4G LTE Network Growth in India and Security Issue in Network

Hina Firdaus
B.Tech CSE, (M.Tech CSE) Jamia Hamdard University, New Delhi-62 7827261428

Abstract:
The advancement and migration of the broadband wireless communication technology into the next generation technology known as Fourth Generation (4G) network has indeed become the next emergent wireless revolution, as an important milestone beyond third generation. 4G networks are introduced with the main intention of customization of a flexible and ubiquitous service provision in the middle of 2012 based on digital broadband packet and all IP very high throughput speed of 100-300 Mbps in peak. The widespread growth of the 4G technology in India will be driven by set of new services which will be made useful for the customers such as accessing the internet and video anywhere, any time and in any places with global roaming and full-fledged support for all other multimedia applications. In India even though 4G technology is introduced early in the year 2014, it's still not widespread due to some of the challenges faced by the mobile or wireless communication service providers. 4G has the advantage of mobility, high data rates, high capacity and preservation of full backward compatibility. The high speed capability and wider coverage has been a good achievement for 4G networks. Nevertheless, security and improved higher speed with a better quality of service (QOS) has been an issue in its network operations due to the open nature and all IP infrastructure of 4G network. Long-Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (Wimax) are among the numerous new innovation technologies which have evolved as leading contenders for the 4G technology. This article explores the trends in the evolution of 4G wireless technology and its security limitations. Finally, it evaluates and recommends ways of tackling the security issues in 4G network.

Index Terms
Security, 4G Wireless, LTE, Wimax, Wireless communication, Jio 4G,VoLTE.

1. Introduction

4G (fourth generation) network provides data access at superfast speeds for mobile devices. The technology used for 4G makes it up to 100 times faster than 2G or 3G speeds. A 4G system provides mobile ultra-broadband Internet access, for example to laptops with USB wireless modems, to smartphones, and to other mobile devices. Conceivable applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, 3D television and Cloud Computing. Two 4G candidate systems are commercially deployed: the Mobile WiMAX standard (at first in South Korea in 2006), and the first-release Long Term Evolution (LTE) standard (in Oslo, Norway since 2009). It has however been debated if these first-release versions should be considered to be 4G or not. In the U.S., Sprint Nextel has deployed Mobile WiMAX networks since 2008, and MetroPCS was the first operator to offer LTE service in 2010. USB wireless modems have been available since the start, while WiMAX smartphones have been available since 2010 and LTE smartphones since 2011.

Equipment made for different continents are not always compatible, because of different frequency bands. In India BSNL first launched a 4G service through 4G WiMAX Broadband in Kochi Kerala in 2011. But even today 4G wireless services have not spread to some rural areas of India other than some major cities. Recently in 2016 Reliance launches Jio 4G network in India as trial which will be fully functional after December 2016 in Indian market. In this article, we discuss the growth of 4G technology in India. Challenges and opportunities of 4G technology in India are studied using the ABCD model. The main features of 4G services of interest to users are application adaptability and high dynamism users traffic, radio environment ,air interfaces, and quality of service. The major difference is the fact that 4G wireless network operates entirely on the IP protocol and architecture, which is what brought about the similarity between LTE and Wimax. However, these two technologies also differ from each other in some other aspects such as network architecture and security. Consequently, the open nature and all IP base infrastructure of these 4G wireless networks have increase security issues when compared with other wireless technologies and also significant attention has been given to security design during the development of both the LTE and Wimax standards. The mission of securing 4G wireless networks and systems is a very challenging one owning that a lot of sacrifice must be made each time extra security mechanisms are carried out in its network as an IP based network, there is an impact on the performance and traffic handling capacity of the network and quality of service.

II. Background

India will become a dominant market for 4G technology due to the development of telecommunication industry and increased population. One of the main obstacles for the future and growth of 4G technology in India is the reduced speed of the internet compared to the developed

Manuscript received November 5, 2016
Manuscript revised November 20, 2016

countries like USA. The introduction of 4G technologies in India is benefited to different sectors such as telecommunication, healthcare, education and entertainment. In India the increased use of smart phone users has positive impact on the popularity and growth of 4G technology. Network discovery, access technologies, network architectures, network conditions, charging and billing, large number of operators, security, congestion control are the some of the research challenges that need to solve for the development and advancement of the 4G networks.

In India almost everyone ended up upgrading 2G to 3G network, due to the faster availability of services and without more difference in terms of cost. The upgradations from 2G to 3G network do not require a complete reworking of the architecture of the network system. But in case of 4G network, it becomes necessary, adopting a new equipment or handset in order to avail new services. This becomes costly for the Indian customers, is also one of the hindrance to the growth of the 4G technology. In 2G and 3G spectrum band is uniform across different countries where as 4G is offered in different countries with different frequency bands. Reliance Jio has the most amount of liberalized spectrum among Indian carriers, with a nationwide license on the 2300MHz frequency, along with airwaves in the 1800MHz band and 10MHz spectrum in the 850MHz frequency that's purchased from RCOM in ten circles: Assam, Bihar, Haryana, Himachal Pradesh, Jammu and Kashmir, Madhya Pradesh, Mumbai, North East, Odisha, and Uttar Pradesh (East). The carrier is looking to create an integrated 4G network that leverages all three frequencies to provide seamless connectivity.

