경동대학교
KYUNGDONG UNIVERSITY

BACHELOR OF SMART COMPUTING.

DATACOMMUNICATION AND TELECOMMUNIACTION SYSTEMS

GROUP PRESENTATION

GSM

GROUP 1

MIKAEL GOMBE TENGEMANO - 2217160
LYIMO JOHNSON SAMWEL – 2217141
JEAN PIERRE DUFITUMUKIZA- 2217059
ANTONY SUSANI MREFU – 2217152
MESHACK TIROP-2217164

GROUP: A
PROFESSOR: BASEEM

Contents

PART 01: INTRODUCTION TO GSM 3
1.1 GSM stands for Global System for Mobile Communication. 3
1.2 GSM subsystems. 4
1.3 Examples of gsm technologies: 4
1.4 How gsm develop over the years: 5
PART 2: GSM NETWORK COMPONENTS 6
2.1 mobile station (ms) 6
2.2 base station subsystem (bss) 6
2.3 network and switching subsystem (nss) 7
PART 3: GSM COMMUNICATION AND PROTOCOLS 8
3.1 Gsm communication process 8
3.2 gsm air interface 10
3.3 gsm protocols 11
PART 4.GSM SERVICES 13
4.1 teleservices 14
PART 5: SECURITY AND EVOLUTION OF GSM 21
5.1 Gsm security features 21
5.2 Challenges and Vulnerabilities 21
5.3 Evolution of GSM 21
5.4 Future Prospects 22
5.5 Open-Source GSM Software 22
Conclusion 22
References 23

PART 01: INTRODUCTION TO GSM

1.1 GSM stands for Global System for Mobile Communication.

Mobile services based on GSM were first launched in Finland in 1991.The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories .

GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.

GSM is the most widely accepted standard in telecommunications and it is implemented globally.GSM is an open and digital cellular technology used for mobile communication. It uses 4 different frequency bands of 850 MHz, 900 MHz, 1800 MHz and 1900 MHz .

GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.

It uses the combination of FDMA and TDMA(*Overview of the GSM System and Protocol Architecture. IEEE Communications Magazine, 31(4), 92–100 | 10.1109/35.210402*, n.d.)

FDMA(FREQUENCY DEFINITION MULTIPLE ACCESS)

FDMA assigns individual channels to individual users. These channels are assigned on demand to subscribers who request service. Guard bands are maintained between adjacent signal spectra to minimize cross talk between channels. During the period of the call, no other user can share the same frequency band. In frequency division duplex (FDD) systems, the users are assigned a channel as a pair of frequencies; one frequency is used for the upward channel, while the other frequency is used for the downward channel.

TDMA(TIME DEFINITION MULTIPLE ACCESS)

Time Division Multiple Access (TDMA) is a digital modulation technique used in digital cellular telephone and mobile radio communication. TDMA is one of two ways to divide the limited spectrum available over a radio frequency (RF) cellular channel. TDMA enables multiple users to share the same frequency by dividing each cellular channel into different time slots. In effect, a single frequency supports multiple and simultaneous data channels. So, with

a two-time slot TDMA, two users can share the same frequency. With a three-time slot TDMA, three users can share the same frequency and so on.

1.2 GSM subsystems.

- **BSS** : BSS stands for Base Station Subsystem. BSS handles traffic and signaling between a mobile phone and the network switching subsystem.

- **NSS** : NSS stands for Network and Switching Subsystem. NSS is the core network of GSM. That carried out call and mobility management functions for mobile phone present in network. NSS have different components like VLR, HLR and EIR.

- **OSS :** OSS stands for Operating Subsystem. OSS is a functional entity which the network operator monitor and control the system. Purpose of OSS is to offer the customer cost-effective support for all GSM related maintenance services.

1.3 Examples of gsm technologies:

1. Basic Voice calls:

Making and receiving phone calls is one of the simplest and most fundamental uses of GSM technology. This uses standard GSM voice channels, which operate on circuit-switched network.

2. SMS (Short Message Service):

Sending and receiving text messages is widely used and very simple feature of GSM technology. Most phones have a dedicated messaging app.

3. USSD (Unstructured Supplementary Service Data):

USSD codes e.g. (*123#) allow users to check balances, access services and perform various tasks without needing internet access. These are often used for quick, interactive sessions with the service provider. Messages travel over GSM signaling channels and realtime sessions between the user and the service provider

1.4 How gsm develop over the years:

1982 Conference of European Posts and Telegraph (CEPT) establishes a GSM group to widen the standards for a pan-European cellular mobile system.

