http://dx.doi.org/10.5392/JKCA.2011.11.10.030

# LTE 망을 위한 에이전트-서버 기반의 프로토콜 분석기

## Agent-Server based Protocol Analyzer for LTE Network

피준일*, 이락규*, 임종태**, 복경수**, 유재수**
주식회사 두두원*, 충북대학교 정보통신공학과**

Jun-Il Pi(pji@dodo1.co.kr)*, Nak-guy Lee(nglee@dodo1.co.kr)*,
Jong-Tae Lim(jtlim@chungbuk.ac.kr)**, Kyoung-Soo Bok(ksbok@chungbuk.ac.kr)**,
Jae-Soo Yoo(yjs@chungbuk.ac.kr)**

### 요약

최근 무선 통신 기술의 발전과 함께 스마트 폰 사용자의 급증으로 차세대 이동 통신에 대한 요구가 증가하고 있다. 차세대 이동통신 플랫폼을 빠른 시간 내에 효과적으로 구축하기 위해서는 프로토콜 개발 단계부터 안정화 단계까지 프로토콜의 검증 및 분석을 위한 지원도구가 필요하다. 따라서 본 논문에서는 차세대 이동통신 플랫폼의 선두 주자인 LTE 망을 위한 프로토콜 분석기를 제안한다. 제안하는 분석기는 연동 메시지를 XML 메타데이터로 기술하여 분석 시 활용한다. 또한, 디코더 라이브러리 로딩 기능을 이용하여 LTE 망에 적용된 인코딩 메시지에 대한 분석이 가능하다. 제안하는 분석기는 자체 설계된 LTE 망과의 연동 테스트를 통해 우수성을 검증한다.

■ 중심어 : | LTE | LTE-Advanced | 프로토콜 | 분석기 |

### Abstract

Recently, together with the development of wireless communication technologies and the wide use of smart phones, the demand of the next generation mobile communication has been increased. To construct the next generation mobile communication platform efficiently for a short period from protocol development phase to protocol stability phase, an protocol analyzer is required to verify and analyze the protocol. In this paper, we propose the protocol analyzer of LTE network which is the leader of the next generation mobile communication platforms. The protocol analyzer is a software based agent-server architecture and uses XML metadata which defines intercommunication messages to analyze the protocol of the next generation mobile communications. We can analysis the encoding messages applied to LTE network using the loading of the decoding library. We verify the superiority of the proposed analyzer through an integrated test with LTE network.

■ keyword : | LTE | LTE-Advanced | Protocol | Analyzer |

* 이 논문은 2011년 교육과학기술부"(지역거점연구단육성사업/충북BIT연구중심대학육성사업단)"와 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업의 결과임.(No. 2009-0089128)

접수번호 : #110610-004
접수일자 : 2011년 06월 10일
심사완료일 : 2011년 09월 15일
교신저자 : 유재수, e-mail : yjs@chungbuk.ac.kr

## I. 서 론

최근 스마트폰, 태블릿 PC 등 모바일 기기의 보급이 급증함에 따라 기존 데이터와 음성 위주의 이동통신 서비스에서 멀티미디어 콘텐츠 영역으로 확대되고 있다. 뿐만 아니라 4세대 이동통신에서는 고속 영상 서비스 제공을 목표로 하고 있는 상황이다[1][2]. 이런 멀티미디어 콘텐츠와 대용량 영상 콘텐츠들의 특성상 대량의 트래픽이 발생하며, 이를 처리하기 위한 네트워크 대역폭 확보 및 통신 속도 향상을 위한 연구들이 진행되고 있다. 통신 사업자들 역시 사용자들의 요구사항을 만족시키고자 다양한 형태의 차세대 이동통신 플랫폼을 도입하고 있는 상황이다. 현재 차세대 이동통신 플랫폼의 대표적인 것이 LTE(Long Term Evolution)와 WiMAX(Worldwide interoperability for Microwave Access)이다[1]. SK와 LG 유플러스 등과 같은 국내 통신 사업자들은 3.9세대라 불리는 LTE 기술을 도입하여 망을 구축하고 있으며, 향후 LTE-Advanced로 확대할 예정이다.

LTE/LTE-Advanced는 Layer1, Layer2, Layer3로 구성된 프로토콜들을 통해서 사용자의 요청을 처리한다[3][4]. Layer1은 물리 계층인 PHY에 해당하며, Layer 2는 MAC(Medium Access Control), RLC(Radio Link Control)등으로 구성되어 있다. Layer 3는 사용자 요청을 IP 기반으로 처리할 수 있는 프로토콜로 사용자 인증과 세션 관리를 담당하는 EMM(EPS Mobility Management), ESM(EPS Session Management) 프로토콜[6], 사용자 트래픽을 eNodeB 와 Gateway간에 연동하도록 지원하기 위하여 논리적 베어러를 생성 및 삭제, 관리하기 위한 GTP(GPRS Tunneling Protocol) 프로토콜[8], eNodeB와 MME(Mobility Management Entity)간에 연동을 위한 S1 프로토콜[7]로 구성이 된다. 이러한 프로토콜들을 통해 사용자들에게 멀티미디어 콘텐츠 서비스를 제공하고 있으며, 보다 빨리 안정적인 서비스를 제공하기 위해서는 LTE/LTE Advanced 시스템의 개발 단계부터 안정화단계까지 프로토콜 검증을 위한 도구가 필요하다.

현재 LTE/LTE-Advanced와 같은 차세대 이동통신망을 개발하는데 사용되는 프로토콜 분석기는 wireshark[9], GL-communication[10]와 Tektroniz[11]에서 개발한 프로토콜 분석기 등이 있다. 하지만 wireshark의 경우 LTE 프로토콜 분석 기능이 미흡하며, 여러 시스템이 연동되는 경우 통합적인 수집 및 분석이 어렵다. 또한, 기존 LTE 프로토콜 분석기의 경우 LTE 프로토콜 수집을 위해 별도의 하드웨어가 필요하며, LTE의 각 서브 시스템간 연동 프로토콜에 대한 수집 및 분석은 가능하지만 내부 연동 메시지는 수집할 수 없다. 추가적으로 연동 규격이 변경되는 경우 프로토콜 분석기를 수정해야 하므로, 변경된 프로토콜을 즉시 반영하여 분석에 사용할 수 없다는 문제가 있다.