Unlike 3G, 4G does not offer voice based services through mobile networks, instead it offers voice over internet protocol (VoIP) and it’s based on packet switching technology. In India not all the service providers have the option to provide seamless 2G, 3G and 4G services using same spectrum band. In India 4G Jio's network is VoLTE, which allows for high-definition voice calls to be placed over the data network. VoLTE has significant cost benefits as it reduces the need to install a lot of base towers. Coverage on the 700MHz band is twice that of the 1800MHz band, and four times as much as what you get on the 2300MHz frequency.4G services are limited to data only without voice services. Portability and file clearing process are the two biggest obstacles or barrier for 4G implementation and development in India. The mobile telecommunication service provider’s who develops 4G networks exclusively and greatly depends upon advanced technologies and higher speed in order to dominate over their counterparts. 4G requires a data transfer rate at least 100 megabits per second when the user is moving at high speed and 1giga bits per second when the user are stationary or in a fixed position.

III. 4G Network Standards

The International Telecommunication Union (ITU) named the International mobile Telecommnication- 2000 (IMT-2000) as a global standard for 3G wireless communications in previous time but later went further to improve the initiative by introducing IMT-Advance which is considered as the specification for 4G wireless. The objective of IMT Advance stated that 4G wireless technology must support the following:

1) High data rate (1Gbps peak rate for low mobility and 100Mbps peak rate for high mobility).
2) High capacity.
3) Low cost per bit.
4) Low latency.
5) Good quality of service (QOS).
6) Wider coverage.
7) Mobility support at high speeds.

Several broadband wireless access technologies have been developed but only LTE developed by 3GPP and Wimax developed by IEEE 802.16 got the characteristics for 4G wireless technology.

IV. 4G LTE Network Architecture

4G LTE architecture was developed by 3GPP taking into consideration security principles right from its inception and design based on five security feature groups.

(i) Network access security, to provide a secure access to the service by the user.

(ii) Network domain security, to protect the network elements and secure the signaling and user data exchange.

(iii) User domain security, to control the secure access to mobile stations.

(iv) Application domain security, to establish secure communications over the application layer.

(v) Visibility and configuration of security, bring the opportunity for the user to check if the security features are in operation.

The latest study being developed by 3GPP is an evolution of 3G into an evolved radio access called LTE and evolved packet access core network in the System Architecture Evolution(SAE).

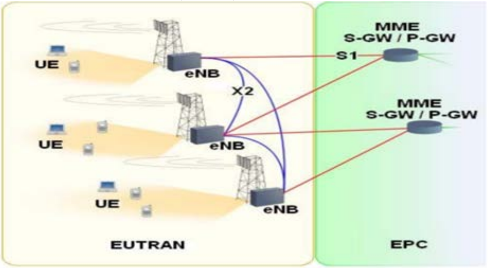

Figure 1 LTE-System Architecture

Figure 1 above shows the LTE architecture. The User equipment (UE) like mobile phone or computer connects to the wireless through the eNodeB within the E-UTRAN (Evolved UMTS Terrestrial Radio Access Network).The E-UTRAN connects to the EPC (Evolved Packet Core) which is IP-based. The EPC connects to the provider wire line IP network. An LTE network has two types of network elements :-

(i) the eNodeB which is an enhanced base station which incorporates all the radio interface-related functions for LTE. The eNodeB also carried higher functions like Inter-cell radio resource management (RRM), Radio admission control, Scheduling via dynamic resource allocation, Enforcement of negotiated QoS on Uplink and compression/decompression of packets destined to/from the UE.

(ii) The Access Gateway (AGW) which comprises all the functions for the EPC. The AGW consist of multiple of modules such as Home Subscribe Server (HSS), Packet Data Network Gateway (P-GW), Serving Gateway(S-GW) and Mobility Management Entity (MME) which is the key control node responsible for managing the UE identity as well as security authentication and mobility.

The LTE standard is flexible which makes it to allow the combination of these AGW modules into a single or multiple devices. LTE maintains a meshed architecture which allows greater efficiency and performance gains. For instant a single eNode can communicate with multiple Access Gateways. LTE utilizes a flat all IP-based architecture and traffic originating at a UE is generated in a native IP format and then processed by eNodeB & AGW [4]. The main task of AGW is to distribute the migration of messages to eNodeBs; security control, encryption of user data ,switching of U-plane to support UE mobility and idle mode mobility handling.

V. Growth of 4G in India

Telecom tower companies are expected to see a sharp upswing in volume growth with India’s largest telcos — Bharti Airtel, Vodafone India, Idea Cellular and new entrant Reliance Jio Infocomm likely to step up expansion of highspeed data communication networks after beefing up their 4G spectrum holdings across key markets in the largest airwaves sale. India has among the world’s lowest percapita data consumption due to the lack of wired Internet. The total number of wired connection is estimated to be just around 3540 million in a country of 1.3 billon people. As such, 4G wireless is expected to create a revolution in the country. Jio has invested significantly in its telecom infrastructure and expects to cover 90% of the population by March 2018 (over 70% currently).

