Journal of Ubiquitous Systems & Pervasive Networks
Volume 3, No. 2 (2011) pp. 55-58

Implementation of Decoders for LTE Interface Messages

Manjula M, G. Varaprasad*

Department of Computer Science and Engineering, B.M.S.College of Engineering, Bangalore560 019, India.

Abstract

Long-term evolution is the next-generation network beyond 3G. In order to initiatively imitate and improve network performance, by research and analysis of signaling message which is transmitted in the LTE network architecture, a decoder module is needed. In this paper, the decoding modules for decoding S3, S4, S5/S8, S10 and S11 interfaces, which use GTPv2 protocol to transmit the messages between the various entities such as SGSN – MME, SGSN - SGW, SGW - PGW, MME – MME, MME - SGW and MME – EIR, respectively are explained. Further, in LTE architecture, there is another interface S1MME which uses S1AP protocol between the eNB and MME entities; in similar way interfaces S13(MME to EIR), S6a (MME to HSS), Gx (PCRF to PCEF), and SGi (between PGW & PDN) which uses diameter protocol, need to be decoded. Hence, to incorporate the decoding of message fields of above said interfaces in the proposed system, the existing Alcatel-Lucent framework LTEPA is enhanced as the project work.

***Keywords:** LTE; GTPv2; Diameter; S1ap;*

1. Introduction

With the development of mobile communication technology and the integration of mobile communications and broadband wireless access technology, 3GPP carried out long term evolution of Universal Terrestrial Radio Access (UTRA) Technology (i.e., Long Term Evolution (LTE)). Compared to the previous TD-SCDMA 3G mobile communication system, LTE can provide support for various data transmission rates.

The LTE system architecture is evolved from 3GPP. It integrates the NodeB, RNC and CN of WCDMA and TDSCDMA architecture. The system architecture is simplified and only contains two network elements, eNodeB and EPC. The eNodeB is a merger of NodeB and RNC and Evolved Packet Core (EPC) is the all-IP mobile core network for 3GPP LTE. EPC embodies three logical entities such as Mobility Management Entity (MME), Serving Gateway (S-GW) and PDN Gateway (P-GW). P-GW is the termination towards of PDN's, which implements policy enforcement, charging support, DHCPv4 or DHCPv6 functions. In the LTE EPC architecture, P-GW locates at the edge of the core network and subscribes external IP network via P-GW. It implements the Authentication, Authorization and Accounting (AAA) services and serves as one of the extended applications based on diameter/radius protocol named as Network Access Server Requirement (NASREQ). The rest of this paper is organized as follows. In section 2, we present some background information on GTPv2, diameter and S1ap protocols. Section 3 describes the interfaces. In section 4, working model is explained. Finally, conclusion is presented in section 5.

2. Preliminaries

2.1. GTPV2 Protocol

The GTP tunnels are used between two nodes communicating over a GTP based interface, to separate traffic into different communication flows [1]. A GTP tunnel is identified in each node with a Tunnel Endpoint Identifier (TEID), an IP address and a UDP port number. The receiving end side of a GTP tunnel locally assigns the TEID value which the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C. GTPv2-C shall be used across the EPC signaling interfaces such as S3, S4, S5, S8, S10 and S11. Control plane GTP uses a variable length header. Header length shall be a multiple of 4 octets. The GTP-C header is followed by subsequent Information Elements (IE's) dependent on the type of control plane message.

The section heading is centered within the column and the style is 10-point Times New Roman boldface. The format includes 18-point spacing before and a 3-point after. Note also the added blank line after. Specific information on other important items follows. All sections and 1st, 2nd and 3rd level sub-section headings should be copied on from the samples provided herein with numbering scrupulously observed.

[*] G.Varaprasad. Tel.: +91-9449612596
E-mail: varaprasad555555@yahoo.co.in

DOI: 10.5383/JUSPN.03.02.003

2.2. Diameter Protocol

The diameter protocol [2] was derived from the RADIUS protocol with a lot of improvements in different aspects and is generally considered to be the next generation Authentication, Authorization and Accounting (AAA) protocol. The diameter protocol has been widely used in the Internet Protocol Multimedia Subsystem (IMS) architecture for IMS entities to exchange AAA-related information. Because the IMS system might be the next important issue in the telecom industry, we believe that a clear understanding of the diameter protocol is necessary for understanding the essence of the IMS architecture. The diameter-based protocol is extended for each particular application, which has been extended for diameter NASREQ application[3], in order to support NASREQ function. In this circumstance, the diameter client is also named as Network Access Server (NAS).

