(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106031105 B
(45)授权公告日 2020.04.24

(21)申请号 201480075824.3

(22)申请日 2014.12.18

(65)同一申请的已公布的文献号
申请公布号 CN 106031105 A

(43)申请公布日 2016.10.12

(30)优先权数据
13290320.4 2013.12.19 EP

(85)PCT国际申请进入国家阶段日
2016.08.18

(86)PCT国际申请的申请数据
PCT/EP2014/078605 2014.12.18

(87)PCT国际申请的公布数据
WO2015/091878 EN 2015.06.25

(73)专利权人 诺基亚技术有限公司
地址 芬兰埃斯波

(72)发明人 B•兰代斯 L•蒂埃博
N•德勒冯

(74)专利代理机构 北京市中咨律师事务所 11247
代理人 杨晓光

(51)Int.Cl.
H04L 12/801(2013.01)
H04W 12/06(2009.01)
H04W 28/02(2009.01) (续)

(56)对比文件
CN 102223634 A,2011.10.19,
CN 102595508 A,2012.07.18,
WO 2013004905 A1,2013.01.10,
3GPP."3rd Generation Partnership Project;Technical Specification Group Service and System Aspects;Architecture enhancements for non-3GPP accesses (Release 12)".《3GPP TS 23.402 V12.3.0》.2013,第242-244页.
3GPP."3rd Generation Partnership Project;Technical Specification Group Service and System Aspects;General Packet Radio Service(GPRS)enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 12)".《TS 23.401 V12.3.0》.2013,说明书4.3.7.4.2.2部分.
3GPP."3rd Generation Partnership Project;Technical Specification Group Service and System Aspects;Study on Core Network Overload(CNO)solutions(Release 12)".《TS 23.843-120_including editorial updetes_clean》.2013,说明书第39页1-10行.

审查员 刘叶

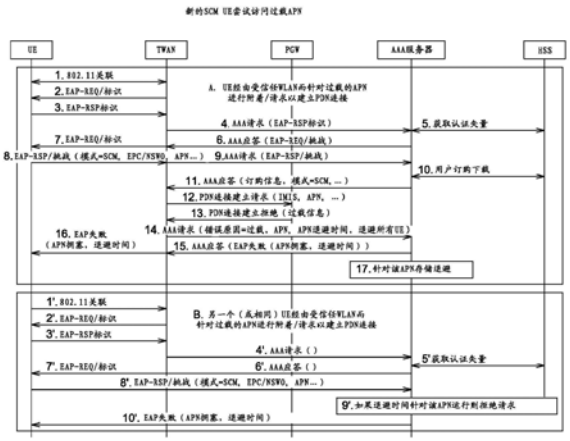
权利要求书1页 说明书11页 附图3页

(54)发明名称

针对EPC的受信任WLAN访问的过载控制

(57)摘要

在一个实施例中提供了一种用于针对EPC进行受信任WLAN访问的过载控制的方法,包括:-当针对认证和授权用户拒绝单连接模式(SCM)的UE的请求时,网络在针对所请求的APN的拥塞控制活动时针对该APN以信号向UE通知退避时间,-一旦接收到该退避时间,UE在该退避时间的持续时间内不针对该拥塞APN发起新的请求。



CN 106031105 B

[转续页]

[接上页]

(51)Int.Cl.

H04W 74/08(2009.01)

H04W 76/18(2018.01)

H04W 76/12(2018.01)

H04W 84/12(2009.01)

1.一种用于通信的装置,包括处理器和存储有指令的存储器,所述指令在被执行时使所述装置:

-请求在单连接模式下对演进分组核心网络的受信任无线局域网络访问;

-从认证、授权和计费服务器接收响应消息,所述响应消息包括由于拥塞的失败原因和退避时间;以及

-在所述退避时间的持续时间内不发起新的请求。

2.根据权利要求1所述的装置,其中,所述请求是针对请求的接入点名称,并且所述退避时间是针对所述请求的接入点名称。

3.一种用于针对演进分组核心网络的受信任无线局域网络访问的过载控制的方法,包括:

-请求在单连接模式下对演进分组核心网络的受信任无线局域网络访问;

-从认证、授权和计费服务器接收响应消息,所述响应消息包括由于拥塞的失败原因和退避时间;以及

-在所述退避时间的持续时间内不发起新的请求。

4.根据权利要求3所述的方法,其中,所述请求是针对请求的接入点名称,并且所述退避时间是针对所述请求的接入点名称。

5.一种用于通信的装置,包括处理器和存储有指令的存储器,所述指令在被执行时使所述装置:

-从演进分组核心网络的分组数据网络网关接收过载信息,其中,用户设备请求在单连接模式下对所述演进分组核心网络的受信任无线局域网络访问;以及

-拒绝所述请求,并向认证、授权和计费服务器发送由于拥塞的失败原因和退避时间,以向所述用户设备发送所述由于拥塞的失败原因和退避时间,以使所述用户设备在所述退避时间的持续时间内不发起新的请求。

