JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 4, pp. 639-647, Apr. 2018

3GPP 5G 시스템에서 Trusted Non-3GPP 액세스 연동 기술

강 유 화* · 김 창 기
한국전자통신연구원

Trusted Non-3GPP Access Interworking in 3GPP 5G System

Yoohwa Kang * · **Changki Kim**
Electronics and Telecommunications Research Institute

[요 약]

3GPP 5G 시스템은 서로 다른 액세스 네트워크를 하나의 인터페이스로 수용하는 Common Core (코어) 네트워크 구조를 지향하고 있으며, 이를 기반으로 한 3GPP 5G 시스템 Phase 1 (Release 15) 규격에서는 Untrusted Non-3GPP 액세스를 3GPP 액세스와 동일한 인터페이스로 코어 네트워크와 연결되는 하나의 액세스 네트워크로 수용하고 있다. Untrusted Non-3GPP 액세스를 수용하기 위하여, 3GPP 5G 시스템은 RAN 위치에 N3IWF (Non-3GPP Inter-Working Function)을 두고 UE와 코어 네트워크 간의 인터페이스를 지원하며, Trusted Non-3GPP 액세스 네트워크의 수용은 Release 16를 목표로 하고 있다. 본 논문에서는 3GPP 5G 시스템에서 Trusted Non-3GPP 액세스를 수용하기 위한 네트워크 구조 및 시그널링, 각 기능 구조 등의 설계 방안을 제안하고, 이를 기반으로 구현한 5G 시스템의 동작 결과를 보여준다. 제안된 방식은 N3IWF가 Untrusted/Trusted 액세스 네트워크를 모두 수용할 수 있도록 설계되었고, Untrusted/Trusted와 같이 서로 다른 종류의 Non-3GPP 액세스를 수용하더라도 N3IWF의 기능은 동일하다는 장점이 있다. 구현된 시스템 결과물은 3GPP 5G 시스템 Phase 1 구조를 그대로 수용하며 Trusted Non-3GPP 액세스 네트워크를 위한 별도의 추가기능 없이도, 액세스 독립적인 인터페이스를 코어 네트워크로 제공할 수 가능성을 보여준다.

[Abstract]

A common core network is the one of main architectural principles in 3GPP 5G System which has common interfaces with different multiple accesses. 3GPP 5G System Phase 1 (Release 15) supports Untrusted Non-3GPP access as well as 3GPP access with common interfaces. Non-3GPP Interworking Function (N3IWF) has been defined to interface with a UE and a core network for supporting Untrusted Non-3GPP access in 3GPP Release 15. However, interworking with Trusted Non-3GPP access is under study to be completed in 3GPP 5G System Phase 2 (Release 16). Therefore, this paper proposes a Trusted Non-3GPP access network architecture and related signaling procedures, and then the implementation based on the proposal shows how to interwork between Trusted Non-3GPP access and the 5G core network. In our proposal, N3IWF can interwork with either Untrusted or Trusted Non-3GPP access without any architectural modification or addition of 3GPP 5G system Phase 1.

색인어 : 3GPP, 5G 시스템, Non-3GPP, 신뢰 액세스, N3IWF
Key word : 3GPP, 5G System, Non-3GPP, Trusted access, N3IWF

http://dx.doi.org/10.9728/dcs.2018.19.4.639

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-CommercialLicense(http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 16 April 2018; **Revised** 24 April 2018
Accepted 21 April 2018

***Corresponding Author; Yoohwa Kang**
Tel: +82-42-860-6364
E-mail: yhkang@etri.re.kr

Ⅰ. 서 론

5G 서비스는 브로드밴드 액세스뿐만 아니라, 다양한 IoT 센서 네트워크, 자율주행 자동차 등 서로 다른 서비스 요구사항과 다양한 액세스 네트워크를 수용한다. Enhanced Mobile Broadband (eMBB), Massive IoT (mIoT), Ultra Reliable Low Latency Communication (URLLC)는 5G 대표 서비스로 3GPP 5G 시스템은 이와 같은 다양한 서비스 요구사항을 만족하기 위한 표준규격작업을 진행하고 있다. 특히, LTE, 5G RAN, WLAN, Fixed 등 다양한 종류의 액세스 네트워크를 동시에 수용하기 위한 Access agnostic 코어 네트워크 구조를 제시하고자 한다.

3GPP 4G EPS (Evolved Packet System)에서도 3GPP 액세스 네트워크뿐만 아니라, WLAN, Fixed와 같은 Non-3GPP 액세스 네트워크도 수용하였다. 현재 대다수의 스마트폰은 LTE, WiFi 인터페이스를 모두 가지고 있으며 애플리케이션의 특징에 따라 선택적으로 사용할 수 있다. 또한, 서비스 향상을 위하여 LTE와 WLAN을 RAN level에서 결합하는 LAA (Licenses Assisted Access), LWA (LTE Wi-Fi Aggregation), LTE-U 와 같은 기술도 개발되었다.

이처럼, 5G 시스템에서도 Non-3GPP 액세스 수용을 반드시 필요로 하며, 3GPP 5G 시스템 (5GS: 5G System) Phase 1에서는 Untrusted Non-3GPP 액세스를 수용하기 위한 규격이 2017년 12월에 완료되었으며[1], [2], Trusted Non-3GPP 액세스를 수용하기 위한 규격작업은 2020년 Phase 2 (Release 16)을 목표로 현재 스터디작업이 시작되었다. 아직 Trusted Non-3GPP 액세스를 수용하기 위한 방안은 제시되지 않았으며, 이에 본 논문에서는 3GPP 5G 시스템에서 Untrusted Non-3GPP 액세스 네트워크와 Trusted Non-3GPP 액세스를 동시에 수용할 수 있는 네트워크 구조를 제안하고자 한다. 제안된 네트워크 구조를 기반으로 Trusted Non-3GPP 액세스 네트워크 기능을 구현하고, 5G 시스템과 연동하는 것을 보여줌으로써 실현 가능성을 검증하고자 한다.

