**24**

**GSM – Глобальна система мобільного зв’язку (Global System for Mobile Communications)**

1. **Історичний огляд**

GSM - наразі найбільш успішна система мобільного зв'язку в усьому світі. Його розробка була розпочата у 1982 році. Європейська конференція адміністрацій поштових служб та служб зв’язку (CEPT), попередниця Європейського інституту стандартів електрозв'язку (ETSI), заснувала групу Speciale Mobile, завданням якої було розробляти пропозиції щодо створення загальноєвропейської цифрової системи мобільного зв'язку . Необхідно було досягнути дві мети:

* По-перше, краще та більш ефективне технічне рішення для бездротового зв'язку - в той час стало очевидним, що у порівнянні з тодішніми аналоговими системами, цифрові системи будуть кращим рішенням для забезпечення обслуговування великої кількості користувачів, простоти використання та кількості можливих додаткових послуг .
* По-друге, єдиний стандарт повинен був бути реалізований по всій Європі, що дозволить здійснювати роумінг через кордони. Раніше це було неможливо, оскільки в різних країнах працювали несумісні аналогові системи.

У наступні роки декількома компаніями було розроблено різні пропозиції для подібної системи. Ці пропозиції охоплювали практично всі можливі технічні підходи в різних технічних сферах. Для множинного доступу було запропоновано доступ з часовим розподілом (TDMA), частотний розподіл (FDMA) та кодовий розподіл (CDMA). Для модуляції було обрано гаусівська частотна маніпуляція з мінімальним зсувом (GMSK), 4-частотна маніпуляція (4-FSK), квадратурної амплітудної модуляції (QAM) та адаптивна диференціальна імпульсно-кодова модуляція (ADPM). Швидкості передачі варіювали від 20 кбіт / с до 8 Мбіт / с. Всі запропоновані системи були перевірені як в польових випробуваннях, так і в канальному симуляторі (у Парижі 1986 р.). На процес прийняття рішень, крім технічних міркувань, вплинули маркетинг та політичні аргументи. FDMA не міг використовуватись, оскільки це б вимагало встановлення кілька різних антен на мобільній станції (MS). Незважаючи на те, що технічні переваги використання декількох антен були продемонстровані японською цифровою системою, збільшеня розмірів антен було вкрай небажано. Від CDMA врешті-решт відмовились, оскільки необхідна обробка сигналу на той час видавалась надто дорогою та ненадійною. Таким чином, лише система TDMA може пережила процес відбору. Проте різними компаніями були розроблені різні системи TDMA, тож остаточна TDMA була розробкою компромісного рішення поміж багатьох компаній. Причини цього носили політичний, а не технічний характер: вибір пропозиції однієї компанії як стандарт давав би цій конкретній компанії велику конкурентну перевагу. Конкретні деталі фінальної системи були розроблені комітетом протягом наступних двох років і послужили основою для систем, впроваджених в Європі після 1992 року.

На початку 1990-х років стало зрозуміло, що GSM мусить мати функції, які не були включені в початковий стандарт. Тому до 1995 року були розроблені так звані специфікації другої фази, що включали ці функції. У подальшому система зазнала додаткових вдосконаленнь, що включають пакетну радіопередачу (Загальний пакетний радіозв'язок (GPRS), див. Додаток 24.C на веб-сайті: www.wiley.com/go/molisch) і більш ефективну модуляцію для збільшення швидкості передачі даних для Evolution GSM (EDGE). Через ці розширення GSM часто називається системою 2.5-го покоління, оскільки її функції не входять у систему другого покоління, але не включають усі функціональні можливості третього покоління (Універсальна система мобільної телекомунікації (UMTS) (порівняйте з Главою 26)).

Успіх GSM перевершив всі очікування. Хоча вона спочатку була розроблена як європейська система, вона поступово поширилася по всьому світу. Австралія була першою неєвропейською країною, яка підписала основну угоду (Меморандум про взаєморозуміння (MoU)). З тих пір GSM став стандартом у всьому світі для мобільних комунікацій, а кількість зареестрованих користувачів, які станом на 2009 рік, досягла 3,5 млрд. Вийнятками лишаються лише Японія та Корея, де GSM так досі і не було впроваджено. У Сполучених Штатах Америки GSM конкурував із системою Проміжних Стандартів-95 (IS-95) на базі CDMA. На відміну від більшості країн, де спектральні ліцензії були надані за умови, що оператор мережі використовуватиме GSM, ліцензії в США були продані, не вимагаючи від компаній впровадження конкретної системи. У 2009 році було два основних оператора, які пропонували послуги на базі GSM, та ще два - що використовували конкуруючі технології (див. Главу 25).

Існує три версії GSM, кожна з яких використовує різні несучі частоти. Оригінальна система GSM використовує несучу частоту близько 900 МГц. Пізніше було додано GSM1800, який також називається цифровою стільниковою системою, в діапазоні 1800 МГц (DCS1800), для підтримки все більшого числа абонентів. Несучі частоти розміщуються близько 1800 МГц, загальна доступна смуга пропускання приблизно в три рази більше, ніж при 900 МГц, при зменшеній максимальній потужності передачі абоненського обладнання (MS). Крім того, GSM1800 ідентичний оригінальному GSM. Таким чином, обробка сигналу та технологія комутації залишаються незмінними. Збільшення несучої частоти, що передбачає менший шлях розповсюдження, і зменшення потужністі передачі, значно знижують розміри стільників. Цей факт у поєднанні з більш широкою смугою пропускання призводить до значного збільшення пропускної здатності мережі. Третя система, відома як GSM1900 або PCS-1900 (персональна система зв'язку), працює на несучої частоті 1900 МГц, і в основному використовується в США.

GSM є відкритим стандартом. Це означає, що вказуються лише інтерфейси, а не реалізація. Як приклад, ми розглянемо модуляцію в GSM, яка є GMSK. Стандарт GSM визначає верхню межу для позадіапазонної емісії, максимальну величину фазового шуму, інтермодуляційні складові тощо. Як досягнути необхідної лінійності (наприклад, шляхом лінійної подачі напруги, використовуючи підсилювач класу А - що малоймовірно через невелику ефективність - або будь-яким іншим способом) залежить від виробника обладнання. Таким чином, цей відкритий стандарт гарантує, що всі продукти від різних виробників сумісні, хоча вони все ще можуть відрізнятися за якістю та ціною. Сумісність особливо важлива для постачальників послуг. При використанні пропрієтарних систем провайдер може вибрати постачальника обладнання лише один раз - на початку реалізації мережі. Для GSM (та інших відкритих стандартів) постачальник може спочатку придбати базові станції (БС) від одного виробника, але пізніше придбати БС для збільшення потужності своєї мережі від іншого виробника, що може запропонувати кращу ціну. Це також доволяє провайдеру збирати систему купуючи компоненти різних постачальників.

1. **Короткий огляд системи**

Система GSM складається з трьох основних частин: Підсистеми базових станцій (Base Station Subsystem (BSS), Підсистема Мережі та Комутації (Network and Switching Subsystem (NSS) та Системи єксплуатаційного контролю (Operation Support System (OSS).

1. Підсистема базових станцій

ПБС (BSS) складається з базових приймально-передавальних станцій (BTS) та контрόлерів базової станції (BSC) (див. Малюнок 24.1). БТС встановлює і підтримує зв'язок з MS у своєму стільнику. Інтерфейсом між MS і BTS є повітряний інтерфейс, так званий Um-інтерфейс в контексті GSM. BTS складається з, як мінімум, антен та радіочастотної (РЧ) апаратури базової станції, а також програмного забезпечення для множинного доступу. Декілька або, рідше, один - BTS підключаються до одного BSC; вони з'єднані наземними проводовими або мікрохвильовими радіорелейними лініями. BSC виконує керуючу функцію. Поміж іншого, відповідає за передачу хендоверу) між двома BTS, які підключені до одного BSC. Інтерфейс між BTS і BSC називається Abis-інтерфейсом. На відміну від інших інтерфейсів цей інтерфейс не повністю означений стандартом. Розподіл функцій між BTS та BSC може відрізнятися залежно від виробника. У більшості випадків один BSC підключений до декількох BTS. Тому більш ефективним та вигідним є перенесення основного функціоналу до BSC. Проте це означає збільшення сигнального трафіку для зв'язку між BTS та BSC, що може бути небажаним (з огляду на те, що наземні лінії зв’зку є арендованими). Загалом BSS включає в себе великий набір функцій. Вона відповідальна за призначення каналів, підтримку якості каналів зв'язку та передачі даних, управління потужністю, кодування та шифруванням.

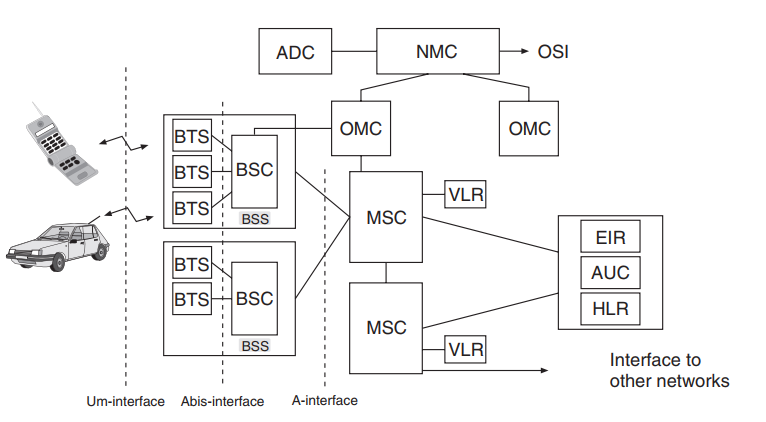


Рис. 24.1 Структурна схема систем Глобальної мережі звязку.

На цьому рисунку: ADC, Центр керування; NMC, Центр контролю мережі; OSI, Системний інтерфейс оператора

Використано з дозволу HP [1994] © Hewlett Packard.

***Підсистема Мережі та Комутації***

Основним компонентом ПМК (NSS) є Центр комутації мобільних послуг (MSC), який контролює трафік між різними BSC (див. Рис. 24.1). Однією з функцій MSC є керування мобільністю, яка включає в себе всі функції, необхідні для забезпечення справжньої мобільності для абонентів. Для прикладу, однією з функцій MSC є управління хендоверами, які виникають, коли MS виходить з області одного BSC і переміщується в область, яку охоплює інший BSC. Серед інших функцій - пейджинг та оновлення місцезнаходження. Всі взаємодії з іншими мережами, зокрема стаціонарною телефонною мережею загального користування (PSTN), також виконуються MSC.

NSS включає також деякі бази даних. Реєстраційний запис про місце розташування (HLR) містить усі номери мобільних абонентів, пов'язаних з одним MSC, та інформацію про місцезнаходження кожного з цих абонентів. У випадку вхідного дзвінка місцеположення потрібного абонента наведено в HLR, і виклик переадресовується до цього місця. Таким чином, ми можемо зробити висновок, що час від часу подорожуюча MS повинна надіслати оновлення свого місцезнаходження до свого HLR. VLR (Visitor Location Register) одного MSC містить всю інформацію про мобільних абонентів від інших HLR, які знаходяться в зоні цього MSC, і можуть перетинатися в мережі цього MSC. Крім того, тимчасовому номеру буде призначено MS, щоб дозволити "приймаючій" MSC встановити з'єднання з «не місцевою» MS.

