UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMMUNICATION ENGINEERING

Kabinad Teshager

STRATEGIC USE OF WI-FI IN MOBILE BROADBAND NETWORKS

Master´s thesis for the degree of Master of Science in Technology submitted for inspection in Vaasa, 21st of May, 2011.

Supervisor	Prof. (Tech) Mohammed Elmusrati
Instructor	M.Sc .(Tech) Reino Virrankoski
	Johan Kaustinen (Anvia Oyj)

ACKNOWLEDGMENTS

First, I would like to thank my supervisor professor Mohammed Elmusrati for his support, sharing his expertise, and fruitful discussions. I would also like to thank my instructors Johan Kaustine and Reino Virrankoski. You have all inspired me and made the work progress well.

My research has been funded by Anvia Oyj . I really enjoyed the experience of working in a cooperative and friendly environment at Anvia Oyj. I have received enormous experience by interacting and collaborating with Johan Kaustinen, Reino Lahdemaki and Esa Honkonen. Thank you all.

Finally I would like to express my special thanks and gratitude to my dearest parents, Teshager and Etagegnehu, and all my friends for their sincere supplication, feelings and love throughout the whole master study and the work with this thesis.

Vaasa, May 10th 2011

Kabinad Teshager

TABLE OF CONTENTS

LIST OF ABBREVATIONS

3GPP	Third Generation Partenership project
AAA	Authentication, Authorizations and Accounting
ANDSF	Access Network Discovery and Selection Function
AKA	Authentication and Key Agreement
AP	Access Point
AuC	Authentication Center
CapEx	Capital Expenditure
CTO	Chief Technical Officer
CS	Circuit Switch
CP	Captive Portal
CG	Charging Gateway
CoA	Care of Address
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EAPoW	EAP over Wireless
EDCA	Enhanced Distributed Channel Access
EIR	Equipment Identification Register
FA	Foreign Agent
EPS	Evolved Packet Core
GGSN	Gateway GPRS Support Node
GW	Gateway

GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GTP	GPRS tunneling protocol
HA	Home Agent
HLR	Home Location Register
HTTP	Hyper Text Transfer Protocol
HNB GW	Home NodeB Gateway (HNB GW)
HMS	Home NodeB Management System (HMS)
HSPA	High-Speed Packet Access
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
IAPP	Inter-Access Point Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
I-WLAN	Interworking WLAN
MMS	Multimedia Messaging Service
MA	Mobility Agent
MIP	Mobile IP
MAC	Media Access Control
MSC	Mobile Switching Center
OCS	Online Charging System
OpEx	Operational Expenditure
PS	Packet Switch
PCRF	Policy and Charging Rules Function
PDG	Packet Data Gateway
PDN	Packet Data Network
PLMN	Public Land Mobile Network
PWLAN	Public Wireless Local Area Network

QoS	Quality of Service
QoE	Quality of Experience
RADIUS	Remote Authentication Dial-In User Service
RNC	Radio Network Controller
SIP	Session Initiation Protocol
SS7	Signaling System 7
SSG	Service Selective Gateway
SSIDs	Service Set IDentifier
SIM	Subscriber Identity Module
SGSN	Service GPRS Support Node
TCO	Total Cost of Ownership
TOS	Type of service
UE	User Equipment
UMA	Unlicensed Mobile Access
UMTS	Universal Mobile Telecommunications System
UICC	Universal Integrated Circuit Card
VLR	Visitor Location Register
VoIP	Voice over Internet Protocol
VoD	Voice on Demand
WARG	WLAN Access Router Gateway
Wi-Fi	Wireless network using IEEE 802.11 standard
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless local Area Network (WLAN)
WISP	Wireless Internet Service Provider
WISPr	Wireless Roaming Intermediary eXchange
WPA2	Wi-Fi Protected Access Version 2

TABLE OF FIGURES

UNIVERSITY OF VAASA		
Faculty of technology		
Author:	Kabinad Teshager Tesfaye	
Topic of the Thesis :	Strategic Use of Wi-Fi In Mobile Broadband Network	
Supervisor :	Prof. Mohammed Elmusrati	
Instructor :	Johan Kaustine Reino virrankoski	
Degree :	Master of Science in Technology	
Department :	Department of computer science	
Degree Programme :	Degree Program in Telecommunication Engineering	
Major of Subject:	Telecommunication Engineering	
Year of Entering the University:	2009	
Year of Completing the Thesis:	2011	**Pages: 83**

ABSTRACT

Mobile networks are facing the growing flood of Internet data. The main reasons for this are the increasing use of smartphones, the availability of flat-rate voice and data bundles, and higher demand for entertainment services like YouTube, Apple's iTunes and service such video streaming from Television Networks. This increase in data traffic is forecast to accelerate. For mobile network operators this means not only massive business opportunity but also huge challenges how to cope with this phenomenal growth. In this paper we are giving some insight to trend of mobile data growth and impact on operator's market.

It seems obvious that traditional cellular networks, even with next generation upgrades, are not able to handle all this traffic and provide required level of new mobile capacity. Operators are now studying various possibilities to encounter the challenge. Obviously solution will be a set of different actions. However, one of those required actions seems to be to offload the data from cellular networks to some other wireless networks. The most promising candidate is Wi-Fi as it has established strong market position and increasing number of devices support both mobile and Wi-Fi connections. By selectively offloading traffic from mobile to Wi-Fi networks, faster data connections and better end user quality of experience are achieved. Moreover, when offloading portion of traffic from mobile to Wi-Fi networks via freed cellular network resources ensuring that mobile network capacity is preserved for high priority.

This thesis work outlines the needs of the mobile community in how it would like to utilize Wi-Fi offload to help promote and develop the usefulness and availability of its services. This paper gives an overview of the current Wi-Fi world, then provides an outline of the necessary standards and requirements in Wi-Fi offload system. Finally, we propose and discuss some architecture capable to provide interworking between Wi-Fi and 3G networks which feature the highest market interest. These architectures can enable 3G subscribers to benefit from high throughput IP connectivity in strategic locations and also to maintain service consistency across WLAN and mobile network.

KEYWORDS: WLAN ,3G , mobile data offloading, 3G/WLAN interworking

1. INTRODUCTION

1.1 Motivation

Mobile networks are facing the growing flood of Internet data. In 2007 monthly traffic in mobile networks was 15000 TB of data. According to prediction by Cisco monthly traffic in mobile networks will exceed 3,6 Million TB already in 2014. 40 X traffic growth in four year is exceeding the capacity of foreseeable cellular networks. This means mobile network operators need solutions that help them reduce network congestion while also helping them reduce costs and preserve customers.

Half of smartphones and over 90% of 3G enabled laptops and notebook PCs are already Wi-Fi enabled. Hundreds of millions ubiquitous Wi-Fi access points provide large enough complementary capacity space for mobile networks.

The motive of this thesis is to study this spectacular growth of the mobile data and discuss about how the Wi-Fi technology can help the operator to turn this overwhelming growth to be an opportunity instead of a threat.

1.1 Scope of the Research

This thesis examines the mobile internet growth, trend and impacts on operator service. Also, the paper addresses the design principles, features, and architecture methods of implementation of Wi-Fi mobile data offloading. This will be done with a certain level of abstraction. Hardware design and experiments are not within the scope of this thesis. However, some basic principles are provided as an abstraction for real practical implementations.Wlan-3G interworking architecture for mobile offloading is proposed and discussed.

1.4 Research question

In this paper we will focus our analysis and discussion on the following research questions:

- How will total data traffic over the cellular network grow over the next five years? What are the possible impacts?
- What strategies have operators evolved to deal with network congestion?
- What are the technical considerations to deploy Wi-Fi mobile data offloading?
- How much Wi-Fi can deliver in complementing cellular network?
- What are challenges in using Wi-Fi mobile offloading?
- what is the current status of Wi-Fi offloading?

In terms of results, the outcomes are:

- WLAN-3g interworking Framework for wifi mobile data offloading.
- WLAN architecture for mobile data offloading.

1.5 Thesis Structure

The subsequent work is organized into the following chapters:

Chapter 2

Provides background and a literature review of those radio access technologies used in this thesis, namely UMTS and WLAN. Additionally, discusses about their network elements and architecture arrangements.

Chapter 3

Examines the market trends with respect to data consumption, present insight to mobile internet grows and impact on the service provider market .Finally discusses the key elements and the driving forces of Wi-Fi offloading.

Chapter 4

Discusses mobile data offloading strategies and provides Wi-Fi use cases. Also discuss operators’ point of view towards Wi-Fi data offloading.

Chapter 5

Presents guidelines and technical considerations to be considered in implementing a practical Wi-Fi mobile data offloading system.

Chapter 6

Proposes and discuses WLAN cellular interworking frame work.

Chapter 7

Offers the conclusions of this thesis investigation and propose areas of future work.

2 BACKGROUND

Wireless communication is today an important utility used by people and businesses all over the world. This Chapter provides a background of those radio access technologies used in this thesis, namely UMTS, WLAN.

2.1 Universal Mobile Telecommunications System

Universal Mobile Telecommunications System (UMTS) is a third generation (3G) mobile communication system, currently representing a large customer base mostly in Asia and Europe. It is designed to deliver graphics, pictures, video communications, and other multimedia information, in addition to voice and data, to mobile wireless subscribers. The spectrum for UMTS lies between 1900 MHz to 2025 MHz and 2110 MHz to 2200 MHz. The air interface used in UMTS is Wideband Code Division Multiple Access (WCDMA).

2.1.1 Network architecture

The UMTS 3G network architecture consists of three domains: The User Equipment (UE) domain, the UMTS Terrestrial Radio Access Network (UTRAN) domain, and the Core Network (CN) domain. A typical UMTS 3G network is shown in Figure 1.The three domains are further described in the following sections.

User Equipment(UE)

The UE domain includes a variety of equipment types with different levels of functionality such as cellular phones, smartphones, tablets PDAs, laptops. These equipment types are usually referred to as user equipment.

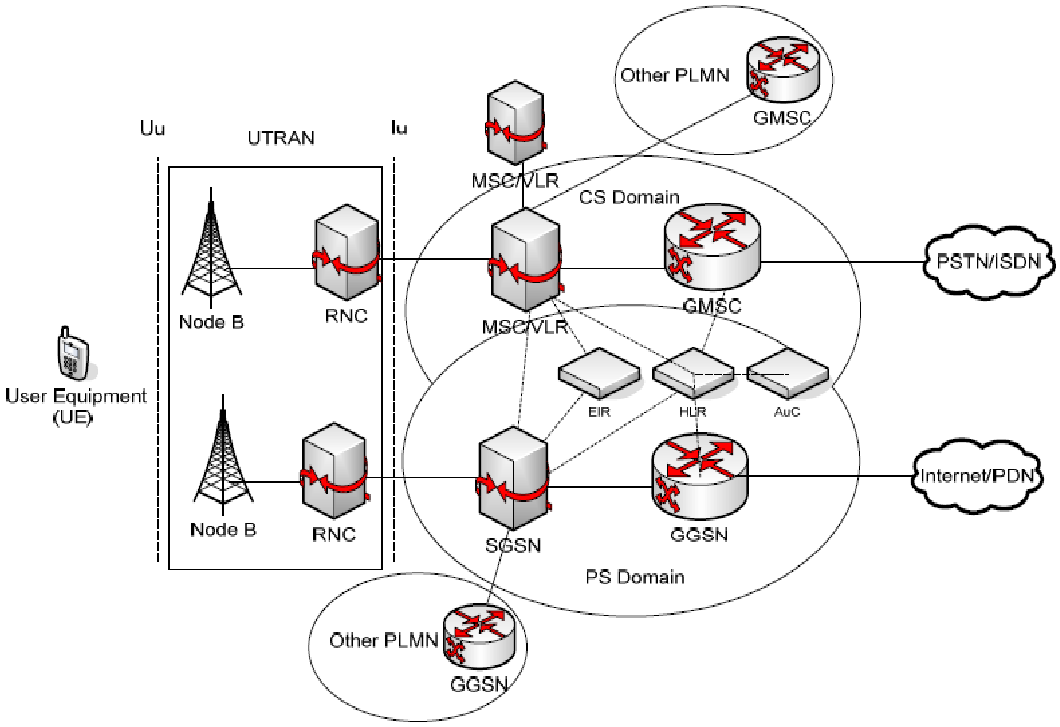


Figure 1. UMTS architecture (Chowdhury, 2010)

The UE domain consists of two parts:

- The *UMTS Subscriber Identity Module* (USIM)

  The USIM is a smartcard that contains user-specific information and the authentication keys that authenticates a user's access to a network.
- The *Mobile Equipment* (ME).

  The ME is a radio terminal used for radio communication with the UTRAN domain over the Uu radio interface.

UMTS Terrestrial Radio Access Network (UTRAN)

UTRAN is responsible for the radio resource management. This includes the responsibility for power control, support for the different handover types and also controlling and managing handovers. UTRAN consists of:

- *Node B*

  The Node B converts the signals of the radio interface into a data stream and forwards it to the RNC. In the opposite direction, it prepares incoming data from the RNC for transport over the radio interface.
- *Radio Network Controller* (RNC).

  The RNC is the central node in the UTRAN that controls one or more NodeBs and is also responsible for the management of all the radio resources in the UTRAN.