3GPP 5G 시스템에서 Trusted Non-3GPP 액세스 연동을 위한 시스템 모델을 제안하기 위하여, 2장에서는 먼저 관련연구를 살펴보고, 3장에 5G 시스템의 Trusted Non-3GPP 액세스 연동 구조 및 관련 시그널링 프로시져를 제안한다. 4장에서는 구현된 Trusted Non-3GPP 액세스 시스템의 동작을 확인하고, 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

3GPP 5G 시스템 Phase 1 (Release 15) 시스템은 2018년 9월에 규격 작업이 완료될 예정이며, 2017년 12월에 코어 네트워크 구조 및 시그널링 규격작업은 1차로 완료되었으며 현재 규격에서는 Untrusted Non-3GPP 액세스만을 수용하고 있다. Trusted Non-3GPP 액세스는 5G 시스템 Phase 2 (Release 16)에서 지원할 예정이며, 현재 3GPP FS_5WWC (Study on the Wireless and Wireline Convergence for the 5G system architecture)[3] 워크아이템에서 스터디 작업이 진행 중이며 구체적인 규격 작업은 2019년에 본격적으로 이루어질 것으로 예상된다.

본 논문에서 5G 시스템에서의 Trusted Non-3GPP 액세스 연동 방안을 제안하기에 앞서, 관련하여 4G 시스템에서의 Trusted Non-3GPP 액세스 연동 구조 및 5G 시스템에서 지원하는 Untrusted Non-3GPP 액세스 구조를 살펴본다.

2-1 4G Non-3GPP 액세스

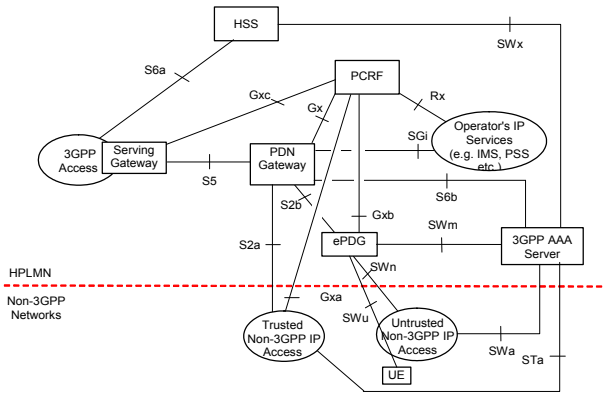

그림 1. EPC 망과 신뢰 WLAN 액세스 구조[4]
Fig. 1. Trusted WLAN access to EPC[4]

WLAN이 사업자에 의해 운영되는 Trusted 망인 경우에는 그림 1에서 Trusted Non-3GPP IP Access에 해당되며, 이는 Trusted Non-3GPP 액세스로 TWAN (Trusted WLAN Access Network)으로 정의하고 EPC (Evolved Packet Core)와 인터페이스한다[4]. TWAN은 WLAN AN (Access Network), TWAG (Trusted WLAN Access Gateway), TWAP (Trusted WLAN AAA Proxy)으로 구성되고, UE 쪽으로는 WLAN AN이 WiFi AP와 연결되고, 코어 네트워크 쪽으로는 TWAG이 PDN GW와 연결되며, TWAP은 3GPP AAA 서버로 연결된다.

그림 1에서 보는 바와 같이, 3GPP 4G 시스템인 EPS는 3GPP 액세스, Untrusted Non-3GPP 액세스, Trusted Non-3GPP 액세스가 서로 다른 각각의 액세스 시스템을 각각 가지고 (예: eNB, ePDG, TWAG 등) , 코어 네트워크와 인터페이스하기 위한 프로토콜 스택도 서로 다르다. 3GPP 액세스와 Non-3GPP 액세스 시그널링 체계는 각각 서로 다른 것을 사용하며, Non-3GPP 액세스 경우에는 시그널링과 데이터 모두 PDN GW를 통해서 EPC로 연동할 수 있다.

2-2 5G Non-3GPP 액세스

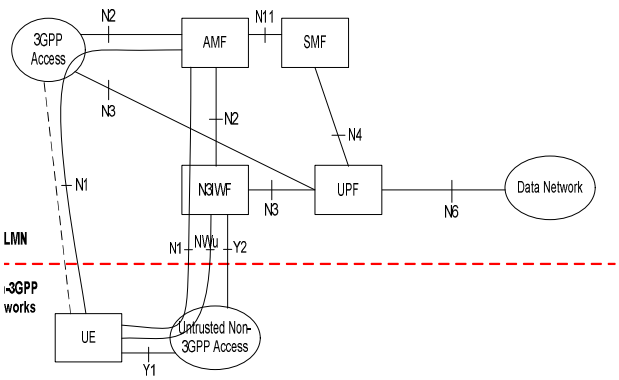

그림 2. 5G 코어 네트워크와 Non-3GPP 액세스 구조[1]
Fig. 2. 5G Core Network with Non-3GPP access[1]

5G 시스템은 액세스 의존성을 최소화하는 common 코어 네트워크를 지향하며, 다양한 종류의 액세스 네트워크를 단일 인터페이스로 수용한다. 그림 2에서 보는 바와 같이 3GPP 액세스와 Non-3GPP 액세스가 동일한 N1 (Reference point between the UE and the AMF), N2 (Reference point between the (R)AN and the AMF), N3 (Reference point between the (R)AN and the UPF) 인터페이스로 코어 네트워크로 연결된다[1]. 따라서, 하나의 UE는 액세스 종류에 상관없이 3GPP 코어 네트워크 시스템에 N1, N2 인터페이스로 시그널링을 수행하고, N3 인터페이스로 서로 다른 액세스 네트워크와 코어 네트워크 간에 데이터 전송이 이루어진다.

