



LTE 网络 S1AP 监测方案的研究与实现^{*}

李 艳, 张治中

(重庆邮电大学通信网与测试技术重点实验室 重庆 400065)

摘 要:为实现对 LTE 网络中 S1AP 的监测,在介绍 LTE 网络测试仪软件平台设计方案的基础上,针对国内外现有网络协议监测技术中协议解码、呼叫记录(call data record, CDR)合成研究方案的时效性的不足,设计了 S1AP 监测模块的实现方案。该方案采用定义和实现相分离的方法进行消息解码,提高了代码的独立性和可移植性,使用散列索引和超时管理机制进行 S1AP 消息合成,保证了合成的准确性和有效性。本文方案已成功应用于 LTE 网络测试仪中,使用仿真数据进行测试,效果良好。

关键词: LTE; S1AP; 协议监测; 散列索引

doi: 10.3969/j.issn.1000-0801.2013.01.005

Research and Implementation of S1AP Monitor in LTE Network

Li Yan, Zhang Zhizhong

(Key Lab on Communication Networks and Testing Technology,

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

Abstract: For realizing S1AP monitor in LTE network, the implementation scheme of S1AP protocol monitoring module was designed to cope with the insufficiency of protocol decoding and CDR synthesis research scheme effectiveness, on the base of introducing LTE network monitor software platform. The scheme adopted the thought of separating definition and realization for message decoding, improving the code independence and portability. The use of Hash index and overtime management mechanism of S1AP message synthesis ensured the accuracy and validity of synthesis. The scheme had been successfully applied to LTE network monitor. It has been proved to have a good effect by simulation data for testing.

Key words: LTE, S1AP, protocol monitor, Hash index

1 引言

作为 3G 与 4G 技术之间的一个过渡, LTE 由于其众多优势, 成为全球移动通信的发展趋势和方向^[1]。在通信网络的监测方面, 国内外均有各种监测产品, 但主要针对 2G 和 3G 网络如 GSM、WCDMA、cdma2000 等, 而针对 LTE 网络的监测产品较少。在 LTE 网络建设和优化、维护过程中, 对网络质量的测试和评估非常必要, 完善 LTE 网络监测技

术十分重要。S1 接口将 EPC 和 E-UTRAN 连接起来, 是 LTE 网络中的核心节点, 所有从接入网到核心网的信令都要经过 S1 接口^[2,3], 若 S1 接口出现故障, 对网络造成的影响不可估计。S1AP 是 S1 接口控制平面的应用层协议, 因此, 对 S1AP 的监测可以迅速感知网络中各节点的运行状况并定位故障, 意义重大。

结合 LTE 网络测试仪的功能和软件架构, 提出了 S1AP 监测方案, 分别对协议解码、CDR 合成、多段关联和

^{*} 国家发改委(渝发改技[2009]1135), 中芬国际合作项目(No.S2010GR0902)



统计的设计与实现进行了详细阐述。针对解码模块中传统的全字段解析,本文采用定义和实现相分离的思想,提高了代码的独立性和可移植性;由于目前国内外 CDR 合成多采用二叉树的查找算法,无法满足现网大数据量合成的需求,导致出现大量 CDR 合成信息丢失、合成不全的严重后果,通过采用散列索引和超时管理机制进行 CDR 合成,保证了合成的准确性和有效性;将多段关联和统计模块的处理流程嵌入合成流程中,增加了可靠性和实时性。最后结合大量仿真数据对 S1AP 监测方案进行了测试和验证,并对解码模块、合成模块和多段关联模块的结果进行了展示和分析。分析结果表明,该方案能够准确、有效地实现 S1AP 的信令监测,达到预期目标。

2 S1AP 监测方案设计

S1AP 作为 LTE 网络监测仪表不可缺少的监测协议,其监测方案的研究与开发依托于仪表架构进行。LTE 网络监测仪表通过采集卡捕获 LTE 网络中的信令数据,并为信令数据加上分组头后存入消息缓存,其中分组头信息包括采集时的链路信息、时间戳和消息编号,消息编号由消息进入缓存的顺序分配,其与消息之间是一一对应的关系。

数据处理层对信令数据进行协议分析,并将分析结果提供给应用层,用于界面显示。结合 LTE 网络监测仪表的信令数据处理流程,S1AP 的监测主要包括协议解码、CDR 合成、多段关联和统计 4 个部分,S1AP 监测总体架构如图 1 所示。

图 1 中,原始数据指的是消息缓存中的信令数据,读取到数据后,进入解码模块对消息进行解码,然后通过 CDR 合成模块、统计模块和多段关联模块进行协议分析,

从而实现对 S1AP 的监测。界面通过消息列表、过滤、CDR 流程图、协议层次和统计结果等来显示 S1AP 分析结果,用户通过查看界面的结果可获取 LTE 网络 S1AP 的运行情况。

3 S1AP 监测方案的实现

3.1 S1AP 解码模块的设计与实现

解码模块包括进行全字段解析的详细解码和进行部分字段解析的简单解码、合成解码。详细解码是将消息进行完整的解码后,为界面提供显示的信息;简单解码和合成解码都只提取必要的信息,简单解码的结果直接用于界面的消息列表和过滤等功能,合成解码的结果则直接提交给合成模块,用于 CDR 合成。解码过程思路是根据协议栈结构对消息进行从底层到上层的“逐层解析”^[4],若 S1AP 中包含了 NAS PDU,则还需进行 NAS 协议的解码。

