TELECOMMUNICATION ENGINEERING CENTRE
दूरसंचार अभियांत्रिक केन्द्र
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
DEPARTMENT OF TELECOMMUNICATIONS
दूरसंचार विभाग
GOVERNMENT OF INDIA
भारत सरकार
सत्यमेव जयते
ISO 9001:2008

Mobile Data Offload-Wi-Fi Offload

Radio Division

1 Introduction

With the advent of smart phones and other similar smart devices which dominate the market, the mobile networks are chiefly dominated by data. The user demand for data is increasing rapidly and reaching to the order of exabytes (1 billion gigabytes). This has led to a paradigm shift in the network planning of the mobile network operators who are now focusing on devising effective and economical ways to cater to the growing user demand. The network operators plan on offloading the data and associated signaling traffic to a cheaper solution to improve their economics. The change in approach is also fuelled by the fact that the further technological developments and enhancements in cellular architecture are bound by physical limitations. Also, to cater to high bandwidth and high speed data, huge capital investments are required which are not economically viable. This has forced the operators to explore alternatives using small cell technologies like Wi-Fi, Femtocells etc. to efficiently handle the growing mobile data traffic. In this paper, we primarily focus on Mobile data offload through Wi-Fi, popularly referred as Wi-Fi offload.

Though the cellular and Wi-Fi radio technologies originated and evolved from two fundamentally different objectives, each has trended towards the other, with wireless data a central use of cellular technology today while over-the-top services provide voice over data networks. This confluence seems headed towards an integrated cellular and Wi-Fi landscape, but the evolutionary nature of the trend has resulted in a broad variety of approaches and solutions. There has been a great deal of interest of late in using Wi-Fi to offload traffic from heavily congested mobile networks. Early deployments consisted of building a parallel Wi-Fi offload network that takes traffic directly to the Internet. The mobile network operator would implement some kind of proprietary client that would manage the offload function. Many subscribers have implemented their own offload strategy by selecting Wi-Fi when it’s available. Now, the industry is shifting its focus toward integrating Wi-Fi RANs into the mobile packet core. In this approach, Wi-Fi would take its place alongside 3G/LTE as a cornerstone technology in the mobile world. The mobile device selects the best radio access technology based on the conditions (typically signal strength, application type, default to Wi-Fi, etc.) and the subscriber is automatically authenticated and connected. All RAN traffic is brought back into the mobile packet core as defined in the 3GPP evolved packet core standards. The subsequent sections explain the different solutions for Wi-Fi offload and other aspects pertaining to it.

2 Roadmap to Cellular/Wi-Fi Integration

Cellular and Wi-Fi radio technologies originated from two distinct goals. While the cellular technology was motivated by the desire to make telephony technology mobile, on the other hand, the Wi-Fi technology aimed at making data communications wireless. Each technology had its own growth and development path until the need for their convergence mainly triggered by user demand was felt by both the Cellular and Wi-Fi community. This led to extensive standardization work to integrate cellular and Wi-Fi technologies. Figure 1 below depicts the development and convergence roadmap leading to cellular/Wi-Fi integration.

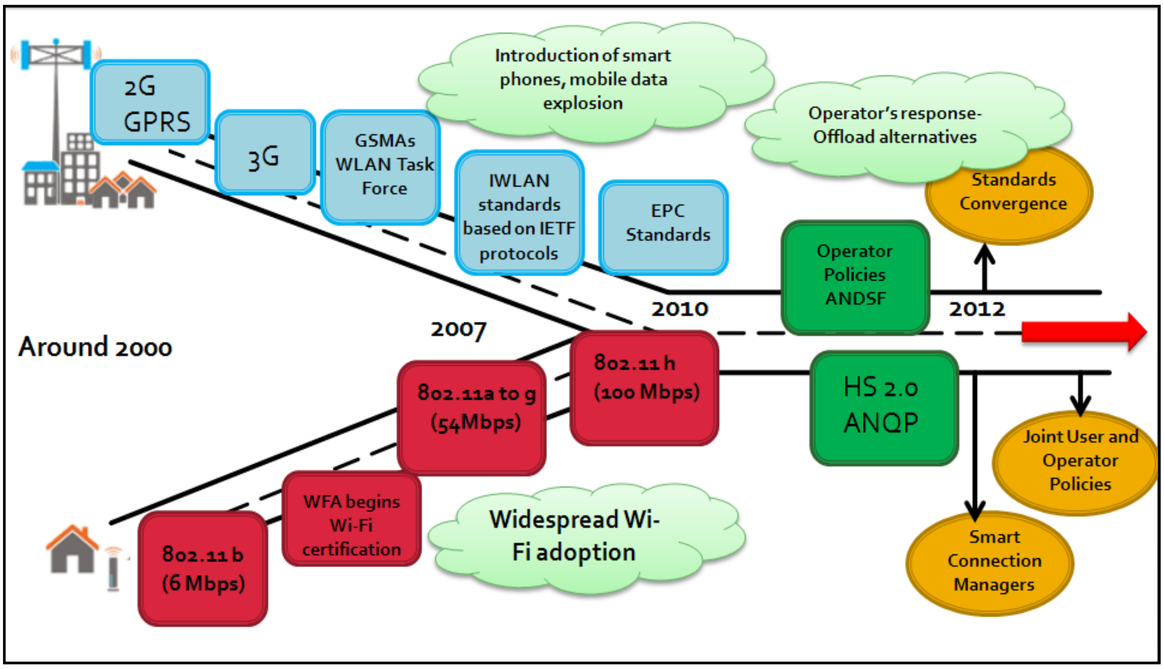
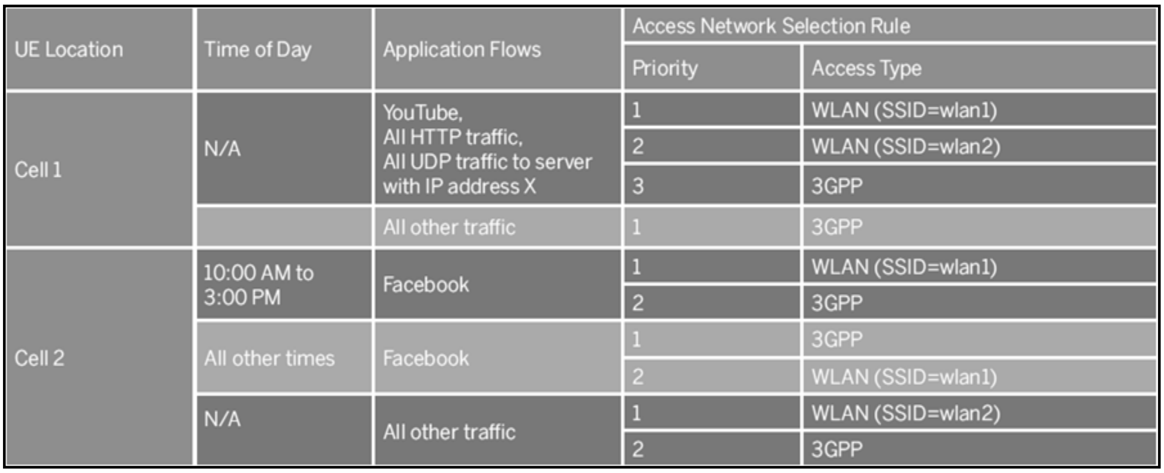