2.3. S1ap Protocol

S1 Application Protocol (S1AP) is the control plane signaling protocol between the eNodeB and MME. The S1AP provides the signaling service between the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and EPC [4]. The S1AP services are divided into two groups:

- Non UE-associated services: They are related to the S1 interface instance between the eNB and MME, utilizing a non UE-associated signalling connection.
- UE-associated services: They are related to one UE.

The S1AP functions that provide UE-associated services are associated with a UE-associated signalling connection that is maintained for the UE in question. The S1AP consists of Elementary Procedures(EPs). An elementary procedure is a unit of interaction between the eNBs and EPC. These EPs are defined separately and are intended to be used to build up complete sequences in a flexible manner. If the independence between some EPs is restricted, then it is described under the relevant EP description. Unless otherwise stated by the restrictions, the EPs may be invoked independently of each other as standalone procedures, which can be active in parallel.

3. Description

In this section, the details about the various interfaces under GTPv2, diameter and S1ap are discussed. To support the new LTE air interface as well as roaming and mobility between the LTE and UTRAN, the Evolved Packet System(EPS) architecture contains the interfaces. The main interfaces in the LTE are depicted in fig.1. The explanations for major interfaces, which are dealt in the paper, are given in this subsection.

The S1-MME is the reference point for the control plane protocol between the E-UTRAN and MME. The eNB and MME communicate using this IP interface. The S1-AP is the application layer interface. The transport protocols used here is Stream Control Transmission Protocol (SCTP). S5 provides user plane tunneling and tunnel management between the SGW and PGW. It is used for serving GW relocation due to UE mobility and if the SGW needs to connect to a non-collocated PDN GW for the required PDN connectivity. S8 is the inter-Public Land Mobile Network (PLMN) reference point providing user and control plane between the SGW in the Visited PLMN (VPLMN) and the PDN GW in the Home PLMN (HPLMN). S8 is the inter PLMN variant of S5.

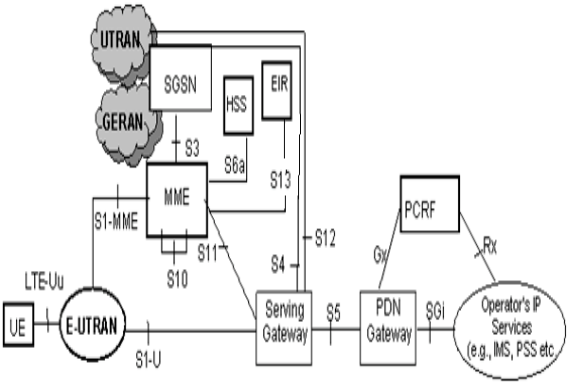


Fig. 1. LTE Network Reference Diagram depicting the Interfaces.

The S10 serves as a reference point between the MMEs for MME relocation and MME to MME information transfer. GTP C is protocol tunnel signaling messages between the MMEs(S10). The UDP protocol is used for transferring signaling messages between the MMEs. S11 is an IP interface between the MME and SGW. GTPv2 is the protocol used at the application layer. GTPv2 runs on UDP transport, which transfers signaling messages. This interface must and should run on GTPv2. The S13 is used to check the validity of the UE identity. This interface enables UE identity check procedure between the MME and Equipment Identity Register (EIR). Diameter protocol does support this. The SCTP protocol transfers the signaling messages. S13 interface enables the MME and EIR to:

- verify that the UE has not been stolen
- verify that the UE does not have faults

LTE S6a interface enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between the MME and HSS. Diameter is used for this. For transferring signaling messages SCTP protocol is used. The S2a interface provides the user plane with related control and mobility support between trusted non 3GPP IP access and the PDN Gateway. S2a is based on Proxy Mobile IPv6 (PMIP). To enable access via trusted non-3GPP IP accesses that do not support. The Gx interface provides transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PGW. The SGi is reference point between the PGW and the packet data network. The packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services.

4. Working of Decoders

When the captured packet data is given to the framework, each layer of the protocol is decoded header by header until there is no more data left for decoding.

4.1. Steps involved in decoder algorithm

- The packet frame data is passed to the main function which frees all memory if allocated for previous packet.

- The frame data is dissected for the arrival time, frame number, frame length etc and displays the same in decode window of the GUI.
- The process of decoding each layer of the protocol continues header by header until it reaches the actual protocol needed and there are no more data to decode or no more registered decoders for the rest of data.
- Different modules are executed based on the port number.

The decoder modules are explained with the flow chart given in fig. 2. Decoding of different protocol messages are based on the port numbers. The header of the message is decoded first and then the remaining data are decoded.

