A Pattern Language for Mobility Management

Rossana Andrade[1] **and Luigi Logrippo**
School of Information Technology and Engineering (SITE),
University of Ottawa
E-mail: {randrade, luigi}@site.uottawa.ca

Mark Bottomley
Firmware Engineer Zucotto Systems Inc.
E-mail: markb@zucotto.com

Todd Coram
Digital Creations, Inc.
E-mail: tcoram@pobox.com

Abstract. The different mobile wireless communication systems that are currently available adopt common solutions for dealing with recurring mobility management problems associated with similar architectural elements. This work extracts and documents patterns that identify such common problems and solutions among second generation systems, for example, GSM-900 and D-AMPS. 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.

1 Introduction

Nowadays, 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) and the Digital Advanced Mobile Phone System (D-AMPS) are cellular systems that provide basic and supplementary telecommunication services [7]. These systems have substantial differences related to their architecture, protocols, and services. However, they adopt common solutions for dealing with recurring mobility management problems [15].

This work investigates these commonalities in order to identify and to document patterns [10][14][26]. These patterns are grouped into a pattern language [1] for mobility management that shows possible relationships among them. Several mobility management 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 development and maintenance processes [20] and to re-use good solutions independent of implementation. For example, a high-level application framework was proposed in [3] based on the commonalities for mobility, communication, and radio resource management functions and was applied to develop a simplified wireless mobile ATM network in [4].

The next section presents typical components of the mobile systems considered in this work. Section 3 introduces a pattern language for mobility management with pattern names indicated in italic. Section 4 and Section 5 describe the patterns related to, respectively, architectural elements and functional behaviors. Finally, Section 6 addresses our main contributions and potential future work. A table with a summary of all patterns presented in this paper is provided in the Appendix.

---

1 Ph.D. Candidate at the SITE, Assistant Professor at the Computer Science Department, Federal University of Ceará, Brazil, and sponsored by CAPES (Brazilian Federal Agency for Graduate Studies).

2 Typical Components of Mobile Communication Systems

As mentioned earlier, different mobile wireless communication systems deal with common mobility management problems associated with similar architectural elements. For example, the GSM 900 is a European-based technology that is the foundation for the digital cellular system 1800 (GSM-1800) [22] and the Personal Communication System 1900 (PCS-1900) [7]. Furthermore, the D-AMPS (also known as Interim Standard 54-B) [7], 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). The American National Standards Institute - 41 (ANSI-41) [2][5][13] provides registration, roaming, call features, and other mobile application protocol features at the network side. The ANSI-41-C supports the D-AMPS air interface.

The GSM and the ANSI-41 based-systems are incompatible due to differences of implementation regarding their architectures, protocols, and services. More specifically, interfaces among physical components, encryption algorithms, and types of handoff are proprietary solutions [15]. On the other hand, these systems have commonalities with respect to their architectural elements and functional behaviors.

Figure 1 illustrates a typical mobile environment with the following common architectural elements that are identified among second generation systems: Mobile Switching Center (MSC), Visitor Location Register (VLR), Home Location Register (HLR), Authentication Center (AC), Base Station Controller (BSC), Base Station Transceiver (BST), and Mobile Station (MS).