Центр авторизації (AUC) перевіряє ідентичність кожного MS, що потребує з'єднання. Реєстр ідентифікації обладнання (EIR) містить централізовану інформацію про вкрадені або неправильно використані пристрої.

1. *Система підтримки експлуатації (OSS)*

OSS відповідальна за організацію мережі та експлуатаційне обслуговування. OSS охоплює такі функції:

1. Облік: скільки коштує конкретний дзвінок для певного абонента? Існує також безліч різних послуг та функцій, з яких кожен абонент може вибрати індивідуальний набір, включений до певного плану. Хоча цей багатий вибір послуг та цін є надзвичайно важливим на ринку, адміністративна підтримка цього індивідуалізму досить складна. Приклади розглянуті в розділі 24.10.
2. Технічне обслуговування: повна функціональність кожного компонента мережі GSM повинна постійно підтримуватися. Несправності можуть виникати в апаратному або програмному компоненті системи. Функціональні збої є більш дорогими, оскільки вони вимагають, щоб технік приїхав до місця несправності. На відміну від програмного забезпечення, яке наразі управляється з пункту управління. Наприклад, нові версії програмного забезпечення для комутації можуть бути встановлені в повній BSS з пункту управління та активовані в усій мережі за певний час. Програмне забезпечення для перегляду та технічного обслуговування часто є значною частиною загальної складності програмного забезпечення для керування GSM.
3. Управління MS: хоча всі MS повинні пройти стандартну перевірку, ніхто не застрахований від бракованих виробів, які, працюючи у мережі, викликають загальні. Ці пристрої повинні бути ідентифіковані, а їх подальша діяльність повинна бути заблокована.
4. Збір даних: OSS збирає дані про обсяг трафіку, а також про якість з’єднань.
5. **Повітряний інтерфейс**

GSM використовує комбінований підхід FDMA / TDMA, який додатково поєднується з дуплексуванням частотного домену (FDD) (див. Розділ 17). Давайте розберемося над цими абревіатурами.

FDD

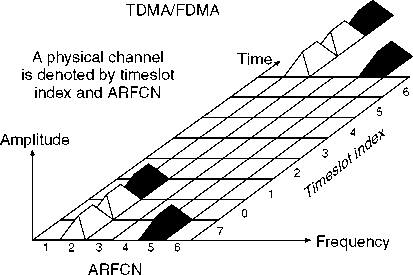
У першій версії GSM доступні частоти від 890 до 915 МГц і від 935 до 960 МГц. Нижня смуга використовується для висхідної лінії зв'язку (аплінк) (з'єднання з MS до BS). Верхня смуга використовується для низхідної лінії зв'язку (даунлінк). Частотний інтервал між висхідною лінією зв'язку та низхідною лінією для будь-якого з'єднання становить 45 МГц. Тому відносно дешеві дуплексні фільтри є достатніми для досягнення дуже хорошого розподілу між висхідною та низхідною лініями зв'язку.

Для GSM1800 діапазони частот 1 710-1785 МГц для висхідної лінії зв'язку та 1,805-1,880 МГц для нисхідної лінії зв'язку. У Північній Америці 1850-1,910 МГц використовуються для висхідної лінії зв'язку та 1,9301,990 МГц для нисхідної лінії зв'язку. Інші смуги додаються, коли вони стають доступними, див. Також главу 27

FDMA

Діапазони частот висхідної лінії зв'язку та низхідної лінії зв'язку розділені на сітку з 200 кГц проміжками. Зовнішні 100 кГц кожної 25-МГц смуги не використовуються, тому що вони є захисними смугами для обмеження перешкод з сусіднім спектром, який використовується іншими системами. Решта 124,200-кГц субдіапазонів нумеруються послідовно так званими абсолютними радіочастотними канальними номерами (ARFCNs).

TDMA

Завдяки технології модуляції з високою пропускною спроможністю (GMSK, див. Нижче) кожна 200-кГц підмережа підтримує швидкість передачі даних 271 Кбіт / с. Кожна підсмуга поділяється вісьмома користувачами. Вісь часу розділена на тимчасові інтервали, які періодично доступні кожному з восьми користувачів (рис. 24.2). Кожен часовий інтервал становить 576,92 мкс, що еквівалентно 156,25 біта. Набір з восьми таймслотів називається фреймом, що становить 4,615 мс.

7

Figure 24.2 Time Division Multiple Access/Frequency Division Multiple Access system. Adapted with permission from HP [1994] © Hewlett Packard.

У кожному кадрі часові інтервали пронумеровані від 0 до 7. Кожен абонент періодично отримує доступ до одного конкретного часового інтервалу в кожному кадрі на підсмузі однієї частоти. Поєднання часового слоту і діапазону частоти називається фізичним каналом. Вид даних, які передаються по одному такому фізичному каналу, залежить від логічного каналу (див. Також розділ 24.4).

Важливі особливості повітряного інтерфейсу далі описані покроково.

**Виділення таймслотів на аплінк даунлінк.**

Абонент використовує часові інтервали з таким самим номером (індексом) у висхідній та низхідній лініях зв'язку. Проте нумерація у висхідній лінії зміщується на три слоти відносно нумерації в низхідній лінії зв'язку. Це полегшує розробку прийомопередавача МС, оскільки прийом та передача не відбуваються одночасно (порівняйте Рисунок 24.3).

**Часові слоти для аплінку та даунлінку**

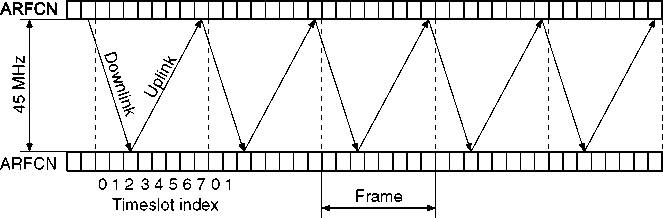


Рис. 24.3 Вирівнювання аплінк та даунлінк слотів

Використано за згоди HP [1994] © Hewlett Packard.

**Техніка модуляції**

GSM для модуляції використовує GMSK. GMSK - це варіант частотної маніпуляції з мінімальним зсувом (MSK); Різниця полягає в тому, що послідовність даних пропускається через фільтр з Гаусівською передаточною характеристикою (див. главу 11).

Ця фільтрація досить ретельна (hard). Тому спектр досить вузький, але існує значна кількість міжсимвольних перешкод (ISI). З іншого боку, міжсимвольні перешкоди через дисперсійну затримку повітряного каналу, як правило, посилюються. Таким чином, в будь-якому випадку потрібно використовувати якийсь вирівнювання. На малюнку 24.4 наведено типовий приклад фазової решітки цього типу GMSK та чистого MSK для порівняння. Метод детектування не визначений стандартом. Можливе використання диференціального детектування, когерентного детектування або детектування обмежувачем-дискримінатором.

**Підскакування “Ramping” потужності**

Якби передавач починав передачу даних точно на початку кожного таймслоту, він мусив би перемикати сигнал за дуже малий проміжок часу (значно менший за довжину символу). Так само, наприкінці часового інтервалу, він повинен був припинити передачу, щоб не створювати перешкод для наступного часового інтервалу. Це важко реалізувати в апаратному забезпеченні та, навіть якщо це можна було б реалізувати, різкий перехід у часовій області призведе до розширення спектру емісії. Тому GSM визначає час, протягом якого сигнали плавно вимикаються та вмикаються (див. Малюнок 24.5). Тим не менше, вимоги до апаратного забезпечення ще значні. У випадку, коли передавач випромінює максимальну потужність сигналу, він повинен підскакувати з 2 × 10-7 Вт до 2 Вт протягом 28 мкс. З іншого боку, під час фактичної передачі даних потужність сигналу може відхилятися лише на 25% (1 дБ) від його номінального значення.

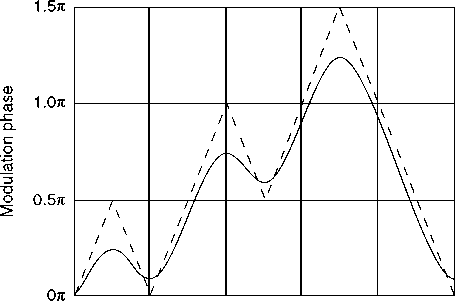


Figure 24.4 Phase diagram for the bit sequence 1011011000 for Gaussian minimum shift keying with BgT = 0.3 (solid line) and pure minimum shift keying (dashed line).

**Контроль потужність сигналу та випромінювання**

GSM забезпечує керування потужністю для потужності передачі. Хоча управління потужністю зазвичай асоціюється з системами CDMA, він також має великі переваги в GSM (та інших системах TDMA / FDMA):

1. Це збільшує час роботи батарей. Підсилювач потужності передачі є основним фактором енергоспоживання MS. Таким чином, можливий час роботи без підзарядки акумуляторів залежить від рівня випущеного сигналу. Таким чином, викидаючи більше енергії, ніж це необхідно для забезпечення хорошої якості прийнятого сигналу на іншому кінці ланки, є витрата енергії.
2. Передача при надто високому рівні потужності збільшує рівень перешкод у сусідніх каналах. Через концепцію стільникового зв'язку кожен передавач є можливим перешкодою для користувачів інших комірок, які використовують один і той же часово-частотний слот. Однак, на відміну від систем CDMA, управління потужністю практично не є необхідним для роботи системи.

GSM визначає різні типи MS, що мають різні максимальні потужності передачі, хоча найбільш часто зустрічаються 2Вт станції (пікова потужність). Контроль потужності може зменшити потужність випромінюваного сигналу приблизно на 30 дБ; регулювання виконується на 2 дБ. Контроль є адаптивним: БС періодично інформує МС про рівень прийнятого сигналу, а МС використовує цю інформацію для збільшення або зменшення його потужності передачі. Максимальний рівень потужності BS може варіюватися від 2 до 300 Вт. Крім того, BS мають аналогічну схему управління потужністю, яка може зменшити вихідну потужність приблизно на 30 дБ.

**Принцип "підскакування потужності"**

Power

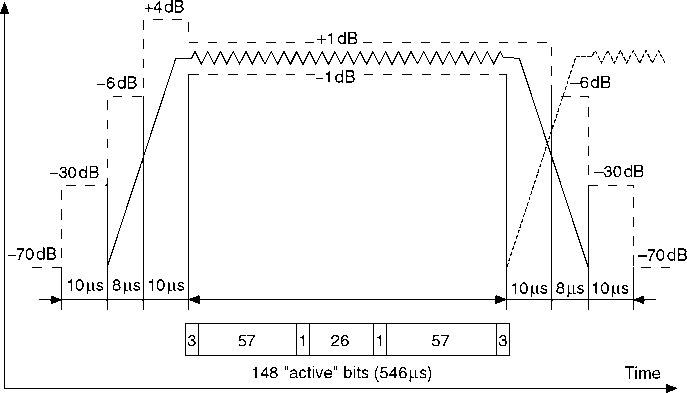


Рис. 24.5 Підскакування потужності в одному таймслоті.