Introduction of smart phones, mobile data explosion
Operator's response- Offload alternatives
2G GPRS
3G
GSMAs WLAN Task Force
IWLAN standards based on IETF protocols
EPC Standards
Standards Convergence
Operator Policies ANDSF
2010
2012
2007
Around 2000
802.11a to g (54Mbps)
802.11 h (100 Mbps)
HS 2.0 ANQP
Joint User and Operator Policies
WFA begins Wi-Fi certification
Widespread Wi-Fi adoption
802.11 b (6 Mbps)
Smart Connection Managers

Figure 1 Cellular Wi-Fi Integration

3 Definition of Wi-Fi Offload

Mobile data offload through Wi-Fi or Wi-Fi offload is one of the implementations of using small cell technologies like Wi-Fi to provide data services to cellular users in a more efficient and economically viable manner. Other small cell technologies like Femtocells etc. may also be employed for the same but Wi-Fi is garnering more attention from the cellular industry to cater to the rising data demand of the users. Smart devices today, are so designed that they prompt the user to log on to Wi-Fi networks for data transfer when one is in range as compared to cellular networks. But this kind of implementation is a very primitive one and is dependent on the user's choice to opt for Wi-Fi network or not. The standardization bodies like IETF, 3GPP, ITU etc. however, have been working to develop specifications for the implementation where the offload from cellular to Wi-Fi networks is more network-driven than user-driven. A typical implementation of Wi-Fi offload indicating selection and prioritization of different types of traffic between Wi-Fi and cellular network is depicted in Figure 2 below.



UE Location	Time of Day	Application Flows	Access Network Selection Rule	
			Priority	Access Type
Cell 1	N/A	YouTube, All HTTP traffic, All UDP traffic to server with IP address X	1	WLAN (SSID=wlan1)
			2	WLAN (SSID=wlan2)
			3	3GPP
		All other traffic	1	3GPP
Cell 2	10:00 AM to 3:00 PM	Facebook	1	WLAN (SSID=wlan1)
			2	3GPP
	All other times	Facebook	1	3GPP
			2	WLAN (SSID=wlan1)
	N/A	All other traffic	1	WLAN (SSID=wlan2)
			2	3GPP

Figure 2 Typical implementation of Wi-Fi Offload

4 Need for Wi-Fi Offload

The following points justify the need for Wi-Fi offload and also build up a business case for the cellular operators to adopt the same:

- It will cater to the growing mobile data demand and the smart devices usage patterns that have the characteristics of short sessions, high throughput and low latency.
- It will enhance the end user experience by improving service capacity and capability. Also the end user devices are so designed that they perform with better data speeds in Wi-Fi networks and so Wi-Fi has an edge over cellular network in this case as well.
- Using a solution which is more economically viable for providing indoor services will reduce the operating expenditure of the service providers as cellular broadband is more expensive than Wi-Fi.
- Address the issue of spectrum crunch whereby the cellular operators can provide high bandwidth consuming services through Wi-Fi.

5 Key aspects for implementation of Wi-Fi offload

For the effective implementation of offloading traffic from cellular networks to Wi-Fi networks, the following aspects need to be addressed:

5.1 Increasing the Wi-Fi footprint to implement offloading solutions

The cellular operators have the option to have agreements with existing wireless internet service providers or to have their own infrastructure to provide traffic offloading. It is up to the operator to choose any of the option that best fits its business scenario. The main intention is to increase the ubiquity of Wi-Fi networks so that they are readily available for offloading mobile data traffic.

5.2 User equipment challenges and enhancements

Wi-Fi offload in true sense requires minimal or no user interaction with the network to initiate offload. Also the seamlessness of the offloading is crucial for satisfying user experience. This requires provision of smart connection manager at the user equipment end which can directly interact with the network and effect offload according to flexible and efficient policies. The connection manager should be able to make decisions regarding network selection, volume of traffic data to be offloaded, application or service specific offload, time-based offload management etc.