1985 A list of recommendations to be generated by the group is accepted.

1986 Executed field tests to check the different radio techniques recommended for the air interface.

1987 Time Division Multiple Access (TDMA) is chosen as the access method (with Frequency Division Multiple Access [FDMA]). The initial Memorandum of Understanding (MoU) is signed by telecommunication operators representing 12 countries.

1988 GSM system is validated.

1989 The European Telecommunications Standards Institute (ETSI) was given the responsibility of the GSM specifications.

1990 Phase 1 of the GSM specifications is delivered.

1991 Commercial launch of the GSM service occurs.

1992 The addition of the countries that signed the GSM MoU takes place. Coverage spreads to larger cities and airports.

1993 Coverage of main roads GSM services starts outside Europe.

1994 Data transmission capabilities launched. The number of networks rises to 69 in 43 countries by the end of 1994.

1995 Phase 2 of the GSM specifications occurs. Coverage is extended to rural areas.

1996 June− 133 network in 81 countries operational.

1997 July− 200 network in 109 countries operational, around 44 million subscribers worldwide.

1999 Wireless Application Protocol (WAP) came into existence and became operational in 130 countries with 260 million subscribers.

2000 General Packet Radio Service(GPRS) came into existence.

2001 As of May 2001, over 550 million people were subscribers to mobile telecommunications. (Eberspächer et al., 2008)

PART 2: GSM NETWORK COMPONENTS

2.1 mobile station (ms)

The Mobile Station (MS) is the end-user device in a GSM network, comprising:

Subscriber Identity Module (SIM):

Security and Subscriber Information: The SIM card securely holds the International Mobile Subscriber Identity (IMSI) and a secret key used for authentication. It stores the subscriber's personal data, network information, and service-related details.(Redl, 2014)

Phone Locking Mechanisms: These include methods like Personal Identification Number (PIN) codes, passwords, and biometric systems (fingerprints, facial recognition) that restrict unauthorized access to the phone and its data, enhancing user security.(Lo & Chen, 1999)

2.2 base station subsystem (bss)

The BSS handles communication between the Mobile Station (MS) and the Network and Switching Subsystem (NSS). It consists of:

Base Transceiver Station (BTS):

Each BTS manages the radio communication with mobile stations within its cell. It handles tasks like frequency allocation, channel coding, and encryption to ensure secure and efficient transmission of data and voice.

Base Station Controller (BSC):

The BSC controls multiple BTS units, coordinating radio resources and handovers. It also manages power levels, frequency assignments, and the allocation of radio channels to ensure seamless connectivity and efficient use of resources.

Functions and Interactions: The BTS and BSC work in tandem to maintain continuous communication as mobile stations move through different cells. The BSC handles handovers between BTS units, ensuring uninterrupted service, while the BTS manages direct communication with the mobile devices.

2.3 network and switching subsystem (nss)

The NSS forms the core of the GSM network, managing call routing, subscriber information, and mobility. Key components include:

Mobile Switching Center (MSC):

The MSC is the central node that routes calls, manages call setup, and handles termination. It also manages handovers between different BSCs and interfaces with other networks, ensuring seamless call connectivity.

Home Location Register (HLR):

The HLR is a central database storing permanent subscriber information, such as service profiles, roaming agreements, and authentication keys. It keeps track of the subscriber's current location and status within the network.

Visitor Location Register (VLR):

The VLR temporarily holds information about subscribers currently in the area covered by its associated MSC. It interacts with the HLR to update the subscriber’s location and manages temporary data needed for call handling and other services.

Authentication Center (AUC):

The AUC is responsible for generating and managing security parameters, including authentication keys and encryption algorithms. It authenticates users by verifying their credentials stored in the SIM against network data, ensuring secure access to network services.

Equipment Identity Register (EIR):

The EIR maintains a list of mobile equipment identifiers (IMEIs) to track authorized, stolen, or defective devices. By cross-referencing this database, the network can block unauthorized or stolen devices, ensuring only approved equipment can access the network.

PART 3: GSM COMMUNICATION AND PROTOCOLS

3.1 Gsm communication process

Call Setup and Teardown

The call setup process in GSM involves several stages, ensuring that a call can be initiated and connected seamlessly.

When a user initiates a call, the mobile station (MS) sends a service request to the network.

This request is routed through the Base Transceiver Station (BTS) to the Base Station Controller (BSC) and then to the Mobile Switching Center (MSC).

The MSC is responsible for setting up the call, which involves allocating the necessary channels and resources to connect the call to the intended recipient.

Once the call setup is complete, the call can proceed with the exchange of voice or data communication. The teardown process occurs when either party terminates the call.

The MS sends a disconnect message to the network, which then releases the resources used for the call. This ensures that the channels are available for other users and that the network maintains optimal performance.