Adapted with permission from HP [1994] © Hewlett Packard.

**Позасмугове випромінення та продукти побічної інтермодуляції**

Обмеження для позасмугового випромінення не такі серйозні, як, наприклад, для аналогових систем. Максимальна дозволена потужність позасмугового сигналу в обох BS і MS становить приблизно -30дБм, що дуже високе значення для бездротового зв'язку. Проте в смузі від 890 до 915 МГц (смуга висхідної лінії зв'язку) потужність, що випромінюється БС, не повинна перевищувати -93 дБм. Це необхідно тому, що БС повинна отримувати сигнали від MS, з рівнем сигналу в діапазоні -102 дБм, у цій смузі. Крім того, передавальні антени розташовані поблизу приймальних антен (або навіть поєднані) на BS, і тому будь-яке позадіапазонне випромінювання в цій смузі викликає серйозні перешкоди. Подібні обмеження застосовуються для продуктів побічної інтермодуляції.

**Структура таймслоту**

Малюнок 24.6 ілюструє дані, що містяться в часовому інтервалі з довжиною 148 біт. Однак не всі ці біти - корисне навантаження. Дані корисного навантаження завантажуються двома блоками з 57 біт. Між цими блоками є так звана міжамбула. Це відома послідовність із 26 біт що забезпечує додатковий контроль, який буде розглянутий в розділі 24.7. Крім того, міжамбула слугує ідентифікатором БС. Існує додатковий контрольний біт між міжамбулою і кожним із двох блоків, що містять дані; мета цих контрольних бітів пояснюється в розділі 24.4. Нарешті, пачка передачі починається і закінчується трьома хвостовими бітами. Ці біти відомі, і дозволяють припинити оцінку послідовності максимальної правдоподібності (MLSE) у певних станах на початку та в кінці сплеску даних. Це зменшує складність та підвищує продуктивність декодування (див. Також главу 14). Часові інтервали закінчуються захисним періодом 8,25 біта. Окрім "звичайних" «сплесків» передачі, є й інші види «сплесків»(bursts). MS передають сплески доступу для встановлення початкового контакту з BS. Переривання корекції частоти забезпечує частотну корекцію MS. Синхронізаційні сплески дозволяють MS синхронізуватись із часом синхронізації баз даних. Ці сплески будуть більш детально пояснені в розділі 24.4.2.

Timeslot (normal burst)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| 3 | 57 | 1 | 26 | 1 | 57 | 3 | 8.25 |

156.25 bits 576.92 |rs

Figure 24.6 Functions of the bits of a normal transmission burst.

|  |  |  |  |
| --- | --- | --- | --- |
| f : | ‘ t ' | ‘ t ' | ‘ t “ |
| Tail | Control | Control | Tail |
| bits | bit | bit | bits |

Data Midamble Data Guard

period

1. **Логічні та фізичні канали**

На додаток до фактичного корисного навантаження, GSM також повинен передавати велику кількість сигнальної інформації. Ці різні типи даних передаються через кілька логічних каналів. Назва пов'язана з тим, що кожний з типів даних передається в певні часові інтервали, які є частинами фізичних каналів. У першій частині цього розділу розглядається тип даних, що передаються через логічні канали. Друга частина описує відображення логічних каналів на фізичні канали.

1. *Логічні канали*

**Канал трафіку (TCHs)**

Корисне навантаження передаються через TCH. Корисне навантаження може складатися з закодованих голосових даних або "чистих" даних. Існує певна гнучкість стосовно швидкості передачі даних: повношвидкісні канали трафіку (TCH/F) та напівшвидкісні канали трафіку (TCH/H). Два напівшвидкісних канали накладаються на один і той же часовий інтервал, але в різних кадрах.

**Повношвидкісні канали трафіку**

* Повношвидкісні звукові канали: швидкість передачі даних голосового кодера становить 13 кбіт / с. Кодування каналів збільшує ефективну швидкість передачі даних до 22.8 кбіт/с. Повношвидкісні канали даних: дані корисного навантаження зі швидкістю передачі даних 9.6, 4.8 або 2.4 кбіт/с кодуються кодами ”forward error correction”(FEC) і передаються з ефективною швидкістю передачі даних 22,8 кбіт/с.

Напівшвидкісні канали трафіку

• Half-rate voice channels: voice encoding with a data rate as low as 6.5 kbit/s is feasible. Channel coding increases the transmitted data rate to 11.4 kbit/s.

• Half-rate data channels: payload data with rates of 4.8 or 2.4kbits/s can be encoded with an FEC code, which leads to an effective transmission rate of 11.4 kbit/s.

**Broadcast CHannels (BCHs)**

BCHs are only found in the downlink. They serve as beacon signals. They provide the MS with the initial information that is necessary to start the establishment of any kind of connection. The MS uses signals from these channels to establish a synchronization in both time and frequency. Furthermore, these channels contain data regarding, e.g., cell identity. As the BSs are not synchronized with respect to each other, the MS has to track these channels not only before a connection is established, but all the time, in order to provide information about possible HOs.

Frequency Correction CHannels (FCCHs) The carrier frequencies of the BSs are usually very precise and do not vary in time, as they are based on rubidium clocks. However, dimension considerations and price considerations make it impossible to implement such good frequency generators in MSs. Therefore, the BS provides the MS with a frequency reference (an unmodulated carrier with a fixed offset from the nominal carrier frequency) via the FCCH. The MS tunes its carrier frequency to this reference; this ensures that both the MS and the BS use the same carrier frequency.

Synchronization CHannel (SCH) In order to transmit and receive bursts appropriately, an MS not only has to be aware of the carrier frequencies used by the BS but also of its frame timing on the selected carrier. This is achieved with the SCH, which informs the MS about the frame number and the Base Station Identity Code (BSIC). Decoding of the BSIC ensures that the MS only joins admissible GSM cells and does not attempt to synchronize to signals emitted by other systems in the same band.

Broadcast Control CHannel (BCCH) Cell-specific information is transmitted via the BCCH. This includes, e.g., Location Area Identity (LAI),[[1]](#footnote-1) maximum permitted signal power of the MS, actual available TCH, frequencies of the BCCH of neighboring BSs that are permanently observed by the MS to prepare for a handover, etc.

**Common Control CHannels (CCCHs)**

Before a BS can establish a connection to a certain MS, it has to send some signaling information to all MSs in an area, even though only one MS is the desired receiver. This is necessary because in the initial setup stage, there is no dedicated channel established between the BS and a MS. CCCHs are intended for transmission of information to all MSs.

Paging CHannel (PCH) When a request - e.g., from a landline - arrives at the BS to establish a connection to a specific MS, the BSs within a location area send a signal to all MSs within their range. This signal contains either the permanent International Mobile Subscriber Identity (IMSI) or the Temporary Mobile Subscriber Identity (TMSI) of the desired MS. The desired MS continues the process of establishing the connection by requesting (via a Random Access CHannel (RACH)) a TCH, as discussed below. The PCH may also be used to broadcast local messages like street traffic information or commercials to all subscribers within a cell. Evidently, the PCH is only found in the downlink.

Random Access CHannel (RACH) A mobile subscriber requests a connection. This might have two reasons. Either the subscriber wants to initiate a connection, or the MS was informed about an incoming connection request via the PCH. The RACH can only be found in the uplink.

Access Grant CHannel (AGCH) Upon the arrival of a connection request via the RACH, the first thing that is established is a Dedicated Control CHannel (DCCH) for this connection. This channel is called the Standalone Dedicated Control CHannel (SDCCH), which is discussed below. This channel is assigned to the MS via the AGCH, which can only be found in the downlink.

**Dedicated Control CHannels (DCCHs)**

Similar to the TCHs, the DCCHs are bidirectional - i.e., they can be found in the uplink and downlink. They transmit the signaling information that is necessary during a connection. As the name implies, DCCHs are dedicated to one specific connection.

Standalone Dedicated Control CHannel (SDCCH) After acceptance of a connection request, the SDCCH is responsible for further establishing this connection. The SDCCH ensures that the MS and the BS stay connected during the authentication process. After this process has been finished, a TCH is finally assigned for this connection via the SDCCH.

Slow Associated Control CHannel (SACCH) Information regarding the properties of the radio link are transmitted via the SACCH. This information need not be transmitted very often, and therefore the channel is called slow. The MS informs the BS about the strength and quality of the signal received from serving BSs and neighboring BSs. The BS sends data about the power control and runtime of the signal from the MS to the BS. The latter is necessary for the timing advance, which will be explained later.

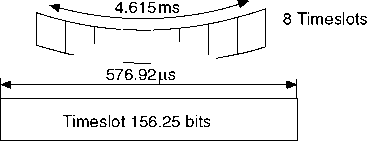
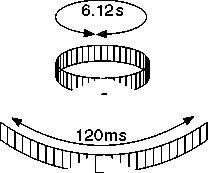
Fast Associated Control CHannel (FACCH) The FACCH is used for HOs that are necessary for a short period of time; therefore, the channel has to be able to transmit at a higher rate than the SACCH. Transmitted information is similar to that sent by the SDCCH.

The SACCH is associated with either a TCH or a SDCCH; the FACCH is associated with a TCH.

1. *Mapping Between Logical and Physical Channels*

The signals of logical channels described above have to be transmitted via physical channels, which are represented by the timeslot number and the ARFCN. In order to better understand the mapping, we first have to realize that the time dimension is not only partitioned into periodically repeated frames of eight timeslots each, but that these frames and timeslots are the smallest units in the time grid. In fact, multiple frames are combined on different levels to make bigger frames (see Figure 24.7).

We have already seen above that eight timeslots with a duration of 577 |is each are combined as a frame. The duration of this frame, 4.61 ms, is the basic period of a GSM system. A total of 26 of these frames are combined as a multiframe, which has a duration of 120ms. Furthermore, 51 of these multiframes are contained in one superframe, which has a length of 6.12 s. Finally, 2,048 of these superframes are combined into one hyperframe, which lasts 3h and 28 min. The hyperframe is implemented mainly for cryptographic reasons, in order to guarantee privacy over the air interface. Therefore, encryption is applied to the payload data and the period of the encryption algorithm is exactly the length of one hyperframe.

**Frames and multiframes**

Superframe

Multiframe

51 Multiframes

26 Frames

Frame

Figure 24.7 Structure of Global System for Mobile communications frames for traffic channels. Adapted with permission from HP [1994] © Hewlett Packard.

Understanding the multiple frame structure enables us to discuss which timeslot contains which logical channel. Not all timeslots have to be used for the TCH, as the available data rate on the physical channel is 2 • 57bits/4.615ms = 24.7 kbit/s, while a full rate TCH requires only a 22.8-kbit/s data rate. Therefore, the remaining 1.9 kbit/s may be used for other logical channels.

SACCH As discussed above, 26 frames are combined as a multiframe. Of these 26, only 24 frames are dedicated to the TCH. The 13th (and sometimes the 26th) frame are used by the SACCH. The 26th frame is only employed if two half-rate connections share one physical channel; otherwise the timeslot of the 26th frame is an idle frame. The transmission rate of the SACCH is 950 bit/s. The data transmitted via the SACCH is processed differently from the data in the TCH. The bits of four consecutive SACCH bursts are processed together. For this purpose, four multiframes might be combined into a (nameless) higher order frame of length 480 ms. These four SACCH bursts contain 456 bits associated with SACCH data and are used to transmit 184 actual data bits. The data bits are (i) first encoded with a (224, 184) block code, (ii) have four tail bits added, and (iii) then everything is encoded with the regular rate-1/2 convolutional encoder; this leads to the total of 2 • 228 bit = 456bit.