Core Network (CD)

The CN domain is responsible for routhing and switching calls and data connections between the UTRAN domain and external circuit and packet switched networks. It is divided into a *Circuit Switched network* (CS-domain) and *Packet Switched network* (PS-domain). The CS-domain contains the following parts:

- *Mobile Switching Center (MSC):*

  The MSC is a switching node that routes data of CS-services within and out of the own network via the Gateway Mobile Switching Center (GMSC). The MSC part is responsible for all signaling required for setting up, terminating, and maintaining connections, and mobile radio functions such as call rerouting, as well as the allocation/deallocation of radio channels.

- *Gateway Mobile Switching Center (GMSC):*

  The GMSC is connected to the MSC and interconnects the own UMTS network to other CS-switched networks like Public Telephone Switched Network (PTSN) or Integrated Services Digital Network (ISDN) .

- *Visitor Location Register (VLR):*

  The VLR saves temporarily security, authentication and identification data of all participants that are currently managed by the MSC. It is used to manage users that are roaming in the area of the associated MSC.

- *Transponder Rate Adapter Unit (TRAU):*
  The TRAU is a gateway between the RNC and the MSC that is responsible for the conversion of the format (Adaptive Multi Rate (AMR) to Pulse Code Modulation 30 (PCM30) and vice versa) of speech data. This is necessary because UTRAN and CN use different formats.

The PS-domain consists of the following parts:

- *Serving GPRS Support Node (SGSN):*
  The SGSN in the PS-domain is similar to the MSC in the CS domain. It routes data of PS services in the own UMTS networks and outside via the Gateway GPRS Support Node (GGSN). It also manages many RNCs that are connected via the Iu-PS interface and is connected to databases like the Home Location Register. The SGSN also is responsible for authentication and mobility management.
- *Gateway GPRS Support Node (GGSN):*
  The GGSN is very similar to the GMSC in the CS-domain. It interconnects the UMTS network with other PS networks like the Internet or X.25 networks and is connected to the SGSN.

There are also some elements that are used by both domains. One important component of them is the following:

- *Home Location Register (HLR)/Authentication Center* (AuC):
  The HLR/AuC is a database that saves data of subscribers that rarely change like security and encryption information, phone number, service entitlement etc.

2.2 Wireless local Area Network

A Wireless local Area Network (WLAN) is a type of local area network that uses electromagnetic waves to send and receive information between mobile host and wired backbone network. The IEEE 802.11 group of standards specifies the technologies for

WLANs. WLAN uses unlicensed spectrum at the 2.4 and 5 GHz band. In public locations known as hotspots, enterprises and homes, WLAN supports seamless connectivity, flexibility, mobility, reliability and high speed access to the internet while maintaining an optimal tradeoff between range and data rates.

Wi-Fi, which stands for Wireless Fidelity, is a trademark name to brand devices compliant to IEEE 802.11 standards. A Wi-Fi ready device simply means that it is ready for network operation with a WLAN. Wi-Fi is considered by the majority as one and the same to actual standard itself.

2.2.1 WLAN standard and performance

The main standards defining all aspects of the layer 1 and layer 2 operations for WLAN radio access mechanism are summarized in Table 1 below. All of the WLAN standards have similar protocol at the MAC layer which uses the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA): If a station wants to transmit, it first senses the medium. If the medium is busy, the state defers its transmission to a later time. Otherwise, it is allowed to use the medium. More standards are listed in Appendix 1.

standard	802.11	802.11a	802.11b	802.11g	802.11n
standard approved	Jul 1997	Oct 1999	Oct 1999	Jul 2003	Nov 2009
Frequency	2.4-2.4835 GHz	5.15-5.35 GHz	2.4-2.4835 GHz	2.4-2.4835 GHz	5 GHz and/or2.4 GHz
Throughput	1 Mbit/s	27 Mbit/s	5 Mbit/s	22 Mbit/s	144 Mbit/s
Data Rate	2 Mbit/s	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s
Modulation	DSSS	OFDM	DSSS	OFDM	OFDM

Table 1. IEEE 802.11 standards

2.2.2 Network architecture and functional elements

IEEE 802.11- based systems are used both for indoor and outdoor installations. Figure 2 represents the structure of a WLAN network.

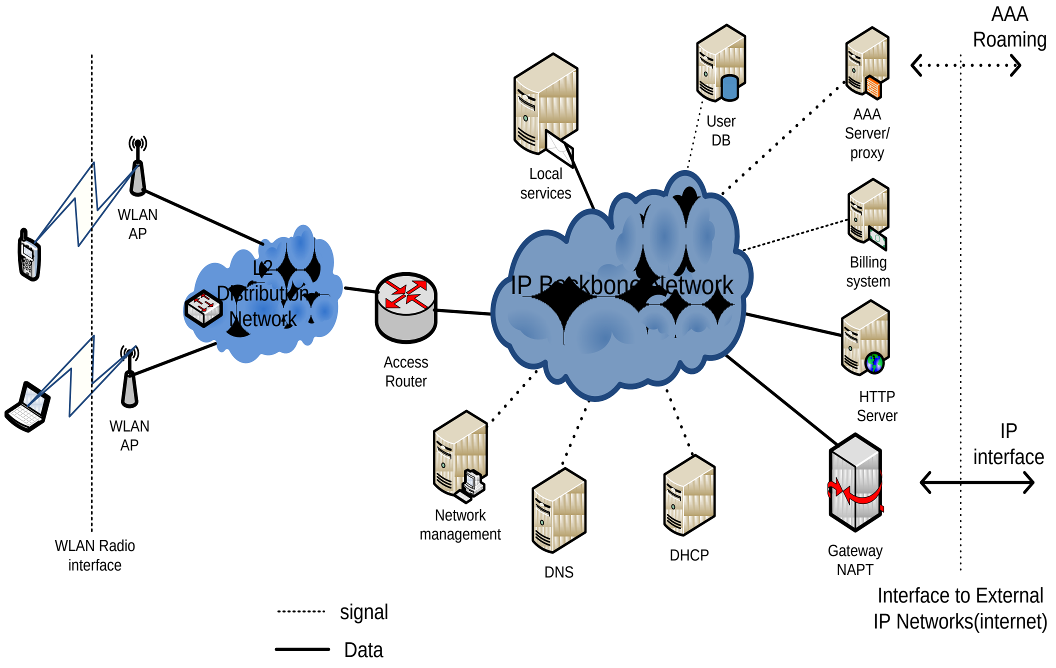


Figure 2. WLAN network architecture

A *Dynamic Host Configuration Protocol (DHCP)* server is required to enable configuration of the WLAN terminal's IP stack. A *Domain Name Server (DNS)* resolves Internet domain name addresses into IP addresses. A Gateway (GW)/Network Address and Port Translation (NAPT) are a entry toward external IP networks. The GW generally also performs IP network address and port translations to allow the WLAN network operator to use private-space IP addresses inside the WLAN system and enable access to services available outside IP networks at the same time. (Garg, 2010)

A *Hyper Text Transfer Protocol (HTTP) server* is used to offer local application-level service for accessing users. Accounting data is treated in the *billing system* server. The *local services server* is a general box covering services at IP level or above, such as mail servers and local web content. *Network management* takes care of the management of all network elements at all layers. It is instrumental in network configuration and monitoring. (Garg, 2010).

The WLAN terminal is typically a laptop computer, a personal digital assistant (PDA), smartphone or tablet with a built-in WLAN module or a PCMCIA WLAN card. The WLAN access point is mostly a layer 2 bridge between IEEE 802.11 and the Ethernet. The AP can also support IEEE 802.11i/802.1X functionality, in which case it is also a Remote Authentication Dial-In User Service (RADIUS) client toward the fixed network and performs radio link encryption toward the WLAN terminal. (Garg, 2010).

Access points are attached to *layer 2 distribution* networks such as a switched Ethernet subnet. The layer 2 distribution network may also provide intra-subnet mobility for WLAN terminals. The layer 2 distribution network enables layer 2 connectivity toward the first IP routing device, the *access router (AR)*. The basic function of AR is to route user IP packets. (Garg, 2010).

When a mobile host moves out of the coverage area of one AP into another, it has to associate with the new AP. After this, the wired network has to be informed of the new association. This inter-AP communication was not standardized. However, IEEE 802.11f has now been developed and allows the transfer of information from one AP to another to carry out fast handovers between APs of different vendors. The work by Salintzis and Passa (Salkintzis & Passa, 2004) discuss WLAN handover procedures in detail. In (Schmidt, 2004) more detail explanation about WLAN network architecture, different services states and mobility management is presented.

2.3 Femtocell

A femtocell, also known as Home Base Station (HBS), is a low-power access point which is used to increase the traditional mobile communication system's coverage and capacity in home and office environments (Khan, 2010). The femtocell operates in the licensed spectrum, and uses broadband connections and optical fiber or wireless lastmile technologies as backhaul to transport data over the Internet protocol. The Home NodeB Gateway (HNB GW) and Home NodeB Management System (HMS) are two new network elements that are introduced in release 8 (TS 25.467) for supporting femtocell operations. The HNB GW is used as a concentrator for all traffic received from the HNB. In the femtocell logical architecture designed by 3GPP in release 8, the HNB GW is placed in the operator's premises. The HMS, on the other hand, is used to ensure services user experience are of high quality and secured enough. More detail explanation about femtocell attributes and features are discussed in (Khan, 2010).

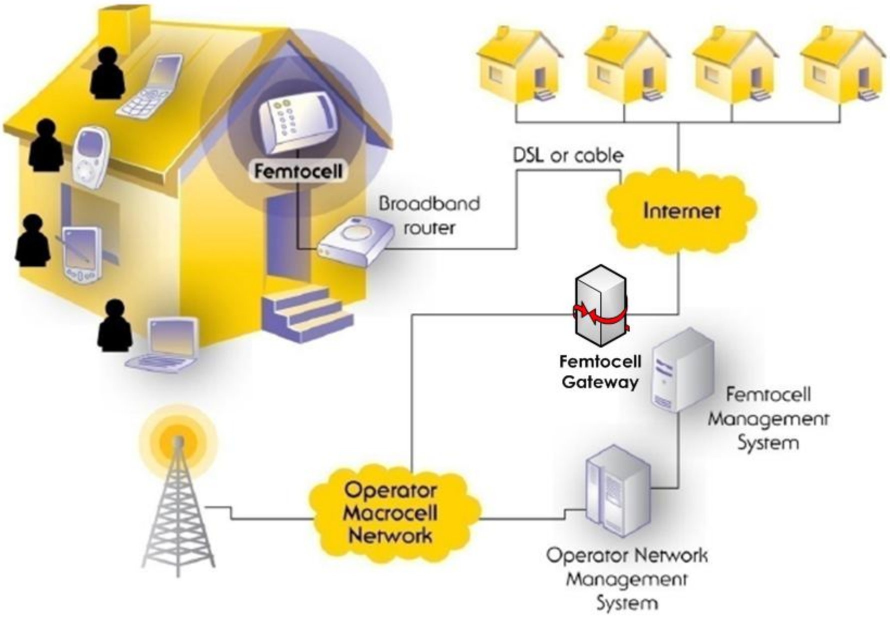

Femtocell
Broadband router
DSL or cable
Internet
Femtocell Gateway
Femtocell Management System
Operator Macrocell Network
Operator Network Management System

Figure 3. Basic femtocell network (Femtoforum, 2010)

Basic femtocell deployment model is illustrated in Figure 3. In order to use femtocell services, a user will buy a femtocell and will connect to it through its own fixed broadband access. Upon being connected to the broadband access, the HNB will further connect to the operator's gateway; thereafter the HNB will be authenticated and configured according to the user's subscription policy. (Khan, 2010).

3. MOBILE INTENET GROWTH AND IMPACT

3.1. Introduction and market trends

The use of smart phones and other mobile devices is changing how we access the Internet. Gone are the days when you had to go to the home office, boot up the PC or laptop, get a cup of tea, login, go for a second cup while the computer started all essential and non-essential services, come back and finally launch your preferred browser to access the Internet.

The new generations of mobile devices are easy to handle and are designed for instant access to the Internet. It takes less than 5 seconds on an iPhone or iPad to start the Internet browser. Furthermore, the way we consume content over the Internet is also changing. The Internet is feeding us with bits of information such as low resolution videos designed to fit on smaller screens. Social networking sites let us to post messages in addition to pictures and short videos. Many major content providers have a web-site that automatically adapts the content to smaller screen sizes and for everything else we go to the App Store or equivalent. In addition, there is growing number of new innovative location based mobile services that are pushing further the mobile use of Internet (Risto & Antti, 2010).

Such adoption of use patterns, applications and services from the main stream Internet to the mobile use is certainly rewriting the rules how data will be consumed in the mobile networks. This phenomenon is not just prediction of the future – the described rapid growth is taking place in many mobile networks today (Risto & Antti, 2010).

Most of research reports, (Cisco, 2011) (Informa, 2010) (ABI,2009) are predicting an increase of mobile data traffic by a factor of 26 in the next 5 years (2010-2015). Here are few numbers that put this trend into perspective:

- Cisco forecasted that (Cisco, 2011) :
    - Global Mobile data traffic will grow at a Compound Annual Growth Rate (CAGR) of 92 percent from 2010 to 2015, reaching 6.3 exabytes[1] per month by 2015.
    - The mobile-only Internet users will grow 56-fold from 14 million at the end of 2010 to 788 million by the end of 2015.
    - Mobile-connected tablets will generate as much traffic in 2015 as the entire global mobile networking in 2010. (i.e. 248 petabytes per month).
    - The average smartphone will generate 1.3 GB of traffic per month in 2015, a 16-fold increase over the 2010 average of 79 MB per month. Aggregate smartphone traffic in 2015 will be 47 times greater than it is today, with CAGR of 116 percent.
- AIB Research (ABI, 2009) forecasted that 48% of mobile data will be off-loaded by 2015. Additionally, mobile data traffic will grow by a factor of 30 meaning off-loading will expand by 100-fold by 2015.
- Two billion mobile broadband users in 2014 – that's 1024% growth[2].
- O2 UK reported that its mobile data traffic in Europe doubled every three months in 2009.
- AT&T reported that its mobile traffic increased 5000 percent in the past 3 years.