S1AP 采用 ASN.1 的基本压缩编码(basic-PER)原则,不同消息中包括了多种类型的信息元素,同时还具有信息元素嵌套定义的特征^[5]。S1AP 消息的特点是手动解码较为复杂,且很多公司推出了第三方的 ASN.1 编译器,因此提出了采用 ASN.1 编译器生成 ASN.1 解码函数的方法,并在此基础上进行二次解码,以满足 LTE 网络测试仪的需求。ASN.1 编译器采用了共用体和链表结合的结构用于存储解码结果,不同类型的消息结果采用共用体存储,而消息内部的协议信息单元则采用链表的方式进行存储。根据 ASN.1 解码函数输出结果的特点,S1AP 的解码流程如图 2 所示。

S1AP 解码流程中,首先需要通过 S1AP 消息参数(如数据头指针、长度等)和 PER 模式构造 ASN.1 解码函数所需的数据块,其中 PER 模式设置为对齐,该数据块作为

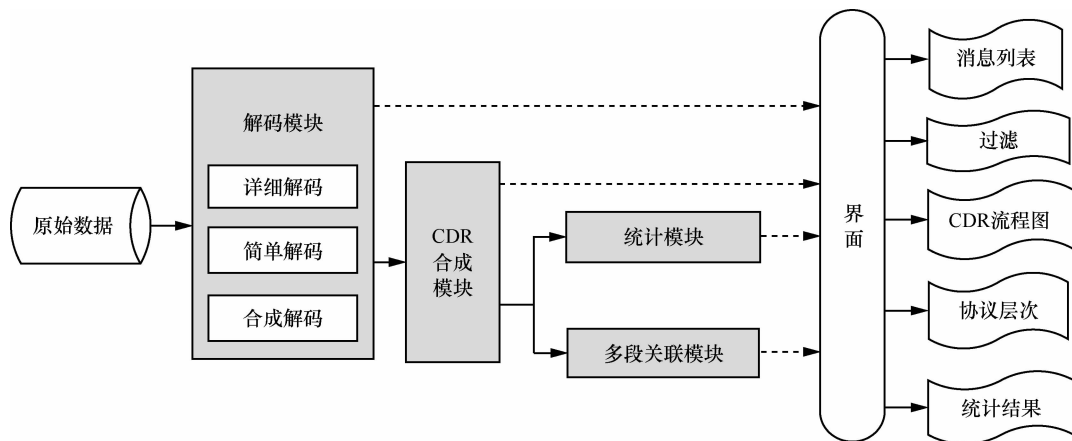


图 1 S1AP 监测总体架构

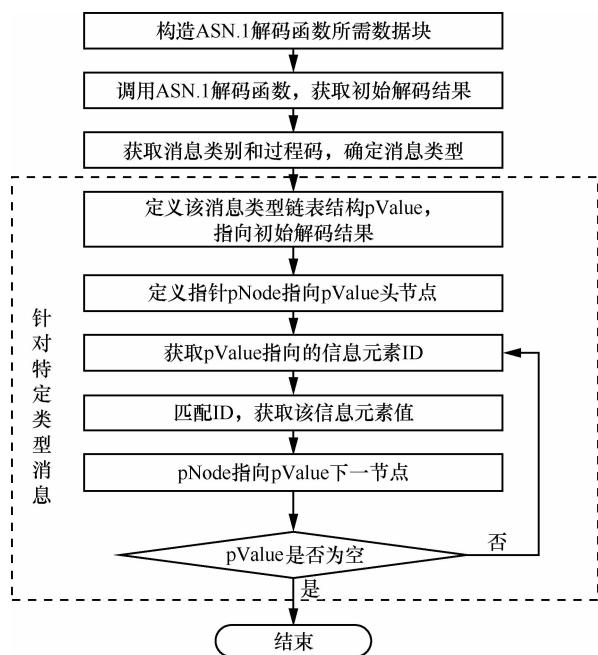


图2 S1AP 解码流程

ASN.1 解码函数的输入。其次调用 ASN.1 解码函数, 获取初始解码结果。通过获取到的消息类别和过程码, 确定该 S1AP 消息属于哪种消息类型, 具体实现为先对消息类别进行判断, 再调用对应消息类别的解码函数, 然后提取过程码, 并通过过程码的取值来确定调用该消息类型的解码函数, 以实现对该消息的解码。最后调用特定消息解码函数进行解码, 针对消息类型定义不同的链表结构和节点指针, 采用循环结构获取该条消息中各信息元素。

3.2 S1AP CDR 合成模块的设计与实现

CDR 合成是将属于同一通信过程的消息关联在一起, 是实现通信结果信息统计监测和网络性能测试的基础^[6,7]。对 LTE 网络中的消息按不同的归属呼叫流程进行归类, 并利用散列索引和超时管理机制把这些属于同一呼叫流程的消息关联到一起, 以便于完成如呼叫合成和呼叫呼损统计等各项高级功能。