FACCH An FACCH does not have to be permanently available. It is only necessary in special situations - e.g., when a handover has to be performed. Therefore, no timeslots are reserved for the FACCH. Instead, normal TCH-related bursts of a connection are partly used for FACCH purposes in case this is required. The above-mentioned control bits (stealing bits) between the midamble and the datablocks of a burst indicate whether an FACCH is present in this burst or not - i.e., “steals” bits from the TCH. The 184 bits of an FACCH are encoded in the same way as SACCH bits. In order to transmit the resulting 456 bits via the normal TCH timeslots, eight consecutive frames are used: the even payload bits of the first four bursts and the odd bits of the second four bursts are replaced by bits from the FACCH.

Common Logical Channels The FACCH and SACCH use the physical channel of the associated connection. This is possible as the physical channel supports a slightly higher data rate than is necessary for one TCH connection. Therefore, it is possible to transmit signaling in timeslots belonging to the same physical channel. However, the other logical signaling channels are not associated with a TCH connection, either because they are required for establishing a connection or because they are used even in the absence of a TCH channel. Therefore, all these channels operate in the first burst of each frame of the so-called “BCCH carrier.” This assignment strategy makes sure that one physical channel in each cell is permanently occupied. This leads, of course, to a loss of capacity, especially in cells that use only one carrier. However, there is one option to overcome this: if the cell is full, no new connections can be established. Therefore, no timeslots have to be reserved for signaling related to new connections, and also the first slot of the BCCH carrier can be used for a normal TCH channel.[[2]](#footnote-2) Furthermore, the frames are combined as higher order frames in a different way. A total of 51 frames are combined into a multiframe, which has a duration of 235 ms. CCCHs are unidirectional, with the RACH being the only channel in the uplink, while several common channels exist in the downlink.

RACH The RACH is necessary only for the uplink. During each multiframe, 8 data bits, encoded into 36 bits, are transmitted via the RACH. These 36 bits are transmitted as an access burst. The structure of an access burst has to differ from normally transmitted bursts. At the time the MS requests a connection, it is not yet aware of the runtime of the signal from the MS to the BS. This runtime might be in the range from 0 to 100 |xs where the maximal value is defined by the maximal cell range of 30 km. Therefore, a larger guard time is necessary to ensure that a random burst does not collide with other bursts in adjacent timeslots. After the connection is established, the BS informs the MS about the runtime and therefore the MS can reduce the size of the guard times by employing timing advance, which will be discussed later. A complete random access burst has the following structure. It starts with 8 tail bits, which are followed by 41 synchronization bits. Afterward, the 36 bits of encoded data and 3 additional tail bits are transmitted. This adds to a total of 88 bits and leaves a guard time of 100 |xs at the end, which corresponds to 68.25 bits. As the RACH is the only unassociated control channel in the uplink, the timeslot numbered 0 may be used for random access burst in every frame.

Common Channels in the Downlink The other common channels - such as FCCH, SCH, BCCH, PCH, and AGCH - can only be found in the downlink and have a fixed order in the multiframe. Figure 24.8 illustrates this structure. Remember that only timeslot 0 in each frame carries a CCCH. Of the 51 frames in this multiframe, the last one is always idle. The remaining 50 frames are divided into blocks of 10 frames. Each of these blocks starts with a frame containing the FCCH. Afterward the SCH is transmitted during the next frame. The first block of frames contains four BCCHs (in frames 3-6) followed by four frames which contain the PCH or AGCH (frames 7-10). The other four blocks of 10 frames also start with the FCCH and SCH frames, and then consist either of PCH- or AGCH-carrying frames. The FCCH and the SCH employ bursts that have a special structure (this is discussed in the next section). As the MSs of neighboring cells continuously evaluate the signal strength of the first timeslot of the frames on the BCCH carrier, the BS always has to transmit some information during these timeslots, even when there is no connection request.

SDCCH The SDCCH may occupy a physical channel by itself, or - in case the common channels do not occupy all the available slots on the BCCH - it may be transmitted during the first timeslots on the BCCH. In the latter case, either four or eight SDCCHs share this physical channel.

F:FCCH S : SCH B:BCCH

C : CCCH (PCH or AGCH) I : Idle

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | TTT | 7 | 0 | 1 | 2 | TTT | 7 | 0 | 1 |

TDMA-

multiframe

1 2

TTT

B

J\_I\_L

TTT

C

\_I\_LL

F

S

TTT

C

\_LLL

TTT

C

TTT

F

S

TTT

C

TTT

TTT

C

TTT

TTT

C

TTT

TTT

C

TTT

F

S

TTT

C

TTT

TTT

C

I I I

~V

Multiframe, consisting of 51 frames (235.4ms)

Figure 24.8 Mapping of broadcast channels (FCCH, SCH, and BCH) and common control channels to timeslots numbered 0 (compare [CME 20, 1994]).

1. **Synchronization**

Up to now, we have assumed that the BS and the MS are synchronized in time and frequency. However, only the BS is required by the standard to have a high-quality time and frequency reference. For the MS, such a reference would be too expensive. Thus, the MS synchronizes its frequency and time references with those of the BS. This is done in three steps: first, the MS tunes its carrier frequency to that of the BS. Next, the MS synchronizes its timing to the BS by using synchronization sequences. Finally, the timing of the MS is additionally shifted with respect to the timing of the BS to compensate for the runtime of the signal between the BS and MS (timing advance).

1. *Frequency Synchronization*

As mentioned before, the BS uses very precise rubidium clocks, or GPS (Global Positioning System) signals, as frequency references. Due to space and cost limitations, the oscillators at the MS are quartz oscillators, which have much lower precision. Fortunately, this is not a problem, since the BS can transmit its high-precision frequency reference periodically and the MS can adjust its local oscillator based on this received reference. Transmission of the reference frequency is done via the FCCH. As we discussed in the previous section, the FCCH is transmitted during timeslots with index 0 of roughly every tenth frame on the BCCH. An FCCH burst consists of 3 tail bits at the beginning, 142 all-zero bits in the middle, and 3 tail bits at the end. The usual guard period (length equivalent to 8.25 bits) is appended. It should be noted that it is not the carrier frequency that is transmitted as a reference, but rather the carrier modulated with a string of zeros. This equals a sinusoidal signal with a frequency that is the carrier frequency offset by the MSK modulation frequency. As this offset is completely deterministic, it does not change the principle underlying the synchronization process.

1. *Time Synchronization*

Time synchronization information is transmitted from the BS to the MS via the SCH. SCH bursts contain information regarding the current index of the hyperframe, superframe, and multiframe. This is not a lot of information, but has to be transmitted very reliably. This explains the relatively complex coding scheme on the SCH. The MS uses the transmitted reference numbers regarding themultiframes, etc. to set its internal counter. This internal counter is not only a time reference with respect to the timeslot and frame grid, but also serves as a time reference within a timeslot with a quarter-bit precision. This reference is initially adjusted by considering the start of SCH bursts received at the MS. The MS then transmits the RACH burst relative to this internal reference. Based on the reception of the RACH, the BS can estimate the roundtrip time between the BS and the MS and use this information for timing advance (described in the next section).

1. *Timing Advance*

GSM supports cell ranges of up to 30km, so that propagation delay between the BS and the MS might be as big as 100 |xs. Thus, the following situation might occur: consider user A being at a 30-km distance from the BS, and transmitting bursts in timeslot TS 3 of every frame. User B is located close to the BS and accesses timeslot TS 4. The propagation delay of user A is around 100 |xs, whereas the propagation delay of user B is negligible. Therefore, if propagation delay is not compensated, the end of a burst from user A partly overlaps with the beginning of a burst from user B at the BS (this situation is illustrated in Figure 24.9).

Overlap

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Signal user A at MS |
|  |  |  | Signal user B at MS |
|  |  |  | Signal user A at BS |
|  | Signal user B at BS |
|  |  |

Figure 24.9 Overlapping bursts assuming uncompensated propagation delay.

To overcome this problem, the propagation delay from MS to BS is estimated by the BS during the initial phase of establishing a connection. The result is transmitted to the MS, which then sends its bursts advanced (with respect to the regular timing structure) to ensure that the bursts arrive within the dedicated timeslots at the BS. As the access bursts are transmitted before the MS is aware of the propagation delay, it now becomes clear why they must have a bigger guard period than normal transmission bursts: the guard period must be big enough to accommodate the worst case propagation delay - i.e., an MS at the boundary of a cell with maximum size.

There are some very big cells in rural areas where propagation delays exceed foreseen timing advances. In these cases, it might be necessary to use only every second timeslot as otherwise timeslots from different users would collide at the BS. This implies a waste of capacity. However, as this might only occur in rural areas with big cell ranges and low subscriber densities, the actual loss for the provider is small.

1. *Summary of Burst Structures*

Finally, Figure 24.10 provides an overview of the different kinds of bursts and illustrates the functions of their bits.

Normal

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 start | 58 data bits | 26 training | 58 data bits | 3 stop | 8.25 bits |
| bits | (encrypted) | bits | (encrypted) | bits | guard period |

FCCH burst

|  |  |  |  |
| --- | --- | --- | --- |
| 3 start |  | 3 stop | 8.25 bits |
| bits | 142 zeros | bits | guard period |

SCH burst

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 start | 39 data bits | 64 training | 39 data bits | 3 stop | 8.25 bits |
| bits | (encrypted) | bits | (encrypted) | bits | guard period |

RACH burst

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 start | 41 synchronization | 36 data bits | 3 stop | 68.25 bits extended |
| bits | bits | (encrypted) | bits | guard period |

Dummy burst

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 start bits | 58 mixed bits | 26 training bits | 58 mixed bits | 3 stop bits | 8.25 bits guard period |

Figure 24.10 Structure of timeslots in the Global System for Mobile communications.

Reproduced with permission from Rappaport [1996] © IEEE.

1. **Coding**

To transmit speech via the physical GSM channel the “speech signals” have to be translated into digital signals. This process should maintain a certain speech quality while keeping the required data rate as low as possible (see also Chapter 15). Different forms of speech coding were considered for GSM, and finally a Regular Pulse Excited with Long Term Prediction (RPE-LTP) solution was chosen (see Chapter 15). The digitized speech that is obtained in such a way then has to be protected by FEC in order to remain intelligible when transmitted over typical cellular channels (uncoded Bit Error Rates (BERs) of ~10-3 to 10-1). Both block and convolutional codes are used for this purpose in GSM.

Thus, voice transmission in GSM represents a typical example of the paradox of speech communications. First, redundancy is removed from the source data stream during the speech-coding process, and then redundancy is added in the form of error-correcting coding before transmission. The reason for this approach is that the original redundancy of the speech signal is rather inefficient at ensuring intelligibility of speech when transmitted over wireless channels. In this section, we first describe voice encoding, and subsequently channel coding; these can be seen as important applications of the principles expounded in Chapters 15 and 14, respectively.