[1] *1 exabyte is 1,000,000,000,000,000,000 bytes =* 10^{18} *bytes = 1 billion gigabytes = 1 million terabytes.*

[2] *Ovum, Mobile Broadband Growth Forecast, April, 2009*

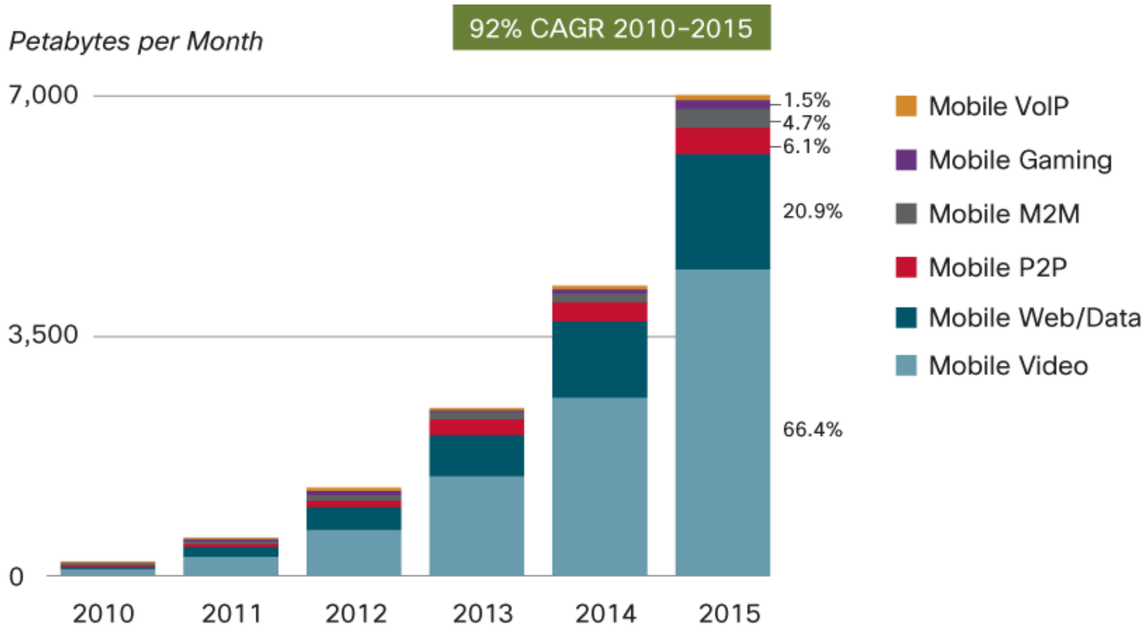


Figure 4. Cisco forecast for mobile data traffic (Cisco, 2011)

As can be seen in Figure 4 above, video streaming is expected to be the major consumer of the bandwidth resources, reaching in 2015 66% of total user's demand for bandwidth. This means, of the 6.3 exabytes per month crossing the mobile network by 2015, 4.2 exabytes will be due to video. In this report (Cisco, 2011) , nine major trends behind the growth of mobile data traffic are identified and explained.

3.2 Mobile Internet in Europe

A study conducted by European Interactive Advertising Association (EIAA) among 15 European markets emphasizes the ways in which consumers are engage with the Internet. According to the study (EIAA,2011), overall, 71 million Europeans browse the mobile Internet in a typical week , with almost an hour a day actively spent going online via their mobile (6.4 hours per week). Moreover, EIAA report also points that Internet continue to prove a popular source of entertainment with 25% of Europeans gaming or listening to the radio online , and 32% watching TV, Video clips or films, online at least once a month. Among those with an Internet-enabled phone, 49 % claim to receive video clips, websites or images on their mobile and 80% say that they pass on the content they receive. (EIAA, 2011).

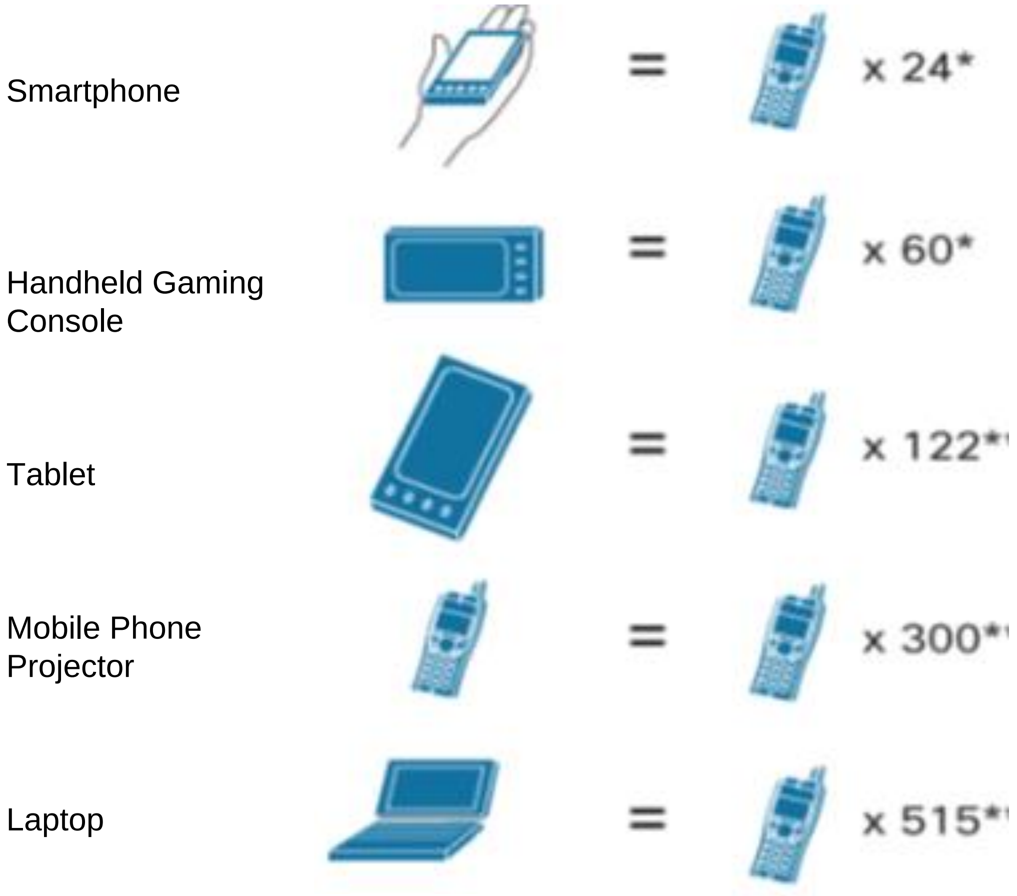
Additionally the EIAA report states that, Word of Web[3] , continues to play a central role in communication, with almost 71% of European internet users admitting that they stay in touch with friends and relatives more as a result of the Internet. Again, Mobile seems to be a big driver, with 48% of Europeans using their internet-enabled phones for more than verbal conversation. 16% say they communicate using social media via their mobile, with 16% also using mobile Instant Messenger. (EIAA, 2011).

In short, many drivers are pushing Internet users towards mobile devices and these changes in consumer behavior are having an impact on mobile networks and the companies who run these networks as discussed next.

3.2 The consequences of Mobile Data Growth on Operators Service

Having spent years planning and building out data-friendly 3G networks, mobile operators were looking just a year or two ago for ways to start filling the oceans of capacity they had created. Now, they are flooded with unprecedented uplift in mobile broadband traffic resulted from the introduction of laptops, tablets, and high-end handsets onto mobile networks.

[3] *EIAA defines it as the developing trend of word of mouth to word of web or communication online*



* Monthly basic mobile phone data traffic

Figure 5. High-end devices can multiply traffic (Cisco VNI Mobile,2011)

As shown in Figure 5, a single laptop can generate as much traffic as 515 basic–feature phones and a smartphone creates as much traffic as 24 basic–feature phones. Consequently, network usage threatens to outstrip capacity and has already done so in select dense urban markets. When a 3G cell reaches its data load, the size of the cell shrinks. This slows network speeds and increases dropped sessions.

AT&T Mobility is perhaps the most well-known operator struggling with a mobile data capacity crunch as the popularity of the iphone and other smartphones pushed data usage over the limit. Company directors have openly admitted that AT&T’s network was not operational up to par in densely populated cities such as New York and San

Francisco. But the company says it has now solved those problems. In related to this, AT&T has also indicated that about 3 percent of its smartphone users are generating approximately 40 percent of the operator's data traffic, and the company is looking at ways to encourage these customers to modify their usage.[4]This phenomenon is not unique for AT&T only but it is a common concern of most mobile operators in the world, especially in developed markets.

Other 3G operators also indicate that data congestion is the biggest challenge on the table. During Mobile World Congress (MWC) trade show in Barcelona, Spain, Vodafone CEO Vittorio Colao expressed his fears that demand for bandwidth-hungry services will outstrip network operators' capacity and their ability to guarantee the smooth flow of data through their networks.

Conversely, there are some groups, like Santiago Tenori of Vodafone, who state that there is no data capacity crunch concern, claiming that data growth can be tackled by a strong capacity planning procedure and sufficient investment and his company is doing this.

The Conflict may lie in what is actually producing the capacity problems. As said by Michael Thelander, CEO of Signals Reaserch Group, the majority of the network congestion is associated to signaling traffic coming from high end user device like smartphones and tablets which are continuously increasing on 3G networks. He reasons out in his Signals Ahead research report that these devices make constant queries to the network as they change among cell sites to push email, access social networking features and perform other repetitive actions. For example, a Skype user may send a message but then wait a couple of seconds between messages. To save battery life, the smartphone transfers into idle mode. The device has to set up a signaling path again, seconds later , when the user pushes another message. (Luna, 2010).

Network capacity will come under pressure not only due to the rise in traffic but also due to the fact that a high percentage of mobile broadband is expected to be consumed

[4] *"AT&T chief addresses network problems in NYC, San Fran," Dec. 9, 2009, FierceWireless*

indoors. According to Informa[5] 70% of all wireless traffic is estimated to be generated in indoors. As (Intellinet, 2010) explains, customers who are farther away from a cell antenna or indoors require more power to transmit and therefore introduce more noise. Hence, the more noise there is the less the capacity of an individual site.

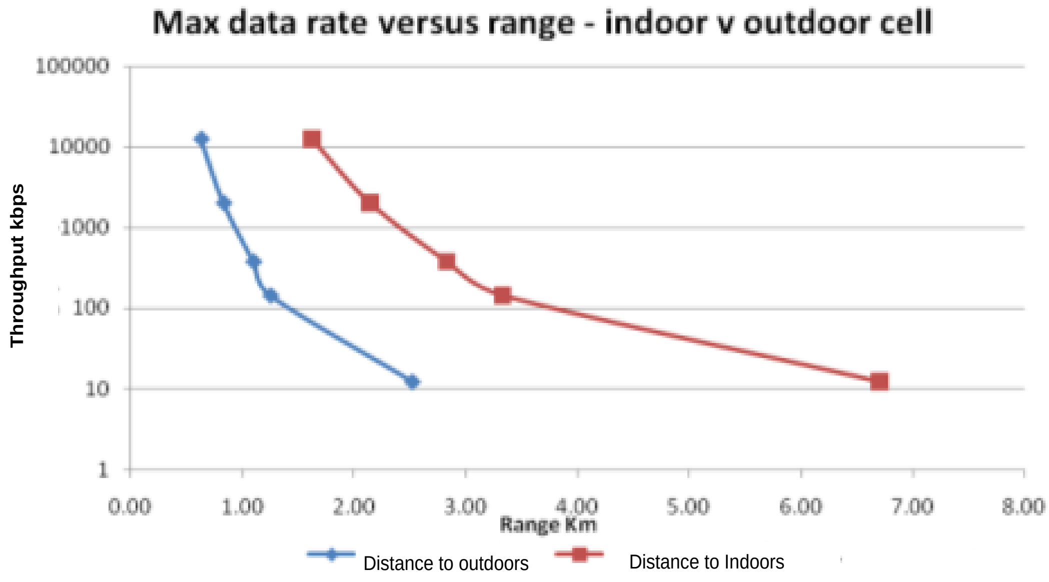


Figure 6. Data rate versus range for indoor and outdoor cells (Intellinet, 2010)

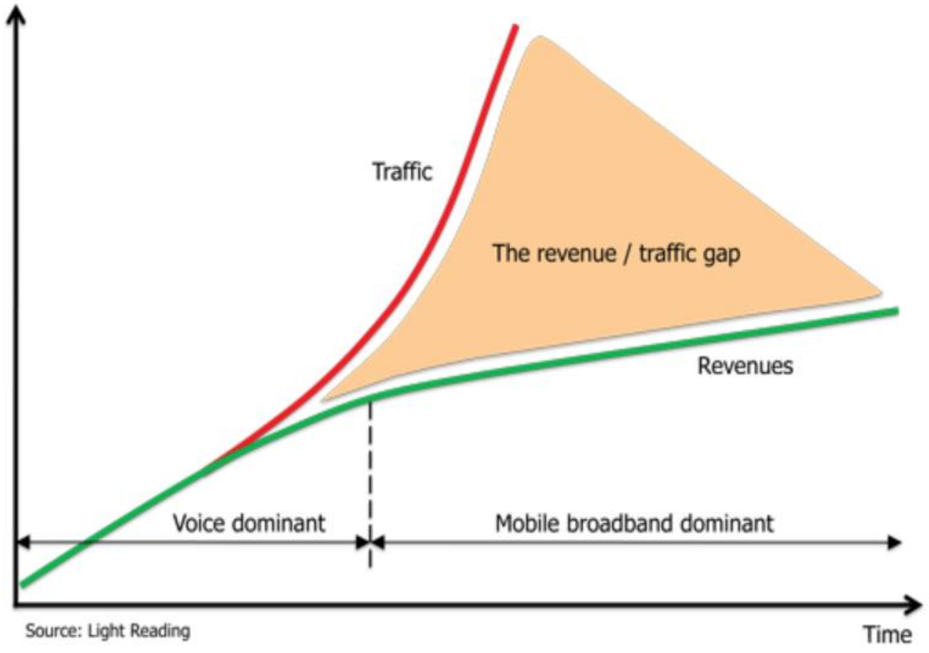
Figure 6 shows the maximum data rate achievable if all a HSPA cell capacity is dedicated to a user for different range and rates available for indoor versus outdoor locations. As it is clearly shown the range and rates available for indoor users are considerably lower than for outdoor user. In terms of cell capacity, this means, indoor users takes significantly more capacity than equivalent outdoor users.