对于 S1AP 消息来说, 不同消息流程可以通过 IP 地址、SCTP 端口号、eNode B UE S1AP ID 和 MME UE S1AP ID 来区分, 其中 IP 地址和端口号可以唯一标识传送地址, eNode B UE S1AP ID 可以唯一标识 eNode B 内 S1 接口上的 UE, MME UE S1AP ID 可以唯一标识 MME 内 S1 接口上的 UE, 因此采用源、目的 IP 地址、源、目的 SCTP 端口号、eNode B UE S1AP ID 和 MME UE S1AP ID 共 6 个参数作为散列索引的关键字段 key 值, 可以唯一确定一次通信

过程。在合成模块中, CS1AP CallInfo 类用于提取消息的关键字段值, 并提交给多段关联模块和统计出表模块, 是消息过程的基本表征载体。考虑到减少代码量和保证代码的整洁性, 定义基本类 CS1AP CDR 用于存储公共属性, 各子 CDR 都从 CS1AP CDR 派生。

S1AP 监测中, CDR 合成采用超时管理机制来处理异常情形, 为每个 CDR 设置一个超时时间, 若 CDR 超过此时间就将其关闭。采用的超时管理机制通过建立专门的时间链表完成, 该时间链表采用时间作为主线, 并建立超时时间与 CDR 之间的对应关系。在实际开发中, 将超时管理的一些基本操作封装成类模板 CTimeCheck, 以避免重复开发。CTimeCheck 声明为 `template <class CHECK_ITEM> class CtimeCheck`。全局 CDR 和各子 CDR 采用相同的超时管理方法, 在合成过程中, 主要涉及 3 个操作: 设置超时时间、删除超时节点和超时检查。

S1AP CDR 合成的基本流程如图 3 所示。

具体实现步骤如下。

(1) 合成解码结束后, 提取合成所需信息, 并触发合成器, 开始合成。

(2) 全局 CDR 超时检查, 检查全局 CDR 对应的缓存中是否有超时的 CDR, 对超时 CDR 进行处理。

(3) 使用 S1 接口的解码结果, 填写全局 CDR 对应的合成关键字 key。

(4) 在全局 CDR 对应的缓存中查找是否有与该 key 匹配的全局 CDR 存在, 如果有, 则进入第(5)步, 否则进入第(6)步。

(5) 在全局 CDR 的缓存中插入 key, 生成一个合成节点, 创建 CDR 并为其分配一个 CDR ID, 使用该消息携带的信息设置 CDR 属性, 同时设置该消息属于全局 CDR, 进入第(7)步。

(6) 从全局 CDR 缓存中获取 CDR, 使用该消息携带的信息更新 CDR 属性, 同时设置该消息属于全局 CDR, 并判断该消息是否为全局 CDR 的结束消息, 若不是结束消息, 进入第(7)步, 否则进入第(9)步。