1. *Voice Encoding*

Like most voice encoders (also referred to as vocoders), the GSM vocoder is not a classical sourcecoding processes like, e.g., the Huffman code. Rather, GSM uses a lossy compression method, meaning that the original signal cannot be reconstructed perfectly, but that the compression and decompression procedures lead to a signal which is similar enough to the original one to allow comfortable voice communications. As GSM has evolved, so has the speech coder. For the first release of GSM, an RPE-LTP approach was used. The idea behind this approach is to considerthe human voice as output from a time-varying filter bank which is excited periodically. Both parameters describing the filter bank and the excitation process are transmitted. Since the samples of a voice signal are correlated, any sample can be predicted approximately by linearly combining previous samples. Evidently, correlation reflects the redundancy of the voice signal. However, the correlation properties of the signal vary with time, therefore the filter bank has to be time varying as well.

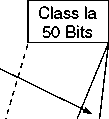
Later on, an enhanced speech coder was introduced that improved speech quality without increasing the required data throughput. A more detailed description of GSM speech coding can be found in Appendix 24.B (see [www.wiley.com/go/molisch](http://www.wiley.com/go/molisch)), and the principles of speech coding in general are described in Chapter 15.

The data created by the vocoder are divided into different classes, which have different vulnerabilities to bit errors. By this we mean that the bits have different levels of importance for the perceived quality of the reconstructed signal. The bits in class 1a are important, as an error in these bits is perceived as a gross distortion of the signal. Therefore, they are protected by a convolutional code and additional block coding. The slightly less important bits of class 1b are protected just by a convolutional code, while the bits associated with class 2 are transmitted without further channel encoding.

Another method to reduce the data rate is Voice Activity Detection (VAD). It detects periods when the user is not speaking, and ceases transmission during these periods - this is Discontinuous Transmission (DTX). DTX increases the battery lifetime of the MS and reduces co-channel interference with other users.

1. *Channel Encoding*

Let us first give an overview of the encoding procedure. Figure 24.11 illustrates the channel coding applied to voice data. For every 20-ms voice signal there are 50 very important bits (class 1a). A block code adds 3 parity bits. This coding is not error correcting, but only allows detection of bit errors within these 50 bits. The 132 bits of class 1b are attached. After attaching 4 tail bits to determine the final state of the Viterbi decoder, a convolutional code with rate-1/2 is applied. This

Class 2 78 Bits

Parity check

Class lb 132 Bits

|  |  |  |  |
| --- | --- | --- | --- |
| 50 | 3 | 132 | 4 |

Convolutional code rate 1/2  
Constraint length 5

378

78

456 bits per 20 ms speech frame

Figure 24.11 Channel coding for voice data in the Global System for Mobile communications.

Reproduced with permission from Rappaport [1996] © IEEE.

results in 378 bits which are transmitted together with the 78 bits of class 2. Thus, for every 20 ms of the voice signal, 456 bits have to be transmitted. In the following, the details of the different encoder blocks will be discussed.

**Block Encoding**

Block Encoding of Voice Data As discussed above, only class-1a bits of the voice data are encoded using a (53,50) block code. This is a very “weak” block code. It is only supposed to detect bit errors and cannot detect more than three bit errors within the 50 class 1a bits reliably. However, this is sufficient, since a block is completely discarded if an error is detected within the class-1a bits; the receiver then smoothes the resulting signal by “inventing” a block. Figure 24.12 shows the linear shift register representation of the block encoder. As the code is systematic, the 50 data bits pass through the encoder unchanged. However, each of them impacts the state of the shift register. The final state of the shift register determines the 3 parity bits which are attached to the 50 class-1a bits. Class 1a, 1b, and parity check bits are then reordered and interleaved. Finally, four all-zero tail bits are attached, which are needed for the convolutional decoder (see below).

Generator-Polynomial  
G4(D) = D3 + D + 1

1 ... 50 CKL: SW closed 51 ... 53 CKL: SW open

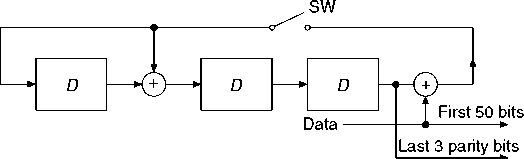


Figure 24.12 Shift register structure for voice block encoding, Cla (53,50) systematic, cyclic block encoder. In this figure: CKL, Clock; SW, Switch.

Reproduced with permission from Steele and Hanzo [1999] © J. Wiley & Sons, Ltd.

Block Encoding of Signaling Data As mentioned in Section 24.4.1, the signaling information has to have stronger protection against bit errors than the voice data. While a bit error in voice-related data might lead to an unintelligible audio signal for 20 ms, a bit error in signaling bits can have a more severe impact - e.g., handover to a wrong cell and therefore loss of connection. Thus, higher redundancy is required. For most of the control channels, only 184 signal bits are transmitted within 20 ms (instead of 260 for speech). This allows better error correction. Signaling bits are encoded with a (224,184) Fire code. The Fire code is defined by the generator polynomial:

G(D) = D40 + D26 + D23 + D17 + D3 + 1 (24.1)

Fire codes are block codes which are particularly capable of correcting burst errors. Burst errors are defined as a series of bit errors, meaning that two or more consecutive bits are wrong; such error bursts occur, e.g., when Viterbi decoding fails (see Chapter 14). A total of 4 tail bits are attached to the resulting 224 bits. The result is fed into the convolutional encoder at code rate-1/2, which is the same as that used for class 1 of the voice signal. For selected logical signaling channels, such as RACH and SCH, different generator polynomials are used. The interested reader is referred to Steele and Hanzo [1999] and the GSM specifications.

**Convolutional Encoding**

Both the class-1 bits of the voice data and all of the signaling information are encoded with a convolutional coder at code rate-1/2 (see Section 14.3). The bits are fed into a 5-bit shift register. For each new input bit, two codebits are calculated according to the generator polynomials

*G1(D) =* 1 + *D + D3 +* D4 *G2(D) =* 1 + D3 + D4

(24.2)

and transmitted. The 4 final tail bits attached to the input sequence ensure that the encoder terminates in the all-zero state at the end of each encoded block.

**Interleaving**

Due to the nature of fading channels, bit errors may occur in bursts in some transmission blocks - e.g., if those blocks were transmitted during a deep fade. Interleaving orders the bits in such a manner that the burst errors due to the channel are (hopefully) distributed evenly (see Section 14.7.1) Evidently, the more the interleaver distributes corrupted bits, the better. However, latency of the speech signal puts an upper limit on interleaver depth: In order to give acceptable speech quality, the delay of the signal should be less than 100 ms.

GSM interleaves the data of two blocks (henceforth called “a” and “b”) in the following way: first, each of the blocks is divided into eight subblocks. Specifically, each bit receives an index i e{0,..., 455}, and the bits are sorted into subblocks with index k e{0,..., 8} according to k = i mod 8. Each subblock of block “a” contributes one half of the bits in a transmission burst (114 bits). The other half is associated with subblocks of either a previous or a succeeding block “b.” Figure 24.13 illustrates diagonal interleaving.

Frame number

i + 0 i + 1 i + 2 i + 3 i + 4 i + 5 i + 6 i + 7

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0a | 4b | 1a | 5b | 2a | 6b | 3a | 7b | 4a | 0b | 5a | 1b | 6a | 2b | 7a | 3b |
| 114 Bits | | 114 Bits | |  | | | | | | | | | | | |

Figure 24.13 Diagonal interleaving for traffic channel/slow associated control channel/fast associated control channel data.

Reproduced with permission from Rappaport [1996] © IEEE.

1. *Cryptography*

One of the most severe shortcomings of analog mobile communications was the ease with which it could be intercepted. Anybody with a frequency scanner was able to eavesdrop on phone conversations. This posed a threat - e.g., for business people dealing with confidential material. Furthermore, even political scandals have been known to develop as a consequence of eavesdropped conversations.

In a digital system, this problem can be solved by “standard” means: once the audio signal is represented by a bitstream, cryptographic procedures, which had long before been developed for military applications, can be easily applied. For GSM, intercepting a conversation requires a man-in-the-middle attack, which involves implementing a BTS, to which the target MS would logon, and forwarding the intercepted signal (to stop the victim noticing the attack) - an exceedingly cumbersome and costly approach. Law enforcement thus typically obtains the collaboration of the network providers, and intercepts conversations not over the air, but after the BTS.

Encryption of the transmitted signal is achieved by simply using an XOR operation on the bits on one hand, and a Pseudo Noise (PN)-sequence on the other hand. A PN-sequence is based on feedback linear shift registers and its periodicity is 3.5 hours. Thus, even knowing the sequence does not enable interception, as the listener has to know which part of the sequence is currently in use. The algorithm for encryption of the data, the A5 algorithm, and algorithms involved in authentication, the A3 and A8, were originally only disclosed to members of the MoU. However, they have been reverse engineered in recent years and successful attacks have been developed. Nevertheless, all these attacks involve a lot of effort and investment. Thus, the GSM air interface still provides the user with a high level of privacy.

1. *Frequency Hopping*

Slow frequency hopping is an optional feature in GSM, where the carrier frequency is changed for each transmission burst (see also Section 18.1). This helps to mitigate small-scale fading: if the carriers employed are separated by more than one coherence bandwidth of the channel (see Chapter 6), each frame is transmitted over a channel with independent fading realization.[[3]](#footnote-3) As the data belonging to one payload (voice data) packet are interleaved over eight bursts, the probability that all of them are transmitted via bad channels is negligible. This makes it more likely that the packet can be reconstructed at the receiver. A similar effect occurs for (narrowband) interference. In either case (fading and interference), frequency hopping leads to an effective whitening of noise and interference.

The coherence bandwidth of GSM channels can vary from several hundred kHz to a few MHz (see Chapter 7). Given that an operator typically owns only a few MHz of spectrum, and only a subset of frequencies can be used in each cell (see Chapter 17), there can be correlation between the frequency channels used for the hopping. Still, frequency hopping provides some advantages even in this case: co-channel interference from other cells, in particular, is whitened.

In order for the receiver to follow the hopping pattern of the transmitter, both link ends have to be aware of the order in which carrier frequencies are to be used. The control sequence governing this pattern can specify hops over up to 64 different carriers, but it may also specify the “degenerated” case (no hopping) in which one frequency is used over and over.

The BS determines the actual frequency hopping sequence by selecting one of a set of predefined PN-sequences and matching this sequence to the available frequencies for the cell. Furthermore, it informs the MS about the hopping sequence as well as the phase of the sequence - i.e., when to start - during call setup (for details see Steele and Hanzo [1999]). Finally, we note that frequency hopping is not applied to the physical channels related to BCHs and CCCHs, as the MS is supposed to “find” them easily.

1. **Equalizer**

Since the symbol duration of GSM is shorter than typical channel delay spreads, ISI occurs, making it necessary to perform equalization (see Chapter 16). However, as GSM is an open standard, neither the structure nor the algorithms of the equalizer are specified. The signal structure just provides the necessary “hooks” (means of implementation), such as a training sequence used to estimate the channel impulse response. The most important properties of the training sequence are as follows:

* The training sequence is 26 bits long.
* It is transmitted in the middle of a burst and, hence, is also called the midamble - it is preceded by 57 data bits, and followed by another 57 data bits.
* Eight different PN-sequences are defined for the midamble - different midambles may be used in different cells, and thus help to distinguish between those cells.