본 논문에서는 기존 프로토콜 분석기의 문제점을 해결하고 4세대 이동 통신 기술인 IMT-Advanced의 선두 주자라고 할 수 있는 LTE와 LTE-Advanced 망의 연동 메시지를 수집 및 분석 할 수 있는 ANPA(Advanced Network Protocol Analyzer) 분석기를 제안한다. 제안하는 분석기는 LTE와 LTE-Advanced의 표준에서 Layer 3에 해당하는 프로토콜들을 수집 및 분석할 수 있으며, 기존 분석기에서는 지원하지 않은 내부 기능 블록들 간의 연동 메시지 역시 분석이 가능하다. 제안하는 프로토콜 분석기는 연동메시지를 XML 메타데이터로 정의하여 분석 시 활용한다. 따라서 개발되는 시스템에 특화하여 적용이 가능하며, 개발 도중 연동 규격이 변경되는 경우에도 XML 메타데이터를 수정하면 즉시 사용이 가능하다는 특징이 있다. 또한, 제안하는 프로토콜 분석기는 LTE에서 제안하는 인코딩 메시지를 분석할 수 있도록 라이브러리를 로딩하는 기능을 두었다. 이를 통해 LTE 프로토콜 중 X2, S1, RRC(Radio Resource Control)등의 ASN.1 인코딩 된 메시지나, GTP, ESM, EMM 등의 바이너리 인코딩 된 메시지 역시 분석이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 LTE와 LTE-Advanced에 대해 상세히 알아보고, 기존 네트워크 프로토콜 분석기에 대하여 알아본다. 3장에서는 제안하는 프로토콜 분석기와 개발에 적용된 기법들에 대하여 상세히 설명한다. 마지막으로 4장에서는 결론과 향후 연구 방향에 대하여 기술한다.

## II. 관련 연구

### 1. LTE (Long Term Evolution)

3GPP(3rd Generation Partnership Project)는 주요 이동통신 기술 회사들의 파트너십 프로그램으로서, 3GPP에서 LTE를 제안하였다. 3.9 세대라 일컬어지는 LTE는 2004년 11월부터 표준화 작업이 시작되어 2008년 12월 3GPP Release 8에서 표준화로 제정되었다[3]. LTE는 20MHz 대역에서 다운링크 100Mbps, 업링크 50Mbps의 데이터 전송 속도를 지원하는 IP 기반의 셀룰러 기술이다.

3GPP 진영에서는 기존 3G(HSPA)에 비해 40배 이상의 전송속도를 제공하여 하나의 모바일 기기로 다양한 멀티미디어 및 융·복합 서비스를 제공할 수 있는 4세대 이동통신 기술인 LTE-Advanced 기술도 제안하고 있다[4]. LTE-Advanced는 최대 100MHz 대역에서 최대 다운링크 1Gbps, 업링크 500Mbps의 데이터 속도를 지원하는 글로벌-컨버전스형 무선통신 기술로 LTE 기술과의 호환성을 유지하고 있다. 또한, LTE-Advanced는 국제 표준 단체인 ITU-R의 4세대 이동통신(IMT-Advanced) 표준 기술로 선정되었다.

이런 기술을 지원하기 위한 LTE와 LTE-Advanced 망의 시스템 구성은 [그림 1]과 같다. UE(User Equipment)는 실제 LTE 서비스를 받는 단말 사용자 장비로 eNodeB와 무선 통신을 통해 LTE 기반 서비스를 제공받는다[2]. eNodeB는 IP 기반으로 단말과 외부망간의 트래픽을 처리하며, 이를 위한 제어 메시지는 MME (Mobility Management Entity)와의 통신을 통해 처리한다. MME 시스템은 단말의 인증 및 이동성 관리, 베어러 관리등의 모든 제어를 담당한다. SGW(Serving Gateway)는 사용자 트래픽의 라우팅과 LTE 망 접근에 대한 포워딩을 담당하는 블록이며, PDN-GW(Packet Data Network Gateway)는 IP 기반으로 UE와 외부 네트워크 상의 서버들과 접점을 이루는 시스템이다. LTE 시스템에서 eNodeB간에는 X2, eNodeB-MME 간에는 S1, MME-SGW간에는 S11, eNodeB-SGW간에는 S1-U 프로토콜을 사용하여 연동한다.

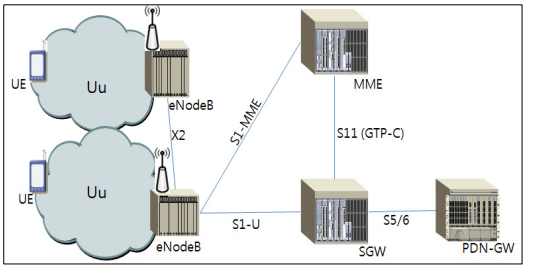


그림 1. LTE/LTE-Advanced 망 구조도

### 2. 기존 프로토콜 분석기

기존 Wireshark[9]와 같은 대표적인 네트워크 프로토콜 분석기는 일반적인 네트워크 패킷을 수집 및 분석할 수 있으나, LTE를 비롯한 각 차세대 플랫폼의 프로토콜과 ASN.1 인코딩이나 Binary 인코딩 된 데이터를 분석할 수 있는 기능은 지원하지 못하고 있다.

GL communication 사에서 개발한 LTE Protocol Analyzer[10]는 LTE 망의 연동 메시지를 수집, 디코딩하여 분석할 수 있는 분석기로 실시간 수집 및 분석과 오프라인 분석이 가능하다. 또한, S1, X2, GTP등의 프로토콜을 수집 및 분석 가능하며, MAC, IP, UDP, SCTP 프로토콜의 분석도 가능하다. 수집 및 분석 결과는 파일로 저장이 가능하며, 추출된 요약 정보는 데이터베이스나 spreadsheet 형태로도 출력할 수 있다는 특징이 있다.

