Secure Interoperation of Wireless Technologies

Neil John Croft

Submitted in fulfillment of the requirements
for the degree Master of Computer Science

in the

Faculty of Engineering,
Built Environment and Information Technology

University of Pretoria,
Pretoria

October 2003

Fair Use

Abstract

Tremendous emphasis has been placed on wireless technologies recently and it is expected that mobile communications will become an even bigger key driver for growth and innovation in the near future.

The purpose of this paper is to study the securing, development, integration and implementation of an always on, always available, and accessible from anywhere secure wireless communication environment.

Our analysis of the different wireless technologies reveals that a number of obstacles have to be managed before truly transparent wireless public data consumer offering is available.

Our concern revolves around the technical development and implementation efforts of integrated wireless technologies enveloped with management processes of change and evolution. Wireless technologies have influenced our daily lives and will undoubtedly continue to play a significant role in the future.

This dissertation focuses on the interoperation of wireless technologies, exploring, evaluating and presenting representations of secure, fully integrated wireless environments. The purpose is to find a cost effective, open, viable, sustainable consumer orientated high data speed offering which not only adheres to basic security requirements but surpasses it. By bringing the network to the subscriber we generate an "always-on" and "always-available" solution for data requirements fulfilling an ever increasing human demand for access to resources anywhere, anytime.

A background literature of various wireless technologies, techniques and value added services is provided. An approach for the securing of critical content over wireless links in chapter seven provides a basis for access by position concepts presented in chapter eight. This secure approach to location-aware mobile access control is an essential security enhancement in the integration and interoperation models illustrated in chapter nine. These models, appropriately named SWARM 1 and SWARM 2 (System for Wireless and Roaming Mobility), illustrate different approaches to achieving a secure, fully coherent, consumer orientated, wireless data communications environment.

Keywords: Mobile, GSM, GPRS, UMTS, Location-Based Services,
WLAN, Integration, Interoperation, XML, Security, Wireless.

Summary

Title: The Interoperation of Wireless Technologies

Candidate: Neil John Croft

Supervisor: Professor Martin S. Olivier

Department: Faculty of Engineering, Built Environment and Information Technology

Degree: Master of Science in Computer Science

Keywords: Mobile, GSM, GPRS, UMTS, Location-Based Services, WLAN, Integration, XML, Security, Wireless.

Acknowledgements

This dissertation project is in fulfilment of the Master of Science (MSc) degree in Computer Science at the University of Pretoria, South Africa. This last assignment is a closure on the education that leads to the title Master of Science.

Writing a dissertation is like completing a marathon, ultimately you finish the race with a sense of pride and achievement, however at the same time you realize just how many people have helped you to get there along the way.

I would like to use this opportunity to thank my supervisor at the University of Pretoria, Professor Martin Olivier, for his valuable support, insight and guidance throughout the duration of my dissertation.

Thanks to family and friends for all the encouragement and understanding they gave me during this period.

I would like to thank my brother, Grant, and girlfriend, Candice, for their moral support and for always being there for me. To coo-coo, I salute you.

I am appreciative of the opportunities awarded to me by my parents, Campbell and Janice, and would like give special thanks to them. They have continually given more than I could ever have asked for and have nothing but inspired me to greater things. Thank you so much.

Pretoria, South Africa
October 2003

Neil Croft

Table of Contents

Chapter 5

Chapter 6

Chapter 7

Chapter 8

List of Figures

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 7

Chapter 8

Chapter 9

List of Tables

Chapter 1

"The real social threat is not that everyone won't be connected but that no one will be able to disconnect"
Wired, Jan 1998

1. INTRODUCTION

1.1 Introduction to Mobile Wireless Communication

Mobile communications and wireless access are continually changing how people communicate with one another, how business is conducted, and how resources are accessed. These technologies significantly increase mobility, communication and facilitate access to information. The promise of communications and information access anytime, anywhere, through any medium, brings with it new inherent security risks, management processes and business models.

The potential of wireless communications empowers not only the individual but the organization too with new capabilities. These enhancements are due primarily to a paradigm shift within wireless communication environments where the network comes to the user as opposed to the user following the network.

The mobile phone industry in South Africa has grown rapidly over the last decade; however new wireless communication technologies have emerged not only to complement but to also compete with existing mobile phone communications. The immense success of mobile network operators in South Africa has resulted in other African countries realizing the opportunities mobile phones and wireless communications offer.

In this dissertation we explore various wireless communications technology standards. We address security at both an authentication and communications level for the purpose of obtaining a completely secure wireless communications environment. Comparisons of

technologies are investigated for the purpose of later exploration, evaluation and presentation of fully integrated wireless environments.

1.2 Problem Statement

To provide a modelled representation of a truly secure, integrated yet flexible high-speed mobile wireless communications environment that is operationally cost effective for network operators while fulfilling subscribers' wireless communication need for a single, always available, inexpensive, high-speed data solution.

1.3 Methodology

The first five chapters are a literary study providing detailed overviews of common wireless technologies and related wireless aspects. Background is necessary in order to appreciate concepts presented later in this dissertation.

Chapters six to nine, in principle, are concerned with comparing, securing and integrating these various wireless technologies using various methods of approach. Comparison of technologies allows for the evaluation and assessment required for the combining and or integration of technologies while providing alternative security methods allows for the convergence to a truly secure wireless communications environment.

Lastly, conclusions and referencing are provided.

In brief, we compare wireless technologies, build novel security enhancements around these technologies and finally integrate these improvements and existing benefits of each technology into a cost effective, flexible, high-speed mobile wireless communications environment.

1.4 Dissertation Document Structure

The dissertation document has been structured as follows:

Chapter 1 introduced wireless communication, identified a problem statement and describes the approach to achieving a suitable solution.

Chapter 2 introduces Global System for Mobile Communication (GSM). This chapter provides for a detailed overview of the GSM architecture, focusing on security aspects and identifying a possible successor.

Chapter 3 continues with an investigation into positioning value added services available to GSM subscribers known as Location-Based Services (LBS).

In Chapter 4 we explore General Packet Radio Service (GPRS). This data bearer service is a readily available addition to GSM networks.

In Chapter 5 we break away from wireless mobile phone technologies and examine Wireless Local Area Network (WLAN). A WLAN in essence is the connection of a Personal Computer (PC) to a network without the inherent restrictions of fixed wires.

In Chapter 6, a comprehensive comparison between WLAN and GSM-GPRS is presented. Tabulation of the most common aspects of each technology provides for a complete direct comparison of the two technologies.

In Chapter 7, we secure content in an XML document for transmission over a wireless connection or Over The Air (OTA). This is achieved by incorporating and applying a novel concept of a security sheet to an XML document. This flexible approach allows for secure user-determined communication.

In Chapter 8 a model is proposed for a secure mobile 3-Dimensional (3D) location-aware mobile access control. This model forms the foundation for an access by position methodology.

In Chapter 9, two models for the integration of WLAN and GSM-GPRS are presented as a means for allowing secure increased data transfer rates for mobile subscribers.

Chapter 10 finally concludes various aspects presented in this dissertation and suggests possible future enhancements and focus areas concerning described approaches.

The location of all referenced material is provided for in the Reference section.

It is important to note that this dissertation contains a large number of abbreviations and acronyms due to the nature of there being specific terms used within wireless technologies. Hence, a complete list of abbreviations and acronyms has been provided for the reader in the Appendix.

Chapter 2

2. GLOBAL SYSTEM FOR MOBILE COMMUNICATION (GSM)

2.1 Introduction to GSM

The Global System for Mobile Communications (GSM) is a common standard issued by the European Telecommunications Standards Institute (ETSI). Phase I of the GSM specification was published in 1990 and was the first and is currently the most widely used mobile phone system in the world. The GSM standard incorporates the 900 MHz and/or the 1800/1900 MHz frequency band and is a digital Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) system.

The most basic service supported by GSM is telephony. GSM also allows data to be transported (both synchronous and asynchronous) as a bearer service.

Due to the tremendous growth of GSM systems, comprehensive security requirements are required in mobile communications, GSM provides for the following security features [0209]:

- Subscriber identity authentication
- Subscriber identity confidentiality, and
- User data and signalling information confidentiality on radio path

The GSM specifications, currently in phase II, were designed by the GSM Consortium in secrecy and have only been distributed to GSM Network operators. The GSM standard is considered to be a "second-generation" or 2G cellular system and was designed to be secure, have strong subscriber authentication and Over The Air (OTA) transmission encryption. This comprehensive GSM Security Model has some cryptographic weaknesses [Pes] and GSM cloning is a possibility [Ano]. The GSM consortium has relied on Security by Obscurity where all algorithms relating to the GSM infrastructure have not been publicly available.

2.2 Overview

In order to understand the authentication process in GSM the respective underlying architecture needs to be understood.

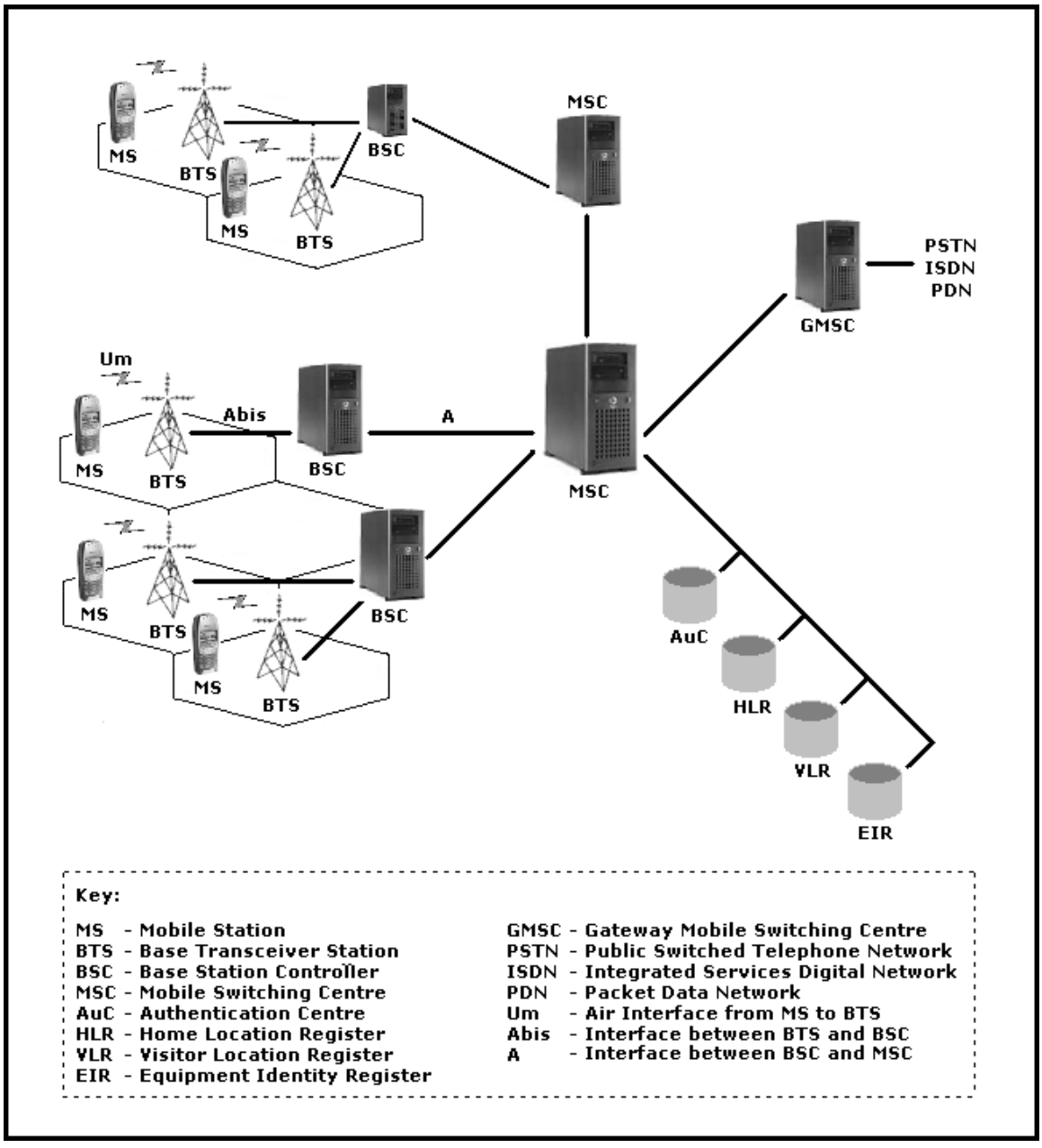

Figure 2-1 GSM Architecture

Figure 2-1 shows the most common components of the GSM architecture (other components such as the Location Measurement Unit (LMU) may exist but are considered outside the scope of this

chapter). We expand on these components and it is recommended that the reader continually refer back to Figure 2-1 to fully understand the GSM architecture and its various elements. These individual components are:

2.2.1 Mobile Station (MS)

The Mobile Station (MS) is the mobile/cellular phone or GSM compliant device. Mobile Stations are low power radio transmitters.

2.2.2 Base Transceiver Station (BTS)

The Base Transceiver Station (BTS) is a radio tower or pico (single) cell with which the Mobile Station communicates. It houses the radio transceivers and handles the radio protocols with the Mobile Station. The BTS is in contact with the MS over the radio interface. The BTS has a range of ±32Km in rural areas, this range diminishes in urban areas due to the nature of radio waves reflecting off solid objects, known as multipath propagation. It is important to note that each BTS operates at a different frequency within the GSM frequency band and an MS can communicate with up to 16 BTSs [Sco].

2.2.3 Base Station Controller (BSC)

The Base Station Controller (BSC) acts as a common node between multiple BTSs and the network's backbone. The BSC manages radio resources for one or many BTSs. It is a connection between the Mobile Station (MS) and the Mobile Switching Centre (MSC). The BSC's main responsibilities include management of the radio channels, handover management and frequency hopping. The BSC also translates the channel used over the radio interface to the channel used over the Public Switched Telephone Network or ISDN, if required. The BTS is in contact with the BSC using a landline interface, usually a high-speed T1 or E1 connection or even a high-speed wireless link. Signalling between functional entities in the network system uses the Signalling System Number 7. This is more commonly known as the SS7 network [Lin].

2.2.4 Base Station Subsystem (BSS)

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The BTS and BSC communicate across the Abis interface (described in 2.2.7). The Mobile Station (MS) and the Base Station Subsystem (BSS) communicate across the Um interface (described in 2.2.7), also known as the air interface or radio link.

2.2.5 Mobile Switching Centre (MSC)

The Mobile Switching Centre (MSC) performs the switching functions of the network. The MSC has an interface to one or more BSCs and to external networks. Its main function is management and coordination of communications between mobile users and other mobile users. The MSC also handles mobility management operations. The Base Station Subsystem (BSS) communicates with the Mobile Switching Centre (MSC) across the A interface (described in 2.2.7).

Several databases are available for control and network management. The following are usually considered to be part of the MSC:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Centre (AuC)
- Equipment Identity Register (EIR)

A discussion of the responsibilities of these four databases follows.

2.2.5.1 Home Location Register (HLR)

The Home Location Register (HLR) contains permanent and temporary data for all registered users with a network operator. Permanent data would include the user's profile while temporary data could include the current location of a user.

2.2.5.2 Visitor Location Register (VLR)

The Visitor Location Register (VLR) is used when the subscriber roams away from the network of his or her own service provider. A VLR is

responsible for a group of location areas and stores the data of those users who are currently in its area of responsibility. Information must be forwarded from the HLR to the VLR, in order to complete the authentication process. The VLR, like the HLR, is maintained on the system of each GSM service provider.

2.2.5.3 Authentication Centre (AuC)

The Authentication Centre (AuC) is used for security purposes. The AuC provides for authentication of an MS on the network and encryption of communication transmissions. The HLR forms part of the AuC.

2.2.5.4 Equipment Identity Register (EIR)

The Equipment Identity Register (EIR) registers equipment data rather than subscriber data with this database. The network is able to check that a mobile device that is used by a particular user is allowed to access the network. If the device is stolen or technologically inappropriate, it can prevent the device from connecting to the network. A unique international recognition number is associated with each device and the Equipment Identity Register (EIR) database uses this number in determining access of a device. The status returned in response to registering equipment (mobile device) with the EIR is one of the following:

- White listed – the mobile device is allowed to connect to the network;
- Grey listed – under observation as it may be a questionable device;
- Black listed – connection to the network is not allowed. A device is black listed after it has been reported stolen, or is a device that is not approved to connect to a GSM network.

Let us resume our look at the individual components of the GSM architecture.

2.2.6 Gateway Mobile Switching Centre (GMSC)

The Gateway Mobile Switching Centre (GMSC) performs the switching functions to external networks. It is involved in the management of communications between mobile users and users that could, for example, exist on a Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN).

A summary of the interfaces that exist in a GSM Architecture is provided in Table 2-1.

2.2.7 List of Interfaces

Um	Um Over The Air Interface from the Mobile Station (MS) to the Base Transceiver Station (BTS)
Abis	Interface between Base Station Transceiver (BTS) and Base Station Controller (BSC)
A	Interface between the Base Station Controller (BSC) and the Mobile Switching Centre (MSC)

Table 2-1 GSM network interfaces

Since the major components and interfaces of GSM have been covered, let's move our attention to what collectively is known as AAA (Authentication, Authorization & Accounting) of GSM. The first two AAs (authentication and authorization) are introduced.

2.3 The Authentication / Authorization Process

The GSM authentication architecture consists of four primary sub-components [Cur]:

- SIM (Subscriber Information Module)
- GSM Mobile Station
- HLR (Home Location Register)/AuC (Authentication Centre), and
- VLR (Visitor Location Register)

In the next section, the four components of the authentication architecture are discussed.

2.3.1 Subscriber Information Module (SIM)

The first component, the SIM, is a small smart card provided by the GSM service provider (SP) to the mobile subscriber. The SIM, considered tamper proof, plays an important role in identifying a subscriber for usage and billing purposes. The SIM is placed inside a GSM device and holds several key elements:

- International Mobile Subscriber Identity (IMSI). This globally registers a unique number to each GSM mobile subscriber
- An Authentication Key, usually denoted by Ki, specific to each mobile subscriber
- A Personal Identification Number (PIN)
- An algorithm called A3 used for mobile subscriber authentication
- An algorithm called A8 used for the generation of session keys

2.3.2 GSM Mobile Station (MS)

The network is able to check that a Mobile Station (MS), the second component is allowed to access the network. The Equipment Identification Register (EIR) is used to check if a device is stolen or technologically inappropriate. If authorization of the device fails, the network prevents the MS from connecting to it. The International Mobile Station Equipment Identity (IMEI) uniquely identifies a Mobile Station (MS) internationally (a unique serial number). The IMEI is allocated by the equipment manufacturer and registered by the network operator. The EIR contains a list of all valid mobile equipment on the network and each MS is identified and authenticated by its IMEI.

An embedded code is contained within the GSM MS to implement the A5 algorithm. This algorithm handles the encryption and decryption of information sent between MS and Base Transceiver Station (BTS) during a GSM communication session.

The GSM network operators assign a unique mobile number to each active subscriber. This number often referred to as Mobile Station International ISDN Number (MSISDN) and has the following format:

- Country prefix, followed by
- Network operator prefix, followed by
- The number assigned to the subscriber

For example, in the MSISDN 27831234567, 27 represents the country prefix (in this case South Africa), 83 represents the network operator's prefix, and 1234567 represents the mobile number assigned by the network operator to the subscriber.

2.3.3 Home Location Register (HLR) and Authentication Centre (AuC)

The third component, the Home Location Register (HLR) and Authentication Centre (AuC), are generally integrated together on the GSM network. They, however, are usually seen as logically independent entities. As previously discussed, the AuC is a database that contains identification and authentication information for each subscriber. The following attributes of a subscriber are stored in this database:

- International Mobile Subscriber Identity (IMSI);
- Authentication Key (Ki);
- Location Area Identifier (LAI); and
- Temporary Mobile Subscriber Identity (TMSI).

When a subscriber switches on his mobile device the IMSI is used for connection to the network. The initial connection is the only time the IMSI is used, as after the connection the network assigns the subscriber a temporary ID known as the Temporary Mobile Subscriber Identity (TMSI). The TMSI has local purpose, as the temporary ID is valid only for a specific area. If the subscriber moves to another area, the network allocates the subscriber a new TMSI. The main purpose of the TMSI is to retain the anonymity of the subscriber since the IMSI can reveal the subscriber's true identity. Within the HLR, the IMSI/TMSI of a subscriber is mapped to the MSISDN or mobile number. This information is primarily used for billing purposes.

The Authentication Centre (AuC) is responsible for generating the following set of three values:

- Random number (RAND)
- Signed response (SRES)
- Session key (Kc)

These values (also referred to as triplets) are stored in the Home Location Register (HLR) for each subscriber, and are principal in authenticating a mobile subscriber.

2.3.4 Visitor Location Register (VLR)

The Visitor Location Register (VLR) is the last component in the authentication architecture. The VLR is maintained on the system of each GSM network and stores the set of triplets (RAND, SRES, and session key Kc) for each subscriber who communicates with the base stations. When the subscriber travels away from the network, information must be forwarded from the HLR to the VLR to complete the authentication process.

The following sections further explain the triplets generated by the Authentication Centre (AuC) and the algorithms used in the GSM Security Model.

2.4 Data Elements in the GSM Authentication Protocol

GSM authentication is based on symmetric cryptographic technologies. The Security Information Module (SIM) and Authentication Centre (AuC) are both provided with the same International Mobile Subscriber Identity (IMSI) and subscriber authentication key (Ki) for each GSM subscriber. The important aspect of the GSM security protocol is that a subscriber's authentication key (Ki), while stored in both the SIM and the Authentication Centre, is never transmitted over the network. In Figure 2-2 we can see that the elements of the triplet are generated by the Authentication Centre. These triplets are initially stored in the Home Location Register (HLR), and then forwarded to the Visitor Location Register (VLR).

2.4.1 Random Number (RAND)

Random Number (RAND) is a 128-bit random number generated by the Authentication Centre (AuC).

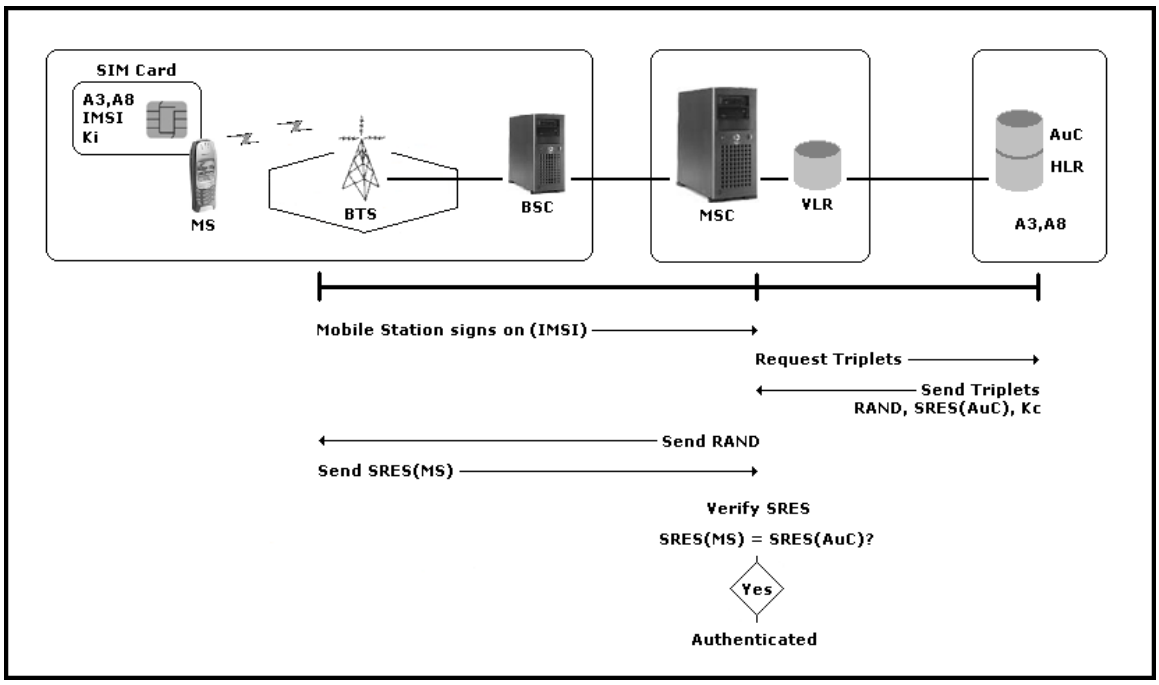

Figure 2-2 GSM Subscriber Authentication process

2.4.2 Signed Response (SRES)

Signed Response (SRES) is a 32-bit number that results when the GSM A3 algorithm is applied to a 128-bit RAND and Session key Kc. Please refer to Figure 2-3.

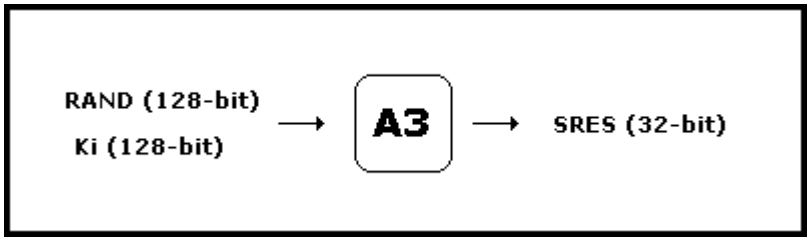

Figure 2-3 Signed Response (SRES) from A3 algorithm

2.4.3 Session Key (Kc)

Session Key (Kc) is a 64-bit session key used to encrypt and decrypt data transmitted between the Mobile Station (MS) and Base Transceiver Station (BTS), during a single GSM communication session. The SIM within the MS generates Kc by feeding the 128-bit

RAND and the subscriber's unique identification key Ki as inputs into the A8 algorithm. Kc is thus unique to each particular communication session. Please refer to Figure 2-4.

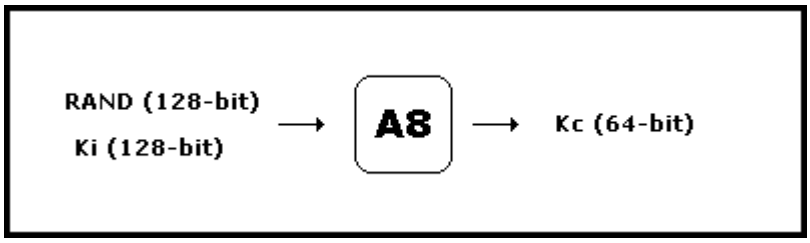

Figure 2-4 Session Key (Kc) from A8 algorithm

Three algorithms are used in the GSM Security Model and each has a different purpose. These are:

- A3 – Mobile Station Authentication Algorithm
- A5 – Over The Air (OTA) Voice-Privacy Algorithm
- A8 – Voice-Privacy Key Generation Algorithm

The algorithms are further explained in the following sections.

2.4.4 The Mobile Station (MS) Authentication Algorithm (A3)

The A3 algorithm is the authentication algorithm in the GSM Security Model. Its function is to generate a SRES response to the RAND, which the MSC received from the HLR. The A3 algorithm takes the 128-bit RAND it receives via the MSC and the 128-bit Ki that resides on the SIM card as inputs and generates a 32-bit output (see Figure 2-3). This 32-bit response is the SRES response.

2.4.5 The Voice-Privacy Key Generation Algorithm (A8)

The A8 algorithm is the key generation algorithm in the GSM Security Model. Its function is to generate a Session key (Kc). The A8 algorithm takes the 128-bit RAND and 128-bit Ki as inputs and generates a 64-bit output. This output is the 64-bit Session key (Kc) [Bri]. See Figure 2-4 for an illustration of the A8 algorithm. The Session key (Kc) is used until the MSC decides that the Mobile Station (MS) needs to be re-authenticated.

Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 and A8 algorithms [Pes]. The COMP128 algorithm takes the 128-bit RAND and 128-bit Ki as inputs and produces a 128-bit output. The first 32 bits of the 128 bits form the SRES response [Bri]. The last 54 bits of the COMP128 output form the Session key. Note that the key length is 54 bits and not 64 bits, ten zero bits are appended to the Kc generated by the COMP128 algorithm. This effectively increases the key space to the required 64 bit Session Kc. See Figure 2-5 for an illustration of the COMP128 algorithm.

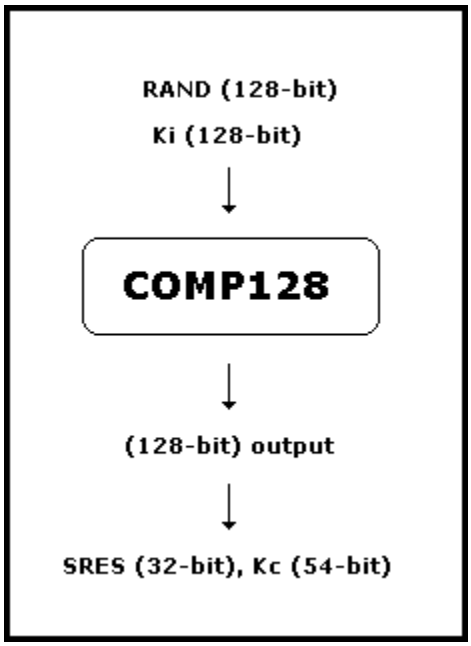

Figure 2-5 COMP128 algorithm

2.4.6 The Over The Air (OTA) Voice Privacy Algorithm (A5)

Only Over The Air (OTA) traffic is encrypted in the GSM network. The A5 algorithm, which is a stream cipher, is responsible for this. The stream cipher is initialized for every frame (or voice packet) that is sent Over The Air. The A5 algorithm takes as input the Session key (Kc) and a 22-bit frame number (see Figure 2-6). The same Kc is used throughout GSM communication, however the frame number changes, which results in the generation of a unique key stream for every frame [And]. The A5 algorithm consists of three LSFRs of different lengths [Sch]. The LSFRs are 19, 22 and 23 bits long with sparse feedback polynomials with a combined length of 64 bits [Pes]. 228 bits of key

stream are generated as output from the A5 algorithm. The first 114 bits are used for MS to BTS encryption, while the next 114 bits are used for BTS to MS encryption. Refer once again to Figure 2-6. The A5 algorithm is re-initialized with the same Kc and the number of the next frame [And].

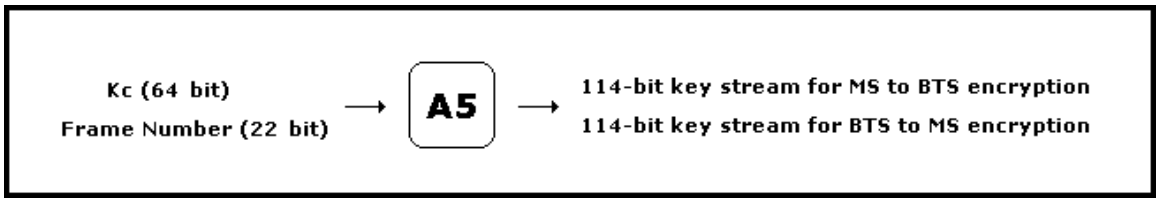

Figure 2-6 Over The Air (OTA) encryption algorithm, A5

Once the frames have been received by the Base Transceiver Station (BTS), the frames are decrypted and sent in plaintext to the operator's backbone network [Mar] (see Figure 2-7).

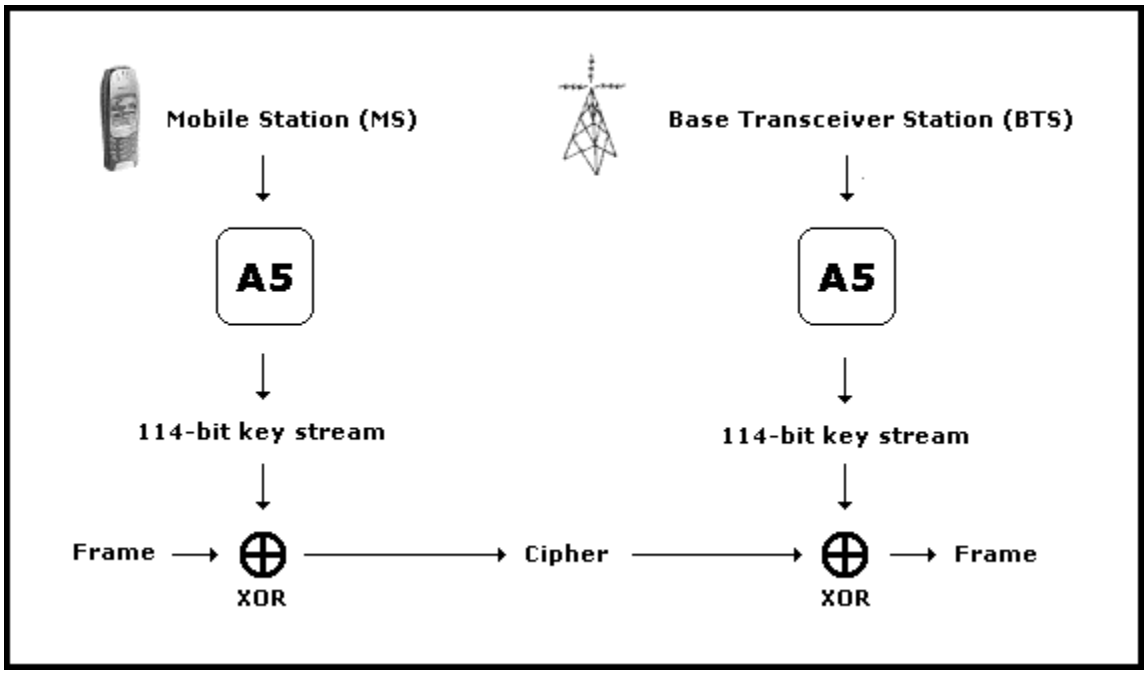

Figure 2-7 Encryption and decryption of a frame

2.4.7 Threats to the GSM Security Model

Since the first implementation of GSM, various forms of the A5 algorithm have been designed and incorporated. The original A5 algorithm was named A5/1. Other versions include the "no encryption"

A5/0 algorithm and the "weaker" Over The Air (OTA) A5/2 privacy algorithm.

There are very real threats to the GSM Security Model. Possible interception attacks include [Pes]:

- Brute-force attack against A5 algorithm
- Divide-and-Conquer attack against A5 algorithm
- Retrieving the Key Ki from the SIM and or AuC
- Retrieving the Key Ki from the SIM Over The Air (OTA)
- Cracking the A8 algorithm

Further aspects making up the GSM architecture (including the accounting of AAA) are discussed in the following section.

2.5 Radio Link, Speech Coding and Channel Structure

The radio spectrum is a limited resource and bandwidth must be divided among as many users as possible. The method chosen by GSM is a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) [Sco].

FDMA involves the division by frequency into carrier frequencies, usually 25 MHz into 124 carrier frequencies spaced 200 KHz apart. One or many carrier frequencies are then assigned to each Base Transceiver Station (BTS).

TDMA involves each of these carrier frequencies to be divided in time into eight time slots, more commonly known as a frame. One unit of time in TDMA is referred to as a burst period and lasts for approximately 0.577ms. One time slot is used for reception and one time slot is used for transmission by the Mobile Station (MS).

In general, FDMA puts each call on a separate frequency and TDMA assigns each call a certain portion of time on a designated frequency (refer to Figure 2-8). Multiple Access refers to the ability for more than one user to utilize each cell.

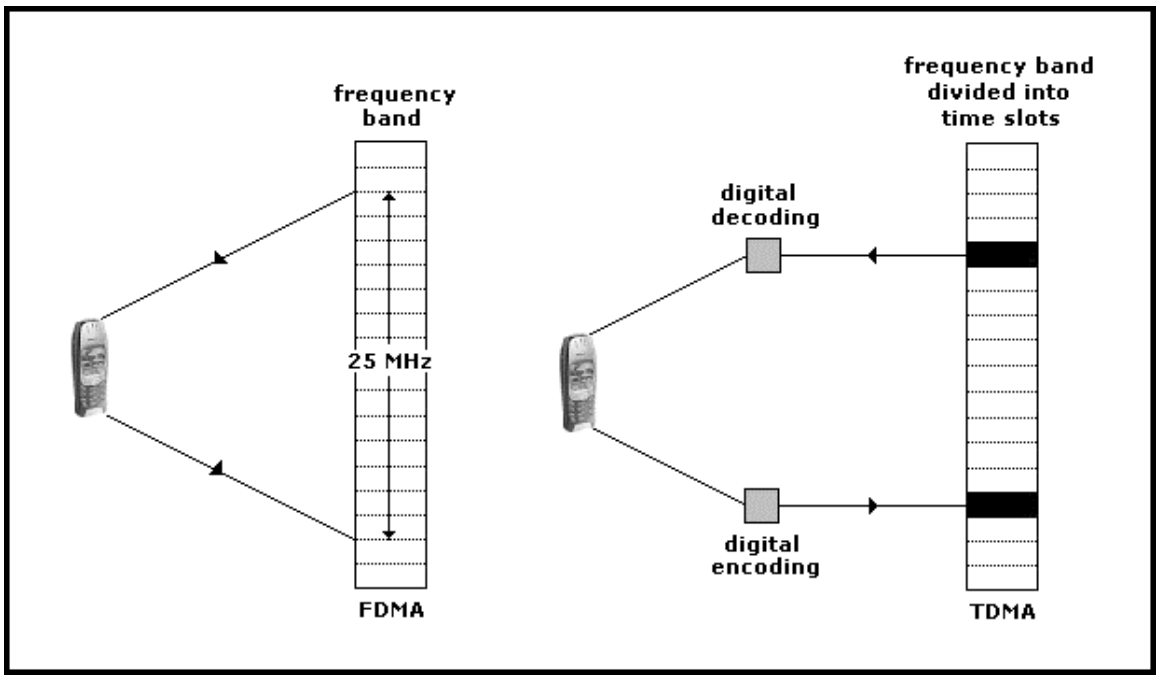

Figure 2-8 Representations of FDMA and TDMA

GSM is a digital system, therefore analog speech signals need to be digitalized. The method currently employed over ISDN for multiplexing voice lines over optical fibre lines, is Pulse Coded Modulation (PCM). The output stream from PCM is 64kbps, originally thought to be too high a rate to be feasible over a radio link, as much of the signal in PCM is redundant. The voice-coding algorithm chosen for use in GSM is Regular Pulse Excited – Linear Predictive Coder (RPELPC). This coding algorithm was chosen on the basis of speech quality and complexity. Speech is divided into 20 millisecond intervals. Each interval is encoded as 260 bits, giving a total bit rate of 13 kbps. This is referred to as Full-Rate traffic channel (TCH) speech coding. A traffic channel (TCH) is used to carry speech and data traffic. Half-Rate traffic channels (TCH) effectively double the capacity of the system providing speech coding at approximately 7 kbps.

2.6 Handover

Handover is the switching of an ongoing call or data communication. Handovers are needed in cellular systems to maintain mobility and acceptable link quality without causing unnecessary co-channel and adjacent channel interference. Handovers are triggered on the basis of algorithms, which measure threshold comparison, or by periodic

comparison fulfilling different reasons and priorities [Ves]. As a Mobile Station (MS) moves between BTSs, a handover is performed from one BTS to another, even while the mobile device is moving at a vehicular speed.

There are four different types of handover in GSM [Sco]. They involve the transfer of a call or data between:

- Channels in the same Base Transceiver Station (BTS)
- Base Transceiver Stations (BTSs) under the control of the same Base Station Controller (BSC)
- Base Transceiver Stations (BTSs) under the control of different BSCs, but belonging to the same Mobile Switching Centre (MSC)
- Base Transceiver Stations under the control of different MSCs

The first two types of handovers are called internal handovers as only one BSC is involved, while the last two are called external handovers as MSCs are involved. Target evaluation is integral in the handover process and influential factors include measurements of signal strength, distance and traffic load. Handovers are handled in the following three ways:

- Network controlled handovers
- Mobile assisted – Network controlled handovers
- Mobile controlled handovers

Mobile assisted – Network controlled handovers are used widely in "second-generation" (2G) GSM networks. Handovers can either be initiated by the MS or by the serving BTS and MSC where both the serving BTS and the MS measure the radio link quality.

The most common handover algorithms are linked with the Mobile Stations (MSs) power control [Bal], however this is not specified in the GSM recommendation.

2.7 Roaming

Roaming occurs when a subscriber is outside the range of its home network but may be in the range of another GSM network. In order for Roaming to take place, contractual agreement between the network operators is required. Schemas also known as "Roaming Agreements" are required between network operators for the exchange of accounting data and billing procedures. The GSM Association estimates

that more than 20,000 individual roaming agreements are currently in place between its operators, with more being added every day.

2.8 Billing

GSM includes a comprehensive billing model. Figure 2-9 illustrates the GSM billing and accounting system. Much of the traffic carried by a GSM Public Land Mobile Network (PLMN) either originates, or terminates in another network. The operator of the local fixed network charges the wireless operator for each call that terminates at one of its fixed subscribers. And likewise, the GSM operator will charge the fixed operator for each call made to a mobile number from a fixed line.

Therefore, GSM network operators and their local fixed counterparts usually negotiate an interconnect agreement to make charging as simple as possible. The other fixed international operators have normally already negotiated similar agreements. Revenue sharing models with other network operators and third parties as content service providers is common.

With the simple objective of global roaming lies a complex process of gathering information about a roaming subscriber and taking a standardized approach to the charges being incurred.

The Transferred Account Data Interchange Group (TADIG) was given the task of implementing roaming billing. The interchange of billing data between different network operators has been defined and implemented using the Transferred Account Procedure (TAP) protocol.

With TAP, roaming partners are able to bill each other for the use of networks and services of roaming subscribers through a standard process (see Figure 2-9).