6.根据权利要求5所述的装置,其中,所述请求是针对请求的接入点名称,并且所述退避时间是针对所述请求的接入点名称。

针对EPC的受信任WLAN访问的过载控制

技术领域

[0001] 本发明总体上涉及移动通信网络和系统。

背景技术

[0002] 移动通信网络和系统的详细描述能够在文献中找到，尤其能够在诸如由例如3GPP(第三代合作伙伴计划)之类的标准化主体所发布的技术规范中找到。

[0003] 通常，在分组移动通信系统中，用户设备(UE)能够访问提供分组数据网络(PDN)连接服务(通常是IP连接服务)的移动网络。移动网络通常包括由访问网络(AN)进行访问的核心网(CN)。除其它之外，CN通常包括与访问点名称(APN)所表示的外部PDN(通常是IP网络，诸如互联网、企业内部网或者运营商的IP网络，例如IMS网络)进行对接的PDN网关(PDN-GW)。在UE和PDN/IP网络之间通过移动网络所建立的PDN/IP连接能够被用来访问到各种基于IP的用户服务或应用。

[0004] 分组移动通信系统的示例是演进分组系统(EPS)。EPS网络包括CN(称作演进分组核心(EPC))，其能够被例如E-UTRAN的3GPP访问网络(3GPP AN)以及例如WLAN的非3GPP访问网络(非3GPP AN)所访问。

[0005] 针对EPC的非3GPP访问尤其在3GPP TS 23.402中有所规定。针对EPC的受信任WLAN访问的架构的示例在摘自3GPP TS 23.402的图1中有所图示。受信任WLAN访问网络(TWAB)经由被称作S2a接口的接口与PDN网关(在EPC中也称作PGW)进行对接，上述接口能够基于GTP(TPRS隧道协议)或PMIP(代理移动IP)。受信任WLAN访问网络(TWAN)还经由被称作STa接口的接口与3GPP AAA服务器进行对接。受信任WLAN访问网络(TWAN)内的功能划分的示例在摘自3GPP TS 23.402的图2中有所图示。特别地，TWAN包括与UE进行对接的WLAN访问网络，终止S2a接口的受信任WLAN访问网关(TWAG)，以及终止STa接口的受信任WLAN AAA代理(TWAP)。

[0006] 这样的系统中的一个重要问题在于性能可能在尤其由于高信令负载所导致的过载情况下发生退化，尤其是在核心网络实体之中。此外还出现具体的问题，尤其是对于针对EPC的受信任WLAN访问以及透明单连接模式(TSCM)或单连接模式(SCM)(针对其并不支持WLAN控制协议(WLCP))而言，因为目前并没有妥善定义的用于在这样的情况下处理网络过载的UE行为。需要解决这样的问题，更一般地是需要避免这样的系统在过载情况下出现性能退化。

发明内容

[0007] 本发明的实施例尤其解决这样的需求。

[0008] 在一个方面，这些和其它目标通过一种用于针对EPC的受信任WLAN访问的受信任WLAN访问网络TWAN而实现，其被配置为：

[0009] -针对认证和授权用户，当由于拥塞而针对单连接模式(SCM)的UE拒绝请求时，以信号向AAA服务器通知拥塞原因和UE的退避时间。

[0010] 在另一个方面，这些和其它目标通过一种AAA服务器而实现，其被配置为对于针对EPC的受信任WLAN访问：

[0011] -从受信任WLAN访问网络TWAN接收拥塞原因以及针对单连接模式的UE的请求的退避时间，

[0012] -将拥塞原因和退避时间包括在其发送至UE的响应消息中，

[0013] -通过返回具有拥塞原因以及剩余退避时间的响应消息来可选地拒绝来自相同UE的任何后续请求直至退避计时器超时。

[0014] 在另一个方面，这些和其它目标通过一种AAA服务器而实现，其被配置为对于针对EPC的受信任WLAN访问：

[0015] -从受信任WLAN访问网络TWAN接收APN拥塞原因以及针对单连接模式的UE的请求的所请求APN的退避时间，

[0016] -将APN拥塞原因和退避时间包括在其发送至UE的响应消息中，

[0017] -通过返回具有拥塞原因以及剩余退避时间的响应消息从而可选地拒绝来自相同UE的以相同APN为目标的任何后续请求直至退避计时器超时。

[0018] 在另一个方面，这些和其它目标通过一种用户设备UE而实现，其被配置为在针对EPC的受信任WLAN访问：

[0019] -根据从AAA服务器接收到拥塞原因和退避时间，在该退避时间的持续时间内不发起任何新的请求。

[0020] 在另一个方面，这些和其它目标通过一种用于针对EPC进行受信任WLAN访问的受信任WLAN访问网络TWAN而实现，其被配置为：

[0021] -当由于拥塞而针对认证和授权用户拒绝SCM模式的UE的请求时，针对该UE或者在拥塞控制对于所请求的APN是活动的时针对该UE和所请求的APN开启退避计时器；

