ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

Vol. 5, Issue 2, February 2017

# Voice and Data communication over Wi-Fi using Mobile Ad-Hoc Network(Voice Over Wi-Fi )

Himanshu Saxena[1], Ajay Kumar[2], Sachin Kumar[2]

M.Tech, Department of ECE, WCTM, Gurgaon (affiliated to Maharshi Dayan and University), Rohtak, Haryana, India[1]

Assistant Professor, Department of ECE, WCTM, Gurgaon (affiliated to Maharshi Dayan and University), Rohtak, Haryana, India[2]

**ABSTRACT:** The purpose of this Paper is to study voice and Data communication over mobile ad-hoc networks and how to implement in Current Mobile Network. Rapid technological changes are facilitating the convergence between Wi-Fi (short for “WirelessFidelity”) and mobile networks, in particular with LTE networks and resulting in the development of Voice over Wi-Fi (Vo Wi-Fi) services. Today the most cost effective use of Wi-Fi is calling over network. We have various facilities today such as Skype, WhatsApp, Facebook, T-Mobile, T-pad, Jaxtr for communicating over network but some restriction is placed on such system like Skype support only pc topc calling for cellular and landline call this free service become paid. T mobile also follows the same problem. Hence to overcome such issue we are developing a system which allows free calling over Wi-Fi network using VoIP service.

**KEYWORDS:** Voice Over Wi-Fi, overview of 3GPP options for Wi-Fi access, Vo Wi-Fi NetworkArchitecture, logical Interfaces, Call flow, Registration process (EPDG selection process), Vo Wi-Fi Call setup with new dedicated Bearer call flow.

## I. INTRODUCTION

Many mobile subscribers will first look for a nearby Wi-Fi service rather than using their cellular network subscription for data services on their smartphones, tablets and laptops. Such behavior is helping to ensure that Wi-Fi remains the dominant way to access data services from smartphones and tablets:

### What is Vo Wi-Fi?

**VoWi-Fi simply stands for voice over (EPC-integrated) Wi-Fi**is the use of a wireless broadband network according to the IEEE 802.11 standards for the purpose of communication. it is a complementary technology to VoLTE and utilizes IMS technology to provide a packet voice service that is delivered over IP via a Wi-Fi network. The mobile user needs the same applications and services with the same accessibility, security, quality-of-service (QoS), and high availability delivered to wired users. The concept, and service, was introduced several years ago, but only in the last several years has the service started tobecome attractive as a result of the increasing possibility of roaming between Wi-Fi and mobile networks

### Benefits of VoWi-Fi?

Both end users and those in the mobile industry will benefit from Voice over Wi-Fi.

### Consumers Benefits:

User Can make calls without the need for a mobile signal, Benefit from security being based on SIM-based authentication as for VoLTEandExperience better indoor coverage.

**Operators Benefits:**
Unlock revenue opportunities, Leverage existing SIM-based security and authentication as for VoLTE, Gain the opportunity to access IMS-based services via Wi-Fi access, Issue a single bill for the user for all IMS-based services across different access types. Ensure ongoing relevance with customers. Gain competitive advantage; andBenefit from voice/video telephony services provided by IMS and the MMTEL application server as for VoLTE/ViLTE.Works on any Wi-Fi (trusted/untrusted) but focus on indoor & poor LTE coverage areas reclaim the indoor/residential space. Single-number reach for SIM/non-SIM based devices Simplified Billing & capture of non-SIM based devices

## II. OVERVIEW OF 3GPP OPTIONS FOR WI-FI ACCESS

As defined in 3GPP TS 23.402. The 3GPP standard defines two types of access; trusted and untrusted non-3GPP access to a WLAN access to EPC, either trusted (S2a interface) or untrusted (S2b interface), Non-3GPP access includes access from for instance Wi-Fi, WiMAX, fixed and CDMA networks.

### 1) Trusted 3GPP Wi-Fi access:

Trusted non-3GPP Wi-Fi access was first introduced with the LTE standard in 3GPP Release 8 (2008). Trusted access is often assumed to be an operator-built Wi-Fi access with encryption in the Wi-Fi radio access network (RAN) and a secure authentication method. In practice the Wi-Fi access network must support the following features to be considered trusted:

- 802.1x-based authentication which in turn also requires encryption of the RAN
- 3GPP-based network access using EAP method for authentication
- IPv4 and/or IPv6

In a trusted access, the device (UE) is connected through a TWAG (Trusted Wireless Access Gateway) in the Wi-Fi core. The TWAG is in turn connected directly with the P-GW (Packet Gateway) in the Evolved Packet Core (EPC) through a secure tunnel (GTP, MIP or PMIP).

A similar concept is also used in non-EPC 3G networks where a WAG (Wireless Access Gateway) is connected with the GGSN through a secure GTP tunnel.

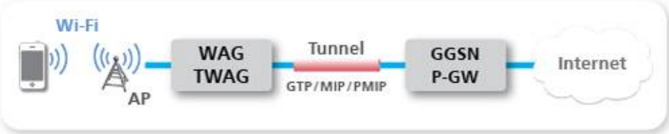

**Fig1: Trusted 3GPP Wi-Fi access**

### 2) Untrusted 3GPP Wi-Fi access:

Untrusted access includes any type of Wi-Fi access that the operator has no control over such as public hotspots, subscribers' home Wi-Fi and Corporate Wi-Fi. It also includes Wi-Fi access that does not provide sufficient security mechanisms such as authentication and radio link encryption.

