UNIVERSITY OF PATRAS

POLYTECHNIC SCHOOL

DEPARTMENT OF COMPUTER ENGINEERING & INFORMATICS

PROJECT SEMESTER

COURSE

PUBLIC NETWORKS AND INTERCONNECTION NETWORKS

LTE-A NETWORKS & FEMTOCELLS

GKANTZOS PANAGIOTIS

A.M 1051309

PROFESSOR: BOURAS CHRISTOS

PATRA 2017

CONTENTS

INTRODUCTION

We definitely live in LTE era. Everyone use LTE or LTE-a (advance) networks daily by having a simple phone call to browsing the internet in a mountain with their mobile phone. But no one seems to know how it works or why it's such a big deal. LTE is termed as 'Long Term Evolution,' which has taken the mobile network standard to a whole new level. LTE is the successor technology not only of UMTS but also of CDMA 2000. LTE made the big jump by bringing up to 50 times performance improvement and much better spectral efficiency to cellular networks. All interfaces between network nodes in LTE are now IP based, including the backhaul connection to the radio base stations. This is great simplification compared to earlier technologies that were initially based on E1/T1, ATM and frame relay links, with most of them being narrowband and expensive. LTE-Advanced is the upgraded version of LTE technology to increase the peak data rates to about 1GBPS in the downlink and 500MBPS in the uplink. In order to increase the data rates LTE-Advanced utilizes higher number of antennas and added carrier aggregation feature. Now imagine that with femtocell implementation. Would you like to find out more about LTE-A with some femtocell uses, but you have no idea what iam talking about? If so, this paper will help get you up to speed in no time. You know, before LTE-A we must mention bacics that you may have heard. So, lets understand first how LTE networks work. After all we need to know basics am I wrong?

1 LTE NETWORKS

1.1 Overview

LTE stands for Long Term Evolution and it was started as a project in 2004 by telecommunication body known as the Third Generation Partnership Project (3GPP). SAE (System Architecture Evolution) is the corresponding evolution of the GPRS/3G packet core network evolution. The term LTE is typically used to represent both LTE and SAE.

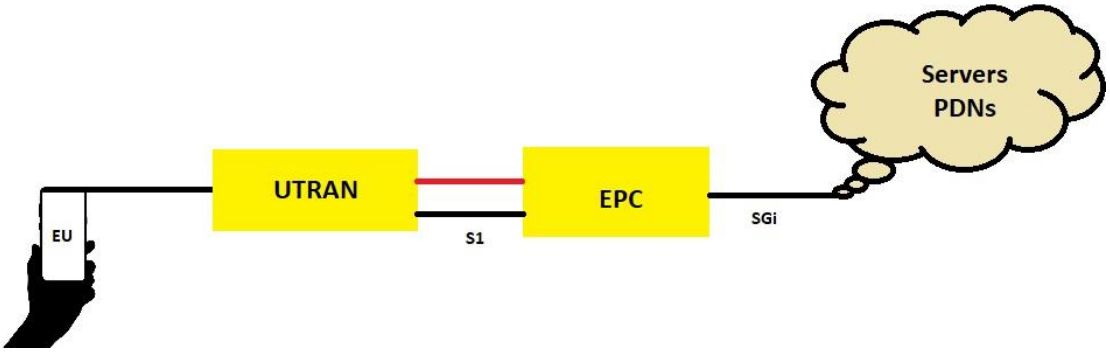
The main goal of LTE is to provide high data rate and low latency. Same time its network architecture has been designed with the goal to support packet-switched traffic with seamless mobility and great quality of service.

LTE evolved from an earlier 3GPP system known as the Universal Mobile Telecommunication System (UMTS), which in turn evolved from the Global System for Mobile Communications (GSM). Even related specifications were formally known as the evolved UMTS terrestrial radio access (E-UTRA) and evolved UMTS terrestrial radio access network (E-UTRAN).

First version of LTE was documented in Release 8 of the 3GPP specifications. It's no lie that the rapid increase of mobile data usage and emergence of new applications such as MMOG (Multimedia Online Gaming), mobile TV, Web 2.0, streaming contents have motivated the 3rd Generation Partnership Project (3GPP) to work on the Long-Term Evolution (LTE) on the way towards fourth-generation mobile.

1.2 Architecture

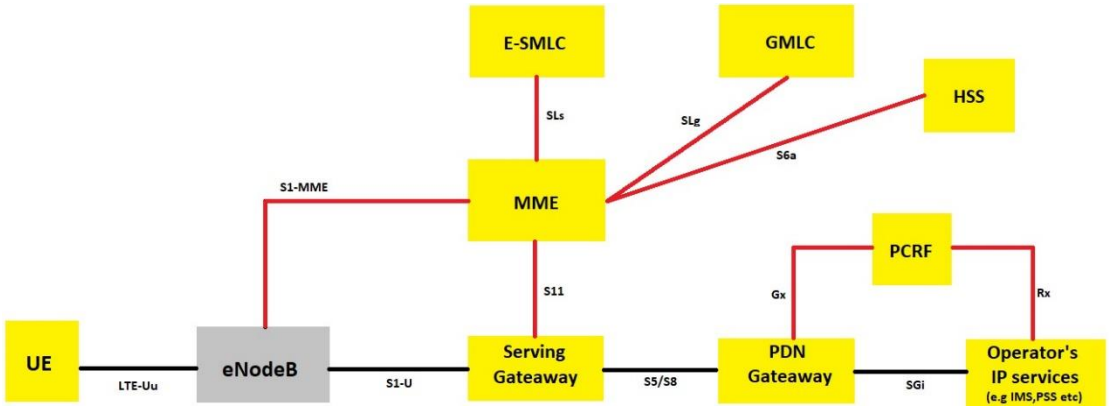
The high-level network architecture of LTE is comprised of the user equipment (EU), the UMTS terrestrial Radio Access Network (UTRAN) and last the evolved Packet core (EPC).



LTE (black is signals, red is traffic)

1.2.1 The Evolved Packet Core

First of all, the term **LTE** encompasses the evolution of the Universal Mobile Telecommunications System (UMTS) radio access through the Evolved UTRAN (E-UTRAN), it is accompanied by an evolution of the non-radio aspects under the term "System Architecture Evolution" (SAE), which includes the Evolved Packet Core (EPC) network. Together LTE and SAE comprise the Evolved Packet System (EPS). EPS uses the concept of EPS bearers to route IP traffic from a gateway in the PDN to the UE. A bearer is an IP packet flow with a defined quality of service (QoS) between the gateway and the UE. The E-UTRAN and EPC together set up and release bearers as required by applications. EPS provides the user with IP connectivity to a PDN for accessing the Internet.