[0022] -通过向AAA服务器返回具有拥塞原因以及剩余退避时间的响应消息从而拒绝来自相同UE的任何后续请求或者来自相同UE的以该APN为目标的任何后续请求直至该退避计时器超时。

[0023] 在另一个方面，这些和其它目标通过一种用于针对EPC进行受信任WLAN访问的受信任WLAN访问网络TWAN而实现，其被配置为：

[0024] -当由于拥塞而针对认证和授权用户拒绝TSCM模式的UE的请求时，在拥塞控制是全局化时按照UE开启退避计时器或者在拥塞控制对于所请求的APN活动时按照UE以及按照SSID开启退避计时器。

[0025] 在另一个方面，这些和其它目标通过一种用于针对EPC进行受信任WLAN访问的过载控制的方法而实现，其包括：

[0026] -当由于拥塞而针对认证和授权用户拒绝SCM模式的UE的请求时，网络以信号向UE通知退避时间，在拥塞控制针对所请求的APN活动时这可能仅能够应用于该APN，

[0027] -根据接收到的该退避时间，UE在该退避时间的持续时间内不发起新的请求或者针对拥塞APN的新的请求。

[0028] 在另一个方面，这些和其它目标通过一种用于针对EPC进行受信任WLAN访问的过载控制的方法而实现，其包括：

[0029] -当由于拥塞而针对认证和授权用户拒绝TSCM模式的UE的请求时，受信任WLAN访

问网络TWAN在拥塞控制是全局化时按照UE开启退避计时器或者在拥塞控制对于所请求的APN激活时按照UE和SSID开启退避计时器。

附图说明

[0030] 现在仅通过示例且参考附图对依据本发明实施例的装置和/或方法的一些实施例进行描述,其中:

[0031] -图1意在回顾针对EPC的受信任WLAN访问的示例架构,

[0032] -图2意在回顾受信任WLAN功能划分的示例,

[0033] -图3意在图示根据本发明实施例的用于处于单连接模式的UE的APN退避机制的示例,

[0034] -图4意在图示根据本发明实施例的用于处于透明单连接模式的UE的APN退避机制的示例。

具体实施方式

[0035] 下文将更为详细地描述本发明的各个实施例和/或方面从而基于示例进行简化。然而,本发明的实施例和/或方面并不局限于这些示例。例如:

[0036] -本发明的实施例和/或方面并不局限于APN拥塞,特别地,能够更为一般地考虑APN拥塞和/或PGW过载,

[0037] -本发明的实施例和/或方面并不局限于使用例如EAP的某些信令协议,而是能够如本领域技术人员所理解的使用其它方式,

[0038] -…等等。

[0039] 3GPP已经在3GPP Release 12中广泛运用于核心网过载解决方案以防止由于过载所导致的网络中断(参见3GPP TR 23.843)。这导致了基于Diameter和GTP-C的接口上的新的负载和过载控制机制。

[0040] 3GPP CT4目前在3GPP TR 29.807中定义了新的GTP-C过载控制过程。由于分散的非3GPP(例如,WiFi)覆盖或者3GPP和非3GPP覆盖之间的大量移动所导致的频繁的RAT重新选择尤其会由于频繁且大量的系统间变化的活动而导致GTP-C过载,上述系统间变化的活动即UE尝试通过新的访问创建PDN连接或者在3GPP和非3GPP覆盖之间移动PDN连接(参见TR 29.807的条款4.1)。CT4因此已经断定在S2a(受信任的非3GPP访问网络-PGW)和S2b(不受信任的非3GPP访问网络-PGW)接口上期望对GTP-C过载控制的支持从而减少TWAN或ePGD根据PGW的可用容量而发送至PGW的信令业务(参见TR 29.807的条款4.2.4.3.3.1)。这之所以甚至更为有用是因为过载控制还在用于3GPP访问的S5/S8接口上被引入,并且因此PGW在体验到PGW级别或APN级别的过载时应当能够以等同的方式分流来自经由3GPP和非3GPP访问所接收到的请求的过度业务。

[0041] 无论在S2a或S2b接口上是否支持过载控制,网络在其无法对UE建立或交换PDN连接的请求进行成功处理时(例如,由于PGW处的过载或者关联于UE所请求的APN的资源(例如,IP地址池)的拥塞)都需要拒绝该请求。

[0042] 然而,对于使用透明单连接模式(TSCM)(*)经由受信任的WLAN访问对EPC进行访问的UE而言,网络却无法向该UE指示其为何拒绝了UE的请求并且其也无法指示UE不要在一段

时间内再次经由受信任的WLAN访问对EPC进行访问。作为结果,UE可能会重复(马上或者在不久之后)经由受信任的WLAN访问获得EPC访问的整个过程,包括针对3GPP AAA服务器和HSS的认证和授权过程。这针对在拒绝之前请求的的原因仍然生效的情况下(例如,PGW仍然过载)将需要再次被拒绝的用户请求而对于TWAN、3GPP AAA服务器和HSS导致了额外且不期望出现的信令(即,3GPP AAA服务器从HSS取得UE的认证矢量,AAA服务器和UE之间的EAP认证交换,从HSS向AAA服务器下载订购信息,AAA服务器将所有订购信息下载到TWAN)。