3GPP 5G 시스템 Phase 1에서는 그림 2와 같이 Untrusted Non-3GPP 액세스를 수용하기 위한 규격과 만들어졌으며, 현재 Trusted Non-3GPP 액세스를 수용하기 위해 스터디 작업이 시작되었다.

Ⅲ. 5G Trusted Non-3GPP 액세스 연동

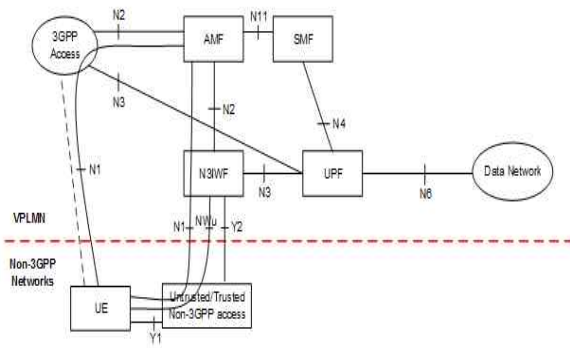

그림 3. 5GS와 비신뢰/신뢰 Non-3GPP 액세스 구조
Fig. 3. 5G Untrusted/Trusted Non-3GPP Access to 5GS

본 논문에서는 5G 시스템에서 Trusted Non-3GPP 액세스도 Untrusted Non-3GPP 액세스와 동일하게 N3IWF로 연동하는 모델을 제안한다. 그림 3은 3GPP 5G 시스템 Phase 1 구조를 기반으로 Untrusted 또는 Trusted Non-3GPP 액세스 네트워크 모두 N3IWF와 연동할 수 있음을 나타낸다. 그림 3에서 Non-3GPP 액세스는 Untrusted WLAN 또는 Trusted WLAN이 가능하며, NWu, Y2 인터페이스는 Untrusted/Trusted Non-3GPP 액세스에 따라 다음의 표 1에서 보는 바와 같이 달라질 수 있다.

표 1. Non-3GPP 액세스 레퍼런스 포인트
Table 1. Non-3GPP Access Reference Points

	Untrusted Non-3GPP	Trusted Non-3GPP
Y1	Reference point between the UE and the Non-3GPP access (e.g. WLAN)	
Y2	Reference point between the untrusted Non-3GPP access and the N3IWF	Reference point between the trusted Non-3GPP access and the N3IWF for establishing secure tunnel(s)
NWu	Reference point between the UE and N3IWF for establishing secure tunnel(s)	Reference point between the UE and N3IWF

Untrusted Non-3GPP 액세스 경우에는 NWu 인터페이스에 IPSec 터널을 설정하여, UE와 코어 네트워크 간에 control plane, user plane 데이터를 시큐어하게 전달할 수 있도록 한다. 반면, Trusted Non-3GPP 액세스 경우에는 Y2 인터페이스에 IPSec 터널을 설정하여 Trusted WLAN을 구성하고, 이 때 UE의 IPSec 기능은 필요로 하지 않는다. 따라서, N3IWF는 IPSec 기능을 공통으로 가지며 Untrusted WLAN 경우에는 NWu 인터페이스에, Trusted WLAN 경우에는 Y2 인터페이스에 IPSec 터널을 생성한다. Y2 인터페이스의 IPSec 터널 암호화 (encryption) 기능을 필요하지 않는 경우에는 off 시킨 후 IPSec 터널링 (tunnelling) 기능만 사용할 수도 있다.

다음의 3-1절에서는 먼저 N3IWF를 통해 Trusted Non-3GPP 액세스와 연동하기 위한 UE, 코어 네트워크 간의 시그널링 프로시져를 제안하고, 3-2절에서는 제안된 시그널링 프로시져를 처리하기 위한 N3IWF, AP, UE 기능 정의 및 블록 단위의 설계를 제안하며, 3-3절에서는 control plane, user plane 프로토콜 스택을 보여준다.

3-1 시그널링 프로시져

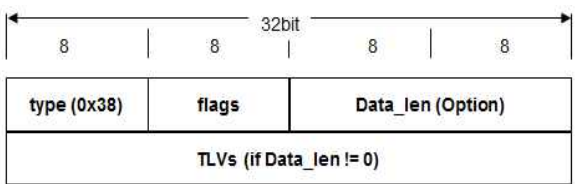

그림 4. EAP-5G 해더
Fig. 4. EAP-5G Header

Trusted Non-3GPP 액세스 연동을 위하여, N3IWF는 NAS over IKE가 아닌 NAS over EAP 방식으로 NAS 메시지를 전달하며, NAS over EAP 방식은 Untrusted/Trusted Non-3GPP 액세스에 공통으로 사용될 수 있다. 따라서 Untrusted Non-3GPP 액세스 네트워크에서 UE – N3IWF 간의 IPSec 터널에서 NAS 메시지 전달과 Trusted Non-3GPP 액세스 네트워크에서 UE – N3IWF 간의 NAS 메시지 전달은 동일한 방식으로 이루어진다. 이때 사용하는 EAP Type은 별도로 정의된 값 (0x38)으로 EAP-5G라고 한다 (그림 4).

표 2. EAP-5G 해더 플래그 값
Table 2. EAP-5G Header flags value

flags	설명
0x80	Data_len included
0x40	Fragment
0x20	EAP5G-Start
0x10	EAP5G-Success
0x08	EAP5G-Registration Complete

그림 4에서 보는 바와 같이 EAP-5G의 Header는 flags와 optional data_len으로 이루어져있으며, Data_len 이 있을 경우 TLVs가 추가된다. flags 값은 표2와 같이 할당하였으며, TLVs 는 Type-Length-Value의 일반적인 TLV 형태로 이루어져 있고 현재는 NAS (0x1) 및 UE_Service_IP (0x3) 두 가지를 정의하였다.