EPS network (black is signals, red is traffic)

Here is a brief description of some components shown in the architecture:

-The Policy Control and Charging Rules Function **(PCRF)** is a component which is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF).

-The Packet Data Network **(PDN)** Gateway (P-GW) communicates with the outside world. Packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN).

-The Home Subscriber Server **(HSS)** component has been carried forward from UMTS and GSM and is a central database that contains information about all the network operator's subscribers.

-The mobility management entity **(MME)** controls the high-level operation of the mobile by means of signalling messages and Home Subscriber Server (HSS).

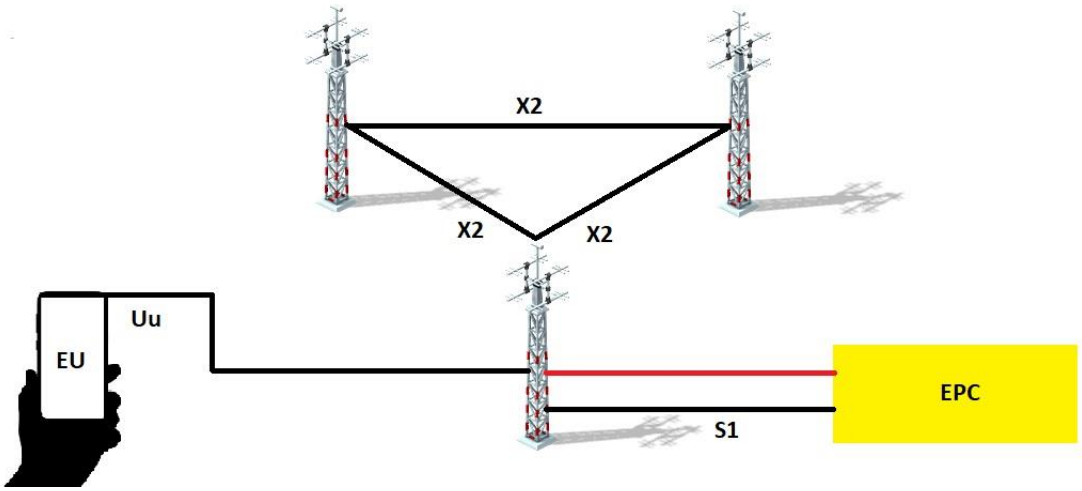
-The **Serving Gateway (S-GW)** acts as a router, and forwards data between the base station and the PDN gateway.

-The interface between the serving and PDN gateways is known as S5/S8. This has two slightly different implementations, namely S5 if the two devices are in the same network, and S8 if they are in different networks.

The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem.

When we are talking about AIR data transferring we can't exclude Security. Security functions are the responsibility of the MME for both signaling and user data. When a UE attaches with the network, a mutual authentication of the UE and the network is performed between the UE and the MME/HSS. This authentication function also establishes the security keys that are used for encryption of the bearers.

1.2.2 The UTRAN (The access nerwok)



The architecture of evolved UMTS Terrest (black is signals, red is traffic)

The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called **eNodeB** or **eNB**. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

LTE Mobile communicates with just one base station and one cell at a time and there are following two main functions supported by eNB:

The eBN sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface also eNB controls the low-level operation of all its mobiles, by sending them signaling messages such as handover commands. Each eBN connects with the EPC by means of the S1 interface and it can also be connected to nearby base stations by the X2 interface, which is mainly used for signaling and packet forwarding during handover.

A home eNB (HeNB) is a base station that has been purchased by a user to provide **femtocell** coverage within the home. A home eNB belongs to a closed subscriber group (CSG) and can only be accessed by mobiles with a USIM that also belongs to the closed subscriber group.

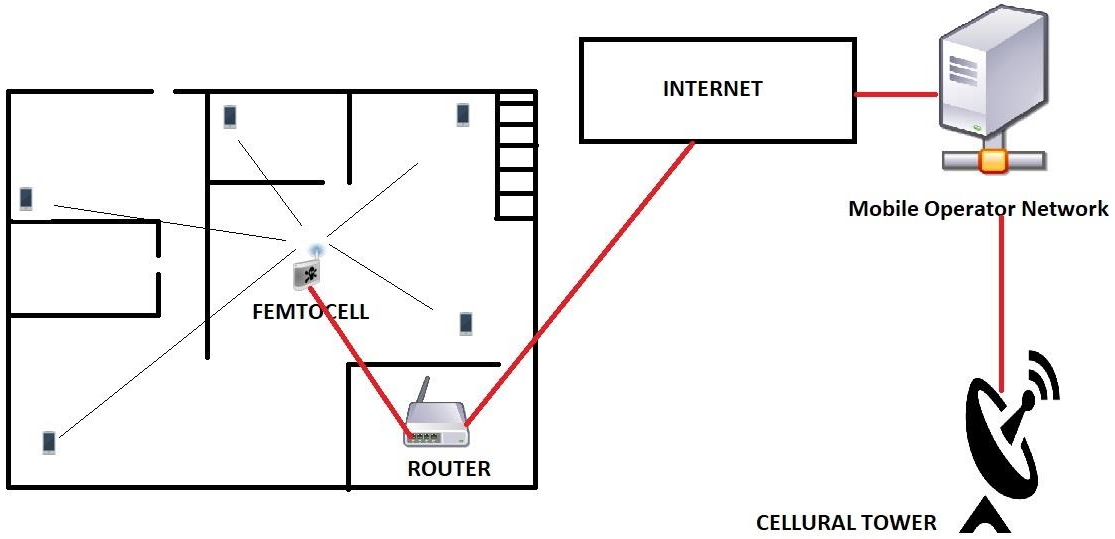
In my opinion know he have a good perspective about LTE networks but before we jump to LTE-A it is as i would say viral to briefly talk about femtocells.