Another challenge is that increase in data traffic does not result in a corresponding increase in revenue for operators. More than 75% of network traffic is broadband data, and the data volumes are growing rapidly. But the revenue generation is the opposite as the average for operators in Europe is that 77% voice, 10% SMS and 13% data

[5] *Informa is an international Research company*

(Mölleryd, 2010). This is because mobile broadband data service is flat fee based. Revenues are decoupled from traffic and therefore also operating costs and investment requirements. Costs are dependent on traffic per user, but not revenues. A study (BelAir, 2010) points, as an example, mobile broadband pricing that has fallen as low as $2 per gigabyte[6].

Consequently, service providers are faced with the prospect of mobile data delivery costs offsetting revenues by 2011 as shown in Figure 7. This paper (Mölleryd, 2010) discusses more about the ongoing academic as well as industry research around the issue of revenue gap.



Source: Light Reading

Figure 7. Growth of mobile data costs and revenues

The impact of mobile internet growth is now being felt alike by service providers and consumers. While subscribers are often not getting the level of service they expect, service providers are faced with the challenge of improving user experience levels and preventing the unacceptable — slow network speeds, dropped data sessions, and pent

[6] *which is nearly half a million times smaller than the price per gigabyte of an SMS message*

up subscriber frustration. Operators must find ways to bring the growth of their network costs associated with delivering mobile broadband services in line with and even lower than the growth in mobile data revenues.

3.3 Solutions for network congestion

Mobile operators have been considering a number of approaches to alleviate the mobile data congestion. The most natural inclination is to add more base stations. But this approach is impractical, costly and time consuming. In many cities, there are legal limits or explicit customer pushback on installing new macro base stations. Some look network upgrades to advanced cellular generations (4G, LTE) as imminent and unavoidable. It will help. However, there is not enough and clear revenue growth justifying for the required CapEx. New spectrum will eventually become available and will also help, but also will not be sufficient. There are multiple optimization techniques happening over 3G networks – Carrier addition to the NodeBs, Fiber to Site (AAV), Direct tunnel for GGSN, PCRF, IMS. Every single one of the changes consumes resources either as part of the spectrum, channel elements on RNCs, power or bandwidth on the core. These options are not a winning strategy especially under a flat price structure where revenue is independent of data usage.

Another method to overcome this capacity crunch is data offloading. Mobile data offloading, also called data offloading is the use of complementary network technologies for delivering data originally targeted for cellular networks (Intellinet, 2010). If the complementary network used by the operators to offload the subscriber's data traffic is Wi-Fi, then it's called Wi-Fi Offload. So far the wireless industry has come up with two offload solutions:

- using femtocells (small micro sites of cellular coverage)
- using Wi-Fi

Both femtocells and Wi-Fi access can mitigate the traffic problem .Many industry experts believe femtocell is a practicable approach given that service providers subsidize it and they are prepared to face the operational complexity of deploying and supporting them. On the other hand, unlicensed nature of spectrum, being a well-established home networking technology with significant penetration, commodity hardware and more importantly the presence of a Wi-Fi radio in all new smartphones, tablets and other consumer electronic devices make it a preferred offloading technology. Moreover, in long term, Wi-Fi can also supplements LTE deployment by taking off significant load from the network.

3.4 Attributes of Wi-Fi technology

Wi-Fi has many unique advantages as illustrated below.

Vast Unlicensed Spectrum

Wi-Fi operates in unlicensed ISM 2.4GHz and 5GHz bands, while femtocells operate in licensed 900MHz and 1800MHz frequency bands.

	Frequency Band	**Spectrum Availability**
Wi-Fi	2.400 to 2.483 GHz	83MHz
	5.250 to 5.875 GHz	505MHz
Femtocell	900 MHz	35MHz + 35MHz
	1800 MHz	75MHz + 75MHz

Table 2: Spectrum size

As shown on Table 2, operators have larger free spectrum available to provide to any size of Wi-Fi deployment, unlike femtocells, which use costly and limited spectrum that requires careful channel planning. Thus, Wi-Fi networks are very cost-effective and can be deployed rapidly with cheap installation costs.

Unmatched Data Rates and User Experience

Next-generation of Wi-Fi networks, known as 802.11n networks, have ushered in improved coverage, capacity and interference handling of Wi-Fi , offering operators the scale they need to effectively offload 3G data traffic onto Wi-Fi infrastructure. 802.11n effectively bumps Wi-Fi's theoretical performance 10-fold and can deliver 20 times the capacity promised by LTE (BelAir, 2010) .The Table 3 provides a comparison of data rates and application level throughputs for Wi-Fi and mobile networks.

	Femtocell (HSPA)	**Wi-Fi (802.11n)**
Data Rates	42Mbps (3GPP release 8)	600Mbps
Throughputs	12Mbps	350Mbps
Modulation	OFDM	DSSS, and OFDM

Table 3. Network speed of Wi-Fi and femtocell

High Quality of Service and Advanced Security

Wi-Fi has gone through a series of improvements to support Quality of Service (QoS) through Wi-Fi Multimedia(WMM) for delay-sensitive voice and video applications, along with, standard-based business-grade security(WPA2). The author in (proxim, 2010) describes QoS and security support in Wi-Fi as equivalent to that of 2G/3G networks. WMM Quality of service is based upon a subset of the IEEE 802.11e standard. It enabled Wi-Fi networks to offer a prioritized treatment to multimedia applications to support the jitter and latency requirements. The WPA2 is based on IEEE 802.11i and it provides 128-bit AES-based encryption using Pre-Shared Key (PSK) or 802.1x RADIUS authentication, which is ideal for operators to provide Authentication, Authorization and Accounting (AAA) services.

Reduced Total Ownership Cost

Wi-Fi technology has evolved and matured, for the last decade, pushing down the equipment cost considerably. Also, with data rates of 600Mbps and availability of more than 500MHz of unlicensed spectrum, Wi-Fi offers huge network capacity compared to 3G/4G. Thus, Wi-Fi requires less equipment to serve a given subscriber base. Besides, the Wi-Fi networks can be simply and cost-effectively scaled without requiring much investment in site surveys and channel planning. So, Wi-Fi offers huge CapEx and OpEx benefits for service providers. (Altai, 2010).

4. WI-FI AS A STRATEGIC TOOLS FOR OPERATORS

3G and Wi-Fi technologies are complementary. Cellular networks provide near-ubiquitous wide-area coverage, chiefly outdoors and on the road, whereas Wi-Fi is a shorter-range technology, but offers higher speeds, low cost and self-installation. While 3G operators are still in the middle of a move to broadband links for radio tower backhaul, Wi-Fi access points are usually backhauled by high-speed LAN or wired broadband connections. And Wi-Fi serves those locations where data usage is highest (at home and in the office) and which; being indoors, also suffer from poor 3G signal penetration.

Wi-Fi Strategic opportunities for operators include using this wireless technology for 3G/4G offload and also for new application such as managed wireless LAN services (i.e. using Wi-Fi for broadband service to high-density user areas where there aren't good wire line alternatives) to offer rich content and communications. In this paper we will focus on the role of Wi-Fi to offload mobile data traffic.

4.1. Type of Offloading

There are two types of Wi-Fi offloading: on-the-spot and delayed. Lee et al explains " On-the-spot offloading is to use spontaneous connectivity to Wi-Fi and transfer data on the spot. In case user move out of the Wi-Fi coverage, they stop the offloading and all the incomplete transfers are transported through cellular networks. Most of the smartphones which give precedence to Wi-Fi over the cellular interface in data transmissions can be expected to currently attain on-the-spot offloading. In delayed offloading, each data transfer is associated with a deadline. As users come in and out of Wi-Fi coverage areas, it continually resumes data transfer until the transfer is complete. Cellular networks lastly complete the transfer in case the data transfer does not finish within its deadline."

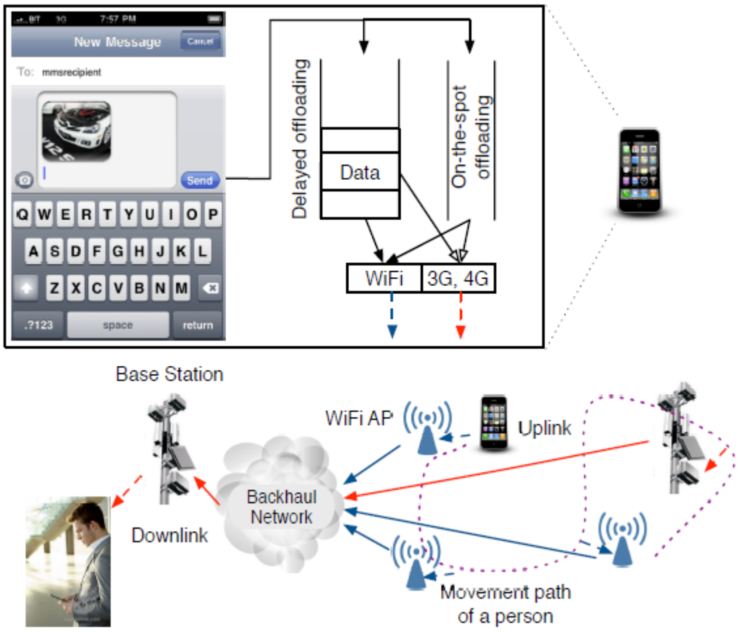


Figure 8. Sketch of mobile data offloading (Lee, 2010)

Most Wi-Fi enabled smartphones are already, by default, performing on-the-spot offloading. Delayed offloading is relatively new. “Its system is very close to that of delay-tolerant networks where applications can tolerate some amount of delays” Lee explains. It is fact that users want to have data as fast as possible but many data transfers can tolerate delays. If network carriers provide more incentives in price for users to use transfers with longer deadlines, it will create demands for them because users will select more judiciously their transfer deadlines based on their own needs. Example of possible scenario is as follow:

- Tom wants to email Mirva a roll of pictures , but there is no rush for immediately delivery and besides the carrier charges less if he choose to have it delivered within thirty minute .

In this paper, we discus only on-the-spot offloading and the term offloading by default stands for it.

4.2 Wi-Fi offloading Strategy

There are several ways for operators to offload mobile data traffic in to Wi-Fi. Based on our study on a number of operators and vendor solutions, we divide the offloading approaches in to three distinct categories based on the level of integration between the two technologies and operator's control of the subscriber. These are:

- network bypass
- managed network bypass
- integrated data offload

4.2.1 Network Bypass

Network bypass is the process of transparently moving mobile subscribers data onto Wi-Fi network, when they are in Wi-Fi range, in the goal of completely bypassing the core network for data access i.e. voice continues to be delivered via the core network. This is achieved by putting a client application on the subscriber's device to detect when they are in a Wi-Fi range and automatically moves all data traffic to Wi-Fi network.

