The Evolution of Mobile Technologies 3G / 4G: Security Issues

Gyan Prakash
M.Tech Scholar in Computer Science & Engineering
Mr.Anoop Singh , Associate Professor Sarvepalli Radhakrishnan University,Bhopal (Madhya Pradesh) India

Abstract -- **During the 20th century, the key technology was information gathering, processing and distribution. This total technology will depend based on the network systems. Which are nothing but grouping of systems that should be controlled by a server. In business and home applications, mobile users, and in all social issues the networks are used. To enhance the benefits of these networks, we are introducing 3G systems. The aim of the 3G security architecture is to improve on the security of 2G systems.3G systems have additional standards like EDGE and CDMA rather than older systems. It has a high quality voice and video services but has limited in coverage area. Now introducing the 4G technologies to full fill the limitations of 3G.**

Keywords -- ***3G*, 4G, CDMA, EDGE, GPRS, GSM, IMT, ITU, UMTS.**

INTRODUCTION

The 3G research and development projects started in 1992.In 1999, ITU approved five radio interfaces for IMT-2000.There are revolutionary standards(EDGE and CDMA) that are backwards compatible extensions to pre-existing 2G networks as well as revolutionary standards that require all new network hardware and frequency allocations. 3G mobile telecommunications is a generation of standards for mobile phones mobile telecommunications service fulfilling the international mobile telecommunications-2000 specifications by the international telecommunication union.

In telecommunications, 4G is the fourth generation of cellular wireless standards. It is a successor to the 3G and 2G families of standards. In 2009, the ITU-R organization specified the IMT-advanced requirements for 4G standards, setting peak speed requirements for 4G service at 100Mbps for high mobility communications and 1Gbps for low mobility communications.

3G – ARCHITECTURE

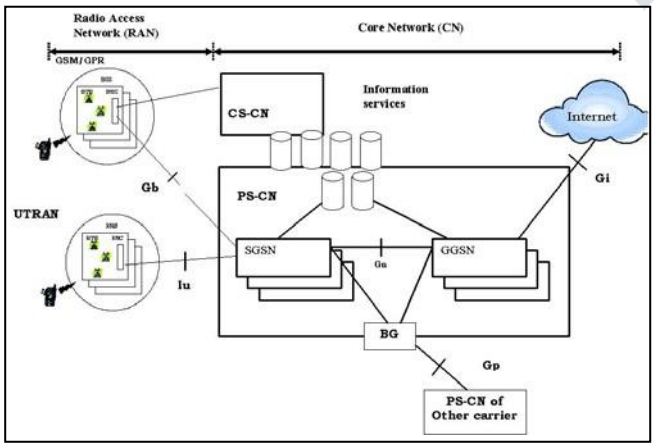

FIG. 1. ARCHITECTURE OF 3G

As can be seen in Fig. 1, the 3G network has two main parts

1. The Radio Access Network (RAN)
2. The Core Network (CN)

The RAN consists of the existing GPRS/GSM RAN system which is connected to the Packet Switched Network (PS-CN) and also to the circuit switched network (CS-CN). The PS-CN will eventually connect to the UTRAN system as part of the full transition to 3G. The UTRAN consists of subsystems, with each subsystem consisting of one Radio Network Controller (RNC) which is connected to several Base Transceiver Stations (BTN). The GRPS RAN has a similar architecture.

The Core Network consists of the PS-CN and the CS-CN. The PS-CN consists of several information servers, the SGSN and the GGSN. Each SGSN connects one or more RSC and BSC with the PS-CN. Its functionality includes access control, mobility management, paging and route management. The GGSN is the logical gateway to the Internet. The BG interface can be used to connect to another PS-CN or to another carrier. The information servers provide several functions. The Home Location Register (HLR) maintains subscriber information and the Authentication Center (AuC) maintains authentication information. There are also IP based servers such as DNS, DHCP and RADIUS servers which interact with the SGSN/GGSN and provide control and management functions.

FEATURES OF 3G

Data Rates:

ITU has not provided a clear definition of the data rate users can expect from 3G equipment or providers.

Security:

3G networks offer greater security than their 2G predecessors. In addition to the 3G network infrastructure security, end-to-end security is offered when application frame works such as IMS are accessed.

ADVANTAGES OF 3G

1. Faster data connectivity.
2. Uninterrupted video streaming on phones.
3. Video calls and big MMS.
4. Good for data intensive applications.
5. Downloading games and songs is much faster with this technology.
6. Access any site on the internet by using phone.
7. To make a wide range of services, both voice and data available to users, irrespective of location.

8. To provide services over a wide coverage area.
9. To provide the best quality of service (QoS) possible.
10. To extend the number of services provided subject to constraints like radio transmission, spectrum efficiency and system economics.
11. To accommodate a great variety of mobile stations.
12. To admit the provision of service by more than one network in any area of coverage.
13. To provide an open architecture which will permit the easy introduction of technology advancements as well as different applications.

BENEFITS OF 3G

High Quality Voice Service:

The quality of voice-falls under 3G will be much higher compared to 2G services.

Enhanced content Service:

3G users can download full music files, full movie files and other files at high speed.

Mobile Broadband:

3G user can use his handset for high speed internet any time any where (where connectivity is available).

Video Services:

3G user can enjoy the video call facility where in both the caller and receiver will be able to see each other while speaking if both have 3G services and 3G enabled handsets.

Mobile TV:

3G users can watch TV programmes of different video channels as per his liking while on the movie.