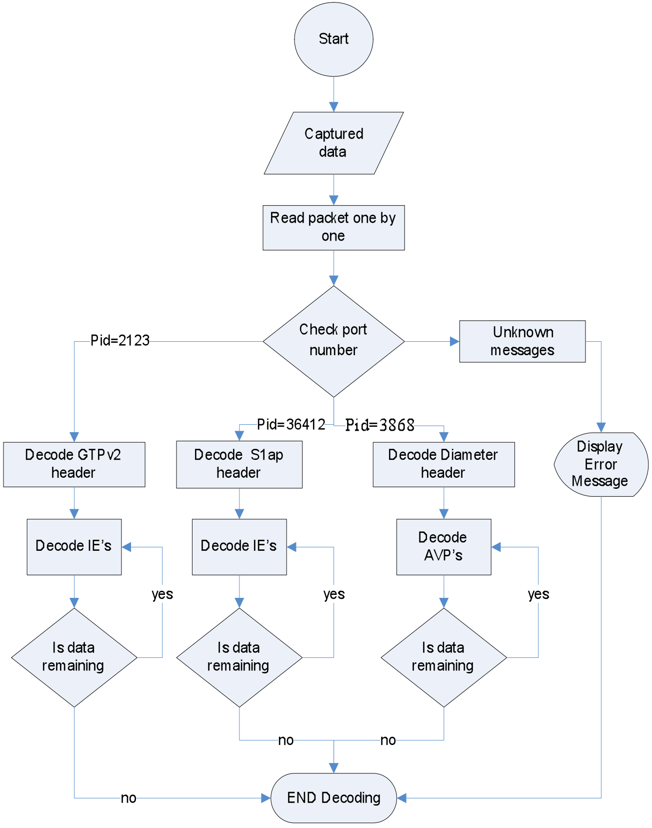


Fig.2. Flow chart for Decoder.

4.2. Implementation of S1ap Module Using ASN.1

In order to realize of ASN.1 decoding module, steps involved are:

(1) Make message (i.e. in s1ap.asn), which is described using ASN.1 language in the protocol stack, compile it into a C language description of the source file (s1ap.h);

(2) Generate the corresponding C data structures codec functions (s1ap.c) from message (s1ap.asn), which is described using ASN.1 language in the protocol stack.

Compilation is done by compiling s1ap.asn, which is described in the ASN.l language, to s1ap.h files and its corresponding s1ap.c file as shown in fig. 3. More to say: each of the ASN.l data types are mapped to the data structure and its corresponding decoding function in C language. s1ap.h files are generated for the statement after the C compiler data types and s1ap.c files are used to implement the decoding functions. Then the decoding functions call decoding ASN.1 basic function library to achieve decoding functions. Finally get the executable files to the framework, thus completing the conversion from the ASN.1 description to the binary bit stream, making its information transmission in LTE system network.

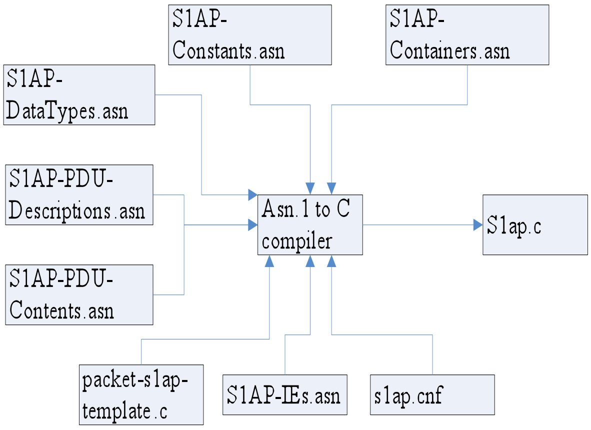
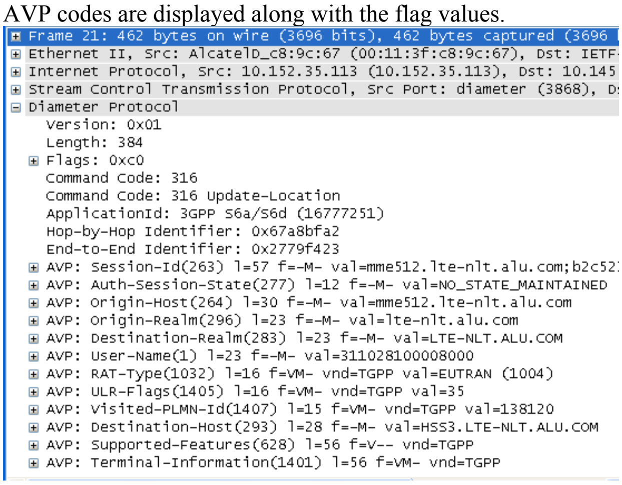


Fig.3. Process of generating ASN.1 S1ap decoder.