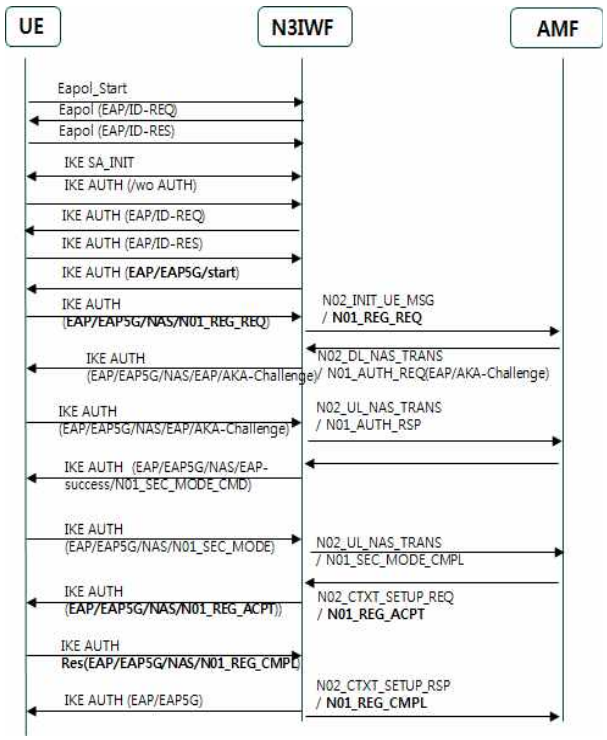

그림 5. 접속 등록 절차
Fig. 5. Registration Procedure

그림 5는 EAP-5G 프로토콜을 사용하여 N3IWF에서의 Registration 절차를 나타낸다. N3IWF는 UE를 대신하여 NAS Registration 메시지를 N2 인터페이스로 전송하는 역할을 수행한다. 또한 EAP 프로토콜을 이용하여 NAS 메시지를 AMF (Access and Mobility Management Function) 로 전송한다. UE – AMF 사이의 NAS 시그널링을 송수신하기 위해서, 먼저 UE – N3IWF 사이의 EAPoL, IKEv2[5]와 N2 시그널링을 이용한 EAP 메시지를 AMF로 전송한다.

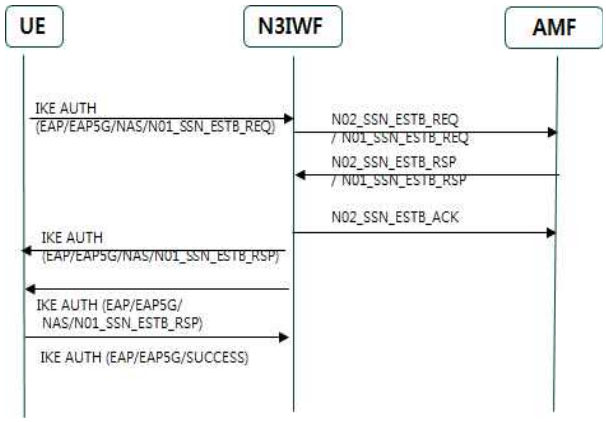

그림 6. 세션 설정 절차
Fig. 6. Session Establishment Procedure

그림 6은 데이터 전송을 위한 PDU Session Establishment 절차를 나타낸다. UE – AMF 사이의 NAS 시그널링을 송수신하기 위해서, 먼저 UE – N3IWF 사이의 EAPoL, IKEv2와 N2 시그널링을 이용한 Session Establishment 단계이다.

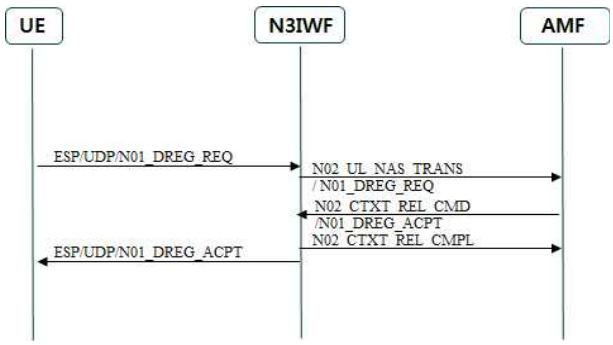

그림 7. 접속 해제 절차
Fig. 7. De-registration Procedure

그림 7은 De-Registration 절차를 나타내며, UE – AMF 사이의 NAS 시그널링을 송수신하기 위해서 먼저 UE – N3IWF 사이의 NASoL과 IPSec, 그리고 N2 시그널링을 이용한 UE의 De-registration 동작을 수행한다.

3-2 N3IWF, AP, UE 기능 설계

N3IWF는 UE가 Non-3GPP 액세스 네트워크를 경유하여 5G 코어 네트워크에서 연결을 할 수 있는 역할을 수행한다. Non-3GPP 액세스를 통한 5G 서비스를 위해서는 N3IWF 및 UE, WiFi AP의 추가적인 개발이 필요로 하며, 이를 위해 wpa_supplicant, hostapd Open source를 사용하여 WiFi Access 및 802.1x 기능을 추가하고, AP에는 추가적으로 별도의 IKE Client/Server 기능을 개발하였다.

1) N3IWF 기능

N3IWF는 AP와 IPSec 터널을 생성하고, AP와 함께 IKEv2/IPSec 프로토콜의 종단점이 된다. 또한, 5G 코어 네트워크에 연결된 N2 (Control plane), N3 (Data plane) 인터페이스의 종단점이 되며, UE와 AMF 간에 전달되는 NAS (N1) 시그널링에 대한 릴레이를 수행한다. 그리고, PDU session과 관련된 N2 시그널 처리 및 PDU session 데이터 전송을 위한 IPSec SA를 생성하고, UE와 UPF (User Plane Function) 사이에 UL(Uplink)/DL(Downlink) 패킷에 대한 릴레이 및 IPSec, N3 터널에 대한 De-capsulation과 En-capsulation을 수행한다.

