NextGen Wireless Access Gateway

Analysis of Combining WiMAX and LTE Gateway functions

K.S. Keshava Murthy, Aricent, India

Abstract — The capabilities of the wireless networks are continuously being enhanced to meet ever growing demand of the higher data rates for accessing wide range of internet services in the mobile node. The IEEE 802.16e Mobile Worldwide Interoperability for Microwave Access (WiMAX), 3GPP Long Term Evolution (LTE) and 3GPP2 Ultra Mobile Broadband (UMB) wireless technologies are identified as next generation technologies beyond 3G to meet this growing demand. All these technologies are using Orthogonal Frequency Division Multiple Access (OFDMA) as the radio access technology to achieve higher data rates, efficient spectrum usage, higher cell throughput, seamless mobility and All-IP based core network for distributed, scalable network architecture to support wide range of applications/services with better quality of experience.

Some of BS Original Equipment Manufacturers (OEM) already support both LTE and WiMAX base station function on the same hardware platform with different software loads. Looking at this trend, and considering the User Plane transport similarities in "beyond 3G" networks, this paper analyses the possibility of having common access gateway functional modules for supporting LTE networks Mobility Management Entity (MME), Serving Gateway (S-GW) functions and WiMAX networks Access Services Network Gateway (ASN-GW) functions.

Keywords: Mobile WiMAX, LTE, IMS, QoS, PCC, AAA, DHCP, PMIP,CMIP, MSS, UE, EPC, EPS

I. INTRODUCTION

The Broadband Wireless Access Networks like Mobile WiMAX and LTE are using ALL-IP based core network to achieve distributed and scalable network architecture with higher throughput per connection. This results in set of features like Security, Quality of Service (QoS), User plane transport protocols, lower layer IP protocols, Element Management, IMS overlay, etc are similar in access gateway node of the different networks. Following NextGen Wireless Access Gateway architecture is one of the possible architecture which can support both WiMAX and LTE access gateway function, having network specific procedures and group of common procedures with generic interface between common and specific procedures:

1. The data path function module can be common for both ASN-GW and S-GW, with following features:
    a. Physical interface to external network elements
    b. IP, IPSec, tunneling, QoS (packet forwarding, queuing, Diffserv marking, etc)
    c. User Plane protocols for different networks.
    d. Except application level protocols, all Transport protocol(s) to support Control plane application protocols.

    The Data path function module can be hosted on dedicated processor having the support of integrated cryptography engines with hardware acceleration of multiple algorithms DES, 3DES, AES, and SHA-1 for IPSec. This can help to meet high performance and scalability.
2. Control plane function module shall be specific to network type, with well defined interface between data path controller and control plane function to configure and setup per connection specific behavior of the data path function.

    This module can be hosted on server, where both WiMAX and LTE applications can run as two logical entities communicating to single data path function module.
3. Common Network Management framework can be used for both ASN-GW and MME/S-GW network elements with NE specific Managed Objects.

Further section of this paper discuss the similarities and differences of key procedures of both WiMAX and LTE access gateway in detail and highlight different modules which can be common or specific to particular network type.

II. NETWORK ARCHITECTURE

As depicted in Fig 1, in Mobile WiMAX network architecture, ASN-GW is connecting Connectivity Service Network (CSN) elements and Base Station (BS) nodes in the Access Service Network (ASN). Based on the different profiles of WiMAX network architecture, ASN-GW hosts the different functionality. The commonly used profile is Profile-C where BS and ASN-GW are distributed. ASN-GW with Profile-C is considered for comparative analysis in this paper.

The ASN-GW is hosting both control (signaling) and user (data/traffic) plane procedures to connect access network and core network elements.