In fact, according to Cyber Media Research, 4G/LTE device shipments in India reached 5.7 million units during April-June 2015, recording a 154 per cent quarteron-quarter growth. This will mean that by next year most of the smartphones sold in India will be 4G devices. Companies like Micromax have already suggested that up to 25 per cent of their smartphones will be 4G by the end of the year. But 3G is not going to become redundant, nor is 2G. Service providers are expected to use these three technologies to help them manage the increasing pressure on spectrum. Actually, it is impossible for any of these technologies to completely solve spectrum issues now. By coming year, we will see 2G, 3G and 4G offering different swim lanes with differentiated user experience. This is why the advent of 4G is important– it is going to free up spectrum in 3G as people migrate to the newer technology. The domino effect of this will be 2G becoming cheaper for the first time Internet users.

VI. Challenges of 4G Technology

Deployment and growth of 4G technology in India is not easy due to several challenges faced by the telecommunication industry or 4G service providers.

A. Security: The 4G, LTE should focus on security objectives and corresponding technologies. Howard, Walker and Wright, of the British company Vodafone quote some security principles for 3G, which hold good, even for 4G Technology as adequately protect information against misuse in different situation/users like while user generating or accessing information, worldwide interoperability and roaming between different operators, between user and provider. It should also ensure that the security features and mechanism can be extended and enhanced as and when required for advanced applications or services.

B. Backhaul: While using the 4G network maximum amount of data transfer takes place between sever and application due to the consumption of bandwidth hungry applications. In order to meet the advanced applications and user requirements operators need to upgrade their backhaul, or bandwidth capacity in exponential form.

C. Multiple Frequencies: One of the major challenges is 4G LTE network uses multiple frequency band or spectrum in different countries. Moreover, operators need to add more radios/ spectrum other than their 2G and 3G spectrum band, which will incur more cost and complexity.

D. Voice over LTE: LTE has the capacity to carry all types of voice, video and data traffic services. But in India most of the operators have given more emphasis for the deployment and development of only data traffic without proper voice and video services. Operators can provide voice over LTE service using three approaches, namely IMS based “one-voice” approach, Voice over LTE via

Generic Access (VoLGA), and Circuit Switched Fallback (CSFB).

E. Price and Smart Phone: India is always priced sensitive market, due to these operators always introducing one or other new cost tariff plans for both data and voice. The price of the 4G network is more, is the one more challenge faced by the operators in India. Compared to the entire population of India only few customers have smart phones and in which all smart phones do not support LTE.

F. Quality of Service: In India the service providers or operators always struggled to provide quality of service, even though they do a lot of efforts due to the large and diverse need of the huge populations. Data coverage has a lot of inconsistency in the rural parts of the country. In 4G, service providers should satisfy the customer as LTE expected to consume heavy data content such as videos, games and stream content.

G. Application/content: With 4G, customers are more interested to watch online video while they are moving or traveling causes more consumption of online videos. As more and more customer's uses HD videos, streaming of HD videos is going to put a huge stress on the LTE network for which operators or telecommunication industry needs to be prepared.

H. Chipset compatibility: LTE chipsets needs to be built based on eco-friendly is one of the barriers around selection of different technologies and in the improvement of chipset performance. While developing chipset vendors should focus on some key parameters like Support for multiple technical parameters, backward compatibility, and reducing power consumption and chip size.

I. Return on Investment (ROI): Migration from 3G technology to 4G LTE entails high capital investment for the service providers due to the high spectrum costs and upgrades in network infrastructure. The biggest risk, therefore for an operator is to justify the ROI and sustaining in the market, in LTE network deployment.

J. Widespread of LTE to rural: All the operators in India focusing their 4G services in some of the Metropolitan cities and urban towns. In order to improve the performance and to get a huge number of customers' operators should focus on deployment of 4G services even rural areas of India.

K. Slow Internet Speed: According to the report, Reliance's 4G network, which is predominantly in 2300 MHz high frequency band, suffers from poor coverage which has been the key issue. Researchers say there is a need to offer higher bandwidth and increase the internet speed, if new technologies like 4G have to be a success.

VII. Opportunities of 4G Technology

4G networks are designed to facilitate the development of different sectors like telecommunication, healthcare, education and entertainment to the existing 3G technologies in terms of quality, bandwidth and data and video transmission and accessing speeds. Following are the different opportunities on 4G technologies.

A. Cost and affordability: When 4G communication technology and network coverage increases the competition between service providers also increases. This creates more demand and popularity in the market. 4G service cost can be reduced with the high demand and popularity of 4G technology. 4G networks are designed in order to create an environment that supports embodied in speed, bandwidth, low cost, better network, efficiency, personalization and advanced access technologies. As the technology reaches more and more customers or public cost and affordability successfully reduces.

B. Personalization: The personalization requires an integration and organization of a user's preferences. 4G Technology adapts sensor network, user profile and databases in order implement personalization or customization of user requirements.

C. Advanced Access Technologies: 4G technology uses MIMO-OFDM (Multi in Multi out Orthogonal Frequency Division Multiplexing) to better distribute resources among available various clients.

D. Coverage and Availability: 4G signals with more than 800MHz super frequency can penetrate to any extent with walls and any object to ensure wider coverage. If the service provider deploys proper and advanced technologies it can be available ubiquitously without any barrier to time, place and locations.

E. M-learning Capability: Using the 4G network in m-learning model, students can login to their notebook through valid username and passwords and can get information in terms of different multimedia applications like plain text, pictures, audios and videos and at the same time authorized instructor can upload information or contents like homework, announcements, SMS and quizzes.

