

Describe traditional telephony and network layouts:

Traditional telephone indicates towards the PSTN (Public Switched Telephone Network), which has been the backbone of voice communication for a very long time. Public Switched Telephone Network uses circuit-switching, in that a communication path is established between two users for the entire call duration (Tarasov, 2025). This gives consistent voice quality but results in not excessive use of network resources when there is a pause or silence during a conversation.

The traditional network layout is hierarchical and contains three main components: trunk lines, local loops, and central offices. Trunk lines interconnect multiple central offices over long distances often it use high-capacity transmission systems like T-carrier or fiber optics. The local loop connects the telephone of subscriber to the nearest central office with the help of copper wires, and central offices manage call routing and signaling. Traditional telephony networks are highly reliable, but they lacked at flexibility and scalability if we compared with the modern IP-based networks. Adding new services or expanding the capacity generally requires necessary hardware upgrades.

Discuss mobile telephony and cellular service:

Mobile telephony enables wireless voice communication by using radio signals instead of wired connections. Cellular service divides a huge geographic area into smaller regions, which are called cells, each of them served by a BTS or base station. This design allows the reuse of radio frequencies, which increases the number of users that can be supported continuously. When users move from one cell to another during a call, that time network performs a handover, transferring the call without any issue to the another base station. Mobile telephone systems depend on a mobile switching center or core networks to manage call routing, mobile management, etc. Modern cellular networks support voice calls and data services like SMS, internet access, and so on (Seck-Sarr, 2024). With the development of mobile telephony, it has developed from an analog system to digital technologies, and the capacity, service quality, and security have improved with it.

What is GSM and how does it work?:

GSM (Global System for Mobile Communications) is a digital cellular communication standard that was actually developed in Europe and after that, adopted by across the world. GSM was designed to provide secure and interoperable mobile communication across different countries and network operators. GSM works by dividing coverage areas into cells. Voice signals are digitized, encrypted, compressed, and then get transmitted over radio frequencies by using a combination of Time Division Multiple Access and Frequency Division Multiple Access. Users are individually assigned to a specific frequency channel and also a time slot within that channel. This architecture contains three main subsystems: the MS (Mobile Station), the BSS (Base Station Subsystem), and the NSS (Network and Switching Subsystem). All together these components handle communication, call control, etc.

High Bandwidth Usage in Digital Signals from Phones to Towers:

Yes, Digital signals transmitted from mobile phones to cellular towers generally utilize low bandwidth, mainly for voice communication.

This is because voice calls do not require large amounts of data to maintain quality. In digital cellular systems, the human voice is initially converted from an analog signal into a digital format, and after that compressed using voice codes. These codecs reduce the amount of data needed by removing silence and frequencies that are less important for hearing. As a result, a general digital voice call may use a few kilobits per second. This allows the network to support many users at the same time (Lu et al., 2022). Low bandwidth usage is important in cellular networks because the available frequency spectrum is limited. Cellular providers can increase capacity and maintain consistent call quality by keeping bandwidth requirements low. It is important that when a mobile phone transmits data services like video calls or large file downloads, during that time, the bandwidth usage becomes higher generally (Jiang & Han, 2024). These services require much more data compared to standard voice calls. Modern smartphones can dynamically switch to higher bandwidth usage when data-intensive applications are in use.

GSM is hardware-specific or not, provide reasons :

No, GSM specifications are not hardware-specific.

GSM was designed as an open and standardized mobile communication system, which means the specifications define how communication should occur, not which hardware must be used. As long as devices and network equipment follow the GSM standards like frequency bands, authentication processes, and encryption algorithms, they can interoperate regardless of the manufacturer.

GSM is not dependent on hardware, which is why mobile phones from different vendors can work on GSM networks which can be operated by different service providers (Hughes, 2022). Just like that, network infrastructure from multiple equipment manufacturers can also exist within the same GSM network. This provides competition and lowers costs for both service providers and also consumers.

The non-mandatory hardware nature of GSM also enabled its worldwide adaptation, and this allows the users to roam internationally by changing SIM cards when they are using the same handset. These are the main reasons behind GSM becoming one of the most widely used mobile communication systems.

Describe FDMA, TDMA, and CDMA. Differentiate their subtle applicability. Then, an example of a provider for each of these technologies:

FDMA:

The available frequency bandwidth is divided by FDMA into distinct non-overlapping channels. Each user is allocated a specific and dedicated frequency band for the duration of the communication. Primarily, it is used in analog systems.

Sublet applicability:

FDMA is very suitable for narrowband, continuous signal applications where low complexity is required, and signal synchronization is not important. It is commonly used in traditional radio broadcasting, specialized land mobile radio systems, etc.

Provider Example:

Icom (NXDN system).

