# 3G & 4G Service Architectures

Vijendra Sahu
Assistant Professor

Anish P.Bhandari
Assistant Professor

Priti B.Dhanke
Asst Prof [M.E] 2nd Year

**Abstract**— These i3G services represent an evolution in telecommunication industry. However, 3G services has not received great adoption rate as expected despite of various benefits provided by this service. This study aims to investigate the factors affecting the intention to adopt 3G services among the university students in Malaysia since they expected to be the group with great potential to adopt 3G services. Diffusion of innovation theory is modified and applied in this study to achieve the objective. Results of this study show that perceived compatibility, perceived relative advantage, perceived results demonstrability, perceived trailability, perceived image, and perceived enjoyment are significantly associated with intention to adopt 3G services. Surprisingly, perceived cost of using 3G services is found to be positive but insignificant associated with intention to adopt 3G services. Managerial implications and Conclusion has been discussed.

**Index Terms**— 3G Services Adoption, Diffusion of Innovation Theory, University Students

.

---

## Introduction:

This paper briefly introduces the overviews of 3G and 4G communication system. With our wireless service needs of wireless network, it causes wireless network service and its technologies rapidly growing, and becomes a basic appliance for contemporary people. This report will provide a brief introduction to the security of 3G and 4G. In this report, we introduce the system overview of 3G and 4G. We also introduce the security of 3G and 4G including security architecture, network security, security weakness, etc. More details information can be referred to the 3GPP related documents [3GPPTS121] [3GPPTS102] [3GPPTR900] [3GPPTS205]. As to the 4G, some of current research results from papers are introduced in this report [Fu04] [Celentano06] [Zheng 05a][Zheng 05c]. Some issues of 4G are also suggested for our future further study [Fu04][O'Drama04] [Dell'Uomo02] [Hui03] [Celentano06]. **4G** (also known as **Beyond 3G**), an abbreviation for **Fourth-Generation Communications System**, is a term used to describe the next complete evolution in *wireless communications*. A 4G system will be able to provide a comprehensive IP solution where voice, data and streamed multimedia can be given to users on an "Anytime, Anywhere" basis, and at higher data rates than previous generations. There is no formal definition for what 4G is; however, there are certain objectives that are projected for 4G. These objectives include: that 4G will be a fully IP-based integrated system. This will be achieved after wired and wireless technologies converge and will be capable of providing between 100 Mbit/s and 1 Gbit/s speeds both indoors and outdoors, with premium quality and high security. 4G will offer all types of services at an affordable cost. According to the 4G working groups, the infrastructure and the terminals of 4G will have almost all the standards from 2G to 4G implemented. Although legacy systems are in place to adopt existing users, the infrastructure for 4G will be only packet-based (all-IP). Some proposals suggest having an open platform where the new innovations and evolutions can fit. The technologies which are being considered as pre-4G are the following: WiMax, WiBro, iBurst, 3GPP Long Term Evolution and 3GPP2 Ultra Mobile Broadband. **3GPP LTE** (Long Term Evolution) is the name given to a project within the Third Generation Partnership Project (3GPP) to improve the UMTS mobile phone standard 4 to cope with future requirements. Goals include improving efficiency, lowering costs, improving services, making use of new spectrum opportunities, and better integration with other open standards. The LTE project is not a standard, but it will result in the new evolved release 8 of the UMTS standard, including mostly or wholly extensions and modifications of the UMTS system. The architecture that will result from this work is called **EPS** (**Evolved Packet System**) and comprehends **E-UTRAN** (Evolved UTRAN) on the access side and **EPC** (**Evolved Packet Core**) on the core side. **Universal Mobile Telecommunications. System (UMTS)** is one of the **third-generation (3G)** cell phone technologies, which is also being developed into a 4G technology. Currently, the most common form of UMTS uses W-CDMA as the underlying air interface. It is standardized by the 3GPP, and is the European answer to the ITU IMT-2000 requirements for 3G cellular radio systems.