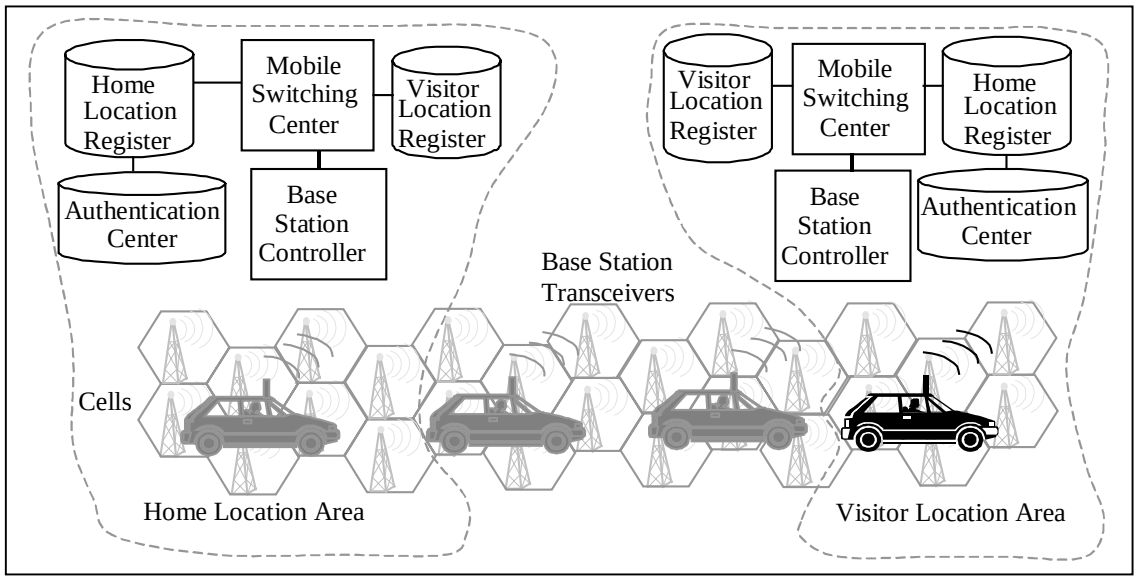

Figure 1. Typical Components of Mobile Wireless Communication Systems

As shown in the figure, all these mobile systems split their environment into cells. Each cell covers a geographical area with a base station transceiver that supports the radio resources. A location area is composed of the base station transceivers and the base

station controller, which is responsible for monitoring a certain number of cells grouped in the location area. This scenario illustrates a mobile station (represented by a car) that is roaming from its home location area to another location area (called visitor location area). The mobile station movement is represented by gray (previous locations) and black (current location) colors.

The mobile switching center is the interface between the base station controller and the home location register as well as the visitor location register. 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 home location register is the database that permanently keeps information about the mobile user profile while the visitor location register is the database that temporarily keeps part of the mobile user profile. The authentication center is the database responsible for the sensitive data related to authentication and ciphering functions.

Recently, third generation systems such as the International Mobile Telecommunications 2000 (IMT-2000) Systems [17][18][19][23] are under development to overcome the incompatibilities among the second generation systems discussed earlier and to integrate the current standardization activities for the air interface and the cellular networks. Meanwhile, other solutions such as signaling protocols for Wireless mobile Asynchronous Transfer Mode (WmATM) systems have been presented in the literature to provide mobility management functions for high-speed Local Area Networks (LANs) and Wide-Area Networks (WANs) [6][11][27]. Both IMT-2000 systems and WmATM networks present commonalities with second generation systems regarding the architectural elements and the functional behaviors involved in mobility management.

Patterns related to architectural elements and functional behaviors that are involved in mobility management are identified among these commonalities and are documented in this work. Details are presented in the next sections.

3 The Pattern Language

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.

In this context, we identify patterns from the common architectural elements, which are discussed in the previous section, and the functional behaviors, which are presented in [3]. These patterns document common solutions for recurring mobility management problems. Furthermore, they 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 development and maintenance processes of mobile systems. The motivation for presenting these patterns in a pattern language arises from the need of showing the interactions among them. The pattern language gives designers the possibility of generating different scenarios related to mobile systems.

Figure 2 depicts the pattern language for mobility management with the patterns classified into two categories that describe functional behaviors (ovals) and architectural elements (plain rectangles). 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 and incoming call labels depict two possible start points for scenarios derived from the pattern language.