Handover Procedures

Handover procedures are crucial in GSM to maintain call continuity as a user moves between cells. There are two main types of handovers in GSM: intra-cell handover and inter-cell handover.

Intra-cell Handover: This occurs within the same cell, typically to balance the load across different frequencies or to reduce interference. For example, if a user experiences poor signal quality, the network may switch the user to a different frequency within the same cell to improve the call quality.

Inter-cell Handover: This occurs between different cells and is more common as users move through the coverage area. The BSC and MSC manage inter-cell handovers to ensure that an ongoing call is maintained without interruption. The handover process involves measuring the signal strength and quality, selecting the best candidate cell, and transferring the call to the new cell.

Handover procedures are designed to be seamless, allowing users to move freely without experiencing dropped calls or interruptions in service.

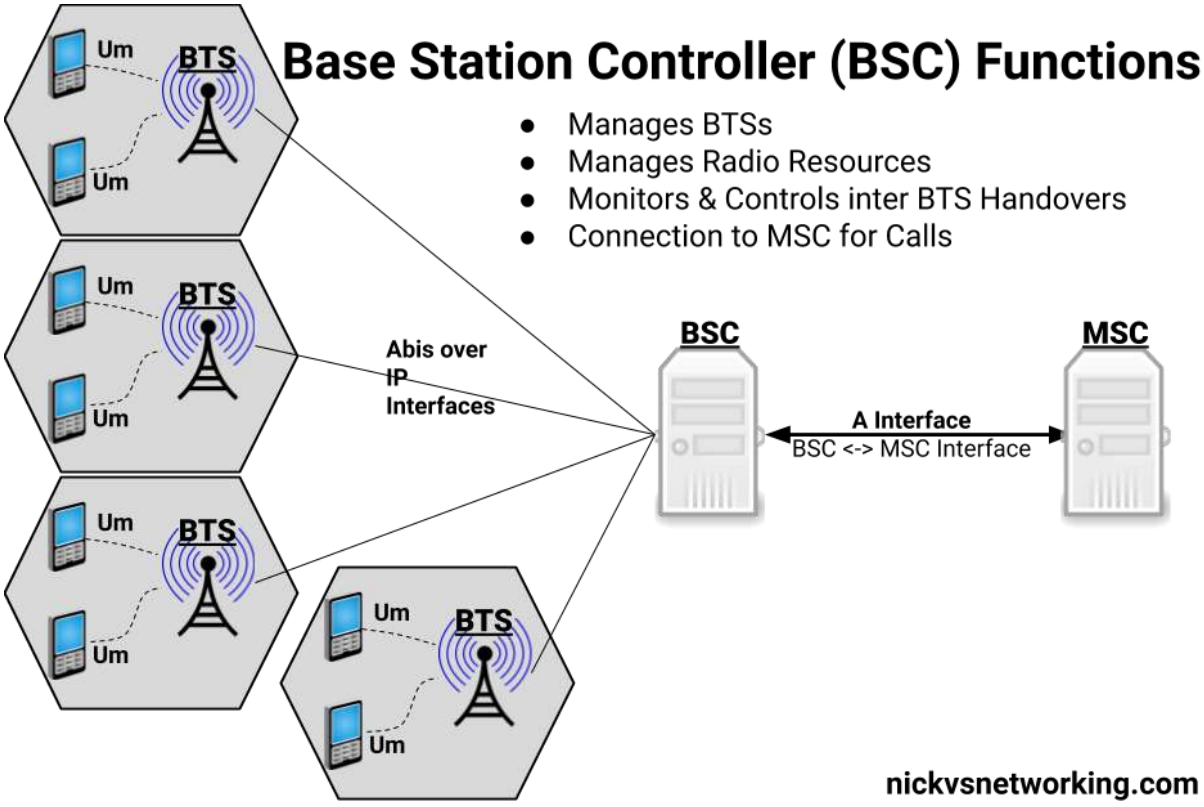

Figure 1Base Station Controller Functions

Roaming Mechanisms

Roaming enables users to access mobile services while outside their home network, ensuring global connectivity.

When a user enters a new network area, the mobile station registers with the new network, updating its location information in the Visitor Location Register (VLR) of the visited network. This process involves several key steps:

Location Update: The mobile station sends a location update request to the new network. The request is routed through the BTS, BSC, and MSC to the VLR.

Authentication: The visited network authenticates the user by communicating with the Home Location Register (HLR) of the user's home network. This ensures that the user is authorized to access services.

Roaming Agreements: Roaming is facilitated through agreements between network operators, allowing users to seamlessly connect to and use services in different network areas.

Roaming mechanisms ensure that calls and services are correctly routed, billing is accurate, and users experience uninterrupted service while traveling.