5.3 User authentication and interaction with cellular core network entities for policy implementation and charging

Wi-Fi and cellular networks have different mechanisms for authentication and so requirement is to have an authentication mechanism which is acceptable for both the networks. Techniques like SIM based authentication for Wi-Fi networks are gaining ground. Also, till now there have been proprietary implementations of how policy and charging rules are applied in offload scenarios. Standards have been developed for the policy and charging rules applicable in offload scenarios and are being enhanced. ANDSF (Access Network Discovery and Selection Function) and PCRF (Policy & Charging Rules Function) servers' specifications developed by 3GPP cater to this functionality.

5.4 Seamless inter-network mobility considerations

Wi-Fi was mainly developed for local area networks and hence lacked any mobility functionalities but as cellular/Wi-Fi integration gained momentum, the aspect of seamless mobility, while the user moves from network to network was seriously considered. IETF (Internet Engineering Task Force) came up with the specifications for MIP (Mobile Internet Protocol) and PMIP (Proxy Mobile Internet Protocol) to address the mobility issues in Wi-Fi.

The aspects discussed above, though not exhaustive but cover the crucial points that need to be considered for effective mobile data offloading through Wi-Fi.

6 Wi-Fi Offload for different cellular architectures

The standardization in the field of cellular/Wi-Fi integration started as early as 2002 when GSMA formed the 'WLAN Interworking Task Force' group to study the possible interworking and integration scenarios for cellular and Wi-Fi technologies. This resulted in 3GPP formulating a number of specifications for cellular/Wi-Fi integration. These specifications can be seen as divided into two groups depending on the mobile core network they pertain to, viz.UMTS (Universal Mobile Telecommunication System) or EPC (Evolved Packet Core)..

The standards dealing with UMTS core network are referred as IWLAN (Integrated/Interworked WLAN) standards and the latter as EPC standards for non-3GPP access. In this section, we discuss in detail these two set of standards and how they are applied on the UMTS and EPC core networks.

6.1 Wi-Fi offload for UMTS core network (IWLAN standards)

Data traffic offload in UMTS core network using Wi-Fi are based on the IWLAN standards. These standards cover the aspects of Common Billing and Customer Care, 3GPP system based Access Control and Charging, Access to 3GPP system PS based services, Service Continuity, Seamless services and Access to 3GPP CS Services. These scenarios were covered under 3GPP TR 22.934 and based on these; various 3GPP TS were released to define the specifications for each scenario.

A simplified representation of UMTS core network architecture incorporating IWLAN is depicted in Figure 3 below.

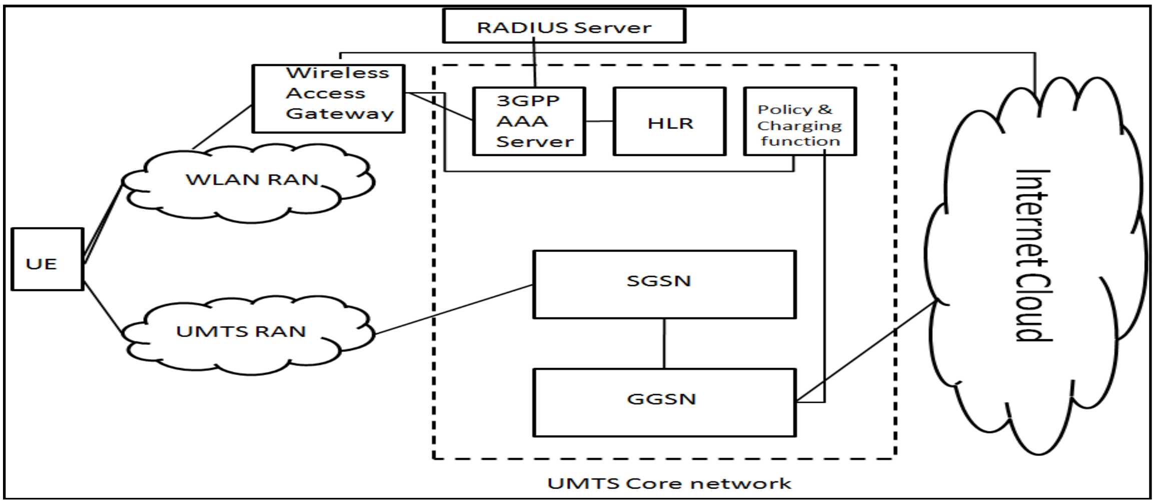


Figure 3 UMTS core architecture supporting IWLAN

Figure 3 describes how the User equipment can be connected through the WLAN RAN or UMTS RAN and then be authenticated by the 3GPP core network and then finally connected to provide services. The details of authentication, mobility and seamless services etc. are described further.

One of the main goals of the IWLAN solutions was to achieve authentication without manual user intervention, such as entering a username-password, as is common is many Wi-Fi networks. This is made possible by developing authentication protocols based on the use of SIM cards, which are already provisioned in the 3GPP handsets. In addition to providing authentication in a manner transparent to the user, SIM based authentication methods are also familiar to 3GPP based network operators and provide the same level of security as 3GPP devices. Since the SIM based authentication is now done via WLAN networks, which are essentially IP Networks, the basic 3GPP authentication protocols are modified and are known as EAP-SIM (Extensible Authentication Protocol-SIM), EAP-AKA (Extensible Authentication Protocol-Also Known As) and EAP-AKA' protocols, which were standardized by the IETF. A typical flow of the EAP authentication is depicted in Figure 4 below.