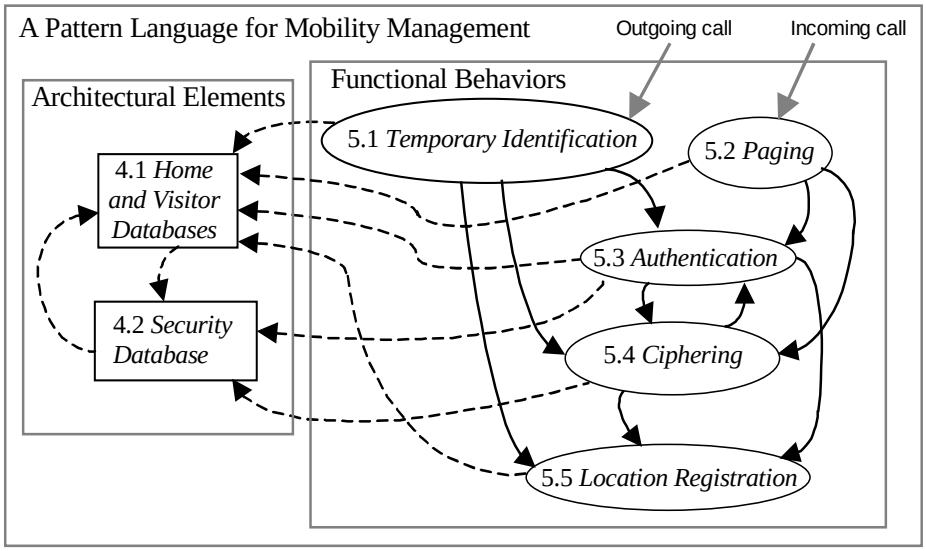

Figure 2. Relationship among the Patterns for Mobility Management

Dashed arrows represent the exchange of the following information requests between patterns: either a request for data items or a request for operations on data items. 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, and *authentication* 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.

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). The context of each pattern in a specific sequence is related to the resulting context of the previous pattern. Figure 3 shows two activity diagrams [12] involving different patterns that describe typical mobility management interactions between the mobile station and the network in the following systems: GSM, ANSI-41, and IMT-2000 based systems.