F. Improved Entertainment for an Individual: An individual can get the benefits of 4G technologies as watching video with HD quality, video calls with high quality and high quality gaming applications. Due to this more and more customers, start watching their hand set for different video purposes will increase the demand and market of smart phones.

G. Banking sectors gets benefited through mobile banking: By adopting 4G technology, banking services can reach to rural area customers with high security through their smart phones. So customers can able to access their banking services anywhere, anytime and anyplace.

H. Private and Public organization Performance Improvement: Private or public organization can improve their performance with the use of 4G technology by reducing their cost of travel, tracking the employees, instant update on all government projects implemented and by utilizing high quality of video conferencing.

VIII. 4G LTE Reasons Lead to Failure in India

Given the present 2G and 3G mobile Internet speeds in India, it could be safe to assume that most users were just waiting for 4G to happen. After all, 4G by definition is fast. Or, it should be. Of course, it is too early to comment on the state of 4G connectivity in India. However, it is clearly visible that telcos are more excited about 4G than consumers, despite the promise of more speed at the same price of 3G.

Here are five obvious reasons as to why majority of subscribers are not eager to join the 4G bandwagon, at least initially.

1. *More the subscribers lesser the speeds:* All three technologies -- 2G, 3G and 4G will continue to coexist in India. By 2020, GSM Association expects around 50% subscribers to continue with 2G. Consumers are well aware that telcos need to upgrade their network capacities to accommodate new subscribers. So, even if users get excellent 4G speeds initially, the speeds are expected to fall as the number of 4G subscribers goes up. To avoid this, telcos will have to constantly upgrade their infrastructure, something very few subscribers are ready to believe.

2. *Device issues:* Most subscribers are still confused with what to expect from 4G connections in terms of device compatibility. Majority thinks they would need to buy a new smartphone altogether to use 4G. Also, the entire 'Indian 4G band' explanations have just added to the confusion.

3. *Super fast 4G connectivity means data packs exhaust faster:* Most subscribers feel 4G will simply increase their mobile bills. As apps constantly consume data with background activities, 4G will simple provide a better highway for them. Also, 4G will promote more gaming, streaming and video consumption among subscribers, accelerating data consumption. Will I actually get 4G always? Given the inconsistency in 3G connectivity, in which most end up with a disappointing loop of either 'H' or 'G', mobile users are skeptical as to whether they will actually get 4G speeds always. Or, will end up again getting 2G. In fact, many consumers have coined a new equation: 4G=3G=2G.

4. *Call drops:* With TRAI struggling to resolve the call drops issue, subscribers feel that if 2G cannot provide quality voice calls then 4G is nowhere close to it, given it is new. Most believe that call drops will only increase with 4G.

5. *And lastly do I really need 4G?* Just because it is fast doesn't mean everybody would need it. Most subscribers are used to whatever 3G speeds they are receiving at the moment and are not willing to bet more on their expectations.

IX. Threats to 4G LTE

The changes specific to 4G permit seven unique variations on older attacks. By understanding the nature of these threats

and vulnerabilities, carriers and service providers can act to mitigate them.

A. Wireless APN flooding

The expanding bandwidth of 4G provides a larger attack surface for cybercriminals. The dribble of data through a 24 kb–256 kb 2G and 3G wireless network becomes a flood of data with 3-150 Mbit 4G networks. In the absence of aggressive counter measures, criminal activities will consume so much of this new bandwidth that users who have paid to upgrade to 4G service will get 2G speeds. Figure 2 illustrates the attackers' automated probing and scanning software and the traffic from "enslaved" devices that can quickly monopolize core bandwidth. These actions can flood the wireless architecturally private network (APN) that connects the mobile devices of the 4G network to the Internet. The attacks can consume the "last mile" of scarce, wireless capacity (radio frequencies are physically limited assets—you cannot add more to get more capacity as with fiber or copper wire) and degrade service levels.

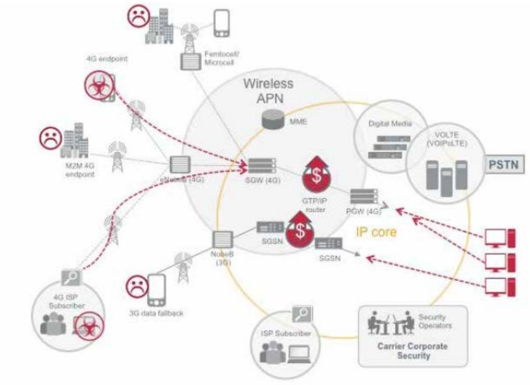

Figure 2 Attacks into a mobile network.

B. Mobile to mobile attacks

Unlike 3G traffic that tunnels directly into the core IP network from the mobile device, 4G traffic is all IP-based and can travel directly from mobile device to mobile device inside the wireless APN. This "peer to peer" (P2P) communication reduces backhaul traffic. However, it also permits mobile-to-mobile (Mob2Mob) attacks.