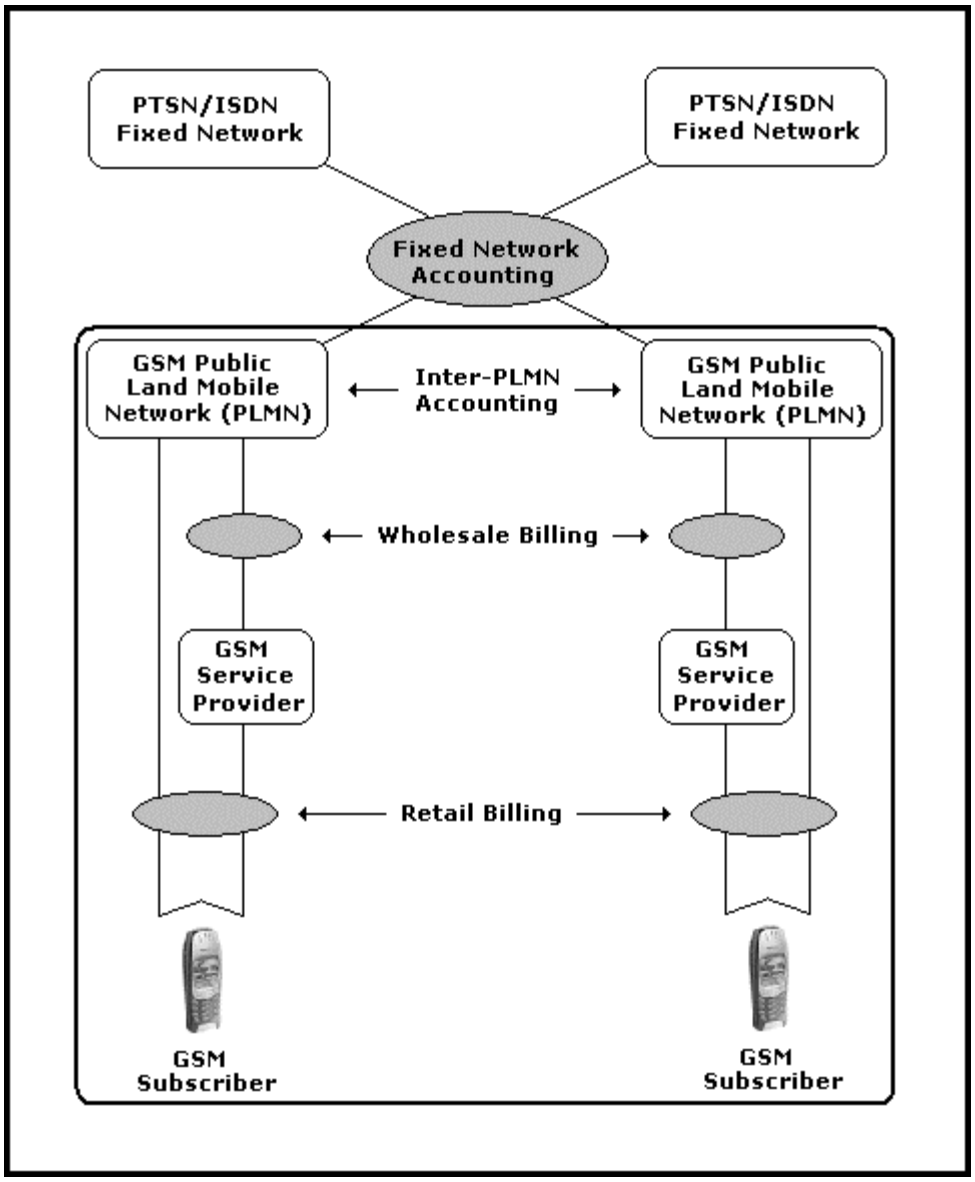

Figure 2-9 GSM Billing and Accounting System

Today, TAP3 is the most commonly used version and supports Single Circuit Switched Data as well as Packet Switched Data. TAP3 is used for billing between GSM to GSM Operators, GSM to non-GSM Operators (supporting Inter-Standard Roaming) and GSM to Satellite Operators.

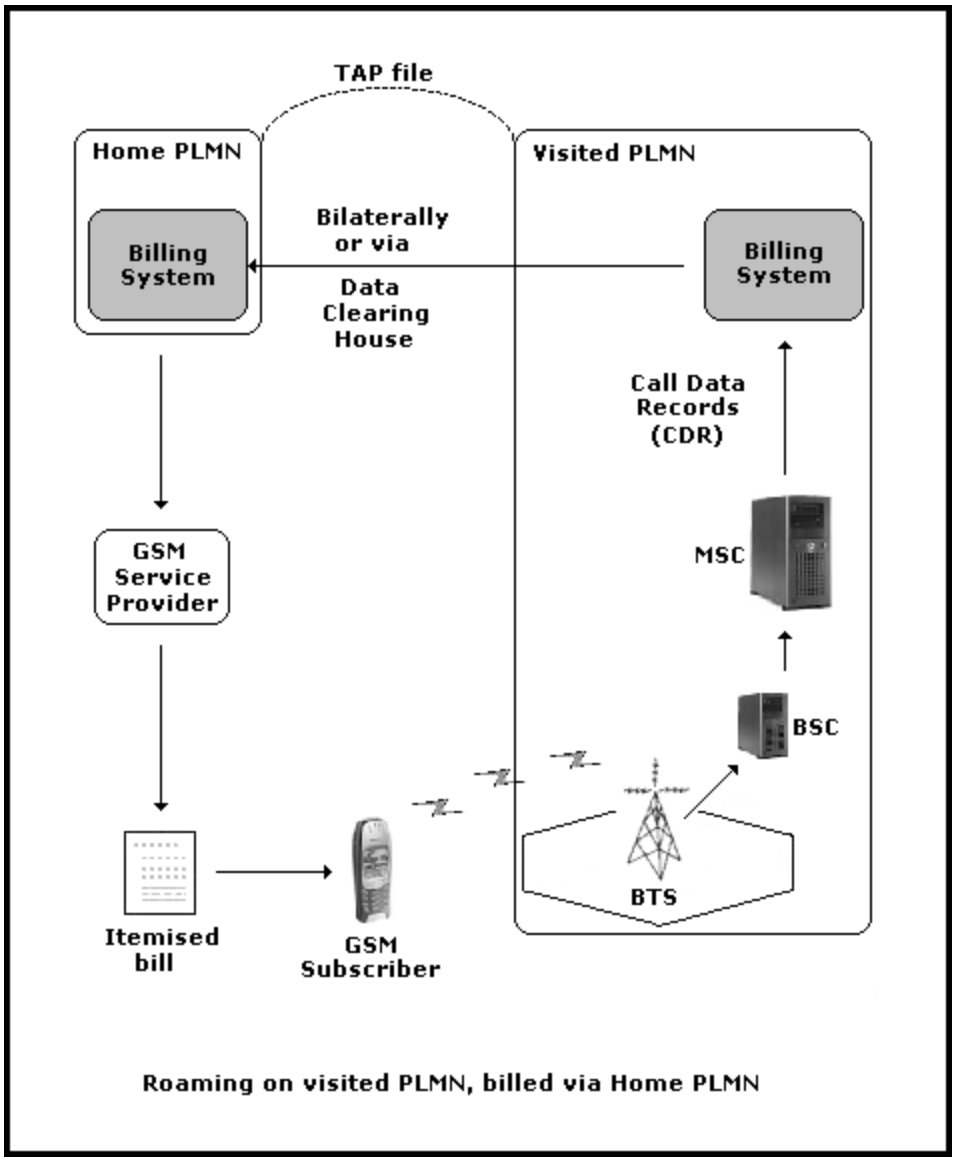

Figure 2-10 TAP information transfer between Visited PLMN and Home PLMN

The transfer of TAP records between the visited and the home PLMN may be performed directly, or more commonly via a Clearing House (see to Figure 2-10). Invoicing between the network operators usually occurs on a monthly basis.

If a service provider serves a subscriber then the records will form the basis of the wholesale billing between the Home PLMN and that GSM Service Provider. On receipt of the information from the Home PLMN, the GSM Service Provider may adjust the data record according to its own tariff rates and produce an itemised bill for the subscriber.

2.9 Future networks and Security

Universal Mobile Telecommunications System (UMTS) is a framework developed in an effort coordinated by the International Telecommunications Union (ITU) to support "third-generation" or 3G wireless communications services. UMTS is also referred to as International Mobile Telecommunications (IMT-2000) and is the successor of GSM. UMTS is a standard that will make it possible for speeds up to 2 Mbps and offer packet-based services to mobile computer or mobile phone users.

UMTS will introduce enhancements to the GSM security architecture by incorporating the following [Aso]:

- Mutual authentication: The serving network is authenticated to the mobile subscriber, as well as the mobile subscriber authenticated to the network.
- Increased support for security and data encryption in the core network.
- Increased key lengths to combat brute force attacks; keys for signal encryption in UMTS will be 128 bits.
- User identity confidentiality will be enhanced through the use of group keys.
- The basic UMTS cryptographic algorithms will be made public, addressing a frequent criticism of GSM, i.e. security by obscurity.
- Support for data integrity as well as confidentiality will be provided.

The private-key architecture of UMTS addresses many of the shortcomings of the "second-generation" (2G) cellular systems, including authentication of the network to the mobile station, user identity and location confidentiality, data integrity, and the use of proprietary cryptographic algorithms [Cur].

2.10 Conclusion

Global System for Mobile Communication (GSM) is a comprehensive wireless mobile telecommunications system. This chapter provided a brief overview of GSM, covering important aspects such as security, mobility management, subscriber authentication, billing and radio link management. GSM has been around for a number of years and has proved a worldwide success. Weaknesses in 2G cellular systems (GSM)

have been identified, rectified and deployed in 3G cellular systems (UTMS). The future can only yield an improved wireless mobile communications system.

The concept of location or the positioning of a Mobile Station (MS) in a GSM network has led to the advent of what has become known as location-based services. In other words, providing a service to a GSM subscriber based on their location. In the next chapter Location-Based Techniques within GSM networks are discussed.

Chapter 3

3. MOBILE LOCATION DETERMINATION TECHNOLOGIES

3.1 Introduction to Mobile Location Technologies

Location can be defined as the knowledge of the location of an object or an individual. A Location-Based Service (LBS) is a service where location is used to personalize a service. These services allow for many useful applications whether it is in a personal or business capacity.

Perhaps the greatest enabling force behind the growth of such services is the Federal Communications Commission (FCC) mandate [Dur]. The interest in radio location algorithms originates from the need to guarantee emergency services to calls made by mobile phone users [Por]. At the beginning of October 2001, the FCC required that emergency calls made from mobile phones must be located within 125m at accuracy of 67%. In the year 1998, the European Commission established a universal 112 call number to support emergency services to both landline and mobile users throughout Europe [Jon]. 112 calls will enable European Union (EU) members to dial for emergencies [Ref].

Location-Based technology consists of the following genres [Sne]:

- Tracking
- Positioning

In Tracking, position is computed by an external source, such as the underlying GSM Network [Mou][chapter 2]. In Positioning however, an object is concerned with being able to compute its own location. Positioning can further be divided into Absolute Positioning (exact position of an object) and Relative Positioning (measuring the movement of an object). In addition, Positioning encapsulates the idea of containment, concerned with the checking of whether an object falls within certain restricting limits [Zim].

There are many beneficial services that arise from Location-Based information. A few examples include:

- Location sensitive billing
- Location of emergency calls
- Descriptive directions
- Mobile directory list of common places
- Tracking of a commodity
- Location-Based messaging (i.e. advertising)

At an elementary level, location can be determined mathematically by calculating the distance using a time interval approach between an object and a fixed known location point known as the Location Measurement Unit (LMU). In the GSM architecture and for future 3G Networks, this location can be determined by calculating the distance between the Base Transceiver Station (BTS) and the Mobile Station (MS). Another elementary level approach would be to determine location according to a mapped area and defining location according to coordinates within that mapped area. For example, consider a mapped area as a city map or as a map of the world. Location in the latter would be described as a longitudinal and latitudinal coordinate. The Global Positioning System (GPS) is a free-to-use global network of 24 satellites run by the US Department of Defense. This means that anyone with a GPS receiver can receive their satellite position as longitude and latitude coordinates relative to a mapped area [Hof].

The focus in this chapter is to examine technologies currently available in determining mobile user location. The first section focuses on different methods in determining location. The use of Global Positioning technologies in determining a mobile user's location is also assessed. The pros and cons of each mobile location method are investigated. The location determination accuracy of all the technologies is finally considered.

3.2 Overview

There are three generic location determining methods [Agr]:

- Proximity
- Triangulation (lateration)
- Scene analysis and pattern recognition

In GSM, both proximity and triangulation are made use of as location determining techniques. Signal strength is often used to determine proximity and range of a Mobile Station (MS) while triangulation is

used when there are a number of fixed known elements available to determine the location of a Mobile Station (MS).

There are several location technologies currently deployed in wireless location determination. They include [Jon]:

- Cell-ID (CGI) and TA
- Angle of Arrival (AOA)
- Time of Arrival (TOA)
- Time Difference of Arrival (TDOA)
- Enhanced Observed Time Difference (E-OTD)
- Assisted GPS (A-GPS)

The CGI and TA, AOA, TOA and the TDOA approaches belong to a network-based solution and fall into the Tracking genre of Location technologies. A-GPS is considered to belong to a handset or mobile-based solution and falls into the Positioning genre of Location technologies. Lastly the E-OTD approach is considered to be a hybrid of the network-based and mobile-based solutions.

In all Location methods geometric concepts are used. Triangulation is used to determine position by measuring the bearings of an object from fixed points. These fixed points are the Base Transceiver Stations or Global satellites. Trilateration is used to determine position by measuring distance, where distance is relative to time in a perfect radio transmissions environment. See Figure 3-1 for an illustration of triangulation and trilateration.

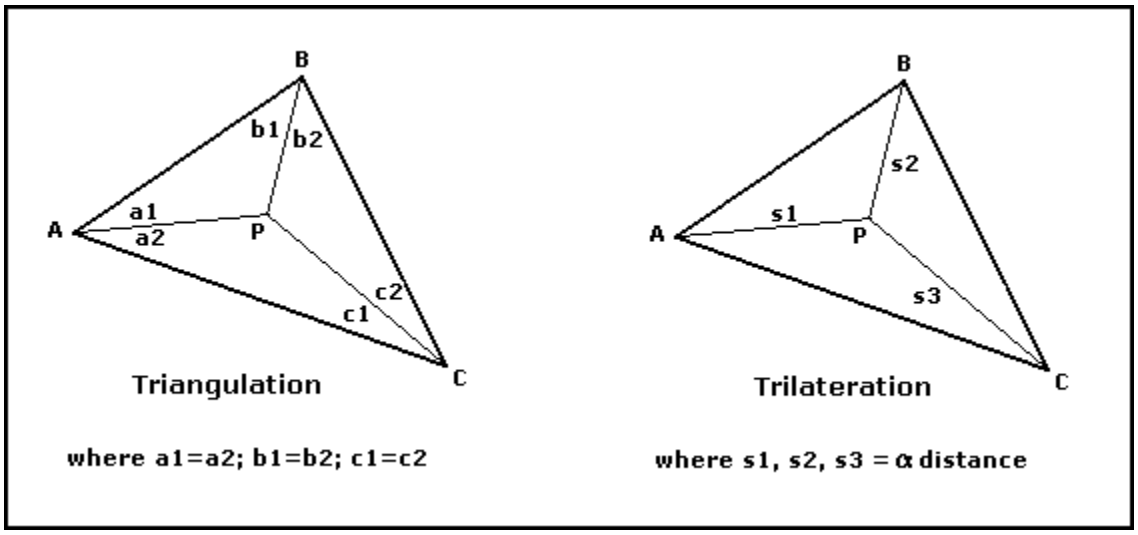

Figure 3-1 Triangulation and Trilateration - Geometric analysis of Positioning

3.3 Sources of Error in Location Estimation

Within any Radio Frequency (RF) environment there are many variables that may influence a system (e.g. atmospheric conditions). Therefore precision, particularly where positioning is being calculated, is influenced and the error of precision thereof must be accounted for. This is known as delusion of precision (DOP). The main sources of error in location methods can be attributed to:

- Multipath propagation
- Unsynchronized Base Transceiver Station Clocks

3.3.1 Multipath Propagation

Multipath propagation will affect any location method that is based on determining location using time. Multipath propagation, as depicted in Figure 3-2, causes error in time estimates and therefore affects all time-orientated location methods. The signals reflect and therefore take a longer path, causing a delay as opposed to taking a direct path. Because multiple copies of the same signal can arrive at different time intervals, it is difficult to estimate the arrival of the initial signal. This is a DOP and accuracy is diminished.

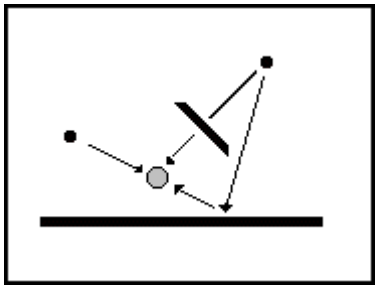

Figure 3-2 Multipath propagation

3.3.2 Unsynchronized Base Transceiver Stations Clocks

GSM networks are normally not synchronized [Jon]. It is important that BTS clocks are synchronized as they can give an error of approximately 15-60m [0510]. This error may become unimportant in future "third-generation" or 3G networks.

Due to the fact that Base Stations (Cell sites) will in future be more densely populated and smaller in size, the accuracy of positioning determination is expected to improve.

3.4 GSM Location Services (LCS) Architecture

Location Services (LCSs) are logically implemented on the GSM structure through one additional network node, the Mobile Location Centre (MLC). Figure 3-3 shows the logical architecture of a generic Location Services (LCS). It is important to note that other elements such as a Cell Broadcast Centre (CBC) may be associated with a Base Station Controller (BSC) and the Serving Mobile Location Centre (SMLC). Additional elements are not covered in this chapter, however please refer to [0341] for more information on elements such as the Cell Broadcast Centre (CBC).

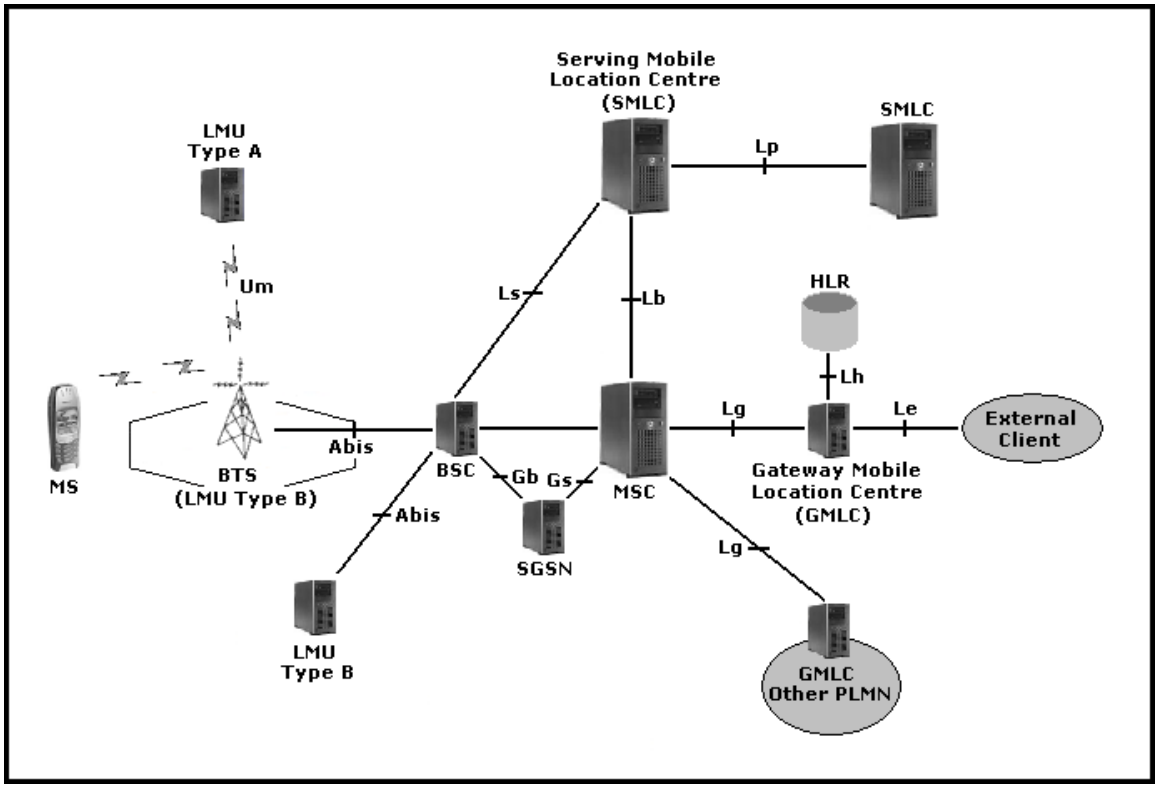

Figure 3-3 Generic Location Service (LCS) architecture

3.4.1 Location Measuring Unit (LMU)

An LMU (see Figure 3-3) produces radio measurements to support one or more location technologies. Two types of LMU exist, namely:

- Type A LMU
- Type B LMU

The type of LMU is dependant on how it communicates with the Base Station Transceiver (BTS). An LMU of Type A can only be accessed via GSM Over The Air interface, meaning there is no wired connection to any other network element. An LMU of Type B is accessible over the Abis interface from the Base Station Controller (BSC).

3.4.2 Serving Mobile Location Centre (SMLC)

The SMLC (see Figure 3-3) manages the overall coordination and scheduling of resources required to perform positioning of an MS. It is also involved in calculating the final location estimate and the accuracy thereof. The SMLC controls a number of LMUs for the purpose of obtaining radio interface measurements to locate, or help locate MS subscribers in the area that it serves [0371].

3.4.3 Gateway Mobile Location Centre (GMLC)

The GMLC is the first node from which external access can be obtained for a client to send location information requests and then receive final location estimates and accuracy.

Additional interfaces exist between the conventional GSM components and the GSM location components. Some of these are highlighted in Table 3-1.

3.4.4 List of Interfaces

Abis	Interface between Location Measurement Unit (LMU) of Type B to BSC
Lb	Interface between Serving MLC (SMLC) and BSC
Le	Interface between External Client and MLC
Lh	Interface between Gateway MLC (GMLC) and HLR
Lg	Interface between Gateway MLC (GMLC) and MSC/VLR
Lp	Interface between SMLC and peer SMLC
Ls	Interface between Serving MLC and MSC/VLR
Um	Um Over The Air Interface to an Location Measurement Unit (LMU) of Type A

Table 3-1 Location Services (LCS) interfaces

3.5 Location-Based Technologies

Location-Based Technologies reside in three forms:

- Network-Based Solution
- Mobile-Based Solution
- Hybrid, which is a combination of both Network-Based and Mobile-Based Solution

In the next section we will look at Network-Based location technologies. It is important to note that more location technologies exist than are covered in this chapter. In Network-Based Solutions, emphasis will be placed on Cell-ID (CGI)/TA, Angle of Arrival (AOA), Time difference of Arrival (TDOA) and Time of Arrival (TOA) methods.

3.5.1 Network-Based Technologies

3.5.1.1 Cell-ID (CGI) and TA

The Cell-ID (CGI) and TA method involves only minor updates to the Network and is currently supported in most Networks. It works with existing MS without any modification. Cell Global Identity (CGI) uses the identity of each cell with coverage area of a BTS to locate an MS. The CGI identifies the cell in which the MS is located (Figure 3-4). This is often complemented with the Timing Advance (TA) parameter to determine the MS's location. The TA parameter is an estimate of the

distance from the MS to the serving BTS. TA values are divided into 64 slots (0-63), each with a radius of 550m [Jon]. By incorporating the TA value, location accuracy can be increased further than by simply making use of the cell identity. The location of the MS can be narrowed to a circle or a sector in steps of a 550m radius from the BTS. The accuracy of this method varies according to the size of the cell where the radius of the cell can vary from anything from 100m to +32Km. Accuracy can be further increased if it is known that the cell is an omni directional cell or triangular cell (refer to Figure 3-4).

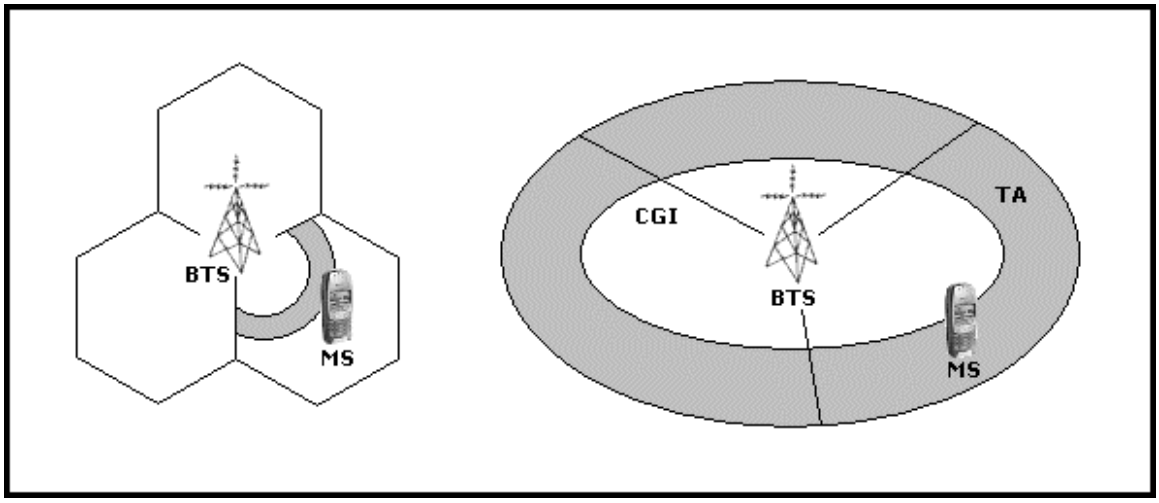

Figure 3-4 Cell-ID (CGI) and TA

3.5.1.2 Angle of Arrival (AOA)

The Angle of Arrival (AOA) method involves the analysis of the Angle of Arrival of the signal between the Mobile Station (MS) and the Base Transceiver Station (BTS). Calculations are performed on the AOA in determining the mobile device position. Figure 3-5 is a simple representation of how position can be determined from the AOA method. In Figure 3-5, A and B represent the cell site or BTS and P represents the Position from the intersection of lines formed from angles of arrival at A and B.

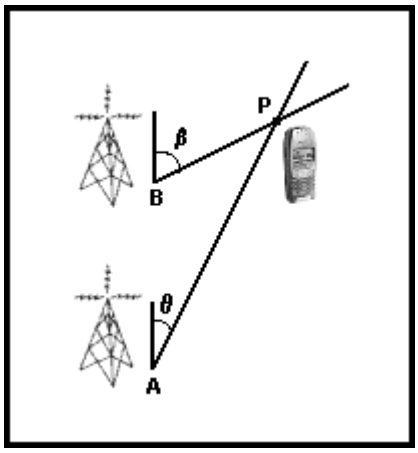

Figure 3-5 Representation of the Angle of Arrival method

The Angle of Arrival method leverages the underlying Network in order to determine location. This method has an impact on the Network, as the Network must perform location calculation and control [Bir]. Additional antenna and cabling (hardware) must be added to the BTSs (Sites) to accommodate the AOA location method. There is no impact on the MS device itself as this method is a Network-Based solution. As MSs are not affected in any way by using AOA, legacy mobile devices are covered by this method.

With the AOA method, a minimum of 2 BTSs (Cell Sites) measure the arrival angle of the MS transmission. The basis of this location solution resides in apparent angle arrival of the received signal. Typically the AOA technique is used to augment the TDOA approach of a location system. A good example of AOA is evident on a major highway where the BTSs are arranged along the length of the highway.

3.5.1.3 Time of Arrival (TOA)

The Time of Arrival method leverages the underlying Network in order to calculate the position of the MS. This method works by having all BTSs within range of a certain MS listen to bursts of signals received by that MS. When a BTS receives a burst of signal from the MS it records the time it was received, position is then determined using these recorded times. Additional hardware (LMUs) may be required to accurately measure the arrival of the bursts or alternatively the measuring units may be integrated into existing BTSs. At a position request, the MS is forced to perform an asynchronous handover. By forcing the MS handover the network receives up to 70 access bursts

which will be used for location determination. Position is then calculated using triangulation (refer to Figure 3-1). Of critical importance is that the Base Stations clocks are synchronized to allow for accurate recording of signal bursts from MSs. Accuracy of this method varies when propagation of the received signals occurs. A minimum of three BTSs (Cell Sites) must exist in order to measure and record arrival times of MS transmissions. In Figure 3-6 the Time of Arrival Method is depicted, where A, B and C represent the Base Transceiver Stations and P represents position of the MS. Once again this method is a Network-Based solution and there is no resultant effect on the MS and therefore latency or legacy mobiles are also included within this location solution.

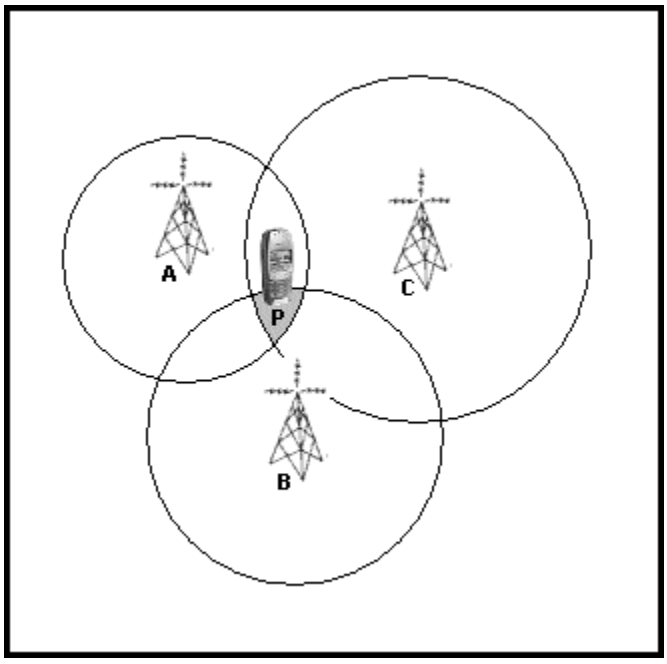

Figure 3-6 TOA method using circles as interception points

3.5.1.4 Time Difference of Arrival (TDOA)

This method involves measuring the Time Difference of Arrival of an MS signal at three or more BTSs. The Serving Mobile Location Centre (SMLC) calculates the TDOA values by pair-wise subtracting the TOA values. It is important to notice that this method works by only calculating the time differences in arrival at the BTSs. Time difference can be used as a technique as radio waves travel at a fixed known rate, i.e. the speed of light, and because of this it is possible to calculate the MS position via hyperbolic trilateration (Figure 3-7). In

Figure 3-7 - A, B and C represent BTSs and P the Intersection of two hyperbolas. The first hyperbola is calculated from the Time Difference of Arrival between C and A, and the second is calculated from the Time Difference of Arrival between B and A. The Time Difference of Arrival method leverages the underlying Network in order to determine location. The Network must perform location calculation and control [Bir]. It is important to note that in the (TDOA) MS position calculation method; there are two associated assumptions when finding the MS location:

- The geographical coordinates of the measurements are known
- If any timing offset exists between the measuring units, that these measurement are known

There is no impact on the MS device itself as this method is a Network-Based solution and as a result latency or legacy MSs are covered.

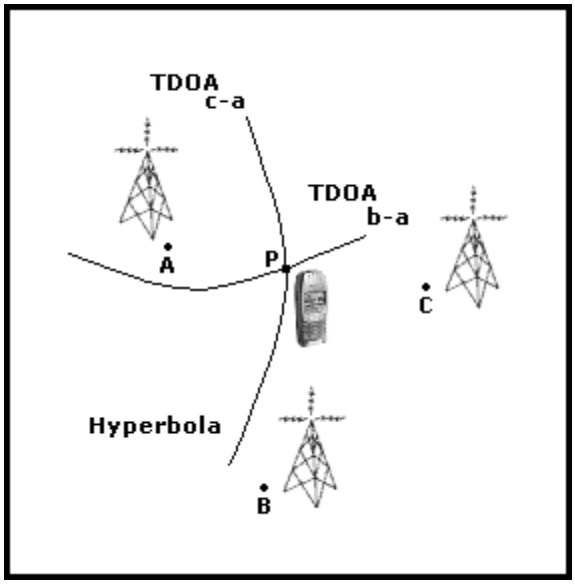

Figure 3-7 TDOA method using hyperbola

A minimum of three BTSs (Cell Sites) measures the arrival time of MS transmissions. In multi-path environments typically urban areas measurements may have to be taken from four BTSs in order to overcome the effects of multi-path propagation. The location solution is based on apparent arrival time differences between pairs of BTSs.

In the next section we will take a look at Mobile-Based Technologies. The Assisted Global Positioning System (A-GPS) method will cover the

Mobile-Based Solution followed by the Enhanced Observed Time Difference (E-OTD) method which forms part of a Hybrid solution (using both Mobile and Network to determine position).

3.5.2 Mobile-Based Technologies

3.5.2.1 Assisted Global Positioning System (A-GPS)

GPS is a wide-area positioning system [Hof]. In GPS, each satellite transmits a unique code. A copy of this code is created in real time in the receiver set. The receiver then gradually time shifts its internal clock until it corresponds to the received code, this event is known as lock-on. Once lock-on to a satellite has occurred, the receiver can then determine the exact time of the received signal in reference to its own internal clock.

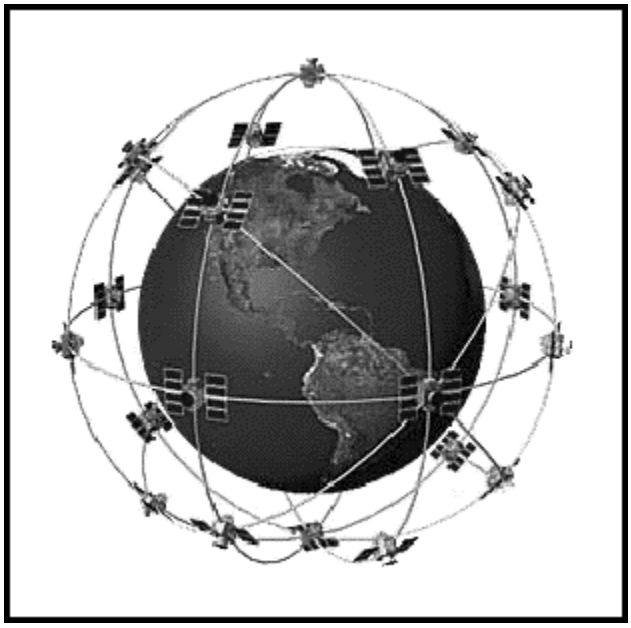

Figure 3-8 24 satellite positioning that constitutes GPS [Zim]

The Global Positioning System (GPS) is a free-to-use global network of 24 satellites run by the US Department of Defence launched in 1994. The Russian version is known as GLONASS. Figure 3-8 is a reference of how these satellites reside in six orbital planes.

A-GPS makes use of a GPS receiver in the MS to find location. When a GPS receiver receives a signal from the satellites, the time of arrival of the signal is used to calculate the receiver's position [Jon]. Although this is a Mobile-Based solution there is an impact on the Network, as the Network must provide for GPS assistance and location calculation [Bir]. The reason for this is merely because when a GPS receiver is switched on it does not know its location and thus takes some time for the GPS receiver to obtain information about its location. A solution to this problem is to leverage the network in providing additional information about the MS's location and hence the name Assisted GPS.

A GPS terminal needs to be able to see four or more satellites and for the A-GPS positioning system there must be a minimum of one BTS (Figure 3-9). The location solution is based on apparent TOA from the GPS satellites. This method has high accuracy outdoors but is ineffective indoors and in dense urban areas as functionality depends entirely on contact with the GPS satellites.

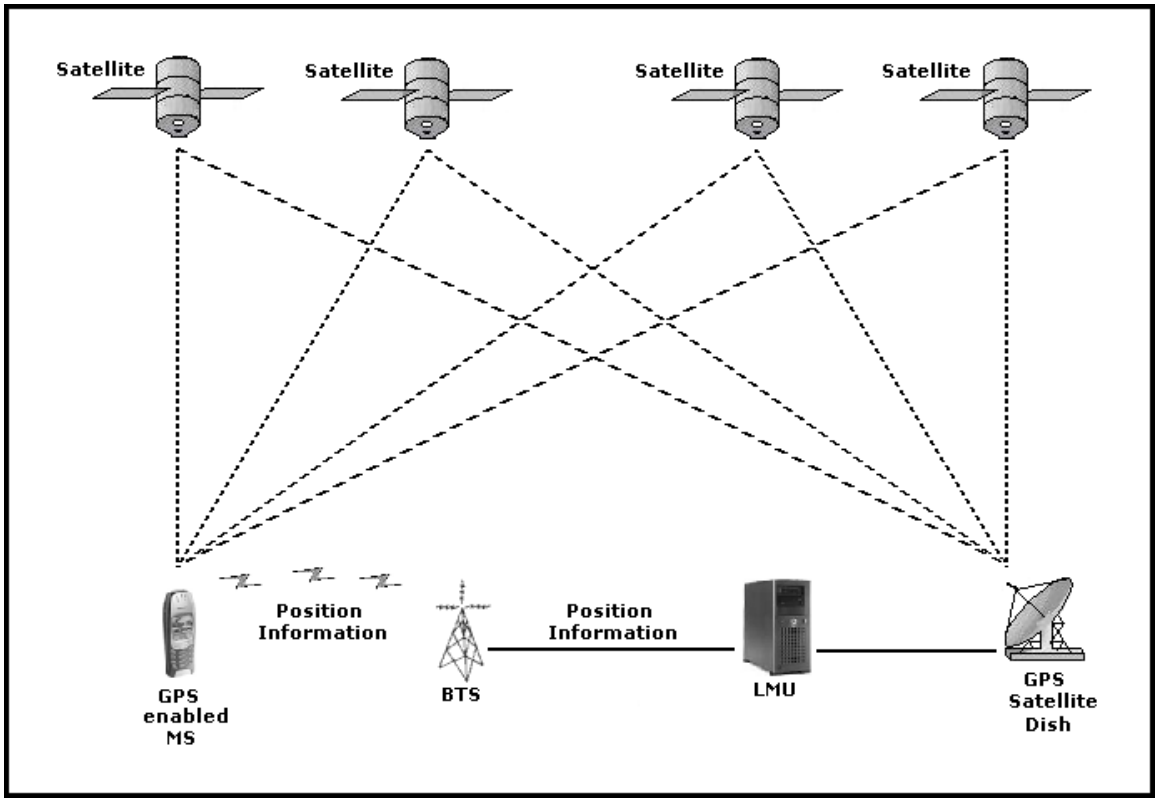

Figure 3-9 Assisted GPS (A-GPS)

This method involves an impact on the MS itself and as a result, latency or legacy MSs are not covered. The reason is that GPS uses a higher frequency band than GSM and therefore MSs must be equipped

with two antennas that can accommodate GPS and GSM respectively. Another factor influencing the MS is that a GPS receiver has high power consumption and therefore new MSs require higher battery capacity.

3.5.3 Hybrid Technologies

3.5.3.1 Enhanced Observed Time Difference (E-OTD)

The Enhanced Observed Time Difference (E-OTD) method is based on measured Observed Time difference (OTD). OTD is the measure of Time Difference between BTSs. Generally the E-OTD method relies on measuring the time at which signals from the BTS arrive at two geographically different locations. The two locations would be the MS itself and a known fixed location measuring point known as the Location Measurement Unit (LMU). E-OTD comes in two forms, namely Circular Variant (E-OTD-C) and hyperbolic variant. The two methods differ only in the relationship between the MS measurement error margin and the location of the MS, which is relative to the BTSs. The two methods are covered later in this section.

This method uses the TOA/TDOA solution in the handset while leveraging the Network for location calculation and control. This is a hybrid solution and there is an impact on the MS and the Network. The MS needs memory and a software upgrade to accommodate E-OTD and as a result latency or legacy models are not covered with this method. The Network either has to undergo time synchronization enhancement or site time error measurement and calibration (LMUs) [Bir]. The Real Time Differences (RTD) between Base Transceiver Stations is measured by a LMU. Arrival time of transmissions must occur from a minimum of 3 BTSs.

Two variants of this model exist. They are:

- Circular E-OTD (E-OTD-C)
- Hyperbolic E-OTD

3.5.3.2 Circular E-OTD (E-OTD-C)

The E-OTD Circular variant measures the arrival of time from each of the BTSs individually at the MS and LMU. This method uses the Time of Arrival (TOA) approach.

There are five quantities associated with this method [0371]:

- The observed time from a BTS to the MS (MOT) is a time measured against the internal clock of the MS
- The observed time from a BTS to the LMU (LOT) is a time measured against the internal clock of the LMU
- Time offset ε is the bias between the two internal clocks of the MS and LMU
- The distance from the MS to BTS (DMB)
- The distance from the LMU to BTS (DLB)

The relationship of these quantities can be expressed in the following equation [0371]:

$$DMB - DLB = c(MOT - LOT + \varepsilon)$$

Figure 3-10 E-OTD-C Equation associated with each BTS

where c is representative of the speed of the radio signals. There will be one such equation for each BTS. This method requires a minimum of three BTSs to calculate location since unknown quantities exist in the equation namely, the MS position and the clock offset ε.

The estimate of the position of the MS is defined as the intersection of circles centred on the BTSs common observations made by the MS and LMUs (Figure 3-11). In Figure 3-11 d_1, d_2, d_3 represents the length of the propagation paths from the BTSs to the MS.

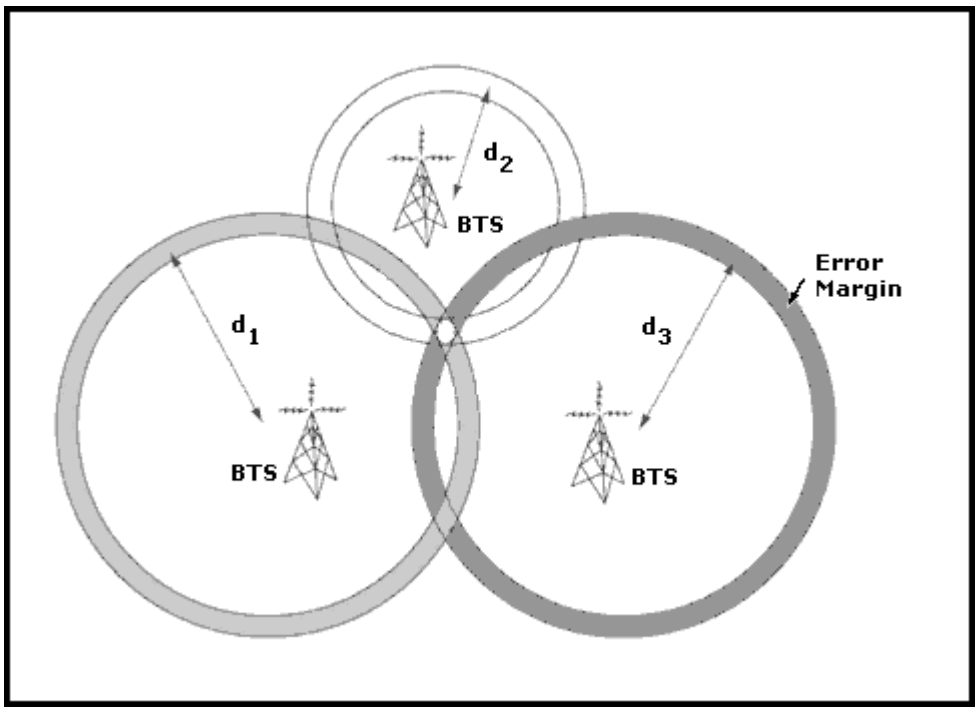

Figure 3-11 The E-OTD-C method

There is an uncertainty associated with the radius of the circle formed and is classified as an error margin measurement. A confidence region, an ellipse, defines the overlapping of the resultant area. The length of the axes and its origin describes this ellipse. Figure 3-12 describes the intersecting circles and elliptical confidence region.

