A Review of Mobility Supporting Tunneling Protocols in Wireless Cellular Networks

Zeeshan Abbas, Wonyong Yoon
Department of Electronics Engineering
Dong-A University, Busan
South Korea

***Abstract*—With recent technology advancements mobility support is one of the major needed parameters by any wireless or mobile networks. Continuous mobile movement from one cell to another or from one network to another requires continuous mobility support. Previously, tunneling protocols employment was the technique to support UE's inter or intra network mobility. More specifically, GRE, GTP, MIPv6 or PMIPv6 were employed for mobility support. In tunneling encapsulation of one protocol over another protocol is performed to deliver IP packet during inter network or intra network handover. In terms of usage scenario of each tunneling protocol, tunnel establishment, data transfer and tunnel release, an overview and comparison of tunneling protocols is presented in this paper. 3GPP and WLAN interworking, and GAN based usage scenarios and supported tunneling mechanisms has been discussed. Some insights regarding security, multiplexing, multiprotocol and packet sequencing support are also provided for each tunneling protocol.**

Keywords*—*Tunneling; mobility; 3GPP; WLAN; interworking

I. Introduction

With the recent advancements in wireless and mobile networks there is need of mechanisms that can support coexistence of multiple radio access technologies. These technologies should not also coexist but also provide seamless mobility between different radio access technologies. Looking on this thing various developments has been performed from different researchers. However, basically mechanism that provides support seamless handover are depends on tunnel that is created between different radio access technologies for establishing connectivity to the core network. Generic Routing Encapsulation (GRE) is one of the pioneering tunneling protocols that provide support for switching from one radio access technology to another. This protocol is based on encapsulation of one protocol over another protocol. Proxy Mobile IPv6 (PMIPv6) is mostly used for encapsulation. It is also specified in standard as IP session continuity signaling being used by Evolved Packet Core (EPC). This protocol supports mobility of terminals or UEs for various radio access technologies, e.g., Long Term Evolution (LTE) radio access, WLAN, 3G radio access, WiMAX and radio standards from 3GPP2. Basically, protocols just like PMIPv6 and MIPv6 manage the path for IP packets destined for different network or radio access technology. This kind of mobility approaches not also support seamless handover but also ensures efficient utilization of network resources, user privacy and network security.

Another type of tunneling protocol being used for supporting terminals mobility is GPRS Tunneling protocol (GTP). This protocol is also being used between different 3GPP core network entities. In which once a tunnel is established between different network entities then IP packets can be encapsulated and tunneled between these network entities. IP Security (IPSec) is another tunneling protocol used for protecting data integrity of wireless devices being delivered to the core network entities. This is the security association mechanism in which mutual authentication between terminal and access gateway is performed. Negotiation of security keys for a connection is also performed. Packets in IPSec are encrypted and encapsulated within a new packet with new control information and are delivered by IPSec tunnel from terminal or user equipment to access gateway.

II. Background

In Fig. 1, we have tried to cover architectural elements needed for supporting different type of technologies. As we can see in upper part of the figure 2G network components that will be needed for Voice Call Continuity (VCC) which provides support for anchoring circuit switched voice call in IP infrastructure by transferring speech path between these two domains transparently to end user [1, 2]. Tunnel is needed when VCC supported UE moves from 3G/4G network to 2G network then signaling messages between MME and Interworking solution Function for 3GPP2 1xCS (1xCS IWS) are transferred using S102 Tunnel. Another tunnel named IPSec is being used in Generic Access Network (GAN) and Wireless Local Area Network (WLAN) between UE to GAN Controller and ePDG network components respectively. GTP, PMIPv6 and GRE tunnels are used for secure data transfer between different network components like SGW, PGW, SGSN MME from 3G or 4G networking technologies, respectively.

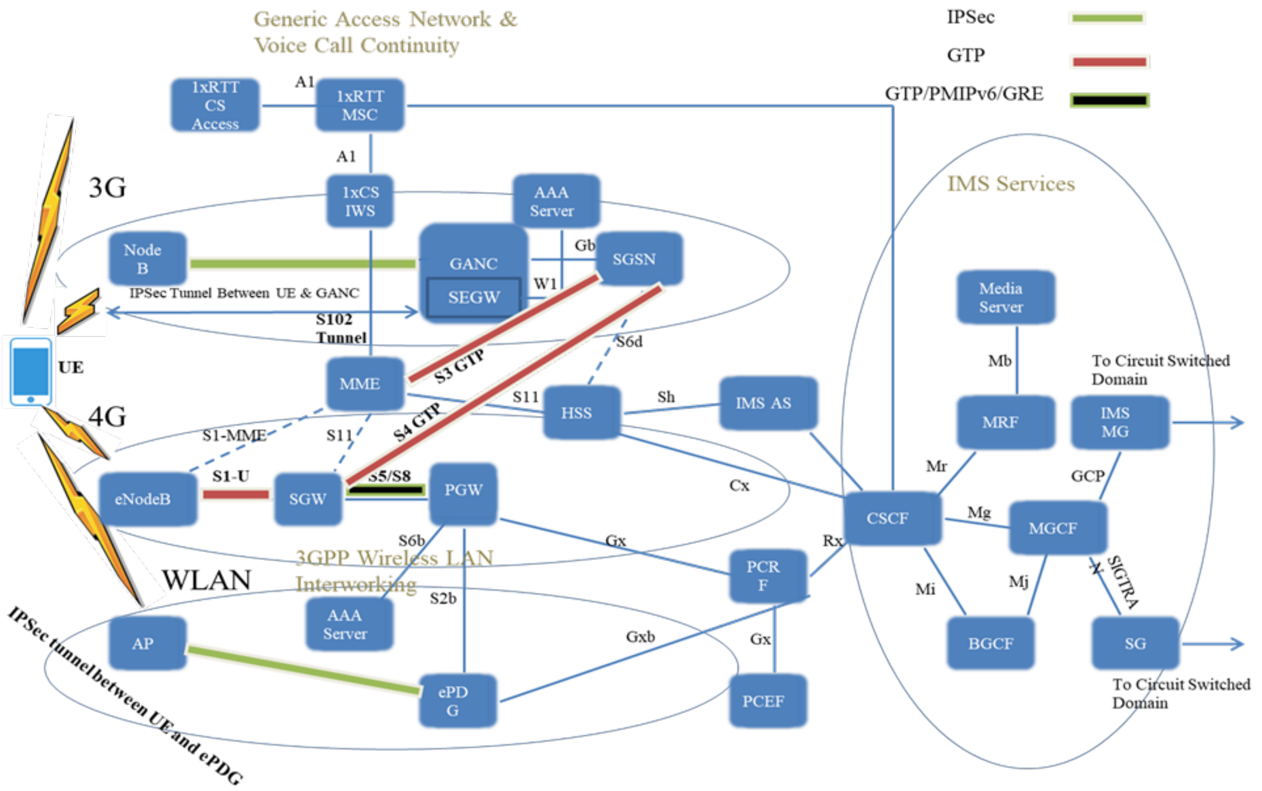

Fig. 1. Generic Heterogeneous Networks and Interworking Architecture.

