

## LTE 시스템을 위한 XML 메타데이터 기반의 프로토콜 분석기 설계 및 구현

### Design and Implementation of an XML Meta-Data based Protocol Analyzer for LTE Systems

피 준 일\*, 이 철 우\*, 복 경 수\*\*, 유 재 수\*\*  
주식회사 두두원\*, 충북대학교 정보통신공학부\*\*

Pi jun-il, Lee Chul-woo\*, Bok kyoung-soo\*\*,  
Yoo jae-soo\*\*  
DoDoWon Co., Ltd\*, Dept. Computer and  
Communication Engineering, Chungbuk National Univ.\*\*

#### 요약

최근 무선통신의 발전과 스마트 폰 사용자의 급격한 증가로 인하여 멀티미디어 콘텐츠에 대한 관심과 요구가 급속히 증대되고 있다. 이를 수용하기 위한 이동통신 시스템 환경 역시 급속도로 변하고 있으며, 그중 LTE 시스템에 대한 관심과 개발이 진행되고 있는 상황이다. 이에 따라 개발단계부터 안정화단계까지 해당 시스템의 프로토콜 검증과 분석을 위한 분석기의 필요성이 대두되고 있다. 본 논문에서는 LTE 프로토콜과 연동 메시지를 XML 메타데이터로 기술한 에이전트-서버 구조의 프로토콜 분석기를 제안한다. 제안하는 프로토콜 분석기는 LTE 시스템에 최적화된 프로토콜 분석이 가능하고 연동 규격 변경시에도 XML 메타데이터 수정만으로 적용가능하다.

#### I. 서론

최근 스마트폰, 태블릿 PC 등 모바일 기기의 보급이 급증함에 따라 기존 데이터 서비스와 음성 위주의 이동통신 서비스에 만족하지 않고, 오디오, 비디오, 데이터 등 다양한 멀티미디어 콘텐츠에 대한 요구와 트래픽이 증가하고 있다. 이런 트래픽의 급격한 증가를 수용하기 위하여 통신 사업자들은 다양한 방법을 제안하고 있으며, 그중 3.9 세대가 일컬어지는 LTE에 대한 관심과 서비스 시스템 개발 상용화가 본격화되고 있다. 하지만 개발되는 LTE 시스템의 유효성과 안정성을 검증하기 위한 연구는 극히 드물며, LTE와 같이 표준화 연구와 개발이 함께 이루어지는 경우 연동 규격 변경이 빈번하게 발생하여 이를 효과적으로 반영할 수 있는 분석기에 대한 연구는 거의 전무하다.

이에 본 논문에서는 LTE 시스템의 연동 메시지를 XML 메타데이터로 표기하고, 수집된 LTE 시스템 연동 메시지를 XML 메타데이터 기반으로 분석할 수 있는 프로토콜 분석기를 제안한다.

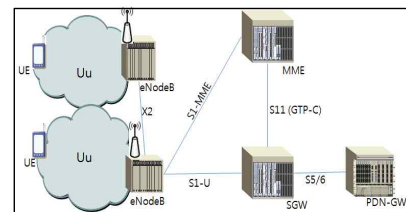
#### II. 관련 연구

3GPP는 주요 이동통신 기술 회사들의 파트너십 프로그램으로서, LTE는 2004년 11월부터 표준화가 시작되어 3GPP Release 8에서 표준화되었다[1]. LTE는 20MHz 대역에서 다운링크 100Mbps, 업링크 50Mbps의 데이터

이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업의 결과임. (No.2009-0089128)

전송속도를 지원하는 IP 기반의 셀룰러 기술이다.

LTE의 시스템은 [그림 1]과 같이 UE, eNodeB, MME, SGW, PDN-GW로 구성된다. UE(User Equipment)는 실제 LTE 서비스를 받는 단말 사용자를 의미하며 eNodeB와 무선 통신을 통해 LTE 기반 서비스를 받는다 [2]. MME 시스템은 모든 제어메시지 처리를 담당하며, UE 인증, 이동성 관리, 베어러 관리, Non-Access Stratum(NAS) 처리를 담당한다. SGW는 사용자 트래픽의 라우팅과 LTE 망 접근에 대한 포워딩을 담당하는 블록이며, PDN-GW는 UE와 IP 기반 외부 네트워크 상의 서버들과 접점을 이루는 시스템이다. LTE 시스템에서 eNodeB간에는 X2, eNodeB-MME 간에는 S1-MME, MME-SGW간에는 S11 (GTP-C), eNodeB-SGW간에는 S1-U, SGW-PDN-GW간에는 S5/S6 프로토콜을 사용하여 연동한다.



▶▶ 그림 1. LTE 시스템 구성도

기존 네트워크 프로토콜 분석기들 중 Wireshark[3] 는 pcap 라이브러리를 사용하는 것으로 세계에서 가장 널리 사용되는 네트워크 분석 프로그램중의 하나이다. Wireshark는 네트워크 상에서 캡처한 데이터에 대한 네트워크와 상위 레이어 프로토콜의 정보를 제공한다. 하지만 LTE의 프로토콜 및 하위 노드간의 연동 메시지에

대한 세부 분석이 용이하지 않다.

### Ⅲ. LTE 프로토콜 분석기

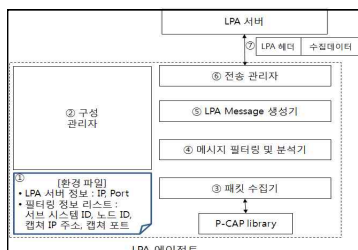
#### 1. 특징

기존 연구들은 일반적인 네트워크 패킷을 수집 및 분석할 수 있으나, LTE 프로토콜에 맞게 메시지를 분석 및 도시할 수 있는 방안을 제시하지 못하고 있다. 제안하는 LTE 프로토콜 분석기(LPA)의 특징은 다음과 같다.