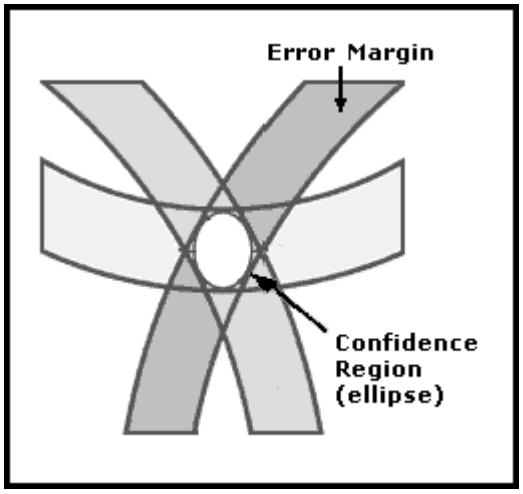

Figure 3-12 Intersection region of E-OTD-C method

3.5.3.3 Hyperbolic E-OTD

The Hyperbolic E-OTD method is similar to E-OTD-C except that hyperbolas are calculated from the GTDs (Figure 3-14). This method uses the Time Difference of Arrival (TDOA) approach. Position can be formulated with formulas describing hyperbolas having their foci at the BTSs coordinates. The intersection of the hyperbolas constitutes an exact solution, which defines the location of the MS.

There are three basic timing quantities associated with E-OTD location. They are defined as follows [0371]:

- Observed Time Difference (OTD). This is the time interval that is observed by an MS between the receptions of signals (bursts) from two different BTSs. A burst from the BTS 1 is received at the moment t1, and a burst from the BTS 2 is received at the moment t2. Thus the OTD in this case is: OTD = t2 - t1. If two bursts arrive at exactly the same moment, then OTD=0.
- Real Time Difference (RTD). This is the relative synchronization difference in the network between two BTSs. If the BTS 1 sends a burst at moment t3, and the BTS 2 at the moment t4, the RTD between them is: RTD = t4 – t3. If the BTSs transmit at exactly the same time that means the network is synchronized, and hence RTD=0. RTDs' values are measured by the LMUs in the network.
- Geometric Time Difference (GTD). This is the time difference between the receptions of MS bursts from two different BTSs due to geometry. If both BTSs are equally far from the MS, then GTD=0.

The relationship between these quantities is (Figure 3-13):

$$GTD = OTD - RTD$$

Figure 3-13 Determining Geometric Time Difference

OTD is the quantity measured by the MS to be located. RTD is the quantity related to the network. GTD is the quantity related to the geometric situation, which represents the positions of the MS and BTSs. GTD is the actual quantity that is useful for location purposes, since it can provide information about the position of the MS [Jon].

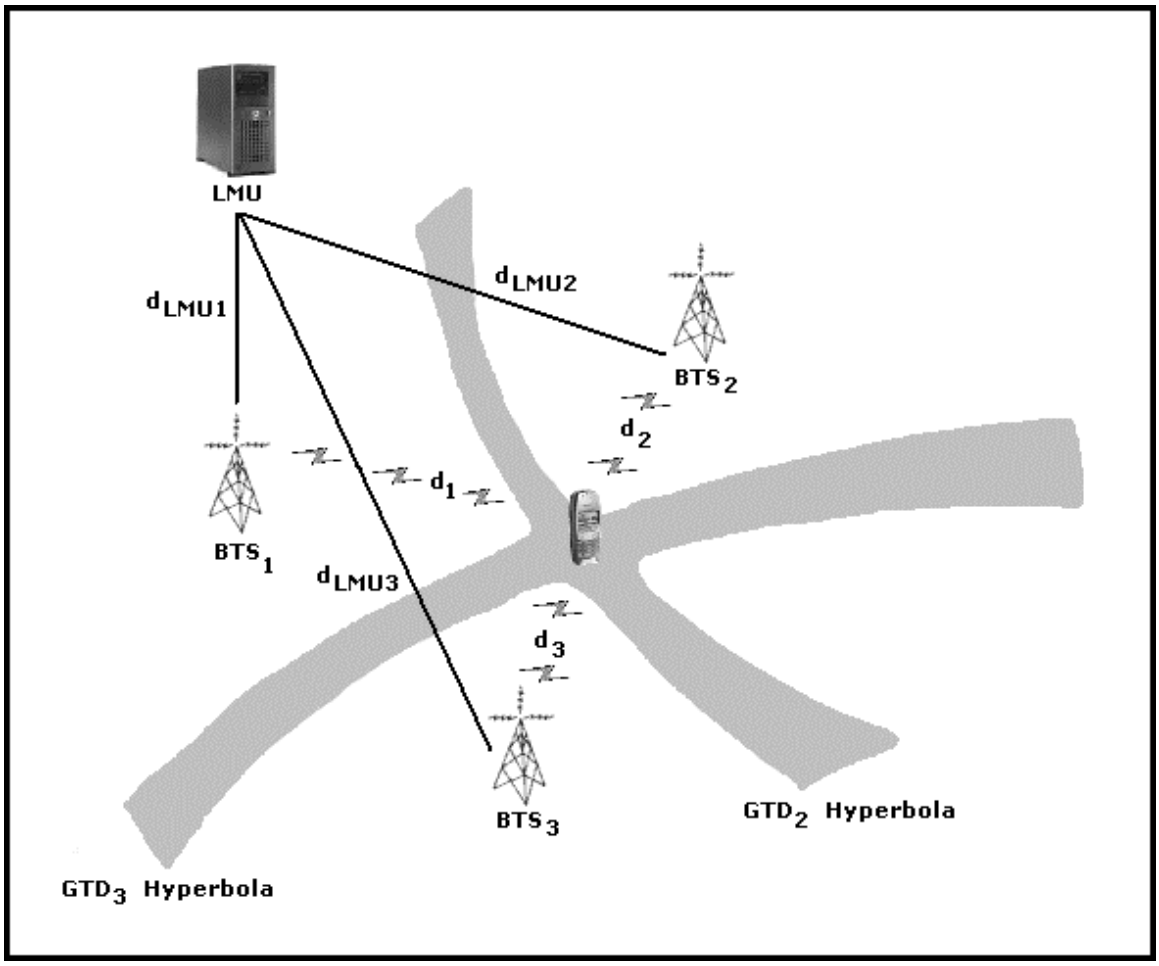

Figure 3-14 The hyperbolic E-OTD method

There is an uncertainty associated with the hyperbolas formed from the GTD constant and this is known as an error margin. In Figure 3-14 d_1, d_2, d_3 represent the length of the propagation paths from the BTSs to the MS. Likewise d_{LMU1}, d_{LMU2}, d_{LMU3} represents the length of the propagation paths from the BTSs to the LMU.

3.6 Comparison of Technologies

A brief comparison and summary of the location technologies mentioned within this chapter is presented (Table 3-2).

Method	Accuracy	Coverage		Effect	
		Indoor	Outdoor	Mobile	Network
CGI & TA	Estimate: 100-1000m Accuracy depends on cell size (coverage) whether pico cell or BTS used	Yes	Yes	None	Mobile Location Centre (MLC)
AOA	Estimate: 300m	Limited	Yes	None	Directional antennas (BTSs) & Mobile Location Centre (MLC)
TOA	Estimate: 50-200m Better accuracy than CGI & TA, but not as good as A-GPS	Yes	Yes	None	Mobile Location Centre (MLC) & Location Measurement Unit (LMU)
TDOA	Estimate: 50-200m Better accuracy than CGI & TA, but not as good as A-GPS	Yes	Yes	None	Mobile Location Centre (MLC) & Location Measurement Unit (LMU)
A-GPS	Estimate: 10-20m High accuracy	Limited	Yes	Additional GPS hardware (receiver)	Additional network hardware & Mobile Location Centre (MLC)
E-OTD	Estimate: 50-400m Better accuracy than CGI & TA, but not as good as A-GPS	Yes	Yes	Additional software only	Mobile Location Centre (MLC) & Location Measurement Unit (LMU)

Table 3-2 Comparison of Location-Based Technologies

3.7 The Future in Location-Based Technologies

Irrespective of the underlying architecture, positioning methodology will remain intact. This occurs due to the nature of radio signal properties and characteristics.

As previously mentioned, due to the fact that UMTS networks will be synchronized, LMUs will become redundant. The basic principles for the positioning methods will be identical to those used in GSM. Due to

the nature of UMTS networks having densely populated cells and having the entire network synchronized, accuracy of certain positioning methods is expected to improve. Future applications may require the accuracy to within meters with a low degree of error. As Mobile Stations (MSs) evolve they will undoubtedly have increased processing power and location positioning may be entirely computed at the Mobile device.

3.8 Conclusion

This chapter delved into some location-based technologies currently available in GSM networks. Different methods provide for different levels of accuracy and adaptation to existing infrastructures. Comparisons of the different location methods were provided for. In most cases a hybrid approach accommodates most requirements. It is recommended that the MS itself perform location determination if possible. This local location determination enforces privacy of location information and allows for the leveraging of underlying networks for additional information and calculations. No doubt smarter MSs as well as improved mathematical approaches will emerge resulting in location determination accuracy and performance improving.

GSM is a technology originally built for mobile voice calls; in the next chapter we introduce an addition to GSM networks for the sole purpose of data transfers.

Chapter 4

4. GENERAL PACKET RADIO SERVICE (GPRS)

4.1 Introduction to GPRS

General Packet Radio Service is a bearer service for GSM designed for digital cellular networks. GPRS like GSM is standardized by the European Telecommunications Standards Institute (ETSI). The Special Mobile Group (SMG) of ETSI is responsible for this standard [0360].

There has been impressive growth in mobile telephony in the last decade. Within the next few years, there will be an extensive demand for wireless data services. In particular, high-performance wireless Internet access will be requested by users [Bet].

The desire for wireless data services has led to the design and implementation of GPRS, often referred to as a 2.5G standard. Data applications are generally not as delay sensitive as voice applications are. GPRS has thus been designed to transfer data and signalling in an efficient way optimizing the use of radio and network resources. GPRS is designed to support intermittent and/or bursty data transfers. GPRS enables fast access to packet switched data networks, such as corporate intranets or the Internet.

The technical security offered by GPRS is very similar to that offered by GSM. Identity, user data and signalling confidentiality as well as identity authentication must be considered. In addition to the GSM standard there is the security of the GPRS backbone to consider. The detailed security of GPRS is contained within the 3GPP standards [3GP].

This chapter serves as an overview of GPRS, focusing on its security aspects. One must be familiar with the basic concepts of cellular networks and GSM to fully understand the concepts presented within this chapter. For an overview of GSM, refer to [chapter 2][Sco][Rah].

4.2 Overview

GPRS is a packet switched technique to transfer high and low speed data. Signalling is achieved in an efficient and reliable manner over GSM radio networks. GPRS greatly improves and simplifies wireless access to packet data networks. Internet Protocol (IP) and X.25 networks are supported in the current version of GPRS. GPRS allows Short Message Service (SMS) over GPRS radio channels [0360].

New GPRS radio channels are defined and anything from one to eight radio interface timeslots can be allocated per TDMA frame. Timeslots are shared by active users and uplink and downlink channels are allocated separately. The uplink channel is shared by a number of Mobile Stations (MSs), and its use is allocated by a Base Station Controller (BSC) [chapter 2.2.3]. The MS requests the use of a channel and the BSC allocates an unused channel to the MS. The downlink channel is fully controlled by the serving BSC. The radio interface resources can be shared dynamically between data and voice services as a function of load on the network or assigned according to network operator preference. In GSM, a channel is permanently allocated for a particular user during the entire voice or data call period. In contrast GPRS channels are allocated when data packets (PDUs) are sent or received and are subsequently released after the transmission ends. Various radio channel coding schemes (CS) are specified to allow bitrates from nine to more than 150 kbits per second.

GPRS improves the utilization of radio resources, offers volume-based billing, higher transfer rates, shorter access times and simplified access to packet data networks [Bet]. A first true application for GPRS could be fast access to corporate intranets [Rau].

The growth potential for GPRS is immense. To fully understand GPRS, the architecture and integration of GPRS into a GSM Network is presented in Figure 4-1.

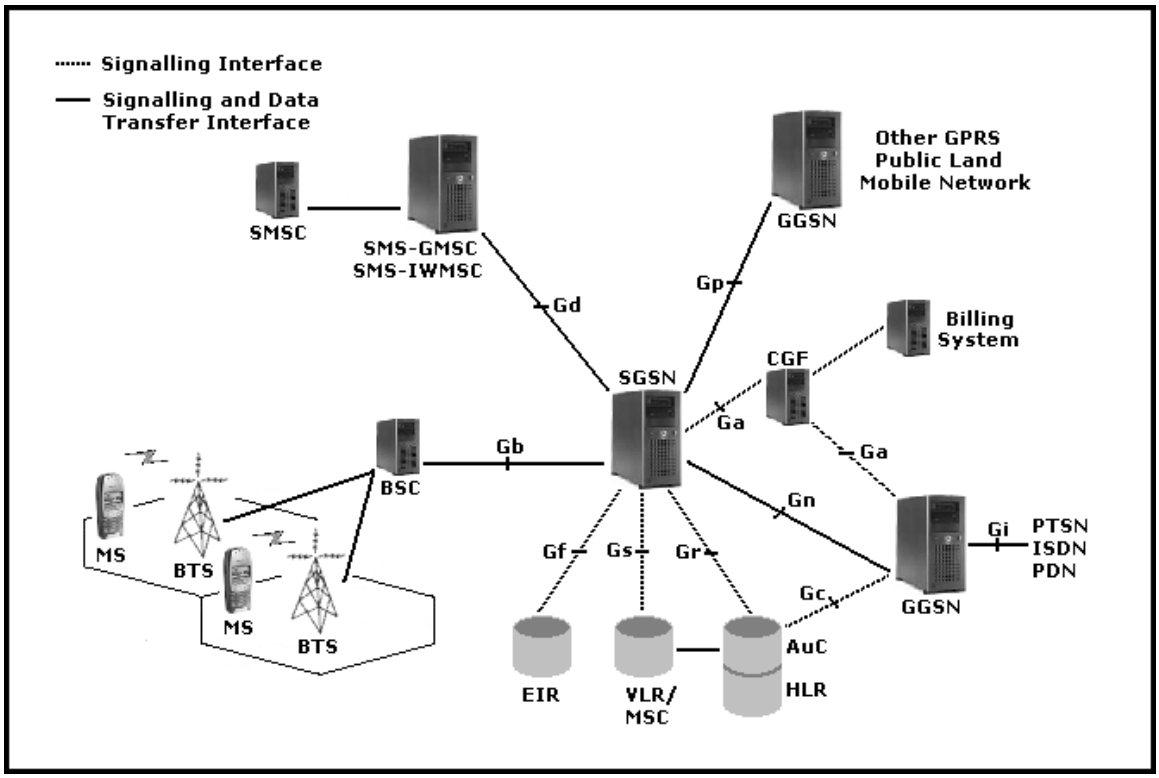

Figure 4-1GPRS Architecture

Figure 4-1 shows the most common components of the GPRS architecture (other components such as the Border Gateway (BG) may exist but are considered outside the scope of this chapter).

GPRS introduces a new class of network nodes. These are referred to as GPRS support nodes (GSN). GSNs are responsible for the delivery and routing of data packets between the Mobile Stations (MSs) and the external Packet Data Networks (PDN) [Bet]. Two additional nodes have been added to the GSM architecture, namely:

- Serving GPRS Support Node (SGSN)
- Gateway GPRS Support Node (GGSN)

The SGSN and GGSN functionalities may be combined in the same physical node, or they may reside in different physical nodes. A detailed description of these two nodes follows, illustrating how these nodes are integrated with the existing GSM components. Some GSM components require revision to include GPRS functionality and are discussed in this section.

4.2.1 Serving GPRS Support Node (SGSN)

The SGSN is responsible for the delivery of data packets (PDUs) to and from Mobile Stations (MSs). The serving GPRS Support Node (SGSN) exists at the same architectural level as the Mobile Switching Centre (MSC) [chapter 2.2.5] in the GSM Network but performs different functions. The SGSN keeps track of the individual's Mobile Station (MS) location and performs security functions and access control [0360] much like the Mobile Switching Centre (MSC) does in the GSM network. Its main functions include packet routing, mobility management, logical link management, authentication and charging. It also controls ciphering, compression and interaction with the GSM circuit switched services. The SGSN is seen as a separate node as its packet switching functionalities set it apart from any existing node within the GSM architecture. The SGSN is incorporated in the GSM architecture and is connected to the Base Station Subsystem (BSS) [chapter 2.2.4].

4.2.2 Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node (GGSN) provides Interworking with external packet-switched networks, and is connected with SGSNs via an IP-based GPRS backbone Network [0360]. The GGSN is responsible for converting incoming GPRS packets coming from a SSGN into the appropriate packet data protocol (PDP) format, either IP or X.25, and routing them out to the subsequent Packet Data Network (PDN). The GGSN stores the current SGSN address and profile of a subscriber in its location register. The GGSN also performs authentication and charging functions. Several SGSNs may use a GGSN to interface to external packet data networks and an SGSN may route packets to different GGSNs in order to reach different packet data networks. The GGSN is also seen as a separate node as no current GSM node provides for Interworking with existing packet-switched networks.

4.2.3 GPRS Backbone

All GPRS Support Nodes (GSNs) are connected via an IP-based GPRS backbone. Within the GPRS backbone the GSNs encapsulate data packets, transmitting them using the GPRS Tunnelling Protocol (GTP). GTP is a secure 128 bit encryption protocol tunnelling through IP, also

referred to as GTP/IP. For more on the GPRS Tunnelling Protocol (GTP), see [0960]. Encapsulation refers to the addition of address and control information to a data unit for routing packets within and between PLMNs [0360].

Two kinds of GPRS Backbone Networks exist:

- Intra Public Land Mobile Network (Intra-PLMN) backbone network. GSNs are connected on the same PLMN and are considered to be a private IP-based network (refer to Figure 4-2).
- Inter Public Land Mobile Network (Inter-PLMN) backbone network. GSNs are connected on different PLMNs. Roaming agreements are necessary between GPRS network providers to make this backbone network plausible (refer to Figure 4-2).

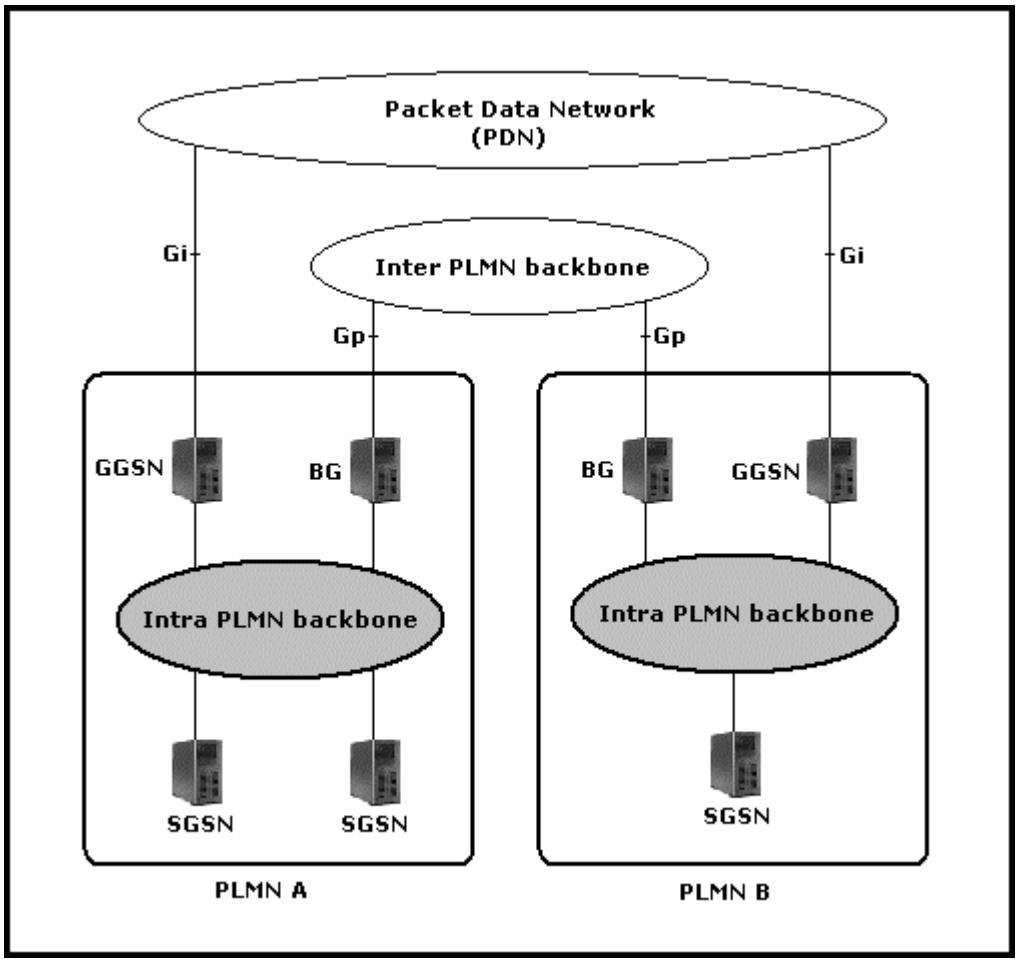

Figure 4-2 Intra-PLMN and Inter-PLMN backbone networks

Every intra-PLMN backbone network is a private IP network intended for GPRS data and GPRS signalling only [0360]. Two intra-PLMN

backbone networks are connected via the Gp interface using Border Gateways (BGs) and an inter-PLMN backbone network (Figure 4-2). The Inter-PLMN backbone can be a Packet Data Network (PDN) for example the public Internet or leased line.

The GTP tunnels the subscriber's data packets and related signalling information between the GPRS support nodes (GSNs). The GTP is defined both between GSNs within one PLMN and between GSNs in different PLMNs.

4.2.4 GPRS Mobile Station (MS)

In order to use GPRS, Mobile Stations (MSs) must be GPRS compatible. Three GPRS MS modes of operation are supported:

- Class-A mode of operation - operates GPRS and other GSM services simultaneously
- Class-B mode of operation - monitors control channels of both GPRS and GSM services simultaneously but can operate only one service at a time
- Class-C mode of operation operates GPRS services exclusively

The majority of MSs used in South Africa are of the Class-B mode of operations type. This typically means when an MS is in an active GSM service for example a voice call, no GPRS traffic can switch between the MS and an external Packet Data Network (PDN). Likewise if the MS is in the process of an active GPRS service for example downloading email, no GSM service can take place.

4.2.5 List of Interfaces

A summary of the interfaces that exist within a GSM-GPRS Architecture (refer to Figure 4-1) is provided in Table 4-1.

Ga	The charging data collection interface exists between Call Detail Record (CDR) transmitting unit, i.e. the GGSN and a Call Detail Record (CDR) receiving unit, i.e. the Charging Gateway Functionality (CGF).
Gb	Interface between an SGSN and a Base Station Subsystem (BSS). The Gb Interface allows the exchange of signalling information and user data. It allows many users over the same physical resource. Gb is defined in [0814].
Gc	Interface between a GGSN and a HLR. The GGSN may request location information from the HLR via the optional Gc interface.
Gd	Interface between an SMS-GMSC and an SGSN, and between an SMS-IWMSC and an SGSN.
Gf	Interface between an SGSN and an Equipment Identity Register (EIR).
Gi	Reference point between GPRS and an external Packet Data Network (PDN). Gi is defined in [0961].
Gn	Interface between two GGSNs within the same PLMN.
Gp	Interface between two GGSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the cooperating GPRS PLMNs. The Gp interface is functionally identical to the Gn interface except that it provides for security functionality required for the inter-PLMN communication.
Gr	Interface between an SGSN and a Home Location Register (HLR).
Gs	Interface between an SGSN and an MSC/VLR. The SGSN may send location information to the MSC/VLR via the optional Gs interface. For more on the Gs interface, see [0918].

Table 4-1 GPRS Interfaces

4.2.6 Home Location Register (HLR)

The HLR is an existing database that contains GSM subscriber information. With the addition of GPRS services, the HLR includes GPRS subscription data and routing information. The HLR is accessible:

- From the SGSN via the Gr interface
- From the GGSN via the Gc interface

If an MS is roaming (connected to a network other than its home network) the HLR will exist in a different PLMN than the SGSN currently being used.

4.2.7 Short Message Service Gateway MSC (SMS-GMSC) and Short Message Service Interworking MSC (SMS-IWMSC)

SMS-GMSC and SMS-IWMSC are connected via the Gd interface to the SGSN. This allows GPRS-enabled MS to send and receive Short Messages (SMSs) over GPRS.

4.2.8 Charging Gateway Functionality

The Charging Gateway Functionality (CGF) is described in [1215].

New nodes and various adapted components have been covered in the GSM-GPRS architecture. In the following section we describe how an MS registers with the GPRS network and becomes known to an external Packet Data Network (PDN).

4.3 Session Management

In order for an MS to make use of GPRS services, it must first register with the SGSN of the GPRS network. If authorized, the subscriber's profile is copied from the Home Location Register (HLR) to the SGSN. A packet temporary mobile subscriber identity (P-TMSI) is assigned to the subscriber. If the subscriber does not have an associated P-TMSI, the MS will provide its International Mobile Subscriber Identity (IMSI). This process is referred to as a GPRS attach. A GPRS detach is the process whereby an MS disconnects from the GPRS network. A GPRS detach can be MS or network initiated. For a Class-A mode of operation MS (a Mobile Station using both circuit switched and packet switched data simultaneously) a combined GPRS/IMSI attach and detach procedure may take place.

When an MS is switched on the first function it performs is a GPRS attach. This GPRS attach includes GSM access authentication after which the user profile is downloaded from the HLR to the server SGSN. Thus GPRS authentication is identical to that of GSM [refer to chapter 2.3]. When the GPRS attach is complete, the MS is physically connected to the network; however the MS is not yet able to send or receive IP traffic.

In order to be able to send and receive data, the MS must set-up a packet data bearer. The bearer services of GPRS offers end-to-end packet switched data transfers. Two different kinds of packet data transfer exist:

- Point-to-point Services (PTP)
  The PTP services offer transfer of data packets (PDUs) between two users. It exists in a connectionless mode for IP networks and in a connection-orientated mode for X.25 networks.
- Point-to-multipoint Services (PTM)
  The PTM services offer transfer of data packets (PDUs) from one user to multiple users. Two kinds of PTM services exist, the first where data packets are broadcast in a certain geographical area and the second where data packets are addressed to a particular group of users [Wal].

The MS must apply for one or more addresses used in the PDN. This address is called a Packet Data Protocol (PDP) address. The allocation of a PDP address can be static or dynamic and can be allocated in one of the following ways:

- GGSN Address Pools
  The GGSN may have its own address pool and static or dynamic allocation can take place at GPRS packet data activation.
- Home Location Register (HLR)
  The HLR may keep a static IP address for a subscriber that is retrieved by the SGSN at the GPRS attach.
- Remote Authentication Dial in User Service (RADIUS)
  The GGSN may interact with an Authentication, Authorization, and Accounting (AAA) Server for dynamic IP address allocation at GPRS packet data activation also known as a RADIUS server.
- Dynamic Host Configuration Protocol (DHCP) Server
  The GGSN may interact with DHCP server for dynamic IP address allocation at GPRS packet data activation.

Characteristics of the GPRS session are described in a PDP context. A PDP context describes requirements of the connection to the packet networks. At PDP Context Activation, the SGSN establishes a PDP context, to be used for routing purposes, with the GGSN that the GPRS subscriber will be using [0360]. A PDP context consists of the following:

- PDP Type
- Network Address (IP Address)
- Requested Quality of Service (QoS)
- Access Point Name (APN)

Refer to Table 4-2 for a list of the elements that make up each PDP context. PDP configuration options may be used to request optional PDP parameters from the GGSN [0960]. These requested optional PDP parameters are outside the scope of this chapter.

PDP context	Description
PDP Type	The Packet Data Protocol Type describes what type of PDP is being used for example X.25 or IPv4.
Network Address (IP Address)	This is the PDP Address assigned to the Mobile Station. The MS will use the PDP address to indicate whether it requires the use of a static or dynamic PDP address. If no PDP address is stipulated, i.e. left blank, then it is assumed a dynamic PDP address is requested.
Requested Quality of Service (QoS)	QoS allows specific profiles with parameters: service precedence, reliability, delay and throughput to be established. The GGSN operator configures compatible QoS profiles. A different quality of service (QoS) may be requested for each PDP address. Interactive applications, for example, may require a high level of throughput while application such as email can tolerate lengthy response times.
Access Point Name (APN)	This is the address of a GGSN that serves as an access point to the PDN. The APN is a service indicator submitted by the MS in request for a specific service. In other words, the APN is a logical name referring to the external Packet Data Network (PDN) to which the subscriber wishes to connect. The APN is used by the SGSN to check if a subscriber is authorized for a service by making a comparison to the HLR subscriber info. The APN is also used by the GGSN to provide special services for example: • Access to a specific ISP; APN=Internet • Access to a corporate; APN=company.gprs • Access to a special service; APN=special.service

Table 4-2 Elements of a PDP Context

A subscriber may have multiple simultaneous PDP contexts at any instant in time. The PDP context is stored in the MS, the SGSN and the GGSN and each PDP address is described by an individual PDP context. Figure 4-3 illustrates the PDP context activation procedure where the elements that make up the PDP context are passed between the MS, SGSN and the GGSN.

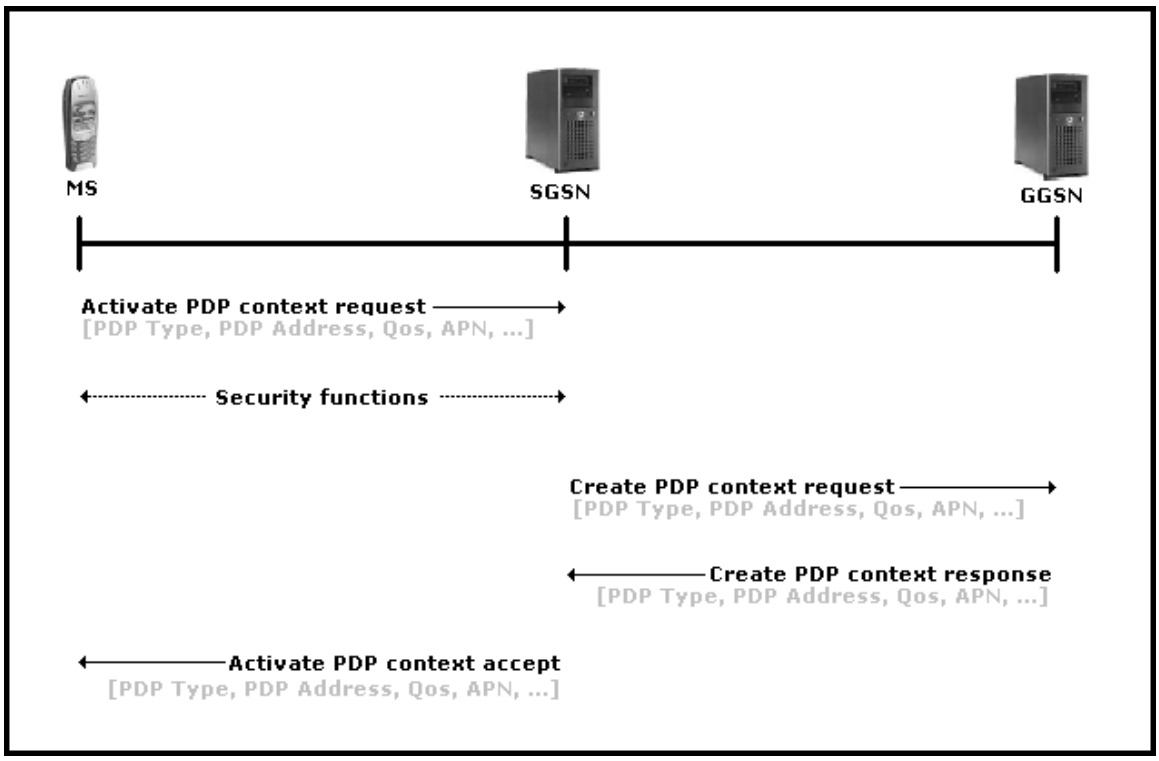

Figure 4-3 PDP context activation procedure

The GGSN creates a new entry in its PDP context table and generates a charging identifier (Id). The new entry allows the GGSN to route PDP Packet Data Units (PDUs) between the SGSN and the external PDP network [0360]. Charging can now take place.

4.4 Mobility Management

The Mobility Management (MM) activities related to a GPRS subscriber can exist in any one of three different states:

- IDLE (GPRS) State
- STANDBY State
- READY State

Each state describes a certain level of functionality and information allocated. The information sets held at the MS and SGSN are denoted as a MM context [0360].

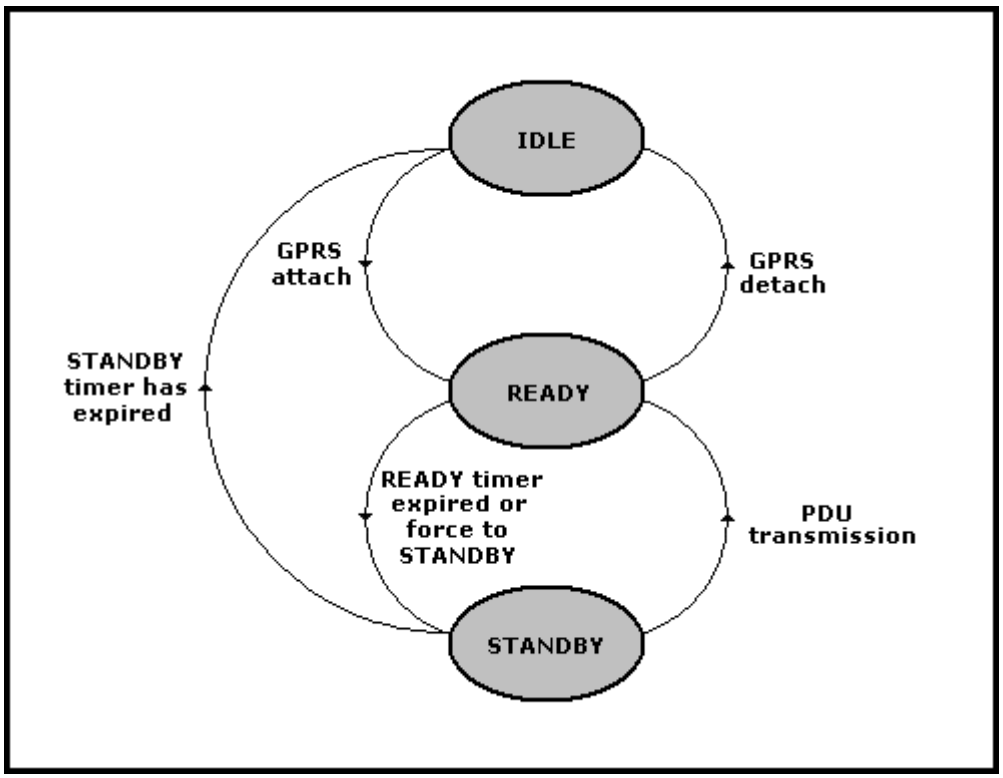

Figure 4-4 State Model of GPRS Mobile Station (MS)

In the next section each different State will be investigated further.

4.4.1 GPRS State Model

4.4.1.1 IDLE (GPRS) State

In GPRS IDLE State, the subscriber is not attached to the GPRS network. Data transmission to and from the MS is not possible in IDLE state. The GPRS MS is seen as unreachable in this case [0360]. In IDLE State, the current location of the MS is unknown to the network as no location updating is performed. In order to move to the READY State the MS must perform a GPRS attach procedure (Figure 4-4). The MS or the network may initiate a GPRS detach procedure causing a shift to the IDLE State. If this occurs then all PDP contexts are deleted.

4.4.1.2 STANDBY State

Data transmissions and receptions are not possible in the STANDBY State. This occurs due to the fact that a PDP context must be activated before data can be transmitted or received. The STANDBY State will be achieved when the Mobile Station (MS) does not transfer any PDUs for a set period of time (network operator specific). This occurs when the READY timer, which is initiated at the GPRS attach procedure, expires. The SGSN may have to send data or signalling information to an MS and vice versa. The status is changed to READY in the MS and SGSN only when data or signalling information is received at that particular component.

4.4.1.3 READY State

The MS can send and receive PDUs in the READY State. The SGSN transfers data to the BSS that is responsible for a subscriber. As previously stated the READY State is supervised by a timer that is activated on a GPRS attach. While in the READY State, the MS performs procedures to provide the network with actual cell selected information. In GSM, a Location Area (LA) is divided into several Routing Areas (RAs) and a RA can consist of one or several BTSs.
GPRS BTS selection is performed locally by the MS or may even be controlled at a network level. When the MS moves into a new Routing Area (RA), the BSS provides the SGSN with the relevant cell identifier information from which it can derive the new Routing Area (RA) location.

The MS may activate or deactivate PDP contexts while in the READY State.

Every PDP context exists in one of two PDP states, namely:

- INACTIVE State
- ACTIVE State

Figure 4-5 illustrates possible causes of these PDP State changes.

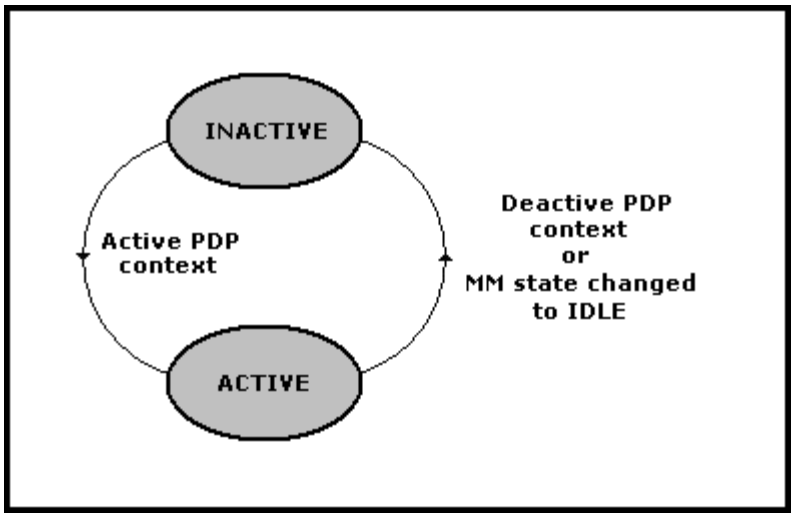

Figure 4-5 PDP Functional State Model

4.4.2 PDP Functional State Model

4.4.2.1 ACTIVE State

While in the ACTIVE state, the PDP context for the PDP address in use for a subscriber is activated in the MS, the SGSN and the GGSN.
The PDP state ACTIVE is permitted only when the mobility management state of the subscriber is STANDBY or READY [0360].
The MS initiates the movement from the INACTIVE to ACTIVE state.

4.4.2.2 INACTIVE State

The INACTIVE state occurs when a certain PDP address of the subscriber is not activated, meaning no data can be transferred. An active PDP context for an MS is moved to an INACTIVE state when the deactivation procedure is initiated or when the MM state changes to IDLE.

Radio resource management principles and channelling within the GPRS architecture is outside the scope of this chapter. For more on these aspects see [Bet].

Overviews of the various components that make up the GSM-GPRS architecture have been provided and Session and Mobility management have been discussed.

4.5 Billing

The volume-based charging approach is usually adopted. In other words, the subscriber is charged per Kilobyte (Kb) or Megabyte (Mb) of data transferred (both uplink and downlink). In South Africa the current billing models provide for a charging at around 50 Rand (R) per Mb or alternatively divided into 20 Kb segments costing around 1 Rand each.

Finally through the use of an example the possible routing of packets in GPRS is demonstrated.

4.6 Routing

Figure 4-6 illustrates how Packet Data Units (PDUs) are routed in GPRS where the Packet Data Network (PDN) is an IP-based network.

In our example, a GPRS MS that is located in PLMN A wishes to send IP data packets to an IP-based host. The SGSN (with which the MS is registered) encapsulates IP packets coming from the MS. The serving SGSN then examines the PDP context, and routes the IP packets through the intra-PLMN GPRS backbone to the appropriate GGSN using the Gn interface. The GGSN decapsulates the IP packets and sends them out over a PDN via the Gi interface to where the host is indirectly connected. Routing mechanisms transfer the packets to the router of the destination LAN. From this router the packets are delivered to the intended host. The corresponding host now wishes to send IP packets back to the Mobile Station (MS). Suppose the MS's home PLMN is actually PLMN B and the MS's IP address assignment was made by the GGSN of PLMN B. Thus packets sent out have to be routed via the Gi interface to the GGSN of PLMN B, this occurs as the MS's IP has the same network prefix as the IP address of the GGSN in PLMN B. The GGSN of PLMN B has to make a Home Location Register (HLR) query in order to obtain the MS location. The result returned states that the MS is in PLMN A. The GGSN of PLMN B then encapsulates the IP packets sent by the host and tunnels them through the inter-PLMN GPRS

backbone to the MS's serving SGSN in PLMN A. The serving SGSN then decapsulates these packets and delivers them to the MS.