(7) 设置全局 CDR 的超时时间, 将全局 CDR 存入缓存。

(8) 结合 S1AP 和 NAS 协议的消息类型, 判定该消息是否属于某一子 CDR 的信令流程, 是则进入对应的子 CDR 合成, 否则结束合成。

(9) 关闭全局 CDR, 并删除该全局 CDR 对应的超时节点, 合成结束。

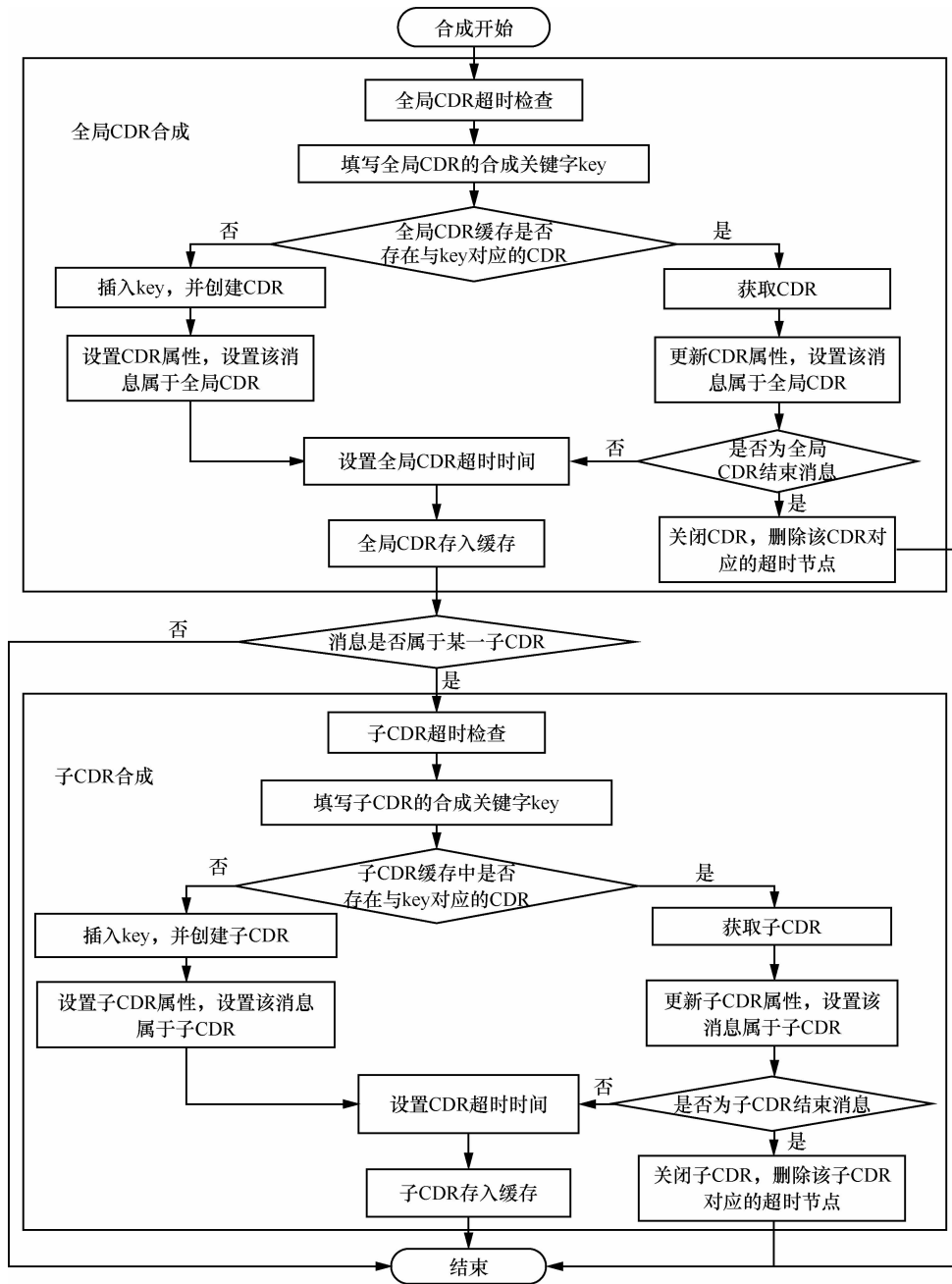


图3 S1AP CDR 合成基本流程

3.3 多段关联模块的设计与实现

在CDR合成结果的基础上,多段关联实现S1接口与EPC侧的接口之间的关联,关联接口包括了S1接口、S6a接口和S11接口。通过多段关联为用户呈现完整的信令流程,从而获取到完整的通信过程信息。在LTE网络测试仪器中,GTPv2-C协议主要定义了创建会话CDR、创建承载CDR、更新承载CDR、修改承载CDR、删除承载CDR和删除会话CDR,Diameter协议主要定义了鉴权CDR和更新

CDR。一种类型的CDR对应了一个信令流程,如S1AP的附着CDR对应S1AP上的一次附着流程。因此,以上接口的多段关联就可以转换成对S1AP、GTP-C协议和Diameter协议3种协议CDR的关联。

LTE网络监测仪表的多段关联是基于文本配置,并采用了消息触发机制,在CDR合成过程中,需要进行建立或索引的消息到来时,就触发多段关联对象完成关联。多段关联基于文本配置主要体现在关联规则通过填写文本配

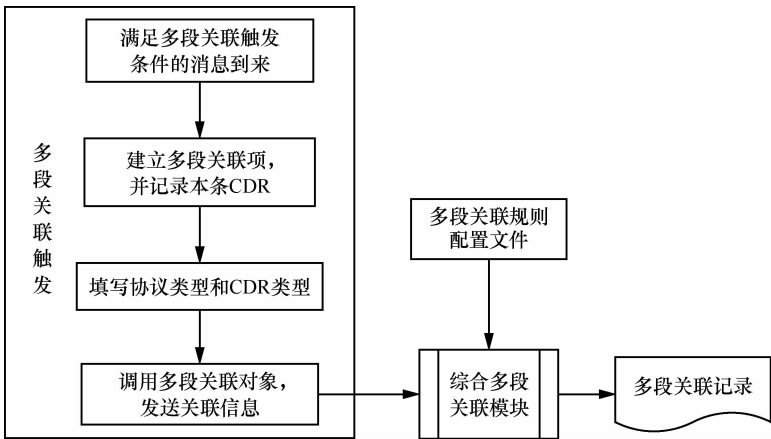


图 4 多段关联处理流程

置文件进行设置,这样就可以根据实际情况灵活地修改多段关联规则^[8]。不同的信令流程由不同消息交互完成,各消息携带的参数也不尽相同。因此,需要根据各信令流程之间的关系,选取不同的参数实现 CDR 之间的关联。多段关联处理流程如图 4 所示。

以最典型的开机附着业务为例进行说明,手机开机就需要通过附着流程登记到网络中,以获取 EPS 的分组服务。在收到用户发送的附着请求后,MME 向 HSS 请求鉴权信息,之后如果鉴权成功,MME 向 SGW 发送创建会话请求并通过 SGW 转发至 PGW,由 PGW 为 UE 分配 IP 地址等。结合附着业务的过程,将 S1、S6a 和 S11 接口之间所需关联的 CDR、关联参数等关联规则归纳为表 1。

表 1 附着业务关联规则

序号	关联 CDR	关联参数	关联接口
1	附着 CDR 与鉴权 CDR	IMSI	S1 与 S6a
2	附着 CDR 与创建会话 CDR	IMSI	S1 与 S11