The eight PN-sequences are designed in such a way that their autocorrelation function has a peak of amplitude 26 at zero offset, surrounded by at least five zeros for positive and negative offsets. Therefore, the channel impulse response can be simply estimated by cross-correlating the received midamble with the sequence, as long as the channel impulse response is less than 5 symbol durations long. The cross-correlation thus represents a scaled version of the channel impulse response. This information is used to correct the ISI for all symbols within one burst.[[4]](#footnote-4)

GSM uses a mid amble for training as it is supposed to support MS speeds of up to 250 km/h. At this speed, the MS covers roughly one-eighth of a wavelength during transmission of a burst (500 |is). The impulse response of the channel shows some variations over this distance. Were the training sequence transmitted at the beginning of the burst (preamble), the resulting channel estimate would no longer be sufficiently accurate at the end of the burst. Since training is transmitted in mid-burst, the estimate is still sufficiently accurate at both the start and the end of a burst.

As mentioned above, the GSM standard does not specify any particular equalizer design. Actually, the equalizer is one of the reasons that products from different manufacturers can differ in price and quality. However, most implemented equalizers are Viterbi equalizers. The assumed constraint length of the channel, which relates to the number of states of the trellis, reflects a tradeoff between the complexity and performance of a Viterbi equalizer. Constraint length is identical to the memory of the channel - in other words, the length of the channel impulse response in units of symbol durations. In Chapter 7 we saw that COST 207[[5]](#footnote-5) channel models normally have impulse response lengths of up to 15 |is, which equals 4 symbol durations.[[6]](#footnote-6) We also note that Viterbi equalization can be well combined with convolutional decoding.

We emphasize again that a delay-dispersive fading channel with an appropriate equalizer at the receiver leads to lower average bit error probabilities than a flat-fading channel. As the different versions of a symbol arriving at the receiver at different time instants propagate over different paths, their amplitudes undergo independent fading. In other words, delay dispersion leads to delay diversity (see also Chapter 13).

Table 24.1 summarizes the key parameters of GSM.

1. **Circuit-Switched Data Transmission**

When the GSM standard was originally drafted, voice communication was envisioned as the main application. Some data transmission - like the Short Message Service (SMS) and a point-to-point data transmission channel with a 9.6-kbit/s data rate - were already included, but were not considered sufficiently important to merit the introduction of much additional complexity. Thus, data transmission was handled in a circuit-switched mode, just like voice transmission.

Table 24.1 Key parameters of the Global System for Mobile communications

|  |  |
| --- | --- |
| Parameter | Value |
| Frequency range | |
| GSM900 | 880-915 MHz (uplink) 925-960 MHz (downlink) |
| GSM1800 | 1710-1785 MHz (uplink) 1805-1880 MHz (downlink) |
| GSM1900 | 1850-1910 MHz (uplink - U.S.A.) 1930-1990 MHz (downlink - U.S.A.) |
| Multiple access | FDMA/TDMA/FDD |
| Selection of physical channel | Fixed channel allocation/intracell handover/frequency hopping |
| Carrier distance | 0.2 MHz |
| Modulation format | GMSK (BgT = 0.3) |
| Effective frequency usage per duplex speech | 50-kHz/channel |
| connection | |
| Gross bit rate on the air interface | 271 kbit/s |
| Symbol duration | 3.7 ps |
| Channels per carrier | 8 full slots (13 kbit/s user data) |
| Frame duration | 4.6 ms |
| Maximal RF transmission power at the MS | 2 W |
| Voice encoding | 13 kbit/s RPE-LTP |
| Diversity | Channel coding with interleaving Channel equalization Antenna diversity (optional) Frequency hopping (optional) |
| Maximal cell range | 35 km |
| Power control | 30-dB dynamics |

In general, the circuit-switched data transmission modes of GSM have severe disadvantages. A main issue is the low data rate of less than 10 kbit/s.[[7]](#footnote-7) Furthermore, the long time needed to set up a connection, as well as the relatively high costs of holding a connection, make it very unattractive, e.g., for Internet browsing. There was simply a significant mismatch between the low-data-rate connection-based services offered by GSM, and the new Web applications, which require high data volumes in bursts interrupted by long idle periods. Only SMS text messaging proved to be successful. For these reasons, packet-switched (also known as connectionless) transmission (see Section 17.4) was introduced later on.

1. **Establishing a Connection and Handover**

In this section, we discuss initial establishing of a connection, and the handover procedure, using the logical channels described in Section 24.4. Furthermore, we explore the kind of messages that need to be exchanged during these processes. As a first step, we define various elements of a GSM system that are required for these functionalities.

1. *Identity Numbers*

An MS or a subscriber can be localized within the network by using identity numbers.[[8]](#footnote-8) An active GSM MS has multiple identity numbers.

**Mobile Station ISDN Number (MS ISDN)**

The MS ISDN is the unique phone number of the subscriber in the public telephone network. The MS ISDN consists of Country Code (CC), the National Destination Code (NDC), which defines the regular GSM provider of the subscriber, and the subscriber number. The MS ISDN should not be longer than 15 digits.

**International Mobile Subscriber Identity (IMSI)**

The IMSI is another unique identification for the subscriber. In contrast to the MS ISDN, which is used as the phone number of the subscriber within the GSM network and the normal public phone network, the IMSI is only used for subscriber identification in the GSM network. It is used by the Subscriber Identity Module (SIM), which we explain later, the HLR, and the VLR. It consists again of three parts: the Mobile Country Code (MCC, three digits), the Mobile Network Code (MNC, two digits), and the Mobile Subscriber Identification Number (MSIN, up to ten digits).

**Mobile Station Roaming Number (MSRN)**

The MSRN is a temporary identification that is associated with a mobile if it is not in the area of its HLR. This number is then used for routing of connections. The number consists again of a CC, MNC, and a TMSI, which is given to the subscriber by the GSM network (s)he is roaming into.

**International Mobile Station Equipment Identity (IMEI)**

The IMEI is a means of identifying hardware - i.e., the actual mobile device. Let us note here that the three identity numbers described above are all either permanently or temporarily associated with the subscriber. In contrast, the IMEI identifies the actual MS used. It consists of 15 digits: six are used for the Type Approval Code (TAC), which is specified by a central GSM entity; two are used as the Final Assembly Code (FAC), which represents the manufacturer; and six are used as a Serial Number (SN), which identifies every MS uniquely for a given TAC and FAC.

1. *Identification of a Mobile Subscriber*

In analog wireless networks, every MS was uniquely identified by a single number that was permanently associated with it. All connections that were established from this MS were billed to its registered owner. GSM is more flexible in this respect. The subscriber is identified by his SIM, which is a plug-in chipcard roughly the size of a postage stamp. A GSM MS can only make and receive calls when such a SIM is plugged in and activated.[[9]](#footnote-9) All calls that are made from the MS are billed to the subscriber whose SIM is plugged in. Furthermore, the MS only receives calls going to the number of the SIM owner. This makes it possible for the subscriber to easily replace the MS, or even rent one for a short time.

As the SIM is of fundamental importance for billing procedures, it has to have several security mechanisms. The following information is saved on it:

* Permanent security information: this is defined when the subscriber signs a contract with the operator. It consists of the IMSI, the authentication key, and the access rights.
* Temporary network information: this includes the TMSI, location area, etc.
* Information related to the user profile: e.g., the subscriber can store his/her personal phone- book on the SIM - in this way the phonebook is always available, independent of the MS the subscriber uses.

The SIM can be locked by the user. It is unlocked by entering the Personal Unblocking Key (PUK). If a wrong code is entered ten times, the SIM is finally blocked and cannot be reactivated. Removing the SIM and then plugging it into the same or another MS does not reset the number of wrong trials. This blocking mechanism is an important security feature in case of theft.

The Personal Identification Number (PIN) serves a similar function as the PUK. The user may activate the PIN function, so that the SIM requests a four-digit key every time an MS is switched on. In contrast to the PUK, the PIN may be altered by the user. If a wrong PIN is entered three times, the SIM is locked and may be unlocked only by entering the PUK.

1. *Examples for Establishment of a Connection*

In the following, we give two examples for the steps that are performed when a connection is established. Both the user identification numbers and the different logical channels (see Section 24.4) play a fundamental role in this procedure.

If a subscriber wants to establish a connection from his MS, the following procedure is performed between the MS and the BTS to initialize the connection:

1. The MS requests an SDCCH from the BS by using the RACH.
2. The BS grants the MS access to an SDCCH via the AGCH.
3. The MS uses the SDCCH to send a request for connection to the MSC. This includes the following activities: the MS tells the MSC which number it wants to call. The authentication algorithm is performed; in this context it is evaluated if the MS is allowed to make a requested call (e.g., an international call). Furthermore, the MSC marks the MS as busy.
4. The MSC orders the BSC to associate a free TCH with the connection. The BTS and the MS are informed of the timeslot and carrier number of the TCH.
5. The MSC establishes a connection to the network to which the call should go - e.g., the PSTN. If the called subscriber is available and answers the call, the connection is established.

A call that is incoming from another network starts the following procedure:

1. A user of the public phone network calls a mobile subscriber, or more precisely, an MS ISDN. The network recognizes that the called number belongs to a GSM subscriber of a specific provider, since the NDC in the MS ISDN contains information about the network. The PSTN thus establishes a connection to a gateway MSC[[10]](#footnote-10) of the GSM provider.
2. The gateway MSC looks in the HLR for the subscriber’s information and the routing information (the current location area of the subscriber).
3. The HLR translates the MS ISDN into the IMSI. If call forwarding is activated - e.g., to a voicemail box - the process is altered appropriately.[[11]](#footnote-11)
4. If the MS is roaming, the HLR is aware of the MSC it is connected to, and sends a request for the MSRN to the MSC that is currently hosting the MS.
5. The hosting MSC sends the MSRN to the HLR. The gateway MSC can now access this information at the HLR.
6. As the MSRN contains an identification number of the hosting MSC, the gateway can now forward the call to the hosting MSC. Additional information - e.g., the caller ID - is included.
7. The hosting MSC is aware of the location area of the mobile. The location area is the area controlled by one BSC. The MSC contacts this BSC and requests it to page the MS.
8. The BSC sends a paging request to all the BTSs that cover the location area. These transmit the paging information via the BCH.
9. The called MS recognizes the paging information and sends its request for an SDCCH.
10. The BSC grants access to an SDCCH via the AGCH.
11. Establishment of the connection via the SDCCH follows the same steps as described in bullets 3 and 4 of the “MS-initiated call.” If the mobile subscriber answers the incoming call, the connection is established.
12. *Examples of Different Kinds of Handovers*

A handover is defined as the procedure where an active MS switches the BTS with which it maintains a link; it is a vital part of mobility in cellular communications. Handover is performed when another BTS is capable of providing better link quality than the current one. In order to determine whether another BTS could provide better link quality, the MS monitors the signal strength of the BCH of neighboring BTSs. Since the BCH does not use power control, the MS measures the maximum signal power available from other BTSs. It transmits the results of these measurements to the BSC. Furthermore, the currently active BTS measures the quality of the uplink and sends this information to the BSC. Based on all this information, the BSC decides if and when to initiate a handover. Since the MS contributes to the handover decision, this procedure is called Mobile Assisted Hand Over (MAHO).