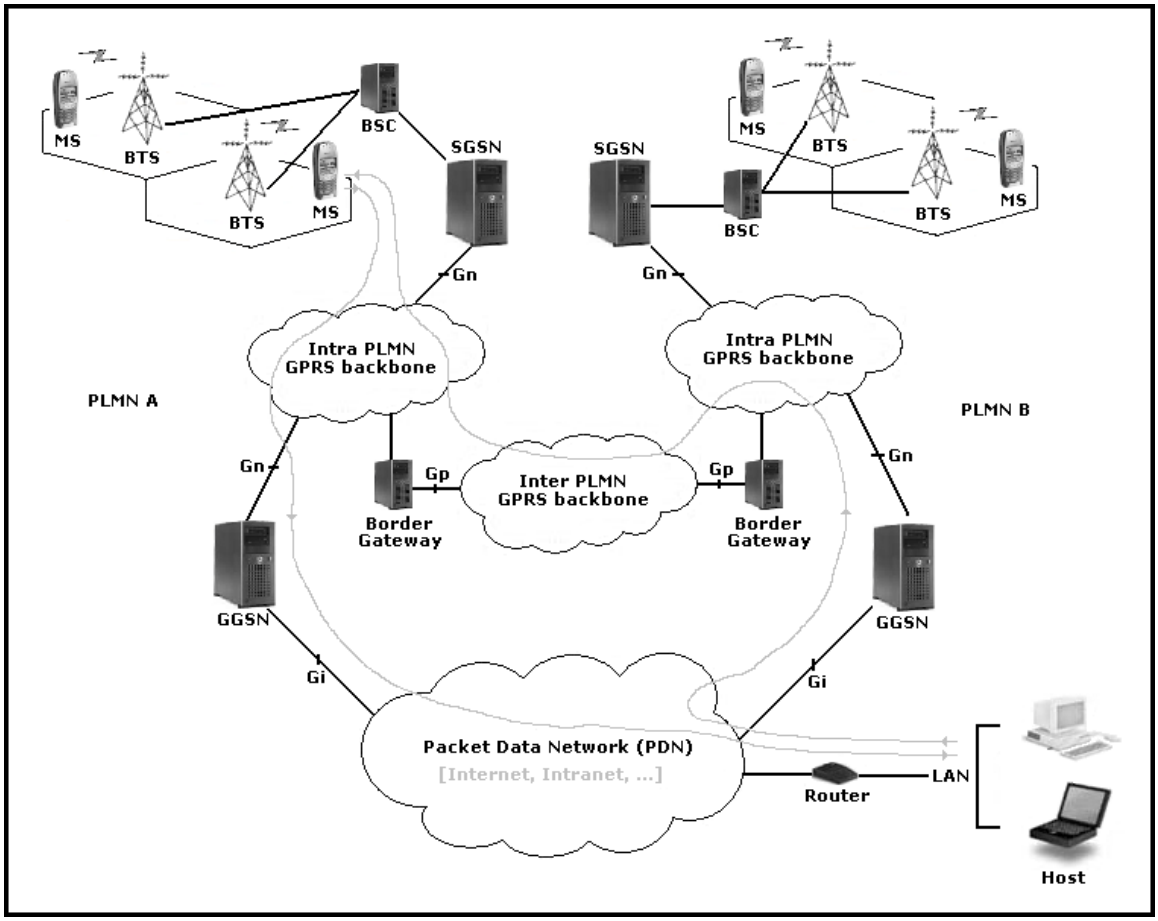

Figure 4-6 IP packet routing example in GPRS architecture

4.7 The Future of GPRS

The Enhanced Data Rate for GSM Evolution (EDGE), which is the successor of GPRS, will increase bit-rate even further and thus boost the opportunities for mobile applications [Wik]. EDGE introduces a new modulation technique and new channel coding that can be used to transmit both packet-switched and circuit-switched voice and data services. EDGE is an addition to GPRS to simply increase data rates on the radio link for GSM and, therefore, cannot work as an independent entity. EDGE is capable of offering data rates of 384 Kbps compared to GPRS which offers data rates of ±150 Kbps (depending on the CS adopted by the serving network) and theoretically up to 160 Kbps on

the physical layer. Edge will be synonymous with true "third-generation" or 3G data services.

4.8 Conclusion

This chapter discussed the most prominent aspects that make up the new packet switched service for GSM, namely GPRS. GPRS which is seen as an "always on" or "always connected" approach allows for data to be transferred Over The Air (OTA). GPRS has huge potential growth for the future as the demand for data services increases. The functionalities of the new additional nodes to the GSM architecture, the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) were highlighted. Session and Mobility Management were covered and a real world working example of data packet switching was illustrated.

Now that the concept of a packet switched addition to GSM has been covered, the theme of wireless data transfer will be continued in Chapter 5 where Wireless Local Area Networks (WLANs) are introduced. Wireless Local Area Networks (WLAN) is as the name implies, a Local Area Network (LAN) without the restrictions and limitations of a wired infrastructure.

Chapter 5

5. WIRELESS LOCAL AREA NETWORK (WLAN)

5.1 Introduction to WLAN

A Wireless Local Area Network (LAN) is a Radio frequency (RF) data communications system. WLANs transmit and receive data Over The Air (OTA) and thus collectively combine data connectivity with ease of mobility. Some existing solutions for Wireless Local Area Networks include the Institute of Electrical and Electronics Engineers (IEEE) 802.11 [Iee] and the European Telecommunications Standards Institute (ETSI)/Broadband Radio Access Network (BRAN) HIPERLAN standard type 1 and 2 [Bra].

So why have WLANs gained popularity in a number of markets? There is a widespread reliance on networking in the business sector to provide shared data and access to shared resources. With a WLAN, users can gain access to shared information without being bound to fixed plug-in point. WLANs can be used to replace wired LANs or simply be used as an extension of a wired infrastructure. Added to the convenience and cost advantages over traditional wired Networks some of the benefits include [Arn]:

- Mobility
- Installation speed, simplicity and flexibility
- Reduced cost
- Scalability

The most distinctive benefit of WLANs is they are easy to understand and use. This can be attributed to the fact that everything to do with wired LANs, with a few exceptions, also applies to a WLAN. They function like, and are commonly connected to, wired Ethernet (IEEE 802.3) Networks.

WLANs have given rise to some new useful applications in different fields, for example:

- Inventory Control
- Medical Care

These and other examples exist due to the fact that instantaneous updates to systems can take place from any location, within a bounded area, in a precise and accurate manner.

The value added by WLANs is immense yet there are many aspects that need to be addressed. Two such aspects are the essential need for security and because it is a Radio Frequency (RF) communications system, the threat of interference with new and existing RF technologies.

This chapter serves as an overview of WLAN technologies. Like GSM, WLAN provides a means to an easily accessible, uninhibited and user orientated communications environment. We investigate how the specifications work, and the corresponding benefits of using a WLAN thus providing the necessary background for the models which later propose the interoperation of wireless technologies. Emphasis is to be placed on the IEEE 802.11 standard and HiperLAN/2; however configuration aspects apply to all major WLAN solutions.

5.2 Overview

WLANs operate under Federal Communications Commission (FCC) Part 15 rules in the United States and under Independent Communication Authority of South Africa (ICASA) in South Africa, which pertain to 2.4 GHz emissions and power limitations. They operate on spread spectrum equipment in the Industrial Scientific Medical (ISM) bands in the 2.4 GHz region (2400 – 2483, 5 MHz), and in some cases in the Unlicensed National Information Infrastructure (U-NII) bands in the 5 GHz region (5725-5850 MHz).

As mentioned before, there are two major existing solutions to WLANs, namely IEEE 802.11 and HIPERLAN.

The IEEE 802.11 working group published the 802.11 standard for wireless LANs in 1999 [Iec]. At present there are task groups ‘a’ through ‘i’, which are working on various methods to standardize improvements on the 802.11 (WLAN) standards.

The Wireless Ethernet Compatibility Alliance (WECA) is the industry organization responsible for certifying 802.11 products that are deemed to meet a base standard of interoperability.

The first family of products to be certified by the WECA is that based on the 802.11b standard. These products are referred to as Wireless Fidelity (Wi-Fi) devices, regardless of the manufacturer.

HiperLAN/2 is a standard being developed by the project BRAN (Broadband Radio Access Network) that is a part of ETSI (European Telecommunications Standards Institute). The HiperLAN standards provide features and capabilities similar to those of the IEEE 802.11 wireless local area network standards.

802.11b and HiperLAN/2 will be addressed individually later on in this chapter.

In order to understand a WLAN's configuration we investigate the topology and discuss the various components that make up a WLAN.

5.3 Wireless LAN Configuration

Each component of a WLAN requires a radio transceiver and must be equipped with an antenna. In a typical WLAN configuration, a device called an Access Point (AP) connects to a wired Network from a fixed location. The AP is responsible for transmitting data and can be considered a bridge between the WLAN and wired LAN infrastructure.

A single AP can support a small group of users, typically between 15 and 50 client devices [Arn], and can cover an indoor range that varies from 20 up to 100 meters and outdoors the range varies from 100 to 400 meters. Greater distances or range can be achieved outdoors by making use of directional antennas and if the direct line of sight is unobstructed.

WLAN clients (stations) can access the WLAN through wireless LAN adapters. These adapters can be incorporated among others into a USB adapter, a PCMCIA or PCI card, or can be integrated into mobile devices. The nature of a wireless connection is transparent to the Network Operation System (NOS). At time of writing, it is important to

note that a station can be associated with only one Access Point at a given time.

WLAN configuration can be simple or complex depending on user requirements. A Basic Service Set (BSS) is formed when two or more stations have recognized each other and established a Network. Clients can be configured to only access the Network via the AP with a specific BSS ID. An example of a BSS ID is 00:04:E2:0E:68:D4. Alternatively, clients can ensure that they connect to the appropriate network, and APs ensure that they only accept connections intended for their network, by using Service Set Identifier (SSID). A SSID is simply a text that names a wireless network. Connection settings may look similar to the following example:

network SSID: airborn
WEP Security: enabled
Encryption key length: 128 bits
Shared key: @!r80rn666666

Wireless networks can be configured in two elementary ways:

- Peer-to-peer or ad hoc mode
- Client-Server or Infrastructure networking

A discussion of these two wireless network configurations follows.

5.3.1 Peer-to-peer Configuration

This configuration occurs when two or more stations equipped with wireless adapters set up an independent network (see Figure 5-1). The stations 'talk' to one another without the use of an Access Point (AP). When two or more stations form a Network, this is referred to as an Independent Base Service Set (IBSS). In this case the client would only have access to the resources of the other client(s) and not a central server.

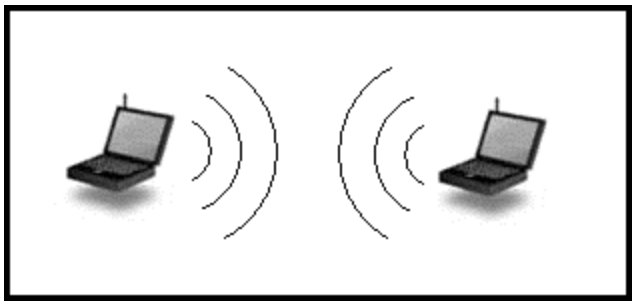

Figure 5-1 Peer-to-peer Wireless LAN Configuration

5.3.2 Client-Server Configuration

Installing an Access Point (AP) can extend the range of the ad hoc Network. This configuration consists of one or multiple stations connected to an AP (see Figure 5-2). Since the AP is connected to a wired Network, each client would have access to server resources. A BSS using a client-server configuration is referred to as being in Infrastructure mode.

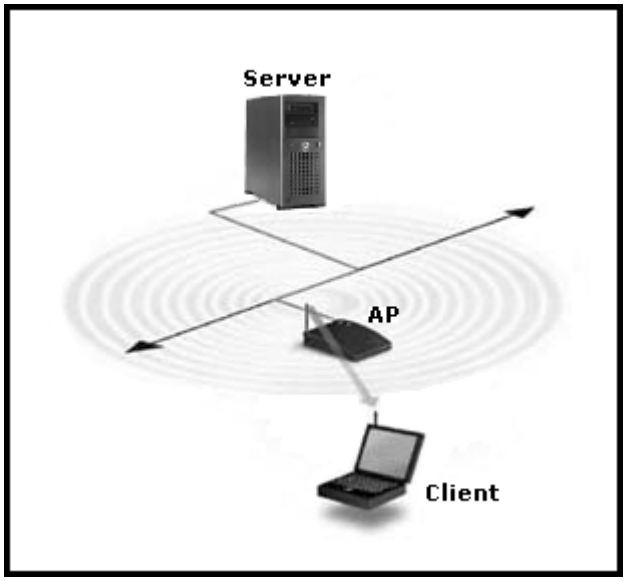

Figure 5-2 Client-Server Wireless LAN Configuration

An Extended Service Set (ESS) occurs when multiple BSSs overlap.
If roaming is supported then all APs and clients should in this case be configured to have the same SSID. Each BSS consists of a group of wireless stations, which execute a Distribution Function (DF) to regulate the exclusive access to the shared wireless medium. These BSSs, each containing an AP, are interconnected together by means of

a Distribution System (DS) (see Figure 5-3). The DS is most commonly a wired Ethernet LAN; however the DS can constitute any fully integrated inter-connecting communications system.

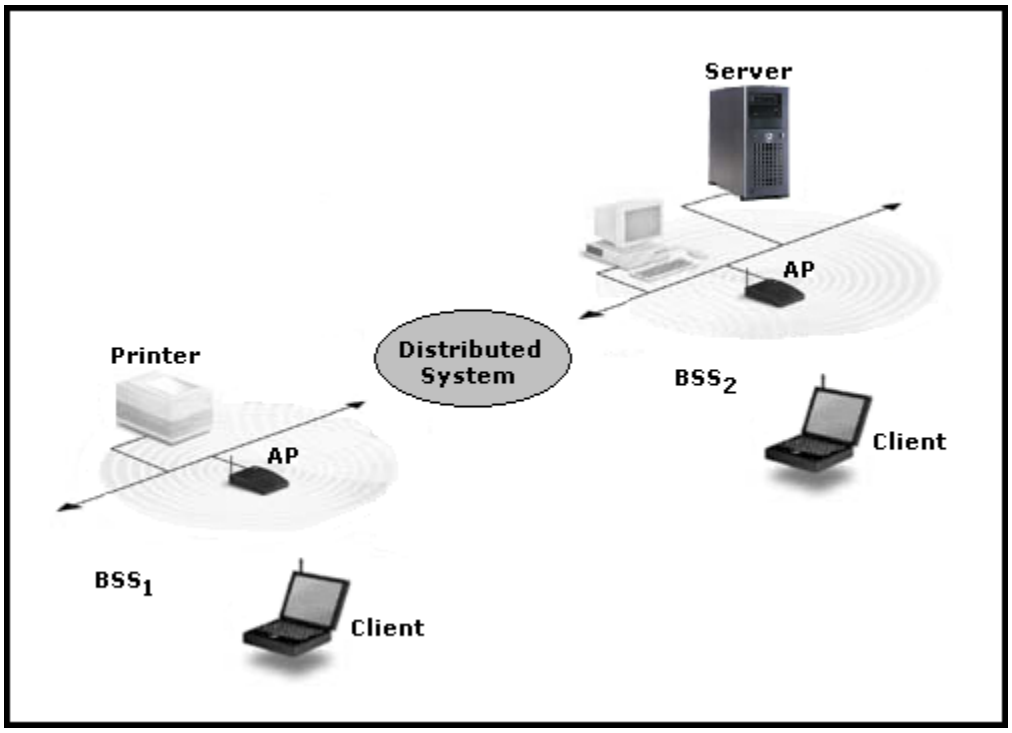

Figure 5-3 Extended Service Set Wireless LAN Configuration

A discussion of the technology infrastructure behind a WLAN now follows.

5.4 WLAN Technology

Radio waves are often referred to as radio carriers. The data being transmitted is superimposed on the radio carrier and can be extracted at a receiving end, this is known as modulation. Once data is modulated onto the radio carrier, the radio signal will occupy more than one single frequency. This occurrence is due to the fact that the frequency or bit rate of the modulating information adds to the carrier. Multiple radio carriers can avoid interferences with each other by merely transmitting on different radio frequencies.

There exists a range of technologies that can be considered when designing a WLAN solution. An overview of these WLAN technologies follows.

5.4.1 Narrowband Technology

A narrowband radio system transmits and receives information on a specific RF. As the carrier is modulated, its power is confined to a relatively narrow frequency band around the carrier's centre frequency. The listener then has to tune his receiver to that particular frequency in order to receive the transmission. This is not a desirable solution, as a licence for each site where the WLAN is deployed, must be obtained from the FCC or ICASA other any other local governing body.

5.4.2 Spread Spectrum Technology

Most WLANs make use of spread-spectrum technology. This wideband/broadband RF technique was developed by the military for use in reliable and secure communications systems. Spread spectrum modulation techniques are defined as those techniques in which:

- Bandwidth of the actual transmitted signal is much greater than the bandwidth of the original message
- Bandwidth of the actual transmitted signal is determined by the message and by an additional signal known as a Spreading Code

More bandwidth is consumed than that of a Narrowband transmission; however the advantage is that in effect the signal is 'louder' and easier to detect. Besides this, by transmitting the message energy over bandwidth that is wider than what is actually required, Spread Spectrum modulation techniques present two major advantages:

- Low power density - Transmitted energy is transmitted over a wide band and therefore, the amount of energy per specific frequency is low
- Redundancy - If a message is presented on different frequencies it may be recovered from one frequency in case of errors

Two types of Spread Spectrum radio exist:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

We now present the two most common WLAN solutions. Firstly, we discuss the IEEE 802.11 standard, followed by a brief overview of the HIPERLAN standard.

5.5 IEEE 802.11

Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels of the ISO Reference Model, the Physical (PHY) layer and the Media Access Control (MAC) layer or data link layer. For a comprehensive overview of the ISO Reference Model, see [SHA].
The MAC acts as an interface to the Logical Link Control Layer (LLC) and the Physical Layer (Figure 5-4).

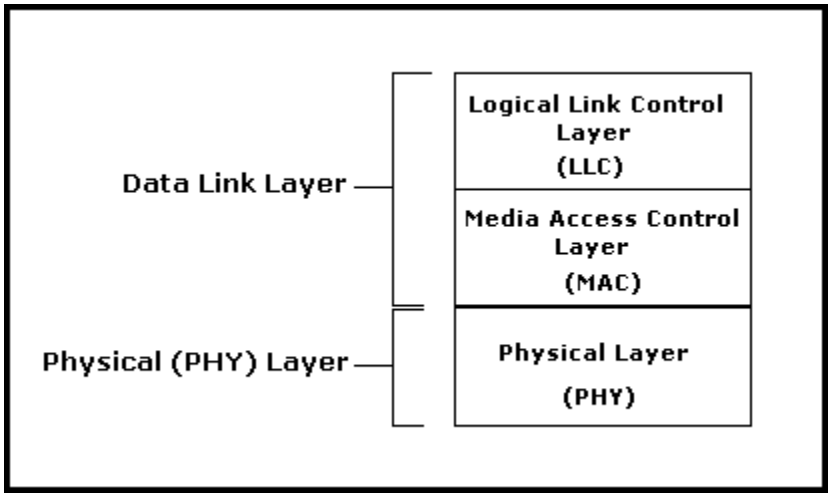

Figure 5-4 Figure Wireless LAN Architectural Layers

5.5.1 802.11 Physical Layer

5.5.1.1 Frequency Hopping Spread Spectrum (FHSS)

FHSS uses a Narrowband carrier that changes frequency for a short period of time in a pattern known to both the transmitter and receiver. The average signal power is thus spread over a wide range of frequencies. In FHSS systems, the Spreading Code is a list of frequencies to be used for the carrier signal, this is known as the hopping sequence. The amount of time spent on each hop is referred to as dwell time. FHSS was originally conceived as a means to hide a transmission from unwanted listeners. However, due to the fact that FHSS is based on a predetermined hopping sequence that is not considered secret, it no longer offers any form of inherent security. Today, FHSS is mainly utilized for another purpose namely the reduction of interference.

5.5.1.2 Direct Sequence Spread Spectrum (DSSS)

DSSS is a technique, which spreads the signal's power across a wider bandwidth by spreading the carrier itself. This is achieved by direct modulation of the carrier with a code sequence. For the duration of every bit within the message, the carrier is modulated following a specific sequence of bits known as chips. In DSSS systems, the Spreading Code is the chip sequence used to represent message bits. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio signal can recover the original data without the need for retransmission [Arn]. To an unintended receiver, DSSS appears as low-powered wideband noise and is generally ignored by most Narrowband receivers.

5.5.1.3 Infrared (IR)

A third technique seldom used in commercial WLANs, is infrared. Infrared systems, also known as IR systems use very high frequencies, based on the 850- to 950- nm frequency. These frequencies are just below the visible light range in the electromagnetic spectrum and are used as data carriers. IR is either directed (line-of-sight) or diffuse technology. Transmission ranges of around 10 meters and the ability of IR to penetrate opaque objects are limitations that make IR an undesirable technology in WLAN usage. IR also tends to perform poorly in the presence of direct sunlight and hence cannot be used outdoors.

5.5.1.4 Orthogonal Frequency Division Multiplexing (OFDM)

OFDM is a multicarrier (also referred to as subcarriers) transmission technique. It is a method of digital modulation in which a signal is split into several narrowband channels at different frequencies, each one being modulated by a low rate data stream. Thus a fast transmission is sent as many slow transmissions, simultaneously, on different frequencies. This technique is not considered to be a Spread Spectrum technique as the subcarriers remain stationary and are not spread.
OFDM uses the spectrum by spacing the channels much closer together. This is achieved by making all the carriers orthogonal to one another, thus preventing interference between the closely spaced carriers. By slowing the speed of the symbol transmission rate, without

affecting the actual data transmission rate, OFDM becomes resistant to intersymbol interference resulting from Multipath propagation.

The OFDM system shows many favourable properties such as high spectral efficiency, robustness to channel fading, immunity to impulse interference, etc [Nee].

We have discussed the various radio frequency techniques that exist on the physical layer. We turn our attention to the layer responsible for maintaining control of the radio frequency band.

5.5.2 802.11 Media Access Control (MAC) Layer

The MAC layer is a set of protocols responsible for maintaining order in the use of a shared medium. MAC supports functions like Fragmentation, Packet Retransmissions and Acknowledges, encryption, power management, synchronization and roaming support where there are multiple APs. The MAC layer remains almost the same throughout all the 802.11x variants. The 802.11 standard uses a Carrier Sense Multiple Access (CSMA) basic access method. While one of the most popular access methods on wired networks is CSMA/CD (Carrier Sense Multiple Access With Collision Detection) used by IEEE 802.3 (Ethernet), this method may not be used for wireless networks. There are several reasons why, they include:

- A full duplex radio capable of transmitting and receiving at once is required for a Collision Detection method
- In a wired network all the stations can hear each other, whereas in a wireless network the station that is transmitting cannot hear any other station in the system which may be transmitting

IEEE 802.11 standard defines a Collision Avoidance (CA) method together with a positive acknowledge scheme to overcome the CSMA/CD problem. This is defined in the standard and is known as a Virtual Carrier Sense mechanism.

Whenever a packet is to be transmitted, the sending device broadcasts a request to send (RTS) frame with information on the length of the signal. If the receiving device permits it at that moment, it broadcasts a clear to send (CTS) frame. After the CTS is transmitted, the sending machine transmits its information. When a packet is received successfully, as determined by a cyclic redundancy check (CRC), the receiving station transmits an acknowledgement (ACK) packet. If

another sending device in the area realizes another machine will be transmitting by the CTS it will allow that signal to go uncontested. RTS/CTS helps in the protection of long data frames against hidden stations.

5.6 802.11 Variants

As mentioned before there are task groups 'a' through 'i' currently working on various methods to improve the 802.11 standard. An overview of these respective task group standards follows.

5.6.1 IEEE 802.11b

Recognizing the critical need to support higher data-transmissions rates, the IEEE in 1999 ratified the 802.11b standard from the original (1997) 802.11 specification. Today 802.11b has become the industry standard for WLANs. The Wireless Ethernet Compatibility Alliance (WECA) certifies equipment as conforming to the 802.11b standard. A Wi-Fi device, short for Wireless Fidelity, is a stamp of approval in an attempt to guarantee interoperability between different 802.11b devices. The 802.11b specification affects only the physical layer, adding higher data rates and more robust connectivity. It makes use of the DSSS and provides for data rates up to 11 Mbps at 2.4 GHz unlicensed (ISM) frequency band. The standard is backwards compatible to earlier specifications, allowing speeds of 1, 2, 5.5 and 11 Mbps on the same transmitters. Its primary use is for TCP/IP and is an extension of the wired Ethernet. There are 14 channels, which are staggered at a few megahertz (MHz) intervals, 3 of which are non-overlapping. Channels 1, 6 and 11 have no overlap among them due to the fact that different channels are legal in different countries.

Roaming is supported in 802.11b, this means that the wireless client may shift from one Access Point to another, while still remaining connected to the network. In a roaming environment, all APs have the same SSID within the existing Extended Service Set (ESS).

For more on 802.11b, see [11b].

5.6.2 IEEE 802.11a

The 802.11a standard, which supplements 802.11, was published in 1999. 802.11a is a Physical Layer standard that utilizes 300MHz of bandwidth in the 5 GHz Unlicensed National Information Infrastructure (U-NII) band. It uses Orthogonal Frequency Division Multiplexing (OFDM) to provide data rates up to 54 Mbps. More available spectrum in the U-NII allows a total of 8 non-overlapping 20MHz channels. This channel spacing enables the deployment of 802.11a Access Points to be placed less densely than in its 802.11b counterpart.

Due to the fact that 802.11b uses the 2.4 GHz range and that 802.11a uses the 5 GHz range results in the incompatibility of the two technologies. One significant benefit is that no interference will occur between 802.11a and 802.11b as signals operate at different frequency bands. Technology is being developed to allow the seamless handoff communication between overlapping or integrated 802.11a and 802.11b networks. Conformance of this interoperability is shown by a Wi-Fi5 mark from WECA.

Additional specifications to the 802.11a standard have been proposed to allow both 802.11a and HiperLAN/2 to coexist. Dynamic channel selection (DCS) and transmit power control (TPC) allow clients to detect the most available channel and use the minimum output power necessary if interference occurs.

For a brief summary of the 802.11 standards, refer to Table 5-1.

There are various upcoming standards, which are focused on improving various aspects of the IEEE WLAN standards. Improvements that are taking place at the MAC layer of the 802.11 standard. They include:

- 802.11e – Quality of Service
- 802.11f – Inter Access Point Protocol
- 802.11i – Enhanced Security aspects

The only standard which includes improvements at the PHY layer is:

- 802.11g – Extension to 802.11b

5.6.3 IEEE 802.11e

802.11e supplements the MAC layer to provide Quality of Service (QoS) support. It will apply to 802.11 Physical standards of a, b and g. The purpose of 802.11e is to provide service with managed levels of QoS for data [Gar], voice and streaming video application.

5.6.4 IEEE 802.11f

802.11f standard defines the registration of AP within a network and the interchange of information between APs when a user is handed over from one AP to another. This will allow reduced vendor lock-in and allow multi-vendor infrastructures.

5.6.5 IEEE 802.11i

802.11i supplements the MAC layer to improve security. It will apply to 802.11 Physical standards of a, b and g. It provides an alternative security mechanism to that found in 802.11b, with new encryption methods and authentication procedures.

5.6.6 IEEE 802.11g

802.11g uses the same OFDM scheme as 802.11a and should deliver speeds on a par with that of the 802.11a standard. However, 802.11g will operate in the 2.4 GHz frequency band and hence will remain backward compatible with existing 802.11b WLAN infrastructures. At present the 802.11g standard exists only in draft form and is awaiting approval from the FCC and IEEE ratification. Like 802.11b, 802.11g will be limited to three nonoverlapping channels.

5.7 Security

Security is always a concern when data is being communicated and WLANs are no exception. Some inherent security risks to WLANs include:

- Insertion Attacks - Unauthorized devices on the WLAN
- Interception and monitoring of wireless traffic
- Misconfiguration - Security levels not set by default
- Jamming – Illegitimate traffic overwhelms frequencies

For more on known vulnerabilities in WLAN security, see [Yas].

There are three basic methods to secure access to an Access Point that are built into 802.11 networks:

- Service Set Identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

5.7.1 Server Set Identifier (SSID)

Each AP in the WLAN has associated with it a SSID. This is an identifier to access a particular network and clients must be configured with the correct SSID in order to gain access at the AP or group of APs. However, this minimal security is compromised if the AP is configured to broadcast its SSID. Using the SSID for access control purposes has two major downfalls:

- Too many users have to know the SSID to make it secure
- The SSID is broadcast in cleartext, thus making it easy for an intruder to obtain

5.7.2 Media Access Control (MAC) Address Filtering

A client can be uniquely identified by the MAC address associated with the 802.11 network card. To increase the security, each AP can be programmed with a list of MAC addresses allowing only those clients to access the AP. If a client's MAC address does not occur in this list at an AP, the client will not be allowed to associate with that AP.

5.7.3 Wire Equivalent Privacy (WEP)

Security in the IEEE 802.11, and in particular the 802.11b standard, comes in the form of a stream cipher to protect data communication exchange. It is known as Wired Equivalent Privacy (WEP) algorithm. This algorithm uses the RC4 PRNG (Pseudo-Random Number

Generator) encryption algorithm from RSA Data Security and comes in the form of a:

- No encryption mode
- 40-bit encryption
- 128-bit encryption

Only clients that know the "secret key" can associate with an access point or peer-to-peer group. To ensure that a packet has not been modified in transit, WEP makes use of an Integrity Check (IC) field in the packet. An Initialization Vector (IV), also included in the packet, is used to avoid encrypting two ciphertexts with the same key stream. The IV is used to augment the shared key and produces a different RC4 key for each packet. However, according to [Gol] this can be seen as a poor security implementation as common attacks on WEP are feasible.

It is important to note that WEP was never intended to be a complete end-to-end security solution. It merely protects the wireless link between the mobile client and the APs. Encryption only occurs at the link layer and not at an application layer and as a result only the communication channel is protected. In order for a complete secure end-to-end solution SSH tunnelling can be used [Fli].

5.8 HIPERLAN/2

HiperLAN/2 is a wireless worldwide specification developed by the project BRAN (Broadband Radio Access Network) that is part of European Telecommunications Standards Institute (ETSI). It is similar to the 802.11a standard at the Physical Layer. It makes use of OFDM and operates in the (U-NII) 5 GHz frequency band. The MAC layers of 802.11a and HiperLAN/2 differ somewhat, while 802.11a uses CSMA-CA, HiperLAN/2 utilizes Time Division Multiple Access (TDMA). Because the 5 GHz U-NII equivalent bands have been reserved for HiperLAN/2 systems in Europe, 802.11a is not yet certifiable in Europe by ETSI.

The MAC layer is optimized for radio communication and realizes new features such as Quality of Service (QoS), high-speed transmission, automatic frequency allocation, mobility support and security support. The HiperLAN/2 network has support for both authentication and encryption. The default encryption scheme is based on DES with a 56 bits key. Optionally, HiperLAN/2 can support either encryption or

support no encryption options. The Diffie-Hellmann key exchange is used for the encryption key creation.

For more information on HIPERLAN/2, see [Bra] [Tr1].

For a summary of the HiperLAN/2 standard, see Table 5-1.

Standard	Operating Frequency	Maximum Data Rate
IEEE 802.11	FHSS and DSSS in 2.4 GHz band	1 or 2 Mbps
IEEE 802.11b	DSSS in 2.4 GHz band	5.5 or 11 Mbps
IEEE 802.11a	OFDM in 5 GHz band	Up to 54 Mbps
HiperLAN/1	OFDM in 5 GHz band	20 Mbps
HiperLAN/2	OFDM in 5 GHz band	Up to 54 Mbps

Table 5-1 Summary of WLAN solutions

802.11b has become the only standard developed for Public WLANs. Public WLANs are found at commercial public areas such as airports, hotels and conference centres.

5.9 Public Wireless LANs

A new business world has noticed potential in the WLAN industry, and many providers of public WLAN (usually 802.11b) services have emerged so far. These providers are referred to as Wireless Internet Service Providers (WISPs). Such third parties also provide billing solutions, as well as authentication and cryptography. Venues such as airports, hotels and cafés are prime locations for deployment of public WLAN and are often referred to as "hot spots". Perhaps a good example of the benefit of WLANs would be students able to access academic information from anywhere on campus. A problem remaining to be solved is the different billing structures. Some WISPs have a fixed rate charge, others have adopted a volume-based charge, and yet others have a "per logon" charge or no charge at all. This complicates the clearing between them [Tho]. Another problem is that most public WLAN access points are not WEP enabled. If the AP does not enable WEP, the wireless clients cannot make use of WEP encryption. If WEP is not enabled any communication that takes place wirelessly either from peer-to-peer or from peer-to-server will be sent in the clear.

Public WLANs are gaining in popularity, forcing a real need for alternative security measures and standardized billing structures.

5.10 Future of Interoperable Standards for Broadband Wireless Access

IEEE 802.16 has been developed as a point-to-multipoint (PMP) broadband wireless metropolitan area network (WirelessMAN) access standard, more commonly known as WiMAX. The standard also covers both the Media Access Control (MAC) and the physical (PHY) layers. The initial version was developed to operate between 10-66 GHz but task groups "a" and "b" have produced an amendment to extend the specification to include both licensed and unlicensed bands in the 2-11 GHz range. The 802.16a standard, approved in January 2003, provides for up to 50Km range without needing direct line of sight with the base station. At high frequencies, faster data rates can be achieved; however line of sight to the base station is required. Alternatively, low frequencies result in lower data rates without line of sight being required.

The IEEE 802.16 Air Interface Specification is flexible as it was designed to the needs of an assortment of situations. Allowance has been made for different physical (PHY) layers for different frequency bands. The technology integrates well with IEEE 802.11 and will therefore be a candidate for linking WLAN "hotspots". For more on 802.16, see [216].

5.11 Related Broadband Wireless Technologies

Bluetooth is a short-range radio technology that enables wireless connectivity between mobile devices. The three main design goals for Bluetooth were:

- Small size
- Minimal power consumption
- Low price

The technology was designed to be uncomplicated, and the target was to have it become a de facto standard in wireless connectivity.
Bluetooth resolves the problems that both Infrared and cabling synchronizing systems presented. Bluetooth is inexpensive and does not rely on user input for communication between devices to occur.

Bluetooth uses spread-spectrum frequency hopping. In the case of Bluetooth, transmitters change frequencies 1600 times every second, meaning more devices can make full use of the limited radio spectrum. With a fast hop rate, good interference protection is achieved.

Bluetooth communicates on a frequency of 2.45 GHz, which by international agreement is for the use of industrial, scientific and medical devices (ISM). Bluetooth avoids interference by sending out very weak signals, this low power however limits the range of the Bluetooth device to around 10 meters. [Van] illustrates by simulation the radio frequency interference occurrence in an environment where both Bluetooth and IEEE 802.11 exist. Bluetooth, unlike Infrared (IR), does not require direct line of sight and even at low power has the ability to traverse through most objects making this standard useful in communicating with several devices for example in different rooms of a house.

Electronic connections are established automatically and a network is formed. The connection to a desired device is made by a page message. If the address of the recipient is unknown, an inquiry message is needed before paging. Before any connections are made, all units are in standby mode. A unit in a standby mode wakes up every 1.28 seconds to listen to page/inquiry messages. Each time a unit wakes, it listens on one of the 32 defined hop frequencies. In connection state, the Bluetooth unit can be in several modes of operation:

- Sniff mode
- Hold mode
- Park mode

These modes are used to save power or to free the capacity of a Bluetooth network.

Bluetooth systems create what is known as a personal area network (PAN) or piconet. Once a piconet is established, members randomly hop frequencies in unison so as to remain in contact with one another and avoid interference with other members and or piconets. A piconet has a master and up to seven slaves. The master transmits in even timeslots, slaves in odd time slots. When there are many slaves the data rate is limited. One device can also be connected in two or more piconets. This is referred to as a scatternet. A device can, however, only be a master to one piconet at a time.

For more on Bluetooth, see [Blu]. For security-related aspects of Bluetooth refer to [Sig].

5.12 Conclusion

A brief overview of the WLAN technologies and standards has been presented in this chapter. Different WLAN configurations were discussed, peer-to-peer and client-server communication. Various Radio Frequency (RF) spectrum techniques were covered. IEEE 802.16 (WiMAX), Infrared (IR) and Bluetooth were incorporated as these technologies are future and related standards for broadband wireless communications.

It is important to note that high data rates, Quality of Service (QoS) and compatibility with latency or legacy standards are essential, however the most pressing and immediate need for WLANs lies in the security aspect. The commercial viability of WLAN truly depends on the satisfaction of the user's requirements that communication channels are indeed secure.

In the next chapter we provide a comparison of the GSM and WLAN technologies to later formulate a new approach to an "always connected" or "always on" integrated packet switching model.

Chapter 6

6. COMPARISON BETWEEN GSM AND WLAN

6.1 Introduction to GSM and WLAN Comparison

Wireless mobile communication and the Internet are two communication techniques that have emerged and grown substantially over the last two decades. These technologies nowadays influence our daily lives in a significant way in terms of mobility, communication and easy access to information. Mobile telephony has offered mobile communication between people, while the Internet has provided for flexible communication and access to the information.

We have witnessed the emergence of new communication platforms which today have become common industry standards.

In this chapter, we examine the similarities and differences of two such communications platforms: Global System for Mobile Communication (GSM) and Wireless Local Area Network (WLAN). The benefits and disadvantages of each technology platform are then explored in detail.

To be able to complete a comprehensive analysis of both the communication platforms we need to consider the infrastructures of these architectures, how these infrastructures differ and compare and lastly whom these technologies are intended to serve.

This chapter, in conjunction with [chapter 3] and [chapter 4], serves as motivation to a later detailed proposal of how the integration of the two technologies into one workable infrastructure is achievable.

6.2 Overview

GSM and WLAN technologies are similar technologies that partly compliment one another. Both support mobility and both are built on broadband radio communication technologies. However, there are a quite a few notable differences; they have different technological origins, different development infrastructures, implementation strategies and finally they are distributed differently. In order to be able to define these technologies as infrastructures, firstly we encapsulate what constitutes an infrastructure.

6.3 What is an Infrastructure?

An Infrastructure is a multi-layered collection of various resources for communication and interchange of data. Hardware, software and services along with the necessary support organization and personnel are required to develop and maintain an infrastructure. An infrastructure is considered to be an "invisible" structure that only really becomes apparent when a breakdown occurs.

An infrastructure can be confined in an organizational structure or could be a very large general public infrastructure. While a general infrastructure is aimed at supporting a very large or unlimited community of users and all types of applications, a corporate infrastructure will have a restricted set of users and type of applications, and aims at interconnecting and integrating the different information and communication systems within an organization. GSM can be seen as a very large general public infrastructure while WLAN presently is confined usually within an organizational structure but evidently is moving towards a general public infrastructure with the introduction of Public WLANs [chapter 5-9].

An infrastructure is intended to support certain communities of users. Infrastructures may conform to generally accepted practices or procedures or may even break away from existing conventions. A good example of this would be how communication changed by the introduction of mobile communication devices. The GSM infrastructure for example is the direct consequence of a new idealistic approach.

Infrastructures are fundamentally and always a relation [Sta] and the relationship that exists between various elements mutually shape and

redefine the infrastructure. From this it is evident that an infrastructure can not be designed and implemented as a linear process, from specification to implementation. Rather, it will evolve through a multifaceted relationship between various users and groups, the designers and implementers of standards, the product developers and the service providers combined with the context in which it is found.

It is important to emphasize the role of users, individuals as well as user organizations, as an infrastructure value to a large extent is defined by its users and user groups. An infrastructure is always related to its intended users and other relevant actors, and must be understood in their context [Sta]. Currently different user groups exist for the GSM and WLAN infrastructures. If these infrastructures were to coexist as one conjoined infrastructure then users will define functional requirements and interoperability needs and hence a new user group will be established.

An approach is needed in order to be able to define or categorize an infrastructure into a particular nature. Previous work by [Mcg] claims that the following features are essential: sharable, common, enabling, physical embodiment, enduring, scale, and economic sustainability. [Sta] holds the following aspects as crucial: Embeddedness, transparency, reach of scope, learned as part of membership, links with conventions of practice, embodiment of standards and built on installed base.

Key characteristics that define an infrastructure and hold true for GSM and WLAN include the following: enabled, shared, open, heterogeneous, viable, enduring and subscriber orientated. As GSM and WLAN possess common key characteristics it affords a relatively suitable platform for direct comparison.

GSM and WLAN characteristics are closely linked to its user community as both conform to heterogeneous applications and usage patterns while a need is maintained for viable economic sustainability.

A brief recap of both the GSM [chapter 2] and WLAN [chapter 5] technologies follows.

6.4 Global System for Mobile Communication (GSM)

GSM is the European standard for "second-generation" (2G) mobile telephone system. GSM is a Circuit-switched network, implying that connections are dependent on availability of free circuit (time slots). It was standardized by ETSI in 1990. It is primarily used for voice data but does allow for both synchronous and asynchronous data to be transported as a bearer service. GSM is currently the most widely used mobile telephone system in the world.

6.5 Wireless LAN (WLAN)

WLAN is a flexible data communication system implemented as an extension of, or as an alternative to, a wired LAN implementation. Two types of configurations arrangements namely, a peer-to-peer connection or a client-server connection. WLAN is designed to be deployed in corporate organizations and in public "hot spots". IEEE 802.11x and HIPERLAN/x are the WLAN standards which relate to other LAN standards, for example IEEE Ethernet 802.3. The standard fits into the two lower levels of the OSI model (the physical and the link layer). The standard most frequently used is the IEEE 802.11b or more commonly referred to as Wi-Fi.

We have provided a definition for an infrastructure. We now focus our attention on the main characteristics of the two infrastructures at hand.

6.6 Main Characteristics of GSM and WLAN

In order to make a comparison between GSM and WLAN we first identify the main characteristics that make up the two technologies. Table 6-1 provides a summary of the main characteristics.

Characteristic	GSM	WLAN
General	Universal standards for wireless telephony and data transfer, including global roaming, handover functionality, security and billing models in standard.	Universal standards for wireless access to fixed LAN. Supports all types of communication, but lacks comprehensive security model and billing infrastructure in standard.

Standards body	European Telecommunications Standards Institute (ETSI) now in Phase II GSM.	Institute of Electrical and Electronics Engineers (IEEE) 802.11x and the European Telecommunications Standards Institute (ETSI)/Broadband Radio Access Network (BRAN) HIPERLAN standard.
Security	Comprehensive Over The Air (OTA) security model. Risk of having SIM cloned or Mobile Station (MS) stolen a possibility.	Low security in current standard. Wired Equivalent Privacy (WEP) keys optional. Two other possible security implementations; Service Set Identifier (SSID), Media Access Control (MAC) address filtering. Focus from IEEE to enhance standard solely for security reasons. Third parties may deliver additional security option.
Billing	Comprehensive billing model, but also incorporates other billing models for GPRS data transfer. In addition there are revenue sharing models with third parties as content service providers.	No billing functionality in standard. Different suggestions for billing models: Fixed, volume, per logon or none. Third party WISPs may provide functionality for billing.
Roaming	Optimized for roaming. Mobility management responsible for handover roaming of Mobile Station (MS). Requires contractual agreement between the network operators, and schemas for exchange of accounting data, billing procedures.	Not implemented in the standard. Users must manually connect to different WLAN. Third parties may support roaming and seamless access to WLAN services from different providers (WISPs).
Networking equipment	Base Transceiver Station (BTS) or pico cell acts as access point to underlying network.	Access Point (AP) acts as entry point to underlying network.
Range of Network equipment	BTS has a range of ±32Km in rural areas, this range diminishes in urban areas due to Multipath propagation.	Access Point has indoor range which varies between 20 and 100 m and an outdoor range that varies from 100m to 400m.
Frequency Spectrum	900 MHz or 1800 MHz or 1900 MHz frequency band.	2.4 GHz or 5 GHz frequency band.
Regulation of Frequency Spectrum	Regulated frequency spectrum, licences provided through governmental bodies.	Unregulated, unlicensed frequency spectrum.