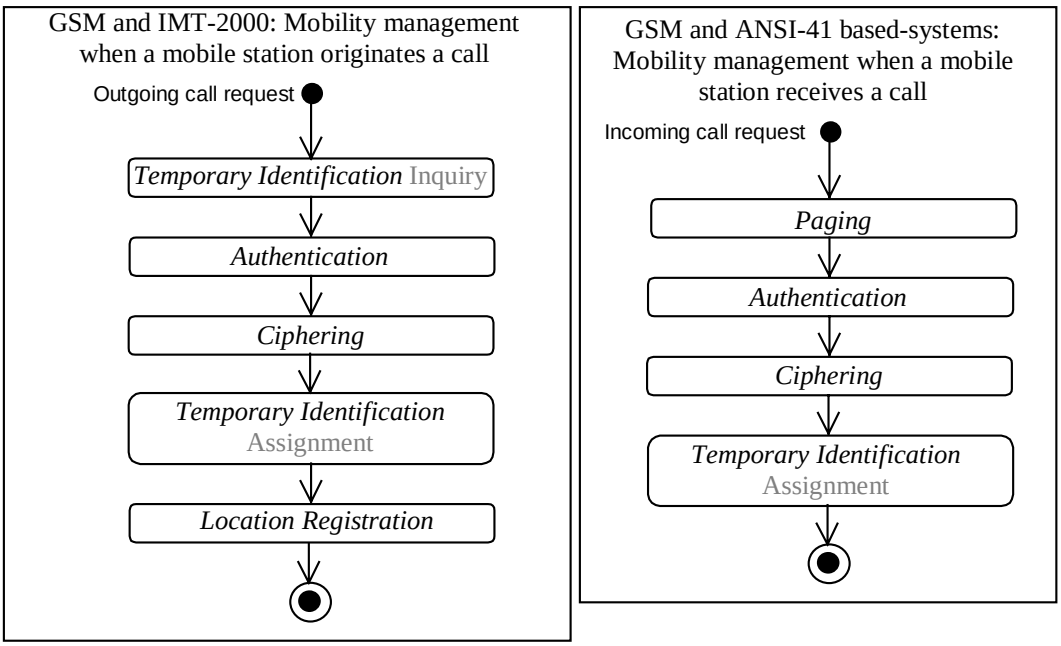

Figure 3. (a) Outgoing call (b) Incoming call Scenarios

Figure 3a shows a scenario with the sequence of patterns that describe what happens when a user powers on the mobile station and tries to make call (outgoing call request). First, the network inquires the *temporary identification* of the mobile station, 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.

In Figure 3b, an incoming call 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.

This work focuses on the architectural elements that support mobility management operations in the application layer such as mobile switching center, authentication center (*security database*), home location register, and visitor location register (*home and visitor databases*). Base station transceivers and base station controllers also support the mobility management operations that are documented within the patterns discussed earlier. However, they are related to the lower layer protocols and are not represented in the message sequence charts [16] that illustrate patterns related to functional behaviors in Section 5.

It is also important to mention that each pattern is documented with the following template: name, context, problem, forces, solution, and resulting context [10][14]. In addition, pattern names are given in sub-section headings. When we reference patterns that are included in the pattern language for mobility management, we identify them within the context or the resulting context sub-sections. However, a separated sub-section describes other related patterns to *ciphering*, *authentication* and *location registration*.

4 Patterns related to Architectural Elements

4.1 Home and Visitor Databases

Context

In the mobile wireless network world, the capability of users moving from one location area, which groups a set of cells, to another is called “roaming”. As a result of roaming, users change to location areas other than their own home area.

Problem

How do you enable the users’ 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 5.5) procedure updates the home, previous, and current location information.

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).

Resulting Context

Home and visitor databases are keeping track of users’ information through *location registration* (Section 5.5). 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 5.1) as well as part of the user's profile information.

The mobile user's location information is needed for *authentication* (Section 5.2) purposes and for *paging* (Section 5.4) 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, which results are requested by the *home and visitor databases*.

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 4.1).

Problem

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

Forces

- All the security mechanisms, for example, *ciphering* (Section 5.3) and *authentication* (Section 5.2), rely on the secrecy of their keys and algorithms that should be a concern for the operators and manufacturers;
- 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 5.4) and *location registration* (Section 5.5). 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 4.1) have small roles during the security management process. For example, they store complementary information that is necessary to perform the authentication and ciphering computations.

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 5.3) and the *authentication* (Section 5.2) functions use this information in order to guarantee privacy and security to the mobile user.

5 Patterns related to Functional Behaviors

5.1 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 [25]. 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 [13].

Problem
How do you 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 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 5.3) 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 5.3) 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 4.1).

Figure 4 illustrates two scenarios that represent, respectively, a *temporary identification* inquiry and a *temporary identification* assignment (see also Figure 3a). 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*.

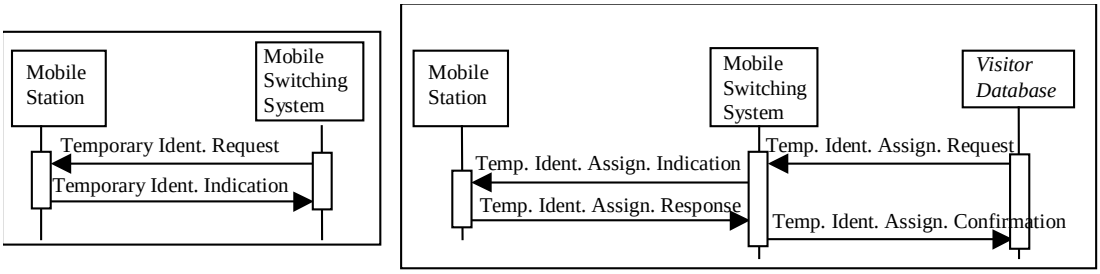

Figure 4. Temporary identification (a) Inquiry and (b) Assignment

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 5.2) and the exchanged information over the dedicated channel can be secured through *ciphering* (Section 5.3).