However, authors in [3, 4] surveyed various tunneling protocols for supporting mobility. These tunneling protocols are IP based tunneling protocols used to support mobility in IPv6 based networks. Implementation of these protocols depends on usage scenario, as scenario can be host based, network based, soft handoff or hard handoff based Micro and Macro Mobility usage scenarios. Depending on these each different protocol is discussed for supporting seamless handover and mobility support in IPv6 networks [5]. However, some authors discussed these protocols from centralized or distributed point of view. Implementation of these protocols can be dependent on centralized or distributed support of these protocols. Authors suggested that use of protocols like GTP and PMIPv6 in centralized fashion may be not an effective solution because of single point of failure and scalability issues. So, they think that some distributed usage scenarios should be discussed. However, they mentioned the few by employing some already defined techniques just like de coupling control and user plane.

III. Tunneling Protocols for 3GPP

A. *Generic Routing Encapsulation (GRE)*

Currently, various protocols support encapsulation of one protocol over another. Generic Routing encapsulation (GRE) is among one of the encapsulation protocols which provide support for encapsulation of one protocol over another protocol. Simple IP packets are encapsulated in GRE header and transmitted to different intervening routers [6, 7].

1) Usage scenarios: GRE tunnel implementation is based on GRE encapsulation of data from network entity to another network entity over some other mobility supported protocol i.e., PMIPv6. Basically, GRE is used with PMIPv6 that can support mobility for UE if it is moved from one network to another. Then data can be transferred by using GRE encryption and PMIPv6 mobility support option [8].

2) Tunnel establishment and data transfer: Fig. 2 illustrates GRE tunnel establishment procedure. By adopting PMIPv6 as mobility support protocol and employing GRE as data encryption technique for security purposes a tunnel can be established between as Mobility Access Gateway (MAG) and Local Mobility Anchor (LMA). GRE key option is needed for establishing a tunnel between MAG and LMA. GRE keys are exchanged between these two entities by using Proxy Binding Update (PBU) defined in PMIPv6. MAG and LMA establish a GRE tunnel by the agreed GRE keys to transmit uplink and downlink traffic [9].

3) Tunnel release: Once a tunnel is established for data transfer it can also be removed from network. By following some steps tunnel between MAG and LMA can removed. MAG transmits a PBU message to LMA for release of the LMA binding. LMA completes release of binding by transmitting an acknowledgment message to MAG. During tunnel release process all resources just like IPv6 Home Network Prefix, IPv4 Home Address, Downlink and Uplink GRE Key, GRE Tunnel Tear-down deletion and de-assignment is performed [6].

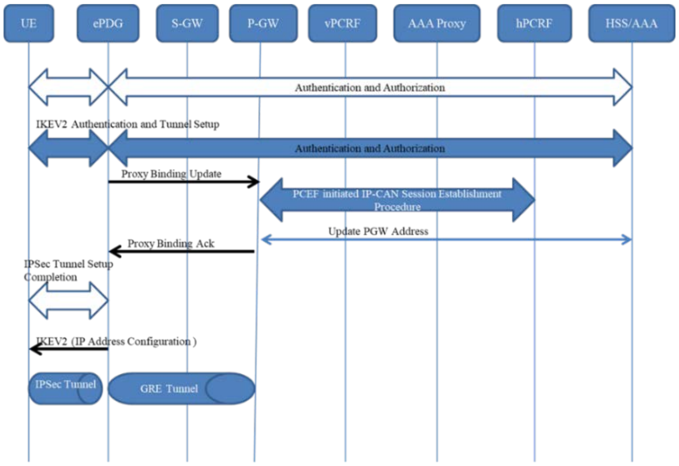
UE
ePDG
S-GW
P-GW
vPCRF
AAA Proxy
hPCRF
HSS/AAA
Authentication and Authorization
IKEV2 Authentication and Tunnel Setup
Authentication and Authorization
Proxy Binding Update
PCEF initiated IP-CAN Session Establishment Procedure
Update PGW Address
Proxy Binding Ack
IPSec Tunnel Setup Completion
IKEV2 (IP Address Configuration)
IPSec Tunnel
GRE Tunnel

Fig. 2. An Initial Attachment over GRE and Tunnels Establishment.

B. *GPRS Tunneling Protocol (GTP)*

For transporting IP packets with in network or outside network GPRS tunnels concept is used. In which a tunnel is established between different network entities for successful transmission of IP packets within the network. For this purpose, a tunnel is established between different end points for data transmission and a unique identity named Tunnel End Point Identifier (TEID) is assigned to IP packets. Packets being received at different end points are forwarded based on their TEID's. According to 3GPP technical documents there are two types of protocols used in GTP one is GTP-U [6] and other is GTP-C [10]. GTP-U is used for delivering user data to different network entities. However, GTP-C is used to exchange control plane messages among different network entities.

1) Usage scenarios: GPRS Tunneling protocol implementation can be observed in various scenarios depending on type of interfaces being used. As, previously in [11] enhanced GTP was employed for GSM network which adopted Packet Data Protocol (PDP) to reduce tunneling overhead being faced at that time. Basically, one usage scenario that can be observed in different standard documents is 3GPP wireless LAN interworking. GTP can be implemented on different interfaces for providing connectivity between different network interfaces. GTP implementation using 3GPP plus trusted Non-3GPP access over S2a interface or 3GPP plus untrusted Non-3GPP access over S2b are provided to support usage scenarios. Seamless IP session continuity is supported between cellular networks and wireless local networks without the change of the address [12].

