



LTE 网络测试仪中 S6a 接口 Diameter 协议监测方案研究^{*}

王朝阳¹, 曹龙汉², 张治中¹

(1. 重庆邮电大学通信网与测试技术重点实验室 重庆 400065;

2. 重庆通信学院控制工程重点实验室 重庆 400035)

摘要: 在介绍 LTE 网络测试仪功能的基础上, 阐述了 S6a 接口 Diameter 协议的基本概念和功能, 设计了 Diameter 协议的监测方案。针对 Diameter 消息结构的特点, 利用模块化的思想设计了 Diameter 协议的解码方案。针对以前网络监测技术中 CDR (call detail record, 呼叫详细记录) 合成时效性不足的问题, 提出了基于缓存索引算法和超时管理机制的 CDR 合成方案, 保证了合成的有效性和准确性, 大大提高了合成的效率。最后使用 LTE 现网数据对该方案进行测试, 结果准确, 效果良好。

关键词: LTE; Diameter; 监测方案; 解码模块

doi: 10.3969/j.issn.1000-0801.2014.05.022

Research on Diameter Protocol Monitoring Scheme of S6a Interface in LTE Network Tester

Wang Chaoyang¹, Cao Longhan², Zhang Zhizhong¹

(1. Key Laboratory on Communication Networks and Testing Technology,

Chongqing University of Posts and Telecommunications, Chongqing 400065, China;

2. Key Laboratory on Control Engineering, Chongqing Communication College, Chongqing 400035, China)

Abstract: On the basis of introducing the functions of LTE network tester, the Diameter protocol's basic concept and functions of S6a interface were described, and the Diameter protocol monitoring scheme were designed. In consideration of the characteristics of Diameter message structure, the Diameter protocol decoding scheme was designed with the idea of modularization. Previous networks monitoring technology for CDR synthetic has the problem of insufficient timeliness, so a new CDR synthetic scheme with caching index algorithm and overtime management mechanism was proposed. It ensures the effectiveness and the validity of CDR synthetic, greatly improving the efficiency of synthesis. Using the LTE networks data to test the scheme, the results are accurate and the effects are good.

Key words: LTE, Diameter, monitoring scheme, decoding module

1 引言

中国移动 LTE 试验商用网已经在上海、广州、深圳等

城市实现了主城区的全覆盖, LTE 基站数已达到 2 万个左右, LTE 网络也将逐渐在全国各个城市布局^[1]。为了保证 LTE 网络的质量和稳定性, 对网络的监测显得非常重要。

^{*} 国家科技重大专项基金资助项目 (No.2012ZX03001021-004), 国家发展和改革委员会电子信息产业振兴项目 (No.2012[995]), 国家火炬计划基金资助项目 (No.2012GH011751)



LTE 网络测试仪通过对 LTE 网络中各个接口信令数据的采集与分析,实现对整个 LTE 网络运行状况的监测。LTE 网络测试仪采用分布式、模块化、可组合的架构体系,易于维护和扩展,能够针对不同的需求进行快速的个性化设计,对网络的监测更加高效、可靠、稳定^[23]。LTE 网络测试仪能够进行网络监测、故障定位和网络优化,为 LTE 网络的运行维护提供强大的技术支撑,从而加速 LTE 网络的推广和产业化发展。S6a 接口 Diameter 协议的监测方案是 LTE 网络测试仪中重要的组成部分,本文重点介绍监测方案的设计,包括整体方案设计、协议解码设计、CDR 合成设计,并利用 LTE 现网数据对监测方案进行了测试。