5.2 Authentication

Context

A *temporary identification* (Section 5.1) 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 5.3) 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 has occurred. As a result, the stolen identification codes could have been used to obtain airtime fraudulently.

Problem

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

Forces

- When the subscriber's identity is transmitted without any form of 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;
- Without verifying with a strong degree of confidence the identity of the mobile station, any fraudulent mobile station programmed with a valid subscriber's identification can make calls, which lead to incorrect billing to the legitimate user, or receive calls as if it were the original legitimate mobile station;
- Passwords only 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 and 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 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 5.3) radio path and the electronic serial number has been previously stored in the *home database* (Section 4.1).

Figure 5 illustrates a typical mobile wireless communication environment with a scenario (represented by a message sequence chart) that shows the authentication operations performed by a mobile station and its home network provider. The bottom of the figure shows the architectural elements of a ANSI-41-C based system that are

involved in the authentication of a terminating mobile station (see also Figure 3b). In this case, the VLR is physically integrated with the MSC.

First, the network sends the *authentication* request message with a random value from a pool of free numbers. The mobile station performs the authentication operation based on the authentication encryption algorithm, this random value, and the authentication inputs assigned previously. The operation result is sent to the network through the authentication indication message. The comparison between these results (respectively, UsrAuth and NetAuth in the figure) is made at the network side with the following architectural elements involved: mobile switching center; *home database* (Section 4.1), and *security database* (Section 4.2). The mobile user is successfully authenticated and able to access communication services according to the authentication result message.

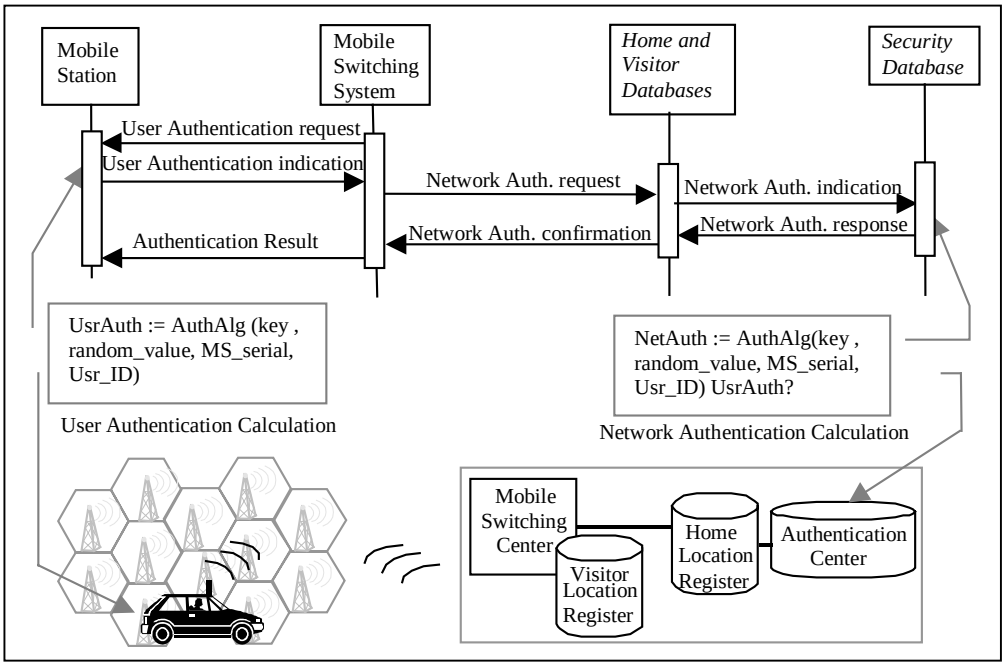

Figure 5. Successful Authentication Operations

Resulting Context

The *authentication* operation has protected the network against unauthorized access and the mobile user from fraudulent impersonations by certifying her identity. As a result, a secure mobile communication environment is offered to the subscribers before the user's *location registration* (Section 5.5), before an attempt to make a call, or when a mobile user has received an incoming call request through *paging* (Section 5.4).