2) Tunnel establishment and data transfer: Fig. 3 illustrates GTP tunnel establishment procedure. First of all, Non-3GPP IP Access specific procedures takes place after that UE Authentication and authorization is performed by looking into HSS where subscription information of the user/subscriber is stored. 3GPP AAA transmits a reply to trusted non-3GPP network with information on all the authorized APNs and additional PDN GW selection. Upon completion of authentication and authorization, L3 attach procedure specific to non-3GPP access is initiated. UE transmits a request for session start from the obtained list of available APNs. Otherwise, PDN gateway selection procedure takes place. If UE connection to the particular APN becomes successful, trusted non-3GPP network transmits a message for making a connection (IMSI, APN, RAT type, Trusted non-3GPP IP Access TEID, etc.) message to PGW. After that PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF. PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules and event triggers. Then, the selected PDN GW informs 3GPP AAA server about PDN GW identity and the APN corresponding to the UE's PDN connection and also information about selected S2a protocol (GTP). PDN GW replies with a create session response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Protocol Configuration Options and Cause message to the Trusted non-3GPP IP Access, with IP address assigned to the UE. Then, GTP tunnel is set up between trusted Non-3GPP network and the packet gateway. Once a tunnel is established, data transfer can take place [12].

3) Tunnel release: To release the tunnel or detach procedure is accomplished by following a procedure. First of all, a mobile or Trusted Non-3GPP network starts an access specific detach procedure from the network. Access technology specific detach trigger procedure is performed for tunnel release. Then, active bearers for UE and PDN connection are deactivated by the trusted non-3GPP IP Access sending a Delete Session Request to the gateway. Then the gateway informs AAA of PDN detach. PDN Gateway on receiving message deletes IP session associated with that particular UE. PDN Gateway and PCRF perform PCEF-Initiated IP CAN Session Termination Procedure. Then PDN Gateway sends a message to acknowledge with delete session response message. Finally, resources for trusted Non-3GPP network will be freed [9].

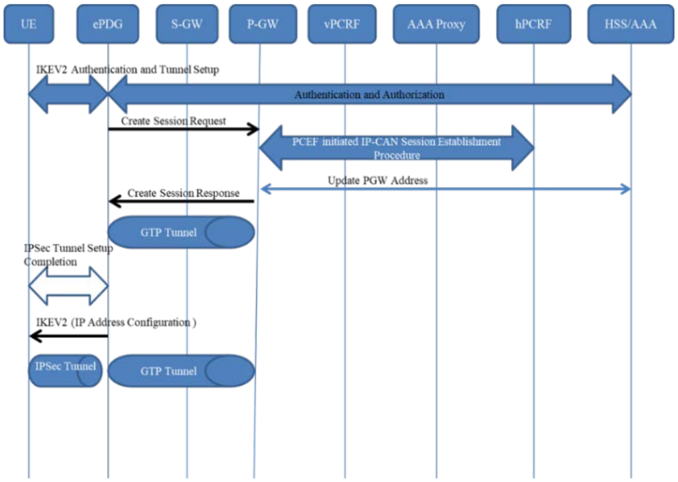
UE
ePDG
S-GW
P-GW
vPCRF
AAA Proxy
hPCRF
HSS/AAA
IKEV2 Authentication and Tunnel Setup
Authentication and Authorization
Create Session Request
PCEF initiated IP-CAN Session Establishment Procedure
Update PGW Address
Create Session Response
GTP Tunnel
IPSec Tunnel Setup Completion
IKEV2 (IP Address Configuration)
IPSec Tunnel
GTP Tunnel

Fig. 3. An Initial Attachment over GTP and Tunnels Establishment.

C. *Proxy Mobile IPv6*

For supporting mobility of end users in different networks a protocol was introduced named Mobile IPv6. This protocol allows the users to keep online with mobility within IPv6 network. The basic concept behind this protocol is each node has a home address when connected to some network. However, by moving to another network it is associated to other network based on Care-of–Address (CoA). The address provides information on UE's latest point-of-contact. The protocol supports IPv6 nodes to store information on UE's home address and CoA. It also allows to send packets destined for UE by utilizing UE CoA. Tunneling mechanisms like GTP or GRE can also be used to support MIPV6 data transfer [13].

In network-initiated mobility control, network side maintains of the location of UE and triggers the necessary mobility message exchange. A proxy mobility agent is responsible for performing the mobility signaling with home agent. UE upon reaching to another network will try to connect to an access link. MAG over the link will perform authorization for network-based mobility. After authorization UE can perform address configuration and can move anywhere in PMIPv6 domain [14]. Authors in [15] presented some analytical studies regarding PMIPv6 where LMA is placed far from current MAG. In that case PMIPv6 will suffer from significant handover delay. So, based on mechanisms for supporting mobility whether predictive or reactive the authors in [15-18] suggested some enhancements to reduce handover latency, signaling cost and network utilization. Similarly, authors in [19-22] investigated messaging, data transmission, and tunneling overhead of different protocols with respect to PMIPv6.

1) *Usage scenarios:* Proxy Mobile IPv6 implementation is basically for supporting for transfer of control information between different network entities whether it is 3GPP or WLAN for handling network-based mobility. Basically, GRE is used with PMIPv6 that can support mobility for UE if it is moved from one network to another. Then data can be transferred by using GRE encryption and PMIPv6 mobility support option.

2) *Tunnel establishment and data transfer:* Fig. 4 illustrates PMIPv6 tunnel establishment procedure. For establishing tunnel between different network entities PMIPv6 follows some procedure in order to establish connection. Entities deployed with PMIPv6 protocol are named as MAG and LMA. MAG entity acts as SGW in 3GPP or ePDG in WLAN network environment. MAG initiates the tunnel establishment procedure for UE attach for the first time. MAG first transmits a PBU with APN to LMA. This results in LMA binding for UE's PDN attach. LMA completes binding by transmitting an acknowledgment to MAG. In the case of multiple PDN support for a single APN, each PDN connection ID is included in the acknowledgment. MAG generates a downlink GRE key distinct from any existing connection. MAG assigns a Fully Qualified PDN Connection Set Identifier. This identifies a group of PDN connections belonging to a group of UEs. MAG Includes LMA User Plane Address Mobility Option if the MAG supports the capability to receive from the LMA an alternate LMA address for user plan. On PBU reception, LMA selects the PDN based on APN information delivered in the PBU. LMA allocates an IPv4 or IPv6 address on receipt of PBU. Also, LMA generates uplink GRE key distinct from existing PDN connection's uplink traffic for that UE. After tunnel is established between different network entities data can be transferred by using any type of encapsulation, i.e. GRE [6].