2 FEMTOCELLS

2.1 Overview

In telecommunications, a **femtocell** is a small, low-power cellular base station, typically designed for use in a home or small business. A broader term which is more widespread in the industry is small cell, with femtocell as a subset. It is also called femto Access Point. It connects to the service provider's network via broadband (such as DSL or cable). Current designs typically support four to eight simultaneously active mobile phones in a residential setting depending on version number and femtocell hardware, and eight to sixteen mobile phones in enterprise settings. A femtocell allows service providers to extend service coverage indoors or at the cell edge, especially where access would otherwise be limited or unavailable.

Use of femtocells benefits both the mobile operator and the consumer. For a mobile operator, the attractions of a femtocell are improvements to both coverage, especially indoors, and capacity. Coverage is improved because femtocells can fill in the gaps and eliminate loss of signal through buildings. Capacity is improved by a reduction in the number of phones attempting to use the main network cells and by the off-load of traffic through the user's network to the operator's infrastructure. Instead of using the operator's private network the internet is used.



Consumers and small businesses benefit from greatly improved coverage and signal strength since they have a de facto base station inside their premises. As a result of being relatively close to the femtocell, the mobile phone expends significantly less power for communication with it, thus increasing battery life. They may also get better voice quality via depending on a number of factors such as operator/network support, customer contract/price plan, phone and operating system support. Some carriers may also offer more attractive tariffs, for example discounted calls from home.

Femtocells are an alternative way to deliver the benefits of fixed–mobile convergence. The distinction is that most FMC architectures require a new dual-mode handset which works with existing unlicensed spectrum home/enterprise wireless access points, while a femtocell-based deployment will work with existing handsets but requires the installation of a new access point that uses licensed spectrum.

Many operators worldwide offer a femtocell service, mainly targeted at businesses but also offered to individual customers when they complain to the operator regarding a poor or non-existent signal at their location. Operators who have launched a femtocell service include SFR, AT&T, Sprint Nextel, Verizon, Zain, Mobile Tele Systems, T-Mobile US, Orange, Vodafone, EE, O2, Three, and others...

In 3GPP terminology, a Home NodeB is a 3G femtocell. A Home eNodeB is an LTE 4G femtocell. Typically the range of a standard base station may be up to 35 kilometers, a microcell is less than two kilometers wide, a picocell is 200 meters or less, and a femtocell is in the order of 10 meters, although AT&T calls its product, with a range of 12 m, a "microcell". AT&T uses "AT&T 3G Microcell" as a trade mark and not necessarily the "microcell" technology.

2.2 Operating mode

Femtocells are sold or loaned by a mobile network operator to its residential or enterprise customers. A femtocell is typically the size of a residential gateway or smaller, and connects to the user's broadband line. Integrated femtocells also exist. Once plugged in, the femtocell connects to the MNO's mobile network, and provides extra coverage. From a user's perspective, it is plug and play, there is no specific installation or technical knowledge required literally anyone can install a femtocell at home.

In most cases, the user must then declare which mobile phone numbers are allowed to connect to his femtocell, usually via a web interface provided by the MNO.This needs to be done only once. When these mobile phones arrive under coverage of the femtocell, they switch over from the microcell (outdoor) to the femtocell automatically. Most MNOs provide a way for the user to know this has happened, for example by having a different network name appear on the mobile phone. All communications will then automatically go through the femtocell. When the user leaves the femtocell coverage (whether in a call or not) area, his phone hands over seamlessly to the macro network. Femtocells require specific hardware, so existing WiFi or DSL routers cannot be upgraded to a femtocell.

Once installed in a specific location, most femtocells have protection mechanisms so that a location change will be reported to the MNO. Whether the MNO allows femtocells to operate in a different location depends on the MNO's policy. International location change of a femtocell is not permitted because the femtocell transmits licensed frequencies which belong to different network operators in different countries.

2.3 Benefits for users

Some of the main benefits for an end user are "5 bar" coverage when there is no existing signal or poor coverage. Also, higher mobile data capacity, which is important if the end-user makes use of mobile data on his or her mobile phone (may not be relevant to a large number of subscribers who instead use WiFi where femtocell is located). Depending on the pricing policy of the MNO, special tariffs at home can be applied for calls placed under femtocell coverage. For enterprise users, having femtos instead of DECT ("cordless" home) phones enables them to have a single phone, so a single contact list, etc. Improved battery life for mobile devices due to reduced transmitter–receiver distance. The battery draining issue of mobile operators can be eliminated by means of energy efficiency of the networks resulting in prolongation of the battery life of handsets.

2.4 Air interfaces

Although much of the commercial focus seems to have been on the Universal Mobile Telecommunications System, the concept is equally applicable to all air-interfaces. Indeed, the first commercial deployment was the cdma2000 Airave in 2007 by Sprint. Femtocells are also under development or commercially available for GSM, TD-SCDMA, WiMAX and LTE. The H(e)NB functionality and interfaces are basically the same as for regular High Speed Packet Access or LTE base stations except few additional functions. The differences are mostly to support differences in access control to support closed access for residential deployment or open access for enterprise deployment, as well as handover functionality for active subscribers and cell selection procedures for idle subscribers. For LTE additional functionality was added in 3GPP Release 9 which is summarized in.

As any technology femtocells have some issues. The main one is Interference.

2.5 Interference

The placement of a femtocell has a critical effect on the performance of the wider network, and this is the key issue to be addressed for successful deployment. Because femtocells can use the same frequency bands as the conventional cellular network, there has been the worry that rather than improving the situation they could potentially cause problems.

Femtocells incorporate interference mitigation techniques—detecting macrocells, adjusting power and scrambling codes accordingly. Ralph de la Vega, AT&T President, reported in June 2011 they recommended against using femtocells where signal strength was middle or strong because of interference problems they discovered after widescale deployment. This differs from previous opinions expressed by AT&T and others.

3 LTE-A NETWORKS

3.1 Overview

Long Term Evolution (LTE) describes the standardization work by the Third Generation Partnership Project (3GPP) to define a new high-speed radio access method for mobile communication systems. In order to successfully compete to other existing and future wireless, cellular and wire-line services, the network designers need to fully consider the technical constraints that influence the whole design process of this kind of networks. The number of combinations of network elements and parameters that can be configured (e.g. antenna tilt, azimuth, base station location, power) constitutes the solution space of the design process. The size of this space determines the degree of complexity of finding appropriate solutions. In Wireless Metropolitan Area Network (WMAN) scenarios like LTE, the number of options is high, so it is very unlikely that the optimal network configuration can be found using a manual method.