A compromised mobile device can target and scan large numbers of other, locally adjacent, mobile devices at once, consuming huge amounts of spectrum. This activity frequently goes unseen by the carrier because the wireless APN to which the device connects has limited instrumentation and few internal security capabilities. In addition to siphoning off spectrum, a mobile to mobile attack drains the battery on the victim's device by maintaining a network connection. The attack can also cause a denial-of-service (DoS) situation due to signaling congestion. In an attack, the traffic may enter the network from one mobile device, perform an automated scan to look for devices with similar IP numbers (indicating that the devices are on the same subnet), and then reach back out over the 4G network to contact those devices.

Once an attacker has exhausted one range of IP addresses, the attack moves to the next range and begins to attack and infect the new devices. Unfortunately, the mere act of scanning for responding IP addresses of other mobile devices can cause severe DoS due to the previously mentioned signaling congestion. To avoid users being denied a connection, the operator would need to invest in better security or: more spectrum, more LTE base stations (eNodes), and more backhaul network—which lead to more capital expense, more operating expense, and more management complexity. The user may experience degraded service and also shoulder the burden of these incremental costs over time. Inevitably, unhappy users lead to account churn.

C. eNodeB/Femtocell/Microcell compromise

As part of a cost containment strategy, many carriers are adopting virtualization technology at the radio edge, in the mobility management infrastructure, and even in the networks. These commodity hardware platforms and commercial, off-the-shelf software components have the ability to increase equipment utilization and drive down capital and operating costs. However, virtualization in mobile networks may also introduce vulnerabilities that attackers can exploit. For example, a common eNodeB (4G basestation) may use a virtualized Linux operating system instead of a custom OS that has been explicitly hardened—made secure—during development. If a virtualized eNodeB in the 4G network is successfully attacked through a security flaw in the commercial hypervisor or operating system of application (radio) software, it may fail. Or, worse, it may become a launching pad for attacks against the overall network management infrastructure behind it. Each lost Femtocell hurts service availability for multiple users. With its position in the IP core, loss or compromise of the management infrastructure takes down a much higher number of users. It is the critical control point for the 4G network, accessible from Femtocells, Microcells, and eNodeB as a matter of design.

It's true that the management infrastructure generally shelters within the protection of the network, but this infrastructure still needs to maintain open connections to service its users. If an attacker can get into a trusted device like an eNodeB, the attacker can navigate to many other internal devices (such as the management infrastructure). Once they have penetrated the network infrastructure, attackers have many ways to disrupt services or cause outages—outcomes that hurt revenue and customer retention. Specialized security optimized for hypervisors and other virtualization technology can mitigate the risks of attack. This security adds comparatively minor costs relative to the costs of service degradation, as measured in lost usage revenues, customer churn, service level breaches, and regulator audit and inquiry.

D. Machine to machine fragility

The Internet of Things (IOT) includes not only devices managed by people, such as desktops and smartphones, but semi-automated and fully automated devices that control physical outcomes, such as traffic lights, pipeline pressure sensors, electrical grids, and water utilities. These devices are sometimes referred to as engaging in "machine-to-machine" (M2M) networking. Traditionally, these fixed-function devices were built without much concern for security, since they used limited, dedicated networks that were not connected to a public network.

Simple probing of the network (performed by vulnerability scanners as well as would-be attackers) can have adverse effects by destabilizing controllers. Hindering potential mitigations, field-based sensors are resource-constrained, with minimal memory and CPU to spare: there is no "room" to install firewalls or even basic security capabilities. In some cases, these devices run legacy, unpatched, and unpatchable operating systems. In most cases, even modern M2M systems and devices are not intended to operate within the hostile and unhygienic environment of the Internet—yet that is what 4G will become without adequate security. When attacked, devices may just shut down—without warning, and sometimes without an easy or fast recovery.

Disruption of ICS devices can lead to costly civil emergencies or loss of life. This feared scenario is driving critical infrastructure operators and the governments that regulate them to invest heavily in understanding and implementing more rigorous security controls. For service providers looking to provide the networks for these burgeoning new M2M applications, a degree of security and awareness related to mobile-on-mobile attacks will be a business enabler.

E. Lawful intercept compliance

National regulations and licensing rules typically obligate carriers to intercept many different types of traffic when they receive a judicial order. In 4G networks, full interception for a given endpoint requires data collection at up to three different places in the IP
network, as seen in Figure 3:

- *Edge cache traffic*—Create a system for managing copies of frequently requested content that is stored at the edge of the network, so one copy can serve many endpoints without multiple downloads through the backhaul network.
- *Voice calls*—Track and intercept voice over IP and voice over LTE traffic.
- *Internet traffic*—Intercept “long haul” email and web interactions headed to and from the Internet directly (versus the
edge cache).

Government regulators expect carriers to solve this problem before LTE services go live. Actually, regulators don’t necessarily possess any awareness of LTE or 4G network improvements. They simply require that judicial orders are fulfilled. The problem of “how” is largely left to the service provider to figure out.

Additionally, lawful access requests typically come with precious little compensation for service providers, so the more efficient and elegant the solutions, the better! Designing this interception, monitoring, and collection capability into the relevant points of the network will allow you to preserve your network compliance with lawful access requests and judicial orders.