通过表 1 可知,S1 接口的附着 CDR 与 S6a 接口的鉴权 CDR 通过 IMSI 关联,S1 接口的附着 CDR 与 S11 接口的创建会话 CDR 通过 IMSI 关联。

3.4 统计模块的设计与实现

统计模块是对 S1AP 的统计,包括流量统计、消息统计和业务统计的功能。流量统计和消息统计是基于消息的统计,消息统计包括了对 S1AP 和 NAS 消息的统计,业务统计是基于 CDR 的统计,包括附着统计、E-RAB 统计、切换统计、分离统计、跟踪区更新和业务请求统计。统计结果通过界面直观地呈现给用户,此外还能通过 excel 表格输出以满足用户的需求。流量统计、消息统计和业务统计的统

计思想相同,区别主要在于统计指标不同,为提高处理效率,统计中也采用了散列方式进行索引,统计方法的具体处理流程如图 5 所示。

统计基本处理流程主要包括以下步骤。

(1)判断是否为第一次统计,若是则记录第一次统计和本段统计的开始时间,并将统计状态设置为统计中,然后填写统计结束时间,若不是则直接填写统计结束时间。

(2)进行单次统计,通过调用单次统计函数进行计算,生成单个统计结果记录 SItem。

(3)填写统计关键字 key,在缓存中查找是否存在与该 key 对应的节点,如果是则获取统计项对象,否则插入 key 并建立 key 与 SItem 的映射关系。

(4)进行统计运算,通过调用统计指标计算函数,将 SItem 与统计项对象按照各统计指标进行计算获取统计结果,并将统计结果存入缓存。

(5)判断统计结束时间与本段开始时间之间的时间差是否大于或等于 5 min,若是则将统计结果写入索引文件中,清空缓存中的统计 key 以及与 key 对应的统计项对象之间的映射关系,同时更新本段统计开始时间。

4 实测数据及软件运行结果

通过与原始数据及协议进行比对,S1AP 的详细解码能够准确地对选定的消息进行逐字节、逐比特的解码,且解码结果正确。如图 6 所示的 S1AP 解码结果,协议从底层到上层的显示顺序依次为 Ethernet、IP、SCTP 和 S1AP,并通过字段名、字段值、解释和位掩码对消息进行详细说明。

该消息的消息类别为成功输出,过程码为 9,对应的消息类型为初始上下文建立成功。此外,该消息还包含了

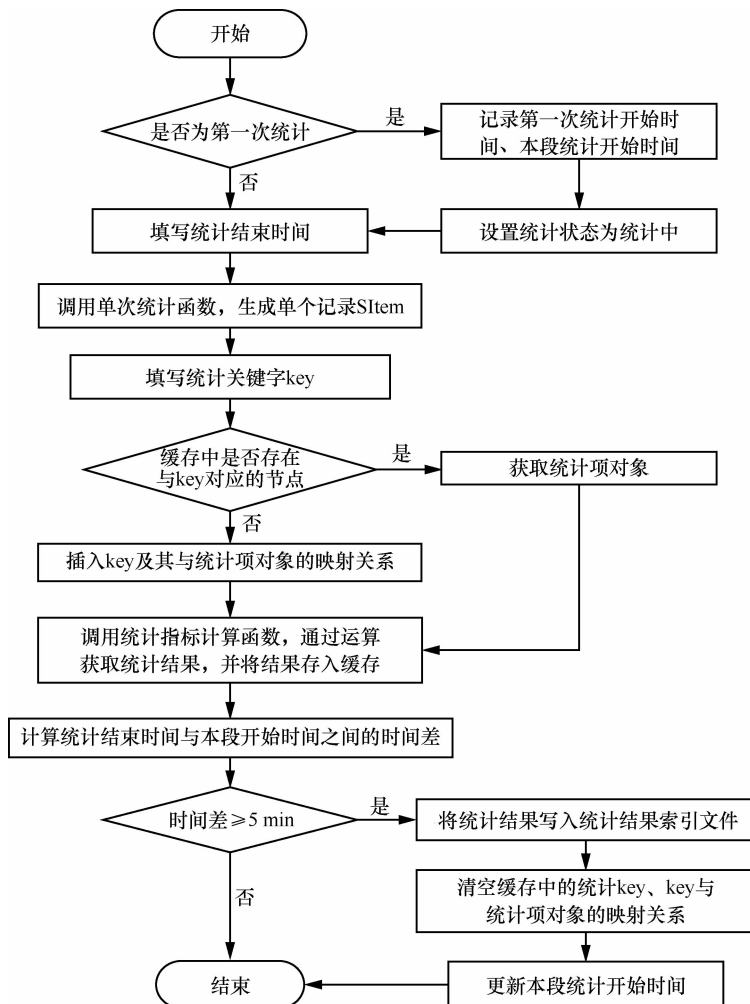


图5 统计基本处理流程

字段名	字段值	解释	位
Result			
Ethernet: 分组长度 102			
IP: 分组长度 88			
SCTP: 分组长度 68			
SIAP: 分组长度 38			
成功输出			
过程码	9	初始上下文设置响应	
关键性	0	拒绝	
值			
协议信息单元[0]			
id	0	MME_UE_SIAP_ID	
关键性	1	忽略	
值	53		
协议信息单元[1]			
id	8	ENB_UE_SIAP_ID	
关键性	1	忽略	
值	22		
协议信息单元[2]			
id	51	RAB设置列表上下文SU响应	
关键性	1	忽略	
值[0]			
id	50	RAB设置单元上下文SU响应	
关键性	1	忽略	
值			
e_RAB_ID	5		
传输层地址	0xc0a803c9	GTP隧道端点ID=0x0000001e	