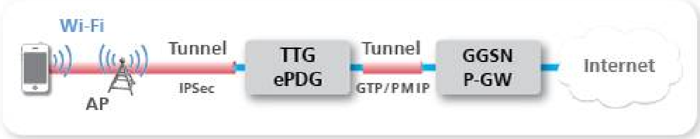

**Fig2: Untrusted 3GPP Wi-Fi access**

The untrusted model requires no changes to the Wi-Fi RAN (Radio Access Network) but has an impact on the device side which requires an IPsec client in the device. The device is connected directly to the ePDG (Evolved Packet Data Gateway) in the EPC through a secure IPsec tunnel. The ePDG is connected to the P-GW where each user session is transported through a secure tunnel (GTP or PMIP). A similar concept is also used in non-EPC 3G networks where the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

device is connected to a TTG (Tunnel Termination Gateway) through a secure IPsec tunnel. The TTG is in turn connected to the GGSN via GTP.

### 3) Non SIM Based Web Authentication:

One of the key aspects of the solution is to offer Internet services to Non-SIM subscribers by connecting to Open SSID. This presents a key challenge, as this type/scale of integration between Portal, Database, Provisioning System, PCRF and OCS is the first in the country. It focuses on the integration & deployment of SaMOG solution into the Wi-Fi environment.

## III. VO WI-FI NETWORK ARCHITECTURE

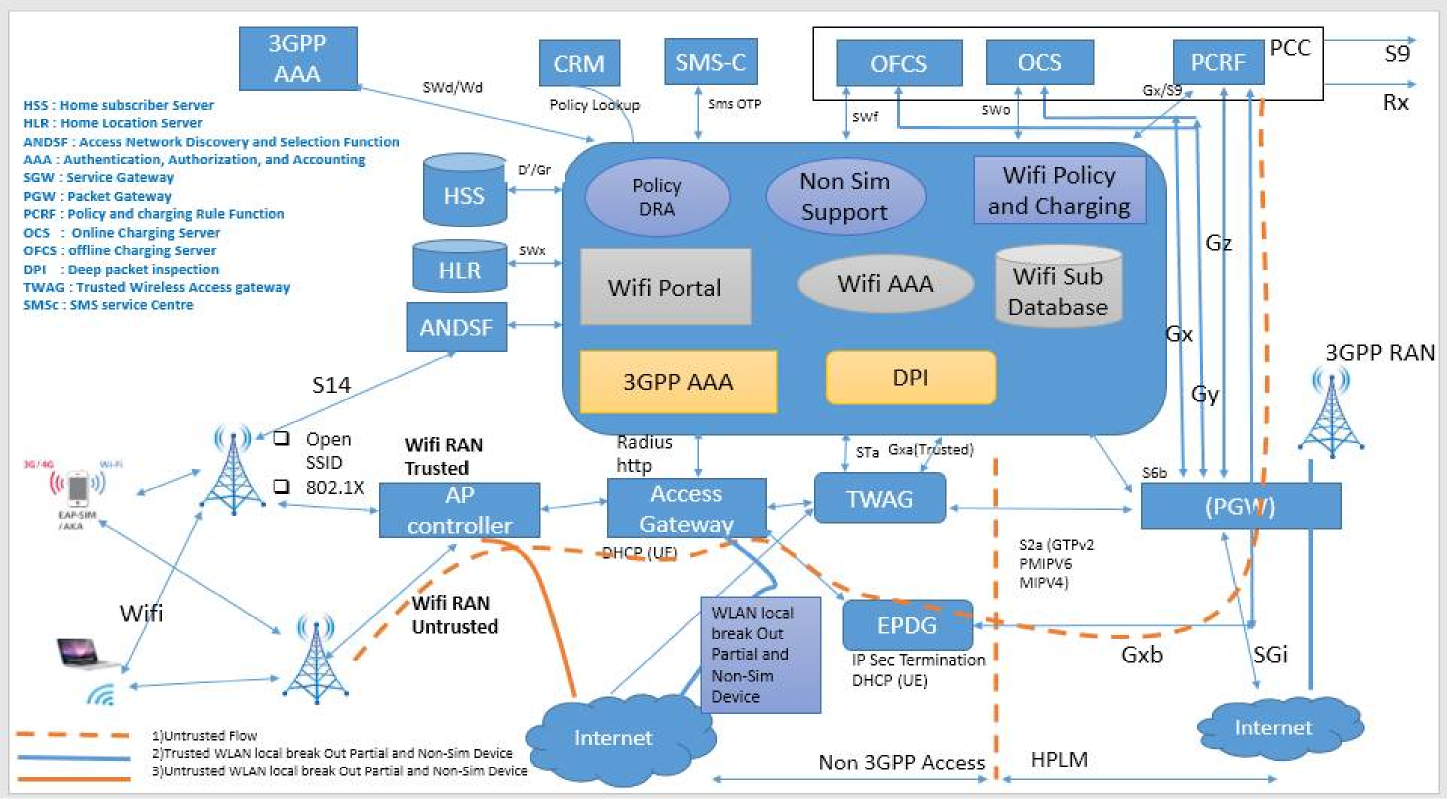
3GPP AAA
CRM
SMS-C
OFCS
OCS
PCRF
PCC
S9
Rx
SWd/Wd
Policy Lookup
Sms OTP
SWf
SWo
Gx/S9
HSS : Home subscriber Server
HLR : Home Location Server
ANDSF : Access Network Discovery and Selection Function
AAA : Authentication, Authorization, and Accounting
SGW : Service Gateway
PGW : Packet Gateway
PCRF : Policy and charging Rule Function
OCS : Online Charging Server
OFCS : offline Charging Server
DPI : Deep packet inspection
TWAG : Trusted Wireless Access gateway
SMSc : SMS service Centre
HSS
D'/Gr
HLR
SWx
ANDSF
Policy DRA
Non Sim Support
Wifi Policy and Charging
Wifi Portal
Wifi AAA
Wifi Sub Database
3GPP AAA
DPI
Gz
Gx
Gy
3GPP RAN
S14
Open SSID
802.1X
Wifi RAN Trusted
3G/4G
Wi-Fi
EAP-SIM /AKA
Radius http
STa
Gxa(Trusted)
S6b
AP controller
Access Gateway
TWAG
(PGW)
DHCP (UE)
S2a (GTPv2 PMIPV6 MIPV4)
Wifi
Wifi RAN Untrusted
WLAN local break Out Partial and Non-Sim Device
EPDG
IP Sec Termination DHCP (UE)
Gxb
SGi
Internet
Internet
Non 3GPP Access
HPLM
1)Untrusted Flow
2)Trusted WLAN local break Out Partial and Non-Sim Device
3)Untrusted WLAN local break Out Partial and Non-Sim Device