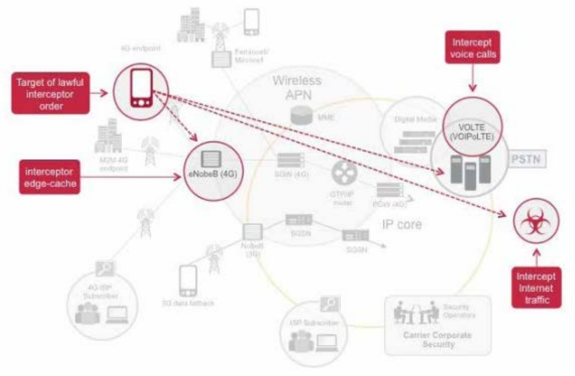

Figure 3 Compliance requires support for multiple lawful access intercept point

F. VOLTE service assurance

So far, we have looked at the weaknesses of different devices that participate in the “data” side of the 4G network, which leads to the open Internet and the wealth of data and services to be found there. However, there are other services that will reside entirely inside the 4G network. These services represent substantial value to device users: namely, the voice services and media services. VOIP attack tactics that have evolved on the Internet can be used just as effectively against VOLTE, even if the VOLTE infrastructure is not accessible from the Internet. Why? Because VOLTE infrastructure must be accessible from any mobile device subscribing to voice services from the service provider. In this age of pre-paid accounts and phones purchased and topped-up from automated kiosks, restricting only “friendly” and recognized subscribers to the VOLTE infrastructure is difficult.

There are several thousand known attacks against VOIP protocols that range in outcome from capturing administrative privileges to denial-of-service attacks. The impact on voice services to consumer and business users, as well as emergency services that support police, fire, and medical resources, can be highly disruptive and dangerous and result in regulatory issues. Because VOLTE traffic remains largely within the wireless APN, carriers need different monitoring equipment to detect attacks as they move through the 4G infrastructure to the VOLTE service infrastructure.

G. Content and media delivery

Paid-for content and media, such as movies or music-on-demand, are another element of the 4G broadband ecosystem. They present the potentiality of significant additional revenues to service providers, especially since up to 50 percent or more of the data travelling over the Internet is already video, according to Cisco. Making video and music available from localized portals connected directly to the wireless APN can offer performance and variety (due to formalized licensing and digital rights management) that cannot be had from “over the top” services accessed via the Internet. As was the case with VOLTE, unauthorized access and denial-of-service attacks can jeopardize expected revenue from broadband media services, degrade services, and erode subscription and adoption rates.

Carriers should expect attackers to attempt to disrupt content delivery systems during peak times. Internet criminals, hacktivists, and other malicious parties are adept at unleashing their attacks during major events—World Cup matches, elections, or royal weddings, for example. Additionally, wholesale disruption of a broadcast service will be much more visible than a large number of usually unrelated dropped calls. Subscribers who have paid a premium to watch a major sporting event will quickly share their anger through social media. This damages your organization’s reputation and can dampen subscriptions and long-term adoption of new services.

X. Security Risks in 4G LTE

For purposes of this article, the 4G LTE architecture model has been divided into the following network segments: user equipment (UE), Access, Evolved Packet Core (EPC)/Transport and Service network (Figure 2).

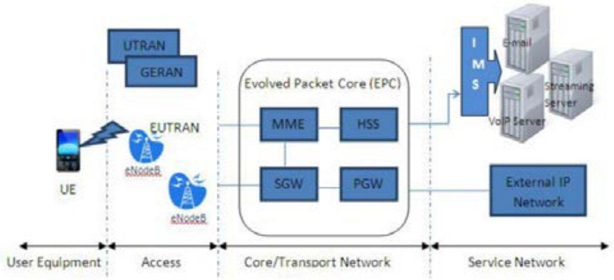

Figure 4. Basic LTE/SAE architecture

Key security threats/risks:

- Distributed network and open architecture
- Decentralised accountability for security
- Complex business models (IS/Service sharing)
- Minimising security spend

Distributed network & open Architecture: 4G LTE architecture brings with it an end to physically segregated networks owned and operated by a single MNO and the security that came with it. With legacy technologies, operators could enforce security policies on their own infrastructure, secure their perimeter and be reasonably confident that a subscriber while on their platform was protected. 4G LTE is an all IP based end to end deployment where seamless roaming with service continuity is offered to the end user. As a result, the MNO entrants to the LTE market, share security risks and threats as their respective infrastructures and services are now interconnected into one aggregated service providing network. Distributed network and open architectures enables weak security configurations on one device or interface provide the entry point to attackers looking to compromise the LTE network.

Complex business models with infrastructure (IS) and service sharing: LTE offers network sharing capabilities that present new business models for MNOs. Service could be offered to end customers by a virtual network operator, where one MNO owns the E-UTRAN while a different one owns the MMEs. Cost benefits will lead MNOs into various models of active infrastructure sharing arrangements with new revenue sharing business models. An example of such network sharing is the joint venture of rival Swedish operators Telenor and Tele2 called Net4Mobility where the radio network and certain part of the access network are shared. Ovum forecasts that by 2015, 30% of all LTE networks will involve some form of active network sharing [6] indicating that complex business models with LTE deployment are here to stay. These types of LTE arrangements bring with it challenges with ensuring consistent security configurations and security management across such virtual network operators. Multiple MNOs with varying security controls and standards interconnecting with shared pools of network elements pose a threat to security levels.