[0043] 对于使用单连接模式(SCM)(＊＊)经由受信任的WLAN访问对EPC进行访问的UE而言,3GPP AAA服务器能够经由新的EAP扩展而向UE返回失败原因。然而,这里还没有定义防止UE在一段时间内经由受信任的WLAN访问再次访问该网络的机制,这使得TWAN、3GPP AAA服务器和HSS承担了导致额外信令负载的相同风险。

[0044] 因此需要保护3GPP AAA服务器、HSS和TWAN免受UE尝试访问过载APN或PGW的影响并且确保S2a上新的GTP-C过载控制并不会针对3GPP AAA服务器和HSS增加信令负载的机制。

[0045] 注意1:TR 29.807的条款4.2.4.3.3.3中的编辑标注指示了如何解决这些问题有待进一步研究。

[0046] 注意2:对于使用多连接模式(MCM)(＊＊＊)而经由受信任的WLAN访问对EPC进行访问的UE,TR 29.807(参见条款4.2.4.3.3.3)提出在TWAN和UE之间的WLCP协议(WLAN控制协议)中规定新的APN退避机制以便防止UE重试。

[0047] (＊)TSCM＝在Rel-11(SaMOG)中针对受信任的WLAN访问所规定的仅有的通信模式,对于UE是强制的,其在UE和受信任的WLAN之间每次仅能够支持单个连接,并且其中该连接相关联的参数从UE的订购以及UE所选择的WLAN SSID得出。

[0048] (＊＊)SCM＝在eSaMOG Rel-12中增加的新的通信模式,对于UE是可选的,其在UE和受信任的WLAN之间每次仅能够支持单个连接,并且其中该连接相关联的参数(例如,用于NSWO,用于PDN连接、APN等)能够在通过TWAN的认证期间进行协商。

[0049] (＊＊＊)MCM＝在eSaMOG Rel-12中增加的新的通信模式,对于UE是可选的,其在UE和受信任的WLAN之间能够支持单个或多个连接。

[0050] 本发明的实施例包括两种用于保护3GPP AAA服务器、HSS和TWAN免受UE访问过载APN或PGW的反复尝试的影响的两种互补的机制。这两种机制的实施例将分别在下文的段落1)和2)中被加以考虑。

[0051] 1)TWAN和3GPP AAA服务器针对处于SCM的UE执行新的退避机制,如下所述:

[0052] 在拒绝来自认证和授权用户的UE请求(受信任的WLAN访问中的新的PDN连接或切换请求)时,在拥塞控制针对APN活动时(例如,PGW已经针对以该APN为目标的业务而对TWAN触发了过载控制),网络可以针对所请求的APN以信号向UE通知退避时间。TWAN针对该APN将APN退避时间传输至3GPP AAA服务器,并且3GPP AAA服务器将该退避时间包括在其发送至UE的EAP失败消息之中。

[0053] 这样的机制利用单连接模式的扩展而对EAP协议进行了加强。

[0054] 在拒绝UE请求时,TWAN将新的APN拥塞原因和APN退避计时器返回至3GPP AAA服务器,3GPP AAA服务器将其经由EAP扩展传播至UE。

[0055] 当接收到该退避时间时,UE在该退避时间的持续时间内将不会针对拥塞APN发起

任何新的PDN连接请求(其经由3GPP或非3GPP访问)。UE可以针对其它APN发起新的请求。

[0056] 此外,例如对于其中新的APN退避机制(以上)在3GPP标准中被决定为UE可以选择支持的情况下,或者例如为了保护网络免受行为不当或"欺诈"UE的影响,3GPP AAA服务器可以立即拒绝来自相同UE的以该APN为目标的任何后续请求直至退避计时器过期。在该情况下,3GPP AAA服务器并不从HSS下载用户的订购信息而且并不授权TWAN继续应对UE请求。

[0057] 除此之外,如果TWAN还向3GPP AAA服务器指示以该APN为目标的任何其它用户的请求(处于SCM或TSCM)也应当受到节制直至该退避计时器超时,则3GPP AAA服务器可以立即拒绝来自任何UE的以该APN为目标的任何后续请求直至该退避计时器超时。

[0058] 2)TWAN针对处于TSCM的UE代表UE执行退避机制,如下所述:

[0059] 在拒绝来自认证和授权用户的UE请求(受信任的WLAN访问中的新的PDN连接或切换请求)时,TWAN可以在拥塞控制针对APN活动时(例如,PGW已经针对以该APN为目标的业务而对TWAN触发了过载控制)按照UE(以及可能地按照SSID)开启退避计时器。

[0060] 注意1:在给定SSID上,TSCM UE仅能够访问一个预定义APN,因此如果UE的尝试已经在该SSID上由于拥塞而被拒绝,则任何另外的UE连接尝试在退避时间期间都会被拒绝。