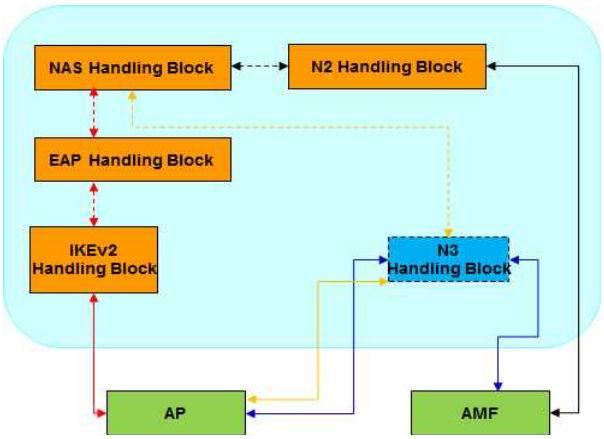

그림 8. N3IWF 블록도
Fig. 8. N3IWF Block Diagram

그림 8은 N3IWF 기능 블록도이며, N3IWF 내 NAS Handling 블록은 AP로부터 수신된 NAS 메시지를 N2처리 블록과 연동하고, Registration Complete 이전에는 AMF로부터 수신된 NAS 메시지를 EAP 처리 블록과 연동한다. EAP Handling 블록은 UE와 N3IWF 사이에서 5G EAP 종단 처리를 수행한다. IKEv2 Handling 블록은 AP와의 IKEv2 시그널링을 수행하고, NAS 처리 블록으로 수신된 EAP 메시지를 IKEv2를 통해 AP로 전달하며, AP로부터 IKEv2를 통해 수신된 EAP 메시지를 NAS 처리 블록으로 전달한다. N2 Handling 블록은 N3IWF와 AMF 사이의 N2 시그널링을 담당하며, NAS 처리 블록으로 수신된 N1 메시지를 N2 인터페이스를 통해 AMF로 전달하고, AMF로부터 N2 인터페이스를 통해 수신된 N1 메시지를 NAS 처리 블록으로 전달한다. N3 Handling 블록은 UE로 부터의 PDU 트래픽 처리 수행하여 코어 네트워크 UPF로 패킷을 전달하고, NAS 처리 블록으로부터 수신한 시그널링 패킷을 IPSec 패킷으로 En-capsulation하고 AP로부터 수신된 시그널링 패킷을 IPSec 패킷으로 De-capsulation하여 NAS 처리 블록으로 전달한다. AP로 부터 받은 IPsec 패킷을 (PDU 데이터) 수신하여, GTP 패킷으로 암호화 처리하여 UPF로 전달하고, 또는 그 반대의 동작을 실행한다. N3IWF는 ESP[6]로 들어온 사용자 트래픽을 UPF로 전송하는데 사용한다.

2) AP 기능

AP는 IKEv2 Client 로 N3IWF와 IPSec 터널 생성하고, UE와 EAPOL 메시지를 처리한다. PDU session 트래픽을 지원하기 하기 위하여 IPSec SA를 생성하고, UE와 N3IWF 사이의 EAP 메시지 릴레이 및 IPSec/IKEv2를 EAP 메세지 암호화를 수행한다.

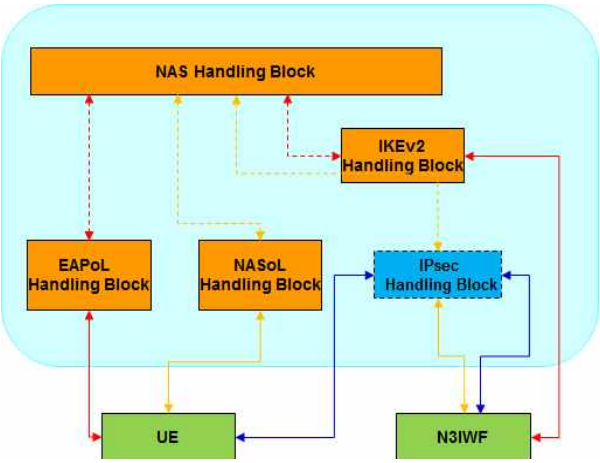

그림 9. AP 블록도
Fig. 9. AP Block Diagram

그림 9는 AP 기능 블록도이며, NAS Handling 블록은 Registration Complete 이전에는 UE로부터 수신된 NAS 메시지를 IKEv2 처리 블록과 연동하고, Registration Complete 이후에는 UE로부터 수신된 NAS 메시지를 IPSec처리를 위하여 LBAP와 연동한다. 또한, Registration Complete 이전에는 N3IWF로부터 수신된 NAS 메시지를 EAPoL처리 블록과 연동하고, Registration Complete 이후에는 N3IWF로부터 수신된 NAS 메시지를 NASoL처리 블록과 연동한다. EAPoL Handling 블록은 NAS 처리 블록으로 수신된 EAP 메시지를 EAPoL을 통해 UE로 송신하며, UE로부터 수신된 EAP 메시지를 NAS 처리블록으로 전달한다. NASoL Handling 블록은 NAS 처리 블록으로 수신된 EAP 메시지를 NASoL을 통해 UE로 송신하고, UE로부터 수신된 NAS 메시지를 NAS 처리블록으로 전달한다. IKEv2 Handling 블록은 IKEv2 시그널링을 담당하며, NAS 처리 블록

으로 수신된 EAP 메시지를 IKEv2통해 N3IWF로 송신하고, N3IWF로부터 IKEv2를 통해 수신된 EAP 메시지를 NAS 처리 블록으로 전달한다.

3) UE 기능

UE는 NAS 시그널링 메세지를 EAP 메세지에 포함하여 전달하고, UE 세션에 대한 생성/삭제 관리를 수행하며, UE PDU 데이터를 각각 WLAN 인터페이스로 전달한다.