Fig.3 : Voice over Wi-Fi Network architecture

**VoWi-Fi E2E architecture requirements:**

- UE clients: iWLAN and VoLTE ,Wi-Fi access
- EPDG,TWAG,TWAP,AAA,PGW with s2b support
- VoLTE service infrastructure
- Support for non-UICC devices – Wi-Fi/VoLTE
- Mobility support
- Optionally enterprise integration (ISC) – VoLTE
- QoS guidelines for Wi-Fi
- SAMOG
- 3GPP SaMOG Definition : SaMOG (S2a Mobility Over GTPv2) provides EPC Access over Trusted WLAN.

DOI: 10.15680/IJIRCCE.2017. 0502054

**SAMOG Components:**

- WLAN Access Network
- Trusted (Operator owned)
- WLAN AAA Proxy
- TWAP
- WLAN Access Gateway
- TWAG

**EPDG Main Functions :**

- **User Authentication and Authorization**
  - IKEv2 based on EAP-AKA
  - De-capsulation/Encapsulation of packets for IPSec
  - Tunnel authentication and authorization
  - APN authorization and PWG selection
  - Provide PWG identity if static address
  - Local Mobility Anchor
  - PGW address from AAA in inter system handovers
- **Tunnel and QoS mapping between S2b bearers and access network**
  - Mapping of S2b bearer(s) to SWu (IPSec) sessions
  - Mapping of dedicated bearers on S2b using TFT packet filters
  - DSCP marking and/or 802.1p tagging for QoS
- **Routing of downlink packets towards the SWu instance associated to the PDN connection;**
  - Transport level packet marking in the uplink;
  - Enforcement of QoS policies based on information received over S2b control plane

**Trusted WLAN AAA Proxy (TWAP)**

- Provides a Radius Interface towards WLAN AN for UE authentication and accounting.
- Uses Diameter-based Interface towards the 3GPP AAA server
- Supports EAP based UE Authentication (EAP-SIM, EAP-AKA, EAP-AKA')
- Binds the UE’s WLAN identity to UE’s subscription data (APN Profile, IMSI, MSISDN)
- Provides the UE Attach and Detach triggers to the TWAG

**Trusted WLAN Access Gateway (TWAG)**

- Gateway to connect the Trusted
- WLAN to the EPC
- Terminates the S2a interface, carrying the UE packets from the WLAN in the S2a tunnel based on GTPv2.
- Packet forwarding in the TWAN is based on PMIPv6 tunnel between WLC and TWAG, GTPv2 Tunnel between TWAG and EPC.
- Receives and responds to triggers from the TWAP for UE Attach, Detach

## IV. LOGICAL INTERFACES

**SWu Interface:**

SWu is a Secure Interface to UEs in a non-3GPP access network. This interface carries IPSec tunnels. The IKEv2 protocol is used to establish IPSec tunnels between the UEs and ePDG.

**SWm Interface:**

SWm is the interface used to connect to the 3GPP Diameter AAA server. It is used to transport UEs mobility parameters and tunnel authentication and authorization data using EAP-AKA method.

**SWx Interface:**

SWx is the interface used to connect 3GPP Diameter AAA server to HSS. It is used to transport UEs mobility parameters and fetch User authorization data.

**Sh Interface:**

Sh interface is used by 3GPP AAA to send UDR (User Data Request) to HSS over Sh interface asking for EPS User state, subsequent to which HSS sends IDR to MME to get the user state details.UDA (User Data Answer) is then accordingly passed onto to AAA by HSS with this info.