### 3G/3GPP System Overview

3G is the next generation wireless network which is to provide a world wide standard and a common communication for mobile networking. 3G standard is defining on 3GPP bodies. 3G features exceeding over 2G provide higher data rate, massive network capacity, interactive multimedia service, QoS, global roaming [3GPPTS121] [3GPPTS102]. Initially, there are several communication technologies as WCDMA, TDMA, CDMA2000 applied for 3G. Up to 3GPP be organized, UMTS included WCDMA is proposed as 3GPP

communication standard. In 3GPP, All IP becomes an important feature. The services associated with 3G include wide-area wireless voice telephony and broadband wireless data, all in a mobile environment. In marketing 3G services, video telephone has often been suggested as the killer application for 3G. 3G support higher network access rate than 2G system. Because of the enhancement of bandwidth, mobile application can make much application than before, such as video phone, some real-time services.

The main technology used in 3G system is Code division multiple access (CDMA) which a form of multiplexing and a method of multiple access that divides up a radio channel not by time, nor by frequency, but instead by using different pseudo-random code sequences for each user [wiki, CDMA]. There are several types of CDMA exist, WCDMA, TD-SCDMA, CDMA2000. In Asia, Europe, and the USA and Canada, telecommunication companies use W-CDMA [wiki, 3G].

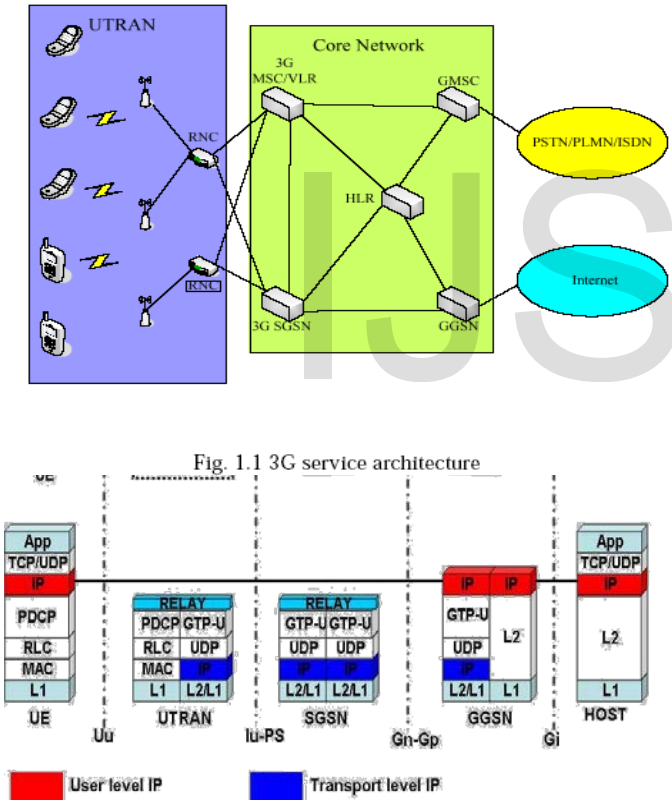


Fig. 1.1 3G service architecture

**Fig. 1.1 3G service architecture**

3G service architecture is illustrated as Fig. 1.1 [3GPPTS121]. A subscriber connects to another connected user through Node B (base transceiver station BTS), Radio Network Controller (RNC), Mobile Service Switching Center (MSC) and GMSC (Gateway Mobile Switching Centre) of core network to the PSTN. The BSC or RNC control the resource allocations and QoS. The RNC is charged of the switching and control in UTRAN. UTRAN, short for **U**MTS **T**errestrial **R**adio **A**ccess **N**etwork, is a collective term for the Node B's (base transceiver station BTS) and Radio Network Controllers which make up the UMTS radio access network. The

UTRAN allows connectivity between the UE (user equipment) and the core network. A Gateway Mobile Switching Centre (GMSC) provides an edge function within PLMN Public Land Mobile Network). It terminates the PSTN (Public Switched Telephone Network) signalling and traffic formats and converts this to protocols employed in mobile networks. For mobile terminated calls, it interacts with the HLR (Home Location Register) to obtain routing information. MSC and GMSC transmit communication signal to PSTN. On the other hand, 3G also supports the GPRS service through SGSN and GGSN to internet.