2 Diameter 协议监测方案设计

S6a 接口是 LTE 网络中 MME (mobility management entity, 移动性管理实体)与 HSS(home subscriber server, 归属用户服务器)之间的接口,Diameter 协议是 S6a 接口的应用层协议,是支持基于 IP 技术的 AAA 框架的 AAA 协议。AAA 包括认证、计费 and 鉴权。认证是网络系统对用户身份的确认;计费是指网络系统根据用户对资源的使用情况进行收费;鉴权是指用户在网络系统授权的情况下以特定的方式使用其资源。网络系统对特定用户资源使用情况的准确记录是依靠认证、计费、鉴权实现的,这样既保障了合法用户的权益,又保障了网络系统安全可靠地运行。Diameter 协议包括基础协议、网络接入服务协议、可扩展鉴别协议等,其作用是对用户认证、计费和鉴权等相关信息进行处理^[4]。

根据相关测试规范的要求,Diameter 协议监测主要包括以下几个功能:Diameter 协议简单解码、详细解码和 CDR 合成。Diameter 协议监测流程如图 1 所示。

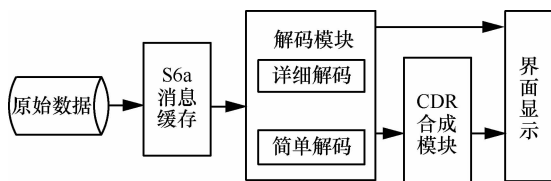


图 1 Diameter 协议监测流程

根据原始数据的不同来源,监测模式可分为实时监测模式和数据回放模式^[6]。在实时监测模式下,原始数据来源于采集卡捕获的现网数据;在数据回放模式下,原始数据来源于从现网上采集并已保存的数据。原始数据经过 S6a 接口的筛选,将消息保存到消息缓存中。S6a 接口解码模

块从消息缓存中取出消息,逐跳逐层次地解码,详细解码模块获得消息每一个比特的详细信息,简单解码模块只提取消息的关键字段,如消息特征字段信息等,并把关键字段封装到 CDR 合成信息类中。CDR 合成模块的功能是把同一用户同一业务中相关联的信息组合在一起,形成一个完整的信令流程,如认证、位置更新等。用户在界面上可以根据需要触发解码、CDR 合成等流程,或检查网络运行情况。

对各个模块进行独立设计,并以动态链接库的形式进行连接,模块之间耦合度低,功能独立,从而既能防止故障扩散,又能缩短软件开发周期,并具有良好的扩展性。

3 Diameter 协议监测分析及实现

3.1 Diameter 协议解码

Diameter 协议解码由简单解码和详细解码两部分组成。简单解码是 CDR 合成的基础,对信令消息进行部分解析,主要包括消息 ID、消息来源、消息接收时间、消息类型等基本信息,便于界面消息索引;详细解码是对消息进行逐比特地解码,将 Diameter 消息的所有字段全部解析出来,并将解码结果反馈给显示模块用于界面呈现。解码思路是采用逐跳逐层次的方式对消息进行解析,将解码函数模块化、定义和实现相分离,从而提高代码的独立性和可移植性。

Diameter 消息结构如图 2 所示^[9],从功能上可以划分为 Diameter 消息头和一个或多个属性值字段——AVP (attribute value pair, 属性值对)。Diameter 消息头包括版本号、消息长度、命令标识位、命令字、应用 ID、逐跳标识符和端对端标识符;AVP 字段用于封装协议应用的信息,如路由消息、计费消息等。

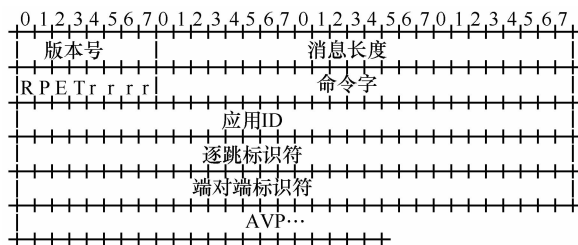


图 2 Diameter 消息结构

针对 Diameter 消息结构的特点,设计 Diameter 详细解码流程如图 3 所示。在详细解码线程启动后,详细解码函数通过函数入参获取待解码消息的数据长度和头指针,然后函数会进行数据是否有效的判断,如 Diameter 的消息头