Tektronix[11]에서 개발한 시스템은 LTE 인터페이스 프로토콜들을 수집 및 분석할 수 있는 분석기로서, 하드웨어 기반의 probe를 별도로 설치하여 패킷을 수집하는 방식이다. 이 probe를 통해 타 서브시스템과의 송수신 데이터를 수집하여 분석할 수 있다. K2Air, K18, NAS 장비들을 통해서 RF, MAC을 비롯하여, NAS, S1, X2, GTP등의 프로토콜을 수집 및 분석 할 수 있다. 이를 기반으로 성능 및 통계 정보를 제공할 수 있으며, 단말 사용자의 attach, detach등 호처리(CallTrace) 정보를 제공할 수 있다.

기존 Wireshark의 경우 네트워크 프로토콜을 수집 및 분석할 수 있으나, LTE 프로토콜의 세부 정보를 분석할 수 있는 기능은 극히 제한적으로 지원하고 있어서 LTE 프로토콜 검증에 사용하기에는 다소 문제가 있으

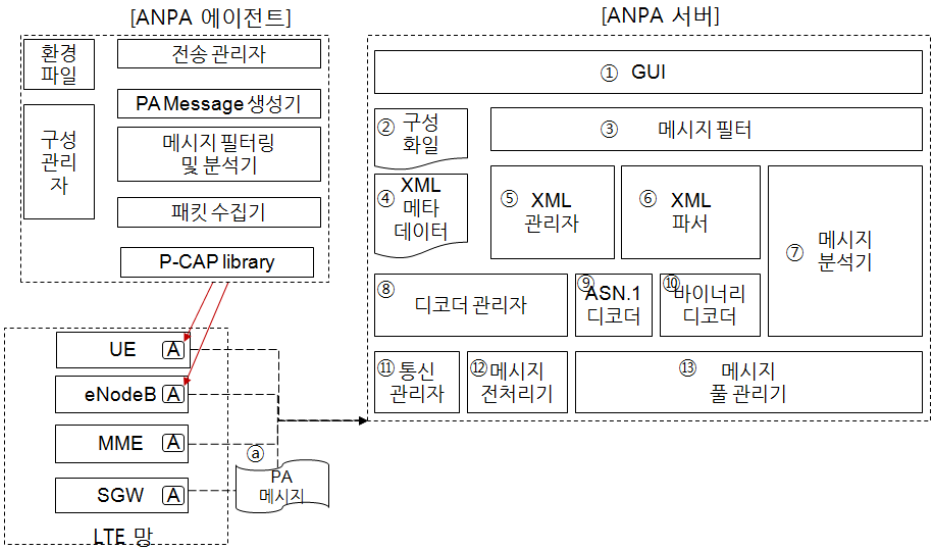


그림 2. ANPA 시스템 구조

며, 여러 시스템을 통합적으로 분석하기에는 무리가 있다. 또한, [10]와 [11]의 분석기 경우 외부 서브시스템과의 인터페이스 데이터를 수집 및 분석할 수 있으나, 내부 기능 블록간의 연동 메시지는 분석이 어렵다는 문제점이 있다. 연동 메시지 수집을 위해서는 별도의 하드웨어 시스템이 있어야 하며 LTE/ LTE-Advanced 표준 규격이 변경된 경우 이를 반영하기 위해 프로토콜 분석기 자체 코드 수정이 불가피 하다는 문제가 있다.

## III. ANPA(Advanced Network Protocol Analyzer)

### 1. 시스템 특징 및 구조

기존 분석기들이 LTE 메시지를 수집하기 위하여 별도의 하드웨어가 필요하며, 외부 시스템간의 연동 프로토콜에 대해서만 수집 및 분석이 가능하다는 문제점이 있다. 본 논문에서는 LTE/LTE-Advanced 시스템에서 기존 분석기의 문제점을 해결하기 위한 새로운 분석기를 개발한다. 제안하는 프로토콜 분석기는 다음과 같은 특징이 있다.

- 소프트웨어 기반의 에이전트-서버 구조
- 연동 메시지를 XML 메타데이터로 정의
- 다양하게 인코딩된 메시지 분석

먼저 제안하는 프로토콜 분석기는 소프트웨어 기반의 에이전트-서버 구조로 LTE/LTE-Advanced 망을 구성하는 시스템에 하드웨어/소프트웨어적으로 추가적인 부하는 없다. 에이전트는 연동 메시지를 수집하기 위하여 pcap 라이브러리를 사용하며, LTE/LTE-Advanced 의 각 서브시스템에 설치된다. 서버는 에이전트에서 수집한 데이터를 분석 및 GUI 상에 도시하는 역할을 한다. 제안하는 프로토콜 분석기는 연동 메시지를 XML 메타데이터로 정의하여 프로토콜 분석 시 활용한다. 이를 통해 개발되는 LTE 시스템들에 맞게 특화하여 구성이 가능하며, 연동 규격이 변경되는 경우에도 프로토콜 분석기 자체 코드 수정 없이 XML 메타데이터 변경만으로도 프로토콜 분석이 가능하다. 또한, 인코딩된 메시지에 대해서도 분석이 가능하다.

LTE/LTE-Advanced에서는 ASN.1 인코딩과 바이너리 인코딩 룰을 사용한다. LTE/LTE-Advanced 프로토콜 중 ESM, EMM, GTP등은 바이너리 인코딩 룰을 사용하며, S1, X2, RRC 등은 ASN.1 인코딩 룰을 사

용한다. 제안하는 프로토콜 분석기는 LTE/LTE- Advanced 개발 시스템에 적용된 디코딩 라이브러리를 로딩할 수 있는 기능을 제공하여, 해당 시스템에서 인코딩되어 연동되는 프로토콜에 대해서도 분석이 가능하다.