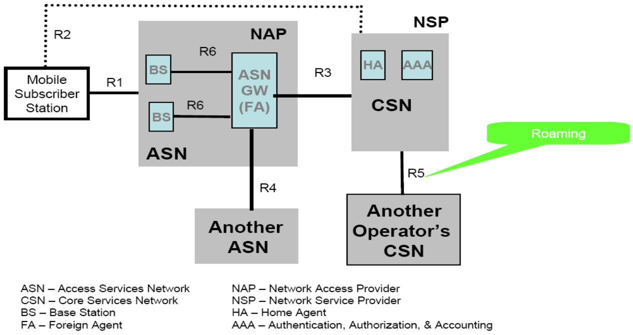

R2
NAP
NSP
R6
BS
ASN
GW
(FA)
R3
HA
AAA
Mobile
Subscriber
Station
R1
BS
R6
CSN
Roaming
ASN
R5
R4
Another
ASN
Another
Operator's
CSN
ASN – Access Services Network
CSN – Core Services Network
BS – Base Station
FA – Foreign Agent
NAP – Network Access Provider
NSP – Network Service Provider
HA – Home Agent
AAA – Authentication, Authorization, & Accounting

Fig1: WiMAX Network Architecture

As depicted in Fig 2, in 3GPP LTE network architecture, the MME and S-GW in the Evolved Packet Core (EPC) inter connects Evolved Universal Terrestrial Radio Access Network (E-UTRAN) nodeB (eNB) and core network elements. The control and user plane procedures are split between MME and S-GW respectively. But 3GPP recommends combining these functions in a single node which provides similar functionality like ASN-GW in WiMAX. For comparative analysis MME and S-GW co-located node is considered.

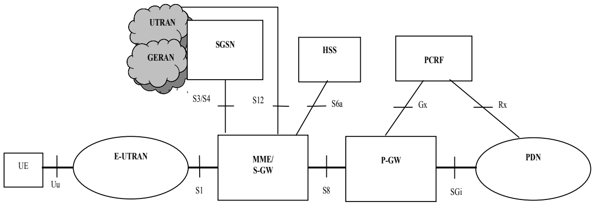


Fig 2: LTE network Architecture

III. WIMAX ASN-GW AND LTE MME/S-GW FUNCTIONAL COMPARISON

A. *User identity Confidentiality*

WiMAX: In WiMAX networks, Network Access Identifier (NAI) is used as user identity. There are two identifiers called inner and outer identity. Inner identity is real identity of a user like IMSI in 3GPP network, which is used by MSS and authentication server, and not shared with ASN-GW or any other Network Element (NE). The user name and realm part of the NAI (outer identity) is used as user identity in ASN-GW for CSN procedure.

LTE: In LTE network, User permanent identity International Mobile Subscriber Identity (IMSI) or temporary identifiers like Globally Unique Temporary Identity (GUTI) or Shortened-Temporary Mobile Subscriber Identity (S-TMSI) is used to identify user. Other than very first network entry procedure, UE always sends temporary identifier GUTI in the NAS messages to keep user real identity IMSI as confidential. On successful authentication and security mode procedure, MME allocates GUTI to the user and sends to the UE with ciphering and integrity protection.

User Identity procedures in WiMAX and LTE networks are specific to each network.

B. *Authentication and Key Distribution*

WiMAX: In WiMAX networks two level of authentication known as device and user authentication is supported. Extensible Authentication Protocol (EAP) based authentication procedures are used for both device (optional) and user authentication between server and the Mobile Subscriber Station (MSS). The EAP methods, EAP with Transport Layer Security (EAP-TLS) for device authentication, EAP Authentication and Key Agreement (EAP-AKA) or EAP Authentication with Tunneled TLS (EAP-TTLS) for user authentication are supported. In EAP based user authentication, ASN-GW gets pair wise master key (PMK) from authentication server and generate Authorization Key (AK) and distribute to BS. The AK verification between network and the MSS is done at the BS using Privacy Key Management (PKM) three-way handshake procedures.

LTE: In LTE network, *Evolved Packet System* authentication and key agreement (EPS-AKA) procedure is used between the UE and MME for user authentication. There is no device authentication in E-UTRAN network, only equipment verification with Equipment Identity Register (EIR) is optionally done by MME during attach procedure.

In EPS-AKA procedures, MME gets the authentication vector from authentication server which includes Authentication key K_{ASME} and executes authentication procedure with UE to verify the authentication result. On successful authentication, MME generates security keys required for Non-Access Stratum (NAS) signaling integrity, ciphering and K_{eNB} from the key $K_{ASME.}$ Key K_{ASME} is stored in the MME and key K_{eNB} is transferred to eNB.

The EAP-AKA procedure in WiMAX and EPS-AKA procedure in LTE are based on the AKA protocol. But the algorithm and the procedures are specific to each network. The common AAA based interface can be used in both networks between ASN-GW/MME and AAA/HSS network elements.