**S2b Interface:**

S2b is the interface used to connect to the P-GW. It is based on GTPv2 protocol and used to establish WLAN UE sessions.

**S6b Interface:**

S6b is the interface used to connect 3GPP Diameter AAA server to PGW. It is used to update PGW address to HSS, when the UE is attached on non-3GPP access.

## V. REGISTRATION PROCESS (EPDG SELECTION PROCESS)

**EPDG selection process:**

a) UE selects ePDG: UE constructs an FQDN and performs a DNS query to resolve it. Response contains 1 or more IP addresses in IPv4/IPv6 format. UE select an address in the same format.
b) ePDG select AAA: ePDG is provisioned with a pair of 3GPP AAA IP Addresses (Primary/ Secondary). DIAMETER watchdog process monitors primary/secondary link for failover.
c) ePDG selects PGW: For a given APN, the ePDG will construct an APN FQDN based on the format of: apn.epc.mnc.mcc.3gppnetwork.org. The ePDG will perform DNS S-NAPTR query to get PG
d) The NAPTR response will contain three Records with “a” flag but different “Service Parameters”. TheePDG will then perform a DNS AAAA query. This will result in the IP address of S2b interface of the provided PGW.

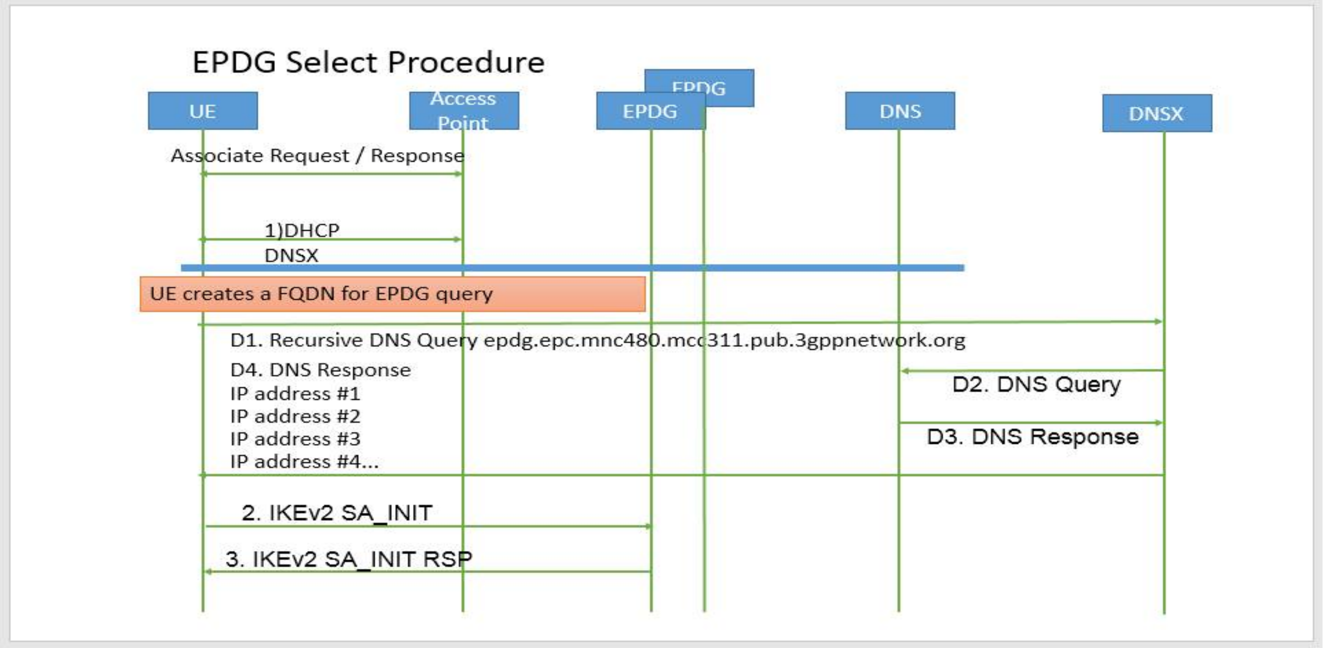

**Fig4: EPDG Select Procedure**

**EPDG Tunnel Setup**

1) UE attach to Wi-Fi and obtain IP connectivity
2) UE selects ePDG based on static IP configuration or DNS
3) UE and ePDG perform mutual authentication during IPsec tunnel establishment using public key certificates
4) UE sends encapsulated EAP-AKA messages over IKEv2 to ePDG incl. user identity (NAI) and potential APN (for IMS)
5) ePDG de-capsulate EAP-AKA messages and sends to AAA for authentication and authorization
6) AAA fetch AKA authentication vectors generated by the HSS (if not available). AAA extract IMSI for the user
7) AAA initiates the authentication challenge with ePDG and UE
8) If successful, the AAA initiates the subscriber profile retrieval with the HSS to check if the user is authorized for the untrusted access and sends server registration.
9) If successful, the AAA sends the final authentication answer incl. IMSI and MSK (Master Session Key)