Let us now consider some more details in this procedure:

* The received signal strength from different BTSs is averaged over a few seconds (the exact values are selected by the network provider); this ensures that small-scale fading does not lead to a handover. Otherwise, an MS exposed to a similar signal strength from two BTSs would constantly switch from one BTS to the other by just moving over a small distance.
* Receive power is measured at 1-dB resolution in the range of -103 dBm to -41 dBm. The lower bound reflects the sensitivity of GSM receivers - i.e., the minimum signal power required for communication.
* Furthermore, a handover is initialized when the necessary timing advance exceeds the specified limit of 235 |xs. If the MS is so far away from the BTS that a bigger timing advance is necessary, a handover is made to a closer BTS.
* Even more importantly, a handover is initialized when the signal quality becomes too low due to interference.
* The BS transmits (via the BCCH) several parameters that support the handover procedure.

In the following, we describe three different types of HOs: the most simple involves only BTSs controlled by the same BSC. A more complex case arises if two different BSCs are connected to the same MSC. The most complex case involves different MSCs.

**Case 24.1 - Handover between BTSs Belonging to the same BSC**

The steps for this case are illustrated in Figure 24.14:

1. The BSC orders the new BTS to activate a new physical channel.
2. The BSC uses the FACCH of the link between the MS and the old BTS in order to transmit information about the carrier frequency and timeslot of the physical channel for the new BTS.
3. The MS switches to the new carrier frequency and timeslot and sends handover access bursts. These bursts are similar to RACH bursts: they are shorter than normal transmission bursts, as the necessary timing advance is unknown and has to be evaluated first by the new BTS.
4. After the new BTS has detected the handover bursts, it sends the necessary timing advance and power control information to the MS via the FACCH of the new channel.
5. The MS informs the BSC that the handover was successful.
6. The BSC requests the old BTS to switch off the old channel.

2.

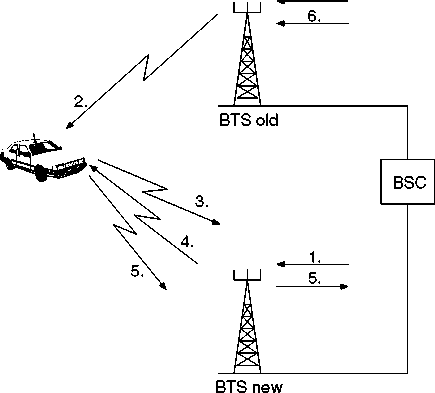


Figure 24.14 Handover between two base transceiver stations of the same base station controller.

**Case 24.2 - Handover between Two BTSs that are Controlled by Different BSCs but the Same MSC**

The steps for this case are illustrated in Figure 24.15.

1. The old BSC informs the MSC that a handover to a specific BTS is necessary.
2. The old MSC knows which BSC controls this BTS (the new BTS) and informs this new BSC about the upcoming handover.

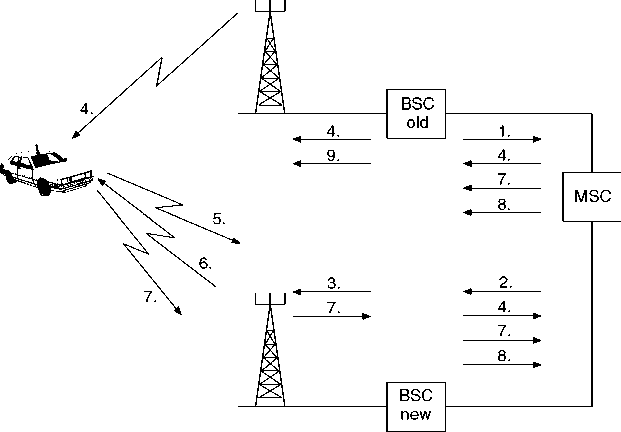


Figure 24.15 Handover between two cells belonging to different base station controllers but the same mobile switching center.

1. The new BSC requests the new BTS to activate a physical channel.
2. The new BSC informs the MS about the carrier frequency and timeslot for the new link. This information goes via the MSC, the old BSC, and the old BTS, and is finally transmitted to the MS on the FACCH of the old BTS.
3. The MS switches to this new carrier frequency and timeslot and transmits access bursts (compare item 3 in Case 24.1).
4. After detecting handover bursts, the BTS transmits information regarding timing advance and power control to the MS via the FACCH.
5. The MS informs the old BSC about the successful handover (via the new BSC and the MSC).
6. The new BSC instructs the old BSC (via the MSC) to relinquish the connection to the MS.
7. The old BSC instructs the old BTS to deactivate the old physical channel.

**Case 24.3 - Handover between Two BTSs which are Associated with Two Different MSCs**

The steps for this case are illustrated in Figure 24.16:

1. The old BSC informs its own MSC (in the following called “MSC-A”) about the necessary handover.
2. MSC-A recognizes that the requested handover involves a BTS associated with another MSC (in the following called “MSC-B”) and contacts this MSC-B.
3. MSC-B associates a handover number with the process, so that it is able to reroute the connection. Subsequently, it informs the new BSC about the upcoming handover.
4. The new BSC orders the new BTS to activate a physical channel.
5. MSC-B gets the information about the carrier frequency and timeslot of the new physical channel and forwards this information to MSC-A. Furthermore, it informs MSC-A about the handover number of the connection.

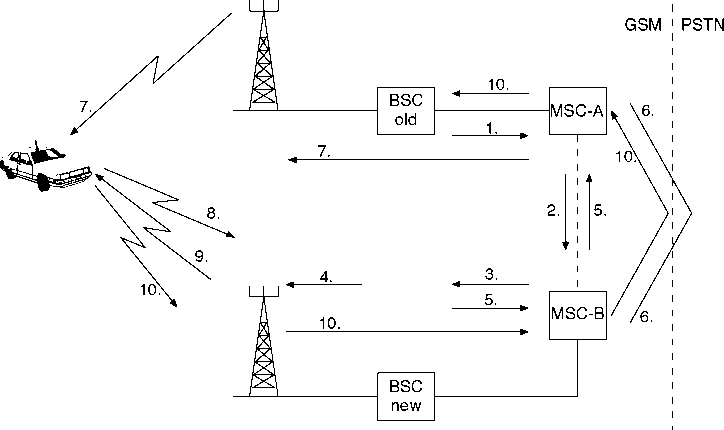


Figure 24.16 Handover between two cells belonging to two different mobile switching centers.

1. A connection between MSC-A and MSC-B is established.
2. MSC-A informs the MS about the carrier frequency and timeslot of the new physical channel. The information goes from MSC-A via the old BSC and the old BTS, whence it is transmitted to the MS via the FACCH.
3. As in Cases 24.1 and 24.2, the MS transmits handover bursts on the new physical channel.
4. After detecting the handover bursts, the new BTS instructs the MS about power control and timing advance.
5. The MS informs MSC-A about the successful handover; this information goes via the new link over the new BTS, the new BSC and MSC-B. From this time on, MSC-A forwards the connection to MSC-B. However, the connection is still maintained by MSC-A. MSC-A acts therefore as a so-called anchor MSC.
6. The old physical channel is deactivated.
7. After the connection ends, the new location area of the MS is established. Therefore, the VLR of MSC-B informs the HLR that the MS is now in its area and the HLR updates its entries regarding the location of the MS. Furthermore, the HLR request the VLR of MSC-A to delete all entries associated with the MS.

We see from these examples that the handover procedure depends on where in the network the

switching centers are located.

1. **Services and Billing**

*24.10.1 Available Services*

In contrast to analog cellular networks, GSM offers a variety of services in addition to regular phone calls. Although providing those services is not a big effort for the network provider, they were a major motivation for customers to switch from analog systems to GSM or another digital mobile phone system. We thus briefly discuss in the following the services offered by GSM, distinguishing between (i) teleservices, (ii) bearer services, and (iii) supplementary services. Teleservices provide a connection between two communication partners, though they may use some additional devices to exchange information via this connection. Bearer services allow the subscriber to access another system. Thus, they provide a connection from the MS to an access point to another network (not a specific terminal in another network). Supplementary services support or manage both teleservices and bearer services.

**Teleservices**

* Regular phone calls: this is still the most common application of GSM.
* Dual Tone Multi Frequency (DTMF): this is a signaling method to allow the subscriber to control a device connected to a phoneline using the keypad of the MS. A typical example is the remote checking of an answering machine connected to a regular landline.
* Emergency calls: calls to emergency numbers have priority in GSM. If a cell is already full, an emergency call leads to interruption of another connection. Remember also that emergency calls can be made from any MS, even without a valid SIM.
* FAX: the protocol that is used to transmit Commite’ Consultatif International de Telegraphique et Telephonique (CCITT) group 3 faxes is incompatible with regular GSM connections. The classical fax protocol was developed to transmit a picture that was converted into a specific digital form over an analog phoneline. GSM, on the other hand, provides either voice connections with a voice-encoding function or data transmission channels for digital data. To send or receive a fax via GSM, adapters are thus required both at the GSM network end and at the MS. The Terminal Adapter Function (TAF) provides a general interface between GSM devices and other devices, and is combined with a special fax adapter.
* SMS: a short message consists of up to 160 alphanumerical characters. A short message may be transmitted from or to an MS. If it is transmitted to an MS that is switched off, the message is accepted by the GSM system and stored in a dedicated database (SMS center). The message is delivered once the MS is switched on and its location is known. This service has turned out to be staggeringly successful, with more than a trillion SMSs sent every year.
* Cell broadcast: a cell broadcast transmits a broadcast message of up to 93 alphanumeric characters to all the MSs within the range of a BTS. This may be used to transmit, e.g., news regarding the local (car) traffic situation.
* Voicemail: the voicemail service allows the subscriber to forward incoming calls to a service center of the GSM network that acts like an answering machine. After listening to a message from the subscriber the calling party may leave a voice message, which the subscriber can retrieve by connecting to this service center. Typically, a subscriber is notified about new messages via SMS.
* Fax mail: this is a service that allows the subscriber to forward incoming faxes to a special service center in the GSM network. The faxes can be retrieved by the subscriber by connecting to this center either with a GSM connection or from the PSTN.

**Bearer Services**

* Connections to the PSTN: this allows the user to connect, e.g., to modems connected to an analog landline.
* Connections to the Integrated Services Digital Network (ISDN): all digital information can be transmitted over the digital network.
* Connections to the packet-switched networks: the user may also access packet-switched networks.