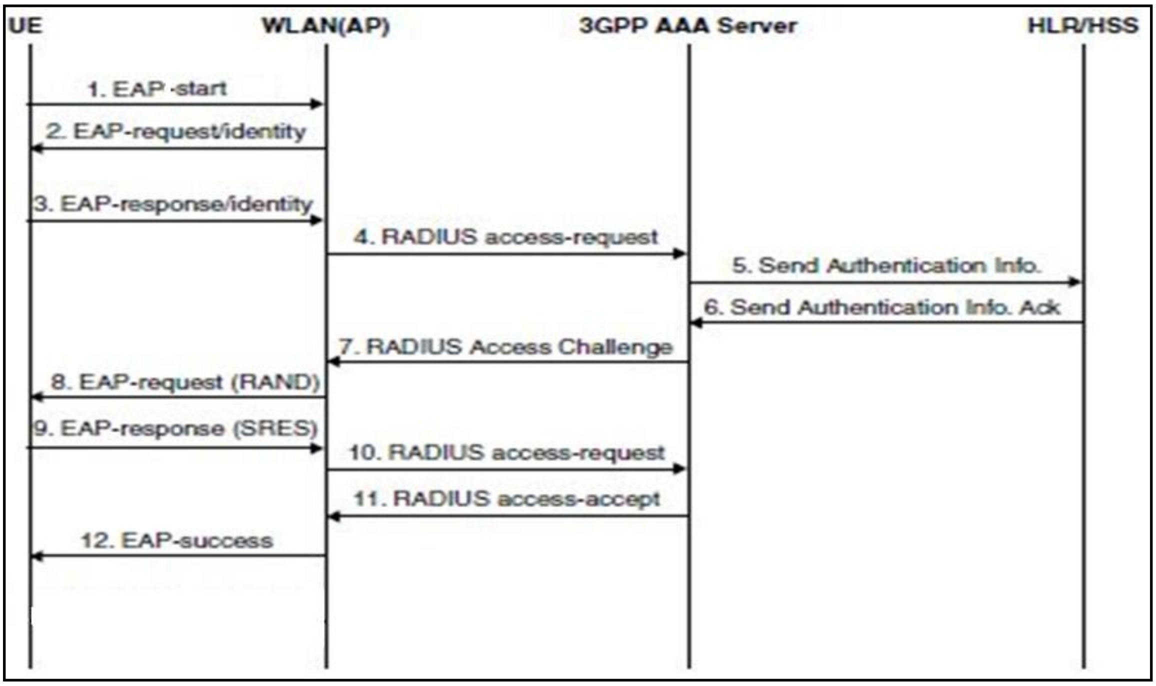


Figure 4 A typical EAP authentication message flow

Another important aspect of effective implementation of offloading was mobility management to provide seamless mobility between cellular RAN to Wi-Fi RAN as well as between inter-operator Wi-Fi RANs to the user. The mobility function is essentially based on an IP-level mobility management protocol called DSMIPv6, which is standardized by IETF. This protocol is implemented in an entity called HA (Home Agent) in the core network of the home 3GPP network and in a peer entity called DSMIPv6 client in the UE. The UE has a single IP address (for the purposes of mobility management), which is called Home Address (HoA) and a Care-of-Address (CoA) which changes as the UE attachment is changed between IWLAN and 3GPP radio interfaces. Changes in CoA address are synchronized between the UE and the HA by exchanging the so-called "Binding Updates" messages. These are sent over the logical interface H1 shown in Figure 5.

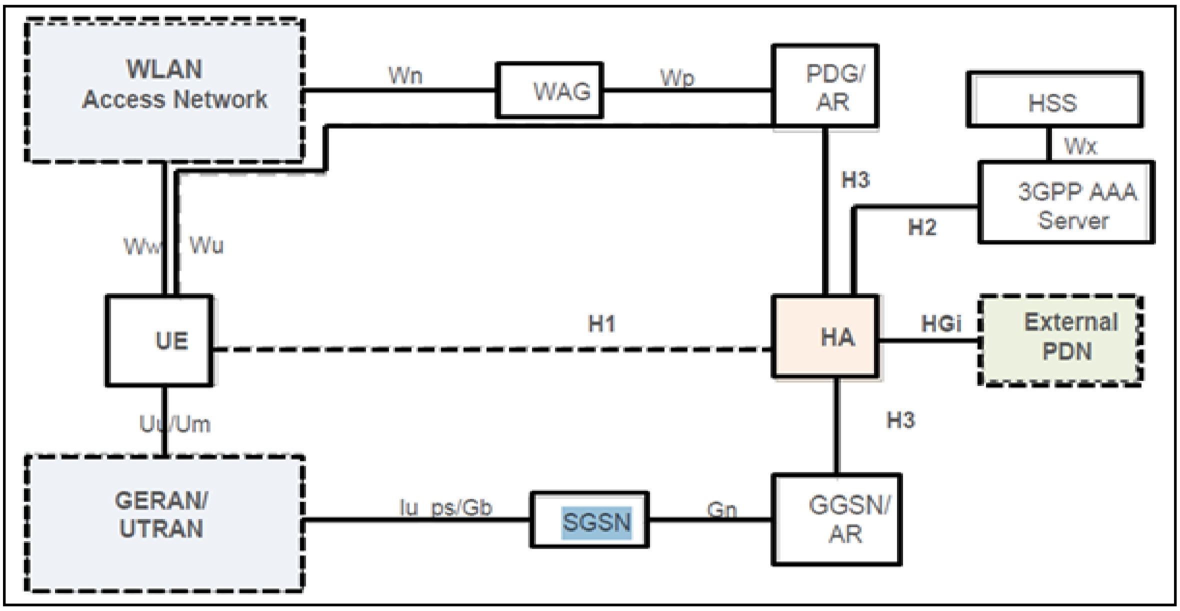


Figure 5 IWLAN architecture for Seamless mobility

DSMIPv6 mobility protocols allow handover from 3GPP access to WLAN access or vice versa. However, in the current version of the standards, only the UE can initiate such a handover procedure. This is based partly on the rationale that the UE has a better knowledge of the WLAN radio networks. However, there are some initiatives in the 3GPP standards organization currently that are seeking to standardize network-initiated handovers as well, since the network has a more comprehensive knowledge of the network congestion state. Although the HA function is shown as a separate function in the above figure, it is often collocated with the GGSN.