**PGW Selection:**

The P-GW selection function enables the ePDG to allocate a P-GW to provide PDN connectivity to the WLAN UEs in the untrusted non-3GPP IP access network. The P-GW selection function can employ either static or dynamic selection

a) **Static Selection:**The PDN-GW-Allocation-Type AVP (in DEA) indicates whether the P-GW address is statically allocated or dynamically selected by other nodes, and is considered only if MIP6-Agent-Info is present. When the PDN-GW-Allocation-Type AVP is absent or is STATIC, and an initial attach occurs, or is DYNAMIC and a handoff attach occurs, the ePDG performs static selection of the P-GW
b) **Dynamic Selection:**For a given APN, when the HSS returns Dynamic Allocation Allowed for the P-GW ID and the selection is not for a 3GPP-to-non-3GPP handover, the ePDG ignores the P-GW ID and instead performs dynamic selection
c) **Topology based Selection:**For topology-based selection, once the DNS procedure outputs a list of P-GW hostnames for the APN FQDN, the ePDG performs a longest-suffix match and selects the P-GW that is topologically closest to the ePDG and subscriber. If there are multiple matches with the same suffix length, the Weight and Priority fields in the NAPTR resource records are used to sort the list. The record with the lowest number in the Priority field is chosen first, and the Weight field is used for those records with the same priority
d) **Weight-based Selection**: For weight-based selection, once the DNS procedure outputs a list of P-GW hostnames for the APN FQDN, if there are multiple entries with same priority, calls are distributed to these P-GWs according to the Weight field in the resource records. The Weight field specifies a relative weight for entries with the same priority. Larger weights are given a proportionately higher probability of being selected. The ePDG uses the value of (65535 minus NAPTR preference) as the statistical weight for NAPTR resource records in the same way as the SRV weight is used for SRV records, as defined in RFC 2782

   When both topology-based and weight-based selection are enabled on the ePDG, topology-based selection is performed first, followed by weight-based selection. A candidate list of P-GWs is constructed based on these, and the ePDG selects a P-GW from this list for call establishment. If the selected P-GW does not respond, the ePDG selects the alternate P-GW(s) from the candidate list.

**PDN Types :**

1) ePDG supports PDN type IPv4, IPv6 and IPv4v6.
2) In IKE_AUTH_REQ CP (CFG_REQ) UE shall request for the IPv4/IPv6/Dual address.
3) ePDG does communicates the requested PDN type in Create Session Request message to PGW.
4) PGW checks the configured APN configuration and allocates the requested PDN type IP address/prefix and assigns to UE which is communicated in Create Session Response.
5) For IPv6 PDN type calls ePDG does sends the Router Advertisement to UE.

**Dedicated Bearer :**

1) PGW triggers Create Bearer Request to ePDG to create Dedicated Bearer if the specific Traffic is supposed to be send on it.

2) ePDG installs Uplink TFT received with Create Bearer Request message.
3) ePDG only handles UL TFT based traffic routing and not DL.
4) Based on configuration(optional), QCI is used to VLAN priority tagging or Outer IP Header DSCP marking for UL traffic.
5) APN-AMBR is also negotiated during Dedicated Bearer creation
6) Maximum eleven bearer (including default) can be created for a particular IMSI.