Related Patterns

The *authenticator* presented in [9] describes identification and authentication mechanisms for distributed object systems. In addition, *sender authentication*, *signature*, *secrecy with sender authentication*, and *secrecy with signature* are presented in [8] within a pattern language for cryptographic software.

5.3 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 5.1) 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 the idle mode to the 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 do you protect the privacy of the communication over an insecure wireless communication channel?

Forces

- When 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 the 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 the dedicated mode. These mechanisms are independent of the exchanged information type.

Figure 6 depicts two scenarios that involve the setup of the ciphering mode and the transmission of the ciphering information in IMT-2000 systems. In Figure 6a, the network is instructing the mobile station that the *ciphering* mode should be employed during the transmission process. Figure 6b illustrates the mobile station sending an encrypted data stream on the radio interface.

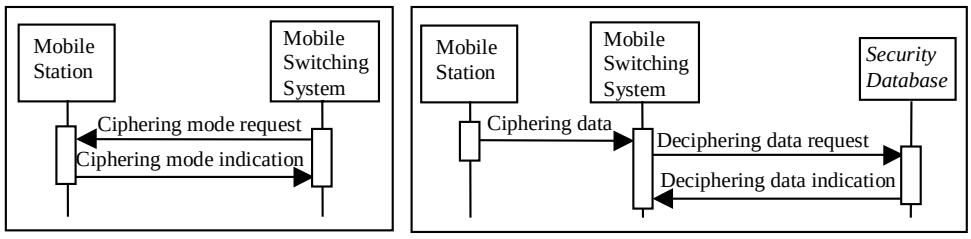

Figure 6. (a) Ciphering Mode Setup and (b) Ciphering Data Exchange

Before setting up the encryption mechanisms as shown in Figure 6a, 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 4.1), and the *security database* (Section 4.2) are responsible for storing the inputs and calculating the operations mentioned previously.

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.

Resulting Context

In the 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 5.4), *ciphering* is applied to assure privacy of the information exchanges between the network and the user who is being called.

In addition to ciphering, the mobile user's *authentication* (Section 5.2) should be performed to prevent fraudulent access.

Related Patterns

The *secure-channel communication* and *information secrecy* are presented in [8] within a pattern language for cryptographic software.

5.4 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 4.1). This request contains the mobile user's identity (dialed number). The network refers to the user as the terminating or called party.

Problem

How do you 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 that 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 4.1) 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 only in the cells within the user's current location area (for example, several dozen cells). The location area information is retrieved from the *home and visitor databases* (Section 4.1), which are kept updated by the *location registration* (Section 5.5). Based on the mobile station reply, the network precisely knows the cell where the terminating user is currently located. Figure 7 shows a successful *paging* scenario after the network receives an incoming call request.

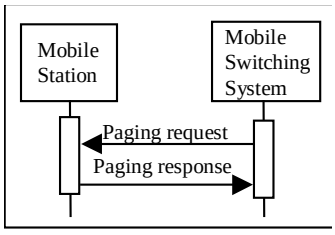

Figure 7. Paging a terminating party

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 5.2) and *ciphering* (Section 5.3), 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. In short, the paging procedure minimizes resource consumption regarding both the signaling load on the radio path and the processing load on the network.

5.5 Location Registration

Context

A user has changed location area in a mobile wireless environment that contains *home and visitor databases* (Section 4.1). The user's location has changed as a consequence of a power-on event[1], an outgoing call, or an incoming call. Optionally, an *authentication* operation (Section 5.2) has been successfully performed.