**IPv6 and 3G**

3G systems introduce All-IP network but the lack of IP addresses may be the bottleneck for toward all-IP network as Fig. 1.3. However, GGSN support NAT to address this problem. But NAT still has many problems to be

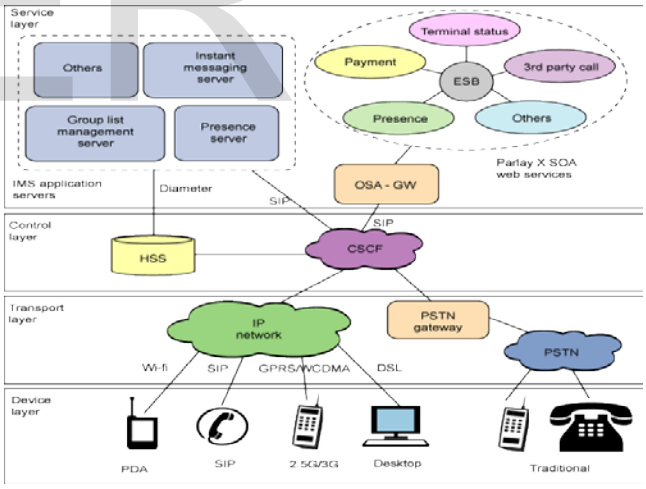


**Fig 1.2:architecture of 4g**

addressed. The best solution that can address the issues is IPv6. The sufficient of IP addresses and enhancement of IPv4 weakness makes IPv6 on 3G system more powerful. As a result, IPv6 was integrated in 3G Rel-5. More specifically, UE and NE in core network have to support IPv6.

In 3G network system, IP address has two main purposes. User-level IP address is used in communication between mobile terminal and application host. Transport-Level IP address is used in communication among network

| | 3G | 4G |
|---|---|---|
| General topics | – Many different standards w orldwide<br>– Combination of real and dev eloped equipment | – Global mobility<br>– Serv ice compatibility<br>– All netw ork elements are Digital |
| Compatibilit y | Backward compatible to2G | – Adv anced 3G-capacity (an order of magnitude) |
| Sw itching Design Basis | Channel and Packet sw itching | All digital with packetized v oice |
| Netw ork architecture | – Wide area cell-based | – Hybrid – Integration of Wireless LAN (WiFi, Bluetooth, hot spots) and w ide area |
| Frequency band | – Regionally different (1800-2400 MHz) | – Higher frequency band (2-8 GHz) |
| Access Technologies | – W-CDMA, 1xRTT, Edge | – OFDM and MC-CDMA (Multi Carrier CDMA) |
| Bandw idth | 5-20 MHz | 100 MHz (or more) |
| Data rate | 384KBit/s up to 2Mbit/s | 20 up to 100 Mbit/s |

entities in 3G network.

**Table 1. Comparison of 3G and 4G**

## 4G Features

4G has not yet reached in industry and standard. Illustration of Fig. 1.4 is a 4G service architecture from Agora Co. *Always-Best-Connected* service on heterogeneous network is hoped to achieve. In order to provide *Always-Best-Connected* service in the future, a universal consensus on features of 4G is achieved. In the understanding, main important characteristics and features are [Fu04][Hui03] [Zheng05a]: All-IP Based network architecture Higher bandwidth (than 3G) Heterogeneous Network (3G/UMTS, Wireless LAN, DVB-T, etc.)

**QoS, Security,**
Full integration of "hot spot" and "cellular "Support for multimedia applications. 4G service architecture is shown in the diagram 4G standard is defining in the countries such as Japan, China, Korea, Europe. Main leading institute of standard defining consists of IMT-Advanced, 3GPP , 3GPP2. For providing 4G service, new technologies and architectures are still on developing at different programs such as NTT DoCoMo, Nokia, Motorola, etc.

Basically, 3G is on developing communication networks, 4G is on defining standards. In spite of some 4G features exceeding over 3G, the future developments are worth our further investigating. In the Table 1, the comparison of 3G and 4G from different features is illustrated.So here always quality of service always matter which provides the authentication of user and prevent his matter from hackers.