APPLICATIONS OF 3G

The bandwidth and location information available to 3G devices gives rise to applications not previously available to mobile phone users. Some applications are

1. Mobile TV.
2. Video on demand.
3. Video conferencing.
4. Telemedicine.
5. Location-based services.
6. Global Roaming.

LIMITATIONS OF 3G

1. With WCDMA based 3G, as the data speed increases the coverage area of the cell become smaller and smaller.
2. There has been some improvement with HSPDA, but still it is impossible to connect these by wireless links in cellular technology.
3. Using WCDMA cells, with increase in data rate, the speed of movement of user terminal also become lesser and lesser.
4. We still have circuit voice, circuit data and packet data bearers.

SECURITY ISSUES IN CELLULAR NETWORKS:

There are several security issues that have to be taken into consideration when deploying a cellular infrastructure. The importance of which has increased with the advent of advanced networks like 3G.

Authentication: The purpose of 3G is to enable people to communicate from anywhere in the world, the issue of cross region and cross provider authentication becomes an issue.

Integrity: With services such as SMS, chat and file transfer it is important that the data arrives without any modifications.

Confidentiality: With the increased use of cellular phones in sensitive communication, there is a need for a secure channel in order to transmit information.

Access Control: The device might access a database where some sort of role based access control is necessary.

Operating Systems in Mobile Devices: Some phones may use a Java Based system; others use Microsoft Windows CE and have the same capabilities as a desktop computer. Issues may arise in the OS which might open security holes that can be exploited.

Web Services: A Web Service is a component that provides functionality accessible through the web using the standard HTTP Protocol. This opens the cellular device to variety of security issues such as viruses, buffer overflows, denial of service attacks etc.

Location Detection: The actual location of a cellular device needs to be kept hidden for reasons of privacy of the user. With the move to IP based networks, the issue arises that a user may be associated with an access point and therefore their location might be compromised.

Viruses and Malware: With increased functionality provided in cellular systems, problems prevalent in larger systems such as viruses and malware arise.

Downloaded Contents: Spyware or Adware might be downloaded causing security issues. Users might download unauthorized copies of music, videos, wallpapers and games.

Device Security: If a device is lost or stolen, it needs to be protected from unauthorized use so that potential sensitive information such as emails, documents, phone numbers etc. cannot be accessed.

TYPES OF ATTACKS

Due to the massive architecture of a cellular network, there are a variety of attacks that the infrastructure is open to.

Denial of Service (DoS): This is caused by sending excessive data to the network, more than the network can handle.

Distributed Denial of Service (DDoS): It might be difficult to launch a large scale DoS attack from a single host.

Channel Jamming: Channel jamming is a technique used by attackers to jam the wireless channel.

Unauthorized Access: If a proper method of authentication is not deployed then an attacker can gain free access to a network.

Eavesdropping: If the traffic on the wireless link is not encrypted then an attacker can eavesdrop and intercept sensitive communication such as confidential calls, sensitive documents etc.

Message Forgery: If the communication channel is not secure, then an attacker can intercept messages in both directions and change the content without the users ever knowing.

Message Replay: Even if communication channel is secure, an attacker can intercept an encrypted message and then replay it back at a later time and the user might not know that the packet received is not the right one.

Man In The Middle Attack: An attacker can sit in between a cell phone and an access station and intercept messages in between them and change them.

Session Hijacking: A malicious user can highjack an already established session and can act as a legitimate base station.

The security architecture needs to provide security for these services.

3G SECURITY ARCHITECTURE

There are five different sets of features that are part of the architecture:

Network Access Security: This feature enables users to securely access services provided by the 3G network. This feature is responsible for providing identity confidentiality, authentication of users, confidentiality, integrity and mobile equipment authentication.

Network Domain Security: This feature enables nodes in the provider domain to securely exchange signaling data, and prevent attacks on the wired network.

User Domain Security: This feature enables a user to securely connect to mobile stations.

Application Security: This feature enables applications in the user domain and the provider domain to securely exchange messages.

Visibility and Configurability of Security: This feature allows users to enquire what security features are available.

4G NETWORKS

4G is the next generation after 3G. Although still 3G has not been fully implemented in the real world, people have started talking about the features of 4G. Some of the 4G services talked about are incorporating quality of service (QoS) and Mobility

1. High usability: Any time, any where and with any technology.
2. Support for multimedia services at low transmission cost.
3. Personalization.
4. Integrated services.

REASON FOR DELAY IN IMPLEMENTING 3G & 4G MOBILE SERVICES:

1. The 3G services had only reached with in some towns of china, so that it may take time to reach to other countries.
2. Another major defect of this is that wide band frequency spectrum, which is needed for 3G, is lacking.
3. Another reason for this is that it is a cost bearing item especially for sending data.
4. If it should be accepted among all customers, firstly it should be available at a lower rate, for which the rate of spectrum should be declined.

CONCLUSION

Security is an ever growing field. What is secure today may not be secure tomorrow. There will always be malicious users trying to exploit and find new holes in a network. Therefore, we need to look into the future so that we are able to face these security issues before they cause damage.

Security is not just about putting big locks on the front door; it also involves making sure all the windows are shut.

Each one can be individually fooled, but the comparison makes the system more secure as a whole.

REFERENCES

[1] 3G, White Paper by Trillium Digital Systems, In.
[2] http://www.cs.wustl.edu/~jain/cse574- 06/f tp/ cellular_security / index.html
[3] International Telecommunication Union
[4] GSM Association.
[5] ITU-T, 2018. Security in Telecommunications and Information Technology: An overview of issues and the deployment of ITU-T Recommendations for secure telecommunications