Problem

How do you 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;
- 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 4.1) 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 8 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).

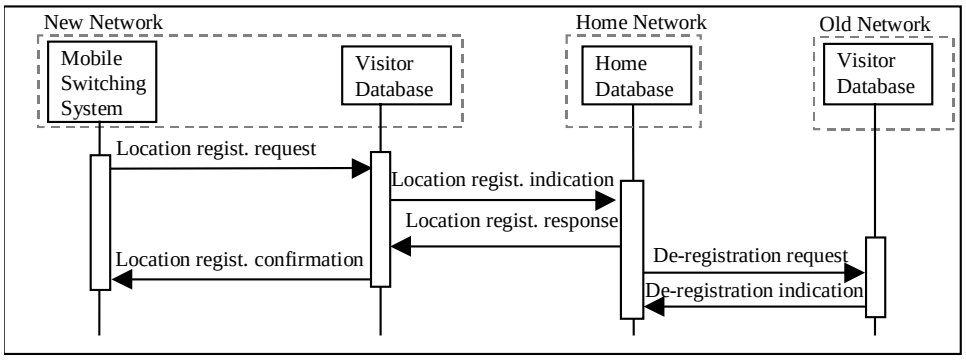

Figure 8. Successful Location Registration

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.

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

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 camp on 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.

Related Patterns

The *Parameter Database* [28] 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).

6 Conclusion

This work presents a pattern language to describe mobility management functions at a high level abstraction. The patterns are extracted from the common solutions used in the following mobile wireless communication systems: GSM [22], D-AMPS [7], ANSI-41 [2][5][13], IMT-2000 [17][18][19][23], and WmATM [6][11][27].

Whether designers are maintaining existing systems or building new ones, they can identify similarities and differences with respect to actual or future systems. This identification is based on the set of patterns that capture the common problems and solutions of the existing mobile systems mentioned above. The pattern language avoids the representation of these patterns as isolated entities. Once one recognizes commonalities among existing systems, it is possible to iron out differences and enable them to interwork. Furthermore, these solutions become more accessible and better understood to novices and experts.

As a future case study, the pattern language for mobility management will be applied to design a hybrid network as presented in [24] that aims to integrate cellular and IP networks. Furthermore, the mobility management functions used by the IS-95 systems [7] can be investigated in order to find similarities and differences in comparison with the mobility management patterns discussed in this work.

7 Acknowledgments

First, we would like to thank our co-author, Todd Coram, not only for his judicious comments on this paper but also for the improvements on our pattern writing skills during the shepherd process. We are indebted towards Jim Coplien for encouraging us to submit a paper to a PLoP conference and towards the "Network of Learning" group (Brian Foote, Terry Fujimo, Robert Hanmer, Brian Marick, William Opdyke, Carlos O'Ryan, and Juha Pärssinen) for their feedback during the PLoP'2000 writers workshop. Finally, we acknowledge CAPES, CITO, and NSERC for their financial support.

8 References

[1] Alexander, C., et al, *A Pattern Language Towns Buildings Constructions*, Volume 2, Oxford University Press, New York, 1977.

[2] Amyot, D., Andrade, R., "Description of Wireless Intelligent Networks with Use Case Maps", *Proc. Brazilian Symposium on Wireless Networks (SBRC 99)*, 418-433, Salvador (BA), Brazil, 25-28 May 1999.

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

[4] Andrade, R., "Applying Use Case Maps and Formal Methods to the Development of Wireless Mobile ATM Networks", to appear in the Proc. of the Fifth NASA Langley Formal Methods Workshop, Williamsburg, Virginia, June 2000.