Main drawbacks of the IWLAN standards based offloading architecture: - The first limitation is that the HA is not connected to policy and QoS management entities in the core network, such as PCRF. This prevents advanced policy and QoS based management of the IWLAN-3GPP mobility.

The second limitation is that the above solution restricts the UE to have only a single radio connection at any given time, namely either to the WLAN or 3GPP radio interface. Modern smart phones allow simultaneous connectivity to both radio interfaces, which raises the possibility of managing 3GPP and WLAN interworking at an individual IP-Flow level. That is, it should be possible to support certain IP-Flows on the 3GPP radio interface and certain others on the WLAN radio interface, based on criteria such as QoS requirements, user subscription, type of user equipment, etc. Furthermore, it could also enable dynamic switching of individual IP-Flows from one radio interface to another.

These drawbacks were addressed in the EPC standards for non-3GPP access which will be discussed in Section 6.2.

6.2 Wi-Fi Offload for Evolved Packet Core network (EPC standards for non-3GPP access)

The offloading concepts defined by IWLAN standards were mainly based on loose interworking. The EPC standards for non-3GPP access aim to provide higher level of integration between the WLAN and cellular technologies ensuring tighter interworking. The WLAN access or non-3GPP access as it is referred to, proposed by IWLAN standards was mainly untrusted IP access as the WLAN operator and cellular operator could be different and the level of trust between them could be dependent upon the level of agreements and co-operation. The EPC standards however ushered the era of trusted non-3GPP access as they provided high level of integration between WLAN and cellular architectures and were mainly developed with the view that the cellular operator will also own the WLAN network. A typical implementation of EPC architecture for trusted non-3GPP IP access is depicted in Figure 6 below.

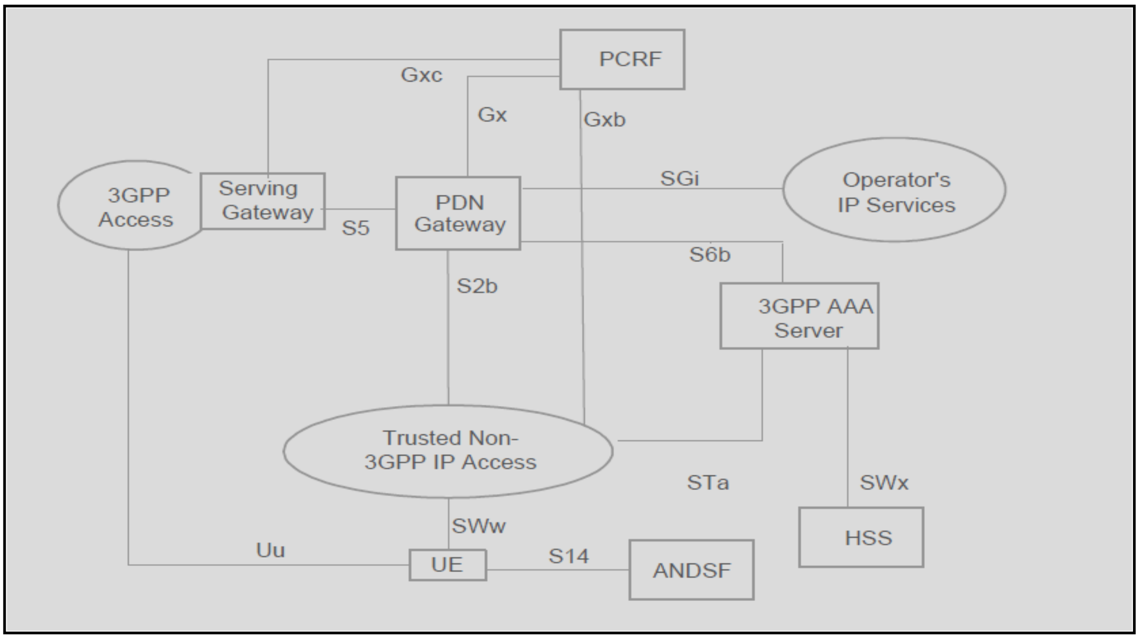


Figure 6 EPC architecture for trusted Non-3GPP access

In the EPC architecture diagram described above, in addition to the functionalities described in the IWLAN standards, enhancements were added like the PGW(Packet Data Network Gateway) includes a HA functionality and that PCRF (Policy & Charging Rule Function) is connected to various gateway functions, each of which has a PCRF or its functional equivalent to enforce the operator policies.