The main radio access design parameters of this new system include OFDM (Orthogonal Frequency Division Multiplexing) waveforms in order to avoid the intersymbol interference that typically limits the performance of high-speed systems, and MIMO (Multiple-Input Multiple-Output) techniques to boost the data rates. At the network layer, an all-IP flat architecture supporting QoS has been defined.

Before 3GPP started working in the real 4G wireless technology, minor changes were introduced in LTE through Release 9. In particular, femtocells and dual-layer beamforming, predecessors of future LTE-Advanced technologies, have been added to the standard. The formal definition of the fourth generation wireless, known as the International Mobile Telecommunications Advanced (IMT-Advanced) project, was finally published by ITU-R through a Circular Letter in July 2008 with a call for candidate radio interface technologies (RITs). In October 2009, LTE-Advanced was submitted seeking for approval as international 4G communications standard. LTE-Advanced LTE-A, the backward-compatible enhancement of LTE Release 8, will be fully specified in 3GPP Release 10. By backward compatibility, it is meant that

it should be possible to deploy LTE-Advanced in a spectrum already occupied by LTE with no impact on the existing LTE terminals. Rel-10 started early in 2010 and was functionally frozen in March 2011 after its approval by the ITU for having met the entire requirement for IMT-Advanced.

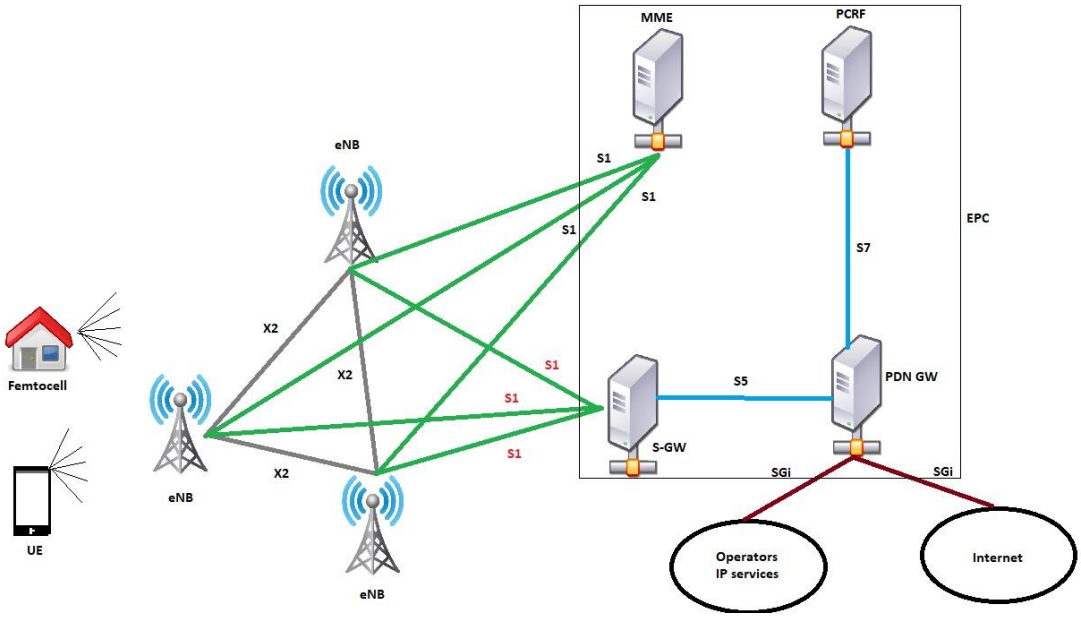
The set of IMT-Advanced high-level requirements established by the ITU-R in [1] is as follows:

- A high degree of commonality of functionality worldwidewhile retaining the flexibility to support a wide range ofservices and applications in a cost-efficient manner.
- Compatibility of services within IMT and with fixed networks.
- Compatibility of internetworking with other radio access systems.
- High-quality mobile devices.
- User equipment suitable for worldwide use.
- User-friendly applications, services, and equipment.
- Worldwide roaming capability.
- Enhanced peak rates to support advanced services and applications (100 Mbit/s for high mobility and 1 Gbit/s for low mobility were established as targets for research).

3.2 Network Architecture

The core network of the LTE-Advanced system is separated into many parts. Figure below shows how each component in the LTE-Advanced network is connected to one another. NodeB in 3G system was replaced by evolved NodeB (eNB), which is a combination of NodeB and radio network controller (RNC). The eNB communicates with User Equipments (UE's) and can serve one or several cells at one time. Home eNB (HeNB) is also considered to serve a femtocell that covers a small indoor area. The evolved packet core (EPC) comprises of the following four components. The serving gateway (SGW) is responsible for routing and forwarding packets between UE's and packet data network (**PDN**) and charging. In addition, it serves as a mobility anchor point handover. The mobility management entity (**MME**) manages UE access and

mobility, and establishes the bearer path for UE's. packet data network gateway (**PDNGW**) is a gateway to the PDN, and policy and charging rules function (**PCRF**) manages policy and charging rules.



Network architecture of LTE-Advanced

Mobile terminal location, can be outdoor or indoor. If the mobile terminal is located inside buildings the environment is called indoor, otherwise it is outdoor. Antenna location, it can be above or below the average rooftop level. In case, when base station antenna array is above average height of the buildings, the environment is considered to be macro-cellular and, in case, when base station antenna array is below average height of the buildings, the environment is considered to be microcellular. There is even smaller type of the cells than macro and micro cells, so called pico cells for which the antennas are located mainly in indoor environments if it located in shopping mall or enterprise. In Femto cells, the antennas are located mainly in indoor environments if it located in home.

Microcells provide big coverage and capacity in areas where there are high numbers of users, for Example, urban and suburban areas. Microcells cover around10% of the area of a Macrocell. The antennas for microcells are mounted at street level, are smaller than Macrocell

antennas and can often be disguised as building features so that they are less visually intrusive. Microcells have lower output powers than marocells, usually a few watts. Microcells are base stations with power between 1 to 5W, that use dedicated backhaul, are open to public access and range is about 500 m to 2 km.

Femtocell base stations allow mobile phone users to make calls inside their homes via their Internet broadband connection. Femtocells provide small area coverage solutions operating at low transmit powers. Femtocells are consumer deployable base stations that utilize consumer's broadband connection as backhaul, may have restricted association and power is less than 100mW.