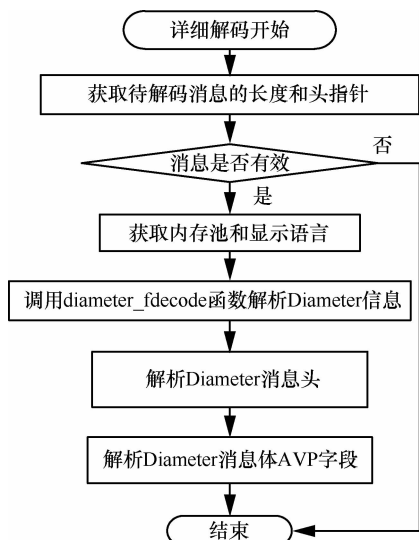


图3 详细解码流程

占 20 byte, 如果数据的长度小于 20 byte, 那么数据无效, 解码结束并返回解码数据出错的提示; 如果数据有效, 解码函数获取内存池句柄和显示语言的种类, 同时调用 `diameter_fdecode` 函数对数据进行解码, 解码函数采用逐层解析的方式, 首先解析 Diameter 的消息头, 然后解析 Diameter 消息体 AVP 字段。如果显示的语言种类为中文, 将调用中文的解码函数; 如果是英文, 将调用英文的解码函数。

3.2 Diameter 协议 CDR 合成

3.2.1 CDR 合成算法设计

CDR 合成是将消息按信令流程归类, 并按照特定关系将其关联起来, 还原出真实的通信流程, 为流程查询、网络指标统计和故障定位等功能提供数据支撑, 是信令监测中非常重要的环节^[6]。

CDR 合成通常采用红黑树索引合成算法, 当网络中的数据量比较小时, 使用此算法是高效、准确的, 但随着网络的飞速发展, 网络中的数据量急剧增加, 继续使用此算法会导致合成效率低下, 部分合成结果不准确。针对网络中数据量庞大的问题, 在 CDR 合成时提出了高效的缓存索引算法, 以空间换时间, 实现了监测系统对海量数据的高效、准确处理。缓存索引算法采用以特定的 key 值为索引、CDRID 为映射值的数据结构模式, 对 key 值和待查找信息的存储地址建立映射关系, 并且映射关系是唯一的, 这样就可以通过 key 值直接找到其对应的存储地址, 从而大大提高了合成效率。

3.2.2 CDR 超时处理机制

采集数据时可能会出现分组丢失、设备故障等问题,

从而有可能导致信令数据不完全等异常情况出现, 信令数据不全会导致 CDR 合成无法结束, 最终导致 CDR 合成错误。针对此问题, 提出了超时处理机制, 原理是通过建立链表记录缓存索引中每个 CDR 的 key 值和超时时间, 创建每个 CDR 时都在超时链表中添加一个节点, 该节点的结构体包括该 CDR 对应的 key 值和预设的超时时间。每当有新的消息进入 CDR 合成模块时, 合成模块都会调用 `CheckTimeCdr` 函数查询并处理超时链表中的超时节点。在对链表中的超时节点处理完成后, 合成模块会删除链表中的超时节点, 这样就消除了缓存索引表中超时的 CDR。

3.2.3 CDR 合成实现

根据 Diameter 协议的特点, S6a 接口 Diameter 的 CDR 合成关键字采用目的 IP 地址、目的 SCTP 端口号、源 IP 地址、源 SCTP 端口号, 四者均能唯一标识传送双方, 会话 ID 在同一个信令流程中是相同的, 因此通过这几个参数就能确定同一个信令流程。CDR 合成建立在简单解码的基础上, 简单解码为 CDR 合成提供必要的信息, 如 Diameter 的应用 ID、消息。CDR 合成流程如图 4 所示, 具体分为如下几步。