Shown also is the ANDSF functionality, which is critical for Cellular-Wi-Fi interworking from an operator policy point of view. Currently, most smart phones choose and camp on to Wi-Fi networks based on explicit user preferences or preconfigured preferences, already stored in the UE. It was clear that if operators were to offer Wi-Fi access as an integral part of the access offerings, they needed to be able to install operator policies on the UE and also be able to change them dynamically, as the conditions may change. To achieve this, the framework of ANDSF was standardized. It essentially consists of an ANDSF server in the operator network, which stores the operator policies regarding discovery and selection of Wi-Fi access. For example, it contains discovery information of Wi-Fi hotspots based on the location of a UE. Regarding selection of Wi-Fi Hotspots, the policies may specify that certain Wi-Fi hotspots are preferred at certain locations and/or certain times of day, or for certain types of applications, such as mobile video etc. These operator policies can be transferred to the UE via the S14 interface using communication procedures based on device management procedures, originally developed by the OMA organization.

Interworking between 3GPP and non-3GPP networks essentially consists of mobility of IP-Flows between the 3GPP and non-3GPP networks. The EPC standards for non-3GPP access provides for the possibility of managing 3GPP and WLAN interworking at an individual IP-Flow level. That is, it should be possible to support certain IP-Flows on the 3GPP radio interface and certain others on the WLAN radio interface, based on criteria such as QoS requirements, user subscription, type of user equipment, etc. Furthermore, it could also enable dynamic switching of individual IP-Flows from one radio interface to another. This is depicted in Figure 7.

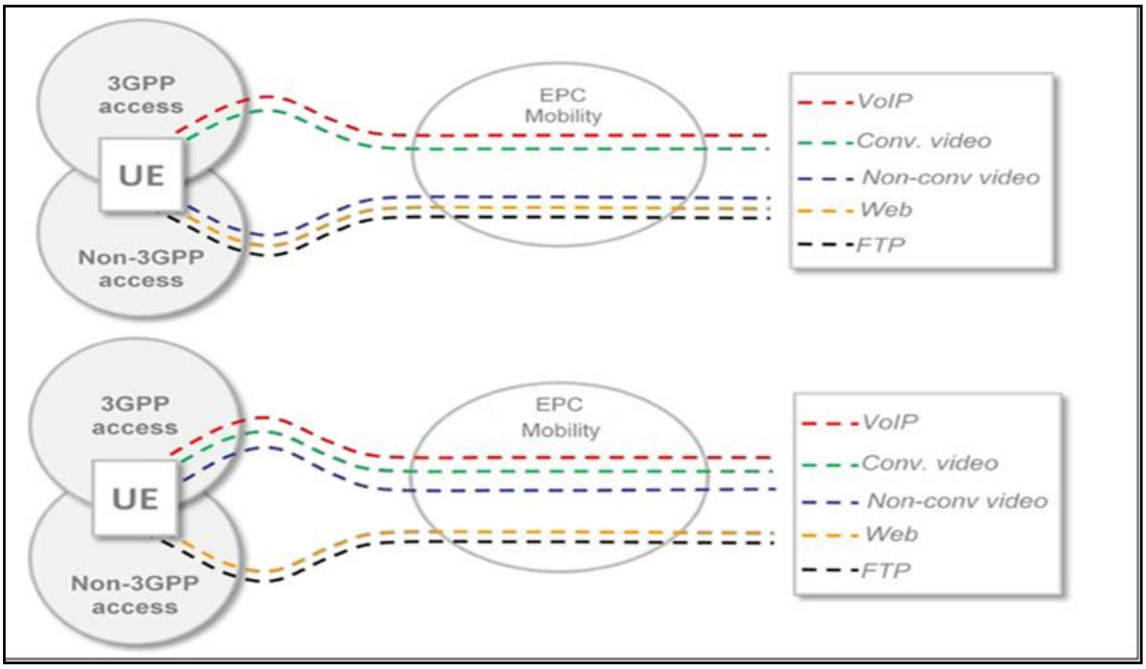


Figure 7 Dynamically moving IP flows between 3GPP and non-3GPP accesses

A number of cases of such mobility can be distinguished depending on the following aspects: (1) mobility is on a per IP-Flow basis or per all IP-Flows associated with a PDN connection; (2) mobility is Seamless or Non-Seamless. Seamlessness is defined as preservation of the IP-address of the UE during the mobility process. Different combinations of these two fundamental aspects result in a number of scenarios, such as Wi-Fi offload, referring to mobility of IP-Flow(s) from 3GPP to Wi-Fi networks, and handovers, referring to mobility of all IP-Flows associated with a PDN connection etc.

The 3GPP standard TS 23.401 describes Seamless and Non-Seamless Handover solutions between 3GPP and Non-3GPP access networks, wherein GTP is used as the protocol for the Handover over the interfaces S2a, S2b and S5. Similarly, TS 23.402 documents similar solutions for the cases where PMIP and DSMIP are used for mobility. Finally, TS 23.261 describes the solutions for Seamless IP-Flow Mobility using DSMIP protocols. This allows for selective assignment of different IP-Flows to different access networks and includes Seamless Wi-Fi Offload as a special case.

In all cases listed above, the mobility is triggered by the UE and not by the network. Efforts are also being made to standardize network-triggered mobility procedures, since the network is often more knowledgeable about the overall network usage and congestion state than the UE.

7 Other offload technologies

At a high level, Cellular Wi-Fi Integration may be seen as a technique for managing data traffic in a mobile operator networks in a smart manner. For example, the traffic would be dynamically routed to use the optimal radio interface to suit the particular application and user at hand, taking into account also connectivity cost, reliability security, network congestion etc.