C. *User Data and Signaling Confidentiality*

WiMAX ASN-GW: The backhaul network side interfaces (R3, R4, R6, R8, etc) in the ASN-GW are not secured. The ASN-GW should use IP Security (IPSec) or Secure Sockets Layer (SSL) Virtual Private Network (VPN) protected tunnel for securing these interfaces. The ASN-GW can also use authentication extension mechanism of the signaling protocol to protect the signaling messages through integrity protection between ASN and CSN. The different integrity protection mechanisms like authentication sub option, authentication extension, etc are supported in ASN-GW for DHCP, MIP and AAA interfaces.

LTE: In LTE network, NAS and Access Stratum (AS) control plane is integrity protected and ciphered between UE and MME/eNB. User plane is always ciphered between UE and eNB. The backhaul network side interfaces like (S1, S5/S8, S6a, etc) in MME/S-GW are not secured. The MME/S-GW should use IPSec ESP protected tunnel for securing these interfaces.

In both WiMAX and LTE networks backhaul network side interfaces required to use IPSec security procedures for protecting the control and user plane.

D. *UE Context Management*

WiMAX: In WiMAX network, ASN-GW maintains UE context mapped to Mobile Subscriber Identity (MSID) and NAI. MSID is the MAC address of the MSS. UE context information depends on the network element function like

Authenticator ASN, Serving ASN, Anchor ASN or Anchor Paging Controller (Anchor PC).

The MSID is used as user identifier in R6 and R4 interface messages. And NAI is used as identifier towards R3 in AAA username, MIP NAI extension and DHCP Subscriber-ID options. During handover all contexts like AK context, Data Path (DP) context, etc need not be transferred to target. Serving ASN can continue as serving authenticator or Serving Service Flow Authorization (SFA) for the duration of the session.

LTE: In LTE network, MME maintains user context mapping with GUTI/IMSI and S-GW maintains Service Data Flow (SDF) context for the default/dedicated bearers established. The IMSI is used as identifier in network side interfaces and GUTI/S-TMSI is used as identifier in access side interfaces. During handover, MME transfers complete UE context to the target which includes IMSI and current GUTI/S-TMSI.

UE Context Management is specific to individual network procedures of WiMAX and LTE.

E. IP Address allocation

WiMAX: In WiMAX network, dynamic IP address to UE is allocated through Client Mobile IP (CMIP) or DHCP based procedures.

For CMIP based Procedure, ASN-GW acts as FA, supports care of address (CoA) procedure and routes the MIP messages between HA and MSS. HA allocates the IP address for the MS. **For DHCP based procedures**, ASN-GW acts as DHCP proxy or DHCP relay depending on the subscriber profile. In DHCP proxy mode IP address available in the subscriber profile is used and ASN-GW proxies the DHCP server behavior. In DHCP relay mode ASN-GW acts as relay agent and IP address is allocated by DHCP server. If DHCP server address is not known but HA address is known, ASN-GW acting as FA (CoA) requests HA to allocate IP address through PMIP procedures.

LTE: In LTE Network, IPv4 address to UE is allocated via default bearer activation or via DHCP procedure on the default bearer.

IPv4 address allocation via default bearer activation: After successful authentication, MME triggers default bearer creation procedure. The Packet Data Network Gateway (P-GW) allocates the IP address to UE. MME sends allocated PDN IP address to UE in the NAS message.

IPv4 address allocation and IPv4 parameter configuration via DHCPv4: After successful establishment of default bearer, UE triggers DHCP Discovery procedure. In this case Serving Gateway acts as DHCP relay agent and forward received DHCP client request to P-GW to allocate IP address to UE.

Both WiMAX ASN-GW and LTE MME/S-GW access gateways are using DHCP relay procedures for IP address allocation and support FA function for PMIP procedures with HA or P-GW. The DHCP relay function and PMIP implementation can be common for both the networks.

F. Quality of Service and Data bearer management

WiMAX: In WiMAX network, ASN-GW hosts Service flow authorization function. This has two functional elements called Anchor and Serving SFA. Anchor SFA receives packet flow description for subscriber on successful authentication and serving SFA creates data path (service flow) for the supported packet flows. Every packet flow is associated with QoS description for the supporting media flow type (Voice over IP, Robust Browser, Control, Data, Streaming, etc) and schedule type (Best Effort (BE), Non-Real Time Polling Service (nrtPS), Real Time Polling Service (rtPS), Unsolicited Grant Service (UGS) and Extended rtPS (ErtPS)).