3) *Tunnel release:* MAG initiates the release of PDN connection to tear down an existing PDN connection with LMA. MAG first transmits a PBU to LMA to delete the LMA binding for the UE's PDN connection. LMA completes deletion of the binding by transmitting a PBA to MAG. During tunnel release procedure, all resources such as IPv6 prefix, IPv4 address, Downlink and Uplink GRE Key, GRE Tunnel Tear-down deletion and de-assignment is performed [6].

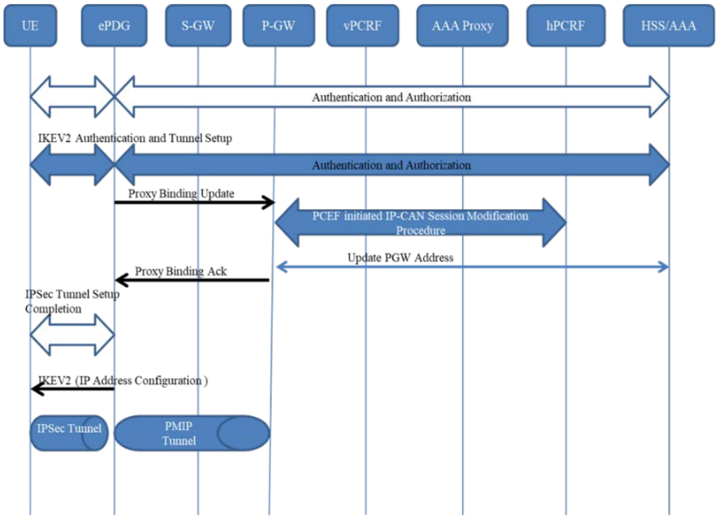
UE
ePDG
S-GW
P-GW
vPCRF
AAA Proxy
hPCRF
HSS/AAA
Authentication and Authorization
IKEV2 Authentication and Tunnel Setup
Authentication and Authorization
Proxy Binding Update
PCEF initiated IP-CAN Session Modification Procedure
Update PGW Address
Proxy Binding Ack
IPSec Tunnel Setup Completion
IKEV2 (IP Address Configuration)
IPSec Tunnel
PMIP Tunnel

Fig. 4. An Initial Attachment over PMIPv6 and Tunnels Establishment.

D. *Dual Stack Mobile IPv6*

Dual Stack Mobile IPv6 (DSMIPv6) is an extension to MIPv6 functions. It allows UEs to request their home agent to forward IP packets addressed to their home address, and to their IP care-of address. A dual stack mobile can simultaneously enable both IPv4 and IPv6. Hence, two different mobility protocols are not needed at the same time [23, 24].

1) *Usage scenarios:* Usage scenarios can be based on for either 3GPP-WLAN interworking or mobility support within 3GPP. Solutions that enable seamless mobility between 3GPP-WLAN interworking and within 3GGP are needed such that current 3GPP based packet sessions can be served without interruption to UE's received service perception during the change of access network [25].

2) *Tunnel establishment and data transfer:* If UE is already on 3GPP Access and discovers the 3GPP I-WLAN domain, it may decide to change point-of-contact to

discovered 3GPP I-WLAN. For that purpose, UE will establish an IPSec Tunnel with ePDG. After establishing IPSec tunnel UE sends Binding Update message to HA and informs HA of its IP address. As a result of BU, DSMIPv6 tunnel is set up between UE and HA. After tunnel establishment, data plane messages can be transmitted using I-WLAN [25]. Fig. 5 illustrates DSMIPv6 tunnel establishment procedure.

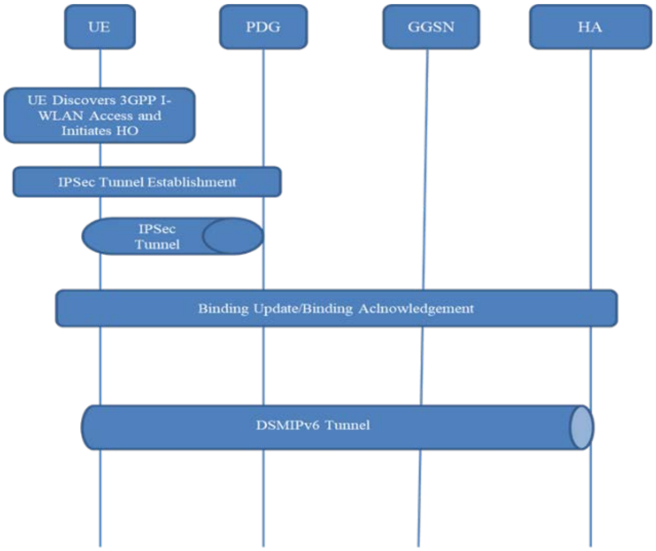
UE
PDG
GGSN
HA
UE Discovers 3GPP I-WLAN Access and Initiates HO
IPSec Tunnel Establishment
IPSec Tunnel
Binding Update/Binding Aclnowledgement
DSMIPv6 Tunnel

Fig. 5. An Initial Attachment over DSMIPv6 and Tunnels Establishment.

E. IP Secure Tunnel (IPSec)

For securing data integrity and for transmission another form encryption protocol is IPSec. This protocol provides support to encapsulate original IP packet and assign a new IP header to deliver the encapsulated data to other side of the network. Authentication header is also included in together with ESP when IPSec is being used in tunnel mode [26-28] for providing security and mobility support.

1) Usage scenarios: UE with connectivity to trusted or un-trusted non-3GPP access needs some security architecture to connect to 3GPP EPS. User identity confidentiality and devices identity confidentiality is needed in 3GPP EPS and Non-3GPP access for providing connectivity for non-3GPP access devices to 3GPP EPS [29].