Device Type	A mobile device enabled for utilizing the services provided by GSM. Some devices able to access all three frequency spectrums (tri band).	Laptop computer, desktop computer, PDA that has an enabled WLAN adapter (PCMCIA or PCI card).
Equipment manufacturers	Providers of mobile stations (MS). Providers of underlying network hardware and software.	Providers of Wi-Fi hardware and software. Providers of access points, mobile device cards.
Mobility	High mobility, with global coverage.	Low mobility, with limited local coverage.
Frequency Modulation	Limited bandwidth among many users; therefore combination of digital Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) used.	Direct Sequence Spread Spectrum (DSSS) used. Signal's power across a wider bandwidth. Direct modulation of carrier.
Bandwidth used	Low bandwidth usage, 9.6 kb for voice calls.	High bandwidth usage, 1 to 54 Mb depending on standard.
End-users	Roaming professional and personal users. Consumers of logistical, entertainment services.	Semi-Mobile LAN market, incorporating travelling professionals, office users.
Usage	Primarily for voice calls, data calls becoming increasingly popular.	Access from public "hotspots" or to corporate networks. Data required. Configuration of ad-hoc networks.
Examples of Implementations	GSM networks spread throughout the world; particularly concentrated in Europe; emerging market in Africa.	WLAN implemented in hospitals, hotels, academic institutes, corporates and other public "hot spots".
Drivers of technology development and dispersal	Telecommunication operators, Mobile Station (MS) and network equipment manufactures, service content providers.	Business sector/Industry, certified bodies, increased need for user mobility.

Table 6-1 Comparison of main characteristics of GSM and WLAN

Taking Table 6-1 as reference we now delve into the similarities, differences and benefits of the characteristics of the GSM and WLAN infrastructures.

6.7 Similarities between GSM and WLAN

One of the major similarities is that both GSM and WLAN make use of radio wave technologies. Mobility and mobility management are primary objectives of both technologies; this has been achieved in GSM and to a lesser degree in WLAN. Session management is a key characteristic of both standards; state must be maintained for communication channels to remain open. Flexibility in both allows ad hoc networks to be added anywhere with relative ease. Networking equipment is similar by design, where Access Points (APs) and Base Station Transceivers (BTSs) are fundamentally functionally alike. APs and BTSs are the first point of connection to the underlying network and communicate with the end-user Over The Air (OTA). End–user equipment has been standardized, Wi-Fi devices in the case of WLAN and 900/1800/1900 MHz compliant devices in the case of GSM. GSM is primarily used for voice calls however there is a greater demand for data, this is illustrated by the advent of new packet-switched networks like GPRS, EDGE and UMTS. In the near future, later versions of GSM and WLAN will be concerned with higher data transfer as principal function.

6.8 Differences between GSM and WLAN

Security and billing are among the most obvious differences between GSM and WLAN. While GSM has a comprehensive security model [chapter 2.3 and 2.4], WLAN has yet to include a fully integrated security model, Wired Equivalent Privacy (WEP) [chapter 5.7.3] is optional implementation at this stage. Future releases of the 802.11 standard will incorporate a fully integrated security system. 802.11i is in development to include an enhanced Security model [chapter 5.6.5]. Billing functionality is provided for in GSM, WLAN on the other hand has no billing functionality built in its standard. Third parties known as Wireless Internet Service Providers (WISPs) may provide a billing structure in WLAN and there remains a variety of different approaches to billing models: Fixed, volume, per logon or none.

Roaming management are prerequisites in any wireless environment; WLAN handover is currently restricted to users serving a particular WLAN as currently handover between different independent WLANs is not possible.

GSM supports full roaming capabilities as long as contractual agreements exist between network operators. Most GSM operators have "Roaming agreements" in place and roaming makes up an integral part of the GSM infrastructure.

Although GSM and WLAN operate in the radio wave spectrum, they operate at different frequencies in the RF spectrum. GSM operates in the 900/1800/1900 MHz frequency band while WLAN operates in the 2.4/5GHz band. 900/1900/1900 MHz frequency band is a licensed and regulated frequency spectrum, the 2.4/5 GHz frequency band is unregulated and not licensed by any governmental or standards body.

Due to the spectrum difference the range of the network operations is dissimilar, network nodes in GSM have a far greater coverage span, ±32Km compared to a couple of hundred meters in WLAN access nodes. Unlike Frequency modulation techniques are used; limited bandwidth is available to many GSM users and therefore a combination of digital Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) is used. WLAN concerns itself with direct modulation of the carrier and Direct Sequence Spread Spectrum (DSSS) across a wider bandwidth is used.

The last remaining noticeable and probably influential difference exists due to the fact that different standards bodies are involved in the development, implementation strategies and dispersal of GSM and WLAN. GSM is standardized by the European Telecommunications Standards Institute (ETSI), now in Phase II while WLAN is standardized by Institute of Electrical and Electronics Engineers (IEEE) 802.11x and the European Telecommunications Standards Institute (ETSI)/Broadband Radio Access Network (BRAN) HIPERLAN. Drivers of technologies are not normally concerned with compatibility issues with other sometimes competitive technologies.

6.9 Benefits of GSM and WLAN

GSM is an established technology that provides a comprehensive security model and billing structure coupled with a viable working roaming solution. True unique identification makes for a secure connection and communication. Inter network operator and local service provider billing supports a reliable billing system. Seamless roaming from network to network provides true mobility end-user fulfilment.

WLAN is an extension to a wired Ethernet network without the limitations of fixed wires and operates at high data rates.

6.10 Conclusion

It would be a near impossibility to fully integrate GSM and WLAN into one complete compatible infrastructure, however because of inherent similarities the benefits of both technologies could be combined in order to provide an end user with comprehensive secure anywhere mobile wireless data solution.

Securing information is essential; a mobile environment is no different. In the next chapter we investigate the adaptation of a secure XML structure for the use in Over The Air provisioning. This XML Encryption Syntax provisions for the flexibility of adjusting security levels on information based on security needs.

Chapter 7

7. SECURING CONTENT OVER THE AIR IN A MOBILE ENVIRONMENT

7.1 Introduction Securing Over The Air Content

In any mobile architecture, security can be divided into three sections namely:

- Security at an application level
- Security in the transfer of information over the radio waves (Over The Air)
- Security on the mobile device itself

In the mobile device application context as with any other application environment we want to produce content that is quick, accurate and transferred in a secure manner. Within the Wireless Application Environment (WAE) it is necessary to produce content quickly, accurately and above all secure. Security is a necessity when vital information is being communicated between parties.

When security is enforced by encryption overhead is added to content. Any mobile device receiving information can ill afford overhead. The problem at present is that content pushed to a mobile device either occurs on a secure or non-secure channel. Secure Socket Layer (SSL) is predominately used to secure content travelling from an origin server to the Mobile Station (MS) and vice versa.

To decrease the overhead implied by this security feature it is evident to secure only the content that requires securing. Currently, in the Wireless Application Environment (WAE) the entire content is encrypted even if only portions of information contained is of a critical nature. To optimize this we must simply encrypt only the critical information thus reducing the total overhead on content.

In this chapter a model is presented for the transfer of information in a secure manner Over The Air while reducing overhead on content. A

brief overview of XML and CSS2 is provided after which we adapt the use of a Cascading Style Sheet (CSS2) to not only include presentation information to applied content but also include security options. This adaptation introduces the concept of a Security Style Sheet (SS) that provides an adaptable approach to securing critical information. The flexibility of the SS will also allow for different levels of security whether it is symmetric key encryption or a message digest algorithm.

7.2 Overview

7.2.1 Extensible Markup Language (XML)

XML stands for Extensible Markup Language [Xml], and is defined by the World Wide Web Consortium (W3C). XML is a subset of the Standard Generalized Markup Language (SGML) [Sgm] and offers a human-readable, self-explaining, well-structured and consistent way to describe and transfer data. XML has become the adopted standard for the transfer of data in a raw extensible format. XML documents generally consist of the following:

- Elements
- Tags
- Attributes
- Entities
- PCDATA
- CDATA

Elements are the main building blocks of an XML document. Elements can contain text, other elements or can simply be empty. Tags are used to mark-up elements for example begin tag <element> and end tag </element>, while attributes provide extra information about elements. Entities are variables used to define common text for example entity reference '&' represents character '&'. PCDATA means parsed character data, in other words the text found between the start and end tags of an XML element that will be parsed by a parser. CDATA is character data that will not be parsed by a parser.

XML namespaces [Nsp] provide a simple method for qualifying element and attribute names used in Extensible Markup Language documents by associating them with namespaces identified by Uniform Resource Indicator (URI) reference. For more on URI, refer to [Uri].

Now that we have an XML structure, how do we define it? This is achieved by making use of a Document Type Definition (DTD) and its purpose is to define the building blocks of an XML document. It defines the document structure with a list of permissible elements. The DTD can be retrieved from an external source or embedded within an XML document. A DTD is generally used for the following reasons:

- Each XML document carries a description
- A common DTD can be used for interchanging data
- Verification that data received is valid

XML Schema is an XML based alternative to, and successor of, DTD. Like a DTD, a Schema describes the structure of an XML document. The XML schema language is referred to as XML Schema Definition (XSD). There are a number of reasons why Schemas are replacing DTDs, they include:

- XML Schemas are written in XML and are therefore themselves extensible
- XML Schemas support data types (string, integer etc.)

The main purpose of XML is to specify information independently of how:

- The information is processed; and
- How this information is displayed.

Often information or parts of information must be rendered, producing a visual or auditory form. An investigation into how XML may be rendered in a visual form follows.

7.2.2 Cascading Style Sheet 2 (CSS2)

Two standards have been specified by the W3C for the rendering of XML information:

- Cascading Style Sheets (CSS)
- eXtensible Stylesheet Language (XSL)

CSS is currently used to render HTML web page while XSL was specifically developed to render information obtained from XML streams.

The W3C has published two versions of CSS, CSS1 and CSS2. CSS2 provides new functionality, updated descriptions and semantic changes from CSS1, see [Css]. It is important to note that Cascading Style

Sheets are unable to alter the order of the objects displayed. It simply is responsible for applying styling information to an XML document which already contains the information to be displayed in the correct order.

Often a XSLT or XSL Transformation Style Sheet is defined and its function is to transform a XML document usually into a HTML document, after which a CSS may be assigned to the resultant HTML document. XSLT may be used to re-render an XML document into a required document format.

For our purpose, we utilize CSS2 and XSL or XSLT are considered outside the scope of this chapter.

7.3 Mobile Content Delivery

Mobile Content Delivery is activated by an MS request, or alternatively known as "pulling". "Pushing" on the other hand occurs when information is sent or pushed to an MS. A good example of "pulling" would be a bank balance or location information request, while a pre-requested daily weather report sent to the MS would constitute "pushing".

Whether "pulling" or "pushing" of Mobile content, a major objective is to produce content quickly and content that abides by security goals [Pfl]:

- Integrity
- Confidentiality
- Availability

Figures 7-1 and 7-2 illustrate the process flow of pulling and pushing of mobile content respectively.

7.4 Secure OTA XML Format

Styling, transformation and security processes can be applied to content that has been retrieved or produced by a provider (Figure 7-1 and 7-2). We choose to transform content into XML as it allows for an easily readable structure and security through encryption.

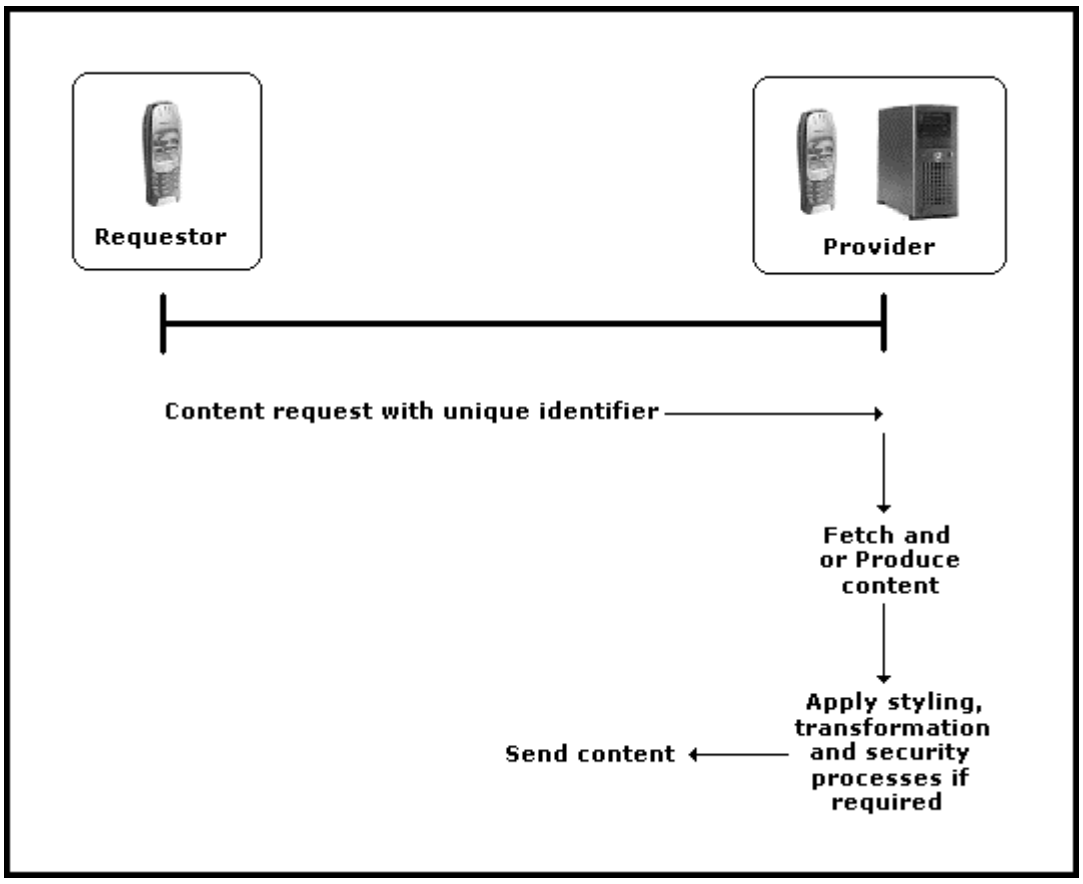

Figure 7-1 Process flow of pulling mobile content

For practical reasons, we choose to allow for the combining of styling and security into a single process, as they possess functional similarities.

The format, first and foremost provides for the inclusion and manipulation of the XML Encryption Syntax and Processing model [Ima] in order to cater for a GSM network, building what will be known as a Security Sheet (SS) around this. The SS if flexible and is ably incorporated within the Cascading Style Sheet 2 structure. We create a SS that can be incorporated within a CSS2 document, allowing for the securing of content while at the same time applying visual aesthetics or styling to an XML structure if required (Figure 7-3). The SS could also be used as a stand-alone document, allowing for the securing of only the necessary content within the XML structure (Figure 7-3). For our purposes for implementation reasons will become evident in the next chapter [chapter 8], we focus our attention on a SS that is exclusive of the CSS2 as visual aesthetics will not be a requirement.

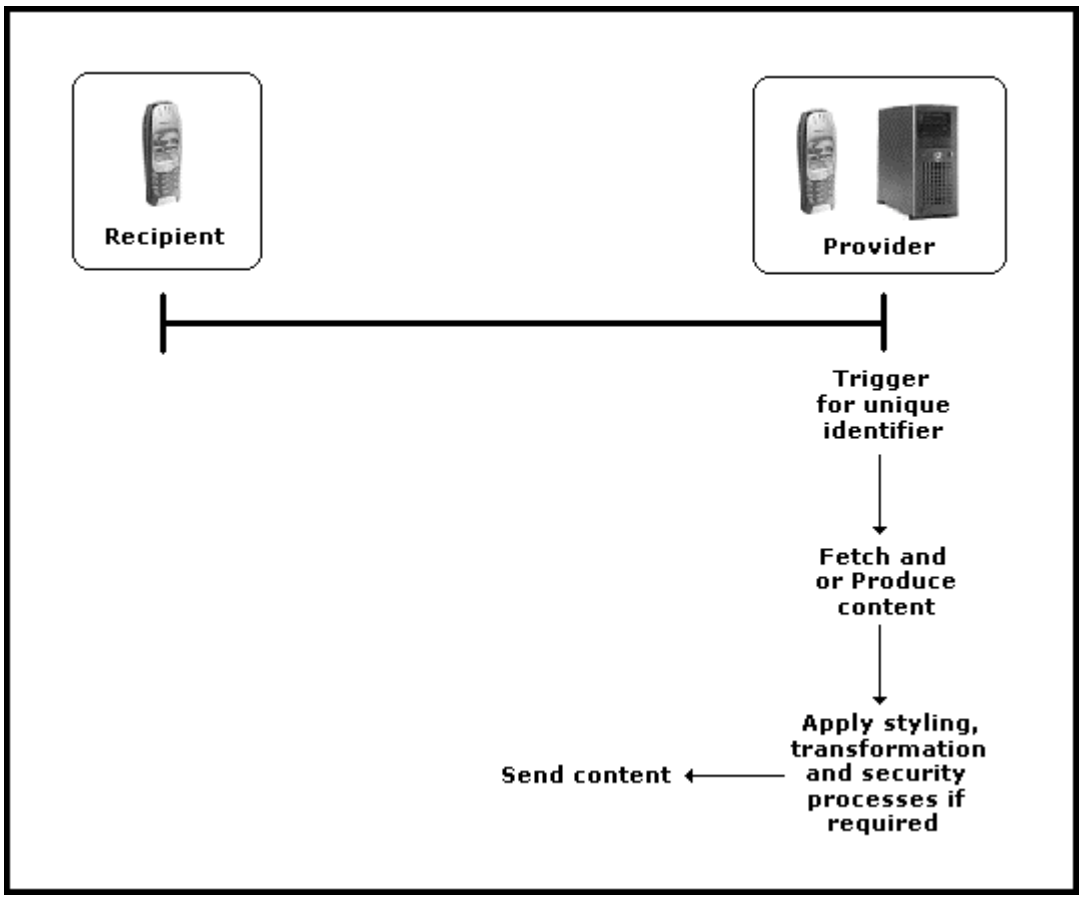

Figure 7-2 Process flow of pushing mobile content

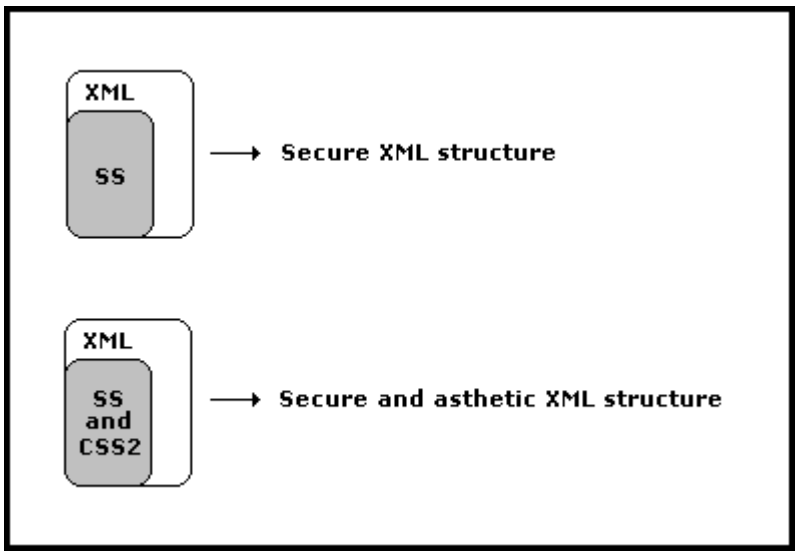

Figure 7-3 SS as stand-alone and SS and CSS2 combination applied to XML document

7.4.1 Secure XML Format

[Ima] specifies a process for encrypting data and representing the result in XML. The data may include arbitrary data such as:

- An entire XML document;
- An XML element; or
- XML element content, this includes either child elements or values between individual tag sets.

The result of encrypting data is an XML Encryption EncryptedData element which contains cipher data or identifies a reference to cipher data via a Uniform Resource Indicator (URI) reference.

A discussion of the XML Encryption syntax follows. Figure 7-4 is a shorthand representation of the XML Encryption syntax and Table 7-1 shows characters representation and their corresponding meanings.

Character	Meaning
"?"	denotes zero or one occurrence
"+"	denotes one or more occurrences
"*"	denotes zero or more occurrences
<tag/>	empty element tag means the element must be empty

Table 7-1 XML Encryption shorthand character representation

```
<EncryptedData Id? Type? MimeType? Encoding?>
        <EncryptionMethod/>?
        <ds:KeyInfo>
                <EncryptedKey>?
                <AgreementMethod>?
                <ds:KeyName>?
                <ds:RetrievalMethod>?
                <ds:*>?
        </ds:KeyInfo>?
        <CipherData>
                <CipherValue>?
                <CipherReference URI?>?
        </CipherData>
        <EncryptionProperties>?
</EncryptedData>
```

Figure 7-4 XML Encryption syntax

For a comprehensive syntax definition of each element, refer to [Ima]. Schemas [Bee] will be used for the verification of the secure XML structure, this will make sure that the XML document is well-formed

(begin tags sequentially followed by corresponding end tags) and data type [Dat] restrictions are adhered to. Schemas and data type restriction fall outside the scope of this chapter.

The CipherData element can either envelope or reference the raw encrypted data. By enveloping we mean the raw encrypted data is contained within the CipherValue element's content. When referencing is used, the CipherReference element's URI attribute points to the raw encrypted data location. Referencing will not be made use of in this approach. CipherData contains a CipherValue, which usually is a base64 encoded octet sequence.

The most important aspects namely, encrypting data and key usage, regarding XML Encryption will for our purposes be demonstrated through the use of an ongoing location example.

Suppose we have the following example:

```
<?xml version='1.0'?>
<LocationInfo>
        <Owner type="MSISDN">27831234567</Owner>
        <Coord>
                <X>301228.302</X>
                <Y>865633.863</Y>
        </Coord>
</LocationInfo>
```

where this simple XML document represents MS with MSISDN number 27831234567 and location coordinates (301228.302; 865633.863). We wish to encrypt only portions of critical information; this is achieved through element encryption.

7.4.1.1 Encrypting an XML Element

Location information, in particular the coordinates of MSISDN 27831234567 is deemed sensitive information that must be kept confidential. Therefore, the coord element is encrypted resulting in a structural change to the XML document to include an EncryptedData and CipherData element.

```
<?xml version='1.0'?>
<LocationInfo>
      <Owner type="MSISDN">27831234567</Owner>
      <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
                     xmlns="http://www.w3.org/2001/04/xmlenc#">
            <CipherData>
                  <CipherValue>encrypted coord data</CipherValue>
            </CipherData>
      </EncryptedData>
</LocationInfo>
```

The Type attribute of the EncryptData element indicates that an XML element has been encrypted, while xmlns refers to the XML namespace.

We may choose to encrypt only an XML element's content rather than encrypting the entire XML element.

7.4.1.2 Encrypting XML Element Content

Consider the application scenario where there is a need for only content to be encrypted. In our example, we choose to encrypt the MSISDN, the associated identifier to which the location information belongs. Without a unique identification, location information is considered worthless information.

```
<?xml version='1.0'?>
<LocationInfo>
      <Owner type="MSISDN">
            <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
                           Type="http://www.w3.org/2001/04/xmlenc#Content">
                  <CipherData>
                        <CipherValue>
                              encrypted MSISDN data
                        </CipherValue>
                  </CipherData>
            </EncryptedData>
      </Owner>
      <Coord>
            <X>301228.302</X>
            <Y>865633.863</Y>
      </Coord>
</LocationInfo>
```

If the application scenario requires all of the information to be encrypted, the entire XML document is encrypted.

7.4.1.3 Encrypting an Entire XML document

Continuing with our example, we may choose to encrypt the entire LocationInfo XML document if all the information was deemed to be sensitive information.

```
<?xml version='1.0'?>
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
                MimeType="text/xml">
    <CipherData>
        <CipherValue> encrypted XML document data</CipherValue>
    </CipherData>
</EncryptedData>
```

Investigation of the EncryptedData and EncryptedKey usage follows through continued use of our ongoing location example.

7.4.1.4 Encrypting Data with a Symmetric Key

We include a Symmetric Key that is associated with the encryption of the coord element.

```
…
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
                Type="http://www.w3.org/2001/04/xmlenc#Element">
    <EncryptionMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>27831234567</ds:KeyName>
        <ds:RetrievalMethod URI="#EK"
            Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" />
    </ds:KeyInfo>
    <CipherData>
        <CipherValue>encrypted Coord data</CipherValue>
    </CipherData>
</EncryptedData>
…
```

The encryption algorithm used is Triple Data Encryption Standard (3DES) Code Block Cipher (CBC) and the Symmetric Key has the associated name 27831234567 and a RetrievalMethod to indicate the location of the encrypted key. Table 7-2 contains a list of possible encryption algorithms.

The EncryptedKey structure referenced by the RetrievalMethod in the example illustrates EncryptingData with a Symmetric Key. The EncryptedKey element is comparable to the EncryptedData element except for the fact that the data encrypted is always a key value.

```
...
<EncryptedKey Id="EK" xmlns="http://www.w3.org/2001/04/xmlenc#">
        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:KeyName>27831234567</ds:KeyName>
        </ds:KeyInfo>
        <CipherData>
                <CipherValue>encrypted key value</CipherValue>
        </CipherData>
</EncryptedKey>
...
```

where the EncryptionMethod in this example is the RSA public key algorithm and the associated name 27831234567 is a property of the key that is required for decrypting the CipherData.

Algorithm	Category	URI	Level of Requirement
TRIPLEDES	Block Encryption	http://www.w3.org/2001/04/xmlenc#tripledes-cbc	REQUIRED
AES-128	Block Encryption	http://www.w3.org/2001/04/xmlenc#aes128-cbc	REQUIRED
AES-256	Block Encryption	http://www.w3.org/2001/04/xmlenc#aes256-cbc	REQUIRED
AES-192	Block Encryption	http://www.w3.org/2001/04/xmlenc#aes192-cbc	OPTIONAL
RSA-v1.5	Key Transport	http://www.w3.org/2001/04/xmlenc#rsa-1_5	REQUIRED
RSA-OAEP	Key Transport	http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	REQUIRED
SHA1	Message Digest	http://www.w3.org/2000/09/xmldsig#sha1	REQUIRED
SHA256	Message Digest	http://www.w3.org/2001/04/xmlenc#sha256	RECOMMENDED
SHA512	Message Digest	http://www.w3.org/2001/04/xmlenc#sha512	OPTIONAL
RIPEMD-160	Message Digest	http://www.w3.org/2001/04/xmlenc#ripemd160	OPTIONAL
XML Digital Signature	Message Authentication	http://www.w3.org/2000/09/xmldsig#	RECOMMENDED
base64	Encoding	http://www.w3.org/2000/09/xmldsig#base64	REQUIRED

Table 7-2 List of algorithms identifying URI for each algorithm

Block encryption algorithms are designed for encrypting and decrypting data in fixed size, multiple octet blocks. Key Transport algorithms are public key encryption algorithms especially specified for encrypting and decrypting keys. Message digest algorithms can be used as part of the key derivation, while Message Authentication is the recommended way to provide key based authentication.

Encryption and decryption operations are transforms on octets. Respective encryption and decryption processes are described in [Ima].

7.4.1.5 Encrypting Data with a Referenced Symmetric Key

We include a Symmetric Key that is associated with the encryption of the coord element, except this time the key is referenced with a RetrievalMethod. In other words, the RetrievalMethod is used to indicate the location of a key with type EncryptedKey.

```
…
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#">
        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-
                                cbc" />
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:RetrievalMethod URI="#EK"
                                Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" />
                <ds:KeyName>27831234567</ds:KeyName>
        </ds:KeyInfo>
        <CipherData>
                <CipherValue>encrypted coord data</CipherValue>
        </CipherData>
</EncryptedData>
…
```

The AES 128 key is located at URI #EK. It is important to note that either or both the KeyName and RetrievalMethod could be used to identify the same key.

We have discussed through the use of examples how secure XML formatting takes place. In order to apply security processes on an XML document we continue with the concept of a Security Sheet.

7.5 The Security Sheet (SS)

The SS document allows for the transformation of an XML document into a secure XML representation. The SS adopts CSS2 formatting and hence can be included within a CSS2 document.

Figure 7-5 is a shorthand representation of the Security Sheet syntax and Table 7-3 shows the corresponding characters representation and their meanings.

Character	Meaning
"?"	denotes zero or one occurrence
"*"	denotes zero or more occurrences

Table 7-3 Security Sheet shorthand character representation

Formatting of the Security Sheet is as follows:

```
@media media type {
Tag name [attribute*;] {
            EncData-Id: URI?;
            EncData-Type: Element; | Content;
            EncData-MimeType: MimeType;
            EncData-Encoding: (base64 | ASCII)?;
            EncData-Algorithm: (TRIPLEDES | AES-128 | AES-256 | AES-192 |
                               RSA-v1.5 | RSA-OAEP | SHA1 | SHA256 |
                               SHA512 | RIPEMD-160 | XML Digital Signature |
                               base64 | URI)?;
            EncData-CipherReference: URI*;
            EncData-EncryptionProperties: (DataTime? | MSISDN? | IMEI? |
                                           MoIP?)*;

            EncKey-Id: URI?
            ((EncKey-Name: URI?)? | (EndKey-RetrievalMethod: URI?)?)
            EncKey-Algorithm: (TRIPLEDES | AES-128 | AES-256 | AES-192 |
                               RSA-v1.5 | RSA-OAEP | SHA1 | SHA256 |
                               SHA512 | RIPEMD-160 | XML Digital Signature |
                               base64 | URI)?;
    }
}
```

Figure 7-5 Shorthand representation of Security Sheet syntax

A detailed description of the Security Style structure referencing the XML structure for securing an XML document follows.

7.5.1 Media Types

A @media rule specifies the target media types, separated by commas, of a set of rules. Curly braces delimit these rules. In the SS structure defined above, the media type can be any of the media types described in [Css] namely screen, braille, print, etc. In this document the media type will be referenced as media type handheld, indicating the output to a mobile device, typically for small screen, monochrome, limited bandwidth devices.

7.5.2 Tag name

The Tag name refers to any element name. The selection patterns could include selections on elements with specific attribute values. Distinction between elements based purely on associated attributes is catered for. This flexibility allows for accuracy to encrypt only the required elements according to various selection patterns, or in other words element attribute patterns. In Figure 7-6, element Owner with attribute type and value "MSISDN" may be encrypted differently to the element attribute pattern of element Owner with attribute type and value "IMSI". Encryption may therefore be made by making use of selection patterns.

```
@media media type {
Owner [type="MSISDN"] {…}
Owner [type="IMSI"] {…}

}
```

Figure 7-6 Example of SS selection patterns

7.5.3 The EncData reference

The EncData reference syntax describes the EncryptData element and builds the attributes and child elements. A detailed description of the EncryptData element follows.

7.5.4 EncData-Id reference

The EncData-Id reference has options URI?, where the URI refers to a Uniform Resource Identifier. The URI may refer to the location of the encrypted data at the source, in our case this will be on the mobile device itself.

7.5.5 EncData-Type reference

The EncData-Type reference has options Element or Content. This reference allows the distinction between the encryption of the element or the content that exists within an element. This is a direct representation of the EncryptedData element's Type attribute indicating the encryption data type refers to Element or Content encryption (Figure 7-7).

<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" **/ >**
or
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Content" **/ >**

Figure 7-7 EncryptedData Element Type Attribute options

7.5.6 EncData-MimeType reference

The MimeType can include any one of the MimeTypes included in [Mim]. This attribute describes the media type of the data which has been encrypted. For example, the data might include an XML document (MimeType="text/xml"), a sequence of characters (MimeType="text/plain"), or a binary image (MimeType="image/png").

7.5.7 EncData-Encoding

The EncData-Encoding reference provides for options base64 and ASCII. Usually encoding is a base64 octet sequence.

7.5.8 EncData-Algorithm reference

The EncData-Algorithm reference has options for inclusion of any of the mentioned algorithms specified in Table7-2 or URI? as options. Note for example 3DES, AES, RSA are standard block encryption algorithms while SHA1 is a standard message digest algorithm. There is also an option to list any other URI reference to a shared source algorithm between the mobile device and the origin server.

7.5.9 EncData-CipherReference reference

The EncData-CipherReference has the following option: URI*. This indicates zero or more references making use of URIs to data that has previously been encrypted with a specific encryption algorithm. Although EncData-CipherReference has been provided for, it will not be used extensively in the remainder of this chapter.

7.5.10 EncData-EncryptionProperties reference

Additional information items concerning the generation of the EncryptedData or EncryptedKey can be placed in an EncryptionProperty element [Ima]. Additional information, for example, may include a DateTime stamp or the serial number of the cryptographic hardware used during encryption. The EncData-EncryptionProperties has DataTime, MSISDN and MoIP as options. The DateTime allows for a Time stamp to be placed within the XML document as an added security feature, allowing the decryption of the secure XML document within a specified time parameter. MSISDN and IMEI refer to the MS unique identifiers that may be used in identifying the MS used during encryption.

As seen in [chapter 4], mobile environments are moving towards packet switched networks and in the not too distant future a mobile device may be assigned a static IP. The Mobile IP Working Group has developed routing support to permit IP nodes (hosts and routers) using either IPv4 [Ms4] or IPv6 [Ms6] to seamlessly roam among IP sub networks. Mobile IP (MoIP) is a means for maintaining transparent network connectivity to mobile hosts and enables a mobile host to be addressed by the IP address it uses in its home network, in spite of the network to which it is currently physically attached. Therefore, ongoing

network connections to a mobile host can be maintained even as the mobile host is moving from one subnet to the other. The wireless industry is considering using Mobile IP as one technique for IP mobility for wireless data including technologies like GPRS, UMTS and CDMA2000. This MoIP address may be used as a further encryption property while securing mobile application content and is thus catered for. For more on MoIP, refer to [Per][Kes].

7.5.11 The EncKey reference

The EncKey reference describes the KeyInfo element and builds child elements with respective attribute values. A detailed description of the digital signature element follows.

7.5.12 EncKey-Id reference

The EncKey-Id reference has only one option: URI?. The URI could be used to reference the location where the Key can be found. The URI could also reference a shared key that could exist on both the mobile device and at the origin server.

7.5.13 EncKey-Name reference

The EncKey-Name reference has options URI?. This reference is merely a name associated with the encryption key. This name association with the encrypted key could exist as a URI to a local name that resides on the MS.

7.5.14 EncKey-RetrievalMethod reference

The EncKey-RetrievalMethod reference also has option URI?. This provides a way to express a link to an EncryptedKey element containing the key needed to decrypt the CipherData associated with an EncryptedKey element.

7.5.15 EncKey-Algorithm reference

The EncKey-Algorithm reference has options for inclusion of any of the mentioned algorithms specified in Table7-2 or URI? as options. This reference is identical in nature to the EncData-Algorithm with the exception that this reference indicates the algorithm to be used for the Key encryption.

We now investigate how the Security Sheet is coupled with XML documents.

7.6 Associating Style Sheets and Security Sheets with XML Documents

We relate a style sheet with an XML document with the following processing instruction:

<?xml-stylesheet href="style sheet" type="MIME type" media="media type"
title="mobile style sheet" alternative="true"**>**

Figure 7-8 Associating CSS with XML document

where attribute:

- href specifies the location of the style sheet as a URI
- type specifies the type of style sheet as a MIME type
- media specifies the target media, in our case the media type is handheld
- alternative specifies if alternative style sheets are available
- title which associates a title describing the style sheet

We choose to relate the processing instruction of a security sheet in the same manner as a style sheet association, the only difference being the tag name.

<?xml-securitysheet href="security sheet" type="MIME type" media="handheld"
title="mobile security sheet" alternative="true"**>**

Figure 7-9 Associating SS with XML document

where attribute href now specifies the location of the security sheet as a URI reference and the MIME type will invariably will reflect "text/xml" as output.

The question is now posed, should the SS exist independently of a CSS2 or not? It is important to note that if the SS is inclusive of the CSS then the processing instruction will be defined as is in Figure 7-8. The benefits of the inclusion or exclusion of the SS from the CSS2 are now deliberated.

7.6.1 SS Independent of CSS2

The benefits of having the SS separate to the CSS2 include having the security aspects processed at the server side and have the aesthetic styling done client side, thus reducing the processing load on the origin server. Perhaps and more importantly the separation of the SS and CSS2 allows for logical benefits. This involves the benefits of deploying a security expert to design and create the SS while allowing the aesthetic styling to be designed and created by a visual design or graphics expert. A "best of both worlds" scenario is achieved with this approach.

7.6.2 SS Included in CSS2

The benefit of this approach is that the document is only parsed once and both security features and aesthetic presentation are performed simultaneously. Processing would be required to take place exclusively at the origin server.

In order to completely understand securing an XML document by making use of SSs for distribution Over The Air we now present a complete industry related example.

7.7 Complete Industry-Related Example

In the banking environment a user may request a bank balance via a mobile request. The vital information requested may include the account number and balance but not the account holder name or type of account. By only allowing security overhead on the account number and balance and not to the entire transferring document we reduce overhead.

Let a resultant XML document produced by the origin bank server look like the one represented in Figure 7-10.

```
<? xml- version="1.0" encoding="UTF-8"?>
<AccountInfo xmlns="http://bank.org/accountinfomation">
<Account min="1000">
        <Name>Neil Croft</Name>
        <Number>0123456789</Number>
        <Issuer>Issuer Bank Name</Issuer>
        <Account_Type>Savings Account</Account_type>
        <Balance>1234</Balance>
        <Currency>zar</Currency>
</Account>
</AccountInfo>
```

Figure 7-10 XML bank balance example

The associated CSS2 for the bank balance example may look something similar to what is presented in Figure 7-11.

```
@media handheld {
name,number,issuer,type,balance{
        display: table; border: solid; text-align: left;
        font-size: 8px;
        }
balance{
        font-weight: bold;
        }
}
```

Figure 7-11 CSS2 bank balance example

We now define the SS that will be responsible for securing the account number and balance (see Figure 7-10).

We choose to encrypt the entire balance element, thus if compromised there is no indication that the encrypted data represents a bank balance amount.

We make use of the RSA-v1.5 key transport algorithm and encrypt data using AES-128 and 3DES purely for demonstration purposes (Figure 7-12).

```
@media handheld {
number{
        EncData-Id: #EDnum;
        EncData-Type: Content;
        EncData-Algorithm: AES-128;
        EncData-CipherReference: none;
        EncData-EncryptionProperties: none;

        EncKey-Id: #EK;
        EncKey-Name: 543645323201;
        EndKey-RetrievalMethod: none;
        EncKey-Algorithm: RSA-1_5;
}
balance{
        EncData-Id: #EDbal;
        EncData-Type: Element;
        EncData-Algorithm: 3DES;
        EncData-CipherReference: none;
        EncData-EncryptionProperties: DataTime;

        EncKey-Id: #EK;
        EncKey-Name: 543645323201;
        EndKey-RetrievalMethod: none;
        EncKey-Algorithm: RSA-1_5;
}
}
```

Figure 7-12 SS bank balance example

Once parsed or processed, the result is a secure XML document which is then be transmitted Over The Air to the Requestor.

```
<?xml- version="1.0" encoding="UTF-8"?>
<AccountInfo xmlns="http://bank.org/accountinfomation">
  <Account min="1000">
  <Name>Neil Croft</Name>
  <Number>
    <EncryptedData id="#EDnum" xmlns="http://www.w3.org/2001/04/xmlenc#">
      <EncryptionMethod  Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-
                                    cbc" />
      <ds:KeyInfo URI="#EK" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>543645323201</ds:KeyName>
        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" />
      </ds:KeyInfo>
      <CipherData>
        <CipherValue>encrypted data</CipherValue>
        <EncryptionProperties>20030623134453</EncryptionProperties>
      </CipherData>
    </EncryptData>
  </Number>
  <Issuer> Issuer Bank Name</Issuer>
  <Account_Type>Savings Account</Account_Type>
```

```
<EncryptedData id="#EDbal" xmlns="http://www.w3.org/2001/04/xmlenc#">
    <EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
      <ds:KeyInfo URI="#EK" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>543645323201</ds:KeyName>
      <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
      </ds:KeyInfo>
      <CipherData>
        <CipherValue>encrypted data</CipherValue>
        <CipherReference/>
         <EncryptionProperties>20030623134453</EncryptionProperties>
      </CipherData>
  </EncryptData>
</Account>
</AccountInfo>
```

Figure 7-13 Secure XML bank balance example ready for OTA transmission

The EncryptedKey, referenced by identifier "EK" is shown in Figure 7-14.

```
<EncryptedKey Id="EK" xmlns="http://www.w3.org/2001/04/xmlenc#">
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:KeyName>102323546345</ds:KeyName>
      </ds:KeyInfo>
      <CipherData>
            <CipherValue>encrypted key value</CipherValue>
      </CipherData>
</EncryptedKey>
```

Figure 7-14 EncryptedKey for secure XML bank balance example

The parsing of the SS and original XML document in order to produce a secure XML document should be achieved quite simply but falls outside the perimeter of this chapter.

In the example, the name, issuer and type of account are pushed to the mobile device in clear text while the account number and balance are encrypted making use of the 3DES encryption algorithm. The account number and balance element's content were encrypted. A DateTime stamp was also inserted as an additional encryption property. This property allows a verification process to occur to indicate whether the encrypted content has passed the window period of time in which decryption can take place.

7.8 Conclusion

By applying encryption to certain deemed crucial information we reduce overhead and allow for flexibility at an application level within the mobile environment. The model described above allows for adaptation into any mobile architecture and achieves the purpose of secure quick transmission Over The Air (OTA). The Security Sheet's flexibility, designed to adhere to the CSS2 structure, adds value to the approach of securing while applying aesthetic representation at the same time.

In the next chapter, we explore the concept of security by position. We investigate the possibility of using one's position as the sole access mechanism to a restricted resource.

Chapter 8

8. ACCESS BY POSITION, A SECURE APPROACH TO LOCATION-AWARE MOBILE ACCESS CONTROL

8.1 Introduction to Secure Location-Aware Mobile Access Control

In [chapter 3], we discussed current approaches of determining a subscriber's position by making use of the GSM network and Global Positioning System (GPS). Location-Based services are primarily used to gain information on demand according to subscriber's location; in this chapter we explore the concept of using location in order to gain access to a restricted resource.

Location of a mobile user is currently described as a two dimensional coordinate. A high and low degree of accuracy is required for different applications, and because of this different location determination technologies are best suited to different situations. We will focus our attention on obtaining a high degree of accuracy and precision in location determination required in particular to accommodate and allow for a security by position approach.

Accuracy is defined as the displacement of a point from its true position with respect to a reference model. Precision refers to the repeatability of this measurement.

In achieving a high degree of accuracy and precision in positioning, location determination should comply with the following:

- Multiple location information sources should be combined to increase accuracy
- Indoor and outdoor operations should not affect location determination
- Cooperation and history between clients should increase accurate positioning and account for repeatability of a measurement
- Future technologies should easily integrated into the existing location architecture

This chapter serves to describe a proposed implementation of location coordination as a 3-Dimensional spatial region with increased degree of confidence by combining multiple location information sources and intelligent Mobile Stations (iMS). This approach will aid in a model for secure access by position for a mobile user.