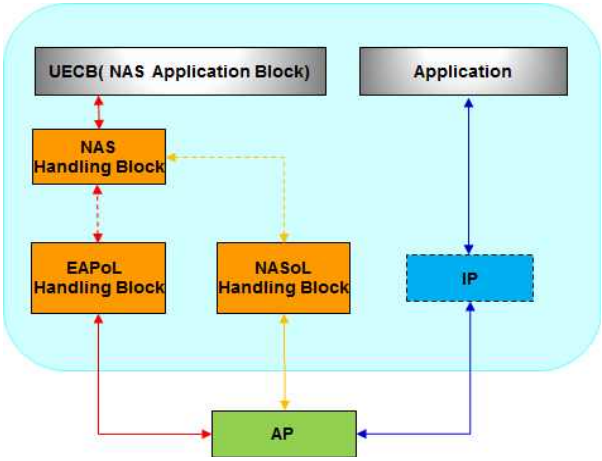

그림 10. UE 블록도
Fig. 10. UE Block Diagram

그림 10에서 NAS Handling 블록은 UECB 블록과 연동 처리하고, UECB으로부터 Registration Req Params 수신하여 EAP 트리거링을 수행하며, Registration Complete 이전에는 EAPoL 처리 블록과 NAS 메시지 송수신을 수행하고, Registration Complete 이후에는 NASoL 처리 블록과 NAS 메시지 송수신을 수행한다. EAPoL Handling 블록은 NAS 처리 블록으로 수신된 EAP 메시지를 EAPoL을 통해 AP와 통신하고, AP에서 수신된 EAP 메시지를 NAS 처리 블록으로 전달한다. NASoL Handling 블록은 EAP success 이후 NAS 처리 블록으로 수신된 NAS 메세지를 NASoL 통해 AP와 통신하고, AP로 부터 수신된 NAS 메세지를 NAS 처리 블록으로 전달한다.

3-3 프로토콜 스택

그림 11은 Registration 프로시져의 초기 접속를 위한 Control plane 프로토콜 스택을 보여준다.

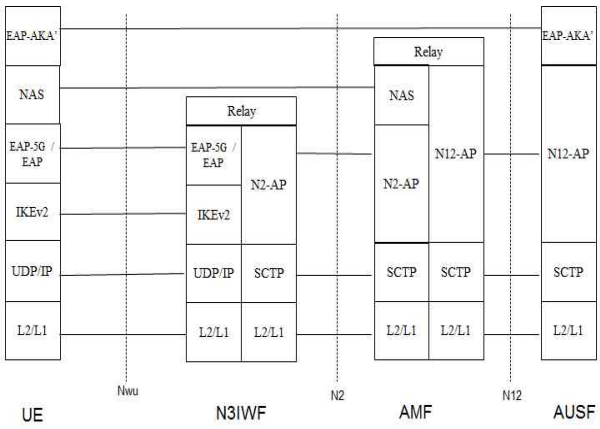

그림 11. N3IWF를 통한 초기 접속을 위한 컨트롤 플레인
Fig. 11. Control Plane for initial attachment via N3IWF

그림 12는 IPsec SA가 완료된 이후에 NAS를 위한 Control plane 프로토콜 스택을 보여준다.

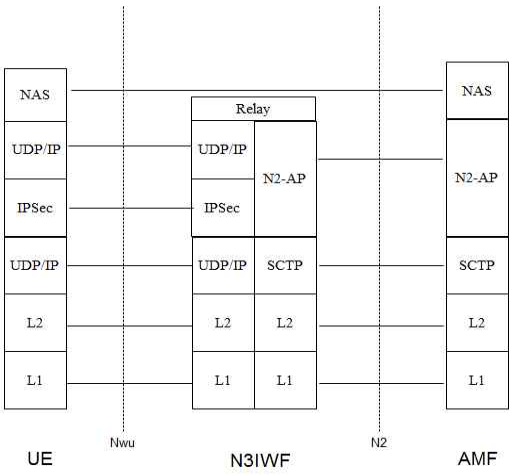

그림 12. IPSec SA 설정 이후 NAS 전송을 위한 컨트롤 플레인
Fig. 12. Control Plane for NAS after IPSec SA is established

그림 13에서는 Trusted Non-3GPP 액세스의 데이터 전송을 위한 User Plane 프로토콜 스택을 보여준다.

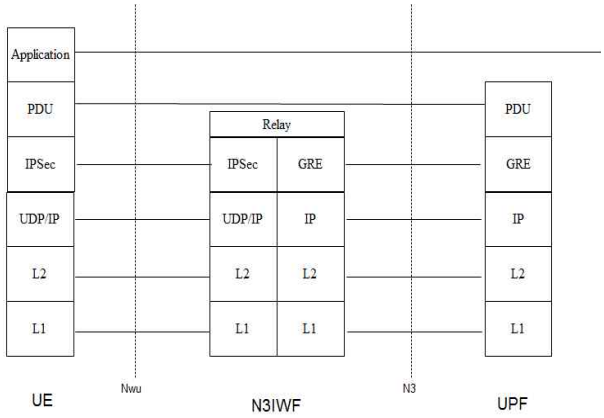

그림 13. 신뢰 Non-3GPP 액세스를 위한 유저 데이터 플레인
Fig. 13. User Plane for Trusted Non-3GPP access

Ⅳ. 구현 및 기능 검증

4-1 개발 환경

N3IWF, UE, AP 기능의 개발은 하드웨어 및 OS 기반 위에 개발이 되었다. UE와 AP는 ubuntu 14.04 kernel 위에서 개발되었으며, Ubuntu OS와 함께 기본으로 사전에 wpa_supplicant 와 hostapd 가 설치되어 있어야 한다.

N3IWF 장비는 Cento-6.8 kernel과 서버에 Cavium Networks 사의 Octeon 프로세서를 장착하여 개발하였다. NPC4212 사양은 표 3에서 보는 바와 같으며, 6개-12개 Core 지원, 이더넷/PCI-Express 인터페이스제공, Host Machine과 별도 Data Plane 분리/운용 고성능패킷처리 어플리케이션에 적합하다.