3.2 gsm air interface

Frequency Bands and Channels

GSM operates across several frequency bands to provide flexibility and wide coverage. The primary frequency bands used are 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz These frequency bands are divided into multiple channels to accommodate a large number of users. (Eberspächer et al., 2008)

Each frequency band is further split into smaller channels, which are used for communication between the mobile station and the network. This division allows GSM to support a high density of users, ensuring efficient use of the available spectrum.

Time Division Multiple Access (TDMA)

Time Division Multiple Access (TDMA) is a key technology used in GSM to maximize the use of available bandwidth. TDMA divides each frequency channel into multiple time slots,

allowing several users to share the same frequency channel by transmitting in different time slots.

In a typical GSM system, each frequency channel is divided into eight time slots. Each user is assigned a specific time slot for transmission and reception. This allows multiple users to share the same frequency without interfering with each other, as each user transmits in rapid succession during their assigned time slot.

TDMA increases the capacity of the network, allowing more users to be served simultaneously and improving the efficiency of the spectrum.

Frequency Hopping

Frequency hopping is a technique used in GSM to improve signal quality and reduce interference. This involves periodically changing the carrier frequency during transmission. By hopping between different frequencies, GSM systems can avoid prolonged interference on a single frequency and make it harder for unauthorized parties to intercept communications.

Frequency hopping also enhances the robustness of the communication link, providing better resistance to multipath fading and improving overall signal quality. This technique is particularly useful in environments with high levels of interference or in areas where spectrum availability is limited.

3.3 gsm protocols

Layered Protocol Architecture

GSM's protocol architecture is designed to provide efficient and reliable communication through a layered structure. The architecture is divided into three main layers: :(Eberspächer et al., 2008)

- Layer 1 (Physical Layer): The physical layer is responsible for the transmission and reception of raw data bits over the air interface. It handles the modulation, demodulation, encoding, and decoding of signals. This layer ensures that data is transmitted accurately over the radio link.

- Layer 2 (Data Link Layer): The data link layer ensures reliable data transfer across the network. This layer manages error detection and correction, flow control, and frame synchronization.
- Layer 3 (Network Layer): The network layer manages network functions and is divided into three sublayers:

- Radio Resource (RR) Management: This sublayer is responsible for managing the allocation and management of radio channels. It handles tasks such as channel assignment, handovers, and power control, ensuring efficient use of radio resources and maintaining the radio link between the mobile station and the network.
- Mobility Management (MM): The MM sublayer manages user mobility, including location updating, registration, authentication, and handovers. It ensures that the network can track the user's location and provide seamless service as the user moves.
- Connection Management (CM): The CM sublayer is responsible for call setup, maintenance, and termination, as well as supplementary services and SMS. It includes protocols for call control, managing the establishment, maintenance, and release of voice and data calls, and handling supplementary services such as call forwarding and call waiting.

Key Protocols

GSM employs several key protocols within its layered architecture to manage various aspects of communication:

Radio Resource (RR): The RR protocol is responsible for ensuring the availability and maintenance of radio channels. It handles channel assignment, handovers, and power control, ensuring efficient use of radio resources and maintaining the quality of the radio link.(*GSM - Architecture, Protocols and Services - Jörg Eberspächer, Hans-Joerg Vögel, Christian Bettstetter, Christian Hartmann - Google Books*, n.d.)

Mobility Management (MM): The MM protocol manages functions related to subscriber mobility, including location updating, authentication, and security measures. It ensures that the network can track the user's location and provide seamless service as the user moves.

Connection Management (CM): The CM protocol is responsible for call control, managing the establishment, maintenance, and release of voice and data calls. It also handles supplementary services such as call forwarding and call waiting, and SMS management.

These protocols work together to provide a comprehensive and reliable communication system, ensuring efficient use of resources, seamless mobility, and high-quality service for users.