When Policy and Charging Control (PCC) procedure is used, Anchor SFA hosts ASN side Policy and Charging Enforcement Function (A-PCEF). The Policy and Charging Rules Function (PCRF) may apply new PCC rules, during IP-Connectivity Access Network (IP-CAN) session establishment. If PCC rules are different than QoS parameters received in the subscriber profile, Anchor SFA modifies the Pre provisioned Service Flow QoS parameters accordingly and executes Service flow modification/establishment procedures.

The QoS Description is used to control data path packet forwarding, prioritizing, rate shaping, etc. Deep packet inspection and Differentiated services IP layer QoS mechanism is supported in ASN-GW to enforce relative priority of packets based on their code points marking.

LTE: In LTE Network, MME receives 'EPS subscribed QoS profile' from the HSS for each Access Point Name (APN) permitted for the subscriber. It contains the bearer level QoS parameter values for that APN's default bearer (QoS Class Identifier (QCI) and Allocation and Retention Priority (ARP)) and that APN's Aggregate Maximum Bit Rate (AMBR).

MME/S-GW sends Evolved Packet System (EPS) bearer QoS parameters received in subscriber profile to P-GW to establish bearer path with P-GW. Based on the applied policy, negotiated QoS parameters are sent back to MME/S-GW. The MME uses the assigned QoS parameters for requesting eNB to establish Radio bearers and no QoS negotiation supported between eNB and EPC.

The bearer level (i.e. per bearer or per bearer aggregate) QoS parameters like QCI, ARP, Guaranteed Bit Rate (GBR), Maximum Bit Rate (MBR), and AMBR are used in S-GW to control bearer level packet forwarding, prioritizing, rate shaping, etc. The QCI scalar value is mapped to traffic class, DiffServ Code Point, traffic handling priority, etc. ARP is used to decide whether a bearer establishment / modification request can be accepted or rejected in case of resource limitations.

In WiMAX and LTE Network access gateways, Packet classification, prioritization, rate shaping, scheduling and differentiated services IP layer QoS mechanism needs to be supported for providing end-to-end QoS. These procedures can be implemented as common data path function for both networks.

G. *Data path function*

WiMAX ASN-GW: ASN-GW receives packet flow list and associated QoS description from the AAA server. This contains packet flows identified by Packet Data Flow Identifier (PDFID) to be supported for the user in both UL and DL direction. Every PDF is associated with QoS Identifier which provides the list of QoS attributes to be used for this Packet Flow. ASN-GW allocates service Flow Identifier (SFID) unique per direction for each packet flow received. This SFID is used to map the data path packets to the specific services using associated classifiers. The SFID does not change when MSS is relocated to another ASN-GW.

The QoS attributes like Minimum Reserved Traffic Rate, Maximum Reserved Traffic Rate, Maximum Latency, Traffic Priority, etc as per [3] are used to support BE, rtPS, nrtPS, UGS and ErtPS scheduling types.

The user plane packets are filtered using classifier rule attributes (Classification Rule Priority, IP TOS/DSCP Range and Mask, etc as per [3]) to identify specific packet forwarding treatment to be applied.

Additional Data Path functions:

1. Acts as Mobility Anchor point for inter-BS handovers
2. Supports tunnel per session, per MS, per service flow towards BS, depending on the configuration.
3. Selects the particular tunnel mapped to SFID with associated GRE keys for routing the DL packets to BS.
4. UL packets from UE are received over GRE tunnel from BS, and routed to HA over GRE/IP tunnel.
5. The Uplink (UL) packets received are routed to the local application or to the external node based on packet forwarding rule applied for the service flow.
6. ASN control protocol (R6) is used between ASN-GW and BS to setup GRE tunnel by exchanging GRE Keys with associated parameters. And MIP protocol (R3) is used between ASN-GW and HA to setup IP/GRE tunnel.
7. Supports both data flow and session based UL/DL packet transfer data counter collection for charging.