이런 특징을 지원하기 위한 시스템 구조는 [그림 2]와 같다. [그림 2]에서처럼 ANPA 에이전트는 UE, eNodeB, MME, SGW의 각 시스템에 설치되어 수집된 메시지를 ⓐ처럼 PA 메시지로 구성한 후 ANPA 서버로 전송한다. ANPA 서버는 이를 분석하여 GUI를 통해 화면상에 도시한다. ANPA를 구성하는 에이전트와 서버의 각 기능 모듈이 담당하는 역할은 다음과 같다.

### 1.1 ANPA 에이전트

ANPA 에이전트는 패킷을 수집할 수 있는 pcap library를 기반으로 운용된다. 에이전트는 환경 파일, 구성 관리자, 전송 관리자, PA 메시지 생성기, 메시지 필터링 및 분석기, 패킷 수집기로 구성된다.

- 환경 파일은 메시지를 캡처하기 위한 룰과 ANPA 서버의 네트워크 정보가 저장된 파일이다. 캡처하기 위한 룰은 이더넷 인터페이스 정보, 송수신 IP 주소, 포트번호로 구성된다.
- 구성 관리자 : 환경 파일로부터 정보를 읽어들여 pcap 라이브러리를 초기화하고, ANPA 서버 네트워크 정보를 추출하는 역할을 한다.
- 패킷 수집기 : pcap 라이브러리를 통해 메시지를 수집하는 역할을 담당한다.
- 메시지 필터링 및 분석기 : 수집된 메시지 중 서버로 전송해야하는 메시지들만을 추출하는 역할을 담당한다. 추출하는 메시지는 환경 파일에 저장된 필터링 정보를 이용한다.
- PA 메시지 생성기 : 필터링 된 메시지에 PA 헤더 정보를 추가하여 서버로 전송하기 위한 PA 메시지를 생성하는 역할을 담당한다. PA 헤더에는 수집된 메시지의 송수신 IP주소, 포트 정보, 메시지 타입 등으로 구성된다.
- 전송 관리자 : 생성된 PA 메시지를 ANPA 서버로 전송하는 역할을 담당한다. ANPA 서버의 정보는 구성 관리자가 환경 화일로부터 추출한 내용으로 구성된다.

### 1.2 ANPA 서버

ANPA 서버는 에이전트에서 수집한 메시지들을 분석 및 GUI 상에 도시하는 역할을 담당한다. 각 모듈들이 담당하는 역할은 다음과 같다.

- 통신 관리자 : 각 서브 시스템에 설치된 에이전트에서 수집하여 전송된 PA 메시지를 UDP/TCP 통신을 통해 수신하는 역할을 한다.
- 메시지 전처리기 : 통신 관리자에서 수집한 메시지 중 PA 메시지의 헤더와 각 메시지별 공통 헤더를 분석하는 기능을 담당한다. 이를 통해 송수신 시스템과 메시지 종류를 판별하여 GUI에 도시할 수 있는 요약 정보를 구성한다. 부가적으로 수신된 메시지 전체를 메시지 풀에 등록한다.
- 메시지 풀 관리기 : 메시지 풀을 관리하며, 사용자가 특정 메시지에 대해 상세 분석을 요청할 경우 해당 메시지를 추출하는 역할을 담당한다. 만약 일정 수준 이상으로 메시지가 수신되면 기존에 수신된 메시지들을 자동으로 파일로 저장한다.
- 메시지 분석기 : 사용자가 요청한 특정 메시지에 대해 XML 파서와 연동하여 상세 분석을 담당한다.
- ASN.1 디코더 : 메시지 풀에서 추출된 메시지가 S1, X2, RRC와 같이 ASN.1 인코딩 된 경우 디코딩을 통해 원 메시지를 추출하는 기능을 담당한다. 추출된 메시지는 메시지 분석기로 전달된다.
- 바이너리 디코더 : 메시지 풀에서 추출된 메시지가 ESM, EMM, GTP와 같이 바이너리 인코딩 된 경우 원래 메시지를 추출하기 위하여 바이너리 디코딩 작업을 수행한다. 추출된 메시지는 메시지 분석기로 전달되어 상세 분석이 이뤄진다.
- 디코더 관리자 : ASN.1 디코더나 바이너리 디코더를 로딩하는 기능을 담당한다.
- XML 관리자 : XML 메타데이터를 로딩하는 기능을 담당한다.
- XML 파서 : 읽어들인 XML 메타 데이터를 분석한 후 메시지 분석기와 연동하여 해당 메시지를 상세 분석한다.

- 메시지 필터 : 사용자가 특정 메시지나 또는 특정 시스템간의 메시지만을 GUI 상에 도시하고자 하는 경우 이를 담당하는 모듈이다.
- GUI : 사용자가 메시지 수집 및 분석의 시작이나 종료, 특정 메시지에 대한 상세 분석 등의 요청을 처리하여 화면상에 도시하는 기능을 담당한다.

## 2. 지원하는 프로토콜

ANPA는 LTE/LTE-Advanced의 Layer 3 표준 프로토콜과 LTE/LTE-Advanced를 구성하는 서브 시스템의 각 기능 노드들 간 연동 메시지를 수집 및 분석할 수 있다.

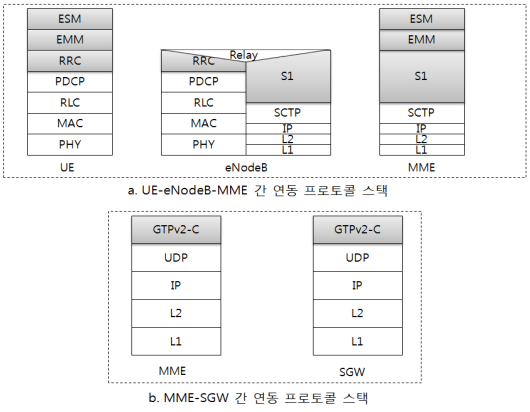


**그림 3. LTE/LTE-Advanced 프로토콜 스택**

[그림 3]은 LTE/LTE-Advanced망의 제어 평면(control plane)에서 연동되는 프로토콜을 나타낸 것이다. (a)는 UE, eNodeB, MME간의 프로토콜 스택이며, (b)는 MME-SGW간 프로토콜이다. (a)와 (b)에서 회색의 사각형에 위치한 프로토콜들이 Layer 3에 해당하며, Layer 1은 PHY, Layer 2는 MAC, RLC, PDCP에 해당한다. Layer 3의 프로토콜 기능은 다음과 같다.