In such a perspective, cellular/Wi-Fi integration is but one technique of such intelligent traffic management, which may be referred to as Radio Interface Offloading. The other technique would be Network Offloading, referring to intelligent routing of traffic within the backend networks. The problem addressed by IP offload is that by default all IP traffic generated by a mobile device (or sent to a mobile device) is routed to and through the mobile core network. There are good reasons for this: i) it is necessary to ensure full mobility support; ii) it allows the operator to manage both the user's QoE and how its network is used; iii) it is necessary to access operator service. However, there may be certain drawbacks in such routing for certain types of traffic. For example, local traffic (i.e. traffic destined to local IP networks) and traffic from public internet (e.g. YouTube traffic, as opposed to Operator service traffic) need not traverse the operator core network. In fact, such routing may introduce additional latencies to local traffic, affecting the user experience. For internet traffic, such routing would unnecessarily load the operator network, which can be avoided. SIPTO and LIPA are two solutions that 3GPP is standardizing for these problems.

The first of these solutions is Selected IP Traffic Offload (SIPTO). Based on network-specified policies, SIPTO supports offload of IP traffic directly to the internet and away from the mobile core network. The upside to the operator is lower load on its network, however there is a significant price to pay – mobility support for SIPTO traffic can be rather limited, and offloaded traffic cannot access operator services. Thus, the operator must be careful in selecting which traffic to offload. For example, offloading a web browsing session is generally considered safe. Any interruptions due to mobility will often go unnoticed because the duty cycle of activity for web browsing is usually low and HTTP initiates a new session for each search. On the other hand, voice call, even when handled as VoIP, should generally be routed through the core network to provide seamless mobility.

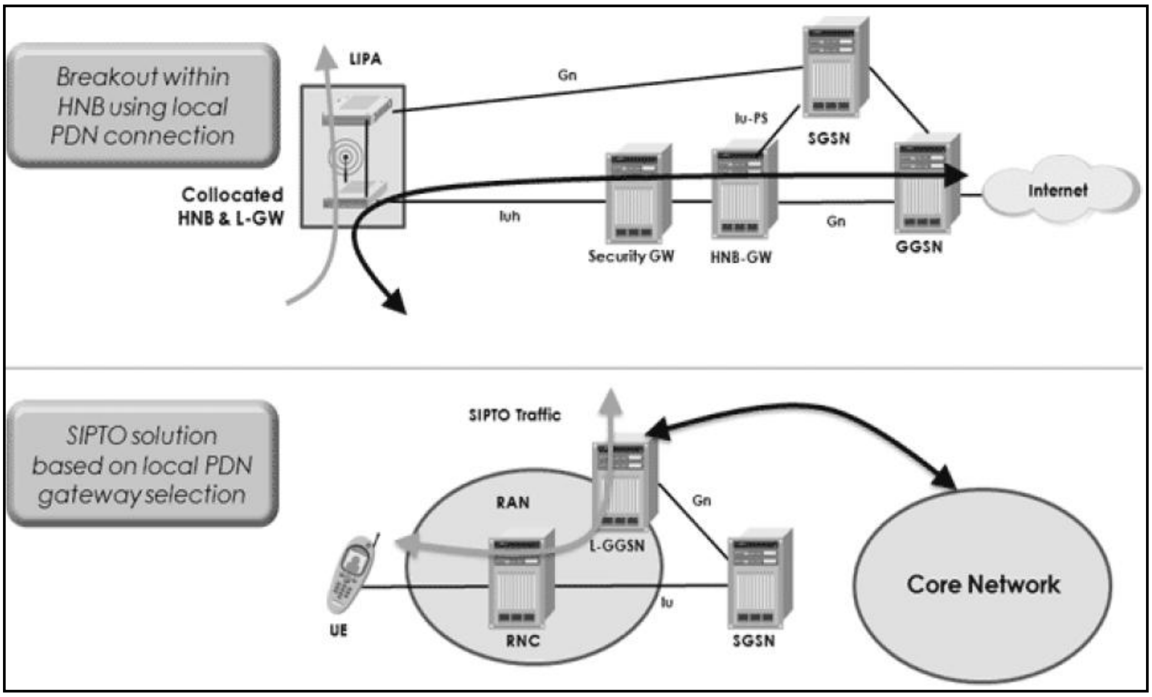


Figure 8 LIPA and SIPTO technologies

Implementation of SIPTO requires a special functionality (in a separate node or integrated with an existing node) to be placed between the Radio Access Network (RAN) and the Core Network (CN) to accomplish this. Traffic selection for offload is based on operator policies – which must strike the right balance for offload decisions – and traffic may be segregated based on 5-tuple IP filters.

Like SIPTO, Local IP Access (LIPA) is designed to optimize IP traffic management. LIPA focuses on IP traffic destined to a local IP Network and is designed to route such traffic locally instead of through the mobile core network. LIPA is defined for use cases such as a home-user trying to access a local server without having to access the wide area network. LIPA is very closely linked to Femtocells implementations and standards specify offload through Home NodeBs or HNBs as shown in Figure 8. As with SIPTO, the price is limited mobility support for the locally routed traffic; also, just like with SIPTO, policy-driven 5-tuple based routing is used to select which traffic is routed locally.

Another hugely popular technology is the one coming from Wi-Fi Association and names as Wi-Fi Certified Passpoint also popularly known as the Hotspot 2.0. Its first release came in 2012. Hotspot 2.0 is focused on enabling a mobile device to automatically "discover" APs that have a roaming arrangement with the user's home network and then securely connect. Hotspot 2.0 facilitates the seamless mobility of users from one WLAN to another or from Cellular RAN to WLAN and vice-versa, with minimal or no user intervention. It is expected to greatly enhance the end user experience and revolutionize the Wi-Fi sector as well as offer efficient offload solutions. The key enabling protocols for this technology are IEEE 802.11u, along with IEEE 802.1X, selected EAP methods, and IEEE 802.11i. The latter three are part of the WPA2-Enterprise certification program in the Wi-Fi Alliance. The IEEE 802.11u protocol enables a mobile device to have a dialog with a Wi-Fi AP "pre-association" to determine the capabilities that the network can support. ANQP (Access Network Query Protocol) and GAS (Generic Advertisement Service) are the two enabling protocols for the pre-association dialog between the network and the user equipment.