TDMA:

By dividing it into distinct time slots, TDMA shares a single frequency channel. Multiple users take turns transmitting in quick bursts by utilizing the entire bandwidth for a very short duration.

Sublet applicability:

TDMA is Ideal for digital cellular networks requiring moderate flexibility and data rates. It is very perfect for voice-centric services where data transmission can be fragmented into packets.

Provider Example:

AT&T or T-Mobile (during 2G GSM usage time).

CDMA:

CDMA allows every user to share the entire bandwidth effortlessly (National Security Agency, 2021). Each signal of a user is coded with a unique, distinct code that allows the receiver to differentiate it from others; they transmit at the same time and frequency through it.

Sublet applicability:

CDMA is very efficient for data-intensive networks with a large number of users, as it offers no strict capacity restriction and better interference management. It is used for 3G (UMTS, CDMA2000) technologies.

Provider Example:

Verizon or Sprint (3G networks).

Enumerate IP Telephony Network issues and vulnerabilities, and briefly describe each issue or vulnerability. List some common attacks on IP Telephony:

IP Telephony transmits voice over IP networks, which makes it flexible and cost-efficient, but it also involves several technical problems and security vulnerabilities, like Latency, which is the delay in transmitting voice packets from sender to receiver. If latency is high, it can be causes of pauses or overlapping speech, and that reduces call quality. Jitter means the variations in packet arrival times (Palamà et al., 2023). Audio can sound distorted when voice packets arrive out of sequence. Packet loss happens when voice packets fail to reach their destination, resulting in dropped calls, and missing words can be happen. Low authentication mechanisms can allow unauthorized users to access the voice over IP system, and they can also make calls or manipulate configurations.

Some common attacks targeting IP telephony systems are:

Capturing voice over IP packets to listen to the conversations, taking control of an active call, or redirecting the call to another location. Gaining unauthorized access to voicemail systems to steal. Preventing legitimate users from making or receiving calls.

Define "rogue" and "softphone":**Rogue:**

A rogue device refers to any unauthorized or unapproved device or service connected to the network in networking and IP telephony (Wang & Zou, 2025). Some examples are a rogue IP phone, rogue wireless access point, etc. These devices bypass normal security controls, and they can also create serious risks.

Softphone:

Softphone is a software-based telephone application that allows users to make and receive voice or video calls over an IP network using any supporting digital device. Instead of dedicated hardware, a softphone uses the microphone, speakers, or headset of the device and communicates using VoIP protocols like SIP. Softphones are mainly used in remote work.

List IP Phone countermeasures (at least 5):

Authentication methods like certificates or some unique credentials are mandatory to ensure that only authorized users and devices can access the VoIP network.

Use encryption protocols like Secure RTP and TLS to protect voice data and signaling.

By deploying firewalls and SBCs, filter VoIP traffic and protect from SIP attacks.

Keep IP phone firmware and VoIP server software updated to fix known vulnerabilities.

Separate the voice traffic from data traffic by using VLANs to improve security and maintain the quality of the call.

References

- Hughes, L. E. (2022). IPv6 Core Protocols. In *Third Generation Internet Revealed: Reinventing Computer Networks with IPv6* (pp. 157-260). Berkeley, CA: Apress.
- Jiang, W., & Han, B. (2024). Evolution to first-generation (1G) Mobile cellular communications. In *Cellular communication networks and standards: The evolution from 1G to 6G* (pp. 7-21). Cham: Springer Nature Switzerland.
- Lu, Y. H., Hsiao, S. H. Y., Li, C. Y., Hsieh, Y. C., Chou, P. Y., Li, Y. Y., ... & Tu, G. H. (2022). Insecurity of operational IMS call systems: vulnerabilities, attacks, and countermeasures. *IEEE/ACM Transactions on Networking*, 31(2), 800-815.

National Security Agency (2021). *Deploying Secure Unified Communications/Voice and Video over IP Systems*. Retrieved from:

https://media.defense.gov/2021/Jun/17/2002744054/-1/-1/1/CTR_DEPLOYING%20SECURE%20VVOIP%20SYSTEMS.PDF

Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, 212, 129-140.

Seck-Sarr, S. F. (2024). Mobile money in sub-Saharan Africa: Innovation and actors' strategies. *Telematics and Informatics Reports*, 13, 100114.

Tarasov, L., Lecavalier, B. S., Hank, K., & Pollard, D. (2025). The glacial systems model (GSM) Version 24G. *Geoscientific Model Development Discussions*, 2025, 1-55.

Wang, W., & Zou, L. (2025, March). Comparison of actual performance between CDMA and DDMA waveforms in vehicle radar application. In *Sixteenth International Conference on Signal Processing Systems (ICSPS 2024)* (Vol. 13559, pp. 1605-1613). SPIE.