LTE MME/Serving GW: During attach procedure MME gets Subscriber profile from HSS which contains provisioned service data flows with the list of services to be supported for the user with pre-emption priority, information on subscriber's allowed QoS, including the Subscribed Guaranteed Bandwidth QoS, a list of QoS class identifiers together with the MBR limit, GBR limit for real-time QoS class identifiers, Service Data Flow Template and also subscriber's charging related information. The services are identified by the services id, this provides the most detailed identification specified for flow based charging of a service data flow.

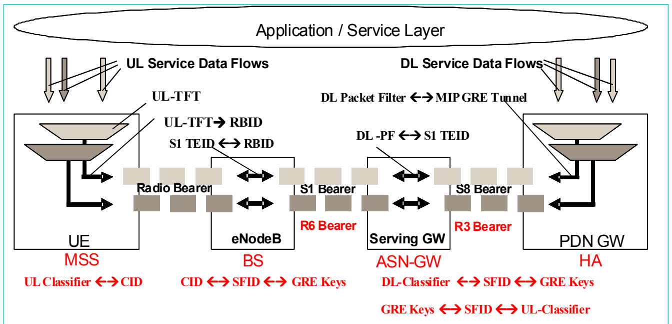
The Service Data Flow Template contains set of service data flow filters required for defining a service data flow matching against IP 5-tuple (source IP address, destination IP address, source port number, destination port number, protocol ID of the protocol above IP). After packet filtering and classification, it is mapped to services ID from which packet control bearer level packet forwarding treatment is identified and applied by S-GW.

The service level (i.e., per SDF or per SDF aggregate) QoS parameters are QCI, ARP, GBR, and MBR. The QCI is mapped to parameters set (Resource Type (GBR or Non-GBR), Priority, Packet Delay Budget, and Packet Loss Rate). The QCI values define generic packet treatment to be used for traffic classes (Conversational, Streaming, Interactive and Background) in edge-to-edge network elements between the UE and the P-GW.

Additional Data Path functions:

1. Acts as Mobility Anchor point for inter-eNB handovers
2. UL packets from UE are received over GTP-U interface, and routed to P-GW over GRE tunnel with associated GRE Keys. And the DL packets received from P-GW are filtered using GRE Keys/TFT and mapped to the service ID. Based on associated TEID, GTP-U tunnel is identified and packets are forwarded to eNB.
3. The UL packets received are filtered and routed to the local application or to the P-GW based on UL TEID/TFTs and packet forwarding rule.
4. GTP-C control protocol is used between S-GW and eNB to setup GTP tunnel. And MIP (PMIP) protocol (S8) is used between S-GW and P-GW to setup GRE tunnel associated with GRE keys. The S-GW allocates GRE Keys used by the PDN GW to encapsulate downlink traffic to the S-GW.
5. Supports both data flow and session based UL/DL packet transfer data counter collection for charging.

LTE and WiMAX packet flow is shown in the Fig 3 below. Both networks use MIP-GRE tunnel between P-GW/HA and S-GW/ASN-GW respectively. But GTP-U tunnel is used in LTE systems between S-GW and eNB, GRE tunnel is used in WiMAX between ASN-GW and BS.



Note: WiMax nodes and their packet classification is marked in **RED** and LTE components are marked in **BLACK**

Fig 3: UL/DL packet flow in WiMAX and LTE networks

Both LTE and WiMAX functions can be supported on a common framework with well defined interface with control application functions for setting up the data path context with required QoS and filtering parameters. The general IP packet forwarding framework is applicable for both the networks.

H. *Mobility Framework*

WiMAX network: ASN-GW creates MSS context when MSS is attached to network. It maintains authentication context, Service Data Flow and associated QoS contexts per MSS as long as MSS is connected.

Handover procedure: When handover trigger is received, serving ASN-GW relays the request to all BS in the list. If BS is connected to different ASN-GW, the request is relayed through target ASN-GW. After successful inter ASN-GW handover, if FA and Authenticator relocation procedures are triggered, then FA (Service Flow and Qos contexts) and Authenticator context may be relocated to target ASN-GW. In case of handover between BSs connected to same ASN-GW, data path switches to target BS on receiving handover confirmation from BS.