2) Tunnel establishment and data transfer: If connection of UE is already established with non-3GPP access network then that UE can also access 3GPP access network by using this security mechanism, during which a secure tunnel is established. An example of such tunnel establishment is one between UE and ePDG. They first exchange some messages known as IKE_SA_INIT. Then UE sends user identity and APN information in IKE_AUTH step. It initiates negotiation of child security associations. ePDG sends Authentication and Authorization Request message to the 3GPP AAA Server containing user identity and APN information. Then 3GPP AAA server checks authentication vectors from HSS/HLR, and stores the information like IMSI and EAP-AKA requested authentication method in HSS. Then, 3GPP AAA server initiates authentication challenge by transmitting a reply to ePDG. ePDG then responds with its identity and a certificate. It sends the AUTH parameter to protect the previous message it sent to the UE. Message sent by 3GPP AAA server is also attached in that response message. UE checks the authentication parameters and responds to the authentication challenge. Then, the ePDG transmits the EAP-Response/AKA-Challenge message to the 3GPP AAA. AAA checks whether the authentication response is correct. If everything is correct, AAA shall initiate the Subscriber Profile Retrieval. It registers to the HSS and checks user's subscription whether it is authorized for non-3GPP access. If all checks are done, AAA transmits a final answer to ePDG. Information consists of MSK (EAP-Master-Session-Key-AVP). ePDG uses the MSK to authenticate IKE_SA_INIT step signalings. The EAP Success/Failure message is delivered to the UE over IKEv2. UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. ePDG checks the correctness of the AUTH sent by the UE. ePDG calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. Then, AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters. Now IKEv2 negotiation ends [29].

In Table I given below, we have some insights of each tunneling technique. First of all is security mechanism that should be supported by each tunneling protocol. Of the above-mentioned protocols IPSec supports complete security mechanism. In IPSec, Authentication Header (AH) protocol provides data origin authentication. Encapsulating Security Payload (ESP) supports data confidentiality [26]. Similarly, GRE provides some security by providing a four-byte key field for the purpose of origin authentication [3]. While regarding GTP security can be provided by assigning a unique tunnel end point identifier. Another key feature for each tunneling protocol is support for multiplexing which means supporting multiple simultaneous end devices. Separate tunnels may be set up; however separate tunnels impose processing overhead and increased delay for tunnel establishment. So, a better option is to share one tunnel among all end devices. A unique field is needed in tunneling IPSec provides this by Security parameter index. However, GRE and GTP provide multiplexing support by using GRE key field and GTP TEID field, respectively [6, 12]. Multiprotocol support is also needed by each tunneling protocol. GRE provides multiprotocol support as it was defined as general encapsulation protocol. However, IPSec fails to provide support for multiple protocols. Another important parameter for each protocol is packet sequencing. IPSec has sequence number such that in-order delivery of packets can be feasible.

TABLE I. COMPARISON OF TUNNELING PROTOCOLS

Protocol	**Security**	**Tunnel Establishment and Configuration**	**Tunnel Management**	**Support for Multiplexing**	**Support for Multi-protocol**	**Support for Packets Sequence**	**Standardizing Body**	**Overview**
GRE [6, 30, 31]	Yes (four-byte key field)	Network Explicit	No	Yes (Using Key field)	Yes	No	IETF	Encapsulation of one protocol over another protocol
GTP [12, 32]	Yes (IPSec ESP with encryption and integrity protection)	Network management Explicit	Yes (Create or Delete Session or bearer)	Yes (TEID will provide that kind of support)	Yes	Yes	3GPP	IP based Transport Protocol
PMIPv6 [14, 33]	Yes (chained-tunnel approach provides hop-by-hop based security protection)	Network Management Explicit (PBU & PBA)	Yes (PBU and PBA containing Uplink and Downlink GRE keys stored in Binding Cache)	Yes (GRE key option will provide support)	Yes (PIMPv6 with GRE encapsulation)	Yes (GRE key field)	IETF	Localized mobility management
DSMIPv6 [23, 33]	Yes (IKEv2 based IPSec Security Association)	Client or Host initiated tunnel establishment (PBU & PBA)	Yes (PBU containing Key Management Mobility Option)	No (Attach needs to be done for separate PDNs)	Yes (I-WLAN Attach with mobility service)	No	IETF	Support MN roaming over IPV6 or IPv4 networks and transmission of IPv4/v6 packets over the tunnel to HA
IPSec [26, 30, 31]	Yes (complete build in security)	IKE interchange Implicit	No	Yes (via Security Parameter Index)	No	Yes (sequence number field)	IETF	Security and protecting data integrity

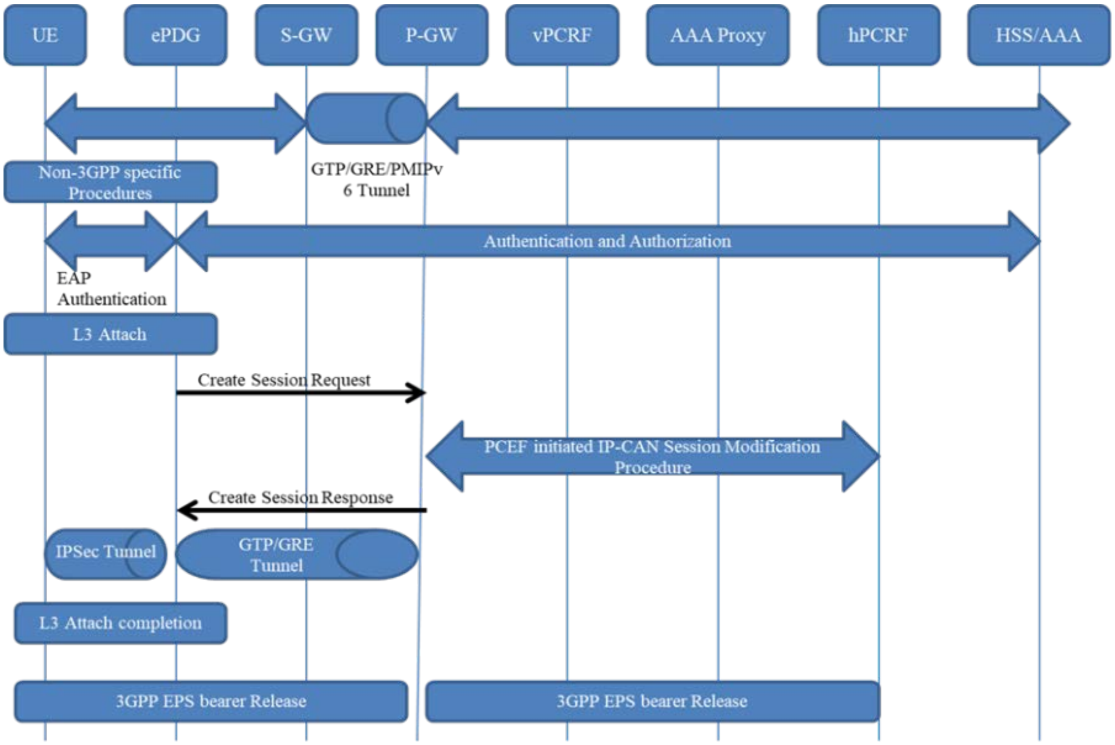

Fig. 6. A Simple 3GPP to WLAN Session Mobility Scenario and Tunnels Establishment.