4.3. Results

The decoder for LTE messages will decode each and every field of the message. For GTPv2, all the message IE's are displayed. The S1ap procedure IE's are also decoded. Fig.4 displays the AVP's which are decoded for diameter protocol messages for the diameter interfaces. It shows the message Update-Location which is a diameter protocol message with the message id 316. The Update-Location command consists of various AVP's which are listed in the GUI. AVP names and AVP codes are displayed along with the flag values.



```
⊞ Frame 21: 462 bytes on wire (3696 bits), 462 bytes captured (3696
⊞ Ethernet II, Src: AlcatelD_c8:9c:67 (00:11:3f:c8:9c:67), Dst: IETF-
⊞ Internet Protocol, Src: 10.152.35.113 (10.152.35.113), Dst: 10.145
⊞ Stream Control Transmission Protocol, Src Port: diameter (3868), D
⊟ Diameter Protocol
    Version: 0x01
    Length: 384
  ⊞ Flags: 0xc0
    Command Code: 316
    Command Code: 316 Update-Location
    ApplicationId: 3GPP S6a/S6d (16777251)
    Hop-by-Hop Identifier: 0x67a8bfa2
    End-to-End Identifier: 0x2779f423
  ⊞ AVP: Session-Id(263) l=57 f=-M- val=mme512.lte-nlt.alu.com;b2c52
  ⊞ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED
  ⊞ AVP: Origin-Host(264) l=30 f=-M- val=mme512.lte-nlt.alu.com
  ⊞ AVP: Origin-Realm(296) l=23 f=-M- val=lte-nlt.alu.com
  ⊞ AVP: Destination-Realm(283) l=23 f=-M- val=LTE-NLT.ALU.COM
  ⊞ AVP: User-Name(1) l=23 f=-M- val=311028100008000
  ⊞ AVP: RAT-Type(1032) l=16 f=VM- vnd=TGPP val=EUTRAN (1004)
  ⊞ AVP: ULR-Flags(1405) l=16 f=VM- vnd=TGPP val=35
  ⊞ AVP: Visited-PLMN-Id(1407) l=15 f=VM- vnd=TGPP val=138120
  ⊞ AVP: Destination-Host(293) l=28 f=-M- val=HSS3.LTE-NLT.ALU.COM
  ⊞ AVP: Supported-Features(628) l=56 f=V-- vnd=TGPP
  ⊞ AVP: Terminal-Information(1401) l=56 f=VM- vnd=TGPP
```

Fig.4. Decoded AVP's for Diameter S6a Interface.

5. Conclusion

The framework, which can decode the interface messages such as for GTPv2, S1ap, diameter protocols are implemented. This framework is used to decode LTE specific interfaces messages (i.e. hex dumps) in easy understandable format. The goal is to enhance the existing framework that empower users to do some basic trouble shooting, with the minimum understanding of the messages that are exchanged within the system. This also helps experienced users to quickly analyze and debug problems by allowing them to dive into the details of the messages between the interfaces. The decoder module must imitate and improve the network performance, by analysis of signaling messages, which are transmitted in the LTE network architecture. The work meets the 3GPP protocol actual requirements.

References

[1] 3GPP TS 29.274 V8.4.0 3rd Generation Partnership Project; Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)

[2] P. Calhoun, J. Loughney, E. Gutman, G. Zorn, and J. Arkko, “Diameter Base Protocol,” IETF RFC 3588, Sept. 2003.

[3] B. Aboba and D. Simon. PPP EAP TLS Authentication Protocol., IETF RFC 2716, October 1999.

[4] 3GPP TS 36.413 V9.5.0 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)

[5] ITU-T Recommendation X.69 1(2002), Information technology-ASN.I encoding rules - Specification of Packet Encoding Rules (PER).

[6] Xiaowen Li, Ning Wang, "Design and implementation of encoder and decoder for ASN.I in TD-SCDMA system". Chongqing University of Posts and Telecommunications (Natural Science), vol. 21, Jun. 2009, pp.358-361.

[7] P. Calhoun, J. Loughney, E. Gutman, G. Zorn, and J. Arkko, “Diameter Base Protocol,” IETF RFC 3588, Sept. 2003

[8] 3GPP. TS 36.331 v.9.2.0 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) protocol specification. Http://www.3gpp.com. 2010

[9] ITU-T Recommendation X.680(2002), abstract syntax notation(ASN.I) - specification of basic notation

[10]Xiaowen Li, Guiyong Li, Xianliang Chen, TD-SCDMA third generation mobile communication systems, signaling and Implementation. Beijing: Posts & Telecom Press, 2003

[11] 3GPP TS 23.402, [UMTS; LTE;Architecture Enhancements for Non 3GPP access], Release 8

[12] 3GPP TS 29.230, [3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Diameter applications; 3GPP specific codes and identifiers], Release 9