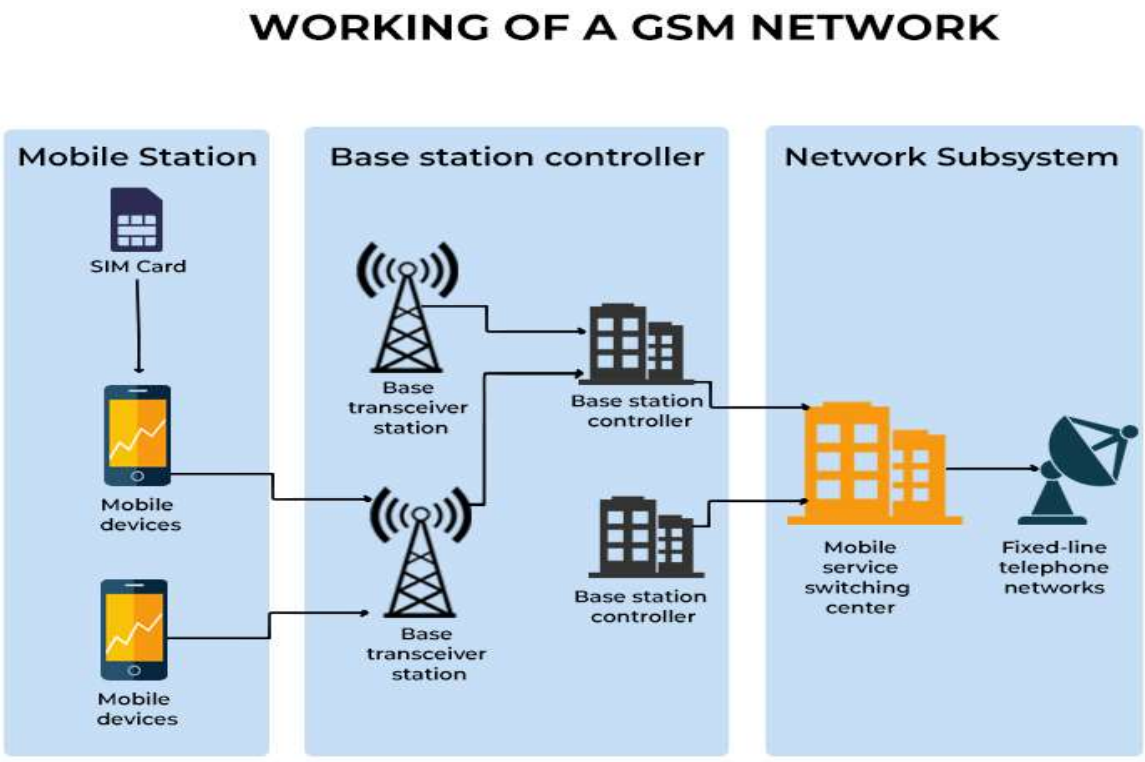

Figure 2 Working of GSM

PART 4.GSM SERVICES

It is important to note that all the GSM services were not introduced since the appearance of GSM but

They have been introduced in a regular way. The GSM Memorandum of Understanding (MoU) defined(Vedder, 1998)

Four classes for the introduction of the different GSM services:

- E1: introduced at the start of the service.
- E2: introduced at the end of 1991
- Eh: introduced on availability of half-rate channels.

- A: these services are optional.

Three categories of services can be distinguished:

- Teleservices.
- Bearer services.
- Supplementary Services.

4.1 teleservices

Voice

Voice services has to implemented by each operator in the start-up phase (E1) by 1991.In this part two teleservices were distinguished: regular telephone service (TS11) and emergency services (TS12). For the transmission of the digitally coded speech signals, both services use a bidirectional, symmetric, full-duplex, point-point connection which is set up on user demand. The sole difference between TS11 and TS12 teleservices is that regular services require an international IWF, whereas the emergency service stays within the boundaries of a national network

Fax Transmission

For the second phase (E2) of teleservices, Implementation of transparent fax services (TS61) was planned. It is called transparent because it uses a transparent bearer service for the transmission of fax data. The coding and transmission of the facsimile data uses the fax protocol according to the ITU-T recommendation T30.The network operator also has the option to implement TS61 on a nontransparent bearer service in order to improve the transmission quality.TS61 is transmitted over traffic channel that is alternately used for voice or fax. Another optional alternative is designed as a fax transfer with automatic call acceptance (TS61). These services can be offered by a network operator when multinumbering is used as the internetworking solution. In the case of multinumbering, a subscriber is designed several MSISDN numbers, and separate internetworking profile is stored for each of them. In this way a specific teleservice can be associated with each MSISDN, the fax service being one of them. If a mobile subscriber is called on their GSM-fax number, required resources in the IWF of the MSC as well as in the MS can be activated; in the case of TS61, fax calls arrive with the same number as voice (multinumbering) and have to be switched over to fax reception manually.(Stuckmann, 2003)

SMS

Short Message Service (more commonly known as text messaging) has become the most used data application on mobile phones, with 74% of all mobile phone users worldwide already as active users of SMS, or 2.4 billion people by the end of 2007.

SMS text messages may be sent by mobile phone users to other mobile users or external services that accept SMS. The messages are usually sent from mobile devices via the Short Message Service Centre using the MAP protocol.

The SMSC is a central routing hub for Short Messages. Many mobile service operators use their SMSCs as gateways to external systems, including the Internet, incoming SMS news feeds, and other mobile operators (often using the de facto SMPP standard for SMS exchange).