Decentralised accountability: MNOs wishing to present universal end to end security levels to subscribers will find it problematic that a single MNO does not have unilateral decision control over security parameters of the LTE networks and operations. For instance, security standards will vary with global roaming or choice of application, based on the security settings of the application service provider. This decentralised accountability and lack of overall control on security of the LTE service experience will be exacerbated as hosted and cloud services penetrate the marketplace creating new and complex operating models.

Minimising security spend: LTE operators are quickly deterred by the millions of dollars required for a full IPSec rollout alongside other security infrastructure deployments and look to cut corners and launch to market with the minimum requirements to provide service. There is significant disparity between network designs of large operators and smaller operators with limited resources. With LTE the interconnectedness of the network brings the security level of the overall architecture to the level of the least common denominator, lowering security thresholds. Preventative measures: Interoperability standards Security audits with remediation commitments Strong partner agreement Security Budget

Interoperability standards: As legacy network architectures have been closed, interoperability with MNO peers were founded on implicit underlying trust, that each MNO would secure their own networks. With subscribers roaming on the LTE ecosystem, and the interconnectedness of legacy platforms, trusted and untrusted networks, it is imperative that MNOs set out interoperability standards and configurations to ensure the MNOs service, network and service promise to the subscriber is not compromised. For example encryption, latency or quality of service (QoS) specifications should be set out between peer operators in order to enable contiguous security and service levels.

Strong partner agreements: MNOs should set out security standards, policies including configuration requirements within their partner and peering arrangements. These agreements should particularly set out implementation of security infrastructure and configuration such as security gateways, security protocols, subscriber security parameters in vertical hand offs, QoS, key management, authentication, encryption, confidentiality and privacy policies. In addition, MNO's should ensure that the set security measures are cascaded down to relevant 3 party agreements, partner MNO's may enter into.

Audits: Regular third party audits of partners should be set out in agreements to verify and enforce required security standards, policies and practices allowing for remediation and hardening as identified, in advance of potential security attacks.

Security Budgets: MNOs should allocate funds for security infrastructure and operations in their LTE deployment to ensure they meet their business objectives while minimising risks to levels acceptable to the MNO. The MNO must keep in mind legal and regulatory requirements for security and privacy while building out LTE networks and plan fund allocation accordingly. Since inadequate security measures have the potential to damage the MNOs business, it is prudent for the MNO to give security investment due consideration and priority.

XI. ABCD Analysis of the 4G Technology

The 4G technology are analyzed using Advantages, Benefits, Constraints and Disadvantages (ABCD) analysis by considering different issues, which includes security, bandwidth, multiple frequencies, voice over LTE, quality of service, application/content, chipset compatibility, return on investment (ROI), widespread of LTE to rural, cost, affordability, personalization, advanced access technologies, availability, m-learning capability, improved entertainment for an individual, mobile banking and private and public organization performance improvement.

Advantages:

- Increased security helps to improve the customer trust over new technology, authentication. There will not be any altering or changes in data during transmission and user cannot deny not sending the message because only sender and receiver will have a unique pair of password or OTP.
- When bandwidth is increased more data can be transmitted between sender and receiver. The user will be satisfied because of high bandwidth while accessing the internet or HD videos. Quickly download a file over the internet, easy access internet or multimedia files and HD videos.
- Implementing standard global frequencies will reduce the cost of the service provider and in a single stream able to deploy 2G, 3G and 4G services.
- Voice over LTE will increase the capacity to carry all types of voice, video and data traffic services; due to this more and more customers are attracted to new technology.
- Quality of services will be improved with the adaptation of proper advanced technologies in terms of availability of audio, HD video, data services ubiquitously.
- Extremely high voice quality and HD video ubiquitously due content/application services.
- Services based on user habit, preferences and needs can be provided due to personalization or customization of services.
- 4G communication technology provides some intelligent networks like open distributed AD-HOC wireless network and software defined radio.
- Through 4G technology Learners can control their own learning time by portable mobile devices. Mobile learning is more helpful for someone who are no longer restricted to time, place and locations.
- Private and public organization can grow due to 4G technology by reducing their cost of travel, tracking the employees, instant update on all government projects implemented and by utilizing high quality of video conferencing.
- With the adaptation of 4G technology, banking institution can provide banking services to its customers in rural areas through mobile banking services.
- When 4G communication technology and network coverage increases the competition between service providers also increases. This creates more demand and popularity in the market.

Benefits

- 4G are very easy to install and maintain.
- Due to higher security, service provider or operators gets more profit and popularity and advancement of the new technology also improved.
- Global or national wide expansion of 4G services.
- The ability to obtain a larger customer base due to ubiquitous services.
- The ability to take advantage of the growing popularity of Smart Phone banking Enhances reputation of the operators by providing fast and secured services to its customer.
- Expansion of Smart Phone users. Banks can able to attract business people, software engineers or other tight scheduled customer pool due to their nature of professions for mobile banking services.
- High quality of services.

Constraints

- Lack of newer technology support.
- Possible failure of new technology due to non-acceptance of customer.
- General competitiveness of the service providers.
- Mandatory of smart phones or shifting of new equipments cost more for the customer reduces the 4G usage in India.

- Government policies will affect on usage of 4G services.
- Different frequencies are used for 4G services in different countries creates an extra burden for service providers.