IDLE Mode procedure: When MSS state change to IDLE indication is received, ASN-GW acting as paging coordinator, creates Location register with associated parameters related to paging information and MS service flow information. The data path between BS and ASN-GW is de-registered and tunnel with HA is retained. If HA sends any downlink packets when MSS in IDLE mode, ASN-GW buffers the incoming packet(s) and triggers paging procedure to request MSS to exit from the IDLE mode.

During IDLE mode, ASN-GW receives periodic location update from the MS. If ASN-GW receives, location update with different paging coordinator ID (PCID), it relays the request to current paging coordinator ASN-GW with relocation indication to retrieve MS context from the current PC. On successful completion of PC relocation, new PC sends relocation indication to Anchor FA/DPF, for receiving DL packet indication.

LTE network: MME creates UE context when UE is attached to network. It maintains authentication context, bearer context and associated QoS contexts per UE as long UE is in the current tracking area. As part of the successful attach procedures, MME creates initial context with default bearer for IP connection functions. And this default bearer remains established throughout the lifetime of the PDN connection. UE/Network can trigger dedicated bearer establishment based on the PDN services needed to be accessed by UE.

Handover procedure: When UE is in CONNECTED state, MME maintains radio bearer connection context and support handover between eNB with/without S-GW relocation and with/without MME relocation. When MME and S-GW are co-located, S-GW relocation results into MME relocation.

In case of inter eNB handover scenario without MME/S-GW relocation, S-GW switches DL packets from P-GW to target eNB once path switch request is received from target eNB. When MME/S-GW relocation is required, serving MME selects the target MME based on selection function and initiate UE relocation procedure with target MME.

IDLE Mode procedure: When UE is moved from CONNECTED to IDLE, all the dedicated bearers are released along with the data path between S-GW and eNB. But data path between S-GW and P-GW are not affected. The S-GW starts buffering downlink packets received from P-GW for the UE in IDLE mode and initiates paging for the "Network Triggered Service Request" procedure. When UE is in IDLE state, MME maintains the UE context as long as it receives periodic Tracking Area Update [1] (TAU) from the UE. Integrity and ciphering should be supported for the NAS messages received in IDLE state. When UE initiates TAU from new tracking area served by different MME, the new MME request the old MME for the context transfer.

Both WiMAX and LTE networks support mobility between 3GPP, 3GPP2 and other wireless networks. But mobility procedures are unique to each network.

I. *IMS support*

IP Multimedia Core Network Subsystem is an overlay to the LTE PS-domain and WiMAX networks. After default bearer or ISF/PPSF establishment, IMS Client on MSS/UE does Proxy- Call Session Control Function (P-CSCF) discovery procedure and initiate IMS registration procedure with P-CSCF. P-CSCF requests the establishment of a new session to the PCRF. The PCRF performs a session binding and identifies the corresponding PCC rules related to IMS signaling for Session Modification for the establishment/activation of the IP-CAN bearers for the IMS signaling.

IMS overlay support and inter-working in both WiMAX and LTE networks is similar but PCC procedure for handling session/bearer binding is specific to each network.

J. *Policy and Charging Control Function*

WiMAX Network: In WiMAX network, ASN-GW hosts PCEF function as part of anchor-SFA to support enforcement of PCC rules and/or charging in the ASN. PCRF communicates with PCEF using Gx interface based PCC-R3-P reference point. PCEF is responsible for the following:

- Serving as the PCEF in the ASN (A-PCEF) by receiving PCC rules from PCC-R3 reference point and performing bearer binding.
- Mapping between IP-level QoS provided in PCC rules and WiMAX Access QoS
- Reporting charging information

LTE Network: In LTE network, PCC function is split between different gateway functions:

- Full PCEF with service-aware end-user charging is located only in P-GW.
- Bearer binding for the S1 interface in case of S5/S8 (PMIP) is performed in the SGW. To enable S1 bearer binding in case of S5/S8 (PMIP), Gx based off-path signalling is applied from the PCRF to S-GW.

Both WiMAX and LTE network PCC framework is complaint to 3GPP TS 23.203. The bearer binding procedures can be commonly implemented as part of data path function, both network use Gx based interface with the PCRF but

1) TAU is similar to Location Area update procedures *applying PCC rules to data bearer is specific to network specific applications.*

K. Network Management Function

The Operation Administration and Management (OA&M) procedures fault, configuration, performance measurement, security and software upgrade framework can be common for both the network functions.