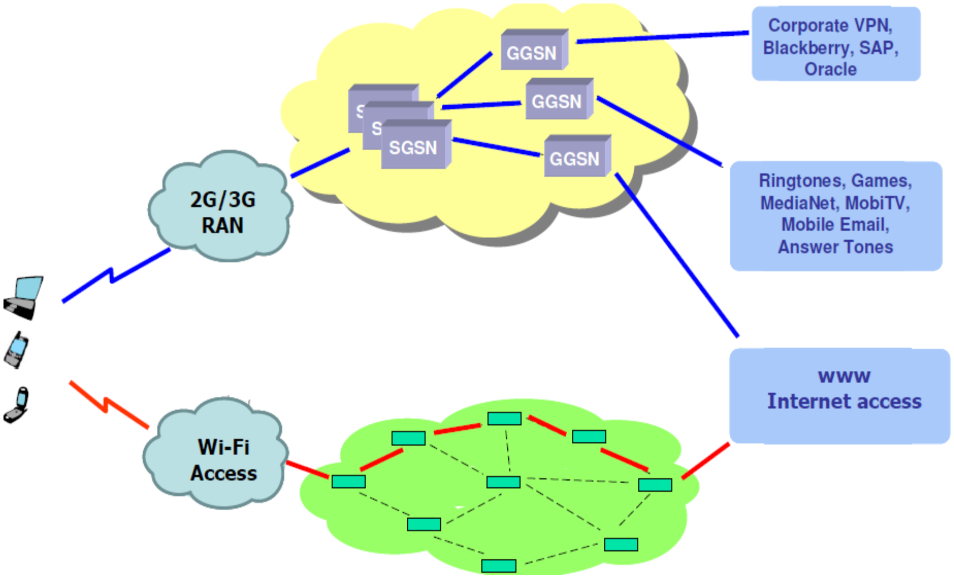

GGSN
GGSN
GGSN
SGSN
2G/3G RAN
Corporate VPN, Blackberry, SAP, Oracle
Ringtones, Games, MediaNet, MobiTV, Mobile Email, Answer Tones
www
Internet access
Wi-Fi Access

Figure 9. Network Bypass (Intellinet, 2010)

Network bypass does not require any additional network equipment to be installed in operators' network. However it has two major limitations. First, the operator loses control of their subscriber while they are connected to internet via Wi-Fi. This will prevent the operator from billing for service. Second, since there is no connectivity between the device and the mobile core network, the operator is unable to provide any 3GPP based services leading to possible loss of revenue. (Intellinet, 2010)

4.2.2 Managed Network Bypass

This offloading strategy is for those operators that are uncomfortable with the previous strategy level of disassociation of the two networks and the resulting loss of control of the subscriber. This may be due to several reasons. Some operators provide metered access to a network that requires subscriber management. While others insist on secure access for their subscribers when they are connected via Wi-Fi. In some cases, operators would just want to be aware of subscribers browsing behaviors for targeted marketing or safety reasons. This solution is provided without the need to fully integrating the two networks.

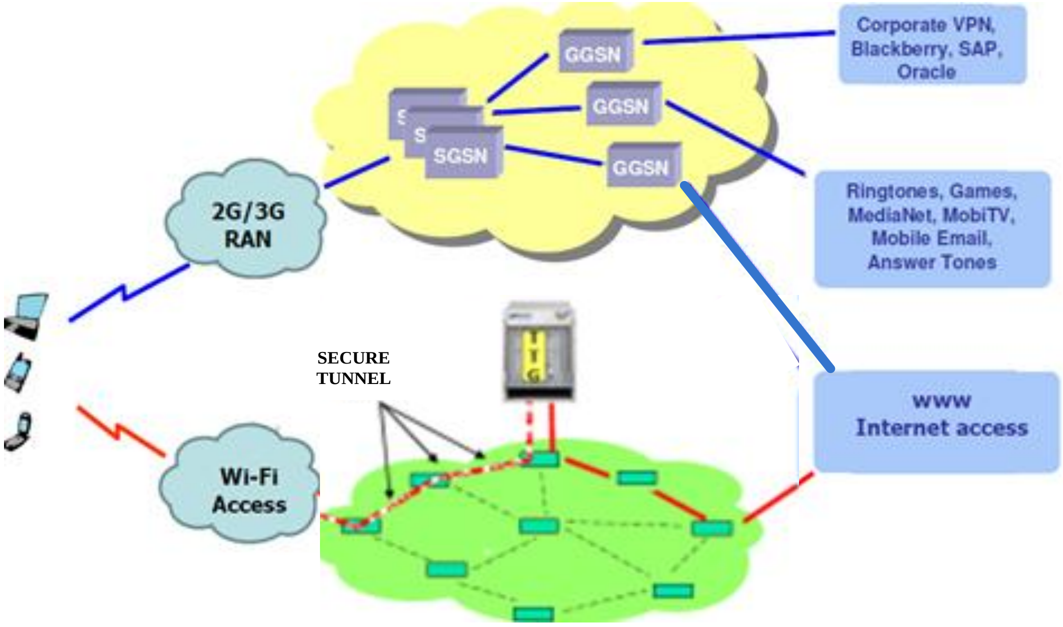

GGSN
GGSN
SGSN
GGSN
Corporate VPN, Blackberry, SAP, Oracle
Ringtones, Games, MediaNet, MobiTV, Mobile Email, Answer Tones
2G/3G RAN
SECURE TUNNEL
TTG
www Internet access
Wi-Fi Access

Figure 10. Managed Network Bypass (Intellinet, 2010)

Nevertheless, although this solution enables the operator to ‘manage’ their subscribers, it still stops them from providing any operator subscribed content via Wi-Fi access. Nevertheless, it does solve the issue of network congestion and may work well for some operators that do not have any noteworthy walled garden content to provide.

4.2.3 Integrated Network Offload

Integrated Network Offload In this method, Wi-Fi is internetworked with the core mobile network through a bridge to provide a seamless experience to subscribers when they move between the two networks. This approach is preferred choice for operators who want not only to manage their customer but also want to be able to deliver carrier subscribed content through Wi-Fi network. The new function that’s introduced in operator network is the TTG which authenticates devices (via AAA queries), decrypts sessions originating from mobile handsets, allocates IP addresses and protects the layer 3 and key exchange infrastructure from denial-of-service attacks.

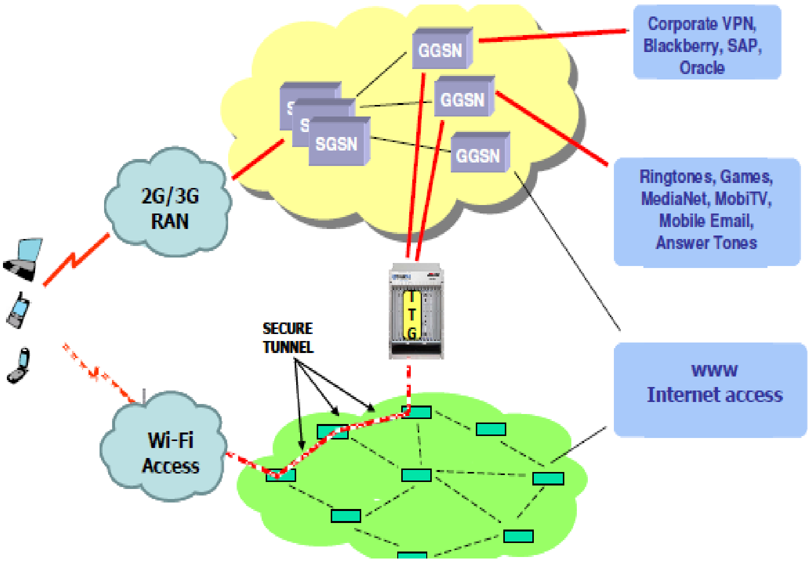

GGSN
GGSN
GGSN
SGSN
Corporate VPN, Blackberry, SAP, Oracle
Ringtones, Games, MediaNet, MobiTV, Mobile Email, Answer Tones
2G/3G RAN
TTG
SECURE TUNNEL
Wi-Fi Access
www Internet access

Figure 11. Integrated Network offloads (Intellinet, 2010)

But this approach is characterized by complex mobile and Wi-Fi network integration challenges and expects mobile devices to be equipped with special software.

In conclusion, the strategy that has to be applied will to a large extent depend on the mobile carrier, their service profile as well as their customer's usage habits. (Intellinet, 2010)

4.3 Use Case – 3G to Wi-Fi offload

In this section we present sample use cases that explain how operators can engage possibly using Wi-Fi offload. This is based on the idea presented on (GSMA,2010)

4.3.1 Use case using Device accessing video – Mobile TV and/or You Tube

A 3GPP network customer has a 3G capable and Wi-Fi enabled smartphone. They subscribe to mobile TV services and often watch music videos on iTune and You Tube. He is a regular traveller and frequently in range of Wi-Fi hotspots in coffee shops, airport and trains terminals as well as hotels.

Scenario:

- On the bus from conference hall , he was attending as a guest speaker, to airport the user starts to watch news from an international news network on the 3GPP network.
- As soon as he enters the airport terminal, his phone detects the presence of a Wi-Fi hotspot.
- The device automatically connects and authenticates the user with the hotspot using USIM.
- Having already checked-in online the user goes directly to security and pockets his phone.
- The moment he is in the departure area, he resumes watching the news programme, however this time the service is being delivered via different Wi-Fi operator, with which his 3GPP operator has roaming agreement.

- The device checks that the new provider is allowed, and checks operator policy on use of the roaming network. If there is no charging difference the operation continues on the visited network. But If charging is different due to the change, the user is notified and he is prompted to approve roaming onto this new network.
- The user arrives at his home airport on his late flight and takes a taxi home. His local Ice hockey team is playing finals tonight and he is about to miss the match so he selects TV application from his device's screen. His pre-existing TV subscription is activated.
- The user selects the Ice hockey match from the lists on his device screen and starts to watch the match via the 3GPP network in the taxi.
- The moment the user enters his concert walled home the coverage from the local 3GPP cell drops but he has home Wi-Fi network.
- Then his device automatically connects and authenticates with the residential hotspot using the USIM or WPA2-PSK.
- The user continues to watch the match on his device, without miss the first goal being scored.

4.3.2 Use Case using multiple SSIDs

A network service provider would like to use custom configured access points with multiple SSIDs to offer WLAN connectivity to casual users who are not the owners or normally resident at the premises where the access point is installed. This may support a commercial relationship between the 3GPP operator and the WLAN provider. The casual users' devices would have to be pre-configured to authenticate to the SSIDs in the access point.

Scenario:

- A customer has a Wi-Fi capable device which has been pre-configured with the SSID(s) allocated by the 3GPP network provider for use in this service. As part of the commercial offering the customer may also be required to advertise the same SSID's on their home Wi-Fi Router.
- The customer receives a call from a colleague who needs a file to be sent to them urgently. There is no easily accessible and/or obviously Wi-Fi capable establishment (coffee shop, hotel etc) in the near locale and macro 3GPP network coverage is poor.

- The customer knows they are a subscriber to this Wi-Fi service and activates the Wi-Fi on their device. Luckily – there is a Wi-Fi Router advertising the pre-configured SSID of the service.

The device authenticates on the Wi-Fi router and he is able to establish a connection and send the file.

There is no doubt that Wi-Fi offloading reduces the load on 3G networks. An ABI Research study (ABI, 2010), Mobile Data Offloading, forecasts that mobile data offloading will triple by 2015 to 48%.Since data traffic volumes will have grown by a factor of 30, it means that the amount of offloaded data will increase 100-fold in real terms. But an important question is, how much benefits offloading can bring to network providers and users. What are the cost savings? In the next section, we try to answer these questions with support of academic and industrial research conducted recently.

4.4 How much Wi-Fi can deliver?

Mobile data offload reduces costs as well as relieve network traffic. Wi-Fi does this at a tiny fraction of the per-Gigabyte cost of a 3G networks. According to a UBS research note, radio access networks and backhaul account for 70 to 80 % of an operators' network CapEx. So offload can save a substantial amount of capacity and cost. The ABI Research (ABI, 2010) report precisely quantifies these savings. In (Mölleryd, 2010), it is explained that service providers deploying a Wi-Fi offload strategy can expect savings in the range of 20 to 25 per cent per annum. In the US market, service providers could save between $ 30 to $40 billion per year by 2013[7].

In (Risto & Antti, 2010), cost impact of Wi-Fi offloading is explained applying the methodology introduced in Nokia Siemens Networks white Paper (Network Nokia Siemens, 2010). Antti el al said " 7% of daily traffic take place during the busiest hour

[7] chetan Sharma consulting ,2009

of the day. If an operator is able to reduce the cellular busy hour traffic in congested areas down to 6% or 5%, it will result in 14% or 28% reduction of the amount of base station sites needed in capacity limited areas." .In supporting the previous taught, this paper (Ang, 2010), explains in detail how operators can start saving network cost through data offloading by making certain network assumptions. The paper asserts that data offloading can bring operators 16% saving of OpEx or 2.9 % of Total Cost of Ownership (TCO).

According to Consumer Report, the average data usage of iPhone users is 273MB per month, while average voice usage is 450min/month. As voice call requires 12kbps bandwidth, this translates to an average per user bandwidth requirements of 120bps and 840bps for voice and data services, respectively. This implies, a carrier can, on average adds 7 additional voice users for every data user offloaded from 3G to Wi-Fi. Thus, a carrier can significantly add voice subscribers to their existing infrastructure and generate additional revenues. It is also interesting to mention that a number of smartphone applications, such as FaceTime on the Apple iPhone, only work via Wi-Fi. Moreover, Morgan Stanley[8] estimates that, for the iPhone, optimized Wi-Fi can be 10x faster than 3G data speeds, and providing Wi-Fi service is only a third of the cost per bit of 3G data networks.

The paper , by Kyunghan Lee el al (Lee, 2010), is presents a quantitative study on the performance of 3G mobile data offloading through Wi-Fi networks by recruiting 100 iPhone users. According to their findings, Wi-Fi offloading can offload about 65 % of total traffic load and can achieve about 55% energy saving for mobile devices because Wi-Fi offloading can reduce the transmission time of mobile devices significantly.

4.5 Partnering models for 3G offload to Wi-Fi

Once data offload is accepted as a requirement for supporting a 3G customer base, the first question to resolve is what type of Wi-Fi network will be targeted. Three partnering models for 3G offload to Wi-Fi are possible:

[8] *Morgan stanley is global financial services firm.*

- Individual users Wi-Fi access point
- A hotspot affiliate or Aggregator's Wi-Fi network
- Operator-owned Wi-Fi network

An initial plan will likely include aspects of each model, but the committed operator will move strategically towards the second or third alternatives.