[0061] 然而UE在其可能被允许对非无缝WLAN卸载或另一个APN进行访问的情况下可以被允许在另一个SSID上进行访问。

[0062] 在退避计时器超时之前,TWAN可以立即拒绝来自UE的以该APN为目标的任何后续请求,即在相同的所选择WLAN SSID上源自于相同UE的MAC地址的任何后续EAP信令。TWAN在该情况下并不针对3GPP AAA服务器生成任何AAA信令。

[0063] 注意2:处于TSCM的UE无法以信号向网络通知其是否请求了EPC访问或非无缝WLAN卸载(NSWO),也无法通知用于EPC访问的相关联参数(例如,所请求的APN)。访问的类型(EPC或NSWO)根据UE所选择的WLAN SSID而得出(在SSID和访问类型之间存在一对一映射),并且用于EPC访问的相关联参数则根据用户的订阅(缺省APN配置)而得出。

[0064] 注意3:该机制还可以针对并不遵循从网络所接收的退避时间的行为不当/欺诈的SCM UE的情形工作,或者在SCM中的新的APN退避机制在3GPP标准中被确定为由UE选择支持的情况下进行工作。

[0065] 本发明的实施例包括用于保护3GPP AAA服务器、HSS和TWAN免受UE访问过载APN或PGW的反复尝试的影响的两种互补机制。针对这些实施例的更为详细的实施例将分别在下文中的段落1)和2)中被加以考虑。

[0066] 1)TWAN和3GPP AAA服务器针对处于SCM的UE执行新的退避机制,如下所述:

[0067] 这样的机制的实施例在图3中有所图示(新的SCM UE尝试访问过载APN)。

[0068] 在拒绝来自认证和授权用户的UE请求(受信任的WLAN访问中的新的PDN连接或切换请求)时,网络可以在拥塞控制针对APN活动时(例如,PGW已经针对以该APN为目标的业务而对TWAN触发了过载控制)针对所请求的APN而以信号向UE通知退避时间。

[0069] 从而在步骤11或13,根据TWAN是否已经知晓APN或PGW过载,TWAN传输APN退避时间而以信号通知UE乃至3GPP AAA服务器(步骤14),并且3GPP AAA服务器将该退避时间包括在其发送至UE的EAP失败消息中(步骤15&16).

[0070] 根据接收到该退避时间,UE在该退避时间的持续时间内将不会针对拥塞APN发起任何新的PDN连接请求(其经由3GPP或非3GPP访问)。UE可以针对其它APN发起新的请求。

[0071] 注意1:在没有退避时间的情况下向UE发送EAP失败并不足以防止UE再次尝试访问过载APN。依据WFA Hotspot 2.0规范,Release 2.0版本3.0.8,Section 6.4.4。

[0072] “移动设备可能无法成功使用特定证书针对热点完成EAP认证。失败可能由于各种原因,包括无效证书、网络问题、错误配置的AP等。然而,认证失败并非必然意味着证书或订阅存在问题,证书对于其它AP可能仍然是有效的。因此,在EAP认证故障的情况下,该移动设备:

[0073] -将不会在10分钟间隔内使用给定证书尝试多于10次的在相同ESS导致EAP认证失败的连续EAP认证。

[0074] -不应当使得该证书无法随其它BSS一起使用。”

[0075] TWAN还在步骤14向被拒绝的APN传输该退避时间以及过载原因代码。3GPP AAA服务器可以立即拒绝来自相同UE的针对该APN的任何后续请求(步骤1’至8’)直至该退避计时器超时。在该情况下,3GPP AAA服务器并不从HSS下载用户的订购信息而且并不授权TWAN继续处理UE请求,并且返回EAP失败消息,其具有指示所请求的APN拥塞的原因以及剩余的退避时间(步骤10’)。

[0076] TWAN还可以在步骤14中指示3GPP AAA服务器是否应当退避来自所有其它UE的以该APN为目标的所有请求。如果TWAN指示如此,则3GPP AAA服务器还可以立即拒绝来自任意其它UE(处于SCM或TSCM)的以该APN为目标的任何后续请求。

[0077] 这样的机制的实施例还可以如下进行描述。

[0078] 单连接模式要求在UE和3GPP AAA服务器之间支持EAP扩展从而设置或切换PDN连接。如图3所描绘的,在没有其它可替换的PGW能够为UE请求进行服务时,这些EAP扩展因此能够被权衡从而将“APN拥塞”原因和APN退避计时器从3GPP AAA服务器送至UE从而防止UE不必要地针对过载的PGW或APN重新尝试新的会话或切换请求。

[0079] 这对应于3GPP TS 23.402中针对单连接模式的图16.2.1-1中所规定的调用流程,其具有以下的增加内容:

[0080] 1.在步骤14,在拒绝来自认证和授权用户的UE请求(受信任的WLAN访问中的新的PDN连接或切换请求)时(在步骤11或步骤13之后),TWAN可以在拥塞控制针对APN活动时(例如,PGW已经针对以该APN为目标的业务而对TWAN触发了过载控制)针对该UE和所请求的APN以信号向3GPP AAA服务器通知APN拥塞原因和退避时间。