Fig. 6 represents a generic session mobility scenario in which different tunneling protocols can be employed for handling mobility and data transfer. Initially Non-3GPP intrinsic L2 signaling is completed. Then EAP authentication procedure is started between UE Trusted Non-3GPP and AAA. As authentication reply by AAA, a group of all the authorized APNs plus additional PDN gateway selection is returned to the access gateway. Upon completion of authentication and authorization, non-3GPP radio specific L3 attach procedure is initiated. Then, ePDG transmits a message to establish a data session to the gateway. PDN gateway initiates the IP CAN Session Establishment Procedure with the PCRF and the PCRF provides the APN-AMBR and Default Bearer QoS to the PDN GW in the response message. In response to the create session request message PGW sends a create session response message caching the all required information. After that session is established successfully and ePDG is also authenticated by the UE. IP session between UE and P-GW is now established. Packets from UE to ePDG are tunneled using IPSec Tunnel and then onward using some other tunneling protocol i.e., GRE or GTP [34].

IV. Tunneling Protocols for 3GPP-WLAN Interworking

Radius or diameter based 3GPP WLAN interworking is discussed in [35] which represents some network some network components WLAN UE, WLAN Access Network (WLAN AN), 3GPP AAA Server and Home Subscriber Server (HSS) database. To connect to WLAN, WLAN UE uses a SIM or USIM (UMTS Subscriber Identity Module) containing the authentication keys for the mobile subscriber. To connect UE to 3GPP network, WLAN Access Network (WLAN AN) plays a role of anchor between them. 3GPP AAA performs authentication and authorization for UE. When the WLAN AN receives a WLAN UE connection request, it may perform an initial access negotiation with the WLAN UE to obtain identity information and then pass this information to the 3GPP AAA server as part of an authentication/authorization request. WLAN AN may be RADIUS or Diameter-based. The 3GPP AAA Server matches data from the authentication/ authorization request with information in a trusted database, called a Home Subscriber Server (HSS). If a match is found, and the subscriber's credentials are correct, the 3GPP AAA server responds with a reply to WLAN AN. This indicates the acceptance of the request. Otherwise or if a problem is found with the subscriber's credentials, 3GPP AAA returns a reject message. This results in the termination of WLAN UE connection.

Upon establishment of WLAN UE connection, WLAN AN may forward accounting information to 3GPP AAA to record the transaction for future price charging. 3GPP AAA must be able to translate between RADIUS and Diameter (and vice versa), to support connection requests from legacy RADIUS WLAN ANs to the 3GPP network which uses the Diameter protocol. HSS stores subscriber data like keys to complete authentication to allow access for user device. It also performs authorization to enable access to limited service and functions. Overall for interworking support tunneling is the mechanism adopted as discussed in [36]. Also, another mechanism that supports offloading end users from Radio Access Network to WLAN using IPSec transport mode has been discussed in [37] to reduce networking security overhead caused by IPSec Tunnel mode. Fig. 6 illustrates 3GPP to WLAN mobility procedure and required tunnel establishment.

A. Directly Accessing to the Internet

In this case, the Internet is connected through WLAN AN. Users access WLAN AN. IMS AAA is responsible for authentication of users. It uses either the EAP-SIM or EAP-AKA protocol that originates from RADIUS and Diameter WLAN ANs. The SIM-authentication mechanism is used against the subscriber information stored in the HSS. Authentication is performed directly from the WLAN AN. Upon completion of authentication, authorization will return policy information for session establishment [35, 38].

B. Accessing through 3GPP

In this case, users can access connection service to the Internet via a secure tunnel to 3GPP IMS. IP packets are forwarded through tunnel to 3GPP IMS network via WLAN Access Gateway (WAG) and ePDG. WAG acts as a dynamically configured firewall. ePDG is a tunnel end-point. Multiple tunnels are possible to support any number of simultaneous services. ePDG requests authorization separately from the authentication request. For example, WLAN UE may initiate a tunnel towards the ePDG. This is followed by authentication and tunnel establishment [35].

C. Generic Access Network (GAN)

GAN was developed as an advancement of Unlicensed Mobile Access. GAN is another type of network that can coexist with 3GPP core network. User equipment with multiple radios (WLAN and 3GPP) can access 3GPP through GAN. GAN is applied usually through IEEE 802.11 WLAN. Gateway in 3GPP core named as Generic Access Network Controller (GANC) is responsible for handling traffic coming from WLAN. Initially, UE starts working on by default 3G settings when powered on using WLAN. UE connects to appropriate AP. IP address is configured to perform GAN discovery. It establishes an IPSec tunnel with Security Gateway (SeGW). It registers with GANC. If GANC accepts connection UE GAN mode is enabled [39, 40].

1) GAN Discovery and registration: First of all, for GAN mode selection is done during Discovery phase. MS transfers its GAN Mode Support information to GANC. GANC can assign appropriate port on default GANC based on the GAN mode support information provided by MS. During discovery phase, MS obtains the address of default GANC. It also discovers that of associated SEGW. Then it establishes a secure IPSec Tunnel. After sending IP address query for both SEGW and GANC, MS opens a TCP session with GANC. GANC responses with Discovery accept message. After discovery phase, MS initiates registration with default GANC, which can act as the serving GANC after establishment of connection and registration procedure. GAN registration procedure confirms adequate registration of a mobile to the controller. The procedure helps the MS for appropriate GAN mode selection. After establishing a secure tunnel with SEGW and IP address has also been obtained. MS can then send a registration request message to GANC. Information contained in registration request message is current camped cell of MS i.e., GERAN/UTRAN/EUTRAN, Last LAI or TAI, IMSI and information about required GAN services. If GANC accepts registration request it responds by sending register accept message to MS.