## 3G Security

This section describes the security architecture of 3G. In the architecture, the security features also described. The detailed features and definitions can refer to the 3G-related documents [3GPPTS102] 3GPPTS121] [3GPPTS102] [3GPPTR900] [3GPPTS205]. For convenience, we follow 3GPP security architecture to describe the security features.Basiacally 3G provides a very fast speed but it has some security issues in its network by which the messages can be leaked.

## 3G/3GPP Security Architecture

3G security concerns is raised from some issues as wireless access is inherently less secure, mobility implies higher security risks, IP-based technologies brings new vulnerabilities, …, etc.3G Security requires consideration of several aspects such as mobility, the particular security threats, the types of information to be protected and the complexity of network architecture over 2G. An overview of 3G security architecture is illustrated as follow [3GPPTS102].When 3G was developed, security issues were taken into consideration. The whole 3G security architecture was designed based on three fundamental principles [3GPPTS120].

(1). The architecture for 3G will build on the security features of 2G system.

(2). The 3G security will improve on the security of the 2G system.

(3). 3G security will offer new features and will secure new services offered by 3G.The following are listed security enhancements in 3G security[3GPPTS120]: Key lengths were increased to allow for the possibility of stronger algorithms for encryption and integrity. Mechanisms were included to support security within and between networks.

-Security is based within the switch rather than the base station as in GSM -Integrity mechanisms for the terminal identity (IMEI) have been designed in from the start, rather than that introduced late into GSM.

-When roaming between networks, such as between a GSM and 3GPP, only the level of protection supported by the smart card will apply.

**3G/3GPP Network Access Security**

Network access security is a mechanism to provide a secure access 3G services and to protect against attacks on the radio interface. In order to provide a secure 3G service, the security features of network access security required for 3G are listed as follows [3GPPTS102].

In order to achieve the security features of network access security, 3GPP defines several mechanisms to achieve these features. The mechanism mainly process the function of the secure access such as (i) user identity confidentiality, (ii) authentication and key agreement, (iii) data confidentiality and (iv) integrity protection of signaling messages.

**User identity confidentiality**

The user identity confidentiality of 3GPP allows user identification to access services by a temporary Mobile Subscriber Identity (TMSI). In initial registration, the network system registered a permanent identity of user. When a user raises a service request, the network system assigned a TMSI to user for his services. The TMSI implies that confidentiality of user identity is protected almost always against passive eavesdroppers. TMSI can also avoid user traceability by changing TMSI in the short time period.

**Authentication/Key Agreement**

In this section, we discuss the 3GPP Authentication/Key Agreement illustrated as Fig. 2.3. Firstly, VLR/SGSN send authentication data request to HE/HLR [3GPPTS102]. More details can refer to 3GPP standard TS 33.102 [3GPPTS102]. After the receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of n authentication vectors to the VLR/SGSN. The authentication vectors are ordered based on sequence number. Each authentication vector consists of several components such as a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is important for one authentication and key agreement between the VLR/SGSN and the USIM.

**Comparison of 2G and 3G Mobile Networks**

As mentioned above, although there are many similarities between 2G and 3G wireless networks (and many of the 2G and 3G components are shared or connected through interworking functions), there are also many differences between the two technologies. Table 1 compares the differences between the core network, th radio portion and other areas of the two networks.