原始数据

Addr: 003E Hex: 20 Dec: 32

0032 75 32 F1 4C 00 01 00 05 00 00 00 12 20 09 00 02 00 00 03 00 00 40 02 00 35 00 08

004D 40 02 00 16 00 33 40 0F 00 00 32 40 0A 0A 1F C0 A8 03 C9 00 00 00 1E 00 00

图6 SIAP 详细解码结果

3 个协议信息单元:ID 为 0, 指示该字段为 MME_UE_S1AP_ID, 字段值为 53;ID 为 8, 指示该字段为 eNode B_UE_S1AP_ID, 字段值为 22;ID 为 51, 指示该字段为 E-RAB 建立列表, 里面仅包含了一个 E-RAB, E-RAB ID 为 5, 传输层地址为 0xc0a803c9, GTP 隧道断电 ID 为 0x0000001e。结合 3GPP 规范 36.413 对原始数据中突出显示部分的 16 进制数据进行分析可知, 该解码结果准确。

图 7 为用户附着成功的 CDR 合成结果, UE 的 IMSI 为在 HSS 中已注册的 460089990000003, 该 MME 在对 UE 进行鉴权、认证等过程后, 发送附着接受消息, 再由 UE 发送附着完成消息。其中只有突出显示的为附着流程的消息, 整个流程中的其他消息都做了灰化处理, 由此把属于该附着 CDR 的消息与整个流程中的其他消息区分开来。对附着消息、附着接受和附着完成消息所携带小区号、M-TMSI 等参数与 CDR 属性相同, 结合协议规范对流程图和模拟场景的流程比较可知, 合成准确。

图 8 为开机附着业务关联流程, 由 IMSI 为 460089990000001 的 UE 执行附着命令发起附着流程, 其中 eNode B 的 IP 地址为 192.168.124.131, MME 的 IP 地址为 192.168.124.128, HSS 的 IP 地址为 192.168.124.130, SGW 的 IP 地址为 192.168.124.129。MME 接收到其中包含

用户的 IMSI:460089990000001 的附着请求后, 向 HSS 发送鉴权请求消息, 确认该用户 IMSI 是否合法、加密算法是否匹配等。鉴权成功后, HSS 向 MME 发送鉴权信息应答消息进行确认。之后, MME 又与 HSS 之间进行了更新位置的过程。鉴权成功后, MME 向 SGW 发送创建会话请求消息, 该消息中携带了用户 IMSI:460089990000001 及用户的 PDN 地址:20.20.20.1。该过程成功后, MME 向用户分配 M-TMSI, 并发送附着接受和附着完成消息, 完成附着流程。实现了 S1AP 的附着 CDR、Diameter 的鉴权 CDR 和 GTPv2 的创建会话 CDR 之间的关联。

5 结束语

本文在研究 LTE 网络监测仪表架构的基础上, 设计了 S1AP 监测方案, 具体分析了 S1AP 解码模块、CDR 合成模块、多段关联模块和统计模块的实现方案。针对 S1AP 的特征, 增加 eNode B_UE_S1AP_ID 和 MME_UE_S1AP_ID 参数作为散列索引的关键字段, 并引入超时管理机制的概念, 极大地提高了协议关联和 CDR 合成及统计效率。该方案已应用到 LTE 网络监测仪表中, 并通过仿真数据测试, 验证了该协议监测方案能有效地进行协议解码、CDR 合成、多段关联和统计等功能, 监测效果良好。本文研究成果