Fig. 7 illustrates GAN tunnel establishment procedure using EAP/SIM(AKA) over IKE. In GAN different tunneling protocols are being supported on different levels of network. During establishment of connection to GANC UE establishes an IPSec tunnel with SEGW. The security association of IPSec tunnel is established. Another tunnel protocol used between GANC and GGSN is GPRS Tunneling protocol. This tunnel is established during data transfer from between UE and the network i.e., 2G or 3G. GA-RRC Packet Transport Channel is made for packet switching domain on both sides of network entities. Connection status of GA-RRC is active or inactive. Some triggers are used for GA-RRC PTC state activation. First one is when GANC receives RAB assignment message from GGSN and second one is when GANC receives relocation request from SGSN. When these two triggers happen SGSN includes the information like RAB ID, IP Address and GTP-U TEID in RAB Assignment Request or Relocation Request message sent to GANC. During that time GA-RRC channel on UE is activated by GANC by forwarding the received message from GGSN to UE. After channel activation at UE now that particular UE will be in GA-RRC-Connected PTC-ACTIVE sub state. RAB Assignment is transmitted to GGSN using the same information received already. Upon establishment of PDP context, a mobile may start transmission upward data in GA-RRC PDU. GANC relays the payload part of PDU to SGSN in Iu-PS G-PDU message. SGSN transmits downward user data in Iu-PS G-PDU toward GANC. The message includes MS TEID already received during RAB Assignment Request or Relocation Request messages [39]. On the other hand, previously some work also focused on mobility management. Mechanism for supporting GAN handoff is presented in [41], in which authors focused on adaptive keep alive interval messages for allocation of resources and mobility management and reducing the handoff failure probability. Similarly, authors in [42] presented a VoLGA based solution. They suggested to with some software and interface addition connectivity for VoLGA can be provided.

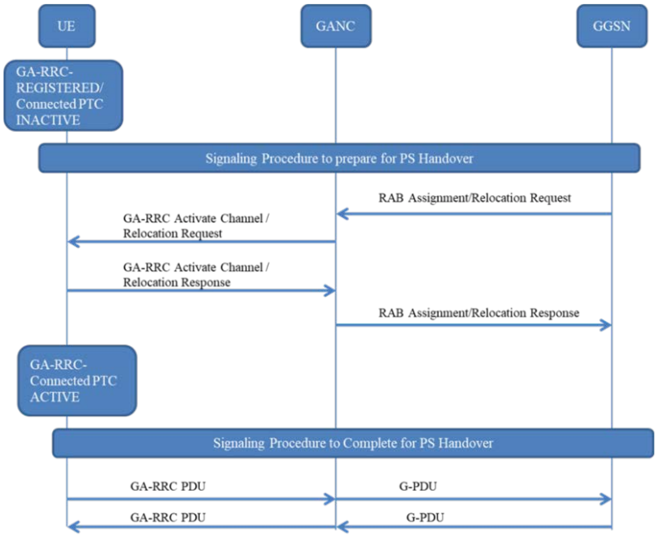
UE
GANC
GGSN
GA-RRC-REGISTERED/ Connected PTC INACTIVE
Signaling Procedure to prepare for PS Handover
RAB Assignment/Relocation Request
GA-RRC Activate Channel / Relocation Request
GA-RRC Activate Channel / Relocation Response
RAB Assignment/Relocation Response
GA-RRC-Connected PTC ACTIVE
Signaling Procedure to Complete for PS Handover
GA-RRC PDU
G-PDU
GA-RRC PDU
G-PDU

Fig. 7. Simple GAN RAB Assignment and Relocation Mechanism and Tunnel Establishment.

V. Conclusion

In this paper, an in-depth review of various tunneling protocols employed by various wireless and mobile networks for supporting mobility is presented. Tunnel establishment, data transfer, tunnel release and respective usage scenarios for each tunneling protocol has been considered for systematic and thorough comparison of existing tunneling protocols. An insight of each tunneling protocol is provided and discussed. Specifically, mechanisms like security, multiplexing support, multiprotocol support and packets sequencing support has been discussed. Focusing usage scenarios, tunneling mechanism being used in 3GPP wireless LAN interworking, and Generic Access, Network (GAN) has been discussed.

Acknowledgment

This work was supported by the Dong-A University research fund. W. Yoon is the corresponding author.

References

[1] A. K. Salkintzis, M. Hammer, I. Tanaka, and C. Wong, "Voice call handover mechanisms in next-generation 3GPP systems," Communications Magazine, IEEE, vol. 47, pp. 46-56, 2009.

[2] J. Namakoye and R. Van Olst, "Performance evaluation of a voice call handover scheme between LTE and UMTS," in AFRICON, 2011, 2011, pp. 1-5.

[3] D. Saha, A. Mukherjee, I. S. Misra, and M. Chakraborty, "Mobility support in IP: a survey of related protocols," Network, IEEE, vol. 18, pp. 34-40, 2004.

[4] W. Lili, G. Jianfeng, Y. Ilsun, Z. Huachun, G. Deyun, Y. Kangbin, and K. Pankoo, "Survey on distributed mobility management schemes for Proxy mobile IPv6," in Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, 2014, pp. 132-138.

[5] N. Chuangchunsong, S. Kamolphiwong, T. Kamolphiwong, R. Elz, and P. Pongpaibool, "Performance evaluation of IPv4/IPv6 transition mechanisms: IPv4-in-IPv6 tunneling techniques," in Information Networking (ICOIN), 2014 International Conference on, 2014, pp. 238-243.

[6] D. Farinacci, T. Li, S. Hanks, D. Meyer, and a. P. Traina, "RFC 2784, Generic Routing Encapsulation (GRE)," RFC 2784, March 2000.

[7] G. Yu, L. Breslau, N. Duffield, and S. Sen, "GRE Encapsulated Multicast Probing: A Scalable Technique for Measuring One-Way Loss," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 2008, p. 1.

[8] 3GPP, "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols," in 3GPP TS 29.275, ed., July 2020.