8 Security Aspects of Mobile Data Offload

The scope of the security aspects of both IWLAN and EPC standards are defined as follows. These aspects are defined in 3GPP TS 33.402 and TS 33.234.:-

8.1 User identity and device identity confidentiality

User identity confidentiality for procedures between the UE and the core is provided as per the framework of EAP-AKA and EAP-AKA' protocols. The details of the procedure are described in 3GPP technical specifications mentioned above.

8.2 Entity authentication

Entity authentication is a must for IWLAN/ cellular interworking as there are trusted and untrusted non-3GPP IP accesses are involved. Mutual authentication i.e. the UE is authenticated by the network and the network entity is authenticated by the UE is supported.

8.3 User data and signalling data confidentiality

Signaling data and user data confidentiality is supported and is mainly provided using the MIP and DSMIP protocols. The details of the procedure are described in 3GPP technical specifications mentioned above. In case of un-trusted access, IPSec tunnels are established between the UE and a trusted entity in the core network to ensure the same.

8.4 User data and signalling data integrity

Signaling data and user data integrity is supported and is mainly provided using the MIP and DSMIP protocols. The details of the procedure are described in 3GPP technical specifications mentioned above. In case of un-trusted access, IPSec tunnels are established between the UE and a trusted entity in the core network to ensure the same.

8.5 Security in roaming scenarios

In roaming scenarios the WAG acts as the anchor between the home and visited networks and all the security mechanisms like authentication policies etc. are relayed by it to the UE.

9 Future advancements in technology

The future advancements in the cellular/Wi-Fi integration aim at higher level of convergence to facilitate improved user experience. Following points elaborate the same:-

- Extensive research is being carried out on the development of smart connection managers at UE end to make the offload process user agnostic.

- Leveraging the seamless capabilities of Hotspot 2.0 in offloading by standardizing the interoperability of ANDSF server and ANQRP protocol supported by Hotspot 2.0.

- Integration of Femtocells and Wi-Fi technologies (feasibility study being carried out by Small Cell Forum).

- Network based IP Flow Mobility that is being studied in a work item called MAPIM by 3GPP.

- 3GPP study groups on OPIIS, which looks into operator policies for IP Interface selection; WORM for including both 3G and 4G in Wi-Fi offloading scenarios; enhancements to ANDSF policy solutions; P4C (formerly called BBAI) for interworking with broadband backhaul networks etc.

- IETF is working on enhancing its mobility toolkit i.e. the MIP and PMIP protocols.

10 Conclusion

Cellular/Wi-Fi integration and one of its outcomes i.e. Wi-Fi offload is a promising technology enhancement both from the operator and the end-user perspective. Its offerings are tremendous and its true potential should be tapped. Wi-Fi offload in the true sense is aimed to be end-user agnostic provider of seamless mobility and service. Though it is still long way to go to achieve these offload features, but the standardization process bears witness that it is going to happen in the near future.

There are some crucial points which need to be considered for effective deployment of Wi-Fi Offload. One, the dawn of this technology can truly be seen only when the Wi-Fi footprint in India increases to the level that the offload scenarios are feasible and economically lucrative. Another important point which can be envisaged is to form policies to facilitate fair revenue sharing between the Wi-Fi Operator, the Mobile Network Operator and other entities involved if any, so that there is minimal dispute. It should also be considered and assessed whether the Wi-Fi service providers, having integration and revenue sharing with licensed networks, will need to have some type of license obligations. Also to be given serious thought is the spectrum crunch that 2.4 GHz band will face, once Wi-Fi offload solutions are widely deployed. In order to address this, 60 GHz band can be considered as an excellent candidate for Wi-Fi deployments. Security considerations like the impact of Wi-Fi offload solutions on Location Based Services need to be thoroughly examined and addressed.

In addition to above, formation of a joint group of TSPs with DoT/TEC to understand the different aspects of Wi-Fi offload and also address the issues pertaining to it in advance will be quite helpful for efficient deployment of Wi-Fi offload solutions.

REFERENCES

1. 3GPP Universal Mobile Telecommunications System (UMTS); LTE; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description
(3GPP TS 23.234 version 11.0.0 Release 11)

2. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS);LTE;Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (3GPP TS 22.234 version 11.0.0 Release 11)

3. 3GPP Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE;Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (3GPP TR 22.934 version 11.0.0 Release 11)

4. Universal Mobile Telecommunications System (UMTS); LTE; IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2 (3GPP TS 23.261 version 11.0.0 Release 11)

5. Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses (3GPP TS 23.402 version 10.4.0 Release 10)

6. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems (3GPP TS 23.327 version 10.0.0 Release 10)

7. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
(Release 12)

8. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) interworking security (Release 12)

9. White paper on Cellular-Wi-Fi Integration by InterDigital Inc., 2012.

10. White paper on Internet Offload for Mobile Operators by Gabriel Brown.

11. Architecture for Mobile Data Offload over Wi-Fi Access Networks, Cisco.

12. WiFi Offload of Mobile data: UE challenges, Reetesh Kumar Varshney, Solutions Architect, Applications and Devices Business, Aricent

13. RFC 5213- Proxy Mobile IPv6

14. RFC 4186-EAP-SIM

15. RFC-4187- EAP-AKA

16. 3GPP TS 23.829 Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)

17. Hotspot 2.0 Whitepaper, Ruckus Wireless.