## VI. VO WI-FI CALL SETUP DESCRIPTION (INITIAL ATTACH FLOW)

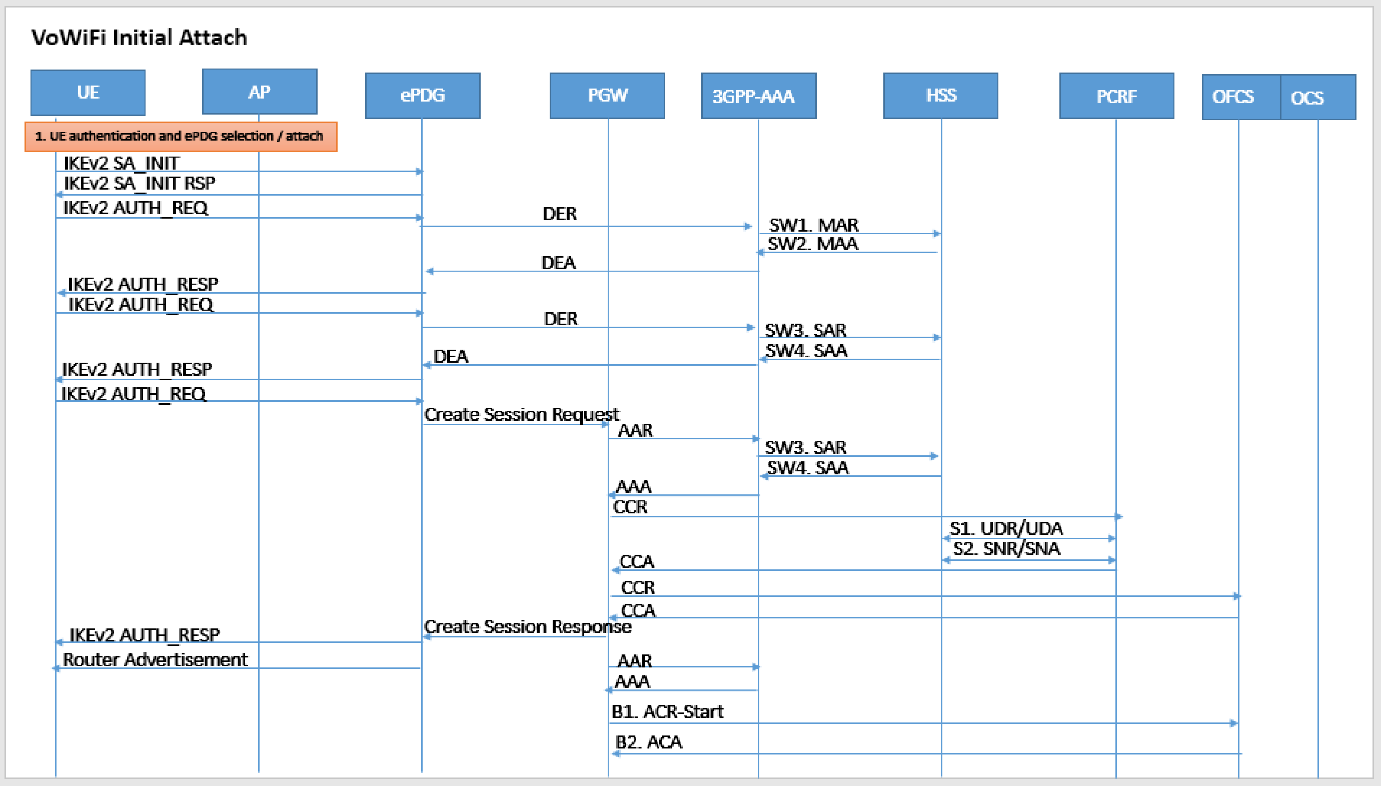

Fig.5: UE Attach and VoWi-Fi Flow

### Vo Wi-Fi Call SetupDescription

**Step 1. Authentication and ePDG selection**
UE detects a suitable Wi-Fi access and associates and completes any required authentication with local ISP. Once the UE obtains an IP address from the Wi-Fi and is in a state to access the Internet, it initiates an IPsec IKEv2 connection to the ePDG for IMS APN. The ePDG selection at UE is done either statically or dynamically using a DNS server. If dynamic selection is enabled, UE will use H-PLMNs MCC & MNC to form the ePDG FQDN. UE gets the home ePDG address in DNS response. (ePDG discovery at UE is explained in ePDG Discovery)

**Step 2. UE toePDG: IKEv2 SA_INIT Request**
The UE sends IKE_SA_INIT Request.

**Step 3. EPDG Toque: IKEv2 SA_INIT Response**
The ePDG sends IKE_SA_INIT Response.
The ePDG will start the IKEv2 setup timer when sending the IKEv2_SA_INIT Response.

**Step 4. UE ToePDG: IKEv2 AUTH_Request**

UE sends IKE_Auth_Requestfor APN IPV4 or IPV6.in this UE also send Idi that Contain FQDN (epc.mnc.mcc.*3gppnetwork.org) and IDr that Contains APN name.*

**Step 5.** **ePDG** To**3GPP-AAA: DER**

The ePDG sends Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN.

**Step 6.** **3GPP AAA** to**HSS: MAR**

The 3GPP AAA server shall lookup the IMSI of the authenticated user based on the received user identity (root NAI or pseudonym) and include the EAP-AKA as “requested authentication” method in the request sent to the HSS. The AAA sends the **Multimedia-Auth-Request MAR**

**Step 7.** **HSS** to**3GPP AAA: MAA**

The HSS shall then generate authentication vectors with AMF separation bit assigned “0” and send them back to the 3GPP AAA server. The HSS sends the Multimedia-Auth-Answer.

**Step 8.** **AAA** to**ePDG: DEA**

The 3GPP AAA Server initiates the authentication challenge and responds with DEA (Session-Id, Base AVPs, Auth-Request-Type, EAP-Payload, EAP-Master-Session-Key.

**Step 9.** **ePDG**to**UE: IKE_AUTH**

The ePDG responds with IKE_AUTH (ID, [AUTH], EAP Payload).

**Step 10.** **UE** to**ePDG: IKE_AUTH Request**

The UE checks the authentication parameters and responds to the authentication challenge.

**Step 11.** **ePDG**to**3GPP-AAA: DER**

The ePDG sends DER to the 3GPP AAA Server.

**Step 12.** **AAA** to**HSS: SAR**

The 3GPP AAA updates the HSS with the 3GPP AAA Server Address information for the authenticated user. The AAA sends Server-Assignment-Request.

**Step 13.** **HSS** to**3GPP-AAA: SAA**

The HSS sends Server-Assignment-Answer

**Step 14.** **3GPP – AAA** to**HSS: UDR**

The 3GPP-AAA CPAR initiates User data request (UDR) to HSS with Data Reference AVP set to user state

**Step 15.** **HSS** to**MME: IDR**

The HSS sends Insert subscriber -data request (IDR) towards MME on S6a/S6d interface with EPS user state bit set in IDR flag

**Step 16.** **MME** to**HSS: IDA**

The MME responds with Insert subscriber data answer with EPS user state in MME_USER_STATE AVP towards HSS.

**Step 17.** **HSS** to**3GPP AAA: UDA**

The HSS responds with user data answer message to CPAR with EPS user, inside User data AVP.The user state to allow is ‘CONNECTED_REACHABLE_FOR_PAGING.