8.2 Overview

Location information can be described in different forms, namely:

- Absolute
- Relative
- Symbolic

Absolute location information provides for a 3-Dimensional position coordinates described in a standard format relative to the earth. This format is defined using the World Geodetic Systems 1984 (WGS84) as reference system [Wgs]. From this, latitude and longitude are defined with respect to the ellipsoid representation of the earth (Figure 8-1).

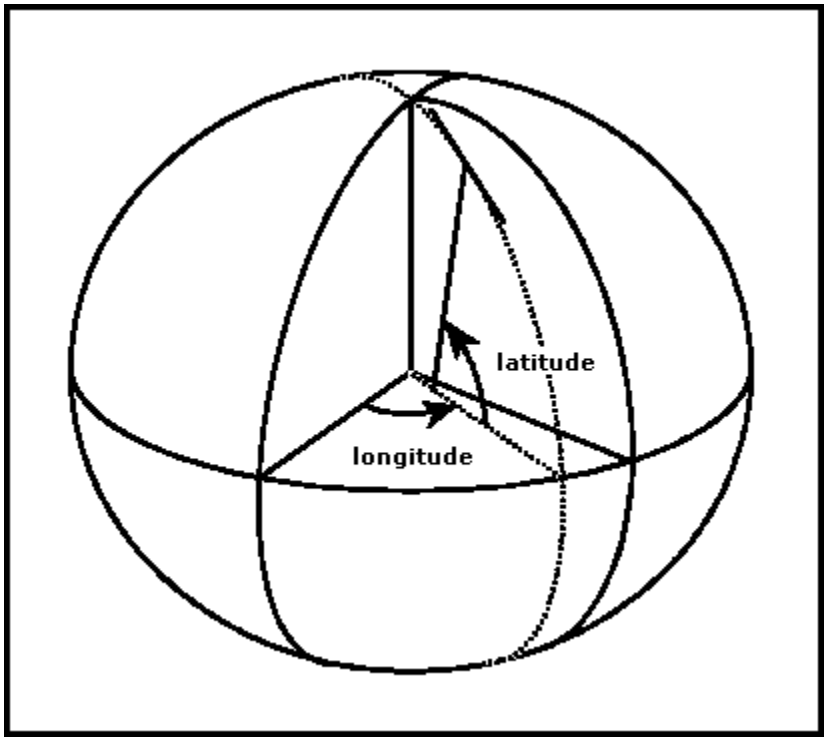

Figure 8-1 Latitude, longitude definition of ellipsoid earth

Altitude is defined as the distance above the earth's surface (ellipsoid representation) (refer to Figure 8-2).

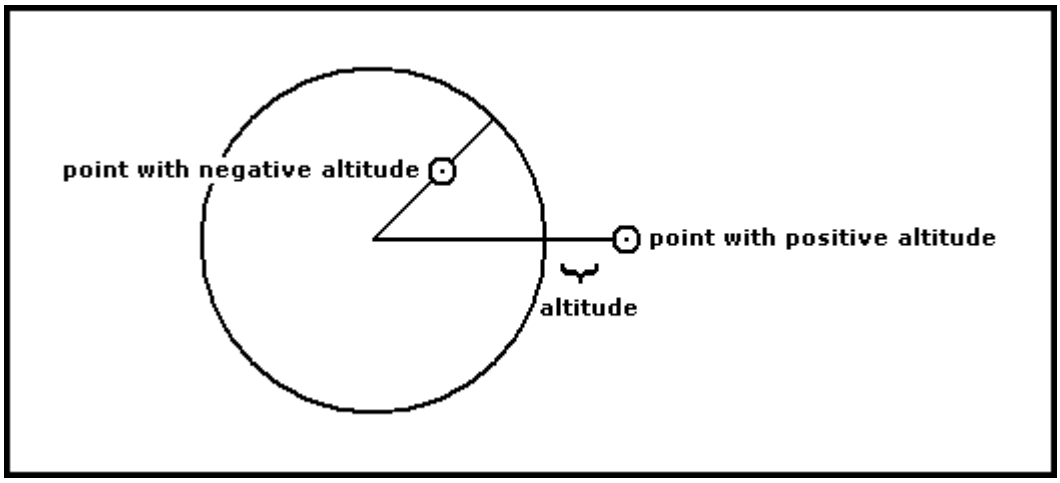

Figure 8-2 Altitude representation of ellipsoid earth

Global Positioning System (GPS) makes use of the WGS84 as reference system.

Relative location is best described as the position with respect to an arbitrary location mark defined as the origin. A relative location coordinate system is characterized by the origin coordinates and a reference system [Arg].

Location that can be described as a position relative to some known entity where the entity's location may or may not be precisely known with attached associative information is known as symbolic location information, for example you are in room 123 on the second level of the President's hotel.

In current GSM location techniques relative positioning is most commonly used, a high degree of accuracy is unachievable with current GSM location technologies [chapter 3.8] hence absolute positioning is unobtainable. Ideally, precise absolute positioning with a low degree of uncertainty and high confidence percentage is a requirement in the generation of "access by position" modelled approach. A proposal of how high accuracy in positioning is achieved is presented later in the chapter.

8.3 Universal Geographical Area Description (GAD)

Within the GSM architecture, [Gad] provides a framework for the establishment of common coordinate system inclusive of error estimation. In [Gad], each 3-D coordinate (latitude, longitude, altitude) is accompanied by an uncertainty estimate that together with the coordinates defines a point and an uncertainty ellipsoid point around that point. The description of an ellipsoid point is that of a point on the surface of the ellipsoid, such a description in this chapter is in reference to a point on the earth's surface, or close to the earth's surface. The uncertainty per coordinate is defined as the distance d_i such that each measured coordinate x_i lies within distance d_i of the actual location coordinate. The confidence, p, is the total probability that each location measurement coordinate x_i lies within the error ellipsoid, i.e. within the distance d_i of the actual location coordinate. High accuracy is dependant on a high degree of confidence and small uncertainty ellipsoid around the ellipsoid point. From [Gad] again, the coordinates of an ellipsoid point are coded with an uncertainty of less than three meters, while uncertainty itself may be coded down to values as small as one meter. Altitude is encoded in increments of one meter.

8.4 Current GSM Location Determination Approach

Currently location determination technologies, only making use of the GSM network, place a mobile user within a 2-Dimensional confidence region. This region is determined using various mathematical formulas. Approaches include Cell-ID (CGI) and TA, Angle of Arrival (AOA), Time of Arrival (TOA), Time Difference of Arrival (TDOA), Enhanced Observed Time Difference (E-OTD) [Chapter 3]. Refer to Figure 8-3.

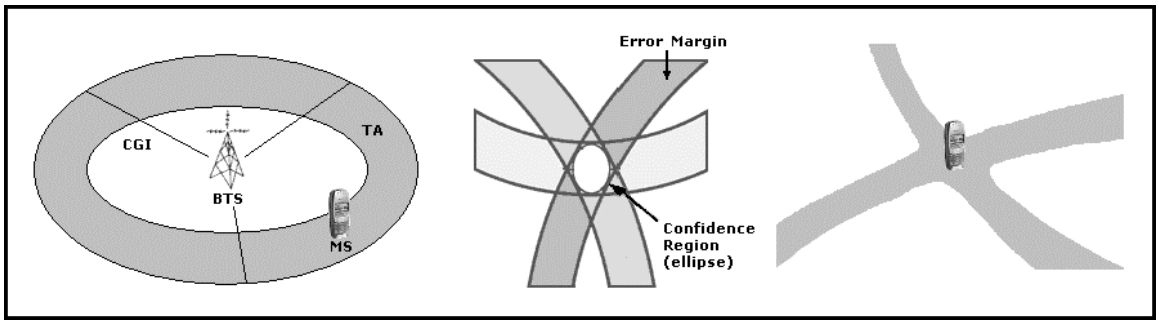

Figure 8-3 Region of confidences for some of the different GSM location determining technologies

8.5 Dimensional Spatial Location Positioning

Third dimension coordination is usually described in a geometric plane. A Cartesian coordinate system is defined by values x, y and z. x is the distance from the x-axis or latitude, y is the distance from the y-axis or longitude, z the distance from the z-axis or altitude .The axis are orthogonal to each other. The unit used for x, y, z are a distance unit, such as meter. These coordinate systems are used for flat "planar" descriptions of points. Position is a referenced point described by an x-axis value, a y-axis value and a z-axis value (latitude, longitude, altitude). Location techniques, in the GSM network, do not provide a z-axis value or altitude of a mobile subscriber. We assume for the purpose of this chapter that a mobile device is able to provide for the determination of its own altitude (Figure 8-4). This is easily achievable by incorporating an alto-meter within the MS, thus providing the third dimension (altitude) when calculating the MS's location. By incorporating the third dimension accuracy in location positioning is increased through the use of triangulation. Figure 8-5 illustrates a real world representation of 3-Dimensional positioning of MS.

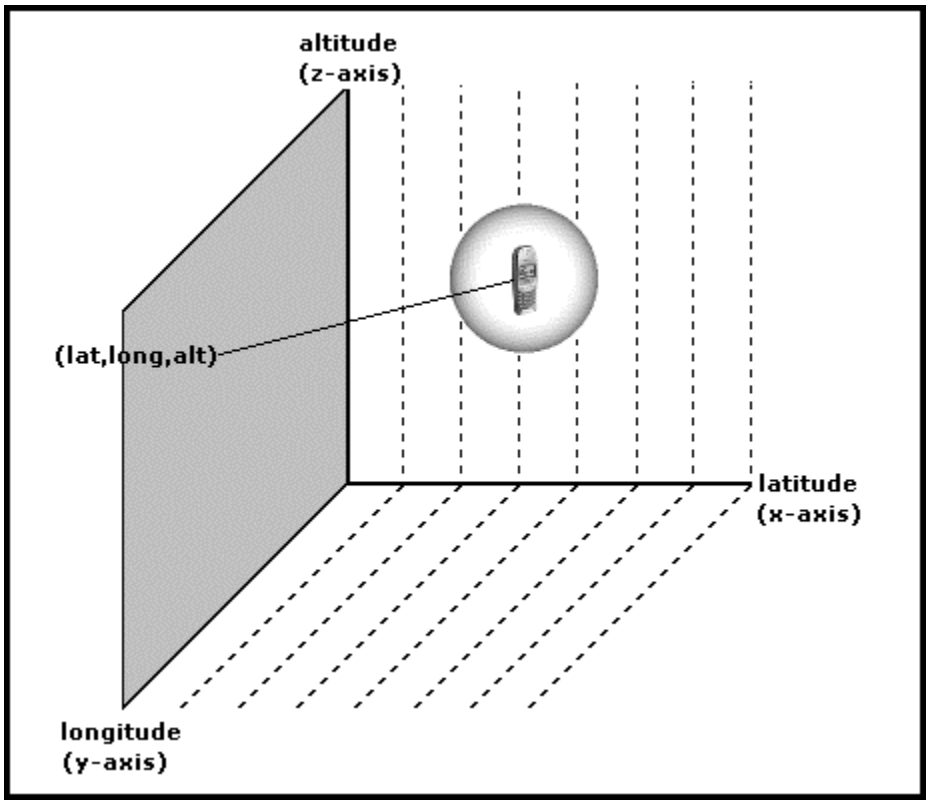

Figure 8-4 Dimensional positioning of Mobile Station

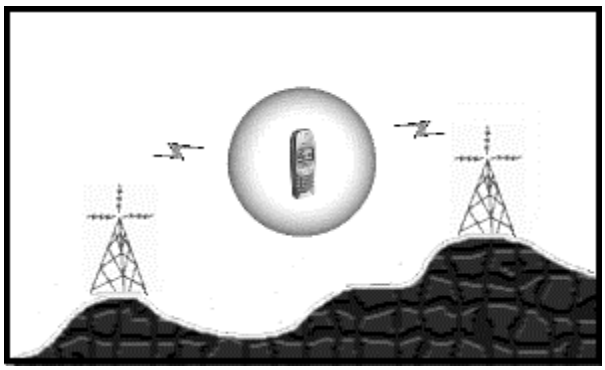

Figure 8-5 Real World representation of 3-Dimensional positioning of Mobile Station (MS)

8.6 Model for Security by Position – Access Through Accurate Mobile Device Location

As stated in [chapter 3.10], ideally a mobile subscriber's locations should be determined locally by the subscriber itself and communicated to the underlying GSM network only on request. This approach reduces GSM infrastructure dependency; however there is an energy trade-off and computational power ability for the MS to consider.

We make provision for access through accurate mobile device location as an additional security enhancement to the models presented in chapter nine.

In the generic "access by position" secure operation process (Figure 8-6), once a mobile device is authenticated on the GSM-GPRS network it may request access to a particular resource. It is assumed using this approach that access will be granted on the basis of position alone; however other security measures may be used in conjunction with this system's operation process. A location server, which may include a mobile subscriber history location file, requests the mobile subscriber's location. In general, the confidence in a location estimate can be enhanced through integration of multiple position measurements stored in a history file [Arg].

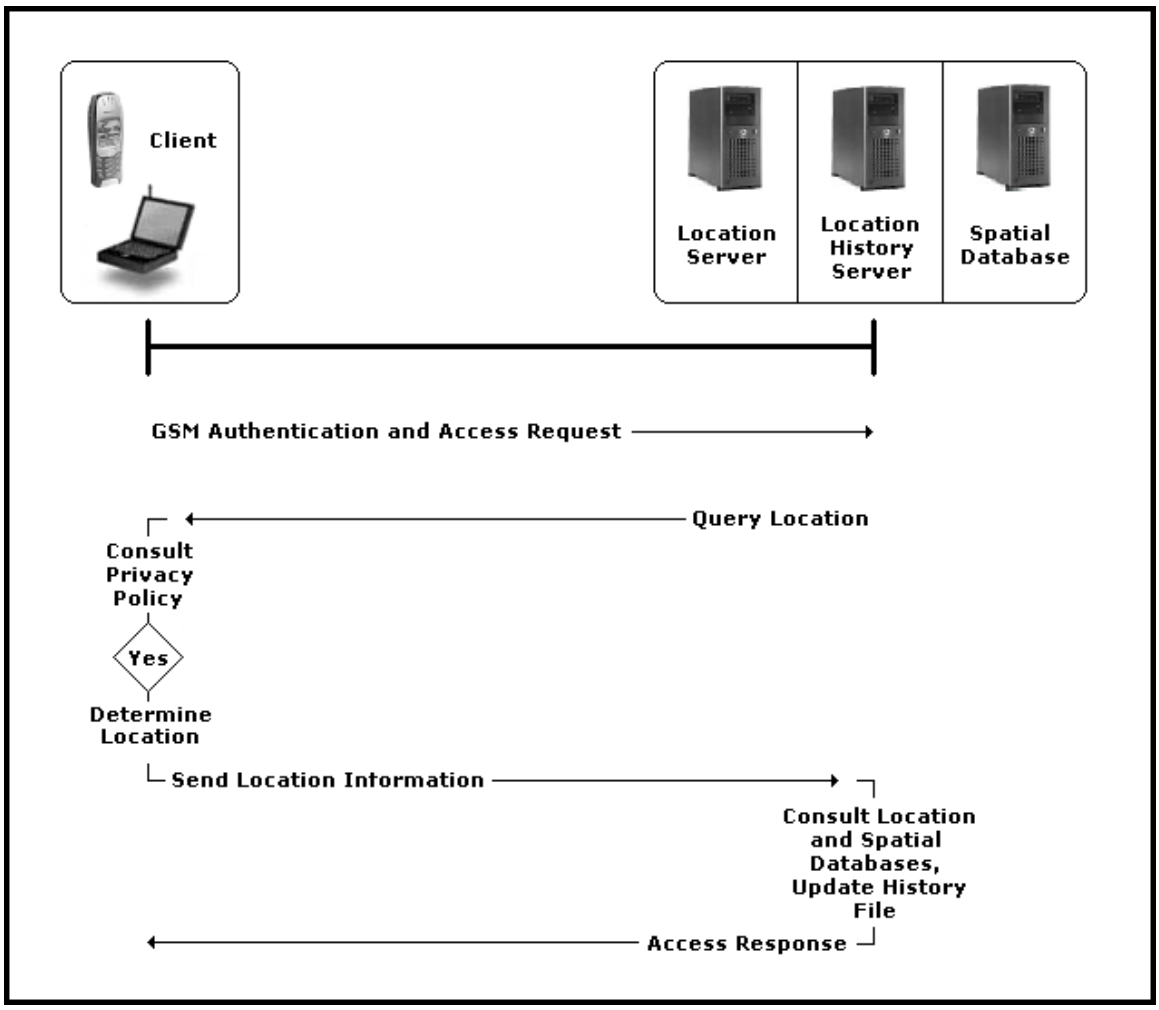

Figure 8-6 Generic "access by position" secure operation process

For the mapping of position to the subscriber's environment, the location server communicates with a spatial database. This spatial database provides relative or symbolic location information. For example, are we able to determine through the use of a spatial database if the subscriber is on campus?

Once a mobile device is queried for its location, irrespective of where the request is being made from, the mobile device queries its local privacy policy to determine if it should respond with its location coordinates and uncertainty thereof to the requesting source. If the privacy policy allows for a location request from the requiring source, the mobile device itself determines its location and sends this location information back to the location server. The location server receives the location information, consults the spatial database if need be, and updates the location history file. The location server requires an interface to the Home Location Register (HLR) which contains

permissions to resources per subscriber or alternatively to a third party Authentication Centre, passing to it the relevant subscriber details and location information. Based on location permissions at the HLR or third party authentication centre, a subscriber's request to access a resource is returned with an appropriate access response.

We now focus our attention on determining location of a subscriber's location accurately.

8.6.1 Accurate Location Determination

There are a number of ways to determine or improve a position estimate through the sharing of information. One of the simplest forms of cooperation location is for a node (mobile device) to request the positions of other nodes (mobile device) in the current communication neighbourhood (GSM-GPRS network), using a broadcast request location message. Depending on the transmission range, a set of regions (ellipsoids) can be collected by the source (requesting mobile device) and used to estimate its own location. The accuracy depends on the density on the responding devices, the environmental characteristics (obstructions) and the effects thereof of radio frequency properties (multipath effects) [chapter 3.3.1].

The model under consideration consists of a collection of intelligent, self-sufficient MSs or mobile devices that can be randomly spatially arranged and have the ability to communicate over wireless links with other clients within a communication environment. Concerning intelligent devices, the assumption made is that a mobile device has the ability to determine its own altitude (through an alto-meter or other means) and equipped with enough computing capability to calculate its own location with the aid of a multi-lateration algorithm. Wireless methods that may currently be deployed in the communication environment include:

- Infrared (IR)
- Bluetooth
- WLAN

For short range radio technologies like Infrared, Bluetooth and WLAN [chapter 5], knowledge of even one single other location information source can provide a significant increase in location determination accuracy. Organizations, such as the Bluetooth Special Interest Group

(SIG) on Location Positioning Profile, are exploring issues involving Bluetooth Personal-Area Networks (PAN) or piconets [Mul].

In general, the more devices that can respond with their position, the more accurate the source position can be determined [Arg]. If one node can communicate with another, a proximity constraint exists between them [Doh]. If, for example, node x has a communication perimeter of 100 m, then all other active communicating nodes will be within a 100 m proximity of node x. We therefore need to increase the proximity communication range in order to accommodate as many available responding devices. Due to communication range limitations that IR, Bluetooth and WLAN possess (measured in meters); we require an alternative to increase the proximity communication constraint to incorporate more responding devices.

To further increase accuracy using this approach, non-GSM entities who know their own position information are included and seen as one of the multiple location information sources (Figure 8-7). For example, a WLAN Access Point (AP) [chapter 5.3] may be used as a non GSM entity (node) as source for external location information.

In general, a set of four non-coplanar (points not in the same coordinate plane) nodes can determine a relative 3D coordinate system, given the ranges to each other [Arg].

Figure 8-7 illustrates location determination from multiple location information sources. Take for instance MS3 that wishes to calculate its location with a high degree of accuracy. MS3 is in communication neighbourhood which includes GSM entities MS1, MS2, MS5 and a single external non-GSM entity. It is assumed that all nodes are non-coplanar. With these multiple information sources and the range known between the communication nodes, MS3 can calculate its own 3D coordinates.

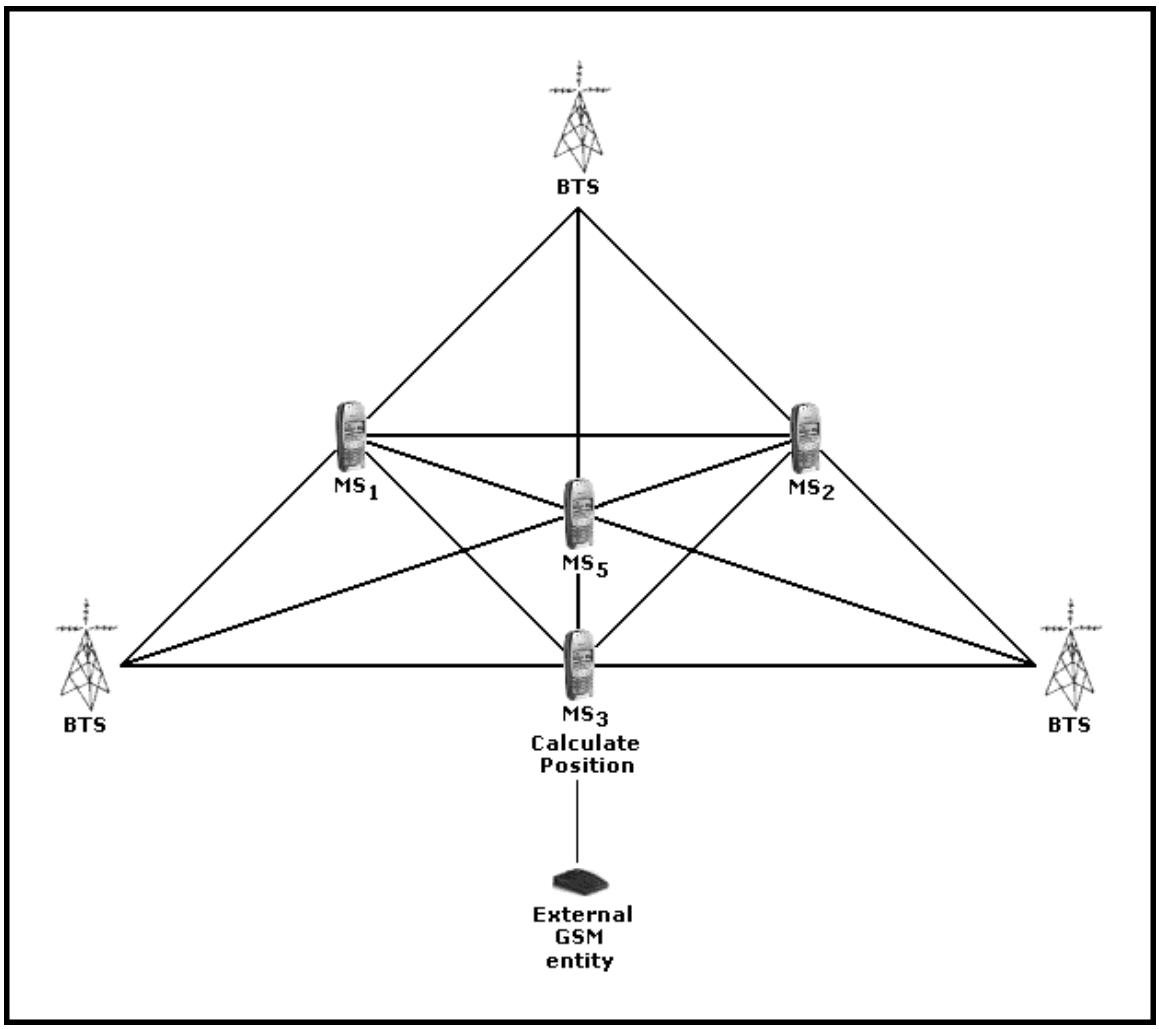

Figure 8-7 Determining positioning via multiple location information sources

To avoid the need for the integration of different wireless communication techniques for the purpose to communicate peer-to-peer location information, we introduce the concept of a peer-to-peer GSM communication connection. This approach allows for a direct peer-to-peer communication between two conventional GSM MSs without the use of the underlying GSM network. Push to Talk over Cellular (PoC) or Push To Talk (PTT) is an example of recent developments in peer-to-peer or mobile-to-mobile voice communication by making use of the underlying GSM-GPRS network. PoC/PTT will effectively turn the MS into a walkie-talkie device without a range limitation. Several companies are currently competing to bring this feature to GSM and CDMA networks. For more on PoC/PTT, see [Poc]. Voice using PoC will not travel via the conventional GSM network but rather travel over GPRS, effectively meaning for a peer-

to-peer connection, voice will travel over IP. This effectively is known as Voice over IP (VoIP). For more on Voice over IP, refer to [Var].

Our approach is a simple concept yet complex to deploy. From [chapter 2.2.2], we recall that the Base Transceiver Station (BTS) is a radio tower or pico (single) cell that the Mobile Station communicates with and it houses the radio transceivers and handles the radio protocols with the MS. We adapt this architecture to accommodate a direct MS-to-MS (peer-to-peer) communication link, introducing the concept of a virtual Base Transceiver Station (vBTS). In other words, all MSs couple in the GSM network as virtual Base Transceiver Stations (vBTSs) (Figure 8-8). vBTSs effectively become extensions to BTSs and the GSM network, thus providing further coverage.

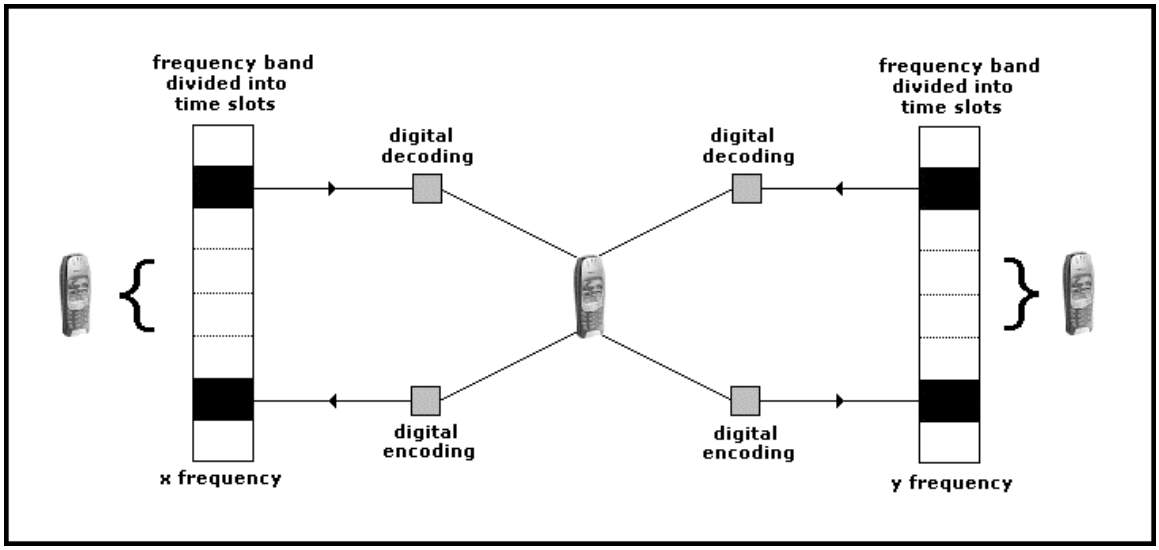

Figure 8-8 intelligent MSs acting as virtual BTSs to which a peer-to-peer connection can be made

There are a number of design and implementation issues that surround the effective deployment of intelligent devices that are able to couple as virtual BTSs namely:

- Frequency interference – multiple BTSs and virtual BTSs operating on exactly the same frequency range within the GSM frequency band
- MS able to accept, receiver and handle multiple peer-to-peer connections
- MS willingness to accept or deny peer-to-peer connections based on privacy requirements
- Handover between BTSs and vBTSs

The advantage of implementing this virtual BTS approach is triple fold as the iMS not only can communicate on a peer-to-peer level for voice and data purposes but can be also be used for routing purposes. This allows a subscriber that is outside the range of a BTS to possibly connect to another MS (seen as a vBTS), and have call or data routed to an actual BTS and the underlying GSM-GPRS network. From the GSM specification and [chapter 2.2.2], we recall that an MS can communicate with up to 16 base stations. This property based on GSM principles will effectively allow for an iMS to connect up to 16 vBTSs.

It is important to note that an MS-to-MS connection is not a permanent connection, unless the MS is being used for routing purposes. For our purpose it shall be used to connect and retrieve location information securely. Once location information is received a subsequent disconnect is performed by the MS.

In the conversion of an MS to a truly intelligent device significant software and hardware upgrades are required. How this conversion is achieved is beyond the scope of this chapter.

Location computation can either occur in a proactive or reactive manner. For our purposes we adopt the approach of determining location on a reactive basis only. In other words, to curb the computation at the intelligent device location is determined only when requested to do so. The only inherent danger may occur by what may be seen as a "ripple effect" whereby a device requests multiple location information from devices that themselves do not know their own location and have to perform location computations. This spawned result is eliminated by the use of location beacons or static nodes within the GSM network or to limit the number of "ripples" allowed when determining location. It is important to note that BTSs are considered as static beacons and may provide location information on demand if it is known.

We require an easy yet flexible way of best describing determined location. A protocol is required that allows for possible attached source identification, Quality of Service (QoS) and region of uncertainty descriptor that falls within the boundaries of a Universal Geographical Area Description (GAD).

The Mobile Location Protocol (MLP) is an XML based protocol and its purpose is to define a simple and secure access method that allows Internet applications to query location information from a wireless network, irrespective of its underlying air interface technologies and

positioning methods [Lif]. We adopt MLP for our purpose. The MLP serves as the interface between a Location Server and a Location Client. For our purposes a Location Server could reflect a beacon or an MS. In a direct peer-to-peer connection a Location Server could engage as a Location Client.

Again from [Lif], the encoding for WGS84 as reference system in MLP is as follows:

```
<CoordinateReferenceSystem>
    <Identifier>
        <code>4326</code>
        <codeSpace>EPSG</codeSpace>
        <edition>6.1</edition>
    </Identifier>
</CoordinateReferenceSystem>
```

MLP allows for the requesting of locations of one or more Mobile Subscribers. It also has support for requesting a certain QoS, Type of location and priority. MLP provides for [Lif]:

- Identity Element Definitions
- Location Element Definitions
- Shape Element Definitions – location falls within bounded region
- Quality of Position Element Definitions

Delivery of location information will usually consist of the following:

- Standard Location Immediate Request
- Standard Location Immediate Answer
- Standard Location Immediate Report

For our purposes we choose to eliminate the Standard Location Immediate Report as the benefit does not outweigh the overhead incurred by its use. Figure 8-9 illustrates the encapsulated message flow of an MS-to-MS Service.

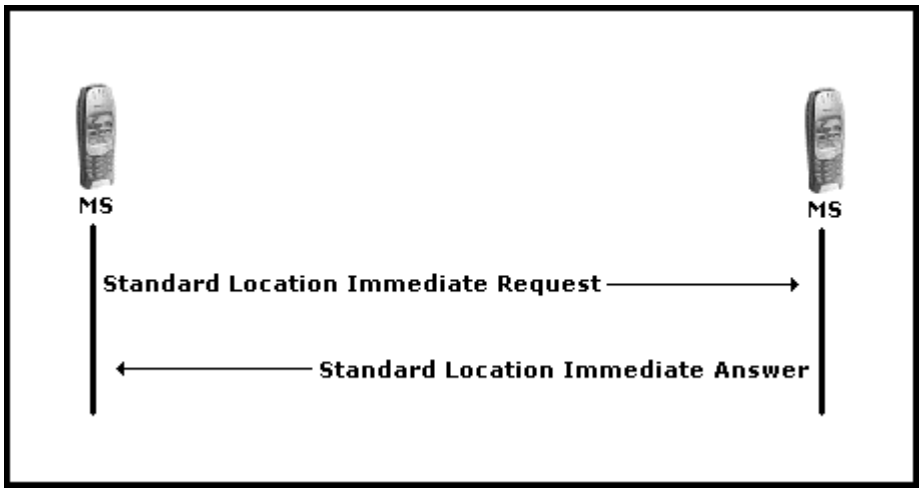

Figure 8-9 Message flow encapsulating MLP for MS-to-MS Service

Let us look at a brief example of a Standard Location Request made by MSISDN 27831235555 and a Standard Location Immediate Answer from MSISDN 27831234567 to a location request in the MLP format. It is important to note that only the basic elements are shown, for a full reference of supported elements, refer to [Lif].

```
<slir ver="3.0.0" res_type="SYNC">
<msids>
        <msid type="MSISDN">27831235555</msid>
</msids>
<eqop>
        <resp_req type="LOW_DELAY" />
        <hor_acc>100</hor_acc>
        <alt_acc>100</alt_acc>
</eqop>
<geo_info>
        <CoordinateReferenceSystem>
                <Identifier>
                        <code>4004</code>
                        <codeSpace>EPSG</codeSpace>
                        <edition>6.1</edition>
                </Identifier>
        </CoordinateReferenceSystem>
</geo_info>
<loc_type type="CURRENT_OR_LAST" />
<prio type="HIGH" />
</slir>
```

where slir represents the Standard Location Immediate Request with a synchronous response type. msid is the unique identifier where the request is being made from, eqop defines the quality of position which in this example incorporates resp_req (response time requirement),

hor_acc (horizontal accuracy in meters) and alt_acc (accuracy of altitude in meters). loc_type defines the type of location requested while prio defines the priority of a location request.

Here is the Standard Location Immediate Answer to the Standard Location Request made by MSISDN 27831235555:

```
<slia ver="3.0.0">
      <pos>
            <msid>27831234567</msid>
            <pd>
                  <time>20030707134454</time>
                  <alt>1200</alt>
                  <alt_acc>1</alt_acc>
                  <shape>
                  <CircularArea srsName="www.epsg.org#4004">
                        <coord>
                              <X>301228.302</X>
                              <Y>865633.863</Y>
                        </coord>
                        <radius>2</radius>
                  </CircularArea>
                  </shape>
            </pd>
      </pos>
</slia>
```

where slia represents the Standard Location Immediate Answer, msid the unique identifier, time the DateTime stamp with attributes available to represent offset of Greenwich Mean Time (GMT), alt the altitude in expressed in meters, alt_acc the accuracy of the altitude expressed in meters and the shaped region of confidence of MSISDN 27831234567's position.

Although complete anonymity in location information may not be appropriate for some instances, in this case no identifiers or authorization information need accompany the location information. However, location information is usually required by law in case of an emergency. Anonymity is entirely up to the discretion of owner of particular location information; this may reside in the owner's Privacy Policy. For example, a static beacon may release its location information with an identifier whereas a mobile subscriber may choose not to. Using this approach, the requesting source will always have to provide identification when asking for location information.

Once multiple locations are gathered (at least four), the iMS calculates its own 3D coordinates by making use of a multi-lateration algorithm.

Such a location determination algorithm falls outside the scope of this chapter. Before location calculations take place, we consider the role privacy plays in locating an object.

8.7 Privacy Policy

Location information is sensitive information. Thus, stringent procedures must be in place to control who obtains this information and under what circumstances. One of the ways that private information can be safeguarded is by making use of privacy policies. Research has gone into automating such policies, as described in the P3P protocol [P3P].

[Sne] formulates key concepts when implementing privacy policies around access to location information depending on intended use and identity of the recipient. [Cue] illustrates the main principles guiding the requirements described in geographic privacy, also referred to as (IETF GEOPRIV), these are:

- Security of the transmission is essential to guarantee the integrity and confidentiality of the location information
- A critical role is played by the user-controlled privacy rules, which describe the restrictions imposed or permissions given by the user
- One type of privacy rules specify in particular how location information should be filtered, depending on who the recipient is
- The located object should be able to carry a limited but core set of privacy rules
- Whenever appropriate, the location information should not be linked to the real identity of the user

In this model, each subscriber will have an associated policy which resides on the MS and is replicated on a Policy Custodian or Policy Authority. For our reference, this policy shall be known as the Mobile Location Privacy Policy or alternatively MLPP. A generic MLPP is available for download on request by a subscriber from a Policy Custodian using the secure Over The Air (OTA) transfer as described in [chapter 7]. A requestor (MS) may request to download, update or even delete its corresponding Privacy Policy from the Policy Custodian (potentially situated within GSM) (Figure 8-10). Change requests initiated by an MS to its Privacy Policy are not dealt with in this chapter.

The HLR identifies the MSs' Policy Custodian and if the requester identifies itself to be the policy owner, the policy may be altered or downloaded. The Privacy Policy Custodian may exist as an external GSM-GPRS entity node; however for security, integration and maintenance purposes it is recommended that the Policy Custodian be incorporated within the realm of the GSM-GPRS network.

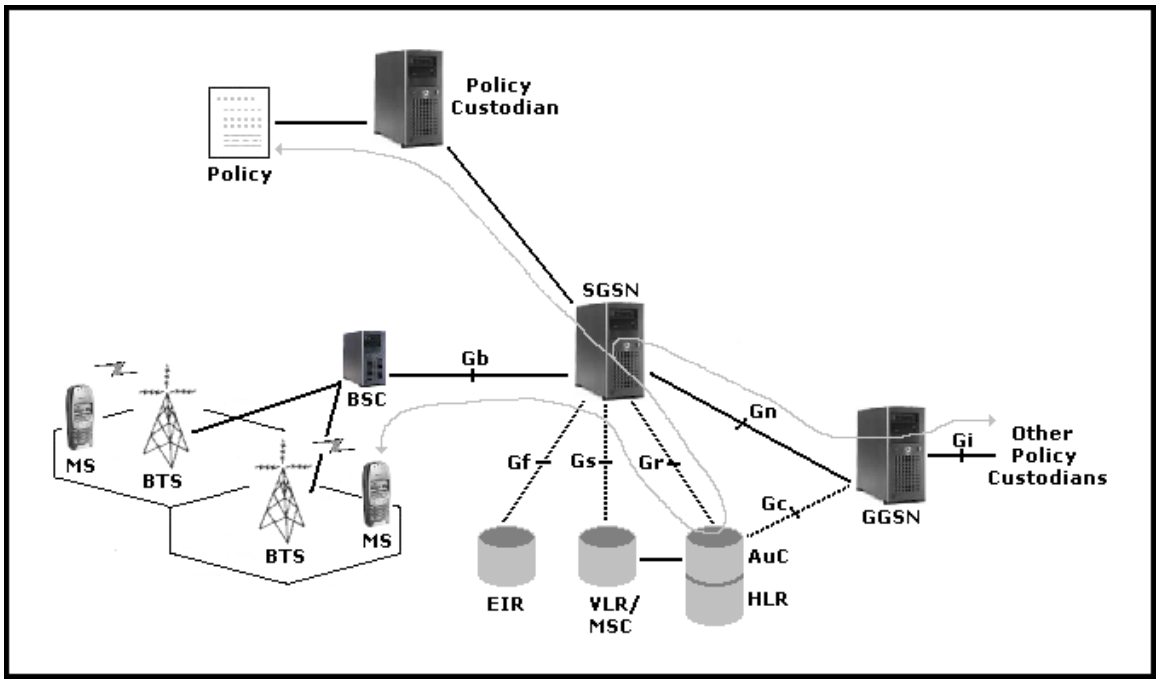

Figure 8-10 Sequence of interactions to alter or retrieve Privacy Policy

It is important to note that the privacy policy, for the purpose of this chapter, will only include privacy issues relating to location information and access to location information. However, the privacy policy may contain other privacy-related information for example if the MS is allowed to call another MS and if so when (time interval) the call is allowed to be made. This allows for business rules to be implemented and enforceable from the MS itself.

8.8 Mobile Location Privacy Policy (MLPP)

A mobile subscriber may restrict delivery of location information based on the following:

- Spatial restriction, for example when a subscriber is on campus only
- Temporal restriction, for example when the current time falls within a specific time zone or business hours only
- Identity restriction: is the requesting source anonymous or known to the subscriber
- Purpose restriction, for example tracking purposes or as reference to multiple location information

Using these possible restrictions we formulate a Mobile Location Privacy Policy Protocol XML format (Figure 8-12) or Location MPP from the Mobile Location Privacy Policy Element Definitions (Figure 8-11). The table below describes the special characters and separators used in the DTD for MLPP.

Character	Meaning
"+"	denotes one or more times
"*"	denotes zero or more times
"|"	denotes or as in "this or that"
"&"	denotes and as in "this and that"
"#"	Required
"{default}"	denotes default value if no value specified
"?"	denotes optional

Table 8-1 Mobile Location Privacy Policy (MLPP) Element Data Type Definition (DTD)

```
<!-- MLPP -->
<!ELEMENT MLPP#                                                    >
<!ATTLIST  MLPP
            ver#                                        {1.0.0}    >
<!ATTLIST  MLPP
            resides# (Local | Custodian)                {Custodian}  >
<!ELEMENT Owner?                                                   >
<!ATTLIST  Owner
            type# (MSISDN | IMSI | IMEI)                {MSISDN}   >
<!ELEMENT StoreLocation?
            (Local | History File)                      {History File}  >
<!ELEMENT Guard+
            (Spatial & Temporal & Identity & Purpose)              >
<!ELEMENT Spatial*
            (Lif Element Definitions)                              >
<!ELEMENT Temporal*
            (Date & Every)                                         >
<!ELEMENT Identity*
            (Owner)                                                >
<!ELEMENT Purpose*                                      {Location}  >
<!ELEMENT Date*
            (StartDateTime & StopDateTime)                         >
```

```
<!ELEMENT Every*
            (Day)                                                    >
<!ELEMENT Day+                                                       >
            (StartTime & StopTime)                                   >
<!ATTLIST  Day
          dow# (Monday | Tuesday | Wednesday | Thursday |
                Friday | Saturday | Sunday)     (#PCDATA)  >
<!ELEMENT StartDateTime                          (#PCDATA)  >
<!ELEMENT StopDateTime                           (#PCDATA)  >

<!ELEMENT StartTime                              (#PCDATA)  >
<!ELEMENT StopTime                               (#PCDATA)  >
```

Figure 8-11 Mobile Location Privacy Policy Element Data Type Definition (DTD)

From the Mobile Location Privacy Policy Element Definitions we formulate the basic structure of the Mobile Location Privacy Policy Protocol XML format.

```
<MLPP ver="1.0.0" resides="Local | Custodian" >
      <Owner type="MSISDN | IMSI | IMEI" ></Owner>
      <StoreLocation>Local | History File</StoreLocation>
            <Guard>
                  <Spatial>
                        <slia ver="3.0.0"></slia>
                  </Spatial>
                  <Temporal>
                        <Date>
                              <StartDateTime></StartDateTime>
                              <StopDateTime></StopDateTime>
                        </Date>
                        <Every>
                              <Day dow="Monday | Tuesday | Wednesday | Thursday |
                                        Friday | Saturday | Sunday">
                                    <StartTime></StartTime>
                                    <StopTime></StopTime>
                              </Day>
                        </Every>
                  </Temporal>
                  <Identity>
                        <Owner type="MSISDN | IMSI | IMEI"></Owner>
                  </Identity>
                  <Purpose>Location</Purpose>
            </Guard>
</MLPP>
```

Figure 8-12 Mobile Location Privacy Policy Protocol XML format

where attribute resides represents whether the MLPP is stored locally (on the device) or at a reachable custodian server. The Owner of the

MLPP is identified by its type, usually by the MSISDN or mobile number. StoreLocation determines where the location information must be kept, usually this is stored in a history file. The Guard, represented as a combination of spatial, temporal, identity and purpose guard, illustrates the restriction requirements that must be adhered to when determining location for distribution.