Individual Users Wi-Fi Access point

Home broadband services are usually delivered by fiber, DSL or cable distribution networks, progressively more terminated by Wi-Fi. Wi-Fi access points can be purchased separately by the consumer, or offered as part of the cable modem or DSL termination. By offering a branded, centrally-managed access point, the operator can remotely configure the access point so smartphones automatically connect without any user intervention, and can maintain a high degree of control over the end-to-end service. If an operator-provided access point is not used, it is up to the user to configure the access point with unique wireless identifiers and authentication key. To offload service from the 3G network, the subscriber must configure their smartphone with these key parameters. This is usually a once-only operation, and thenceforth the smartphone will switch to the access point whenever it is detected. User configuration is as simple, but as random as it sounds. Only those users with the technical ability, knowledge and incentives are likely to set up their devices. Various Quality of Service (QoS) and other Wi-Fi parameters can be set incorrectly and as a result many opportunities for offload will be lost. (Thornycroft, 2010).

Hotspot Affiliate Model

Wi-Fi networks are notoriously fragmented: most cities and countries comprise hotspots from a number of service providers. So to gain coverage in all the places a smartphone user visits, it may be necessary to use many different networks. The fragmentation problem has been somewhat mitigated by hotspot aggregators, who provide a single sign-on that covers many members hotspots. This can be achieved by using web page that allows the user to select their 'home' operator, and enter their credentials.

Nevertheless, as we will discuss later, the mechanisms and protocols used for this type of access are optimized only for PC clients. While users are willing and able to read web pages and enter credentials on a PC, it remains quite challenging to configure today's smartphones to negotiate all the variations encountered in such an environment, and automatically log-in and offload traffic without user intervention. For 'always on' applications such as Facebook, that generate significant data traffic even when the smartphone is pocketed, this is a serious traffic concern. (Thornycroft, 2010).

Operator owned Wi-Fi network

The third option is for the 3G operator to accept that offload to Wi-Fi is an immediate and on-going requirement for offering mobile data services , and to embrace Wi-Fi as a competitive weapon. This captures the Wi-Fi revenue that would otherwise be lost to affiliates and allows tighter integration between 3G and Wi-Fi networks to make maximum use of offload opportunities.

4.6 How Operators Are Responding

Mobile operators has been interested to use low cost Wi-Fi networks to extend or infill service coverage long ago . Initial convergence applications included Orange/France Telecom's 'LiveBox' service in France, BT's 'Fusion Service' in UK,T-Mobile's Hotspot@Home service in the U.S. TeliaSonera's HomeFree service in Denmark and Telecom Italia's Unico service in Italy. These all showed great promise in 2006 as a means of leveraging wireless and DSL services to offer a low cost consumer/business voice offering. However, lack of compelling business cases to move this traffic to alternative access network result commercial failure. Moreover, many operators who already have strong in-door coverage continued negative marketing, calling it an interim technology (Accuris networks, 2010).

Data is a different story. The recent explosion of mobile data traffic taxed 3G capacity up to limit. Interestingly, many carriers are now reconsidering Wi-Fi as a key component of an effective network congestion reduction strategy. Wi-Fi is evidently working for AT&T(in US) and O2 (in UK) with the iPhone. Both China Mobile and Softbank in Japan have announced Wi-Fi offload as an important element of their network strategies.

A number of profile partnerships between Mobile network operators and Wi-Fi providers are already in production. For instance (Accuris networks, 2010):

- July 2008 – O2 UK agreed a partnership with BT Openzone and The Cloud, the two largest Hotspot providers in the UK.
- November 2008 – AT&T acquired Wayport for $275m; gaining 20,000 hotspots across the US and 80,000 globally.
- July 2009 – Verizon announced a partnership with Boingo Wireless for their mobile and DSL customers

Moreover, China Telecom and PCCW in Hong Kong have been bundling mobile broadband with Wi-Fi hotspot coverage. Telenor in Switzerland is moving into the Wi-Fi managed services space. T-Mobile has purchased a nationwide WLAN hotspot network and has been very committed to building out a global T-Mobile branded WISP service since.

More and more carriers around the world are adopting Wi-Fi as a leading solution for data offloading:

John Stankey, AT&T's President and CEO: *“Focusing on how we make Wi-Fi and licensed spectrum a more seamless experience for customers.”*

Masayoshi Son, SoftBank’s CEO and Chairman: *“Wi-Fi is the mouth – it helps you breathe better. We need Wi-Fi to serve that traffic and give our customers a rich media experience.”*

René Schuster, Telefónica CEO: *“We are looking forward to offering customers the ability to enjoy iPad with Wi-Fi + 3G on our network.”*

Yves Maitre, Orange senior vice president of mobile multimedia*: “Wi-Fi offload is becoming more and more of a reality and it is the number one priority for my team for 2010.”*

4.7 Mobile offload challenges

While undoubtedly, there is strong demand for mobile Wi-Fi offloading there are a few major difficulties that have so far hindered the widespread acceptance by mobile operators. lappeteläine et al (Risto & Antti, 2010) point out these challenges as followed:

- how to acquire sufficient Wi-Fi capacity and coverage for offloading
- how to enable flexibility and diversity in data plan pricing schemes
- how to provide simple and secure access with automatic credentials delivery
- how to control congestion of Wi-Fi networks

In addition, a quick scan of online user forums reveals many frustrations and concrete blocking factors to mass adoption of Wi-Fi offloading: mainly through inconsistent user experiences. These complaints were categorized in four groups:

1. **Client software** --needs to be downloaded to the Wi-Fi device. Verizon’s service requires user to register for the service via an online portal (Using their Verizon username and password) and download software to their device that will allow them to connect to a Wi-Fi hotspot. There is hug online frustration with the way it is executed, mostly relating to the need for specific client software and the impact on the device performance.

2. **Discovery** – Is the Wi-Fi network that they can see, a partner for their mobile operator? What about SSIDs that say ‘Free public Wi-Fi ’- why are they being prompted for payment? There is lots of user confusion in this space.

3. **Authentication** – most service providers offer automated login facility. User forums are full of questions about this facility not working; being prompted for usernames and passwords; reset procedures etc.

4. **Service continuity-** user names/passwords, cookies and device IDs are not sufficiently secure for many carriers to open access to premium services such as Mobile TV. This is real disappointment from consumers as they cannot access carrier services they have subscribed to use while connected via Wi-Fi.

5. WIFI MOBILE OFFLOADING DEPLOYEMENT CONSIDERATIONS

It is important that access points and end user devices support the necessary standard amendments to address many of providers concerns about the integration of Wi-Fi into mobile operator infrastructure. These requirements include identifying a suitable network to connect to, security, automated authentication and QoS. This can be accomplished in a number of ways, and we explain in this chapter.

Apart from that, there exist today innovative technology solutions in the market which can leverage mesh networking principles to solve the backhaul challenge or smart antenna technologies which can help to deal with interference or to enhance coverage.

5.1 Identifying Suitable networks for connection

User device must be able to identify a suitable network to connect to. A Wi-Fi access point advertises its services by transmitting periodic beacons, each containing a Service Set identifier (SSID). Smartphones should be pre-configured with a short list of ‘known’ SSIDs corresponding to the operator’s Wi-Fi networks, and affiliated hotspot partners. Device manager are used for provisioning of SSID settings in to device.

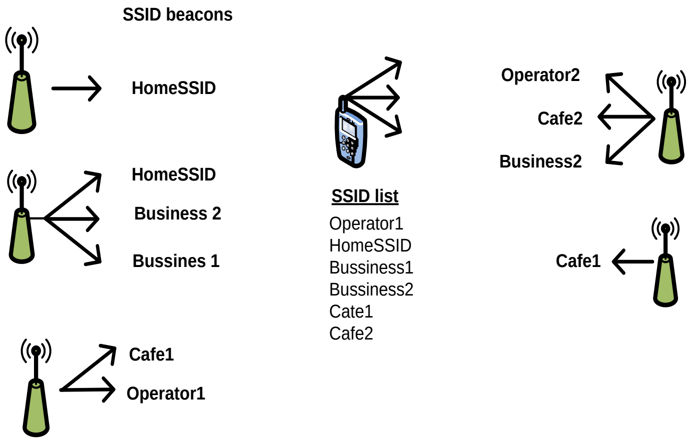


Figure 12. Identifying a Wi-Fi network

In many countries and cities the Wi-Fi market is fragmented, with many small players. Although, they are beginning to consolidate hotspot networks the list off suitable SSIDS may grow over time to maintain coverage in all the places a smartphone user visits. So the operator should ensure that phones can be updated as new Wi-Fi network options are added.

However, there are tradeoffs to configuring a lengthy list of SSIDS. Most smartphones use a combination of active and passive scanning to discover Wi-Fi networks, and a larger range of SSIDs will result in more Wi-Fi transmissions and hence reduce battery life. Inter-access point roaming can also be impaired by excessively long SSID lists. For the present, these challenges are addressed by smartphone vendors' scanning and probing algorithms, but developments in a forthcoming standard, IEEE 802.11u, promise a more scalable and elegant solution in the future. (Thornycroft, 2010).

5.2 Initiation of offloading

There are three main offload initiation schemes:

- Wi-Fi scanning based initiation.
- User initiation.
- Remotely managed initiation.

In the Wi-Fi scanning based initiation the user device performs periodically WLAN scanning. When a known Wi-Fi network is found, an offloading procedure is initiated instantly. For this mode to be effective, network selection should provide the following capabilities:

- The home operator to be able to configure list of preferred SSIDs that can be used for automatic selection on the smartphones.
- The user to be able to configure the list of preferred Wi-Fi access networks that can be used for automatic selection.
- For the device to select network based on parameters such as QoS, connectivity, signal strength

- For device to detect and switch to preferred network when not in an active communication state with the current network.

In the user initiated mode a user is prompted to select, manually from the available Wi-Fi accesses. This happen once per a network access session. Users are also capable to add list of preferred SSIDs that can be used for manual selection.

In the Remotely managed approach a network server initiates each offloading procedure by prompting the connection manager of a specific user device. Operator managed is a subclass of the remotely managed approach .In the operator managed approach operator is monitoring its network load and user behavior. In the case of forthcoming network congestion the operator initiates the offloading procedure.

For operators which have both Wi-Fi and 3GPP infrastructures, it is possible to use Access Network Discovery and Selection Function (ANDSF). This is a layer 3 protocol specified by 3GPP. It enables mobile devices located in areas of two or more different types of access connectivity to select the most appropriate access network by exchanging information between the mobile device and a server. (GSMA, 2010).

5.3 Security and Authentication Option

Users accessing to services via operator hot sports or operator partner Wi-Fi networks need to be authenticated to allow only authorized access to service. As well Wi-Fi network access security is needed to protect against theft of service and other attacks.

There are two sets of security requirements need to be addressed:

- **Wi-Fi network access security:** This concerns authentication of the customer towards the Wi-Fi network, of the network towards the customer device, and the protection of the Wi-Fi access link.
- **Services access security**: This concerns authentication of the customer towards operator or third party services when connected via Wi-Fi (or other non-cellular access networks), and the protection of this link.

Wi-Fi network access security

Currently there are various authentication mechanisms in use , for example web portal based login page requiring username and password , Wireless Internet Service Provider roaming (WISPr) based mechanism, SIM based authentication, certificate based authentication etc. If end user is required to input manually username and password when accessing to services via Wi-Fi network, many users don’t bother and offloading traffic to Wi-Fi is less successful. Thus seamless user authentication when accessing to services via Wi-Fi network is an enabler for offloading traffic to Wi-Fi solution, and it also improves greatly usability.

As offloading traffic from cellular to Wi-Fi involves devices supporting both cellular and Wi-Fi radios and have SIM cards, preferred authentication mechanism is (U)SIM based authentication (EAP-SIM, EAP-AKA). SIM based authentication leverages already existing HLR/HSS and 3GPP authentication standards.

In addition to SIM based authentication, existing devices not supporting SIM based authentication over Wi-Fi and non-SIM devices may need to be supported, like laptop, PCs. In this case, Authentication, Authorization and Accounting (AAA) servers have to support multiple authentication mechanisms allowing to support different devices with their different authentication capabilities.

Authentication preferences for different Wi-Fi networks: (Forseel, 2010)

- Operator Wi-Fi hot spots: (U)SIM based authentication (EAP-SIM, EAP-AKA). WISPr, EAP-TLS or EAP-TTLS/MSCHAPv2 as secondary option to support authentication for devices not having SIM card or not yet supporting SIM based authentication.

- Operator partner Wi-Fi hot spots: Same as for operator Wi-Fi hot spots. Note: In this case partner Wi-Fi provider may require using another authentication mechanism than home operator, like WISPr, requiring separate client/data to be downloaded and installed into a device.

- Private home WiFi network: WPA-PSK, WPA2-PSK or alike
- Shared home WiFi network, public part that also other operator subscribers may use (visitors): Same as for operator WiFi hot spots.

Hot sport authentication using WISPr

Wireless Internet Service Provider roaming (WISPr) is configured behind open access points, with no authentication at the Wi-Fi layer. Any device wishing to connect is accepted .Following client association at the Wi-Fi layer, a captive portal (CP) web page intercepts the first Web request and is used for authentication. An XML protocol allows exchange of userid and password credentials between the client and the service provider's RADIUS server. Once authentication is complete, the client is allowed access to the operator's network or the Internet. Otherwise, there is no accesses beyond the AP. For attractive user experience, credentials have to be entered only once, and a smart client can be configured to connect automatically to a hotspot whenever the device is Wi-Fi range next time. See Figure 13 for authentication procedure.