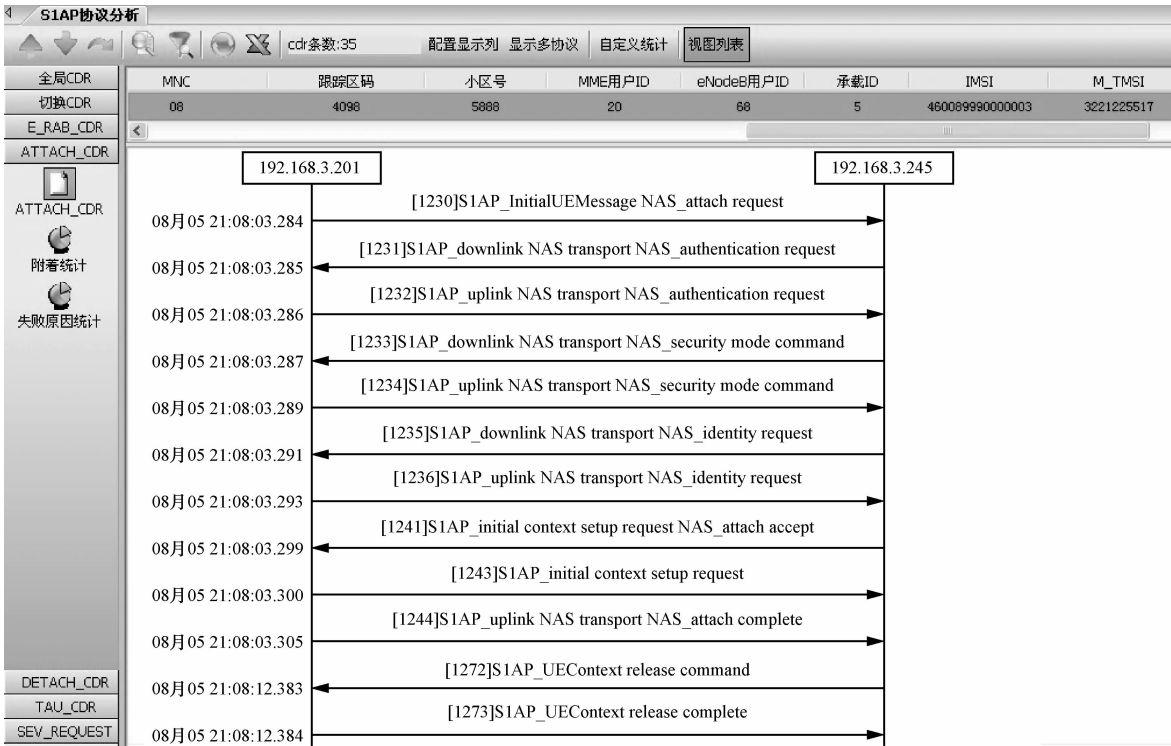


图 7 附着成功的 CDR 合成结果



当前CDR: S1AP(2)S1AP ATTACH CDR 关联CDR: DIAMETER(2)S6a Authen CDR GTPv2(2)GTPV2 CS CDR

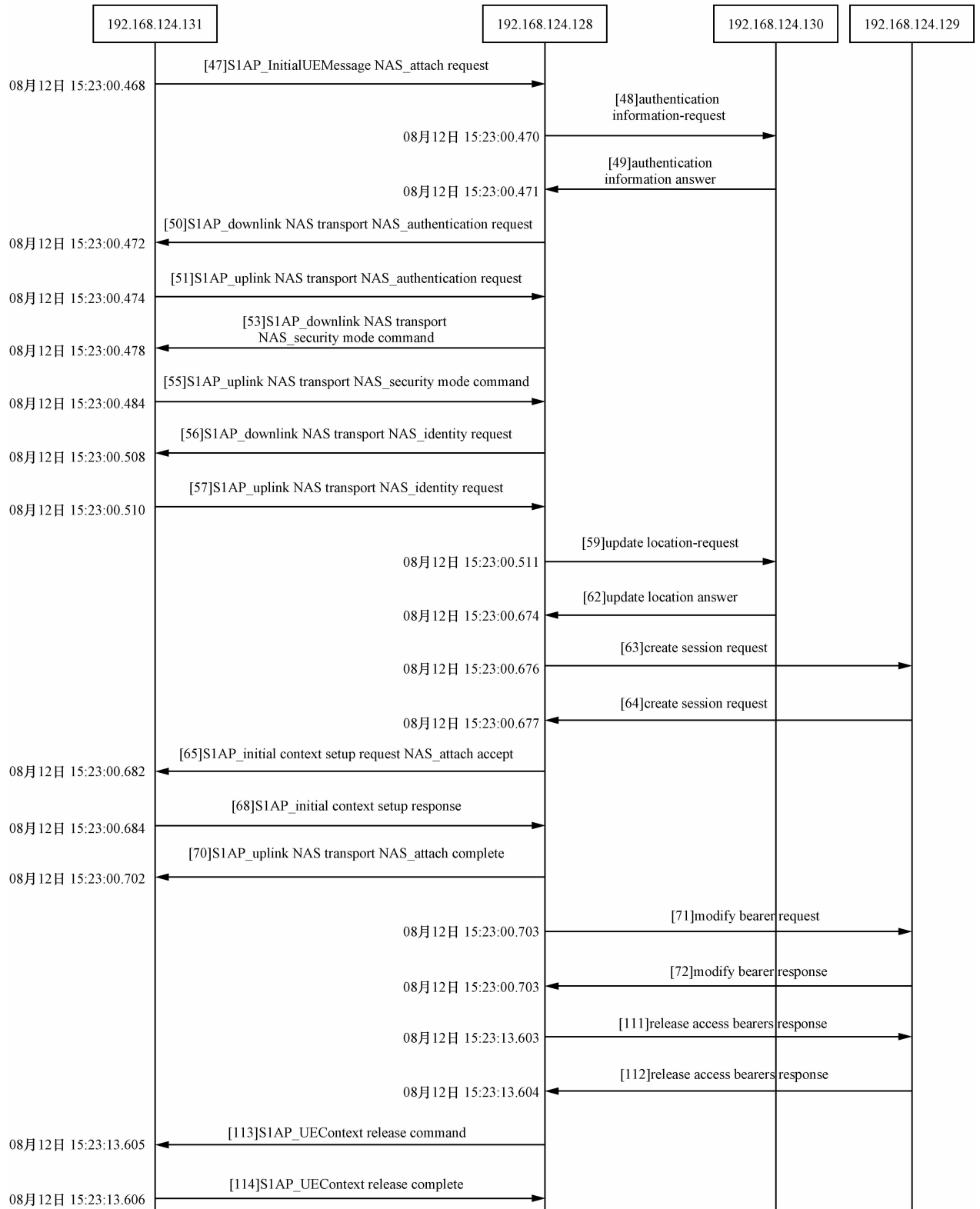


图8 开机附着业务关联流程

(下转第45页)

