaard, G. *Object-Oriented Software Engineering (A Use Case Driven Approach),* ACM Press, Addison-Wesley, 1992.

[29] Meszaros, G., Doble, J. A Pattern Language for Pattern Writing. *Pattern Language of Program Design 3,* edited by R. C. Martin, D. Riehle, and F. Buschmann, Addison-Wesley (Software Patterns Series), 1997.

[30] Mouly, M. and Pautet, M.-B. *The GSM System for Mobile Communications*, 1992.

[31] Kriaras, I. N., Jarvis, A. W., Phillips, V. E., Richards, D. J. Third-Generation Mobile Network Architectures for the Universal Mobile Telecommunications System (UMTS). In: *Bell Labs Technical Journal*, Summer 1997.

[32] Provision of Communication Services over Hybrid Networks. *IEEE Communications Magazine,* Vol. 37, No. 7, July 1999 (Special issue).

[33] Redl, S. H., Weber, M. K., Oliphant, W. *An Introduction to GSM*. Artech House, Inc., 1995. ISBN 0-89006-785-6.

[34] Rising, L., Patterns: A Way to Reuse Expertise. In: *IEEE Communications Magazine*, Vol. 37, No. 4, April 1999.

[35] Rising, L. *The Pattern Almanac 2000,* Software Pattern Series, Addison-Wesley, 2000.

[36] Utas, G. A Pattern Language of Feature Interaction. In: *Feature Interaction in Telecommunications and Software System V*, IOS Press, 1998.

[37] Wesel, E. K. *Wireless Multimedia Communications: Networking Video, Voice, and Data.* Addison-Wesley Wireless Communications Series, 1998.

Appendix

The following table summarizes the patterns for mobility and radio resource management presented in this paper. For more information about each pattern solution, the reader should refer to the respective sections.

Section	**Problem**	**Solution**	**Pattern Name**
4.1	How does one ensure privacy of the subscriber's identity when sending it on the radio path?	Assign a temporary identification to the mobile user in order to avoid exchanging the subscriber's real identity and the electronic serial number of the mobile station over a non-ciphering (Section 4.3) radio path.	*Temporary identification*
4.2	How does one handle the mobile user's sensitive information while assuring its protection on the network side?	Create a repository of the user's sensitive information that is only accessed by functions involved in the security management process.	*Security Database*
4.3	How does one protect the privacy of communication over an insecure wireless communication channel?	Apply digital cryptography mechanisms to the communication when the mobile subscriber uses a digital traffic channel in the dedicated mode.	*Ciphering*
4.4	How does one prevent unauthorized or fraudulent access to cellular networks by mobile stations illegally programmed with counterfeit identification and electronic serial number?	Perform an authentication operation in both the mobile station and the network sides based on an encryption algorithm and a secret key number.	*Authentication*
4.5	How does one reach the terminating mobile user and route the call to the user's actual location?	Send a paging message to reach the terminating mobile user to the cells within the user's current location area where the user is expected to be (for example, several dozen cells).	*Paging*
4.6	How does one enable a user's mobility between location areas of the same provider or between location areas of different providers?	Create two types of repositories to handle the mobile user's information: one is the home database that is responsible for mobile users permanently registered in a location area; and the other is the visitor database that takes care of mobile users currently visiting a particular location area.	*Home and Visitor Databases*

Section	Problem	Solution	Pattern Name
4.7	How does one keep up to date information about a mobile user's location every time the user changes location area?	Perform a location registration procedure that consists of updating and inserting the mobile user's location, respectively, in the home and current visitor databases (Section 4.6) every time the mobile user changes location area.	*Location Registration*
5.1	How do you monitor the quality of the radio communication link between the mobile station and the network to decide whether to trigger a handoff or not?	The decision whether a handoff should be triggered or not is based on the signal measurements of the transmission quality for ongoing dedicated radio connections. These measurements are best taken by the current base station or by both the current base station and the mobile station, with parameters such as: transmission error rate, propagation path loss, propagation delay, traffic considerations, as well as the cell capacity and load.	*Handoff decision*
5.2	How do you manage the network resources involved in information exchanges during an inter-system handoff?	The mobile switching center that has first established the dedicated channel with the mobile station is put in charge of the call. This anchor mobile switching center keeps control of the call processing information including the billing record during the inter-system handoff.	*Anchor Entity*
5.3	How do you guarantee continuous communication service for mobile users, even if they change location area?	Identify the candidate MSC, which is being considered for handoff purposes, and evaluate its reliability before executing the handoff. If the evaluation is successful, the candidate mobile switching center is selected to handle the communication. After this, the mobile switching center detects and accepts the mobile station in its location area and the mobile station tunes to the new channel.	*Inter-system handoff execution*
5.4	How does the network handle an inter-system handoff failure?	Choose one of the following alternatives: a new handoff attempt towards the same cell, a new handoff attempt towards another cell, or tuning to the previous channel (see Figure 1). Then, request the release of all the previously allocated resources (releasing resources in Section 5.5) along the path in which the failure has occurred.	*Handoff Failure Actions*
5.5	How does the network minimize the use of resources that are no longer needed, such as the circuits between the mobile switching centers?	Release the unnecessary inter-mobile switching center circuits by effect of a request from the anchor entity (Section 5.2) to mobile switching centers previously involved in the handoff.	*Releasing Resources*

Table 2 MoRaR Pattern Language Summary: Patterns related to Mobility and Radio Resource Management