- ESM(EPS Session Management) : 서비스 세션 관리 기능을 수행하는 프로토콜로, 사용자 단말(user equipment)의 EPS(Evolved Packet System) 베어러 컨텍스트 제어를 담당한다. EMM(EPS Mobility Management) 프로토콜 및 UI(User Interface)와의 인터페이스를 가진다.
- EMM(EPS Mobility Management) : UE의 네트워크 등록 및 삭제(network attachment/detachment), 서비스 요구(service request), 가입자 인증 및 암호화, 그리고 사용자 호출(paging) 기능을 가진다. 또한 ESM 프로토콜 및 무선 자원을 관리하는 RRC 프로토콜과의 인터페이스를 가진다.
- RRC (Radio Resource Control) : 시스템 정보 전송, 페이징, 이동 관리 및 단말 관리, Radio 베어러 관리, RRC 연결 관리 등을 수행하는 프로토콜이다.
- S1-MME : eNodeB와 MME간 제어메시지를 주고받기 위한 프로토콜로서 ASN.1으로 인코딩되어 연동된다. 주 기능은 베어러 설정 및 해제, NAS 메시지의 전송, 페이징 과 핸드오버 절차 수행의 기능을 담당한다.
- GTP-C (GPRS Tunneling Protocol-Control) : GTP는 GTP-U와 GTP-C로 구분된다. GTP 노드 사이에 데이터 트래픽을 송수신하기 위해 GTP-U 프로토콜의 터널이라는 논리적 베어러를 생성하게 되는데, 이러한 논리적 터널의 설정 또는 해제, 터널 정보의 변경, 핸드오버시 터널의 eNodeB 주소 정보의 변경 등 터널의 제어 및 관리를 담당하는 프로토콜이 GTP-C이다.

## 3. XML 메타데이터 생성 규칙

ANPA는 연동 메시지를 XML 메타 데이터로 정의하여 분석하기 때문에 [그림 3]의 프로토콜이나 내부 기능 노드들 간의 메시지 역시 XML 메타 데이터로 정의하기만 한다면 상세 분석이 가능하다. 또한, S1, RRC 등의 ASN.1 인코딩된 메시지 역시 적용된 디코더 라이브러리만 로딩한다면 원래의 메시지를 추출하여 분석이 가능하다. 이와 마찬가지로 ESM, EMM, GTP등의 바이너리 인코딩된 메시지 역시 바이너리 디코더를 통해 상세 분석이 가능하다. ANPA에서는 이와 같이 연동 메시지를 XML 메타데이터로 정의할 수 있도록 [표 1] 과 같은 메시지 정의 규칙을 제안한다. 메시지 정의 규칙을 활용하여 XML 메타데이터를 생성하면 된다.

**표 1. ANPA XML 메타데이터 정의 규칙**

| Attribute | Value 종류 | 설명 |
|---|---|---|
| type | var | 일반 변수 |
| | array | 배열 |
| | struct | 구조체 |
| | union | Union |
| | enum | enumerate |
| | commonHeader | 메시지 공통 헤더 |
| name | uint8_t | type이 var일 경우 unsigned char |
| | uint16_t | unsigned short (2byte) |
| | uint32_t | unsigned int (4byte) |
| | struct name | type이 struct나 arrayStruct 일 경우 |
| | enum name | type이 enum일 경우 |
| value | anything | 값을 작성, 10,16진수 및 일반 string |
| halfByte | 0 or 1 | Half byte(4비트) 표현 |
| bit | decimal | bit 필드, value는 비트 자리수 |
| msgType | enum | 메시지 타입 |
| mapStruct | struct | 메시지 타입에 맵핑되는 struct 이름 |

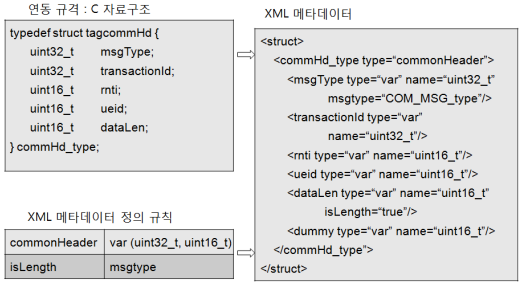


**그림 4. XML 메타데이터 생성 예**

[그림 4]는 메시지 룰을 정의하여 생성된 XML 메타데이터의 생성 예제이다. [그림 4]는 MME내 연동되는 메시지들의 공통 헤더로써 이를 XML 메타데이터로 생성한 것이다. C에서 uint32_t 변수 2개와 uint16_t 변수 2개로 형성된 구조체 commHd_type을 [표 1]에 의거하여 생성한 것으로, [표 1]중 commonHeader, var, uint16_t, uint32_t, msgType 등을 이용하여 정의한 것이다.

[그림 5]는 [그림 4]를 통해 정의된 XML 메타데이터를 이용하여 분석하는 과정을 나타낸 것이다. ANPA 에이전트가 MME에서 수집한 연동 메시지를 ANPA 서버로 전송하고, 이를 ANPA 서버의 메시지 분석기에서 수행하는 분석과정이다. 먼저 수집된 메시지의 hexa 코드가 [그림 5]의 왼쪽 편에 해당한다. ANPA 서버는 [그림 4]의 메타데이터를 로딩한 후 "var" 타입의 "uint32_t"라는 정보를 알아낸다. 이를 통해 수집된 메시지에서 4바이트를 추출하여 1이라는 값을 얻어내고, 연관된 "msgtype"의 "COM_MSG_type" 에서 "MMS1_INIT_DATA_IND"라는 분석결과를 얻게 된다. 다른 메시지 역시 동일한 형태의 연산으로 각 파라미터 값을 분석 및 추출하게 된다.