표 3. NPC4212 사양
Table 3. NPC4212 SPEC

	Specifications
Model	PROCESSOR : OCTEON Plus CN5750 (12CORE-750MHZ) 16Mb NOR Flash memory PCI Express x8 lane PCIe Gen2 Standard
Interface	4x 1Gigabit Ethernet

4-2 네트워크 시험 환경

그림 14는 5G 시스템 개발을 위한 전체 네트워크 시험망이며, Trusted Non-3GPP 액세스 기능 검증을 위해서는 이 중에서 N3IWF, UE, 코어 네트워크 (GW; UPF, CP: Control plane), Fixed AP, WiFi AP를 포함한다. UE가 Fixed 망과 WLAN으로 접속하여 N3IWF를 통해 코어 네트워크에 접속하기 위한 시그널링 및 데이터 전송 시험을 수행하여 5G Trusted Non-3GPP 액세스 연동 기능을 검증하였다.

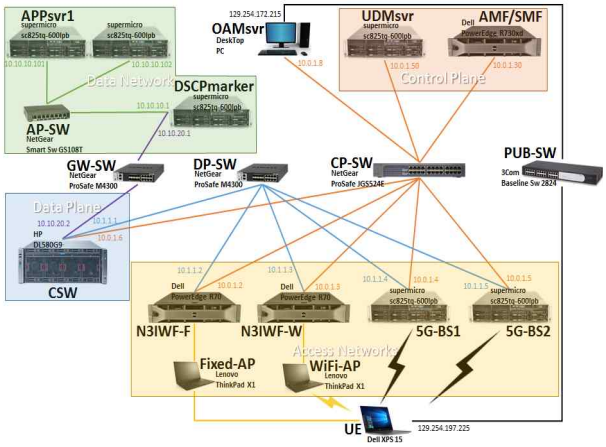

그림 14. 5G 네트워크 시험망
Fig. 14. 5G Network Testbed

4-3 N3IWF 및 UE 기능 검증

5G 네트워크 시험망에서 Trusted Non-3GPP 액세스를 통한 UE와 N3IWF 기능 동작을 확인하기 위하여, dump를 수차례 반복하여 수행한 결과 중에서 일부 로그만을 그림에서 예시로 보여주고 있다.

UE의 경우에는 WLAN과 Fixed 인터페이스를 사용하여 5G 코어 네트워크와 Trusted Non-3GPP 액세스 연동을 수행하였으며, 그림 15는 UE의 Registration 과정을 로그를 통해 확인한 내용 중에서 Registration request NAS 메시지와 Registration accept, Registration complete 메시지 예를 보여준다.

```
...
//EAPOL EAP-5G/NAS/N01_REG_REQ
[Fri Nov 24 10:10:38 2017] eapol: send to AP (87 bytes) ===>
  etherhdr - h_dest: 01:80:c2:00:00:03, h_source: 44:1c:a8:e3:19:0b, h_proto: 0x888e
  eapol - ver: EAPOL_VERSION_2004(0x2), type: EAPOL_TYPE_EAP(0x0), len 69
   eap - code: EAP_CODE_RESPONSE(2), id: 1, len: 69
    eap5g - type: EAP_TYPE_5G(0x38), flags (EAP4G_FLAG_LENGTH|-|-|-|-|-), data_len: 61
     tlv - t: EAP5G_ATTR_TYPE_NAS(0x1), l: 61
      n1 - type: N01_REG_REQ_id(0x2774), rat: 0x1, data_len: 28
       dump[n1 - data]===== len 28 =====
       0000: 00 00 00 01 c2 00 08 31 30 31 32 33 34 35 36 37  ....?..1 01234567
       0010: 38 00 00 00 00 00 00 00 00 00 00 00              8....... ....
       dump===== end =====
...
//Eapol (EAP/EAP5G/NAS/ N01_REG_ACPT)
[Fri Nov 24 10:10:38 2017] eapol: receive from AP (73 bytes) <===
  etherhdr - h_dest: 44:1c:a8:e3:19:0b, h_source: 90:61:ae:c1:73:20, h_proto: 0x888e
  eapol - ver: EAPOL_VERSION_2004(0x2), type: EAPOL_TYPE_EAP(0x0), len 55
   eap - code: EAP_CODE_REQUEST(1), id: 4, len: 55
    eap5g - type: EAP_TYPE_5G(0x38), flags (EAP4G_FLAG_LENGTH|-|-|-|-|-), data_len: 47
     tlv - t: EAP5G_ATTR_TYPE_NAS(0x1), l: 47
      n1 - type: N01_REG_ACPT_id(0x2779), rat: 0x1, data_len: 14
       dump[n1 - data]===== len 14 =====
       0000: 00 00 00 01 c2 00 08 01 01 01 00 00 00 01        ....?...
       dump===== end =====
[Fri Nov 24 10:10:38 2017] <=== sctp: send to UE (23 bytes)
  n1 - type: N01_REG_ACPT_id(0x2779), rat: 0x1, data_len: 14
   dump[n1 - data]===== len 14 =====
   0000: 00 00 00 01 c2 00 08 01 01 01 00 00 00 01        ....?... ......
   dump===== end =====
/// Eapol (EAP/EAP5G/NAS/N01_REG_CMPL)
[Fri Nov 24 10:10:38 2017] ===> sctp: recv from UE (20)
  n1 - type: N01_REG_CMPL_id(0x277a), rat: 0x1, data_len: 11
   dump[n1 - data]===== len 11 =====
   0000: 01 c2 00 08 01 01 01 00 00 00 01                 .?...... ...
   dump===== end =====
[Fri Nov 24 10:10:38 2017] eapol: send to AP (70 bytes) ===>
  etherhdr - h_dest: 01:80:c2:00:00:03, h_source: 44:1c:a8:e3:19:0b, h_proto: 0x888e
  eapol - ver: EAPOL_VERSION_2004(0x2), type: EAPOL_TYPE_EAP(0x0), len 52
   eap - code: EAP_CODE_RESPONSE(2), id: 4, len: 52
    eap5g - type: EAP_TYPE_5G(0x38), flags (EAP4G_FLAG_LENGTH|-|-|-|-|-), data_len: 44
     tlv - t: EAP5G_ATTR_TYPE_NAS(0x1), l: 44
      n1 - type: N01_REG_CMPL_id(0x277a), rat: 0x1, data_len: 11
       dump[n1 - data]===== len 11 =====
       0000: 01 c2 00 08 01 01 01 00 00 00 01                 .?...... ...
       dump===== end =====
```