- 에이전트-서버 구조 : 에이전트는 LTE의 각 서버 시스템에 설치되며, pcap을 통해 데이터를 수집한다. 따라서 LTE 시스템의 각 개별 소프트웨어 블록들과 하드웨어상에 추가 부하는 전혀 없다.
- XML 메타데이터 기반의 유연한 메시지 분석 기법 : 분석하고자 하는 각 메시지에 대해 XML 구조의 메타데이터로 정의함으로써, 적용하려고 하는 LTE 시스템에 특화시킬 수 있다. 또한 연동 규격 변경시에도 XML 메타데이터만을 수정하여 사용이 가능하다.

#### 2. LPA 구조

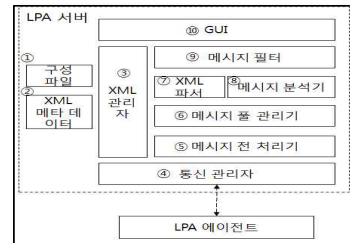
LPA는 에이전트는 LTE 각 서버 시스템에 설치 운영되며, 연동 메시지 수집 및 서버로의 전송 역할을 담당한다. LPA 에이전트는 [그림 2]와 같은 구조로 이루어져 있다. 구성관리자가 ①의 환경 파일을 로딩하여 LPA 서버에 대한 정보를 추출한다. 그리고 패킷 수집해야 할 필터링 정보 리스트를 추출하여 pcap 라이브러리를 초기화한다. ③의 패킷 수집기는 pcap을 통해 데이터를 수집하며, ④의 메시지 필터링 및 분석기를 통해 서버로 전송해야 하는 데이터만을 추출한다. 그리고 ⑤의 LPA 메시지 생성기에서 ①의 환경정보내의 필터링 정보를 기반으로 하여 ⑦의 LPA 연동 메시지(LPA헤더+수집데이터)를 생성한다. LPA 헤더는 수집된 데이터의 송신/수신 노드의 IP주소와 포트번호를 기반으로 서버 시스템 ID와 노드 ID를 추출하여 생성된다. 생성된 LPA 연동 메시지는 전송관리자를 통해 LPA 서버로 전송된다.



▶▶ 그림 2. LPA 에이전트 구성도

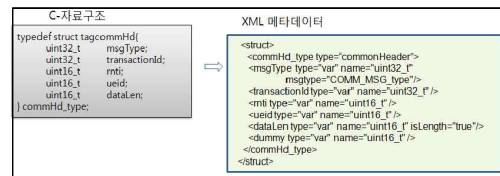
서버는 각 에이전트로부터 연동 메시지를 수집하고, XML 메타 데이터에 맞게 패킷을 분석하는 역할을 담당한다. LPA 서버는 [그림 3]과 같이 구성이 되며, 구성화 일에는 에이전트로부터 메시지를 수신하기 위한 통신정보와 메시지 상세 분석 시 사용을 위한 LTE 시스템의 계층적 구조 정보가 저장된다. XML 메타데이터는 운용자가 시스템의 연동 메시지를 LPA XML 작성 툴을 참조하여 작성한다. ④의 통신관리자는 LPA 에이전트에서 전송한 데이터를 수신하고, ⑤의 메시지 전처리기에서 LPA 헤더를 분석하여 추출한 연동메시지 요약정보는 GUI 상에 도시하고, 수신된 메시지는 메시지 풀에 저장

한다. 운용자가 특정 메시지에 대한 상세 출력을 요청하면, ⑥의 메시지 풀 관리기를 통해 메시지를 추출하고, ⑦과 ⑧을 통해 세부 분석된 데이터를 GUI를 통해 화면 상에 도시한다. 운용자가 특정 시스템이나 특정 메시지에 대해서만 출력을 원할 경우 ⑨의 메시지 필터에서 이를 처리한 후 GUI 상에 도시한다.



▶▶ 그림 3. LPA 서버 구성도

[그림 4]는 기본 연동 규격 메시지를 XML 메타데이터로 작성한 변환 예제를 나타낸 것이다. 제공하는 메시지 규격은 bit, int, long등의 기본 연산자 외에 enum, union, struct 같은 구조화된 형태까지 지원할 수 있다.



▶▶ 그림 4. XML 메타데이터 생성 예

### IV. 결론 및 향후 연구

본 논문에서는 LTE 시스템을 위한 에이전트-서버 구조의 프로토콜 분석기를 제안하였다. LTE 시스템을 구성하는 서버 시스템 및 하위 기능 노드들간의 연동 메시지를 XML 메타 데이터로 표기하고 분석 시 이를 활용할 수 있다. 따라서 LPA 개발되는 LTE 시스템마다 특화하여 적용할 수 있다. 또한, 연동 규격 변경 시에도 XML 메타 데이터만을 수정하여 프로토콜 분석에 사용할 수 있다는 장점이 있다. 본 LPA를 활용함으로써 개발 단계 및 운용 단계에서 발생하는 문제를 파악하여, LTE 서비스를 이용하는 모바일 사용자들에게 보다 안정적인 모바일 멀티미디어 콘텐츠를 제공할 수 있다.

향후 연구는 LTE 프로토콜 중 ASN.1 인코딩이나 바이너리 인코딩되어 연동되는 메시지에 대한 분석 방법을 연구하는 것이다.

#### ■ 참고 문헌 ■

- [1] 오돈성 외, "3GPP LTE 기술 개발 및 서비스 동향", 전자통신동향분석, 제25권, 제6호, pp.20-28, 2010.12.
- [2] 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," Dec. 2009.
- [3] Wireshark, URL [March 28, 2011] : <http://www.wireshark.org>