[5] ANSI/TIA/EIA ANSI-41-D, Cellular Radiotelecommunications Intersystem Operations, 1997.
[6] Bora, A., "Signaling Alternatives in a Wireless ATM Network," *IEEE Journal on Selected Areas in Communications*, Vol. 15, No. 1, January 1997.
[7] Black, U., *Second Generation Mobile & Wireless Networks*, Prentice Hall Series in Advanced Communication Technologies, Prentice-Hall, Inc., 1999.
[8] 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, and H. Rohnert, eds., Addison-Wesley, 337-371, 2000.
[9] 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.
[10] Coplien, J. O., *Software Patterns*, SIGS books and Multimedia, June 1996.
[11] Fang-Cheng and Holtzman, Jack 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.
[12] Fowler, Martin, Scott, Kendall, *UML Distilled: a brief guide to the standard object modeling language*, Second Edition, Addison-Wesley, 2000.
[13] Gallagher, Michael D., Snyder, Randall A., *Mobile Telecommunications Networking with IS-41*, McGraw-Hill, 1997.
[14] Gamma, E., Helm, R., Johnson, R., and Vlissides, J., *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley, 1995.
[15] Grinberg, A., *Seamless Networks: Interoperating wireless and wireline networks*, Addison-Wesley, 1996.
[16] ITU, "Recommendation Z. 120: Message Sequence Chart (MSC)," Geneva, 1996.
[17] ITU-T, "Recommendation Q.1701: Framework for IMT-2000 Systems," March 1999.
[18] ITU-T, "Recommendation Q.1711: Network Functional Model for IMT-2000," March 1999.
[19] ITU-T, "Recommendation Q.1721: Information Flows for IMT-2000" (in preparation).
[20] Jacobson, I. et. al, *Object-Oriented Software Engineering (A Use Case Driven Approach)*, ACM Press, Addison-Wesley, 1992.
[21] Meszaros, G., Doble, J., "A Pattern Language for Pattern Writing," *Pattern Language of Program Design 3*, edited by Robert C. Martin, Dirk Riehle, and Frank Buschmann, Addison-Wesley (Software Patterns Series), 1997.
[22] Mouly, M. and Pautet, M.-B., *The GSM System for Mobile Communications*, 1992.
[23] Kriaras, I. N., Jarvis, A. W., Phillips, V. E., and Richards, D. J., "Third-Generation Mobile Network Architectures for the Universal Mobile Telecommunications System (UMTS)," In: *Bell Labs Technical Journal*, Summer 1997.
[24] "Provision of Communication Services over Hybrid Networks," *IEEE Communications Magazine*, Vol. 37, No. 7, July 1999.
[25] Redl, S. H., Weber, M. K., Oliphant, W., *An Introduction to GSM*, Artech House, Inc., 1995. ISBN 0-89006-785-6.

[26] Rising, L., “Patterns: A Way to Reuse Expertise,” In: *IEEE Communications Magazine*, Vol. 37, No. 4, April 1999.
[27] Wesel, E. K., *Wireless Multimedia Communications: Networking Video, Voice, and Data*, Addison-Wesley Wireless Communications Series, 1998.
[28] Utas, G., “A Pattern Language of Feature Interaction,” In: *Feature Interaction in Telecommunications and Software System V*, IOS Press, 1998.

9 Appendix

The following table summarizes the patterns presented earlier. For more information about each pattern solution, the reader should refer to the respective sections.

Problem	**Solution**	**Pattern Name**
How do you enable the users' 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*
How do you 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*
How do you 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 **5.3**) radio path.	*Temporary identification*
How do you 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*
How do you protect the privacy of the communication over an insecure wireless communication channel?	Apply digital cryptography mechanisms to the communication when the mobile subscriber is using a digital traffic channel in the dedicated mode.	*Ciphering*
How do you 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 only in the cells within the user's current location area (for example, several dozen cells).	*Paging*
How do you 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 4.1) every time the mobile user changes location area.	*Location Registration*

Table 1 Patterns related to Mobility Management