**Step 18.** **AAA** to**ePDG: DEA**

The 3GPP AAA Server sends an EAP success.

**Step 19.** **ePDG**to**UE: IKE_AUTH_Response**

ePDG sends IKE_AUTH_Response (EAP)

**Step 20.** **UE** to**ePDG: IKE_AUTH_Request**

UE sends IKE_AUTH request (AUTH). The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.

**Step 21.** **ePDG**to**PGW: Create Session Request**

ePDG selects the PGW based on Node Selection options implemented. The ePDG sends Create Session Request.

**Step 22.** **PGW** to**PCRF: CCR**

The PGW sends an indication of IP-CAN establishment to the PCRF with CCR to indicate establishment of a new IP CAN session.

**Step 23.** **PCRF** to**PGW: CCA**

The PCRF Acknowledges IP CAN Session Establishment with a CCA message. This message includes the Policy and charging rules, the PGW will enforce and trigger for events that must be reported by the PGW.

**Step 24.** **PGW** to**OCS: CCR**

If the Online is enabled for the user, the PGW shall send a CCR-Initial to the OCS to request online charging quota for the PDN session.

**Step 25.** **OCS** to**PGW: CCA**

The OCS responds with a CCA to the PGW

**Step 26. PGW** to**3GPP-AAA: AAR**
The PGW sends AARto the 3GPP AAA to authorize the PDN for the subscriber and to update PGW address on the HSS for the APN.

**Step 27. 3GPP-AAA** to**HSS: SAR**
The 3GPP AAA updates the HSS with the PGW address for the APN and retrieves Subscriber-APN profiles from the HSS. The AAA sends Server-Assignment.

**Step 28. HSS** to**AAA: SAA**
The HSS sends Server-Assignment-Answer.

**Step 29. 3GPP-AAA** to**PGW: AAA**
The 3GPP AAA sends AAA.

**Step 30. PGW** to**ePDG: Create Session Response**
The PGW allocates the requested IP address session and responds back to the ePDGwith a Create Session Response.

**Step 31. ePDG**to**UE: IKE_AUTH**
The ePDG sends IKE_AUTH

**Step 32. ePDG**to**UE: Router Advertisement**
ePDG sends Router Advertisement to ensure that the IPv6 Stack is fully initialized at UE. This is required only if IMS APN allocates IPv6 address.

**Step 33. UE** to **IMS: SIP Register**
UE sends SIP Register to P-CSCF & registers to P-CSCF using a Default Bearer.

**Step 34. UE** to **IMS: New Call**
UE initiates a Voice call using a SIP Initial message. UE & IMS exchanges SIP messages for a call establishment