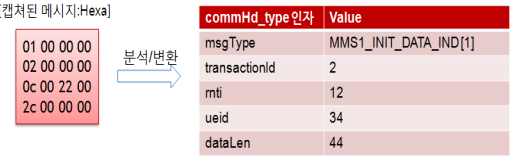


**그림 5. XML 메타데이터 분석 예**

## 4. ANPA 프로토콜 분석 절차

ANPA 서버에서 수집된 연동 메시지를 분석하기 위한 절차는 다음 [그림 6] 과 같다. [그림 6]의 ①처럼 로딩할 XML 메타데이터 파일리스트를 XML Parser에게 전달한다. XML Parser는 ②와 같이 파일로부터 XML 메타데이터를 로딩하여 분석한 결과를 유지하며, ③과 같이 MsgAnalyzer가 메시지를 분석 시 활용한다.

만약 ⓐ와 같이 에이전트로부터 캡처된 메시지가 전송이 되면, CommMgr을 통해 메시지를 수신한다. 수신된 메시지는 MsgPreProcessor를 통해 ⓑ에서 어떤 시스템간의 연동 메시지인지를 파악하여 GUI상에 출력할 정보들을 구성한다. 그리고 ⓒ 과정을 통해 MsgPool에 수신된 메시지를 출력한다. 요약 정보는 MsgPreprocessor에서 발부된 messageID와 함께 ⓓ, ⓔ, ⓕ, ⓖ 절차를 걸쳐 화면상에 도시하게 된다. 사용자가 특정 메시지에 대해 세부 정보를 보고자하는 경우 XMLMgr은 ⓗ 절차로 MsgPool에 요청한다. MsgPool에서 messageID 정보를 이용하여 추출된 메시지는 인코딩 유무를 판단하게 되며, 인코딩이 된 메시지라면 ⓘ절차로 ASN.1 Decoder나 Binary Decoder로 전송된다. 인코딩이 되지 않은 메시지라면 MsgAnalyzer로 전송되며, 인코딩 된 메시지의 경우는 각 디코더를 거친 후 ⓙ절차를 통해 MsgAnalyzer로 전송된다.

MsgAnalyzer는 XML Parser와의 연계를 통해 상세 메시지 형태로 분석하고 그 결과를 GUI 상에 도시한다. 만약 운용자에 의해 필터가 설정된 경우는 ⓕ, ⓖ 절차를 통해 필터링 된 결과가 화면상에 출력되게 된다.

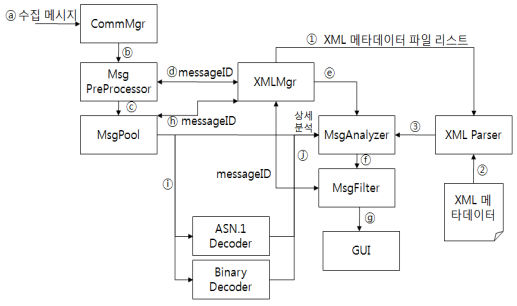


그림 6. 프로토콜 분석 절차

## 5. 구현 및 검증

제안하는 프로토콜 분석기를 적용하여 검증할 수 있는 시스템을 [그림 7]과 같이 설계하였다. 검증망은 LTE/LTE-Advanced 표준을 근거로 하여 설계한 시스템이며, 내부 연동 메시지에 대한 분석 기능을 검증하기 위하여 MME 시스템을 4개의 기능 노드인 S1IB(S1 Interface Block), MMB (Mobility Management Block), SMB(Session Management Block), S11IB(S11 Interface Block)로 구성하였다. S1IB는 eNodeB Simulator와 S1으로 인코딩 된 메시지를 연동하기 위한 인터페이스 블록이며, MMB는 단말의 이동성 관련 메시지인 ESM 프로토콜을 처리하기 위한 블록이다. SMB는 단말의 세션 관련 메시지인 ESM 프로토콜을 처리하기 위한 블록이며, S11IB는 SGW Simulator와 GTP-C 통신을 하기 위한 MME-SGW간의 인터페이스 블록이다. 각 블록간에는 UDP/IP 통신을 통해 메시지 연동한다.

먼저 단말 시스템의 ESM과 EMM 메시지는 ①처럼 RRC 메시지 내에 NAS 메시지로 포함되어 eNodeB Simulator와 연동한다. 그리고 ②처럼 eNodeB Simulator는 NAS 메시지를 S1 메시지 내에 일부로 포함하여 MME와 S1 프로토콜을 따라서 연동된다. MME는 ⑥처럼 SGW Simulator와 S11(GTP-C) 통신을 통해 연동된다. [그림 7]과 같은 메시지 연동을 통해 단말의 요청을 처리하게 되며, LTE/LTE-Advanced 망에서 연동되는 절차는 ATTACH, DETACH, PAGING, HANDOVER등 다수의 절차들이 있으며, 이를 통해 단말 사용자는 LTE/LTE-Advanced 망을 통한 서비스를 받게 된다.

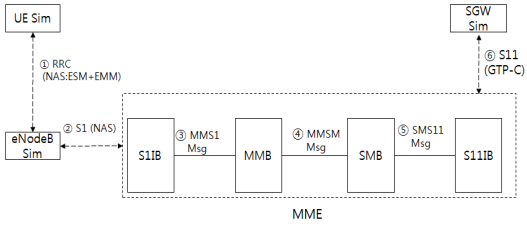


그림 7. 검증망 구조 및 연동 플로우

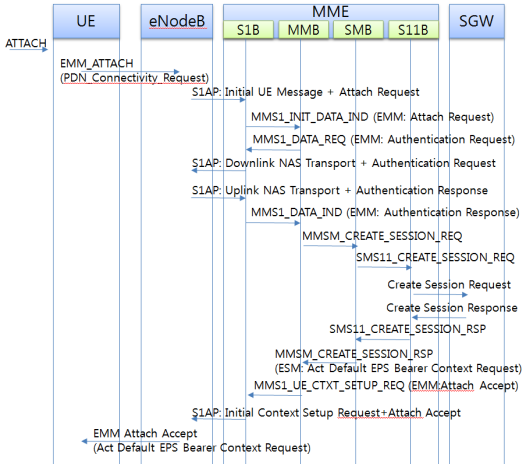


그림 8. LTE/LTE-Advanced Attach 메시지 절차

[그림 8]은 [그림 7]의 검증망을 통해 연동되는 절차 중 Attach 절차 일부를 나타낸 것이다. 기타 모든 절차들이 LTE/LTE-Advanced 표준에 의거하여 동작이 되며, ANPA에서는 이런 모든 절차들에 대해 [그림 8]과 같은 일련의 메시지들을 수집 및 분석하게 된다.