(1) 简单解码结束, 将合成所需的信息提交给合成模块, 并触发合成。

(2) 合成开始后, 检查缓存中的 CDR 是否存在超时的情况, 如果有, 则对超时的 CDR 进行处理。

(3) 从简单解码结果中提取 Diameter 的应用 ID 进行判断。

(4) 根据判定的结果进入不同的应用分支并进行相应的处理, 以 S6a 接口的合成为例进行说明。

(5) S6a 合成模块从简单解码的结果中提取建立合成缓存区所需要的 key 值。

(6) 在 S6a 合成模块的 CDR 缓存中查找是否有与当前 key 值对应的 CDR, 如果不存在, 则进行第 (7) 步, 如果存在, 就进行第 (8) 步。

(7) 在合成缓存区中插入 key 值, 同时创建一个新的 CDR, 并为其分配一个 CDR ID, 同时将简单解码的结果填入对应的 CDR 属性中。

(8) 在合成缓存区中找到与 CDR ID 对应的 CDR, 并利用简单解码的结果更新该 CDR, 更新完成后判断该 CDR 是否结束, 如果没有结束则进行第 (9) 步, 如果结束就进行第 (10) 步。

(9) 设置 CDR 超时时间, 并将其放入 S6a 模块的 CDR 缓存中, 重复上述 Diameter 协议合成流程。

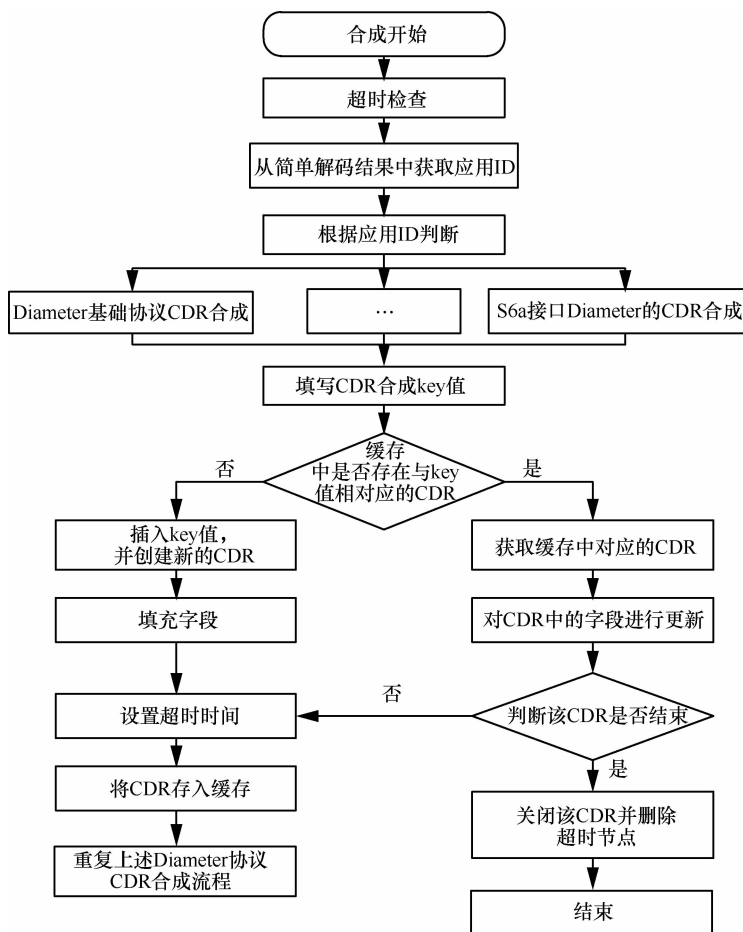


图4 合成流程

(10)关闭该 CDR,删除超时节点,合成完成。

4 测试结果与分析

利用 LTE 网络的现网数据对监测系统进行测试,包括解码测试和 CDR 合成测试。LTE 网络测试仪中详细解码的界面显示为用户提供了中文和英文两种语言,解码结果以树型结构呈现。一条消息的中文解码结果如图 5 所示,在消息列表的消息特征栏中显示这是一条位置更新消息,将 Diameter 协议展开,显示 Diameter 协议的版本号、消息分组的长度以及命令标识、命令码、应用标识、跳到跳标识、端到端标识和一系列 AVP 值。从请求消息标识位的值可知,该消息为 update location request(即位置更新请求消息)。由解码结果的树型结构可知,协议最上层为 Diameter 协议,底层依次是 SCTP、IP、Ethernet 协议,界面上对消息中的字段名、字段值、解释及位掩码等信息进行了详细说明。通过与原始数据及协议进行对比,证实解码结果是完整、正确的。