L. User Plane Interfaces

WiMAX network:

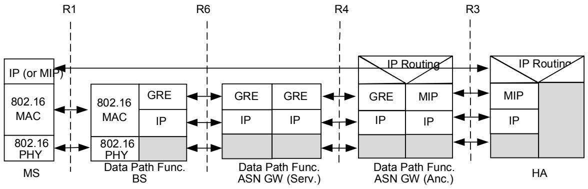


Fig 4: WiMAX network U-Plane protocols

LTE network:

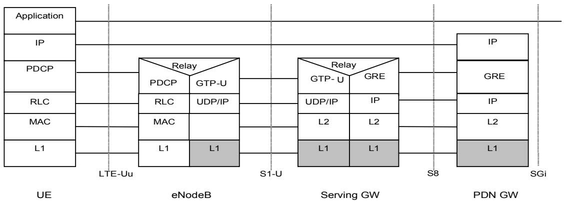


Fig 5: LTE network U-Plane protocols

As Shown above in the Fig 4 and 5, User plane transport protocols are using common IP layer and associated functions in both LTE and WiMAX networks. User plane function of these gateways can be implemented as common data path function as described above in sections F and G. Required transport protocol context with GRE or GTP-U for the data transport with specific security attributes, packet forwarding treatment, filtering rules, QoS attributes, etc can be set up by network specific application using well defined interface with the data path function.

M. Control Plane Interfaces

WiMAX network:

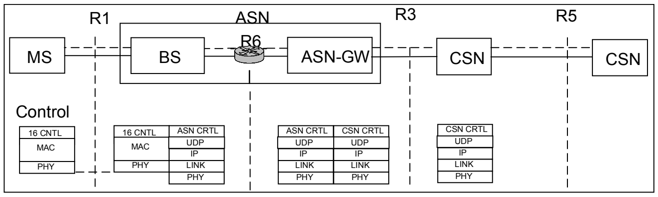


Fig 6: WiMAX network C-Plane protocols

LTE network:

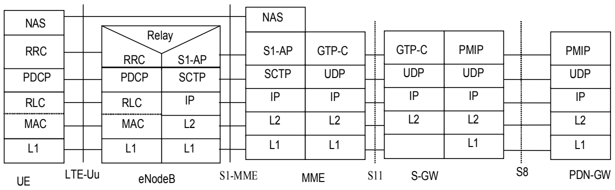


Fig 7: LTE network C-Plane protocols

As shown in Fig 6, in WiMAX network ASN-GW is using UDP as transport protocol to carry ASN-CTRL, MIP, AAA and other protocol packets. And as shown in Fig 7, in LTE network MME and S-GW are using SCTP and UDP transport protocols to carry GTP-C, PMIP and S1-AP packets. All lower layer functions up to these transport protocols can be hosted together with data path function on a dedicated processor. With this, Security and QoS procedures applicable for the signaling procedures will be handled as part of data path function.

IV. CONCLUSION

In this paper, Key features of WiMAX ASN-GW and LTE MME/S-GW are discussed in detail to Highlight similarities and differences of the various procedures. Brief analysis is provided to identify the common and specific procedures for each network. One of the possible architecture to implement the NextGen Wireless Access gateway is outlined. This single node solution can support both WiMAX and LTE networks access gateway function and will have considerable advantageous in the hybrid network deployments.

REFERENCES

[1] IEEE 802.16-2004 October 2004, Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, August 2004.

[2] IEEE 802.16e-2005 March 2006, Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands

[3] WiMAX Forum, WiMAX Forum Network Architecture, Stage 2 and stage 3, Release 1.2.2.

[4] WiMAX Policy and Charging Control – Release 1.5.

[5] WiMAX Forum Network Architecture – IP Multimedia Subsystem (IMS) Interworking- Release 1.5

[6] 3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access – Release 8.

[7] 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses – Release 8

[8] 3GPP TS 23.203, Policy and Charging Control Architecture, Release 8.

[9] 3GPP TS 23.228, "IP Multimedia Subsystem (IMS)", Release 8

[10] 3GPP TS 33.203 "3G security; Access security for IP-based services", Release 8

[11] 3GPP TS 33.102: "3G Security; Security architecture" – Release 8

[12] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture" – Release