Table 1: Comparison between 2G+ and 3G wireless networks

| Feature | 2G | 2G+ | 3G |
|---|---|---|---|
| Core Network | MSC/VLR, GMSC, HLR/AuC/EIR<br><br>MM, CM, BSSAP, SCCP, ISUP,TCAP, MAP, MTP 3, MTP 2, MTP 1<br><br>TDM transport | MSC/VLR, GMSC, SGSN, GGSN, HLR/AuC/EIR, CGF<br><br>GMM/SM/SMS, MM, CM, GTP, SNDCP,NS, FR, LLC, BSSGP, BSSAP, BSSAP+, SCCP, TCAP, MAP, ISUP, MTP 3, MTP 2, MTP 1<br><br>TDM, Frame Relay transport | 3G MSC/VLR (with added interworking and transcoding), GMSC, HLR/AuC/EIR, 3G-SGSN, GGSN, CGF<br><br>GMM/SM,MM,CM,BSSAP, RANAP,GTP,SCCP, MTP3B, M3UA, SCTP, Q.2630.1 (NNI), TCAP, MAP, ISUP, MTP 3, MTP 2, MTP 1, Q.2140, SSCOP<br><br>ATM, IP transport |
| Radio Access | BTS, BSC, MS<br><br>FDMA, TDMA, CDMA<br><br>MM, CM, RR, LAPDm, LAPD, BSSAP, SCCP, MTP 3, MTP 2, MTP 1 | BTS, BSC, MS<br><br>TDMA, CDMA, EDGE<br><br>MAC, RLC, GMM/SM/SMS, LLC, SNDCP, BSSGP, NS, FR,RR, BSSAP, SCCP, MTP 3, MTP 2, MTP 1 | Node B, RNC, MS<br><br>W-CDMA, CDMA2000, IWC-136<br><br>GMM/SM, MAC, RLC, PDCP,RRC,Q.2630.1(UNI+ NNI),NBAP, RNSAP, RANAP, SCCP, MTP3B, M3UA, SCTP, GTP-U, Q.2140, Q.2130, SSCOP, CIP |
| Handsets | Voice only terminals | New type of terminal<br>Dual mode TDMA and CDMA<br>Voice and data terminals<br><br>WAP, no multimedia support | New type of terminal<br>Multiple modes<br>Voice, data and video terminals<br><br>WAP, multimedia mgmt |
| Databases | HLR, VLR, EIR, AuC | HLR, VLR, EIR, AuC | Enhanced HLR, VLR, EIR,AuC |
| Data Rates | Up to 9.6 Kbps | Up to 57.6 Kbps (HSCSD)<br>Up to 115Kbps (GPRS)<br>Up to 384 Kbps (EDGE) | Up to 2Mbps |
| Applications | Advanced voice, Short Message Service (SMS) | SMS, Internet | Internet, multimedia |
| Roaming | Restricted, not global | Restricted, not global | Global |
| Compatibility | Not compatible to 3G | Not compatible to 3G | Compatible to 2G, 2G+ and Bluetooth |

**6. About Trillium**

Trillium Digital Systems is the leading provider of communications software solutions for the converged network infrastructure. Trillium's source code solutions are used in more than 500 projects by industry-leading suppliers of wireless, Internet, broadband and telephony products. Trillium's high-performance, high-availability software and services reduce the time, risk and cost of implementing SS7, IP, H.323, MGCP, ATM, Wireless and other standards-based communications protocols. Trillium actively participates in the development of 3rd generation systems by developing standards-based wireless communications protocols. It is likely that the first 3G mobile terminals will be multi-mode devices, which means that they will support a number of 2nd generation protocol standards in order to reach wide network coverage and to provide 3rd generation advanced services. Trillium has extensive know-how in all the major communications protocol standards in the world and can provide solutions for many types of networks. Trillium designs all its portable software products using the Trillium Advanced

Portability Architecture (TAPA□), a set of architectural and coding standards that ensure the software is completely independent of the compiler, processor, operating system and architecture of the target system. This makes Trillium products portable, consistent, reliable, high quality, high performance, flexible, and scaleable. This architecture also ensures that all Trillium protocols can interwork seamlessly in the same or between different networks. As mentioned above, successful implementation, adoption, and overall acceptance of the 3G wireless networks depends largely on the ability of these new mobile networks to interface and interwork with the existing 2G and legacy networks currently deployed worldwide. Trillium's products allow wireless communications equipment manufacturers to develop "best-in-class" next-generation mobile networks, to ensure success of the network operator and service provider, and to ensure wide acceptance of the new services by end-users.