S6a 接口上一次位置更新消息的 CDR 流程如图 6 所示。首先 MME 向 HSS 发送一条认证请求消息 authentication information request,合成模块提取这条消息的会话 ID、源 IP 地址和目的 IP 地址、源 STCP 端口号和目的 STCP 端口号等信息,并创建 CDR。HSS 收到认证请求消息后,向 MME 回复一条认证响应消息 authentication information answer,合成模块判断该消息携带的 key 值后,对 CDR 进行填充。在收到 HSS 发送的认证响应消息后,MME 向 HSS 发送位置更新请求消息 update location request,HSS 又向 MME 发送位置更新响应消息 update location answer。在收到位置更新响应消息后,合成模块填充了位置更新结束时间,CDR 合成结束。

在此次 CDR 合成中,用户在 HSS 中注册的 IMSI 为 404309990000002,通过消息编号查找这 4 条消息的详细解码结果,这 4 条消息的会话 ID 一致,再结合相关协议规范中 Diameter 同一个信令流程中会话 ID 相同的原则,证明该 CDR 合成正确。



图 5 Diameter 协议解码结果

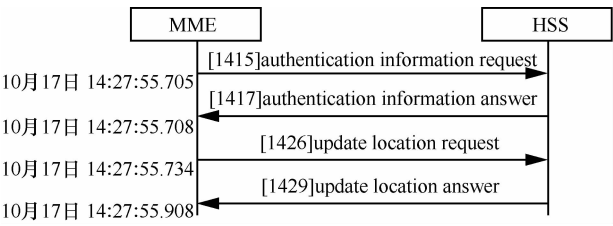


图 6 CDR 合成流程

5 结束语

通过对 LTE 网络 S6a 接口 Diameter 协议的研究,提出了针对 Diameter 协议的监测方案,即协议解码和 CDR 合成方案。监测方案在开发时使用 VS2010 开发环境,利用面向对象的思想,设计了模块化的解码方案和高效的 CDR 合成方案。该监测方案已通过 LTE 现网数据的测试,取得良好的监测效果。该监测方案的设计方法对于设计 LTE 网络中其他协议的监测方案具有指导和推广意义。

参考文献

1 黄海峰. 4G 为移动互联网带来变革 中国移动 TD-LTE 发展思路明确. 通信世界, 2012(21)
2 李艳, 张治中. LTE 网络 SIAP 监测方案的研究与实现. 电信科学, 2013, 29(1):31~38
3 李丹凤, 张治中. LTE 网络监测系统中 DHCP 协议的解码方

案研究. 电视技术, 2012, 36(9):69~73
4 3GPP TS 29272. Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) Related Interfaces Based on Diameter Protocol(Relase 12), 2013
5 IETF RFC5516. Diameter Command Code Registration for Third Generation Partnership Project (3GPP) Evolved Packet System (EPS), 2009
6 杨理想, 张治中. GSM 用户感知系统中 BTSM 协议监测方案研究. 重庆邮电大学学报: 自然科学版, 2012, 24(6):751~755

[作者简介]



王朝阳,男,重庆邮电大学通信网与测试技术重点实验室硕士生,主要研究方向为通信网测试技术、通信协议软件开发。

曹龙汉,男,重庆通信学院控制工程重点实验室博士生导师、教授,主要研究方向为智能信息处理、自动控制等。

张治中,男,重庆邮电大学通信网与测试技术重点实验室博士生导师、教授,主要研究方向为通信网测试技术、宽带信息网络、NGN 等。

(收稿日期:2013-11-22)