ANPA의 에이전트는 리눅스 상에서 개발 및 운용되며, 서버는 윈도우즈 환경에서 개발되었다. ANPA는 다음 [그림 9]에서와 같이 메시지 리스트 보기, 메시지 상세 분석 Trace, 메시지 Dump 및 ASCII 보기, Log 보기 4개로 이루어져 있다.

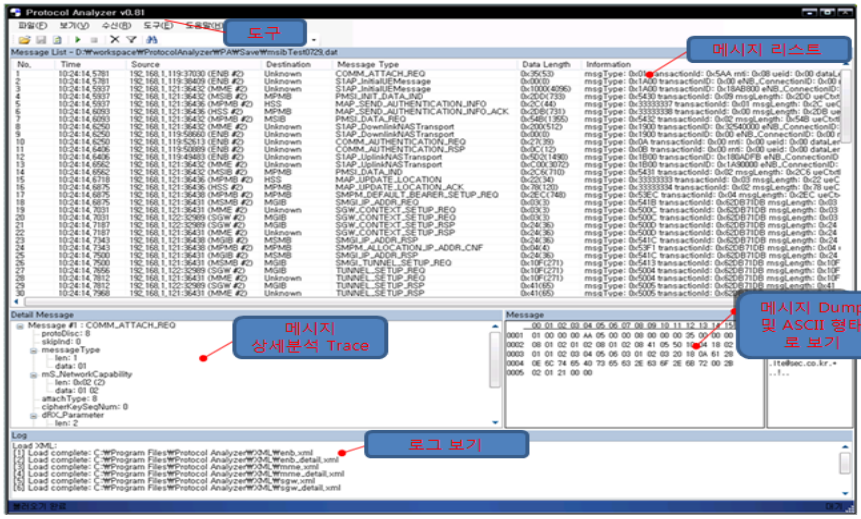


그림 9. LTE 프로토콜 분석기 화면

메시지 리스트 보기는 연동 메시지의 요약 정보를 볼 수 있는 부분으로 송신 노드, 수신 노드, 메시지 ID등을 파악할 수 있다. 메시지 상세 분석 Trace는 메시지 리스트에서 특정 메시지를 선택하였을 경우 출력되는 부분으로 해당 메시지의 전체 구조 및 파라미터 값을 출력해주는 부분이다. 메시지 Dump 부분은 ASCII 형태로 출력하는 부분이며, Log 보기는 실제 운용 시 에이전트와의 연동 및 내부 처리 시 발생하는 로그를 표현하는 부분이다.

[표 2]는 지원 프로토콜 측면에서 기존 LTE 프로토콜 분석기와의 비교 검증이다. 세 개의 프로토콜 분석기 모두 LTE/LTE-Advanced 표준 프로토콜들인 S1, X2, NAS(ESM, EMM), GTP등을 모두 지원한다. RRC의 경우 ANPA에서만 지원하고 있으며, LTE/LTE-Advanced 시스템을 구성하는 세부 기능 노드들 간의 내부 연동메시지는 ANPA에서만 지원하고 있다.

[표 3]는 ANPA와 지원 기능 측면에서 기존 LTE 프로토콜 분석기와의 비교 결과이다. ANPA는 GL Communication 사의 프로토콜 분석기와는 거의 동일한 기능을 지원하고 있으며, Tektronix 사의 프로토콜 분석기는 성능 및 통계 기능과 CallTrace 기능을 추가적으로 지원한다. 하지만 ANPA는 소프트웨어 기반으로 LTE/LTE-Advanced 시스템에 하드웨어적으로나 소프트웨어적으로 부하가 크지 않으며, 연동 규격 변경 시에도 효율적으로 반영할 수 있다는 장점이 있다.

**표 2. 지원 프로토콜 비교**

| 지원프로토콜 | GL | Tektronix | ANPA |
|---|---|---|---|
| S1AP | 지원 | 지원 | 지원 |
| X2AP | 지원 | 지원 | 지원 |
| GTP | 지원 | 지원 | 지원 |
| ESM | 지원 | 지원 | 지원 |
| EMM | 지원 | 지원 | 지원 |
| RRC | X | 지원 | 지원 |
| 내부메시지 | X | X | 지원 |

**표 3. 지원 기능 비교**

| 기능 | GL | Tektronix | ANPA |
|---|---|---|---|
| 패킷수집방식 | 하드웨어 | 하드웨어 | 소프트웨어 |
| 요약보기 | 지원 | 지원 | 지원 |
| 상세분석보기 | 지원 | 지원 | 지원 |
| hexa 코드보기 | 지원 | 지원 | 지원 |
| 검색,필터링 | 지원 | 지원 | 지원 |
| 파일 저장 | 지원 | 지원 | 지원 |
| RRC | X | 지원 | 지원 |
| CallTrace | X | 지원 | X |
| 성능,통계 | 일부 지원 | 지원 | X |
| 연동규격 변경 | 어려움 | 어려움 | 용이 |

## IV. 결론

본 논문은 LTE/LTE-Advanced를 위한 프로토콜 분석기를 제안하였다. 제안하는 ANPA는 연동 메시지를 XML 메타데이터로 정의하여 이를 분석 시 활용하는 기법과 ASN.1 인코딩이나 바이너리 인코딩되어 연동되는 메시지를 분석할 수 있는 기법을 적용한 분석기이다. 연동되는 메시지를 XML 메타데이터로 정의함으로써 본 분석기를 적용하는 시스템에 맞게 특화하여 적용 가능하며, 연동 규격 변경 시에도 XML 메타데이터를 수정하여 분석기에 적용할 수 있도록 분석기를 설계하였다. 또한, ASN.1 디코더나 바이너리 디코더 라이브러리를 분석기에 로딩할 수 있는 기법을 적용하여 연동 메시지 형태에 따라 분석할 수 있도록 지원하였다.