As previously mentioned, the MLPP is representative of an overall view of a Mobile Privacy Policy. However, for our purpose we define our privacy requirements around location and the possible storage thereof. To adjust the MLPP we simply define additional values for the Purpose element within the Mobile Location Privacy Policy Element Definitions. For example, we may define value {call} or value {sms} in the Purpose element together with the Date element to restrict a call being placed or sms being sent to the subscriber within a certain restricted time period. We now illustrate the functionality of MLPP through the use of a simple business-related example.

```
<MLPP ver="1.0.0" resides="Locally">
    <Owner type="MSISDN">27831234567</Owner>
        <Guard>
            <Spatial></Spatial>
            <Temporal>
                <Every>
                    <Day dow="Saturday">
                        <StartTime>000000</StartTime>
                        <StopTime>240000</StopTime>
                    </Day>
                    <Day dow="Sunday">
                        <StartTime>000000</StartTime>
                        <StopTime>240000</StopTime>
                    </Day>
                </Every>
            </Temporal>
            <Identity>
                <Owner type="MSISDN">
                    27831239999
                </Owner>
                <Owner type="MSISDN">
                    27831237777
                </Owner>
            </Identity>
            <Purpose>Location</Purpose>
        </Guard>
</MLPP>
```

Figure 8-13 Example illustrating Location Privacy Policy for weekend restriction

As is generally the case, employees of a business would not like fellow colleagues to know their location over weekends. The following MLPP demonstrates the necessary defined elements in order achieve privacy requirement of this nature (Figure 8-13).

With regard to Spatial Guard, the location would have to be calculated to determine whether location information can be returned to the requesting source or not based on positioning within a location domain. Although not ideal, Spatial Guards' relative benefit is immense and it is recommended for use. Additional restrictions, which may accompany Spatial Guard, might eliminate the necessity to calculate location in order to enforce the Spatial Guard.

8.9 Securely Communicating Location Information

Within this modelled approach it is imperative that once the location is determined locally, it is securely communicated to the requesting source. We introduce the concept of Position over IP and Direct MS-to-MS Positioning (Figure 8-14 and 8-15 respectively), using the secure Over The Air (OTA) approach as described in [chapter 7]. Depending on the source requesting the location information the Security Sheet (SS) may be adapted accordingly to acquire the desired level of security.

Position over IP refers to making use of the underlying GSM-GPRS network for the communicating of multiple location information to the requesting source, this typically occurs when beacons are used for the supplying of location information.

Direct MS-to-MS Positioning refers to the communicating of multiple location information via a peer-to-peer connection, this typically occurs when the Mobile Stations (MSs) couple as virtual Base Transceiver Stations (vBTSs).

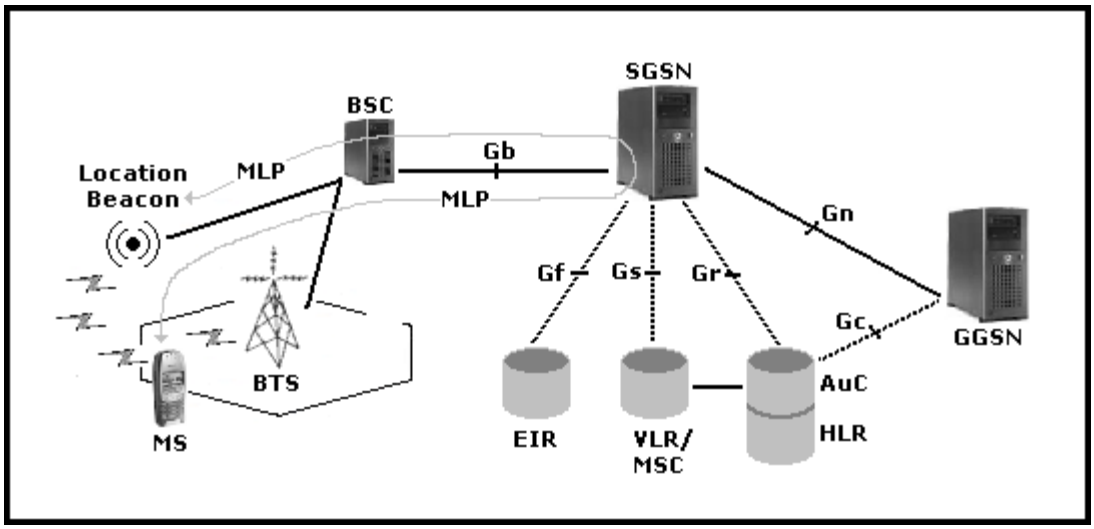

Figure 8-14 Position over IP from location beacon to MS

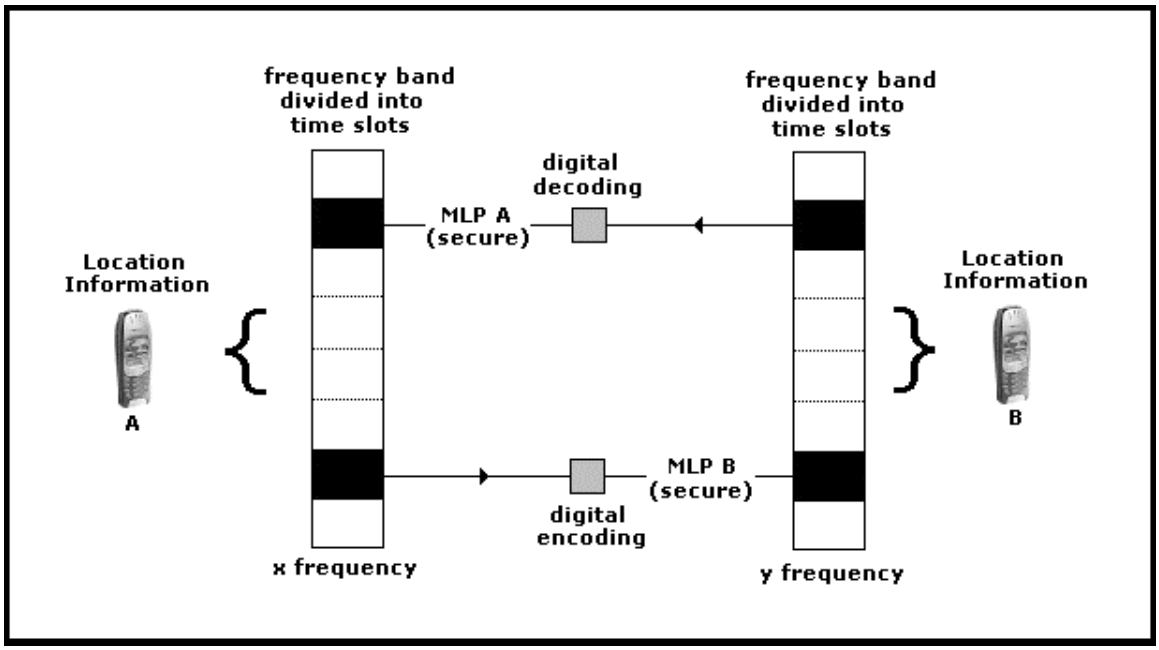

Figure 8-15 Direct MS-to-MS Location communication while adhering to MLPP constraints

8.10 Location History Records

Historical location records are kept within the boundaries of a secure Location History Server and show a subscriber's movement patterns over time. The existence of these location records requires the consent of the subscriber or if a warrant for these location records is presented

by law enforcement personnel. The MLPP caters for the setting of storage of any location determined by the iMS for future use. Again for security purposes, the location information while in transit may be secured using the secure OTA XML approach.

8.11 Location Server and Access Control

Finally, once location has been accurately determined and communicated with a residing network Location Server, it will be used in the determination of access to a restricted resource. In this chapter, the subscriber requests access to a resource based on position alone. The Location server may communicate with the HLR or alternatively with a third party AAA Server in determining Access. An Access response is then communicated to the client and a secure client-to-resource communication channel is established.

8.12 Conclusion

In this chapter we provided a secure approach to location-aware mobile access control or rather simply security by position within the GSM-GPRS infrastructure. Assumptions made included intelligent Mobile Stations (iMSs) capable of self-location determination as 3D coordinates. We incorporated Mobile Location Protocol (MLP) as an accurate location representation. A Mobile Location Privacy Policy (MLPP) was applied to the MLP in order to restrict certain location determination requests. These requests were based on Spatial, Temporal, Identity and Purpose arguments. Secure location communication was for the purpose of access to a protected resource on the basis of position.

In the next chapter we propose models for the integration of WLAN and GSM-GPRS infrastructures while incorporating access by position concepts presented in this chapter.

Chapter 9

9. SYSTEM FOR WIRELESS AND ROAMING MOBILITY (SWARM) - MODELS FOR THE INTEGRATION OF GSM AND WLAN

9.1 Introduction to the System for Wireless and Roaming Mobility

The benefits of both GSM and WLAN have been highlighted in [chapter 6]. An improved Location-Based positioning model has also been described in [chapter 8]. This chapter serves to describe two models for the integration of GSM and WLAN into one new complementary infrastructure (see Figure 9-1), which for our purposes will be known as the System for Wireless and Roaming Mobility or SWARM. Both of the associated benefits of each technology are incorporated.

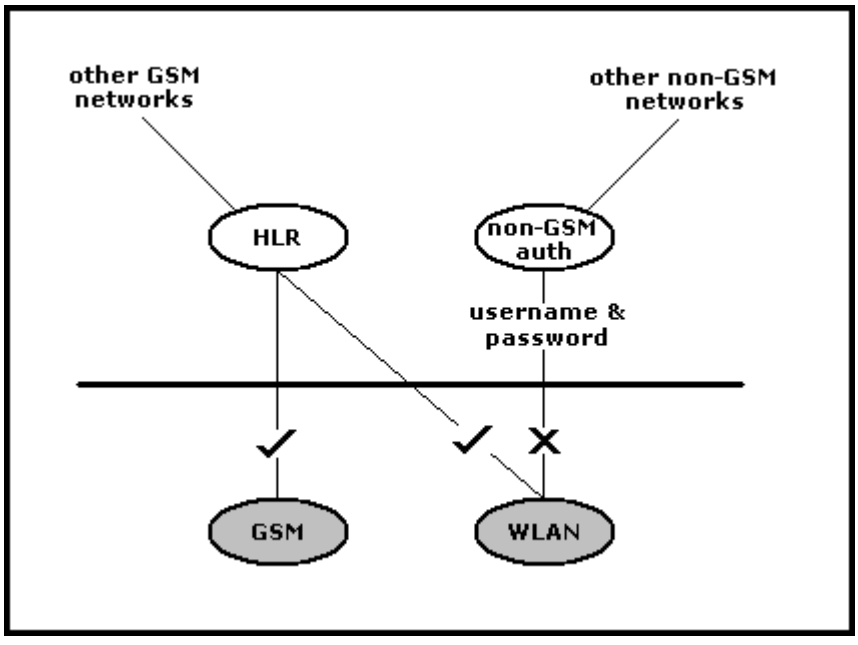

Figure 9-1 Combination of GSM and WLAN infrastructures

The benefits are taken from each wireless technology.
GSM benefits include among others, the following:

- User authentication and authorization
- Centralized billing capabilities
- Roaming capabilities
- Handover capabilities
- Location determination capabilities

WLAN on the other hand has only one major recognizable benefit, namely:

- High speed data access

The SWARM models will cover the basic needs of a wireless user requiring a secure high speed data connection coupled with seamless roaming capabilities and the billing thereof joined to one subscriber account.

It is important to note that in order to achieve WLAN speeds from a WLAN subscriber over one or many links between network nodes to a desired host, all involved links and node elements must comply with WLAN speeds. This can be expressed using the following equation illustrated in Figure 9-2:

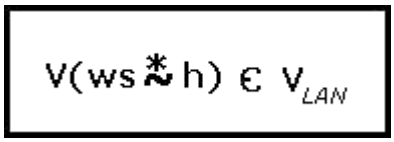

Figure 9-2 Equation for the requirement and upkeep of data transmission speeds

where the Speed (V) of a WLAN subscriber (ws) over one (~) or many (*) links to a desired host (h) is an element of a speed in the LAN range of speeds denoted by LAN (V_{LAN}). To better understand how we get to the equation in Figure 9-2 we use the following:

Suppose e_1 and e_2 are directly connected.
Let $V(e_1 \sim e_2)$ represent the speed over the link e_1 and e_2.

If e_1 is directly connected to e_2, which in turn is directly connected to e_3, then let $V(e_1 \sim e_2 \sim e_3) = \min(V(e_1 \sim e_2) , V(e_2 \sim e_3))$
where $\min(V(e_1 \sim e_2) , V(e_2 \sim e_3))$ represents the speed of the lower of the two links.

Hence for n connected elements (e_n),
$V(e_1 \sim e_2 \ldots e_{n-1} \sim e_n) = \min(V(e_1 \sim e_2) , \ldots , V(e_{n-1} \sim e_n))$

We choose to abbreviate $V(e_1 \sim e_2 \ldots e_{n-1} \sim e_n)$ as follows:
$V(e_1 \overset{*}{\sim} e_n)$

For our purposes e_1 represents the WLAN subscriber (ws) and e_n the desired destination or host (h)

Therefore,
$V(ws \overset{*}{\sim} h) = \min(V(e_1 \sim e_2), \ldots, V(e_{n-1} \sim e_n))$

Or alternatively
$V(ws \overset{*}{\sim} h) \varepsilon V_{LAN}$

Throughout this chapter we make the assumption that the underlying GSM-GPRS network will provide for WLAN data speeds; how this will be achieved is out of the scope of this chapter.

In the remainder of this chapter we will focus our attention on the most obvious and current evolutionary technologies that provide for WLAN data speeds by making use of a Mobile Network, namely EV-DO. We investigate Authentication and Security, Roaming and Handover and the benefits and disadvantages of EV-DO. Due to its costly nature, we propose two cost-effective models for integrated GSM and WLAN systems that imitate EV-DO functionality. Once again we will delve into the authentication process of a GSM-WLAN roaming device to a Wireless LAN. We also cover how security concerns within a WLAN can be eliminated by using each model. We will cover the concept of roaming and the billing of a roaming user to one central account. Location determination as a 3-Dimensional region that enforces security by position will feature in the implementation of each model.

9.2 High Rate Packet Data Air Interface Specification (EV-DO)

Currently GSM air interface is not optimized for data services, however future mobile networks will require optimization and redesign for high rate packet data services.

3G or "third-generation" networks have been designed with this in mind. Unlike GSM, 3G networks make use of Code Division Multiple Access (CDMA) digital system [Cdm]. CMDA, like WLAN, uses spread spectrum technology. Two or more coding schemes, for example Code Division Multiple Access 2000 (cdma2000) [Gar] and Wideband Code Division Multiple Access (WCDMA) [Pra], are being pursued, and have

been built to optimize voice traffic on 3G networks. It is well known that voice and data have very different requirements in terms of latency and transmission loss. For data service, 3GPP2 [3gp] has recently developed and standardized cdma2000 1xEV-DO [Evd] (High Rate packet Data Air Interface Specification) also known as TIA/EIA IS-856 or Evolution Data Only. As an added benefit, 1xEV-DO does not utilize any Mobile Switching Centre (MSC) resources [Qua].

Each Base Transceiver Station (BTS) will integrate 1.25 MHz frequency carriers, which can be used for voice or data services. This effectively means that a Base Transceiver Station (BTS) cell coverage area is the same for both voice and data services (1xEV). Each 1xEV-DO sector is capable of reaching peak rates of 2.4 Mbps on the forward link (downlink – from BTS to MS) and 153.6 Kbps on the reverse link (uplink – from MS to BTS). A 2.4 Mbps data channel is now available and must be shared among all users on a cell sector. Bandwidth in 1xEV is intelligently scheduled to maximize throughput for everyone thus not limiting specific users. The cell site uses a sophisticated scheduling algorithm that tracks the modem's average receive signal strength from millisecond to millisecond and takes advantage of local peaks in the signal conditions to send packets when they are most likely to get through. That way, bandwidth is not wasted on packets that will likely have to be retransmitted anyway, and one user with a bad connection hogging resources with retransmits will not cause a slow down of service for everyone else.

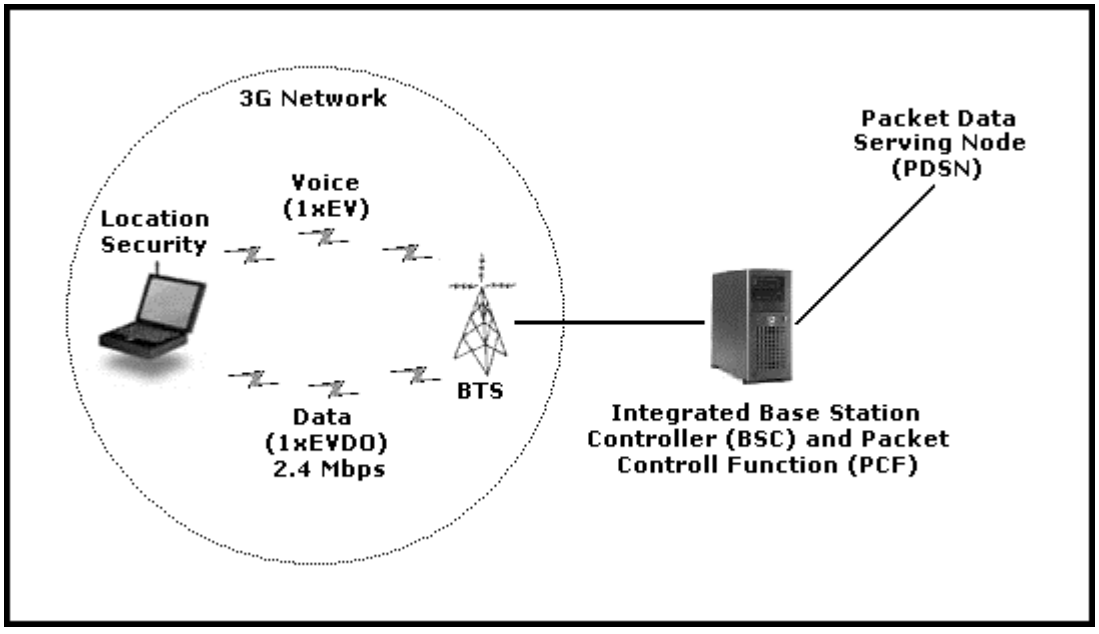

Figure 9-3 1xEV 1xEV-DO architecture

9.2.1 Authentication and Security

1xEV uses Diffie-Hellman public key cryptography to authenticate the connection but does not encrypt the actual traffic. This means that the connection will be hard to hijack but data transmission will occur in the clear. Therefore, it is recommended that subscribers make use of an end-to-end encryption scheme like Internet Protocol Security (IPSec) or a Virtual Private Network (VPN) to keep transmissions secure. 1xEV systems use standard IP networking hardware. Like in GPRS, the allocation of the address can be static or dynamic and are usually allocated using a Remote Authentication Dial in User Service (RADIUS) or Dynamic Host Configuration Protocol (DHCP) server. For further details on 1xEV and 1xEV-DO technologies refer to [Est].

9.2.2 Roaming and Handover

Roaming and handover in 3G networks is based on current GSM-GPRS techniques [chapter 2.6 and 2.7].

9.2.3 Advantages and Disadvantages

High-speed data transfers are achievable entirely on the mobile telecommunications network. However, in order to make use of 1x EV and or 1xEV-DO, major upgrades of network hardware (BTS) and software is required. In order to achieve high data rates, Mobile Stations (MSs) and PC cards modems would also require upgrading. This effectively means an upgrade from GSM (2^{nd} generation network) to UMTS (3^{rd} generation network). The cost implications are immense and can be considered to be too expensive for the return on investment for most GSM network operators worldwide. Spectrum shortage may occur as many users will have to be accommodated at high speeds, having more users will have an adverse effect on transmission rates.

One major benefit is that there is no need for the integration of WLAN or any other infrastructure. Billing, security and roaming functionalities remain 3G network core components.

Very few networks have to date implemented "third-generation" networks due mainly to licensing and implementation costs. As is

common in any industry these costs are directly forwarded onto the consumer.

We now propose two alternative cost-effective workarounds in achieving fast data speeds by integrating existing infrastructures for maximum benefit.

Before we look into the different aspects and processes that surround SWARM let us proceed with an overview of the architectures of the respective models. It is important to note that SWARM incorporates GSM and its packet-switched extension GPRS and makes provisions for future packet-switched advances. We will also make use of 802.11b (Wi-Fi) as the preferred WLAN standard. IEEE 802.16 (WiMAX) may also be used for the interconnecting of WLANs but are out of the scope of this chapter [chapter 5.10].

9.3 SWARM 1 - Architecture

Conceptually this model can be seen as an extension to the radio link layer of an existing GSM-GPRS network. It is concerned with the updating of the communication link between the Mobile Station (MS) and the Base Station Transceiver (BTS).

GSM-GPRS will provide for authentication of a subscriber, session and mobility management, roaming and the billing of a subscriber to one account. The GPRS backbone will provide the platform for the access to Packet Data Networks (PDNs).

9.3.1 Approach to Achieving WLAN Data Rates in SWARM 1

This approach involves the updating of the GSM infrastructure. SWARM 1 involves the integration of WLAN and GSM-GPRS at a radio link layer. We recall from [chapter 5.3.2] that a WLANs Distribution System (DS) can constitute any fully integrated inter-connecting communications system. Our inter-connecting communications system in this case is GSM.

We provide for the adding of a WLAN Access Point (AP) as an extension to an existing Base Station Transceiver (BTS) (refer to Figure 9-4). Essentially this would only occur at the BTSs in Urban areas, those areas indicative to public access for example airport

terminals, coffee shops and business access, for example pico cells in an office park or building.

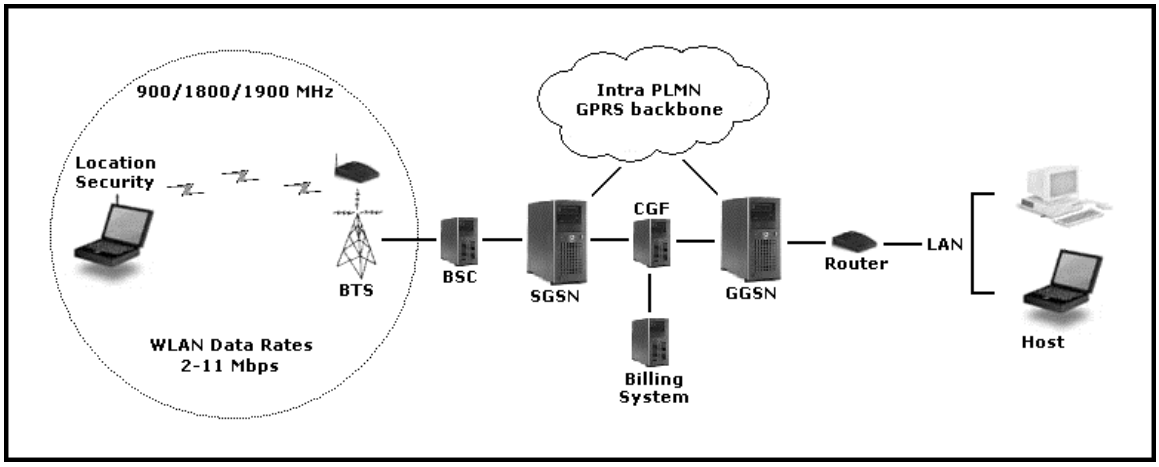

Figure 9-4 The SWARM 1 architecture

The mobile device used will be fully GSM compliant including an embedded GSM Subscriber Information Module (SIM) and have a Wi-Fi enabled PCMCIA or PCI card.

Let us take a look at the radio link layer, Base Station Controller (BSC) and Packet Control Function (PCF) architectural changes that SWARM 1 includes (Figure 9-5).

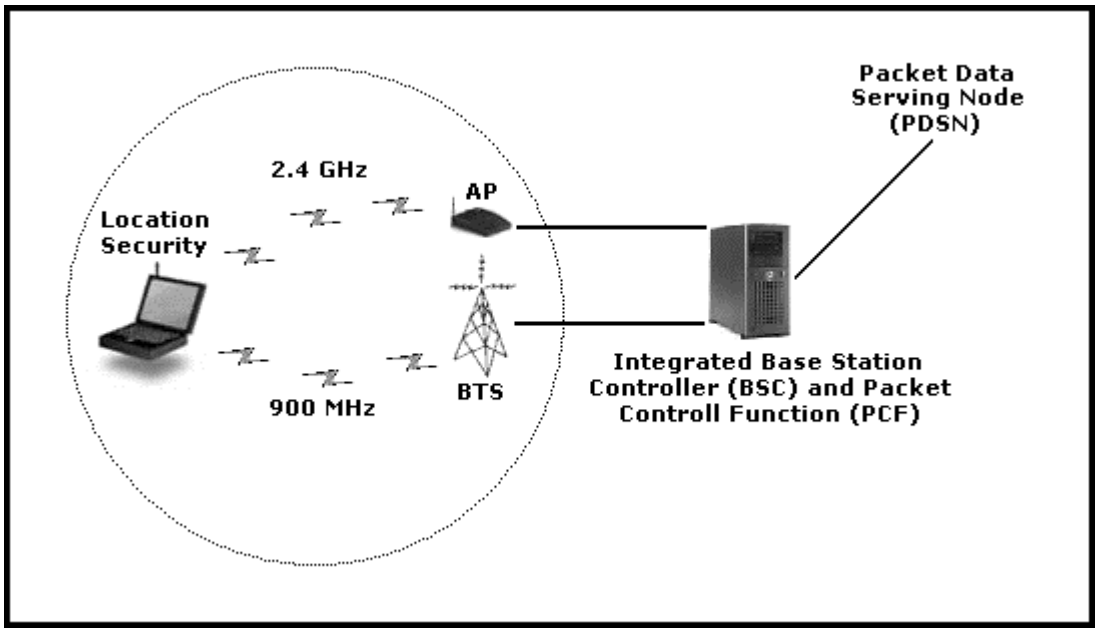

Figure 9-5 SWARM 1 radio link layer and BSC architecture

A GSM-WLAN subscriber would have the prowess of achieving WLAN data rates on a GSM-GPRS network using this approach. The Access Point (AP) would be an off-the-shelf Wi-Fi compliant access device. The Base Station Controller (BSC) will need to be integrated with a Packet Control Function (PCF) thus eliminating the need for updating the Mobile Switching Centre (MSC) or the Serving GPRS Support Node (SGSN). Modulated frequencies arriving at the BSC will vary (900 MHz in the GSM-GPRS case and 2.4 GHz in the WLAN case). Frequency multiplexing will be a requirement at the BSC/PCF. The Packet Data Serving Node (PDSN), in this case, illustrated in Figure 9-5 constitutes the additional packet-switched GPRS network nodes [chapter 4.2.1 and 4.2.2].

We recall from [chapter 4.3] that the Mobile Station (MS) must apply for one or more addresses used in the Packet Data Network (PDN). This address is called a Packet Data Protocol (PDP) address. The allocation of a PDP address can be static or dynamic and can be allocated in one of the following ways:

- GGSN Address Pools
- Home Location Register (HLR)
- Remote Authentication Dial in User Service (RADIUS) server
- Dynamic Host Configuration Protocol (DHCP) server

Allocation of an IP Address for WLAN access will evidently be assigned to a subscriber in the same manner as GPRS address allocation takes place. Ideally for a business orientated subscriber, the HLR may contain the static IP Address for the user or alternatively an IP Address will be allocated from the corporates address pool.

We also remember from [chapter 4.3] that A PDP context describes requirements of the connection to the packet networks, where a PDP context consists of the following:

- PDP Type
- Network Address (IP Address)
- Requested Quality of Service (QoS)
- Access Point Name (APN)

For our purpose we choose to incorporate address allocation (PDP address) and connection requirements to a network (PDP context) from GSM-GPRS.

9.3.2 Authentication and Security

The SIM card will be used to authenticate the subscriber to the GSM-GPRS and WLAN network.

We recall from [chapter 5.7] that there are three basic methods to secure access to a WLAN Access Point (AP):

- Service Set Identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

Access Points (APs), like BTSs, are considered public access points to subscribers to the GSM-GPRS network. Therefore, security by Service Set Identifier (SSID) and Media Access Control (MAC) address filtering will not be a recommended option as stringent control and management procedures will need to be implemented for what can be essentially seen as a public service. For a secure connection between the GSM-GPRS-WLAN enabled subscriber and the Access Point (AP), Wired Equivalent Privacy (WEP) must be implemented until such time that later security releases of IEEE 802.11 are introduced into the market (802.11i). The subscriber's authentication key (Ki) [chapter 2.3.1], which is a unique identifier and forms the basis of the GSM-GPRS security protocol, will be used to create a 128-bit Session Key or "secret key" shared between the subscriber and the Access Point (AP). This is achieved using the algorithm COMP128 [chapter 2.4.5] or some similar algorithm. For our purposes this 128-bit encryption key will be known as Wc and COMP128 is its generation algorithm (Figure 9-6).

Figure 9-6 Session Key for WLAN access (Wc) from COMP128 algorithm

From Figure 9-7 we observe that WLAN authentication occurs in exactly the manner that normal GSM-GPRS authentication takes place. If the Response SRES(MS) to the Random challenge (RAND) is equal to the response from the Authentication Centre SRES(AuC), authentication is successful and the mobile subscriber is allowed to use the GSM-GPRS network services. We provision an additional 128-bit

key (Wc), which is the output generated by the COMP128 algorithm with inputs RAND (128-bit) and Ki (128-bit), to be used as the shared secret key between the WLAN subscriber and the Access Point (AP). Wc, the WLAN Session key, will be used for the purpose of encrypting the WLAN session by making use of the Wired Equivalent Privacy (WEP). Although WEP, which either makes use of no encryption, 40-bit encryption or 128-bit encryption, with this approach WEP will by default make use of 128-bit encryption.

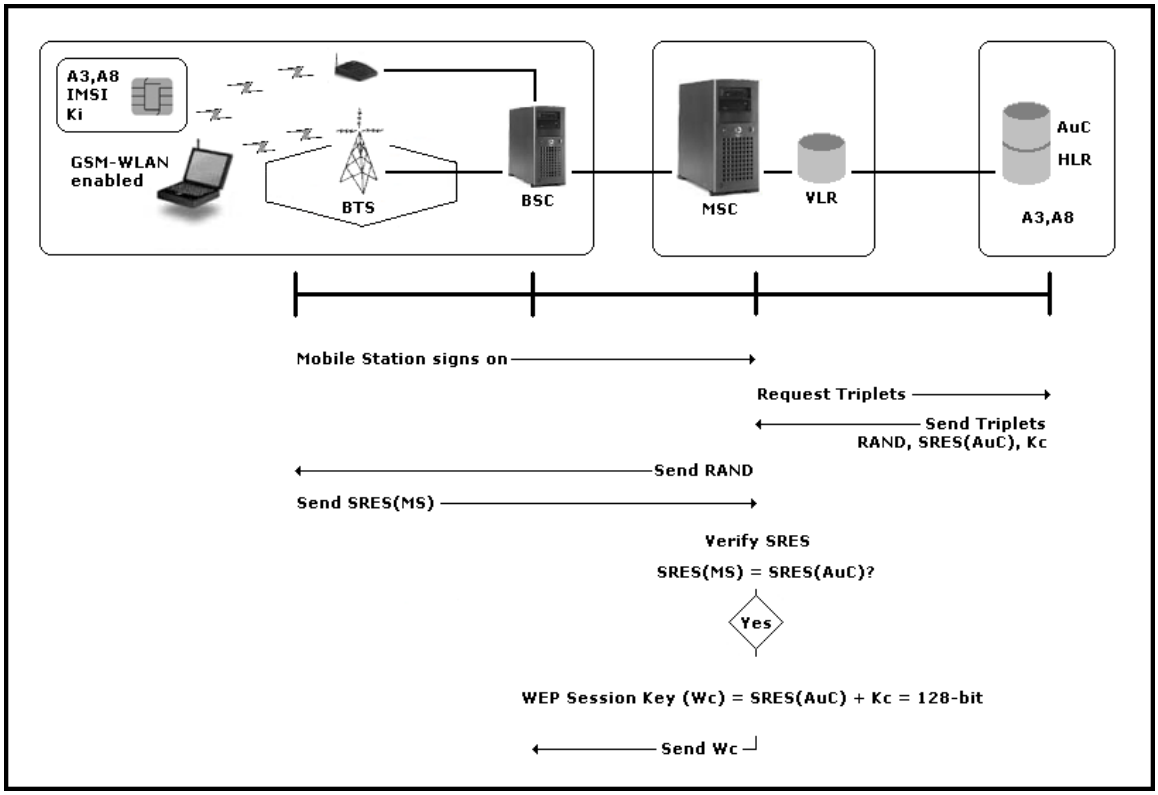

Figure 9-7 Authentication process and Session key creation for SWARM1

A further security implementation shall include the regeneration of the WLAN Session key (Wc) based on a time period of use (network operator determined). A new Session key (Wc) is created for each WLAN authentication attempt. Alternatively a new Session key (Wc) is created when the Mobile Station (MS) is required to re-authenticate itself to the GSM network. The interval for re-authentication request by the GSM network on the Mobile Station (MS) is dependant on the current network load. If the network load is large, the re-authentication request frequency may be in the region of a couple of minutes. Therefore, the Session key (Wc) creation process may occur

independently or depend on the GSM-GPRS frequency of the authentication and re-authentication process.

The subscriber's profile (stored on the Home Location Register (HLR)) would require updating with entries specifying access rights to particular WLANs if a higher level of security implementation is required. This may be a necessity if a public Access Point (AP) is used for the entry to a corporate WLAN, resulting in an increase of control and management procedures to maintain the user profiles of this nature.

A dual mode of operation would allow the subscriber to simultaneously transfer data using WLAN while still making use of GSM resources for example voice service or Short Message Service (SMS).

9.3.3 Roaming and Handover

Handover between GPRS and WLAN conceptually can be best described by the following example. Take subscriber John who has a GSM-GRPS WLAN enabled device and is connected via GPRS to the Internet and is in the process of downloading an MP3 music file. John is on foot and walks within range of a WLAN Access Point (AP) linked to his serving GSM-GPRS network. A combination of location positioning, signal strength, John's profile and the fact that John has an active GPRS session forces the establishment of a WLAN session. The current state of the GPRS session is handed over to the WLAN session and John's MP3 file is downloaded continuously (now at a faster data transfer rate) without John initially being aware of the handover. John ideally would have been informed by positioning information, where his nearest WLAN AP was at the start of his GPRS session.

Handover may also be performed between various Access Points (APs) if they service a common area. WLAN handover will conceptually be performed as and when it occurs within a GSM network. Handovers [chapter 2.6] are network controlled, mobile assisted or mobile controlled. In the WLAN case, handover would occur from one AP to another within range in the event of one of the following:

- Forced network handover due to lack of resources at a particular AP
- A reduction in signal strength would force a mobile-assisted handover
- A WLAN subscriber requests a handover for a particular reason, i.e. higher data transfer rates available at another AP

Roaming would occur as it does currently in GSM [chapter 2.7]. It is important to note that the roaming network ideally would support GPRS and must unquestionably support WLAN access. A "Roaming Agreement" would be required to exist between the home and roaming network for access and correct billing to take place. Billing will take place using TAP records as described in [chapter 2.8].

9.3.4 Advantages and Disadvantages

This solution combines the flexibility, security and seamless integration of GSM-GPRS and WLAN and there are some additional advantages. Technologies like EDGE [chapter 4.6] and WiMAX [chapter 5.10] are technologies that could expand the benefits of this approach.

Handover from GSM-GPRS to WLAN and vice versa is a definite and probable occurrence allowing for continuous data transfers occurring on the one infrastructure and then the other, while all the time appearing seamless to the subscriber. This would provide subscribers with an environment where certain geographical areas become known as fast data transfer regions or "hot spots". The problem of providing limited access exists due to the fact that the extended range of the BTS and the AP are very different, the AP range being a lot smaller [chapter 6.6]. A high density of APs is required for handover to take place, in other words access areas provided by APs would need to overlap for handover between APs to take place. Due to density requirements of APs for effective handover, if a subscriber is travelling at vehicular speeds handover between APs will in all likelihood be highly improbable.

The most obvious drawback is that some urban Base Transceiver Stations (BTSs) will require an AP installation and the Base Station Controller (BSC) will require a change to accommodate the handling, controlling and management of the WLAN 2.4 GHz frequency band. In order for this to take place frequency multiplexing is a requirement. User profiling adaptations can be implemented depending on user

requirements. Further security concerns and packet loss mechanisms may need to be addressed with this approach. Frequency interference must be considered a very real threat.

Subscribers will require a GSM-WLAN compliant mobile device.

The need for the upgrade of the GSM-GRPS network to a "third-generation" or 3G network is eliminated as data rates provided are now comparable to those of 3G networks. However, the GSM-GPRS standards will require adaptation to accommodate SWARM 1.

9.4 SWARM 2 – Architecture

This model provides for the integration of GSM-GPRS and WLAN technologies, incorporating the best of both worlds, but still seeing them as separate entities.

GSM-GPRS will provide for authentication of a subscriber, session and mobility management, roaming and the billing of a subscriber to one account. The WLAN will provide the platform to access Packet Data Networks (PDNs).

9.4.1 Approach to Achieving WLAN Data Rates in SWARM 2

We introduce two new network nodes, namely the Roaming Provider (RP) and the Roaming Data Profiler (RDP) (refer to Figure 9-8). These nodes will act as middleware in the connection of the GSM-GPRS network and a WLAN. Let us take a closer look at the Roaming Provider (RP) and the Roaming Data Profiler (RDP).

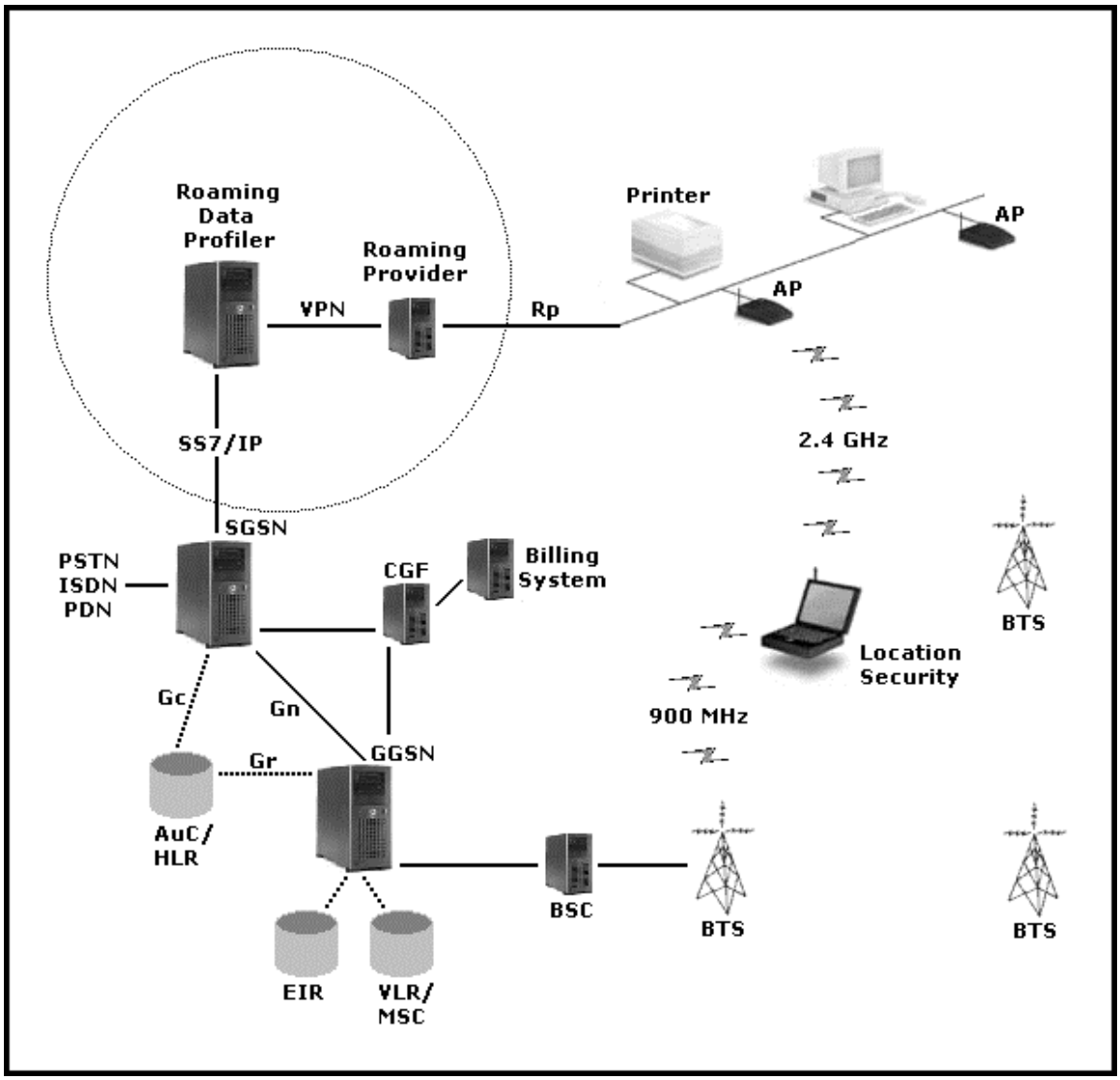

Figure 9-8 The SWARM 2 architecture

9.4.1.1 Roaming Provider (RP)

The Roaming Provider (RP) acts as a common node between multiple WLANs and the networks backbone. The RP manages one or many WLANs. It is a connection between the WLAN resources and the Roaming Data Profiler. Its main responsibilities include management of the WLAN communication channels, handover and mobility management. The Roaming Provider (RP) functionally sits at the same architectural level as the Base Station Control (BSC) in the GSM-GPRS network as it acts as the controller of the communications channels. The Roaming Provider (RP) exchanges authentication and billing

information with the GSM-GPRS network. It may also control access to another IP network through the GSM-GPRS network. For example, if subscriber John connects to, and is authenticated on, the WLAN for the sole purpose of viewing a web page, yet the WLAN he is connected to has no Internet connectivity, he may make use of the Internet connection through GPRS from the WLAN.

The WLAN in this scenario is considered to be secure and therefore the security thereof is not considered in this chapter. In order to protect the link between the two nodes and between the Roaming Provider (RP) and the external WLAN, it is recommended that an end-to-end encryption scheme (a Virtual Private Network (VPN)) be used to keep transmissions secure.