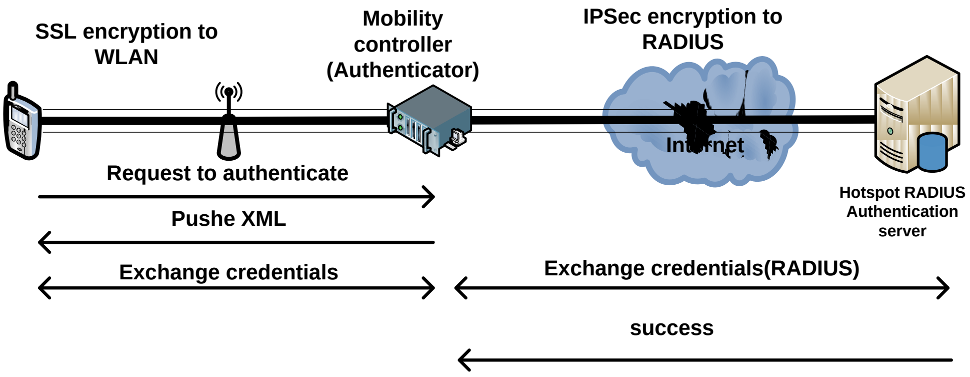

SSL encryption to WLAN
Mobility controller (Authenticator)
IPSec encryption to RADIUS
Internet
Hotspot RADIUS Authentication server
Request to authenticate
Pushe XML
Exchange credentials
Exchange credentials(RADIUS)
success

Figure 13. Hotspot Authentication using WISPr

Most operator hotspots are configured in this way today, using some variation of the WISPr protocol and often based on the subscriber's email address and password for access credentials.

WISPr's primary advantage is that it offers a common authentication regime for all users of a Wi-Fi hotspot. PC users enter login credentials, while for smartphone users do not need to enter this information, as credentials are pre-configured and WISPr takes care of a similar exchange in XML.

However, there are drawbacks to using WISPr. First it is not a tightly-defined protocol, and there are many variants. This is not generally a problem for an operator's smartphones using its own Wi-Fi hotspots, but it may present challenges when roaming to another hotspot network. Second, it is still unusual for smartphones to include a native WISPr client, although several third-party clients, such as the Devicescape Easy-Wi-Fi client (Devicescape, 2009) and the Whisher Wi-Fi.com client, are available and the state-of-the art is evolving swiftly. Third, although credential exchange is protected, subsequent traffic over Wi-Fi is not encrypted, unless the user launches a VPN client on the smartphone or employs a similar end-to-end encryption technique.

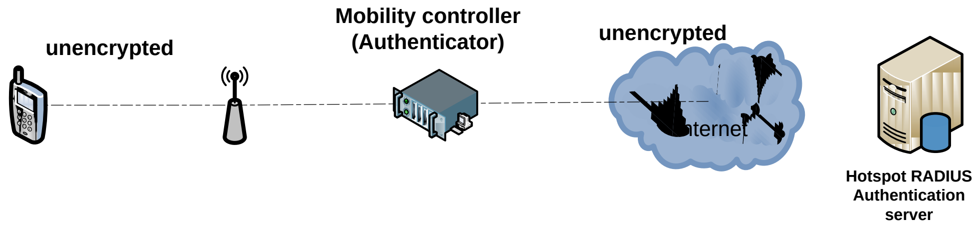


Figure 14. Post-authentication using WISPR

Most operators choosing this option will need to pre-load a WISPr software client on the smartphone, and have the user enter a set of credentials, at least the first time they log onto a hotspot access point. Subsequently the credentials will be cached on the smartphone. (Thornycroft, 2010).

SIM-based WPA-2 authentication

WPA-2 is comprehensive 802.1x-based authentications and encryption protocol, defined at the Wi-Fi layer.WPA2-enterprise networks are extremely secure, but require per user administration and a RADIUS or similar server to store network side user credentials. Most enterprise WLAN networks use WPA-2 authentication.

When used in an operator's Wi-Fi hotspot network802.1X authentication is usually configured to use the Smartphone's SIM credentials. The procedure follows a similar path to WISPr, but uses native 802.11 Wi-Fi frames rather than XML for the authentication protocol.

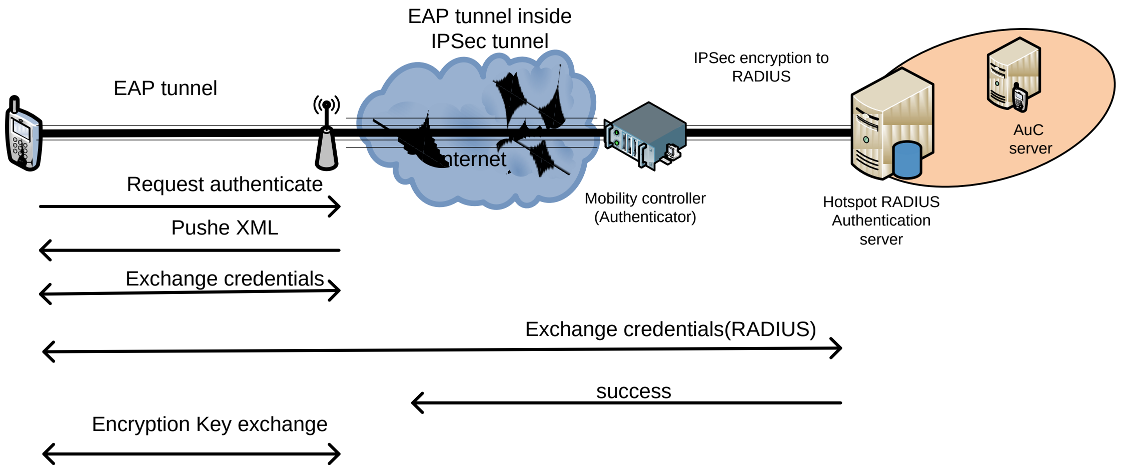


Figure 15. Hotspot authentication using WPA2-enterprise

First, the client authenticates to the access point to initiate a connection. In this pre-authenticated state, it is not allowed to send any type of data except authentication frames. An outer encrypted tunnel is established with the access point, protecting over-the-air transmissions. Next, an inner encrypted tunnel is established with the back-end RADIUS server maintained by the operator. Credentials are exchanged, and on successful completion the access point is informed that it can allow the client onto the network. Finally, a set of session keys is exchanged between the access point and the client, protecting all over-the-air transmissions.

SIM-based authentication main advantage is that, with a RADIUS server fronting the core network AAA server, the credentials on the SIM card can be used for authentication.WPA-2 includes a number of options for ‘inner’ authentication: for an operator’s hotspot network the usual choice would be EAP-SIM, or EAP-AKA. These protocols use SIM/USIM information to identify and authenticate the user removing the need for a separate password for Wi-Fi access, and allowing the 3G operator to maintain a single accounting and policy server for smartphones, whether they access the network over 3G or Wi-Fi.

While SIM-based WPA2 is considered that optimal smartphone authentication method, it is not feasible for PCs, which don’t include SIM cards. Thus the hotspot operator using WPA2 will need to support Web-based authentication in addition, if paid public access is required. Also separate back-end AAA servers and user information will be required.

5.3.2 Services Access Security

One method to service access security is to treat access to operator and 3rd party services over Wi-Fi in a similar way to access to operator and 3rd party services via a PC on the fixed Internet, i.e. username/password based access to a restricted range of services/capabilities. A better approach would be to offer the customer the same experience over Wi-Fi as they obtain via 3GPP access. This would require a more sophisticated solution which leverages SIM card based authentication to provide security for service access. (GSMA, 2010).

5.4 Quality of Service

Earlier wireless standards 802.11a/b/g do not provide any mechanism to guarantee Quality of Service (QoS) in a wireless network. Multimedia applications such as VoIP, IPTV, VoD have different traffic characteristics and QoS requirements as compared to traditional internet data traffic. For example VoD requires high bandwidth while VoIP is bursty in nature and requires low delay and jitter. As a result, to ensure a high level of user experience over Wi-Fi network, these traffic types need to be treated differently from the traditional internet traffic. Further, the available bandwidth in the Wi-Fi is also limited. Therefore it is very vital to manage the access to the Wi-Fi based WLAN resources and priorities the traffic to guarantee appropriate QoS to different kinds of traffic.

IEEE standard 802.11e addresses the link level (between a station and an access point) QoS on Wi-Fi through enhancement to the MAC (Media Access Control) layer protocol. The standard provides two approaches: *Prioritization of Traffic* and *Parameterization of Traffic*. In the traffic prioritization approach, the traffic is classified into one of the four categories - Voice, Video, Best Effort and Background. The transmission is done using Enhanced Distributed Channel Access (EDCA) mechanism. More detail explanation is covered in (California Software Laboratories, 2007). The EDCA parameters for the four categories of traffic are adjusted appropriately to match the requirements of those categories of traffic.

Traffic parameterization approach lets us define traffic streams with appropriate traffic parameter values such as mean and peak bandwidth, burst rate. In this approach, the access point will control the medium and assign transmit opportunities to the station based on the agreed upon traffic specification parameters. As stated on (proxim, 2010) at present most of the QoS solutions for WLAN are based on the traffic prioritization approach.

As mentioned earlier, the QoS capabilities of IEEE 802.11e standard provides QoS on a per-link basis in a Wi-Fi based WLAN. Using this capability existing end-to-end QoS frameworks can be extended to provide quality service to Wi-Fi customers. In general there are two approaches for providing end-to-end QoS - one using differentiated services and the other based on resource reservation. The first approach marks the traffic with appropriate Type of Service (TOS) field based on the category of the traffic. This approach is simple, but does not guarantee QoS. In this paper (California Software Laboratories, 2007), the author outline an approach to extend the reservation based end-to-end QoS to the Wi-Fi based WLAN.

5.5 Integrating Wi-Fi Access into Mobile Core

In many cases an operator is looking to integrate WiFi access as part of mobile core network in order to be able to apply mobile core network functionality into WiFi access as well. Operators have the choice of loosely- or tightly-coupled integration. Loosely coupled means that Wi-Fi network operates largely independently of the cellular network whereas tightly coupled means Wi-Fi is more of a seamless extension of the cellular network and shares some functionality. Such functionality includes charging, secure connections, QoS, policy enforcement, lawful interception, deep packet inspection etc. For example if Wi-Fi access is bundled to mobile subscription, by applying GGSN or PDN-GW functionality to traffic coming via Wi-Fi network, common charging can be applied. Also supporting service continuity (mobility) when device moves between cellular and Wi-Fi networks requires mobile core network involvement.

Currently available solution for integrating WiFi access into mobile core is I-WLAN (WLAN inter-working), as shown in Figure 16.

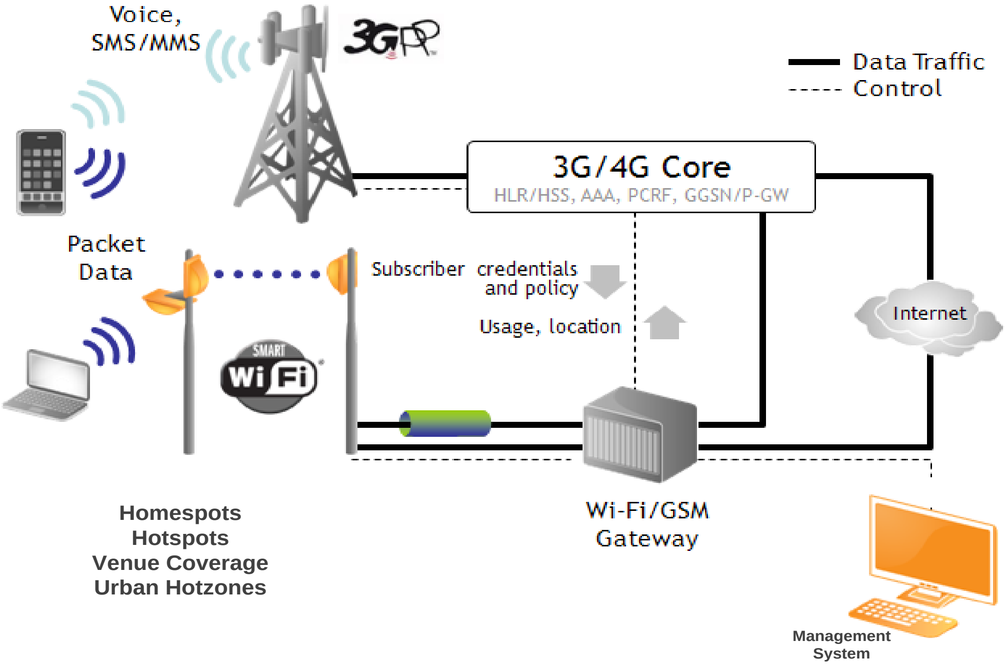


Figure 16. Tightly-coupled Wi-Fi integration (Rysavy, 2010)

I-WLAN can be made available as an integrated solution where I-WLAN PDG functionality consists of (Tunnel Terminating Gateway) TTG and selected GGSN functionalities, like charging, QoS, policy enforcement and lawful interception. I-WLAN can also be made available as a stand-alone solution where I-WLAN TTG functionality mediates traffic between devices and existing GGSNs via Gn interface(see section 6.1.1 for discription), allowing to apply GGSN functionality to traffic coming via Wi-Fi networks. In both cases PDG and TTG functionalities are acting as a gateway towards devices and securing all traffic (IPsec) transferred between device and PDG/TTG over Wi-Fi network. PDG/TTG uses also AAA server for SIM based authentication for the users. Both PDG and TTG allow using mobile network functionality to Wi-Fi access and providing access to operator, 3GPP PS and Internet services via Wi-Fi network.