## VII. VO WI-FI CALL SETUP WITH NEW DEDICATED BEARER CALL FLOW

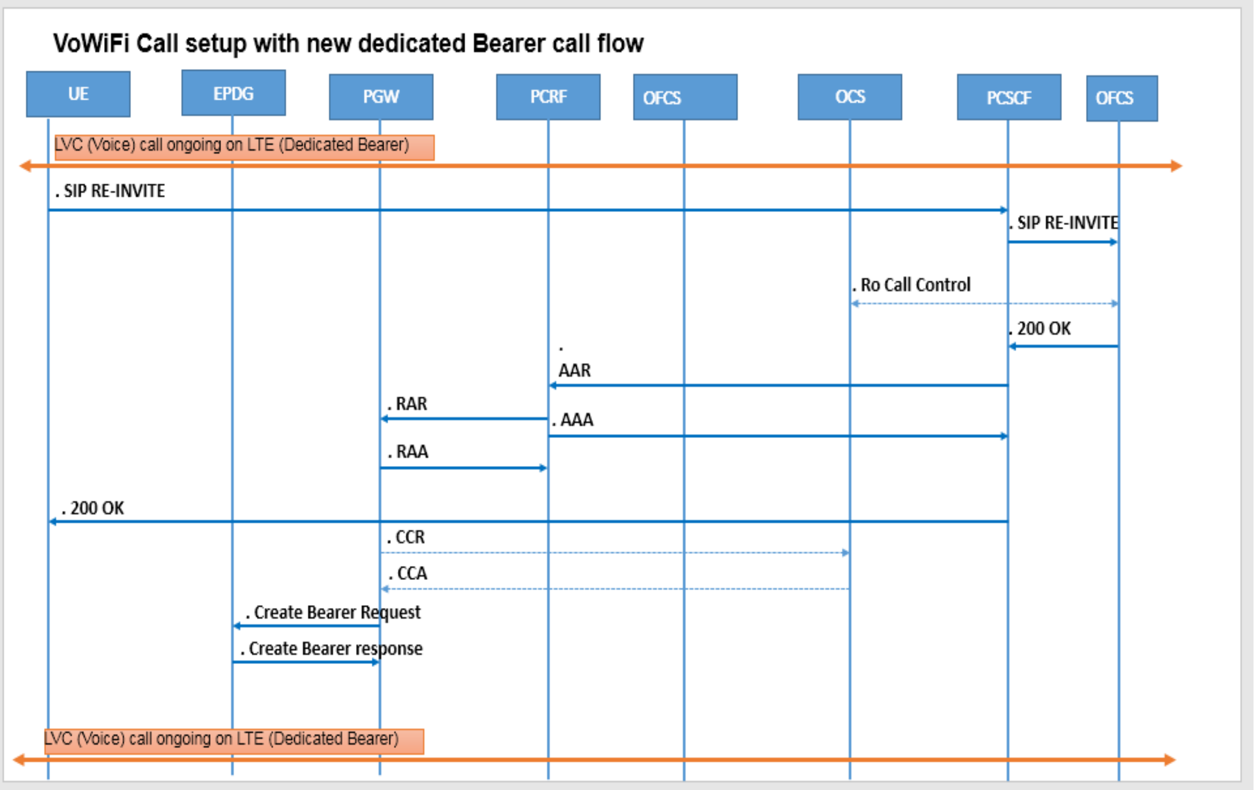

**Fig. 6:Vo Wi-Fi Call setup with new dedicated Bearer call flow**

**Step 35. P-CSCFtoPCRF: AAR**

P-CSCF sends AAR on a Rx interface to PCRF with IP filters, Codec rates, Framed IP address etc.

**Step 36. PCRFToPGW: RAR**

PCRF sends RAR to PGW for an initiation of dedicated bearer

**Step 37. PGW ToePDG: Create Bearer Request**

The PGW sends to the ePDG with a Create Bearer Request (TFT, S2b-U PGW F-TEID, Bearer Level QoS)) message

**Step 38. ePDGtoPGW: Create Bearer Response**

The ePDG sends to the PGW with a Create Bearer Response (TFT, S2b-U ePDG F-TEID) message

**Step 39. PGW toPCRF: RAA**

PGW sends RAA success to PCRF

**Step 40. PCRF toP-CSCF: AAA**

PCRF sends AAA on a Rx interface to PCRF

**Step 41. UEtoIMS: Voice /Video Packets**

All UE packets will now traverse on dedicated bearers between ePDG& PGW

## VIII. CONCLUSION &FUTURE SCOPE

Customers are willing to pay for a service that's expected to perform better than the existing services. Packet based voice services have the potential to disrupt traditional CS based voice services. Operators should launch services like Vo Wi-Fi when the service is stable in the network, delivering a good quality of service. It has happened in the past, that with new services if a customer faces issues he may not use the service again in near future. This can also result in churn for operators. For MVNOs as well, Vo Wi-Fi is good opportunity to enter a new market. Vo Wi-Fi shouldn't be considered as a competitor to VoLTE, rather it complements VoLTE. Time will tell if Vo Wi-Fi will change the way we call each other but if early results are to be followed, then it's on the way to do it!

From a complexity point of view, Vo Wi-Fi makes it very simple to leverage existing 4G andVoLTE.Due to advantages of Vo Wi-Fidescribed above Vo Wi-Fi has the chance to become a widespread Voice over LTE solution and will ensurethat two of the main revenue generators for network operators, voice calls and SMS, will beavailable in LTE networks very early on. The benefits that users experience from Vo Wi-Fi will affect its demand and the market growth ofVo Wi-Fi services over the next few years. Users of dual handsets will be able to make calls more cheaplythan those using mobile phones. Calls generated in hotspots or WLANs are likely to result in considerablesavings by consumers. Vo Wi-Fi also provides innovative new features such as the ability to access e-mail,Internet, location information, etc. at a lower price. Another benefit for existing users of Vo Wi-Fi service isthat they are no longer constrained in obtaining service from a limited area such as a hotspot or within acompany, but are able to have real mobility and ubiquitous access to voice calls as well as data and videoby seamless interconnection with mobile networks with a single handset or portable computer. Using freeInternet within an enterprise's WLAN eliminates mobile network access charges. Therefore, those users,especially business users, are able to improve the efficiency and productivity and reduce costs. However,these possible user benefits will only be realized if the current and emerging issues raised during thedeployment of technology, as indicated in the following section of this paper, are tackled.

## REFERENCES

[1] "Voice over Internet Protocol. Definition and Overview". International Engineering Consortium. 2007. Retrieved 2009-04-27.
[2] "Voice over Internet Protocol. Definition and Overview". International Engineering Consortium. 2007. Retrieved 2009-04-27.
[3] "IP Telephony Vs VoIP". Retrieved 27 April 2011.
[4] Booth, C (2010). "Chapter 2: IP Phones,
[5] Software VoIP, and Integrated and Mobile VoIP". Library Technology Reports 46 (5): 11–19.
[6] "Carriers look to IP for backhaul". Telecommunications Online. January 21, 2009. Retrieved 2009-01-21.
[7] "Mobile's IP challenge". Total Telecom. December 8,2005. Retrieved 2009-01-21.
[8] 3GPP TR 23.879 - Study on Circuit Switched (CS) domain services over evolved Packet
[9] Switched (PS) access; Stage 2, 3GPP Release 8
[10] Voice over LTE via Generic Access; Stage 2 Specification; Phase 1
[11] Martin Sauter, beyond 3G - Bringing Networks, Terminals and the Web Together: LTE,
[12] WiMAX, IMS, 4G Devices and the Mobile Web 2.0, 2009, ISBN: 978-0470751886