**3G Weaknesses and Proposed Improvements 3G Architecture Weaknesses**

Backup procedure for TMSI reallocation. IMSI confidentiality in wireline part

**Firewall Issues**

WAP Architecture (V1.2.1) Data Privacy Voice Call Transcoded Threat Backup Procedure for TMSI Reallocation.VLR cannot associate the TMSI with the IMSI because of TMSI corruption or database failure when the user roams, and the SN/ VLRn cannot contact the previous VLRo.

**Voice Call Transcoded Threat**

Voice calls may need to be transcoded when they cross network borders. Such as, bit rate change it is not possible to apply such transformation on an encrypted signal. Signal has to be decrypted before transcoding. Network-wide confidentiality lacks flexibility.

**3G security weakness and Security Issues**

Important Changes in Security Defeat the false base station attack. Key lengths were increased. Support security within and between networks Integrity mechanisms.

**Types of Attacks**

Eavesdropping Impersonation of a user Impersonation of the network Man-in-the-middle Compromising authentication vectors in the network

**3G Security Feature**

3G network enhances much vulnerability in 2G. Many 2G attacks are not suitable for 3G network.

**Denial of service Attack**

De-registration request spoofing the intruder spoofs a de-registration request (IMSI detach) to the network Location update request spoofing User spoofs a location update request in a different location area camping on a false BS/MS

**Denial of Service Solution**

Integrity protection of critical signaling messages Location update request spoofing and Deregistration request spoofing. In Camping on a false BS/MS Integrity can't prevent the false BS/MS ignoring certain service requests and/or paging requests.

**Identity Catching Attack**

Passive identity catching requires a modified MS. Expect network may sometimes request the user to send its identity in plaintext. Active identity catching Requires a modified BS Requests the target user to send its permanent user identity in plaintext.

**Identity Catching Attack Solution**

Identity confidentiality mechanism counteracts this attack Encryption key shared by a group of users to protect the user identity when new registrations or temporary identity database failure in the serving.

**Eavesdropping on user data**

Suppression of encryption between the target user and the true network Modified BS/MS When set up a connection, false BS/MS modifies the ciphering capabilities of the MS; network may then decide to establish an un-enciphered connection.

**Eavesdropping on user data Solution**

Message authentication and replay inhibition of the mobile's ciphering capabilities. Network can verify that encryption has not been suppressed by an attacker.

**ACKNOWLEDGEMENT**

We express my sincere gratitude to **Resp. Dr D.N.CHAUDHARY sir**, Head of the Department, Computer Science & Engineering for providing their valuable guidance and necessary facilities needed for the successful completion of this seminar throughout.We are also obliged to our principal, Resp. **Dr. A.W.KOLHATKAR** who has been a constant source of inspiration throughout.

Lastly, but not least, we thank all my friends and well-wishers who were a constant source of inspiration.

**REFERENCES**

[1] [3GPPTS202] 3GPP TS 35.202 V3.1.1 Technical Specification.

[2] [3GPPTS205] 3GPP TS 35.205 V6.0.0 Technical Specification.

[3] [3GPPTS201] 3GPP TS 35.201 V6.1.0 Technical Specification.

[4] [3GPPTS121] 3GPP TS 23.121 V3.6.0 Technical Specification.

[5][Zheng05a] Yu Zheng, Dake He; Lixing Xu and Xiaohu Tang, "Security scheme for 4G wireless systems," Proceedings. 2005 International Conference on Communications Circuits and Systems, Vol. 1, Page(s):397 – 401, May 2005 .

[6][Joseph06] Joseph, V.C.and Talukder, A.K.;" Verifiable AKA for beyond 3G wireless packet services," 2006 IFIP International Conference on Wireless and Optical Communications Networks, pp. 11-13 April 2006.

[7] [Zhang05] Muxiang Zhang and Yuguang Fang; "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Transactions on Wireless Communications, Vol. 4, No. 2, PP. 734-742, March 2005.

[8] [Barba93] Barba, A., Recacha, F. and Melus, J.L., "Security architecture in the third generation networks," Proceedings of IEEE Singapore International Conference on Networks,1993. International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Volume 1, PP. 421 - 425 , Sept. 19