3.3 MIMO Techniques

Multi-antenna or MIMO (Multiple Input, Multiple Output) technology is based on transmitting and receiving with multiple antennas and utilizing uncorrelated communication channels when radio signals propagate through the physical environment. If there is enough isolation between the communication channels, then multiple data transmissions can share the same frequency resources. If the multiple transmissions are for a single user, then the technology is called Single-User MIMO (SU-MIMO), for multiple users Multi-User MIMO (MUMIMO).

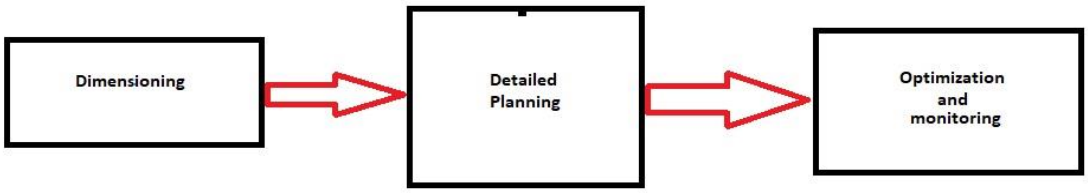
The better the system can utilize these communication channels for multiple transmissions, the higher is the capacity that the system can provide.

MIMO performance is subject to a large number of parameters: the number of transmitter and receiver antennas, reference signals and algorithms for channel estimation, feedback of channel estimation data from the receiver to the transmitter and spatial encoding methods. Consequently, a comprehensive design is crucial to provide optimum system performance.

3.4 LTE-A PLANNING

To be able to plan and implement a cost efficient high quality cellular mobile wireless network, very careful radio network planning procedure must be done. Thus, the planning process carried out in phases and each phase is well documented. The radio network planning procedure requires good knowledge about the coverage area, propagation environment, traffic load and required services to be able to analyses the network and to decide the optimal radio network planning strategy. The fact, that all the above-mentioned aspects are not constant and vary in time, makes the radio network planning a nonstop process, which requires continuous monitroring and optimization.

The radio network planning is a process, which defines different steps, like measurements, planning, documentation, etc. that should be done in different phases to manage connections between coverage, capacity and interference. The coverage or capacity or QoS is not possible to maximize simultaneously, but all of them need to be optimized in order to implement a cost-efficient high-quality radio network. To provide necessary coverage and, at the same time, optimize capacity and quality, the radio network planning can be divided into three main phases, illustrated in Figure 4. These phases can be used from initial deployment of the radio networks to their evolution and further development.



Planning Phases

During the first phase, dimensioning, the planned network configuration is analyzed and an appropriate radio network deployment strategy is defined. In second phase, detailed planning, the detailed design and actual implementation of the radio network is done. First step in detailed planning is the configuration planning, which need to be done prior to coverage and capacity planning to be able to analyses all available coverage and capacity related software and hardware features. The base station site configuration, which is different for different environments, need to be done based on both coverage and capacity requirements. Coverage specific requirements define coverage related base station elements and capacity requirements define capacity related base station elements. And finally, power budget can be calculated based on optimized base station parameters. Eventually, the configuration planning will provide total base station site configuration for different places and environments.

The configuration planning is followed by coverage planning, the aim of which is to minimize the number of base station sites by utilizing output information of the dimensioning and configuration planning. An important role in configuration planning plays surveying which helps to find out potential propagation problems and suggest base station sites locations. After that, some measurements can be done to tune propagation models for the particular areas. The tuned propagation models will give the final locations for base stations, by taking as input base station configuration parameters as well as some information about environment. The final coverage prediction and base station locations are usually defined by the use of advance planning software.

The next step is capacity planning which should be started as soon as the base station sides are selected. The capacity planning is done by the use of planning-tools, as the resource allocation mechanisms are already defined in dimensioning phase. The initial step is to define planning thresholds, after that, the main job will be done by planning-tools. The last step in the detailed planning is parameter planning, which is done immediately before the launch of the network.

The last step in the detailed planning is parameter planning, which is done immediately before the launch of the network.

The last step in the detailed planning is parameter planning, which is done immediately before the lunch of the network. Radio performance has a direct impact on the cost of deploying the network in terms of the required number of base station sites and in terms of the transceivers required. The operator is interested in the network efficiency. He must ask himself: how many

customers can be served how much data can be provided and how many base station sites are required. The efficiency is considered in the link budget calculations and in the capacity simulations. The end user application performance depends on the available bit rate, latency and seamless mobility. The radio performance defines what applications can be used and how these applications perform. Recent works in LTE and LTE-A network planning are divided into two directions. The first direction is solving Capacity and Coverage optimization by Self-Organizing LTE network. In[2] a novel hybrid two-layer optimization framework is proposed to enhance the network capacity and coverage, where on the top layer a network entity of eCoordinator is implemented to ensure overall network coverage by optimizing the antenna tilt and capacity-coverage weight of each cell in a centralized manner, and on the bottom layer individual eNB optimizes cell-specific capacity and coverage by tuning its pilot power in a distributed manner. A heuristic algorithm is developed for the eCoordinator operation at large time granularity and the Genetic Programming (GP) approach is exploited for the eNB operation at small time granularity, for the purpose of tracking overall network performance as well as adapting to network dynamics. Results have demonstrated the usefulness of the proposed algorithms by enhancing network capacity and coverage performance under various system requirements. Present reinforcement learning strategies for selforganized coverage and capacity optimization through antenna down tilt adaptation. This work analyzes different learning strategies for a Fuzzy Q-Learning based solution in order to have a fully autonomous optimization process. The learning behavior of these strategies is presented in terms of their learning speed and convergence to the optimal settings. Simultaneous actions by different cells of the network have a great impact on this learning behavior. Therefore, a study for stable strategy where only one cell can take an action per network snapshot as well as a more dynamic strategy where all the cells take simultaneous actions in every snapshot, also propose a cluster based strategy that tries to combine the benefits of both. The performance is evaluated in all three different network states, i.e. deployment, normal operation and cell outage. The simulation results show that the proposed cluster based strategy is much faster to learn the optimal configuration than one-cell-per-snapshot and can also perform better than the all-cells-per-snapshot strategy due to better convergence capabilities.