본 논문에서는 기존 하드웨어 기반의 GL이나 Tektronix와의 수집 및 분석 지원 프로토콜 및 지원 기능측면에서 비교 검증을 하였으며, 이를 통해 ANPA가 내부 연동메시지 분석 및 연동 규격 변경 및 적용 측면에서 기존 제품보다 우월함을 보였다.

향후 연구에서는 GL이나 Tektronix와의 성능 측면에서 비교 검증을 수행하고자 한다. 또한, ANPA를 Mobile WiMAX를 비롯한 차세대 이동통신 플랫폼에 적용함으로써 다양한 프로토콜을 분석할 수 있도록 기능을 확장할 예정이다.

## 참 고 문 헌


[1] 윤현영, “LTE vs. WiMAX: 차세대 이동통신 동향”, 전자방송통신저널, 제27권, pp.76-87, 2010.

[2] J. M. Chung, K. Park, T. Won, W. Oh, and S. Choi, “New Protocols for Future Wireless Systems,” Proc. IEEE International Midwest Symposium on Circuits and Systems, pp.692-695, 2010.

[3] 오돈성, 이문식, 김일규, 정현규, “3GPP LTE 기술 개발 및 서비스 동향”, 전자통신동향분석, 제25권, 제6호, pp.20-28, 2010.

[4] 송평중, 고영조, 임선배, “LTE-Advanced 표준 기술 동향”, 전자공학회지, 제36권, 제1호, pp.52-63, 2009.

[5] 3GPP TS 36.300 v8.6.0, “Evolved Universal Terrestrial Radio Access(E-UTRA) and Evolved Universal Terrestrial Radio Access Network(E-UTRAN); Overall Description; State 2,” 2011.

[6] 3GPP TS 24.301, “Non-Access-Stratum (NAS) protocol Evolved Packet System (EPS); Stage 3,” 2011.

[7] 3GPP TS 36.413, “Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP),” 2011.

[8] 3GPP TS 29.274, “3GPP Evolved Packet System(EPS); Evolved General Packet Radio Service(GPRS) Tunnelling Protocol for Control plane(GTPv2-C); Stage3,” 2011.

[9] http://www.wireshark.org

[10] http://www.gl.com/lteanalyzer.html

[11] http://www.tektronixcommunications.com/LTE


## 저 자 소 개


**피 준 일(Jun-Il Pi)** 정회원

- 1999년 2월 : 충북대학교 컴퓨터공학과(공학사)
- 2001년 2월 : 충북대학교 정보통신공학과(공학석사)
- 2003년 2월 : 충북대학교 정보통신공학과(박사수료)
- 2003년 3월 ~ 2007년 2월 : (주)코스모 DBMS 개발팀
- 2007년 3월 ~ 2011년 1월 : (주)가인정보기술 차세대 네트워크팀
- 2011년 3월 ~ 현재 : (주)두두원 네트워크 개발팀

<관심분야> : 데이터베이스 시스템, 자료저장 시스템, 차세대 네트워크, 모바일 네트워크

**이 락 규(Nak-Gyu Lee)** 정회원

- 2001년 2월 : 충북대학교 정보통신공학과(공학사)
- 2003년 2월 : 충북대학교 정보통신공학과(공학석사)
- 2006년 2월 : 충북대학교 정보통신공학과(박사 수료)
- 2002년 2월 ~ 2011년 1월 : (주)가인정보기술 솔루션 사업본부
- 2011년 3월 ~ 현재 : (주)두두원 스마트기술 개발팀

<관심분야> : 위치기반서비스, 모바일 P2P 네트워크, 센서네트워크 및 RFID 등

**임 종 태(Jong-Tae Lim)** 준회원

- 2009년 2월 : 충북대학교 정보통신공학과(공학사)
- 2011년 2월 : 충북대학교 정보통신공학과(공학석사)
- 2011년 3월 ~ 현재 : 충북대학교 정보통신공학과(박사 과정)

<관심분야> : 시공간 데이터베이스 시스템, 이동 객체 데이터베이스, 모바일 P2P 서비스 등

**복 경 수(Kyoung-Soo Bok)** 정회원

- 1998년 2월 : 충북대학교 수학과(이학사)
- 2000년 2월 : 충북대학교 정보통신공학과(공학석사)
- 2005년 2월 : 충북대학교 정보통신공학과(공학박사)
- 2005년 3월 ~ 2008년 2월 : 한국과학기술원 전산학과 Postdoc
- 2008년 3월 ~ 2011년 2월 : (주)가인정보기술 연구소
- 2011년 3월 ~ 현재 : 충북대학교 정보통신공학과 초빙조교수

<관심분야> : 데이터베이스 시스템, 자료저장 시스템, 위치기반서비스, 모바일 P2P 네트워크, 센서네트워크 및 RFID 등

**유 재 수(Jae-Soo Yoo)** 종신회원

- 1989년 2월 : 전북대학교 컴퓨터공학과(공학사)
- 1991년 2월 : 한국과학기술원 전산학과(공학석사)
- 1995년 2월 : 한국과학기술원 전산학과(공학박사)
- 1995년 3월 ~ 1996년 8월 : 목포대학교 전산통계학과 전임강사
- 1996년 8월 ~ 현재 : 충북대학교 정보통신공학과 교수

<관심분야> : 데이터베이스시스템, 정보검색, 센서네트워크 및 RFID, 멀티미디어 데이터베이스, 분산객체컴퓨팅 등