For SMS, the network operator has to establish a service centre which accepts short messages from the fixed network and processes them in a store and forward mode. The interface has not been specified and can be by DTMF signalling, special order, email, fax etc. The delivery can be time shifted and is of course independent of the current location of the MS. Conversely, a service centre can accept short messages from MSs which can also be forwarded to subscribers in the fixed network, for example by fax or email. The transmission of short messages uses a connectionless, protected, packet-switching protocol. The reception of a message must be acknowledged by the MS or the service Centre; in the case of failure, retransmission occurs.TS21 and TS22 are the only teleservices which can be used simultaneously with other services, i.e. short messages can also be received or transmitted during an ongoing call.

A further variation of the SMS is the cell broadcast service TS23, SMSCB.SMSCB messages are broadcast only in a limited region of the network. They can only be received by MSs in idle mode, and reception is not acknowledged. A MS itself cannot send SMSCB messages. With this service, message contain category designation, so that MSs can select categories of interest which they want to receive and store. The maximum length of SMSCB messages is 93

character but using a special reassembly mechanism, the network can transmit longer messages of up to 15 subsequent SMSCB messages.

Emergency Calls in GSM Networks

This is a function which ensure user to reach emergency services like police, ambulace, fire brigade in a quick way and reliably in a critical condition

Functionality

- GSM phones are programmed with universal emergency numbers like 112, which work even without a SIM card .
- The phone attempts to connect to the nearest emergency service provider (police, ambulance, fire) based on your location when you dial an emergency number.
- The network prioritizes emergency calls, attempting to connect them even in case of congestion.
- In some cases, even without network reception, emergency calls might connect through special agreements with other operators .

Process

- Dialing: When you dial an emergency number on your GSM phone, the network identifies it as a priority call.
- Network Routing: The network utilizes various methods to determine your location, including cell tower triangulation and A-GPS (Assisted Global Positioning System) if available. This location data is crucial for routing your call to the appropriate emergency service provider in your area.
- Call Connection: The network attempts to connect you to the emergency service provider using the available GSM channels.
- Information Gathering: Once connected, the emergency service dispatcher will ask for details about your emergency and location to provide the most effective assistance.

Importance:

- Emergency calls provide a critical lifeline in times of accidents, medical emergencies or security threats.
- The universality of emergency numbers like 112 ensures easy access to help regardless of location or network provider within GSM coverage areas.

Data Services (or Bearer Services)

Data services, also known as bearer services, are a fundamental category of functionalities offered by GSM networks. These services allow mobile phone users to transmit and receive data packets, enabling a wide range of applications beyond basic voice communication. Below are categories of it;

General Packet Radio Service (GPRS):

General Packet Radio Service (GPRS) is a pioneering technology that introduced packet-based data transmission to GSM networks. It marked a significant leap forward from the traditional circuit-switched voice calls of GSM, enabling basic internet access and laying the groundwork for the mobile internet revolution.(Brasche & Walke, 1997) Here's a deep dive into GPRS:

Function:

- Unlike circuit-switched voice calls, which dedicate a channel for the entire duration of the call, GPRS utilizes a packet-based approach.
- Data is broken down into smaller packets, transmitted over available channels in the network, and reassembled at the receiving end.
- This method allows for more efficient network utilization as multiple users can share the same channel without interrupting each other.

Application

- Enables basic functionalities like:
- Slow internet browsing: Accessing web pages with text and basic images.
- Email access: Sending and receiving emails with limited attachments.
- Simple file transfer: Sharing smaller documents and images between devices.

- ➢ Basic mobile apps: Utilizing applications with limited data requirements.

Limitations:

- ➢ Slow Speeds: Data transfer rates were relatively slow, typically ranging from 56 kbps to 114 kbps, making activities like video streaming or large file downloads impractical.
- ➢ Latency: Delays in data transmission could be noticeable, impacting applications requiring real-time responsiveness.

Enhanced Data Rates for GSM Evolution (EDGE):

Enhanced Data Rates for GSM Evolution (EDGE), also known as EGPRS or IMT Single Carrier (IMT-SC), was a crucial advancement in GSM technology. It aimed to address the limitations of General Packet Radio Service (GPRS) by offering improved data transfer rates for mobile devices. Here's a detailed explanation of EDGE: (Halonen et al., 2004)

Function:

- ➢ Building upon GPRS, EDGE employed more sophisticated modulation techniques to transmit data more efficiently.
- ➢ It primarily utilized 8-Phase Shift Keying (8PSK) modulation, which could transmit 3 bits of information per symbol compared to the single bit per symbol in GPRS (using Gaussian Minimum Shift Keying - GMSK).
- ➢ This allowed for a significant increase in data throughput without requiring major changes to the existing GSM network infrastructure.