3.5 Indoor network planning

Small cells offer mobile service providers (MSPs) a cost-effective alternative to macro-only deployments for meeting growing coverage and capacity demands. That's because as small, low-cost access points, they are selfinstalled (home and enterprise cells) or easily installed by a single person (metro cells). Plus, as small cells are added, they offload traffic from the macro network. This increases available network capacity without the deployment of new macro sites. Owned and managed by the MSP —metro cells, small cells — are most cost effective in areas where new macro sites are required. The larger the number of macro sites, the greater the economic benefits. Metro cells cost much less than macro radio equipment and they do not require civil works that contribute heavily to macro site deployment costs. There are several factors behind the trend to smaller cells, including the perceived risks to health and visual appearance. Larger cells that transmit more radio waves sometimes spark concerns about radiation, while at the same time are held to be less aesthetically pleasing, especially in dense locations. Smaller cells also consume less power, reducing energy demands and offering potential environmental benefits. As the number of cells rises along with the demand for anywhere, anytime access, mobile service providers face a major challenge: How todefine and deliver high-quality services cost-efficiently, and how to address the corresponding infrastructure and management challenges. Meeting this challenge means looking at the full set of requirements from a solutionslifecycle perspective, beginning with architecture and finishing with deployment. Designing for small-cell environments near and in-building can be a daunting task. There is a host of legal, logistical, technological, and other issues to consider from the outset. Nonetheless, quality of design is key to creating a sustainable In-Building solution spanning time, location and mobile generations. In terms of architecture, LTE introduces new concerns and is more complex than 2G or 3G. Capacity requirements must be carefully considered, along with the impact of the macro network. Moreover, new antenna features such as MIMO and Beam Forming have to be taken into account, as well as end-to-end planning, integration and validation of IP networking and applications. Given the range and complexity of these issues, solution architects need to create an end-to-end reference architecture document detailing the necessary products and the interconnectivities among different elements and subsystems of the LTE network. The Solution Architect must also deliver a highlevel

design and well-documented technical interfaces. Technical deliverables must be reviewed to assure consistency with solution architecture, customer requirements, and quality goals. All of this is undertaken in keeping with the mission of the Solution Architect to mitigate delivery risk through careful scrutiny of the scope of work and clear communications.

Low-power base stations such as femtocells are one of the candidates for high-data-rate provisioning in local areas, such as residences, apartment complexes and business offices.

Due to the expected large number of user-deployed cells, centralized network planning becomes impractical, and new scalable alternatives must be sought.

In [3] novel solution is introduced and exploited. It relies on a suite of simulation tools including generation of random 3D femto-cell deployments in real environments, realistic path-loss predictions using a raybased model and a 3D downlink performance analysis (i.e. considering all floors) of heterogeneous LTE networks in terms of coverage, macro offload and throughput. A first study demonstrates a significant macro offload and power consumption reduction in a realistic dense corporate FAP deployment. Then, a second study shows the large growth of indoor capacity enabled by dense FAP deployments but also the coverage degradation for non-subscribers when closed-access mode is used.

In [4] proposes and analyzes a new method for dynamically adjusting LTE femtocell power levels to mitigate interference to meet user selectable network performance goals. This paper proves that the proposed method converges to feasible solutions. The proposed algorithm is suitable for both distributed femtocell control and centralized policy enforcement. Paper [5] introduce a deterministic approach for the simulation and performance evaluation of LTE networks in urban and indoor scenarios. Besides signal levels the expected MIMO capacity is evaluated. Comparisons with two measurement campaigns verify the high accuracy of the presented prediction model.

3.6 Outdoor Planning

The second direction is the study of Energy and cost impacts of relay and femtocells deployments in long-term evolution advanced [6] where presents a methodology for estimating the total energy consumption, taking into account the total operational power and embodied energy, and TCO of wireless cellular networks, and in particular provides a means to compare homogeneous and heterogeneous network (HetNets) deployments. The realistic energy models and energy metrics based on information available from mobile-network operators (MNOs) and base stations manufacturers must taking into consideration. Additionally, up-to-date operational and capital expenditure (OPEX and CAPEX) models are used to calculate TCO of candidate networks. There are two scenarios for HetNets, namely a joint macro-relay network and a joint macro–femtocell network, with different relay and femtocell deployments densities. The results obtained show that compared to macro-centric networks, joint macro-relay networks are both energy and cost efficient, whereas joint macro–femtocell networks reduce the networks TCO at the expense of increased energy consumption. Finally, it is observed that energy and cost gains are highly sensitive to the OPEX model adopted Paper [7] study the Impact of base station antenna eNB configurations on dual-stream Multiple-Input Multiple-Output (MIMO) performance is demonstrated by means of a real-world measurement example.

4 SECURITY

I definitely left security for last by no mistake. I truly believe that in our highly technological era we usually bypass the biggest weak-point in our systems and that is nothing else but security. For example, the security protocol used to protect the vast majority of Wi-Fi connections has been broken, potentially exposing wireless internet traffic to malicious eavesdroppers and attacks, according to the researcher who discovered the weakness. So, lets analyze a few things about LTE security.

4.1 LTE SECURITY ARCHITECTURE

LTE introduced a new set of cryptographic algorithms and a significantly different key structure than that of GSM and UMTS. There are 3 sets of cryptographic algorithms for both confidentiality and integrity termed EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA). EEA1 and EIA1 are based on SNOW 3G, very similar to algorithms used in UMTS. EEA2 and EIA2 are based on the Advanced Encryption Standard (AES) with EEA2 defined by AES in CTR mode (e.g., stream cipher) and EIA2 defined by AES-CMAC (Cipherbased MAC). EEA3 and EIA3 are both based on a Chinese cipher ZUC. While these new algorithms have been introduced in LTE, network implementations commonly include older algorithms for backward compatibility for legacy devices and cellular deployments.

From a security perspective, one of the most important functions of the UICC is cryptographic key and credential storage. In LTE, UICCs are provisioned with a long-term, pre-shared cryptographic key referred to as K. This key is stored within the tamper resistant UICC and also within the core network (in the HSS) and is never to leave either of those locations. All other keys in LTE's cryptographic structure are derived from K, with the session master key referred to as KASME. Security functions such as cryptographic operations and subscriber authentication are

performed by the UICC in conjunction with the HSS and MME. The UICC also plays a role in storing LTE security contexts. Security contexts contain cryptographic keys, UE security capabilities, and other security parameters generated during an attach that can be reused during future system accesses. The UICC also stores the IMSI and IMEI, which are both used to support the use of identities. Some modern mobile equipment operating systems implement the USIM PIN specified by 3GPP TS 121.111. This allows a PIN to be configured on a UICC. Since UICCs can be removed from one mobile device and inserted into another to provide service, the UICC PIN can prevent someone from stealing another user's UICC and obtaining unauthorized network access.