[0081] 2.在步骤15,3GPP AAA服务器将(从TWAN所接收的)APN拥塞原因和退避时间包括在其发送至UE的EAP失败消息之中。

[0082] 3.在步骤16,根据该原因和退避时间的接收,UE在该退避时间的持续时间内将不会针对拥塞APN发起任何新的PDN连接请求(其经由3GPP或非3GPP访问)。UE可以针对NSWO或其它APN发起新的请求。

[0083] 2)TWAN针对处于TSCM的UE代表UE执行退避机制,如下所述:

[0084] 这样的机制的实施例在图4中有所图示(TSCM UE重复针对过载APN的访问)。

[0085] 该UE首先尝试经由受信任的WLAN访问附着/建立或者移动PDN连接。进行完全的认证和授权过程,这涉及UE、TWAN、3GPP AAA服务器(以及漫游情形中的3GPP AAA代理)和HSS之间的多次信令交换(步骤2至11)。一旦UE被认证并授权,TWAN就选择PGW并且尝试针对该PGW建立PDN连接,例如通过发送GTP-C创建会话请求(具有UE的标识、所请求的APN、…)。

[0086] 在该示例中,PGW由于APN过载(例如,没有更多的IP@可用于该APN)或者PGW过载而拒绝该PDN建立请求。PGW可以在其针对TWAN的响应中提供过载信息,请求TWAN节制该TWAN向PGW所发送的某个百分比的业务并且是在某个时间段内进行节制(依据TR 29.807中所记载的原则)。

[0087] TWAN也可能并不通过S2a发起PDN连接建立请求,因为其事先已经接收到了PGW或APN拥塞的请求并且立即决定该UE连接请求要被拒绝。

[0088] 为了拒绝来自UE的请求,TWAN可以(步骤14):

[0089] a)依据3GPP Rel-11的TSCM调用流程和过程,拆除WLAN资源并且通过发送会话终止请求消息而触发在STa上(即在TWAN和3GPP AAA服务器之间)所建立的Diameter会话的释放;

[0090] b)或者可替换地,发送指示过载条件并且要求3GPP AAA服务器针对UE生成相关EAP失败消息的AAA请求。

[0091] 由于处于TSCM的UE并不知晓WLAN资源释放的原因,所以处于TSCM的UE可能会再次重复从新的认证和授权过程开始的整个过程(步骤18以及后续)。

[0092] 注意2:并不可能对TSCM UE的实施方式进行改变—并不允许对3GPP Rel-11中所规定的该行为进行改变。

[0093] 注意3:网络也可能有兴趣针对行为不当的SCM UE(并不遵循机制1中所规定的退避计时器的SCM UE)或者在新的退避机制在3GPP标准中被规定为由UE选择支持的情况下进行自我保护。

[0094] 在没有这样的机制的情况下,整个情形(如针对A所描述的,“UE附着/请求以建立PDN连接”,即图4的步骤1至16)将会再次发生,并且这可能像UE重复其尝试的那么多次。这将引起TWAN、3GPP AAA服务器和HSS之间的无用信令。

[0095] 利用这样的机制,当其拒绝来自被认证和授权用户的UE请求(受信任的WLAN访问中的新的PDN连接或切换请求)时(这可能根据TWAN是否已经知道所请求的APN或PGW是否过载而在步骤11或步骤13之后发生),TWAN可以在拥塞控制针对APN活动时(例如,PGW已经针对以该APN为目标的业务而对TWAN触发了过载控制)按照UE和SSID存储退避时间(步骤17)。

[0096] 在退避计时器超时之前,TWAN可以立即拒绝(或者默默丢弃)来自UE的以该APN为目标的任何后续请求,即通过相同的所选择WLAN SSID源自于相同UE的MAC地址的任何后续EAP信令(在步骤18)。TWAN在该情况下并不针对3GPP AAA服务器生成任何AAA信令。

[0097] TWAN可以通过发送回EAP失败消息(例如,具有依据IETF REC 3748的代码4)(步骤21)和/或通过释放WLAN关联(步骤22)来拒绝UE请求。

[0098] 注意4:UE的MAC地址在SaMOG连接模型中被用于在TWAN中将UE-TWAG点对点链路和S2a隧道进行关联。

[0099] 注意5:图4中的步骤18和19在TWAN内的AP处终止,即步骤20是TWAP所看到的第一个消息。

[0100] 在一种可能的实施例中,TWAG(即,针对PGW终止S2a的TWLAN访问网关,参见TS 23.402条款16.1.2)在步骤11或13之后拒绝UE请求时向TWAP(即,TWLAN AAA代理,即TWAN中针对3GPP AAA服务器终止STa的功能,参见TS 23.402条款16.1.2)过载错误原因和退避时间。TWAP随后创建和维护用于该退避时间的持续时间的新的UE-OC(UE过载控制)记录。