9.4.1.2 Roaming Data Profiler (RDP)

The Roaming Data Profiler (RDP) contains permanent and temporary data for all registered WLAN users. Permanent data would include the user's profile while temporary data would include, for example, the current location of a user. The Roaming Data Profiler (RDP) functionally sits at the same architectural level as the Home Location Register (HLR) and Mobile Switching Centre (MSC) in the GSM-GPRS network. Responsibilities include subscriber state maintenance, account handling as well as Access Point (AP) to WLAN user location determination and optimization. Handovers from one AP to another within the same WLAN will be controlled by the WLAN, reflected to the Roaming Provider (RP) and updated on the Roaming Data Profiler (RDP). Handovers between WLAN, which may result in another Roaming Provider (RP) being used, will be controlled by the Roaming Data Profiler (RDP).

The Roaming Data Profiler (RDP) connects to the GSM network via an Interface to the Gateway Mobile Switching Centre (GMSC) or alternatively to the GSM-GPRS network via an Interface to the Gateway GPRS Support Node (GGSN). This connection may occur over the SS7 network or over an IP link. The security, Interface and connection implementation is out of the scope of this chapter.

9.4.1.3 Authentication and Security

The Subscriber Information Module (SIM) card will be used to authenticate the subscriber to the GSM-GPRS and WLAN network.
The Authentication process used is exactly that used to verify a subscriber in a GSM network [chapter 2.3.4]. The only difference is that the SRES (AuC) is sent to the RDP and shall be known as the expected SRES (eSRES). If this expected response eSRES is equal to the SRES returned by the GSM-enabled device to the RAND challenge it was presented by the network, then the wireless device is authenticated to the WLAN.

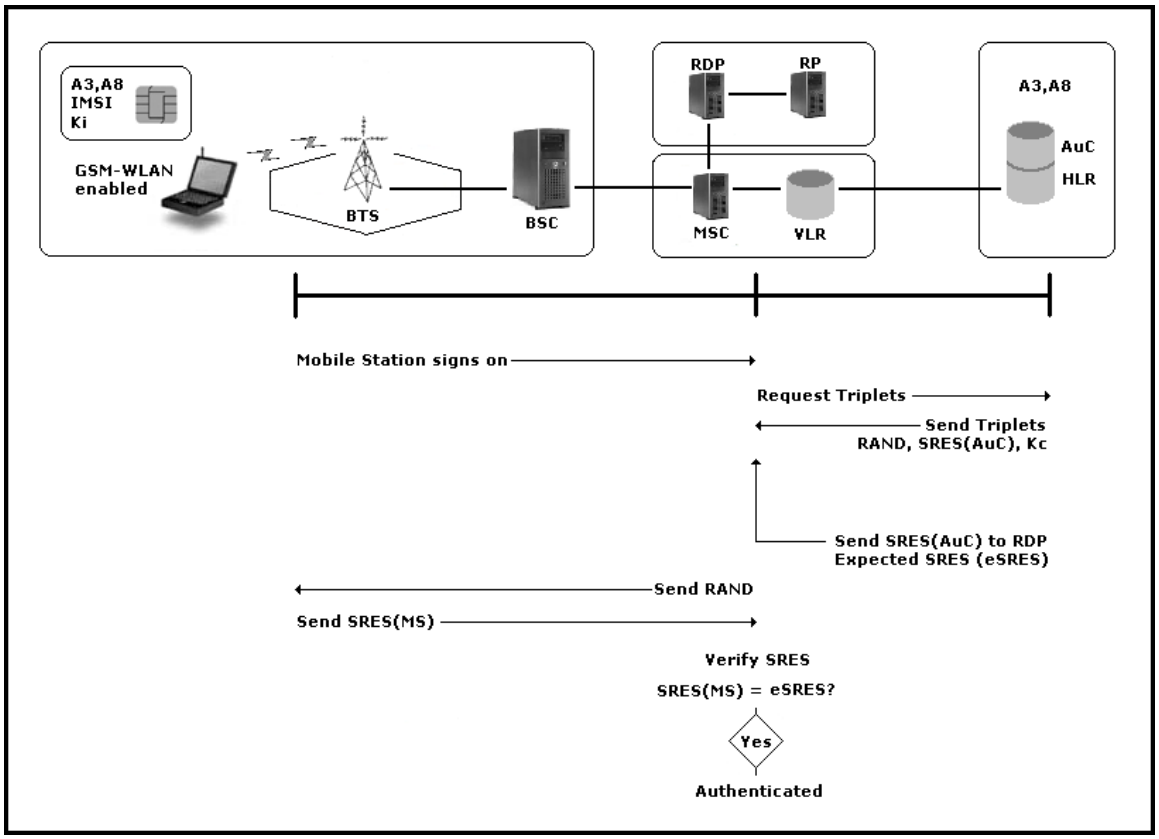

Figure 9-9 Authentication process in SWARM 2 architecture

In this approach, unlike the SWARM 1, we will not make use of SRES (AuC) and Kc as the WEP Session key. Although this may be possible in SWARM 2 we choose not to make use of any keys generated by the GSM-GPRS network for reasons of simplicity. This is a merger of the two infrastructures thus the generation and communication of WLAN session keys will be handled as per normal by the WLAN.

9.4.2 Roaming and Handover

Handover from GSM-GPRS to WLAN and vice versa will be a definite and probable occurrence allowing for continuous data transfers occurring on the one infrastructure and then the other, while appearing seamless to the subscriber. The Roaming Data Profiler (RDP) will be responsible for maintaining data transfer state and transferring state between WLAN and GPRS if required.

9.4.3 Advantages and Disadvantages

The WLAN and GSM-GPRS infrastructures will only be slightly affected due to the addition of compatible interactive connecting nodes (Roaming Provider and Roaming Data Profiler). These elements can be added as an extension to the GSM network. With this approach, an existing WLAN can be added with relative ease to an existing GSM-GPRS network. The WLAN's positioning does not necessarily need to be placed within the realm of the GSM network. The WLAN may leverage off the underlying GPRS network if need be.

For subscribers, connectivity and billing will be transparent. The Interface between the Roaming Data Profiler whether it is using SS7 or IP as carrier, will need to conform to GSM-GPRS network standards. The Roaming Provider will require a secure Interface to WLAN infrastructures. Security at the WLAN level will be left up to the discretion of the WLAN itself, however it is recommended that 128-bit encryption on the wireless communication is used (WEP).

9.5 The Coexistence of SWARM Models

Although the two models presented in this chapter are seen as independent entities it is important to note that SWARM 1 and SWARM 2 may coexist within the same environment. This distinction may occur due to the need for separation of public and corporate market spaces. SWARM 2 may exist entirely as a corporate entity while SWARM 1 may exist as a public entity. Refer to Figure 9-10.

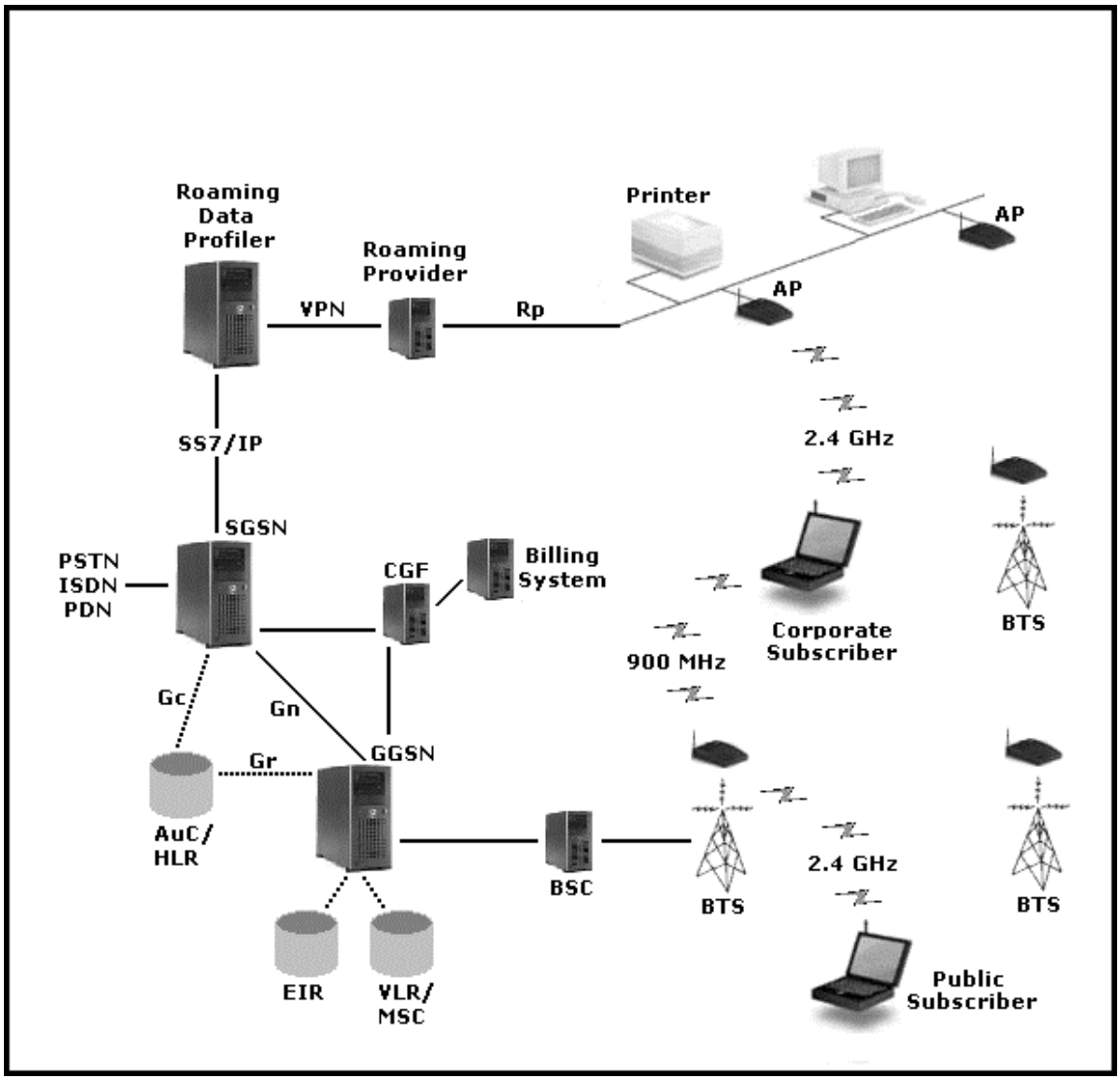

Figure 9-10 The Coexistence of SWARM

By adopting a coexistence SWARM approach we truly can achieve an "always on" fast data access vision with roaming and handover capabilities.

9.6 Security by Position

Location-Based techniques have been covered in [chapter 3] and in [chapter 8] a GSM 3-Dimensional spatial positioning model was proposed. [chapter 7] provides a means for the distribution of sensitive location information Over The Air while minimizing the

inherent overhead the securing of information brings. Security by position is now an easily determined and secure redistributable option.

Security by position is a concept introduced as a Valued Added Service (VAS) that can complement both the SWARM 1 and SWARM 2 models. As WLAN security measures are not extensive, security by position can become the core security mechanism in the integration of WLAN and GSM-GPRS. Both non-GSM and GSM nodes may be used in providing an accurate 3-D coordination reference with a small uncertainty region.

Access only by position provides for a security means that is extremely difficult to imitate as your position becomes a unique identifier. This is evident through the laws of physics as two objects with mass cannot occupy the same space at the same instant in time. This security feature will be particularly useful in a business environment where access to a corporate WLAN can be confined to one or more pico cells (or Base Station Transceivers) within an office building space. If location determination is an accurate 3-D spatial representation (with one meter uncertainty ellipsoid) of the actual position of the subscriber, security by position has immense value add for fixing access permissions rights for a subscriber via their location. In determining the 3-D coordinates of John's position both GSM and non-GSM entities (nodes) may be communicated with in John's location determination. The Access Point (AP) might restrict access to the WLAN based on positioning rules allowing certain mobile subscriber's access to the WLAN. In addition to this, access to a WLAN may be enforced by the subscriber's position only. [Dur] introduces the concept of location domains as service regions.

For example, take business subscriber John who works in office block with WLAN access perimeters. John has WLAN Internet access throughout the office block (A block, B block, C block) and can only connect to his corporate WLAN if he is situated within the access perimeter of his employer's building (C block), refer to Figure 9-11.

John may roam between WLANs by connecting to different Access Points (APs) situated throughout the office block. As John moves between the different blocks, handover between Access Points (APs) will be controlled by the underlying GSM-GPRS network if access regions intersect (C intersects A and B), see Figure 9-11.

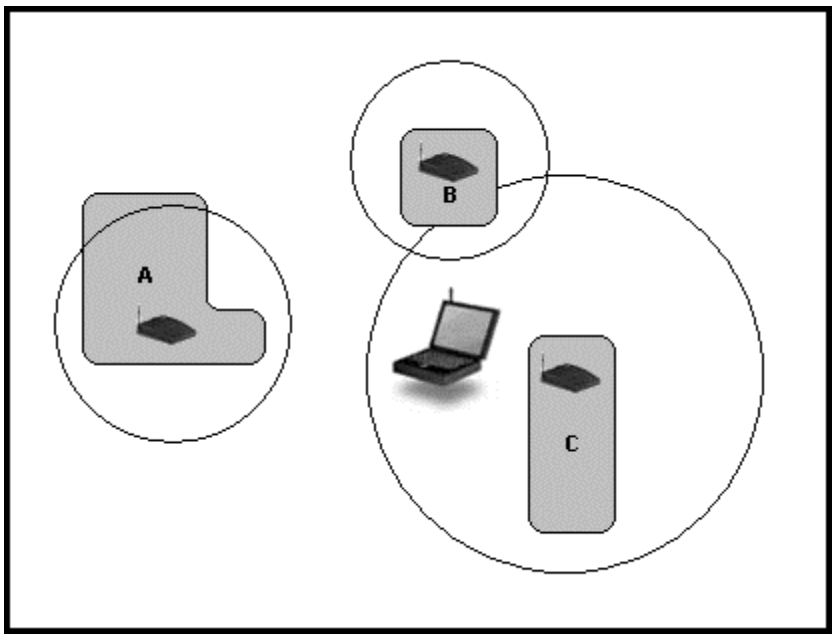

Figure 9-11 Example of inter office block roaming and security by position

If John moves out of the range of the office blocks, his WLAN access will be discontinued and his subscriber profile and status will be updated on the underlying network. If accuracy in positioning allows, John's access may be restricted to something similar to access to the corporate WLAN from only within his particular working floor or even access from only his office. John may or may not be aware that his exact location is known by the underlying network. Ideally John would own his location information and upon his discretion he would make known his exact location to the underlying network and or any other entity requesting his location information.

9.7 Conclusion

In this chapter we presented two different models for the integration of GSM-GPRS and WLAN infrastructures. Both models required for the updating of the original infrastructures, however they provide the mobile subscriber with wireless data access at WLAN speeds. The advantages and disadvantages of each model were discussed. The solutions integrate security, mobility management and a billing mechanism for the provision of allowing mobile subscribers the ability for WLAN connectivity. The concept of access by position was introduced as a security measure for entry to a WLAN and or GSM-GPRS network.

Chapter 10

10. CONCLUSION

This dissertation has examined mobile subscriber authentication and broader issues of wireless communications, information security and location information exchange in wireless networks.

Detailed overviews of various wireless technologies were supplied [chapter 2- 5] after which GSM-GPRS and WLAN were investigated and compared [chapter 6]. A Model was presented for the securing of content Over The Air [chapter 7] forming the basis for a secure, location-aware mobile access control or an access by position approach [chapter 8]. Models for the integration of WLAN and GSM-GPRS infrastructures finally illustrated that the need for increased data rates, while still maintaining an acceptable degree of security, is indeed achievable through integration by combining the strengths of each technology [chapter 9].

In brief, we compared wireless technologies, built novel security enhancements around these technologies and finally integrated these improvements and existing benefits of each technology into a cost-effective, flexible, high-speed mobile wireless communications environment.

We have thus achieved our original objective identified in our problem statement of providing a modelled representation of a truly secure, integrated yet flexible high-speed mobile wireless communications environment that is operationally cost effective for network operators while fulfilling subscribers' wireless communication needs of a single, always available, inexpensive high-speed data solution.

It is important to note that many different wireless technologies exist. The most common technologies were accounted for on the basis of providing an acceptable, most widely supported solution. Although GSM-GPRS and 802.11b WLAN standards were used, principles surrounding authentication security, secure information exchange and location-aware remote access are generically applicable to other wireless technologies within the same genre.

Future related work includes investigation into the concept of a direct MS-to-MS (peer-to-peer) communication connection and the ability of an MS in simulating a BTS (vBTS). So called "intelligent" devices are currently available, however further effort is required in order to achieve a powerful, self-sufficient, location computational MS and underlying network capable of supporting these iMSs.

There is little doubt that technical developments and implementations efforts will progress in wireless technologies, the biggest remaining concern is how to manage the process of change and evolution of these technologies. The future of a truly secure, integrated wireless environment is indeed possible; however much is largely dependant upon how groups of stakeholders (who possesses rather different interests and views) will influence this process. Management of these obstacles is a necessity before wireless technologies are to become a generally excepted, publicly available, inexpensive and fully integrated consumer offering.

References

General

[104] GSM 01.04: "*Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms*".

Chapter 2

[0209] European Telecommunications Institute, GSM 42.009: "*Security aspects*". (previously GSM 02.09).

[And] R. Anderson, "*A5 – The GSM Encryption Algorithm*", June 1994.

[Ano] Anon. "*GSM Cell phones Cloned*", Web reference: http://jya.com/gsm-cloned.htm.
Anon. "*GSM Cloning*", Web reference: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

[Aso] N. Asokan (Nokia Research Center), "*Security Issues in Mobile Communication Systems*", IAB Workshop on Wireless Internetworking, March 2000.

[Bal] D.M. Balston, "*Personal and Mobile Radio Systems*", The pan-European cellular technology, In R.C.V. Macario, editor, Peter Peregrinus, London, 1991.

[Bri] M. Briceno, I. Goldberg, Wagner D, "*An Implementation of the GSM A3A8 Algorithm*".

[Cur] H.W. Curtis, "*Subscriber Authentication and Security in Digital Cellular Networks and Under the Mobile Internet Protocol*", The University of Texas at Austin, May 2001.

[Lin] Y.-B Lin, "Signaling System Number 7", *IEEE Potentials*, p. 5-8, August 1996.

[Mar] D. Margrave, "*GSM Security and Encryption*".

[Pes] L. Pesonen, "*GSM Interception*", Department of Computer Science and Engineering, Helsinki University of Technology, 1999.

[Sch] B. Schneier, "*Applied Cryptography*", 2nd Ed., Wiley, New York 1996.

[Sco] J. Scourias, "*Overview of the Global System of Mobile Communications*", University of Waterloo, 1997.

[Ves] S. Vesala, "*Handover algorithms and parameter and estimation*", Postgraduate notes in Radio Communications, May 2002.

Chapter 3

[0341] GSM 03.41: "*Digital cellular telecommunication system (Phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB)*".

[0371] GSM 03.71 version 8.5.0 release 1999, "*Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Functional description*".

[0510] GSM 05.10 version 8.9.0 release 1999, "*Technical Specification Group GSM/EDGE Radio Access Network; Digital cellular telecommunications system (Phase 2+); Radio subsystem synchronization*".

[Agr] J. Agre, A. Akinyemi, L. Ji, R. Masuoka and P. Thakkar, "*A layered Architecture for Location-based Services in Wireless Ad Hoc Networks*", IEEEAC paper#387, Updated November 2001.

[Bir] M. Birchler, "*E911 Phase 2 Location Solution Landscape*", Wireless Access Technology Research Motorola Labs.

[Dur] A. Duri, A. Cole, J. Munson, J. Christensen, "*An Approach to providing a Seamless End-User Experience for Location-Aware Applications*", IBM Thomas J Watson Research Center.

[Hof] B. Hoffmann-Wellenhof, H. Lichtenegger, J. Collins, "*Global Positioning System: Theory and Practise*", Springer verlag TELOS, 1997.

[Jon] D.K. Jonsson, J. Olavesen, "*Estimated accuracy of location in mobile networks using E-OTD*", Master Thesis in Information Communication Technology, Agder University College, Grimstad May 2002.

[Mou] M. Mouly, M.B. Pautet, "*The GSM System for Mobile Communications*", 1992.

[Por] M. Porretta, P. Nepa, G. Manara, F. Giannetti, "*Analysis of subscriber Radio Location Techniques through a Deterministic Propagation Model*", Dept. of Information Engineering, University of Pisa.

[Ref] "*Report on implementation issues related to access to location information by emergency services E-911 in EU*", Co-ordination Group on Access to Location Information by Emergency Services, CGALIES (2002):

[Sne] E. Snekkenes "*Concepts for Personal Location Privacy Policies*", Norwegian Computing Center, EC '01, October 14-17 2001, Tampa Florida, USA. ACM 1-58113-387-1/01/0010.

[Zim] R. Zimmermann, "*Localization of mobile devices*", Seminar: Mobile Computing, IFW C42, May 2001.

Chapter 4

[0360] GSM 03.60 version 7.3.1 Release 1998, "*Digital cellular telecommunications system (Phase 2+; General Packet Radio Service (GPRS); Service Description; Stage 2*".

[0814] GSM 08.14: "*Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Gb interface layer 1*".

[0918] GSM 09.18: "*Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface layer 3 specification*".

[0960] GSM 09.60: "*Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp interface*".

[0961] GSM 09.61: "*Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN)*".

[1215] GSM 12.15: "*Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Charging*".

[3GP] 3GPP TS43.020 3rd Generation Partnership Project, "*Technical Specification Group Services and System Aspects; Security related network functions*", previously GSM 03.20.

[Bet] C. Bettstetter, H.J. Vogel, J. Eberspacher, "*GSM Phase 2+ General Radio Service GPRS: Architecture, Protocols, and Air Interface*", Technische Universitat Munchen.

[Rau] J. Rautpalo, "*GPRS Security – Secure Remote Connections over GPRS*", Helsinki University of Technology, Department of Computer Science.

[Rha] M. Rahnema, "*Overview of the GSM System and Protocol Architecture*", IEEE Communications, vol. 31, no. 4, pp. 92-100, April 1993.

[Wal] B.Walke, G.Brasche, "*Concepts, Services, and Protocols of the New GSM Phase 2+ General Packet Radio Service*", IEEE Communications, vol. 35, no. 8, pp. 94-104, August 1997.

[Wik] E. Wiklander, "*Mobile Resource Awareness*", Master of Science Thesis, Department of Teleinformatics, Royal Institute of Technology (KTH), Stockholm, February 2001.

Chapter 5

[11b] Institute of Electrical and Electronics Engineers, Inc.
IEEE std 802.11b-1999, 20. January 2000, ISBN 0-7381-1811-7.

[216] Institute of Electrical and Electronics Engineers, Inc. IEEE Standard for Local and metropolitan area networks "*Part 16: Air Interface for Fixed Broadband Wireless Access Systems*", Approved 6 December 2001.

[Arn] S.E. Arnesen, K.Å. Håland, "*Modelling of coverage in WLAN*", Postgraduate thesis Information and Communication Technology, Grimstad, Norway, May 2001.

[Blu] "*Specification Volume 1 and 2, Specification of the Bluetooth System, Core*." Bluetooth Special Interest Group, Version 1.1, February 22, 2001.

[Bra] ETSI TR 101 683 V1.1.1, "*Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview*", 2000-02, Web reference: http://www.etsi.org/bran/.

[Fli] R. Flickenger, "*O'Reilly's Building Wireless Community Networks*", First Edition January 2002.

[Gar] J.Antio, G. Macias, F. Rousseau, G. Berger-Sabbatel, L. Toumi, A. Duda, "*Quality of Service and Mobility for the Wireless Internet*", LSR-IMAG Laboratory CNRS and Grenoble Institute of Technology Grenoble, France.

[Gol] I. Goldberg, N. Borisov, D. Wagner, "*Security of the WEP algorithm*", Berkley University.

[Iec] Institute of Electrical and Electronics Engineers, Inc. ISO/IEC 8802-11, ANSI /IEEE std 802.11, ISBN 0-7381-1658-0, First edition 1999-08-20.

[Iee] ANSI/IEEE 802.11 Release 1999: "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*".

[Nee] R. Van Nee, R. Prasad, "*OFDM for Wireless Multimedia Communications*", Artech House, Boston, 2000.

[Sig] "*Bluetooth security white paper*", Bluetooth SIG Security Expert Group, Web reference http://www.bluetooth.com.

[SHA] W.A. Shay, "*Understanding Data Communications and Networks Second Edition*", 1998 ISBN 0-534-95054-X.

[Tho] B. Thorngren, "*Public WLAN -The interaction between venues and WISPs*", Institute of Economic Research Lund University, Masters Thesis, February 2002.

[Tr1] TR 101 031 V2.2.1 (1999-01), "*Broadband Radio Access Networks (BRAN); High Performance Radio Local Area Network (HIPERLAN) Type 2; Requirements and architectures for wireless broadband access*".

[Van] N. Golmie, R.E. Van Dyck, A. Soltanian, "*Interference of Bluetooth and IEEE 802.11: Simulation Modeling and Performance Evaluation*", National Institute of standards and Technology Gaithersburg, Maryland.

[Yas] A. Yasmin, "*Known Vulnerabilities in Wireless LAN Security*", Department of Electrical and Communication Engineering, Helsinki University of Technology.

Chapter 6

[Mcg] T. McGarty, I. Kahin, "Alternative Networking Architectures: Pricing, Policy and Competition", Building Information Infrastructure, McGraw-Hill, New York, 1992.

[Sta] Star, S.L og Ruhleder, "*Steps to an Ecology of Infrastructure*", CSCW 94 - 10/94, CACM, 1994.

Chapter 7

[Bee] D. Beech, M. Maloney, N. Mendelsohn, "*XML Schema Part 1: Structures*", W3C Recommendation, May 2001. Web reference: http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/.

[Css] B. Bos, H.W. Lie, C. Lilley, I. Jacobs, "*Cascading Style Sheets, Level 2 (CSS2) specification*", May 1998, Web reference: http://www.w3.org/TR/REC-CSS2.

[Dat] P. Biron, A.Malhotra, "*XML Schema Part2: Datatypes*", W3C Recommendation, May 2001. Web reference: http://w3.org/TR/2001/REC-XMLschema-2-20010502/.

[Ima] T. Imamura, B. Dillaway, E. Simon, "*XML Encryption Syntax and Processing*", W3C Recommendation December 10, 2002, Web reference: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

[Kes] G. Kessler, "*Future Mobility: Mobile IP is the Harbinger of Untethered Computing*," Telephony, September 21, 1998, p. 52.

[Mim] N. Freed, N. Borenstein, RFC 2045: "*Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*", Standards Track, November 1996. Web reference: http://www.ietf.org/rfc/rfc2045.txt.

[Ms4] C. Perkins, "*IP Mobility Support for IPv4*", Ed. January 2002
Web reference: http://www.ietf.org/rfc/rfc3344.txt.

[Ms6] D.B. Johnson, C. Perkins, "*Mobility Support in IPv6*", IETF Mobile IP Working Group, Internet-Draft, November 1998.

[Nps] T. Bray, D. Hollander, A. Layman, "*Namespaces in XML*", W3C, Web reference: http://www.w3.org/TR/REC-xml-names/.

[Per] C.E. Perkins, "*Mobile IP: Design Principles and Practices*", Addison Wesley, 1998.

[Pfl] C.P. Pfleeger, "*Security in Computing*", Second Edition. ISBN: 0-13-337486-6, Prentice Hall PTR.

[Sgm] C.F. Goldfarb, "*The SGML Handbook*", ISBN: 0-19-853737-1.

[Uri] T. Berners-Lee, R. Fielding, L. Masinter, RFC 2396: "*Uniform Resource Identifiers (URI): Generic Syntax*", Standards Track, August 1998.

[Xml] T. Bray, J. Paoli, C.M. Sperberg-McQueen, "*Extensible Markup Language (XML) 1.0*", February 10 1998, Web reference: http://www.w3.org/TR/REC-XML/.

Chapter 8

[Agr] J. Agre, A. Akinyemi, L. Ji, R. Masuoka, P. Thakkar, "*A layered Architecture for Location-based Services in Wireless Ad Hoc Networks*", IEEEAC paper#387, Updated November 19, 2001.

[Cue] J. Cuellar, J. Morris, D. Mulligan, "*Geopriv requirements*", Internet-Draft, Internet Engineering Task Force, March 2003.

[Doh] L. Doherty, K.S.J. Pister, L.E. Ghaoui, "*Convex Position Estimation in Wireless Sensor Networks*", Department of Electrical Engineering and Computer Sciences – University of California, Berkeley, Proceedings of IEEE Infocom 2001.

[Dur] A. Duri, A. Cole, J. Munson, J. Christensen, "*An Approach to providing a Seamless End-User Experience for Location-Aware Applications*", IBM Thomas J Watson Research Center.

[Gad] GSM 03.32 Version 7.1.0 Release 1998: "*Digital Cellular Telecommunications System (Phase 2+); Universal Geographic Area Descriptor (GAD)*", European Telecommunications Standards Institute (ETSI).

[Lif] Location Interoperability Forum (LIF), "*Mobile Location Protocol v3.0.0.*", Web reference http://www.locationforum.org.

[Mul] N. Muller, "*Bluetooth Demystified*." New York, McGraw-Hill, 2001.

[P3P] W3C. "*Platform for Privacy Preferences (P3P) Project*", Web reference http://www.w3.org/P3P/.

[Poc] White paper, "*Push to Talk over Cellular*", Nokia Networks, Web reference http://www.nokia.com.

[Sne] E. Snekkenes, "*Concepts for Personal Location Privacy Policies*", Norwegian Computing Center. EC '01, October 14-17 2001, Tampa Florida, USA. ACM 1-58113-387-1/01/0010.

[Var] U. Varshney, A. Snow, M. McGivern, C. Howard, "*Voice Over IP*", COMMUNICATIONS OF THE ACM, Vol. 45, No. 1, January 2002.

[Wgs] "*Department of Defense World Geodetic System 1984 (WGS84)*", 3rd Edition, NIMA TR8350.2, Janruary 2000. Web reference http://www.wgs84.com.

Chapter 9

[3gp] "*Third Generation Partnership Project (3GPP2)*", Web reference: http://www.3gpp2.org.

[Cdm] 3rd Generation Partnership Project (3GPP2), "*cdma High Rate Data Air Interface Specification*", C.S20024, V3.0, December 2001.

[Dur] A. Duri, A. Cole, J. Munson, J. Christensen, "*An Approach to providing a Seamless End-User Experience for Location-Aware Applications*", IBM Thomas J Watson Research Center.

[Est] E. Esteves, "*The High Data Rate Evolution of cdma2000 Cellular Systems*", Multiaccess, Mobility and Teletraffic in Wireless Communications: Vol 5, ed. G.Stuber and BJabbari, Kluwer Academic Publishers.

[Evd] "*cdma2000 High Rate Packet Data Air Interface Specification*", 3GPP2 C.S0024, Version 4.0, October 2002.

[Gar] V.K. Garg, "*IS-95 CDMA and cdma2000*", Prentice-Hall, 2000.

[Pra] R. Prasad, T.Ojanpera, "*A survey on CDMA: Evolution towards wideband CDMA*", in: Proceedings of IEEE International Conference on Spread Spectrum Techniques and Applications, 1998, pp. 323-331.

[Qua] White paper, "*1xEV-DO System Architecture*", 2003, Web reference http://www.qualcomm.com.

Appendix

Abbreviations and Acronyms

For a comprehensive list of GSM-related abbreviations and acronyms please refer to [104].

Abbreviation or acronym	Description
2nd generation (2G)	Current digital mobile networks that allow voice and text transmission. There are a variety of standards, including GSM, which is used worldwide, and TDMA and CDMA which is used primarily in the Americas.
2.5 generation (2.5G)	More commonly known term for General Packet Radio Service (GPRS), a high-speed mobile network that allows for increased data speeds compared with those currently available over GSM.
3rd generation (3G)	Future mobile network that will be able to transmit at even higher data speeds compared with GPRS. One example is Universal Mobile Telecommunication System (UMTS); this will offer high-quality access to the Internet via an "always on" connection.
3GPP	Third Generation Partnership Program. A global organization whose partners have agreed to cooperate in the production of globally applicable Technical Specifications and Reports for 3G based on evolved GSM core networks and the radio access technologies that they support. The partners have further agreed to cooperate in the maintenance and development of the Global System for Mobile communication (GSM) and General Packet Radio Service (GPRS) Technical Specifications.
ACK	Acknowledgement.
A-GPS	Assisted GPS, a satellite positioning system that improves the functionality and performance of GPS. Requires adaptation to the Mobile Station (MS).
AP	Abbreviation for Access Point, a hardware device that acts as a communication hub for users of a wireless device to connect to WLAN.
APN	Access Point Name. This is the address of a GGSN that serves as an access point to the PDN.
AuC	Authentication Centre.
Backbone	The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.
Bluetooth	A computing and telecommunications industry specification for interconnection between mobile phones, computers, personal digital

	assistants (PDAs), fixed line phones and PCs using a short-range wireless connection.
BRAN	Broadband Radio Access Network.
BSC	Base station Controller, a high-capacity switch that performs radio functionality and mobility management in the mobile network.
BSS	Basic Service Set is the name given when two or more devices have recognized each other as Wireless devices and have established a Network.
BTS	Base Transceiver Station, contains transmitters, receivers and other equipment that communicates through radio channels with Mobile Stations (MS) within the coverage area of the cell that it serves.
CDMA	Code Division Multiple Access. A narrowband digital cellular technology.
CGI	Cell Global Identity.
CBC	Code Block Cipher.
CBC	Cell Broadcast Centre.
CS	Coding Scheme.
CSMA	Carrier Sense Multiple Access.
CSMA/CA	CSMA with collision avoidance.
CSS	Cascading Style Sheet.
CSS2	Cascading Style Sheet 2.
CTS	Clear to Send.
DES	Data Encryption Standard.
3DES	Triple Data Encryption Standard.
DSSS	Direct Sequence Spread Spectrum.
DTD	Document Type Definition.
ETSI	European Telecommunications Standards Institute brings together players from the telecommunication industry with the intention of putting forward new and improved wireless standards.
EDGE	Enhanced Data Rates for GSM Evolution. A technology that increases a network's efficiency, allowing transmissions speeds of up to 384 Kbps. EDGE works on the same principle of 'packets' of data as GPRS, though EDGE will be at least three times faster. EDGE makes it possible to run mobile multimedia applications, such as video and videoconferencing, and uses the same modulation technique as UMTS.
E-OTD	Enhanced Observed Time Difference. A positioning technology that compares the differing times of arrival of signals transmitted by at least three Base Transceiver Stations (BTSs). Installation requires hardware to be added to a mobile operator's existing BTSs; software upgrades in the network and a software change to the Mobile Station (MS) are required.
ESS	Extended Service Set. A roaming environment where all Access Points (APs) have the same Server Set Id (SSID).
EU	European Union.
FCC	Federal Communications Commission, the US government agency responsible for regulating telecommunications in the United States.
FHSS	Frequency Hopping Spread Spectrum.
GAD	Universal Geographical Area Description.
GMLC	Gateway Mobile Location Centre.
GMSC	Gateway Mobile Switching Centre.
GMT	Greenwich Mean Time.

GPRS	General Packet Radio Service - permits transmission speeds up to 171Kbps.
GPS	Global Positioning System that uses satellites to calculate positions on or near the earth. A mobile phone requires direct line of sight to at least four satellites.
GSM	Global System for Mobile Communications, the world's leading wireless communication standard.
Handover	Term for the switching between entities while a process is taking place.
HiperLAN	High Performance Radio Local Area Network.
HLR	Home Location Register. A database that holds subscription information about every subscriber in a mobile network.
HSCSD	High Speed Circuit Switched Data. This is an advanced technology that improves the speed data transfer over GSM Mobile Stations (MSs). It is based on circuit-switched technology, similar to that used on traditional telephone lines.
ICASA	Independent Communication Authority of South Africa. Regulator of telecommunications and the broadcasting sectors in South Africa.
IEEE	Institute of Electrical and Electronics Engineers.
IMEI	International Mobile Station Equipment Identity. International identity number that uniquely identifies mobile equipment.
iMS	intelligent Mobile Station.
IMSI	International Mobile Subscriber Identity. This is the unique number assigned to each GSM mobile subscriber.
IMT-2000	International Mobile Telecommunications 2000. Another name for Universal Mobile Telecommunications System (UMTS), a 3G mobile network.
IP	Internet Protocol. An IP address consists of a series of four numbers separated by full stops, that identifies a single, unique Internet computer host. Example: 10.15.22.18.
IPv4	Internet Protocol version 4.
IPv6	Internet Protocol version 6.
IR	Infrared.
ITU	International Telecommunications Union.
Kb	Kilobyte.
Kbps	Kilobits per second.
LA	Location Area.
LAN	Local Area Network.
LBS	Location-Based Services.
LCS	Location Services.
LIF	Location Interoperability Forum, its mission is to define, develop and promote common interfaces allowing user appliances and Internet-based applications to obtain location information from wireless networks, independent of positioning methods.
LMU	Location Measurement Unit to support positioning methods.
MAC	Media Access Control. A MAC address is the hardware address of a device connected to a network.
Mb	Megabyte.
Mbps	Megabits per second, or one million bits per second. This is the standard measure for determining speed of broadband transmission.
MLC	Mobile Location Centre.

MLP	Mobile Location Protocol. External interface from the location requester to the location requestee.
MLPP	Mobile Location Privacy Policy.
MoIP	Mobile Internet Protocol.
MPP	Mobile Positioning Protocol.
MS	Mobile Station.
MS-to-MS	Mobile Station to Mobile Station. This refers to a direct peer-to-peer connection of Mobile Stations.
MSC	Mobile Switching Centre, a node that performs the switching functions of the GSM Network.
MSISDN	Mobile Station International ISDN Number.
Namespace	Namespaces provide a simple method for qualifying element and attribute names used in Extensible Markup Language (XML) documents by associating them with namespaces identified by Uniform Resource Indicator (URI) reference.
NOS	Network Operation System.
OTD	Observed Time Difference.
OFDM	Orthogonal Frequency Division Multiplexing.
OTA	Over The Air.
P3P	Platform for Privacy Preference Project.
PAN	Personal Area Networking Profile defines IP-based personal networking.
PDN	Packet Data Network.
PDP	Packet Data Protocol.
PDSN	Packet Data Serving Node aggregate user traffic and provides the entry point into the data network.
PDU	Packet Data Unit.
PHY	Physical Layer.
PLMN	Public Land Mobile Network.
PoC	Push to Talk over Cellular.
Position over IP	Location Information Data transported over the TCP/IP Protocol.
PRNG	Pseudo-Random number Generator.
PSTN	Public Switched Telephone Network is the international telephone system based on copper wires carrying analog voice data.
Pulling	The receiving of Mobile content on request by the Mobile Station (MS).
Pushing	The receiving Mobile content triggered by an event other than a request.
QoS	Quality of Service.
RA	Routing Area.
RDP	The Roaming Data Profiler (RDP) contains permanent and temporary data for all registered WLAN users. Exists within SWARM 2 approach.
RF	Radio Frequency.
Roaming	Allows subscribers to send and receive calls in territories where their home network is unavailable, typically overseas. Roaming agreements are set up between operators in different countries to facilitate this service.
RP	Roaming Provider. The RP acts as a common node between multiple WLANs and the network operator's backbone. The RP

	manages one or many WLANs. Exists within SWARM 2 approach.
RSA	Rivest-Shamir-Adelman. Public key encryption algorithm.
RTD	Real Time Difference.
RTS	Request to Send.
Schema	Used to verify an XML document. Successor of DTD.
SGML	Standard Generalized Markup Language.
SGSN	Serving GPRS Support Node, a functional node of GPRS.
SIG	Special Interest Group.
SIM	Subscriber Information Module. A SIM is a unique small card that is placed inside a Mobile Station (MS) and is used to authenticate a subscriber to a GSM-GPRS network.
SMLC	Service Mobile Location Centre. The SMLC manages the overall coordination and scheduling of resources to perform positioning of a mobile device.
SMS	Short Message Service, allows the transmission of messages up to 160 alphanumeric characters to be sent to or from a GSM Mobile Station (MS).
SMS-C	Short Message Service Centre, serving node that handles SMS traffic.
SS	Security Sheet.
SS7	Signalling System #7, a signalling support network of GSM-GPRS based on the SS7 protocols.
SSID	Server Set Id that identifies the Access Point that acts as a single key or password that is shared with all connecting wireless clients.
SSL	Secure Socket Layer.
SWARM	System for Wireless and Roaming Mobility. Two versions exist namely, SWARM 1 and SWARM 2, and are models for the integration of WLAN and GSM-GPRS.
TA	Timing Advance, GSM standard protocol.
TADIG	Transferred Account Data Interchange Group was given the task of implementing roaming billing.
TAP	Transferred Account Procedure protocol. The interchange of billing data between different network operators.
TCP	Transmission Control Protocol. Protocol layer on top of conventional Internet protocol used to control end-to-end connections.
TDMA	Time Division Multiple Access, a digital cellular technology.
TOA	Time of Arrival.
UMTS	Universal Mobile Telecommunications System, the "third-generation" (3G) mobile standards that will build on the success of GSM/GPRS and on the GSM operators' existing investment in infrastructure. Data rates offered will be up to 2 Mbps.
U-NII	Unlicensed National Information Infrastructure.
URI	Uniform Resource Identifier.
vBTS	virtual Base Transceiver Station.
VoIP	Voice over IP.
VPN	Virtual Private Network a network that is constructed by using public infrastructure to connect private network nodes, for instance between a company's remote sites and head office.
W3C	World Wide Web Consortium.
WAE	Wireless Application Environment.
W-CDMA	Wideband Code Division Multiple Access. Radio access technology

	used in UMTS.
WECA	Short for Wireless Ethernet Compatibility Alliance, an organization made up of leading wireless equipment and software providers with the mission of guaranteeing interoperability of Wi-Fi products and to promote Wi-Fi as the global WLAN standard across all markets.
WEP	Short for Wired Equivalent Privacy, a security protocol for 802.11b WLAN.
WGS84	World Geodetic Systems 1984.
Wi-Fi	It is a trade term promulgated by WECA for WLAN equipment. Products certified as Wi-Fi by WECA are interoperable with each other even if they are from different manufacturers.
WiMAX	Broadband Wireless Metropolitan Area Network (802.16).
WISP	Wireless Internet Service Provider.
WLAN	Wireless Local Area Network.
XML	Extensible Markup Language, universal format for structured documents and data on the web.
XSD	XML Schema Definition.
XSL	eXtensible Stylesheet Language.
XSLT	eXtensible Stylesheet Language Transformation.