4.2 E-UTRAN SECURITY

The radio access network and associated interfaces make up the E-UTRAN portion of the LTE network, and which is the midway between a handset and an MNO's core network. Handover is one of the most important functions of a cellular network. This allows the user the ability to be moving, such as traveling on a highway, and maintain call connection. Base stations will often need to communicate between themselves to enable this "mobility," and they do so via the X2 interface. 3GPP specifies multiple security mechanisms to ensure a secure handoff of call related information. Two types of handovers exist: X2 handover and S1 handover. During an S1 handover the MME is aware that a handover is going to occur before it happens. Within an X2 handover, the MME is unaware and the transition occurs purely between eNodeBs via the X2 interface. There are unique security considerations for both methods of handover. With an S1 handover, the MME can refresh the cryptographic parameters used to protect the air interface before the connection is severed. With an X2 handover, fresh keying material can only be provided after the handover for use in the next handover. When handover occurs, new keys are generated, partly separating the new session from the previous one, although a new master session key (i.e., KASME) is not generated. The KeNB is used, alongside other cryptographic parameters and the cell ID of the new eNodeB, to generate KeNB*, which is used to protect the new session after handover occurs. It is of note that the source base station and MME control key derivation and the new eNodeB is not meant have knowledge of the keys used in the original eNodeB session

4.3 THREATS

LTE infrastructure components (e.g., eNodeB, MME, S-GW) may run atop of commodity hardware, firmware, and software, making it susceptible to publicly known software flaws pervasive in general purpose operating systems (e.g., FreeBSD and other *nix variants) or other software applications. Although heavy customization of systems may occur, commodity hardware and well-known operating systems that are utilized should be identified and understood. This implies that these systems need to be properly configured and regularly patched to remediate known vulnerabilities, such as those listed in the National Vulnerability Database. The following subsections will address malware threats to specific network components and the management of an LTE network.

Malicious code infecting a mobile device's operating system, other firmware, and installed applications could prevent a UE from accessing a cellular network. Malware could directly attack the baseband OS and its associated firmware. Attacking the baseband OS could change important configuration files for accessing the network or prevent important routines from running, such as those interpreting the signaling from a base station. Either of these would cause a denial of service.

Malware installed on a mobile device, or infecting a mobile device's operating system and other firmware, could be part of a botnet launching an attack against a carrier's radio network infrastructure. A Distributed Denial of Service (DDoS) attack could be launched via a continuous stream of attach requests, or requests for high bandwidth information and services. An unintentional DDoS attack on a carrier's radio infrastructure has been seen to occur via a mobile application making a large number of update requests. Malware can also compromise base station operating systems causing unexpected and undesirable equipment behavior.

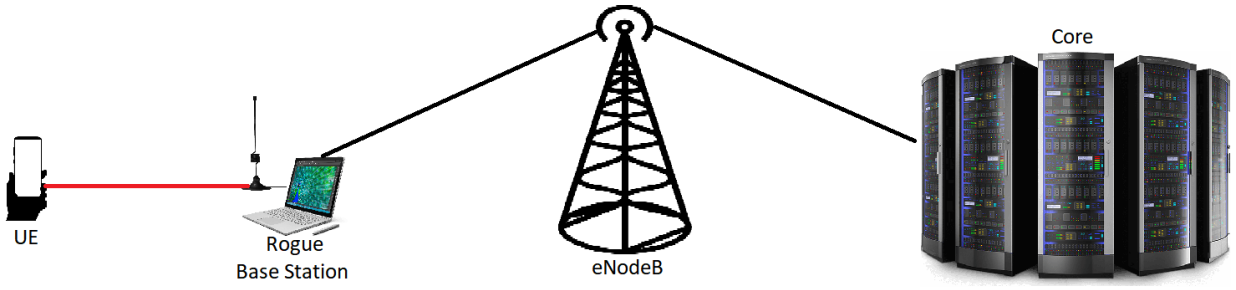
Malware infecting components a carrier's core network infrastructure would have the potential to log network activity, modify the configuration of critical communications gateways, and sniff user traffic (e.g., call traffic, SMS/MMS) depending on which components are infected. These types of attacks have been previously observed in GSM networks, but as of this time there is no known example of this attack within backend LTE infrastructure. A Distributed Denial of

Service (DDoS) attack against an MME could be launched via a continuous stream of attach requests.

Operational and Access Management (OAM) networks are a vital part of an operational cellular network, providing remote access into geographically dispersed components of the network. These OAM network interfaces provide quick access to network components, allowing MNOs to manage and tune networks from one central location. Poor design, lax configuration management, and lack of hardening of these management networks and interfaces create a serious security risk to the network's operational stability. Unauthorized access to management interfaces can potentially allow malicious and unintentional misconfigurations of critical network systems.

4.4 ROGUE BASE STATIONS

Rogue base stations are unlicensed base stations that are not owned and operated by an authentic MNO. They broadcast a cellular network masquerading as a legitimate carrier network. The necessary hardware to construct these devices can be inexpensively obtained using commercial off-the-shelf (COTS) hardware. The software required to operate a 2G (GSM) base station is open source and freely available, and can be configured to operate as a rogue base station.



Rogue base stations exploit the fact that mobile handsets will attach to whichever base station is broadcasting as its preferred carrier network and is transmitting at the highest power level. Therefore, when a rogue base station is physically proximate to a mobile handset while transmitting at very high-power levels, the handset may attempt to connect to the malicious network. Mobile handsets are engineered to be backwards compatible with older cellular systems providing a consistent user experience during mobility. Rogue base stations take advantage of this backward compatibility and exploit weaknesses in these older cellular systems. At the time of this writing, a majority of rogue base stations broadcast a 2G GSM cellular network. The security protections offered by GSM lack mutual authentication between the handset and cellular network, and strong cryptographic algorithms with keys of sufficient length. Additionally, there is no requirement mandating that the 2G GSM air interface is encrypted.