[0101] (针对处于TSCM的UE)该UE-OC记录应当包含UE的MAC地址、SSID、UE的IMSI以及退避时间(或者后续请求在其之前都需要被节制的绝对时间戳—这是等同的)。由于针对给定UE的TSCM而言在SSID和APN之间存在有一对一映射,所以并不必在该记录中存储APN(或者可以存储通配符APN),即在UE-OC记录中存储SSID(而不是APN)允许对来自使用相同的所选择SSID的UE的后续EAP信令进行节制(不包含/不必再次从3GPP AAA服务器下载订购信息)。

[0102] 注意6:该机制还能够在TWAN中用来拒绝来自处于SCM模式的UE(行为不当/欺诈的UE或者在针对SCM的新的APN退避机制可由UE选择支持的情况下)的UE重试。在该情况下,UE-OC记录应当包含UE的IMSI、APN和退避时间(该UE可以合法地请求针对另一个可能并不拥塞的APN的连接)。UE-OC记录还可以被用来应对TWAG拥塞,在这种情况下APN可以被给以通配数值。

[0103] 在上下文中存储IMSI允许防止被侵犯的(hacked)UE使用具有相同IMSI的多个MAC地址(这会导致许多UE-OC记录要存储在TWAN中的存储器DoS攻击)。

[0104] 在接收到来自UE的新的后续EAP信令时,TWAP通过检查其是否具有针对相同的UE的MAC地址和SSID的UE-OC上下文来检查其是否需要退避该UE。如果是这种情况,则TWAP如以上所描述的拒绝UE请求(步骤21)而不是针对3GPP AAA服务器触发认证和授权过程。

[0105] 注意7:如果该机制被用于处于SCM的UE,则TWAP在步骤11针对相同的IMSI和APN检查其是否具有UE-OC上下文。

[0106] TWAN应当基于从PGW所接收到的负载/过载信息(和/或本地提供的数值)来计算退避时间。PGW并不发送退避时间而是发送过载亮度的有效性周期,后者同样可以被用于计算退避时间的数值。

[0107] 这样的机制的实施例也可以如下进行描述。

[0108] 对于处于透明单连接模式(针对其并没有扩展也不能在网络和UE之间定义扩展)的UE而言,TWAN可以如图4中所描绘的代表UE支持退避机制。

[0109] 这对应于3GPP TS 23.402中针对透明单连接模式的图16.2.1-1中所规定的调用流程,其具有以下增加内容:

[0110] 1.在步骤17,在拒绝来自认证和授权用户的UE请求(受信任WLAN访问中的新的PDN连接请求)时(在步骤11或步骤13之后),TWAN在拥塞控制针对APN活动时(例如,PGW已经针对以该APN为目标的业务而对TWAN触发了过载控制)可以按照UE和SSID开启退避计时器。

[0111] 注意3:在给定SSID上,处于透明单连接模式的UE仅能够访问一个预定义的APN以便进行EPC访问,因此如果UE的尝试在该SSID上已经由于拥塞而被拒绝,则任何另外的UE连接尝试在退避时间期间都会被拒绝。然而UE可以被允许在另一个SSID上进行访问,该UE在那里可以被容许访问NSWO。

[0112] 注意4:在该示例中,PGW由于APN过载或PGW过载而拒绝PDN连接建立请求。PGW可以在其针对TWAN的响应中提供过载信息,请求TWAN对其向该PGW发送的业务的某个百分比进行节制。但是,TWAN在其事先接收到PGW或APN过载的指示的情况下也可能并不通过S2a发起PDN连接建立请求,并且立即决定该UE连接请求要被拒绝。

[0113] 2.在步骤21,在退避计时器超时之前,TWAN可以立即拒绝(或者默默丢弃)所接收到的来自UE的以该APN为目标的任何后续请求,即通过相同的所选择SSID源自于相同UE的MAC地址的任何后续EAP信令。在这种情况下,TWAN并不针对3GPP AAA服务器生成任何AAA信

令。TWAN可以通过发送回EAP失败消息(例如,具有依据IETF RFC 3748[x]的代码4)和/或通过释放WLAN关联而拒绝UE请求(步骤21'和步骤22)。

[0114] 注意5:UE的MAC地址在SaMOG连接模型中被用于在TWAN中将UE-TWAG点对点链路和S2a隧道进行关联。

[0115] 注意6:如果TWAN在步骤21并未立即拒绝UE请求,则可能再次进行整个序列(步骤1至16),并且这可能像UE将在过载情形期间重复其请求的那么多次。

[0116] 作为可能实施方式的示例,TWAG(即,针对PGW终止S2a的TWLAN访问网关,参见TS 23.402条款16.1.2)在步骤11或13之后拒绝UE请求时向TWAP(即,TWLAN AAA代理,即TWAN中针对3GPP AAA服务器终止STa的功能,参见TS 23.402条款16.1.2)过载错误原因和退避时间。TWAP随后创建和维护用于该退避时间的持续时间的新的UE-OC(UE过载控制)记录。