Improvements and Applications:

Compared to GPRS, EDGE offered:

- ➢ Increased data transfer rates: Theoretical peak rates of up to 384 kbps, with typical real-world speeds ranging from 100 kbps to 250 kbps.
- ➢ Enhanced user experience: This improvement allowed for faster web browsing, more efficient email with attachments, and even basic video streaming (depending on network conditions).

Benefits and Impact:

- ➢ EDGE played a vital role in bridging the gap between the limited data capabilities of GPRS and the faster speeds offered by 3G technologies.
- ➢ It provided a noticeable improvement in mobile data usability, allowing users to experience a more web-connected mobile experience.

Supplementary Services

This is a category features in which it acts as an ass-ons that enhance the user experience and provide more control over communication.

Function:

- ➢ Supplementary services modify or extend the capabilities of basic telephony and data services offered by GSM.
- ➢ They are activated and managed through user codes or menus on the mobile phone.

Common Supplementary Services:

Call forwarding: This allows you to divert incoming calls to another number, such as your voicemail or another phone. It offers flexibility in managing your calls based on your availability or preferences.

Call waiting: This alerts you when you have a new incoming call while you are already on a call. It gives you the option to answer the new call, put the current call on hold, or even conference them together.

Call barring: This allows you to block incoming, outgoing, or both types of calls. It can be useful for managing call costs, preventing unwanted calls, or controlling accessibility.

Caller ID: This service displays the phone number of the person calling you on your phone's screen. It helps you identify incoming calls and decide whether to answer.

Multiparty conferencing: This allows you to have a call with more than two people, facilitating group conversations.

Call hold: This allows you to put a call on hold while you answer another incoming call or attend to other tasks. You can then resume the held call at your convenience.

Call transfer: This allows you to seamlessly transfer a call to another number, often used to connect callers with the appropriate person within an organization.

Short Message Service (SMS) waiting: This alerts you when you receive a new SMS message while you are on a call or using another application.

Advice of Charge (AoC): This service provides an estimated cost of a call before you connect, allowing you to manage call expenses.

Benefits of Supplementary Services:

- ➢ Increased call management flexibility.
- ➢ Improved accessibility and control over incoming and outgoing calls.
- ➢ Enhanced user experience for various communication scenarios.

Availability and Usage:

- ➢ The availability of specific supplementary services might vary depending on your network operator and subscription plan.
- ➢ Users typically activate and manage these services through USSD codes (Unstructured Supplementary Service Data) or menus on their mobile phones.

Evolution and Future:

- ➢ Many supplementary services introduced in GSM networks continue to be relevant and valuable features in modern mobile communication, even with the emergence of new technologies.
- ➢ Some functionalities might be integrated into the core services or offered through applications as technology evolves.

PART 5: SECURITY AND EVOLUTION OF GSM

5.1 Gsm security features

Authentication and Encryption (A5/1, A5/2): GSM uses a challenge-response mechanism for authentication. The process involves a secret key (Ki) stored in the SIM card and the network's Authentication Center (AuC). A random number (RAND) is sent to the mobile station (MS), which computes a signed response (SRES) using Ki. The network then verifies SRES to authenticate the user. For encryption, GSM uses the A5 family of algorithms. A5/1 is a stronger encryption algorithm, while A5/2 is weaker and was intended for export.

TMSI (Temporary Mobile Subscriber Identity): To protect subscriber privacy, GSM uses a Temporary Mobile Subscriber Identity (TMSI) instead of the IMSI (International Mobile Subscriber Identity). This temporary identifier reduces the risk of tracking and eavesdropping.

Key Generation and Management: Key management in GSM involves generating session keys for encryption. The session key (Kc) is derived from the RAND and Ki during the authentication process. These keys are managed securely to maintain the integrity and confidentiality of communications.

5.2 Challenges and Vulnerabilities

Security Weaknesses and Attacks: GSM has known vulnerabilities, such as weak encryption in A5/2 and the potential for IMSI catchers (fake base stations) to intercept and track communications. Cryptographic weaknesses and the lack of mutual authentication between the MS and the network also pose risks.

Measures to Enhance GSM Security: Enhancing GSM security involves adopting stronger encryption algorithms (e.g., A5/3), implementing mutual authentication, and regularly updating security protocols. Network operators can also use more sophisticated intrusion detection systems to monitor and respond to security threats.

5.3 Evolution of GSM

Transition to GPRS, EDGE, and Beyond: GSM evolved to support higher data rates and new services. GPRS (General Packet Radio Service) introduced packet-switched data, allowing continuous data connections and improved internet access. EDGE (Enhanced Data rates for GSM Evolution) further enhanced data throughput and efficiency.