그림 15. UE 동작
Fig. 15. Operations of UE

```
//N02_DL_NAS_TRANS
[Fri Nov 24 10:07:01 2017] sctp: recv from AMF (162) <===
  dump[from AMF]===== len 162 =====
...                                  ..
  dump===== end =====
  n2 - type: N02_DL_NAS_TRANS_id(10201,0x27d9), ueid: bs-0x3c572b4e/am-0xa6dc6b4e19958, data_len: 142
   n1 - type: N01_AUTH_REQ_id(0x2775), rat: 0x2, data_len: 133
    dump[n1 - data]===== len 133 =====
    0000: 01 2c 00 85 17 73 65 63 71 00 73 65 63 77 00 73  .,.?.sec q.secw.s
    0010: 65 63 66 00 00 00 00 00 00 00 00 00 00 00 00 00  ecf.....
    0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0080: 00 00 00 00 00                                    .....
    dump===== end =====
...
//N02_UL_NAS_TRANS
[Fri Nov 24 10:07:01 2017] sctp: send to AMF (166 bytes) ===>
  dump[to AMF]===== len 166 =====
...                                  ......
  dump===== end =====
  n2 - type: N02_UL_NAS_TRANS_id(10202,0x27da), ueid: bs-0x3c572b4e/am-0xa6dc6b4e19958, data_len: 142
   n1 - type: N01_AUTH_RSP_id(0x2776), rat: 0x2, data_len: 133
    dump[n1 - data]===== len 133 =====
    0000: 02 2c 00 85 17 00 00 00 00 00 00 00 00 00 00 00  .,.?....
    0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
    0080: 00 00 00 00 00                                    .....
    dump===== end =====
```

그림 16. N3IWF 동작
Fig. 16. Operations of N3IWF

그림 16에서는 N3IWF 기능 동작 중, DL NAS, UL NAS 메시지 전송을 확인한 내용을 보여준다. n1_data 에 NAS 파라미터를 포함하고 있으며 dump로 확인한 예이다.

Ⅴ. 결 론

본 논문에서는 3GPP 5G 시스템에서 Trusted Non-3GPP 액세스를 수용하기 위한 연동 기술을 제안하였다. 제안된 방안은 현재 3GPP 5G 시스템 규격에서 제공하는 Untrusted Non-3GPP 액세스 네트워크 구조를 그대로 수용하여 Trusted Non-3GPP 액세스와도 연동이 가능하도록 하며, IPSec 터널을 AP, N3IWF 구간에 설정하여 사용할 수 있도록 하였다. 따라서, UE에서 Trusted Non-3GPP 액세스와 연동하기 위한 추가적인 기능을 필요로 하지 않으며 단순하게 IPSec 기능을 off 시키기만 하면 된다. N3IWF 기능 또한 Untrusted Non-3GPP 액세스 연동과 동일하며, Trusted Non-3GPP 액세스의 경우에는 UE 대신 AP와 IPSec 터널을 구성할 수 있으며, 시큐어 터널이 필요없는 경우에는 UE와 마찬가지로 IPSec 기능을 off 시키기만 하면 된다.

Untrusted Non-3GPP 액세스와 Trusted Non-3GPP 액세스를 동시에 지원하는 경우, 하나의 N3IWF 가 Untrusted/Trusted Non-3GPP 액세스를 동시에 연동 가능한지, 또는 액세스별로 N3IWF가 필요한지에 대한 연구도 필요할 것으로 보인다.

감사의 글

이 논문은 2018 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구로서, 관계부처에 감사드립니다. (No. 2015-0-00042-004, 유/무선 액세스에 비종속적인 5G 코어 핵심기술 개발)

참고문헌

[1] 3GPP TS 23.501 v15.0.0, “System Architecture for the 5G System; Stage 2,” December 2017.
[2] 3GPP TS 23.502 v15.0.0, “Procedures for the 5G System; Stage 2,” December 2017.
[3] 3GPP TR 23.716 v0.3.0, “Study on the Wireless and Wireline Convergence for the 5G system architecture,” March 2018.
[4] 3GPP TS 23.402 v15.3.0, “Architecture enhancements for non-3GPP access,” March 2018.
[5] IETF RFC 7296, "Internet Key Exchange Protocol Version 2 (IKEv2)," October 2014.
[6] IETF RFC 4303, “IP Encapsulating Security Payload (ESP),” December 2005.

강유화(Yoohwa Kang)

2000년 : 포항공과대학교 대학원 (공학석사)

2000년～현 재: 한국전자통신연구원 책임연구원
※관심분야 : 5G 네트워크, 액세스 트래픽 관리 등

김창기(Changki Kim)
1997년 : 부산대학교 잔자공학과 (공학석사)
2006년 : KAIST S/W 공학 (공학석사)
2016년 : 선문대학교 컴퓨터공학과 (공학박사)

1997년～2000년: 삼성전자 네트워크 사업부 전임연구원
2001년～ 현재: 한국전자통신연구원 책임연구원
※관심분야 : 차세대 이동통신 네트워크, 미디어 전송 등