**Supplementary Services**

GSM enables the network provider to offer the subscriber a variety of additional, supplementary

services:

* Call forwarding: the user can select under which conditions calls to his/her mobile number are forwarded to another number: (i) always; (ii) in case the MS cannot be reached; (iii) the user is making or receiving another call; or (iv) the user does not answer after a specified number of rings.
* Blocking of outgoing calls: the user or the provider may block outgoing calls under some of the following conditions: (i) all outgoing calls; (ii) all international calls; or (iii) all international calls, with the exception of those to the country of origin in case the subscriber is abroad.
* Blocking of incoming calls: this feature is of interest when the subscriber has to pay part of (or all of) the charges for an incoming call. The feature may be activated always or when the user is roaming out of the original network.
* Advice of charges: the user may be able to access an estimation of the call charges.
* Call hold: the user may put a connection on hold to make or receive another call and then continue with the first connection.
* Call waiting: during a call, the subscriber may be informed about another incoming call. He/she may either answer this call by putting the other call on hold or reject it. This feature is available for all circuit-switched connections except emergency calls.
* Conference calls: this feature enables connection to multiple subscribers simultaneously. It is only possible for normal voice communications.
* Caller ID: the phone number of the incoming call is displayed.
* Closed groups: subscribers in GSM, ISDN, and other networks may be defined as a specific user group. Members of this group can, e.g., be allowed to make calls only within the group.

1. *Billing*

In GSM, billing for the variety of different subscriber plans is not only an economics issue but also a technical challenge that involves the design of an OSS. In contrast to the regular public phone system, not all fees have to be paid by the party initiating the calls. Furthermore, accounting for supplementary services has to be done separately. To give an impression of the complexity of the accounting involved, we discuss one particular example here.[[12]](#footnote-12)

Example 24.1 *Billing in the Global System for Mobile communications.*

The example involves the following communication parties:

* Subscriber A originates from Austria but is temporarily in Poland.
* Subscriber B is an English subscriber staying in France with a rented MS but his own English SIM.
* Subscriber C is Italian. He is on vacation and the option “If user does not answer, forward call to Subscriber B” is activated.
* Subscriber D is a subscriber to a U.S. service, but is currently in Mexico.

Communication now follows the steps below:

1. Subscriber A calls subscriber C in Italy.
2. As subscriber C is not answering, the call is forwarded to subscriber B.
3. Subscriber B is in France and is currently speaking on his MS. Therefore, subscriber A activates the option “automatic call to busy MS.” Thus, the MS automatically initiates a call the moment the other MS is no longer busy.
4. After subscriber B finishes his conversation, the MS of subscriber A initiates a connection to the MS of subscriber B.
5. This connection is first routed to England, where the HLR of subscriber B is located.
6. From there it gets forwarded to France, where subscriber B is right now.
7. During the conversation, subscriber B needs some information from subscriber D. Therefore, he initiates a “conference call” and calls subscriber D.
8. The call to subscriber D is first routed to the U.S.A. and from there to Mexico, where subscriber D is temporarily staying.

Now the question arises as to which subscriber is charged for which fees?

* Subscriber A has to pay the fees for a call from Poland to Italy. He has to pay both the “international call” charges, and the roaming fees (as he is not in his home country). Furthermore, he has to pay for the service “automatic call to busy MS.”
* Subscriber B has to pay for a connection from England to France (for the incoming call), the charges for an international call (from France to the U.S.A.), and the roaming charges (initiating a call while being in a different network). Further, he has to pay for the “conference call” feature.
* Subscriber C has to pay for the connection from Italy to England and the “call forwarding” feature involved.
* Subscriber D has to pay for a “received call” in the U.S.A. (note that in the U.S.A., the called party pays for a received call the same way as for an active call), and the roaming fees from the U.S.A. to Mexico.

We see that for the same conversation different subscribers get charged different fees depending on their roaming. Subscribers do not have to be actively involved in the conversation to be charged (see subscriber C in the above example). This example gives a taste of the complexity of the billing software in the OSS.

1. **Glossary for GSM**

AB

AC

ACCH

ACM

AGCH

ARFCN

AUC

BCC

BCCH

BCF

Access Burst

Administration Centre

Associated Control CHannel

Address Complete Message

Access Grant CHannel

Absolute Radio Frequency Channel Number

Authentication Center

Base station Color Code

Broadcast Control CHannel

Base Control Function

Broadcast CHannel

BCH

Bm

BN

BNHO

BS

BSC

BSI

BSIC

BSS

BSSAP

BTS

CA

CBCH

CC

CCBS

CCCH

CCPE

CI

CM

CONP

CUG

DB

DCCH

DRM

DTAP

DTE

DTMF

DRX

DTX

EIR

FB

FACCH

FACCH/F

FACCH/H

FCH

FN

GMSC

GSM

HDLC

HLR

HMSC

HSN

IAM

ICB

ID

IMEI

IMSI

ISDN

IWF

Kc

Traffic channel for full-rate voice coder Bit Number

Barring all outgoing calls except those to Home PLMN

Base Station

Base Station Controller

Base Station Interface

Base Station Identity Code

Base Station System

Base Station Application Part

Base Transceiver Station

Cell Allocation

Cell Broadcast CHannel

Country Code

Completion of Calls to Busy Subscribers

Common Control CHannel

Control Channel Protocol Entity

Cell Identify

Connection Management

Connect Number Identification Presentation

Closed User Group

Dummy Burst

Dedicated Control CHannel

Discontinuous Reception Mechanisms

Direct Transfer Application Part

Data Terminal Equipment

Dual Tone Multi Frequency (signalling)

Discontonuous Reception

Discontonuous Transmission Mechanisms

Equipment Identify Register

Frequency correction Burst

Fast ACCH

Full-rate FACCH

Half-rate FACCH

Frequency Correction Channel

Frame Number

Gateway Mobile Services Switching Centre

Global System for Mobile communications

High Level Data Link Control

Home Location Register

Home Mobile-services Switching Centre

Hop Sequence Number

Initial Address Message

Incoming Calls Barred

Identification

International Mobile station Equipment Identity International Mobile Subscriber Identity Integrated Services Digital Network Inter Working Function Cipher Key

|  |  |
| --- | --- |
| Ki  Kl  Ks  LAC  LAI  LAP  LPC  LR  MA  MACN  MAF  MAIO  MAP  MCC  ME  MEF  MIC  MNC  MS  MSC  MSCU  MS  MSL  MSRN  MT  MTP  MUMS  NB  NBIN  NCELL  NDC  NF  NM  NMC  NMSI  NSAP  NT  OACSU  O&M  OCB  OMC  OS  PAD  PCH  PIN  PLMN  PSPDN  PSTN  PTO  RA | Key used to calculate SRES Location Key Session Key Location Area Code Location Area Identify  hyphen;Dm Link Access Protocol on Dm Channel Linear Prediction Coding (Voice Codec)  Location Register Mobile Allocation Mobile Allocation Channel Number Mobile Additional Function Mobile Allocation Index Offset Mobile Application Part Mobile Country Code Maintenace Entity Maintenace Entity Function Mobile Interface Controller Mobile Network Code Mobile Station  Mobile-services Switching Centre Mobile Station Control Unit ISDN Mobile Station ISDN Number Main Signaling Link Mobile Station Roaming Number Mobile Terminal Message Transfer Part Multi User Mobile Station Normal Burst  A parameter in the hopping sequence  Neighbouring (adjacent) Cell  National Destination Code  Network Function  Network Management  Network Management Centre  National Mobile Station Identification number  Network Service Access Point  Network Termination  Off Air Call Set Up  Operations & Maintenance  Outgoing Calls Barred  Operations & Maintenance Center  Operating Systems  Packet Assembly/Disassambly facility Paging CHannel Personal Identification Number Public Land Mobile Network Public Switched Public Data Network Public Switched Telephone Network Public Telecommunications Operators Random Mode Request information field |

|  |  |
| --- | --- |
| RAB | Random Access Burst |
| RACH | Random Access Channel |
| RFC | Radio Frequency Channel |
| RFN | Reduced TDMA Frame Number |
| RLP | Radio Link Protocol |
| RNTABLE | Table of 128 integers in the hopping sequence |
| RPE | Regular Pulse Excitation (Voice Codec) |
| RXLEV | Received Signal Level |
| RXQUAL | Received Signal Quality |
| SABM | Set Asynchronous Balanced Mode |
| SACCH | Slow Associated Control Channel |
| SACCH/C4 | Slow, SACCH/C4 Associated Control CHannel |
| SACCH/C8 | Slow, SACCH/C8 Associated Control CHannel |
| SACCH/T | Slow, TCH Associated Control CHannel |
| SACCH/TF | Slow, TCH/F Associated Control CHannel |
| SACCH/TH | Slow, TCH/H Associated Control CHannel |
| SAP | Service Access Points |
| SAPI | Service Access Points Indicator |
| SB | Synchronization Burst |
| SCCP | Signalling Connection Control Part |
| SCH | Synchronisation CHannel |
| SCN | Sub Channel Number |
| SDCCH | Standalone Dedicated Control CHannel |
| SDCCH/4 | Standalone Dedicated Control CHannel/4 |
| SDCCH/8 | Standalone Dedicated Control CHannel/8 |

1. **Appendices**

Please go to [www.wiley.com/go/molisch](http://www.wiley.com/go/molisch)

**Further Reading**

This current chapter is of course only a brief overview of GSM technology. Much more detailed information may be found in the GSM specifications. Note, however, that they encompass 5,000 pages and are also written as a technical specification and not as a textbook, and most engineers only read small sections of them. Another useful source of information is the monograph by Mouly and Pautet [1992]. A detailed GSM chapter can also be found in Steele and Hanzo [1999], Steele et al. [2001], and Schiller [2003]. GPRS is discussed in Cai and Goodman [1997]; Bates [2008]; GSM network aspects are discussed in Eberspaecher et al. [2009].

For updates and errata for this chapter, see wides.usc.edu/teaching/textbook

1. A Location Area (LA) is a set of cells, within which the MS can roam without updating any location information in its HLR. [↑](#footnote-ref-1)
2. Nevertheless, this option is not implemented by most providers. [↑](#footnote-ref-2)
3. This is particularly important if the MS is not moving: without frequency hopping, it would “see” the same channel at all times; thus if it is in a fading dip, the Bit Error Rate (BER) would be very high. [↑](#footnote-ref-3)
4. Note that the SCH and the RACH use longer training patterns. To simplify implementation, the same algorithm is normally used for equalization of all three different bursts. [↑](#footnote-ref-4)
5. COST stands for European COoperation in the field of Scientific and Technical research. [↑](#footnote-ref-5)
6. Note that the constraint length of a Viterbi equalizer can be required to be longer due to other effects - e.g., ISI due to the GMSK. Therefore, 4-6 is a practical value for constraint length. [↑](#footnote-ref-6)
7. The High Speed Circuit Switched Data (HSCSD) mode provides higher data rates based on circuit-switched transmission. [↑](#footnote-ref-7)
8. Note that we distinguish between a subscriber and the hardware (s)he is using. [↑](#footnote-ref-8)
9. Emergency calls can be made without a SIM. [↑](#footnote-ref-9)
10. A gateway MSC is an MSC with a connection to the regular phone network. [↑](#footnote-ref-10)
11. This information is found in the HLR as well. [↑](#footnote-ref-11)
12. Note that we base the discussion of this example partly on European billing procedures. This is fundamentally different from U.S. billing. In the U.S.A., mobile numbers are similar to landline numbers. Therefore, the calling party just pays the regular fees for a landline call, whereas the mobile subscriber pays the landline-to-mobile fees even for incoming calls. [↑](#footnote-ref-12)