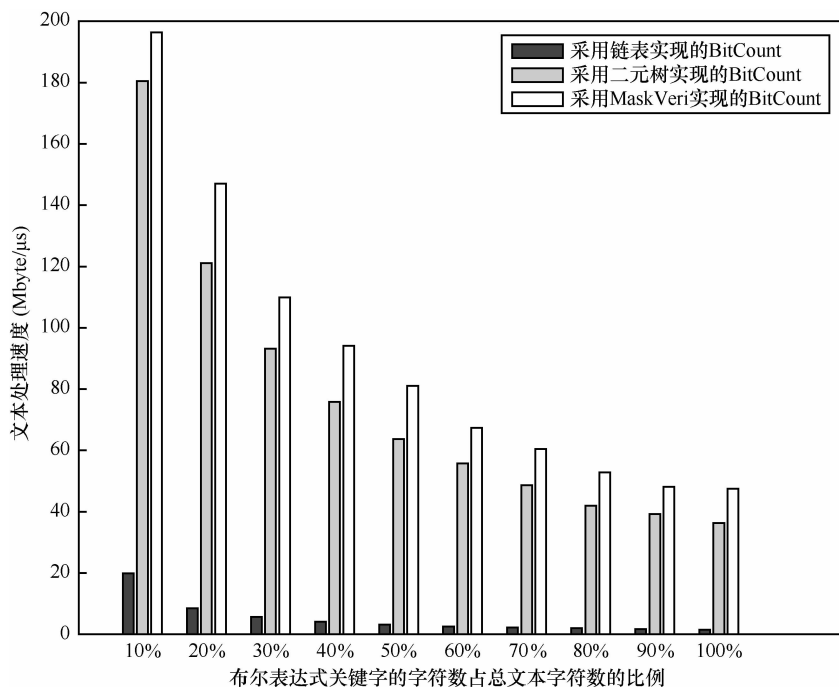


图2 3种掩码表达式验证方法性能比较

2012(2289): 1~4

- 7 Karnough M. The map method for synthesis of combinational logic circuits. AIEE, 1953:593~599
- 8 McCluskey E J. Minimization of Boolean function. Bell System Tech Journal, 1956, 35(5):1417~1444
- 9 曹京,谭建龙,刘萍等.布尔表达式匹配问题研究.计算机应用研究,2007(9): 70~72,108
- 10 曹京,刘燕兵,刘萍等.定序窗口布尔表达式匹配技术研究.通信学报,2007(12):125~130

11 张树壮.面向网络安全的高性能特征匹配技术研究.哈尔滨工业大学博士学位论文,2011

12 宋云,龙际珍.规则数量无关的多布尔表达式匹配算法.软件导刊,2012(3):57~59

【作者简介】 杨天龙,男,哈尔滨工业大学博士研究生,主要研究方向为大规模特征集串匹配技术。张宏莉,女,博士,哈尔滨工业大学教授、博士生导师,主要研究方向为网络与信息安全、网络测量与建模、网络计算、并行处理等。

(收稿日期:2012-09-19)

(上接第38页)

的应用,不仅为LTE网络优化提供了分析工具,也为网络监测和质量评估提供强有力的支撑。

参考文献

- 1 唐海.TD-LTE的标准化工作及进展.电信科学,2009(1): 22~26
- 2 3GPP TS 36.300.Evolved Universal Terrestrial Radio Access Network (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN),Overall Description V8.12.0, 2010
- 3 3GPP TS 36.410.Evolved Universal Terrestrial Access Network (E-UTRAN), S1 General Aspects and Principles V8.3.0, 2010
- 4 魏辉,张治中.TD-SCDMA网络测试仪中SCCP解码及上层PDU获取方案.重庆邮电大学学报(自然科学版),2007,19(1):

47~52

- 5 3GPP TS 36.413. Evolved Universal Terrestrial Radio Access Network (E-UTRAN):S1 Application Protocol V8.10.0, 2010
- 6 夏韪,雒江涛,张治中.TD-SCDMA测试仪中Iub接口CDR的合成方案.重庆邮电大学学报(自然科学版),2007(2):35~38
- 7 陈玉花,张治中,左书川等.TD-SCDMA网络Iu-PS口CDR合成方案研究.电信科学,2009(11):50~54
- 8 舒忠玲.基于文本配置文件的多段关联方法.中国:CN 101527653A, 2009

【作者简介】 李艳,女,重庆邮电大学硕士研究生,主要研究方向为通信协议及软件、LTE网络测试技术。张治中,男,重庆邮电大学教授、博士生导师,主要研究方向为第三代移动通信测试技术、宽带信息网、NGN、LTE网络等。

(收稿日期:2012-10-28)