[9] 3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)," in 3GPP TS 29.281, ed, September 2021.

[10] 3GPP, "Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C)," in 3GPP TS 29.274, ed, December 2021.

[11] T. Shiao-Li Charles, "Enhanced GTP: an efficient packet tunneling protocol for General Packet Radio Service," in Communications, 2001. ICC 2001. IEEE International Conference on, 2001, pp. 2819-2823 vol.9.

[12] 3GPP, "Study on S2a Mobility based on GPRS Tunnelling Protocol (GTP) and Wireless Local Area Network (WLAN) access to the Enhanced Packet Core (EPC) network (SaMOG)," in 3GPP TS 23.852, ed, September 2013.

[13] C. Perkins, Ed., Johnson, D., and J. Arkko, "RFC 6275 Mobility Support in IPv6," RFC 6275, July 2011.

[14] S. Gundavelli, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "RFC 5213,Proxy Mobile IPv6",," RFC 5213, August 2008.

[15] L. Jun and F. Xiaoming, "Evaluating the Benefits of Introducing PMIPv6 for Localized Mobility Management," in Wireless

Communications and Mobile Computing Conference, 2008. IWCMC '08. International, 2008, pp. 74-80.

[16] J. Inwhee and L. Hyojin, "An efficient inter-domain handover scheme with minimized latency for PMIPv6," in Computing, Networking and Communications (ICNC), 2012 International Conference on, 2012, pp. 332-336.

[17] L. Meng-Hsuan, C. Whai-En, and H. Chao-Hsi, "HF-PMIPv6: An enhanced fast handovers for network-based mobility management," in Advanced Infocom Technology 2011 (ICAIT 2011), International Conference on, 2011, pp. 1-7.

[18] A. Rasem, M. St-Hilaire, and C. Makaya, "A comparative analysis of predictive and reactive mode of optimized PMIPv6," in Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, 2012, pp. 722-727.

[19] H. Ali-Ahmad, M. Ouzzif, P. Bertin, and X. Lagrange, "Comparative performance analysis on dynamic mobility anchoring and proxy mobile IPv6," in Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on, 2012, pp. 653-657.

[20] P. Seung Yoon and J. Jongpil, "On Pointer Forwarding Based Mobility Management for Cost-Optimized Proxy Mobile IPv6 Networks," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on, 2013, pp. 29-36.

[21] G. Song, X. Wang, X. Li, J. Huo, and Y. Liu, "Cost Analysis of a Novel Mobility Management: Interworking between PMIPv6 and MIPv6," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on, 2012, pp. 1-4.

[22] L. Jong-Hyouk, Y. Zhiwei, J. M. Bonnin, and X. Lagrange, "Dynamic tunneling for network-based distributed mobility management coexisting with PMIPv6," in Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on, 2013, pp. 2995-3000.

[23] H. Soliman, Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[24] K. Mitsuya, R. Wakikawa, and J. Murai, "Implementation and Evaluation of Dual Stack Mobile IPv6," in Asia BSD Conference (AsiaBSDCon2007), 2007.

[25] 3GPP, "Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems," in 3GPP TS 23.327 ed, September 2016.

[26] S. a. K. S. Kent, "RFC 4301, Security Architecture for the Internet Protocol," RFC 4301, December 2005.

[27] K. Byoung-Jo and S. Srinivasan, "Simple mobility support for IPsec tunnel mode," in Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, 2003, pp. 1999-2003 Vol.3.

[28] J. Younchan and M. Peradilla, "Tunnel gateway satisfying mobility and security requirements of mobile and IP-based networks," Communications and Networks, Journal of, vol. 13, pp. 583-590, 2011.

[29] 3GPP, "3GPP System Architecture Evolution (SAE); Security Aspects of non-3GPP Accesses," in 3GPP TS 33.403, ed, July 2020.

[30] T. Saad, B. Alawieh, S. Guider, and H. T. Mouftah, "Tunneling techniques for end-to-end VPNs: generic deployment in an optical testbed environment," in Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on, 2005, pp. 859-865 Vol. 2.

[31] A. Zhao, Y. Yuan, Y. Ji, and G. Gu, "Research on tunneling techniques in virtual private networks," in Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on, 2000, pp. 691-697 vol.1.

[32] 3GPP, "3G security; Network Domain Security (NDS); IP network layer security," in 3GPP TS 33.210, ed, July 2020.

[33] 3GPP, "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses," in 3GPP TS 33.402 ed, July 2020.

[34] M. Crosnier, F. Planchou, R. Dhaou, and A. Beylot, "Handover Management Optimization for LTE Terrestrial Network with Satellite Backhaul," in Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd, 2011, pp. 1-5.

[35] 3GPP, "3GPP System to Wireless Local Area Network (WLAN) interworking; system Description," in 3GPP TS 23.234, ed, March 2015.

[36] G. Chai-Hien, L. Yung-Chun, Y. Shun-Neng, and L. Yi-Bing, "A Seamless Multi-link Switch Solution for LTE and Wi-Fi Integrated Networks," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on, 2013, pp. 19-23.

[37] D. Migault, D. Palomares, E. Herbert, Y. Wei, G. Ganne, G. Arfaoui, and M. Laurent, "E2E: An Optimized IPsec Architecture for Secure and Fast Offload," in Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, 2012, pp. 365-374.

[38] D. Celentano, A. Fresa, M. Longo, and A. L. Robustelli, "Improved Authentication for IMS Registration in 3G/WLAN Interworking," in Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on, 2007, pp. 1-5.

[39] 3GPP, "3GPP. Generic Access Network (GAN); Stage 2. ," in 3GPP TS 43.318, ed, July 2020.

[40] J. Kellokoski, "Challenges of the always-best-connected enablers for user equipment in Evolved Packet System," in Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on, 2012, pp. 174-180.

[41] C. Kai-Hsiu and C. Jyh-Cheng, "Handoff Failure Analysis of Adaptive Keep-Alive Interval (AKI) in 3GPP Generic Access Network (GAN)," Wireless Communications, IEEE Transactions on, vol. 10, pp. 4226-4237, 2011.

[42] O. Stepaniuk, "Voice over LTE via Generic Access (VoLGA) as a possible solution of mobile networks transformation," in Modern Problems of Radio Engineering, Telecommunications and Computer, 2010.