5.6 Policy and Charging Rule Function (PCRF)

Wi-Fi network is shared among multiple users. Even though Wi-Fi network is able to provide faster connection than 3G networks, this may change when an operator starts offloading traffic to Wi-Fi and more users start using Wi-Fi. In addition to Wi-Fi radio, transport and network elements behind Wi-Fi AP may be exploited and result decrease in end user Quality of Experience (QoE).

PCRF allows ensuring comprehensive end user experience and fair network resource usage when accessing to services via mobile and Wi-Fi networks. PCRF contains subscriber specific QoS policies that help networks to treat traffic related to different users fairly and ensure QoE for important users/services during e.g. busy hour. PCRF distributes the policies to GGSN, P-GW/HA, and PDG handling user traffic. PCRF is also involved in unifying charging policies when accessing to services via cellular and Wi-Fi networks.

6. ANVIA WLAN CELLULAR INTEGRATION FRAMEWORK

This chapter of the thesis contain confidential information and removed .

7. CONCLUSION AND FUTURE WORK

In recent months many mobile operators have been caught by surprise by the unprecedented rise in data traffic generated by smartphone users, particularly with the new generation of 'smartphones' which offer fascinating experiences for streaming video, Web browsing, social networking and other high-bit-rate traffic. The wireless way to access Internet is starting to be more a norm than exception and continues to climb up with yearly growth rate being over 100%. Mobile growth starts to alarm network engineers. Those not already experiencing congestion recognize that it is a matter of time.

This situation has caused on an exploration for remedies. Most operators recognize new 3G capacity cannot be added quickly enough; given the shortage of spectrum, tower sites backhaul capacity and reliable revenue to support the heavy investment. And even though new radio technologies such as HSPA+ and LTE offer more over-the-air capacity, they will not be able to satisfy demand if it continues on its present trajectory. The solution must be pursued elsewhere, in moving high-volume traffic off the mobile network wherever possible: the only two suitable technologies are Wi-Fi and femtocell.

While femtocells will undoubtedly find a place, they have not yet progressed much beyond the trial stage due to difficult technical problems involving the integration of radio and control functions with the existing network, and an as-yet unproven business case. In contrast, Wi-Fi access points are widespread and inexpensive, there is one global, interoperable standard, and every new smartphone includes a Wi-Fi interface.

As discussed in this thesis is Wi-Fi offload is a 'WIN-WIN-WIN' strategy. Mobile can save 20 to 25 percent per annum and generate additional revenue. Customer will experience high data rates and ubiquitous experience. Wireless service providers enter to new business model to share mobile broadband market.

Deploying Wi-Fi for commercial networks poses many challenges and need a thoughtful consideration. Challenges include interference mitigation, coverage and capacity in complex environments, security and fraud, seamless authentication.

However, these are no longer a sit back as they are addressed with different techniques and new standards in IEEE 802.11. Some of the capabilities are advanced radio technology and interference rejection techniques, comprehensive end-to-end management, higher speed and lower cost long-range 802.11n backhaul links.

The availability of an automatic client in end user device has resulted in tremendous increase in utilization of Wi-Fi hotspots in offloading of the 3G data. It is therefore desirable that more work be done on the standardization and optimization of such clients to promote their acceptance and use across all 3G and LTE dual mode devices.

To protect user from eavesdropping of the wireless traffic between the customer's client device and the Wi-Fi access point, it is recommended that the access points support SSID that has encryption using WPA2 compliant with IEEE 802.11i .QoS can be ensure to different kinds of traffic by prioritization and parameterization traffic.

Finally, we offer a Wi-Fi architecture that is compliant with the 3GPP I-WLAN framework. The proposed architecture allows a single access point to be the point of delivery for multiple services including secure inside-the-firewall access from public hotspots.

In this thesis much of the conclusion about mobile data growth and impact is taken from global point of view. It was hard to find research done on the trend of mobile internet in Finland .We believe ,such study are necessary for service providers to make the right decision at the right time about their broadband business strategies .We understand the necessity of such studies and it will be our next task.

REFERENCES

ABI (2009). ABI Research press release .Singapore.March 10, 2009.

Akyildiz I.F (2004). *Survey of Mobility Management in next-generation all-IP-based wireless systems*. IEEE Wireless Communications, August 2004.

Accuris networks. (2010). *The Business value of Mobile Data Offload*. Accuris Network *whitepaper*.

Altai. (2010). [online] Available: . < http://www.altaitechnologies.com/tech_wifi_cellular.php >

Ang, J. (2010). *Operators Can Save $14 Million Yearly*. [online] Available <http://www.broadbandworldforum.com/manual/platinum_level/greenpacket_bbwf2010/workspace/Operators_Save_$14M_Yearly_Through_Data_Offloading.pdf >

BelAir (2009). *Alleviating Data Congestion in Mobile Networks.* BelAir Network white paper. 2009.

California Software Laboratories. (2007). *Extending End-to-End QoS to WiFi based WLAN*.[online] Available: < http://www.calsoftlabs.com/downloads/W_qos-wireless-lan.pdf>.

Chowdhury, A. s. (2010). *The Next Generation Mobile Wireless Hybrid Network Interworking Architecture*. Masters thesis. March 2010.RMIT UNIVERSITY.

Cisco (2011). *Global Mobile Data Traffic Forecast Update*, 2010-2015. [online] Available:<http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf>.

Devicescape. (2009). *Easy Wi-Fi*. Devicescape Software Inc.

EIAA (2011). *European Mobile Internet Use*. [online] Available: <URL:http://www.eiaa.net/Ftp/casestudiesppt/EIAA_Mobile_Internet_Use_Executive_Summary.pdf >.

FemtoForum (2010) .Femto Forum [Online] <http://www.femtoforum.org/femto/>

Fierce broadband wireless. (2010). [online] Available <http://www. fiercebroadbandwireless.com/special-reports/wi-fi-offload-mobile-networks-20-traffic-and-counting >

Forseel, M. (2010). *Smart WLAN Connectivity*. Techinical Solution Description Customer. Nokia Siemens Networks.

Garg, V. (2010). *Interworking between WLANs and 3G - Part 1: Interworking objectives & approaches*. [Online] Available: http://www.eetimes.com/design/ embedded-internet-design/4210252/ Interworking-between-WLANs-and-3G---Part-1--Introduction--interworking-objectivesapproaches?pageNumber=3& Ecosystem=microcontroller-mcu

GSMA (2010), Wi-Fi offload.GSMA Whitepaper .[online]. Available: <http://www.gsmworld.com/newsroom/document/library/alldocuments.html >

Ghosal Anjan (2010). *Mobile Data offload: Can Wi-Fi Deliver?*. January 2010.[online] Available:<http://www.intellinettech.com/Media/PagePDF/Mobile%20Data%20Offload%20-%20Can%20Wi-Fi%20Deliver.pdf>.

Informa (2010). *Mobile Internet Traffic: Analysing Global Usage Trends*.[online] Available: < http://media2.telecoms.com/downloads/mobileinternet-traffic trends.pdf >

Intellinet (2010). *The Business Case for Mobile Data Offload*. Intellinet Technology white paper. January 2010.[online] Available: < http://www.intellinet-tech.com/Media/PagePDF/Data%20Offload%20Business%20Case.pdf >

Khan, M. F. (2010). *Femtocellular Aspects on UMTS Architecture.* Msc Thesis, Aalto University, Department of Communications and Networking, Espoo.

Luna, L. (2010, march). *What's really causing the capacity crunch?* [online] Available < http://www.fiercewireless.com/nextgenspotlight/story/whats-really-causing-capacity-crunch >

Leu J. (2005). *Practical Considerations on End-to-End Cellular/PWLAN Architecture in support of Bilateral Roaming.* Wireless Communication and Networking Conference, IEEE 2005, vol. 3, pp. 1702-1707.

Lee Kyunghan, Rhee Injong, Lee Joohyun, chong Song (2010). *Mobile Data Offloading: How Much Can Wi-Fi Deliver?* SIGCOMM 10th ,2010 , New Delhi, India.

Li Ma, FeiYu and V.C.M. Leung (2004). *A new method to support UMTS/WLAN Vertical Handover using SCTP.* IEEE Wireless Communications. August 2004.

Mölleryd B., Markendahl J., Werding J. & Mäkitalo Ö. (2010). *Decoupling of revenues and traffic - Is there a revenue gap for mobile broadband,* IEEE, Telecommunications Internet and Media Techno Economics (CTTE) 9th conference, October 2010,pp. 1

Nokia Siemens Networks (2010). *Mobile Broadband with HSPA and LTE – capacity and cost aspects*. Nokia Siemens Networks White paper, 2010 .

Perkins, C.E. (1997). *Mobile IP*.IEEE Communications Magazine, 1997, vol. 35, issue 5, p.84-99.

Proxim (2010). *Mobile Data offloading through Wi-Fi*. Proxim wireless white paper , 2010.

Rahman, E., & Jaffar, J. (2006). *Investigation of WLAN-Cellular Integration Architecture for Cellular Operators and Deployment Issues at King Fahd International Airport.* Senior Design Project, King Fahd University of Petroleum and Minerals.

Antti, L. & Risto, S. (2010). *uAxes offloading : Rethinking the Problem*. Notava *whitepaper*. [online] Available< http://www.notava.com/notava/uploads/ Whitepapers/Rethinking_the_problem_V10pdf >.

Rysavy. (2010, october 14). Strategic use of Wi-Fi in Mobile Broadband Networks. Rysavy reasearch. [online] Available < http://www.rysavy.com/Articles/ 2010_10_Strategic_Wi-Fi.pdf>

Salkintzis, A., & Passa, N. (2004). *A New Approach for Fast handovers in Mobile Multimedia Networks*. Vehicular technology Conference, pp. 2972-2976.

Schmidt, A. L. (2004). *UMTS and WLAN interoperability*. M*aster's theisi*. Technical University of Denmark. [online] Available<http://oldwww.com.dtu.dk/ research/networks/OPNET/UMTS%20and%20WLAN%20interoperability.pdf

Salkintzis A (2004). *WLAN/3G Interworking Architectures for Next Generation Hybrid Data Networks* . IEEE International Conference on Communications 2004, vol. 7, pp. 3984-3988

Thornycroft, P. (2010*). 3G Data offload strategies and Architectures for Mobile Operators.* Aruba Networks white Paper.

Tsao, Shiao-Li,Chia-Ching Lin (2002). *Design and evaluation of UMTSWLAN interworking strategies*. Vehicular Technology Conference, 2002. Proceedings VTC 2002-Fall. 2002 IEEE 56th , Volume: 2, Pages:777 – 781, 24-28 Sept. 2002.

TS 23.234 (2005). *3G System to WLAN Interworking*; System Description (Release 6), Sept. 2005.

TS 22.220 3GPP.Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB); Release 9, TS 22.220; <http://www.3gpp.org/>.

TS 25.4673 GPP, Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home Node B (HNB); Stage 2, Release 8 and Release 9, TS 25.467; <http://www.3gpp.org/>.

Wiederkehr, P. (2009). *Approaches for Simplified Hotspot Logins with Wi-Fi Devices*. Master Thesis. Swiss Federal Institute of Technology Zürich . [online] Available < http://e-collection.library.ethz.ch/eserv/eth:208/eth-208-01.pdf>.

Wu W., N. Banerjee, K. Basu and S. K. Das (2005). *SIP-based Vertical Handoff between WWANs and WLANs*", IEEE Wireless Communications, June 2005.

Appendixes

Appendix1. Wi-Fi standards

802.11n

This is an amendment to increase the maximum data rate from 54 Mbps to a maximum of up to 600 Mbps with the use of MIMO (multiple input multiple output) antenna and spatial multiplexing technologies where multiple independent data streams are simultaneously transmitted within the same spectral channel. It also includes a wider (40 MHz) channel and provides significant improvements (frame aggregation) to the Media Access Control layer (MAC) which makes the usage of the shared wireless channel more efficient.

802.11u

This amendment to 802.11 provides additional information over the air about a Wi-Fi network allowing the network selection to be made on the basis of network characteristics and service offerings such as the service operator identity, QoS, charging structure, supported services, etc.

802.11r

This amendment to 802.11 provides for fast and secure inter-access point handoff by cashing part of the encryption key to speed up the authentication process, thus allowing service continuity while the wireless device moves between access points.

802.21

This standard provides for seamless handover between different types of base stations or access points such as between Wi-Fi, Bluetooth, GSM, UMTS, and WiMAX systems.

802.11e

This is a QOS amendment to ensure the quality of the link between the client and the Wi-Fi access point.

802.11i

This is a security standard that addresses some of the problems in the original WEP-based encryption system of Wi-Fi. It is a standard to secure and encrypt the wireless link between the client and the Wi-Fi access point.

802.1X

This protocol provides for an access point to act as an authenticator by allowing a device, termed a supplicant, to present its credentials to the access point and for the access point to pass these credentials to an authenticating server for verification. Upon approval, the access point will then allow the supplicant access to the network hence acting as a gate keeper barring unauthorized access to the network.