Attackers using a rogue base station could prevent mobile devices physically close to the rogue base station from accessing emergency services. This occurs when the rogue station fails to forward user traffic onward to the MNO. If this attack occurs during an emergency, it could prevent victims from receiving assistance from public safety services and first responders. This attack may be detectable, since the UE believes it has cellular service but is unable to make calls or send/receive data. This attack takes advantage of another vector that comes into play while making emergency phone calls when the preferred network is not available. When making an emergency phone call the UE might attach and attempt to send the call through a rogue base station, even if the base station is not masquerading as a legitimate network. There is a risk that the rogue base station will not forward the emergency call appropriately.

4.5 CONCLUTIONS

When compared to previous cellular networks, the security capabilities provided by LTE are markedly more robust. The additions of mutual authentication between the cellular network and the UE, alongside the use of publicly reviewed cryptographic algorithms with sufficiently large key sizes are positive steps forward in improving the security of cellular networks. The enhanced key separation introduced into the LTE cryptographic key hierarchy and the mandatory integrity protection also help to raise the bar.

Yet LTE systems are rarely deployed in a standalone fashion - they coexist with previous cellular infrastructure already in place. Older cellular systems continue to be utilized throughout many different industries today, satisfying a variety of use cases. With this in mind, it's easy to see why LTE networks are often deployed in tandem with GSM and UMTS networks. This multigenerational deployment of cellular networks may lead to an overall decrease in cellular security. A primary example of this is the requirement for the baseband firmware to remain backward compatible, supporting legacy security configurations.

The interconnection of these technologies introduces additional complexity into an already complicated system that is distributed over an immense geographic area, that is continental in scale. Cellular networks traditionally use separate networks to communicate call signaling information. Specifically, the SS7 network has been in use for decades and has its own unique set of security challenges that is separate from the cellular network technology. An LTE-specific version of Diameter was specified by 3GPP to, in part, resolve the challenges associated with the use of SS7, although it is not widely deployed. The Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 10 issued a report on SS7 security issues, but more work is needed before these threats are fully resolved. It's important for MNOs and all interested parties to perform their own security analysis of this technology in order to understand how to appropriately mitigate the risks introduced by these signaling technologies. This security analysis should include how any partnering MNO also mitigates these risks in their own network, since a weakness in one MNO's network adversely affects the security of those its connected to.

LTE's sole use of IP technology is a major differentiator from previous cellular networks. LTE does not use circuit switching, instead opting to move to a purely packet switched system. IP is a commoditized technology that is already understood by Information Technology practitioners, which presents both challenges and opportunities. Attackers may be able to leverage existing tools for exploiting IP-based networks to attack the LTE core and other associated cellular infrastructure within an MNO's network. Conversely, this may allow already existing IP-based defensive technology to be immediately applied to LTE networks. Hopefully, the application of these technologies will offer novel ways to increase system security.

The following list highlights areas of the LTE security architecture that either lack the appropriate controls or have unaddressed threats:

• **Default Confidentiality Protection for User Traffic**: The LTE standards do not provide confidentiality protection for user traffic as the default system configuration. Enabling user traffic encryption by default, except for certain scenarios such as emergency calls, would provide out of the box security to end users.

• **Prohibiting user traffic integrity**: Although the LTE standards require integrity protection for critical signaling traffic, integrity protection for user traffic is explicitly prohibited, as stated in section 3.4.

• **Lack of protection against jamming attacks**: This is an active area of research, and mitigations have been proposed, although it is unclear if these mitigations have been appropriately vetted and considered for inclusion into the LTE standard.

• **OAM Networks**: Vulnerabilities potentially exist on the OAM network depending on how it is architected and managed.

5 CONCLUSIONS

In this paper we outlined the mechanisms which EPS provides user equipment with IP connectivity to the packet data network. Also, we talked about Femtocells, Pico cell provide a one-box solution: a small, low-cost, low power unit that can be self- installed to provide mobile 4G coverage to the home. Femtocells or Pico cells are not simple standalone devices. They must be integrated into the mobile operator's network to enable seamless service and to ensure optimal performance across both femtocell and macrocell networks. It is also expected that the use of femtocells, small cell, Pico cell, self-organizing networks, and energy management systems will drive the evolution of current and future mobile wireless networks. In the future the efforts must be focused on improving the support of heterogeneous networks, as well as device and machine-type communications.

6 REFERENCES

[1] ITU-R, Requirements related to technical performance for IMTAdvanced radio interface(s), Report M.2134, 2008.

[2] Jietao Zhang, Chunhua Sun, Youwen Yi, and Hongcheng Zhuang, "A Hybrid Framework for Capacity and Coverage Optimization in Self-Organizing LTE Networks", 2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications: Mobile and Wireless Networks.

[3] Letourneux, F.; Corre, Y.; Suteau, E.; Lostanlen, Y., "3D Performance analysis of a heterogeneous LTE network with indoor small-cells in a real urban environment," Communications (ICC), 2013 IEEE International Conference on, vol., no., pp.5209,5213, 9-13 June 2013 doi: 10.1109/ICC.2013.6655412

[4] C. Khirallah, J.S. Thompson, H. Rashvand, " Energy and cost impacts of relay and femtocells deployments in long-termevolution advanced" , IET Communications 2011, Vol. 5, Iss. 18, pp. 2617–2628 2617, doi: 10.1049/iet-com.2011.0111

[5] Oliver Stäbler, Reiner Hoppe, GerdWölfle, Thomas Hager, Timm Herrmann," Consideration of MIMO in the Planning of LTENetworks in Urban and Indoor Scenarios".

[6] C. Khirallah, J.S. Thompson, H. Rashvand, " Energy and cost impacts of relay and femtocells deployments in long-termevolution advanced" , IET Communications 2011, Vol. 5, Iss. 18, pp. 2617–2628 2617, doi: 10.1049/iet-com.2011.0111

[7] J. Salo, M. Nur-Alam, K. Chang "Practical Introduction to LTE Radio Planning", Multimode System Selection (MMSS)- Basic Provisioning.

BOOKS:

[8] [Stallings] Data and Computer Communications

[9] Computer Networks [Tanenbaum,Wetherall]

[10] Computer Networks and Internets [Comer]

[11] Networking Foundations [Ciccarelli,Faulkner]