Disadvantages

- New frequency requires added components in the service provider's tower.
- 4G does not offer voice services through mobile phone rather than it uses voice over internet protocol (VoIP).
- When the user logged on to 4G services will be transferred to 3G services, when the user receives a voice call.
- Voice over LTE (VoLTE) new services of VoIP in 4G technology, is not widespread or it's in infant stage.
- Portability and file clearing in 4G technology is a lengthy process, which is very costly, not affordable by ordinary customer.
- Requirement of high memory and processors at service provider's servers.
- Lack of technology support.
- Initial investment in technology will be expensive.
- Lack of trained staff.

XII. Conclusion

4G wireless technologies provides a wide variety of services, which includes improved bandwidth, advanced personalization or customization, high speed HD video and multimedia services. With the deployment of 4G technology Indian Telecommunication industry and Information technology witnessed massive significant transformations. In this paper we have discussed the some of the challenges in terms of Security, Bandwidth, Multiple Frequencies, Voice over LTE, Price and Smart Phone, Quality of Service, Application/content, Chipset compatibility, Return on Investment (ROI), Widespread of LTE to rural area. We have also discussed opportunities of 4G technology in India in terms of Cost and affordability, Personalization, Advanced Access Technologies, Coverage and Availability, M-learning Capability, Improved Entertainment for an Individual, mobile banking, Private and Public organization Performance Improvement.

The 4G technology is analyzed using the ABCD model which explains the advantages, benefits, constraints and disadvantages of 4G technology with special reference to Indian market. 4G LTE brings with it increased complexity in security management for the MNO, however, with proper diligence MNOs can minimize the impacts of various security threats. It is well known that security is a moving target that needs continuous attention and investment to keep abreast of the changing threatscape. Security is an integral part of the business lifecycle of MNOs and will continue to remains as such with the adoption of 4G LTE services and technologies.

The Indian market will play a significant role in the future growth of 4G technology due to its population and a wide variety of customer requirements. Wish this article could help to understand the growth rate of 4G technology in India with its consecutive security issues and threats.

Acknowledgment

We would like to thank Mr. Akeel Khalique for his suggestions and comments to improve the contents and presentation.

References

[1] K. Krishna Prasad, P.S. Aithal, " The Growth of 4G Technologies in India-Challenges and Opportunities", IJMIE, Volume 6, Issue 1,Jan 2016.

[2] Priya Gautam, Savneet Kaur, Ramandeep Kaur, Sumeet Kaur,Harish Kundra, " Review Paper on 4G Wireless Technology", International Journal of

[3] Advances in Science and Technology (IJAST) Vol 2 Issue I March 2014.

[4] K.R Rakesh, " A Framework of (4G) Wireless Networks- Overview and Challenges", Journal of Excellence in Computer Science and Engineering, Vol. 2(1) 2016.

[5] Chukwu Michael .C, " Comparative study and Security Limitations of 4G Network", Case Study LTE and WIMAX.

[6] Sinha Naveen Kumar, " EMERGENCE OF 4G TECHNOLOGY IN INDIA AND ITS FUTURE IMPLICATIONS", I.J.E.M.S., VOL.4(2) 2013.

[7] Sonali Chavan, Vanita Mane, " 4G Wireless Networks Challenges and Benefits", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 7, July 2013.

[8] Daksha Bhasker, " 4G LTE Security for Mobile Network Operators", Journal of Cyber Security and Information Systems, 2016.

[9] Sumant Ku Mohapatra, BiswaRanjan Swain and Pravanjan Das, " COMPREHENSIVE SURVEY OF POSSIBLE SECURITY ISSUES ON 4G NETWORKS", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015.

[10] Tyson Macaulay, " The 7 Deadly Threats to 4G", VP Global Telco Strategy, McAfee.

[11] "India's Slow Internet Speed Threatens 4G Adoption", by CXOtoday News Desk Oct 27, 2014.

[12] "Will 4G drive India's Internet growth?", The Indian Express, 2016.

[13] " Tower companies to see rise in volume growth on expansion of data network by telcos", The Economic Times, Oct 2016.

[14] " Reliance Jio to ride India's telecom growth story", RTN.ASIA, June 2016.

[15] " 5 reasons why 4G is not able to excite mobile users in India", Debashish Sarkar, TOI Tech, 2016.

[16] " 4G in India: Everything you need to know", HARISH JONNALAGADDA, Android Central, May 2016.

[17] " Qualcomm looks at India 4G growth to replicate China story", Alnoor Peermohamed, Business Standard, Nov 2016.

[18] " It’s Superfast and Awesome. But How Secure is Your 4G Network?", VPNCREATIVE.NET

Author Biography

Hina Firdaus was born on 29th March 1995, in Bilaspur, Chhattisgarh. She did her schooling in Sri Chaitaniya Videyaniketan CBSE school in Vishakhapatnam (Andhra Pradesh) and secured 79.9% in the Higher Secondary Examination. She persuaded her B.Tech. Degree in Computer Science and Engineering in the Department of Computer Science and Engineering of B.S. Abdur Rahman University, Chennai with 9.0/10.0 CGPA points. Currently, she is pursuing her M.Tech in Computer Science and Engineering from Jamia Hamdard University New Delhi. Her area of interests include Cryptography, Computer Graphics, Computer Animation and Big Data. The e-mail ID is : hinafirdaus95@gmail.com and the contact number is :7827261428