Comparison with Other Technologies (UMTS, LTE): UMTS (Universal Mobile Telecommunications System) and LTE (Long Term Evolution) represent significant advancements over GSM. UMTS introduced 3G capabilities with higher data rates and better

spectral efficiency. LTE, a 4G technology, offers even higher speeds, lower latency, and improved capacity, focusing on an all-IP network.

5.4 Future Prospects

GSM in the Context of Modern Technologies: Despite the advent of 4G and 5G, GSM remains relevant in many regions, especially for voice communication and basic data services. Its widespread infrastructure and compatibility make it a fallback option.

GSM's Role in IoT and M2M Communications: GSM's low cost and extensive coverage make it suitable for IoT (Internet of Things) and M2M (Machine-to-Machine) communications. Many IoT devices use GSM/GPRS for connectivity due to its reliability and affordability.

5.5 Open-Source GSM Software

Standards and Public Availability: GSM standards are publicly available through organizations like 3GPP, facilitating development and innovation in open-source projects.

Issues with Patents and Development Constraints: Open-source GSM software projects often face challenges related to patents and proprietary technologies. Licensing fees and legal constraints can hinder development and deployment.

Projects like Osmocom and OpenBTS for Academic and Hobbyist Engagement: Osmocom is a collection of open-source projects that implement various aspects of GSM technology. It includes components like OsmocomBB (GSM baseband software), OsmoBTS (BTS implementation), and OsmoMSC (mobile switching center). These projects enable enthusiasts, researchers, and educational institutions to study and experiment with GSM technology cost-effectively. OpenBTS converts standard computer and radio hardware into a functioning GSM base station, widely used for research, development, and experimentation in low-cost telecommunication systems.(Paudel et al., 2016)

Conclusion

By delving into these sub-parts, team members will gain a comprehensive understanding of GSM security, its evolution, and future prospects. This knowledge will enhance their technical expertise and prepare them to tackle real-world challenges in mobile communications. For further reading and deeper insights, consulting the relevant 3GPP specifications and technical reports is highly recommended, as they provide authoritative and detailed information on GSM and its related technologies.

References

Brasche, G., & Walke, B. (1997). Concepts, services, and protocols of the new GSM phase 2+ general packet radio service. *IEEE Communications Magazine*, *35*(8), 94–104. https://doi.org/10.1109/35.606036

Eberspächer, J., Vögel, H., Bettstetter, C., & Hartmann, C. (2008). *GSM-architecture, protocols and services*. https://books.google.com/books?hl=en&lr=&id=v6eN1tt9CEUC&oi=fnd&pg=PR5&dq=gsm+&ots=LGP_FUE1T_&sig=a1OI0QAHS3RXHOqBj2NwLDlFrGo

GSM - Architecture, Protocols and Services - Jörg Eberspächer, Hans-Joerg Vögel, Christian Bettstetter, Christian Hartmann - Google Books. (n.d.). Retrieved June 9, 2024, from https://books.google.co.kr/books?hl=en&lr=&id=v6eN1tt9CEUC&oi=fnd&pg=PR5&dq=gsm+components&ots=LGP_FUD0MY&sig=I6fGc5Abd-rQFfw6aQ0WmT1bWZE&redir_esc=y#v=onepage&q=gsm components&f=false

Halonen, T., Romero, J., & Melero, J. (2004). *GSM, GPRS and EDGE performance: evolution towards 3G/UMTS*. https://books.google.com/books?hl=en&lr=&id=cgAroFIOyZIC&oi=fnd&pg=PR5&dq=gsm+&ots=tSE8WicVTx&sig=45COXCmel4XIrIULc6LI0dN_V-M

Lo, C. C., & Chen, Y. J. (1999). Secure communication mechanisms for GSM networks. *IEEE Transactions on Consumer Electronics*, *45*(4), 1074–1080. https://doi.org/10.1109/30.809184

Overview of the GSM system and protocol architecture. IEEE Communications Magazine, 31(4), 92–100 | 10.1109/35.210402. (n.d.). Retrieved June 10, 2024, from https://sci-hub.se/10.1109/35.210402

Paudel, S., Do, V. T., & As, L. (2016). *Investigation, Analysis and Implementation of Open Source Mobile Communication Software*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2433785

Redl, S. M. (2014). *An Introduction to GSM (Artech House Mobile Communication Series)*. https://books.google.com/books/about/From_GSM_to_LTE.html?id=uso-6LN2YjsC

Stuckmann, P. (2003). *The GSM evolution: mobile packet data services*. 256. http://books.google.co.ke/books?id=bQKOse85OHkC

Vedder, K. (1998). GSM: Security, Services, and the SIM. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1528*, 224–240. https://doi.org/10.1007/3-540-49248-8_10