[0117] 该UE-OC记录包含UE的MAC地址、UE的IMSI以及退避时间(或者后续请求在其之前都需要被拒绝的绝对时间戳)。在上下文中存储IMSI允许防止被侵犯的UE使用具有相同IMSI的多个MAC地址(这会导致将许多UE-OC记录存储在TWAN中的存储器DoS攻击)。

[0118] 本发明的实施例的好处包括保护TWAN、3GPP AAA服务器(以及漫游情形中的3GPP AAA代理)和HSS免受由于在例如APN拥塞或PGW过载的期间拒绝经由受信任WLAN访问的建立或移动PDN连接的UE请求将会导致的大的信令开销的影响。这还使得能够在S2a接口上部署GTP-C过载控制而并不在网络中增加认证和授权信令。

[0119] 在一个方面,提供了一种用于针对EPC的受信任WLAN访问的受信任WLAN访问网络TWAN,其被配置为:

[0120] -针对认证和授权用户,当由于拥塞而针对单连接模式(SCM)的UE拒绝请求时,以信号向AAA服务器通知拥塞原因和UE的退避时间。

[0121] 提供了各个实施例,它们可以单独或组合使用。

[0122] 在一个实施例中,该TWAN被配置为:

[0123] -针对认证和授权用户,在由于拥塞控制针对APN活动而拒绝处于单连接模式(SCM)的UE的请求时,以信号向AAA服务器通知拥塞原因以及针对该UE和所请求APN的退避时间。

[0124] 在一个实施例中,该TWAN被配置为:

[0125] -针对以所请求的APN为目标的业务或者针对任何业务而从已经对TWAN触发了过载控制的PDN网关接收过载控制信息。

[0126] 在一个实施例中,该TWAN被配置为:

[0127] -向AAA服务器指示该AAA服务器是否应当对来自其它UE的以相同APN为目标的请求进行退避。

[0128] 在另一个方面,提供了一种AAA服务器,其被配置为对于针对EPC的受信任WLAN访问:

[0129] -从受信任WLAN访问网络TWAN接收拥塞原因以及针对单连接模式的UE的请求的退避时间,

[0130] -将拥塞原因和退避时间包括在其发送至UE的响应消息中,

[0131] -通过返回具有拥塞原因以及剩余退避时间的响应消息从而可选地拒绝来自相同UE的任何后续请求直至退避计时器超时。

[0132] 在一个实施例中，该AAA服务器可以被配置为：

[0133] -如果该AAA服务器已经从TWAN接收到该AAA服务器应当对来自其它UE的以相同APN为目标的请求进行退避的指示，则拒绝来自其它UE的以该APN为目标的任何后续请求直至退避计时器超时。

[0134] 在另一个方面，提供了一种AAA服务器，其被配置为对于针对EPC的受信任WLAN访问：

[0135] -从受信任WLAN访问网络TWAN接收APN拥塞原因以及针对单连接模式的UE的请求的所请求APN的退避时间，

[0136] -将APN拥塞原因和退避时间包括在其发送至UE的响应消息中，

[0137] -通过返回具有拥塞原因以及剩余退避时间的响应消息而可选地拒绝来自相同UE的以相同APN为目标的任何后续请求直至退避计时器超时。

[0138] 在一个实施例中，该AAA服务器可以被配置为：

[0139] -如果该AAA服务器已经从TWAN接收到该AAA服务器应当对来自其它UE的以相同APN为目标的请求进行退避的指示，则拒绝来自其它UE的以该APN为目标的任何后续请求直至退避计时器超时。

[0140] 在另一个方面，提供了一种用户设备UE，其被配置为在针对EPC的受信任WLAN访问：

[0141] -根据从AAA服务器接收的拥塞原因和退避时间，在该退避时间的持续时间内不发起任何新的请求。

[0142] 提供了各个实施例，它们可以单独或组合使用。

[0143] 在一个实施例中，该UE被配置为在针对EPC的受信任WLAN访问：

[0144] -根据从AAA服务器接收的拥塞原因和退避时间，在该退避时间的持续时间内不针对拥塞APN发起任何新的请求。

[0145] 在一个实施例中，该UE被配置为：

[0146] -在来自AAA服务器的响应消息中接收该拥塞原因和退避时间。

[0147] 在另一个方面，提供了一种用于针对EPC进行受信任WLAN访问的受信任WLAN访问网络TWAN，其被配置为：

[0148] -当由于拥塞而针对认证和授权用户拒绝SCM模式的UE的请求时，针对该UE或者在拥塞控制对于所请求的APN活动时针对所请求的APN开启退避计时器；

[0149] -通过向AAA服务器返回具有拥塞原因以及剩余退避时间的响应消息而拒绝来自相同UE的任何后续请求或者来自相同UE的以该APN为目标的任何后续请求直至该退避计时器超时。

[0150] 在另一个方面，提供了一种用于针对EPC进行受信任WLAN访问的受信任WLAN访问网络TWAN，其被配置为：

[0151] -当由于拥塞而针对认证和授权用户拒绝TSCM模式的UE的请求时，在拥塞控制是全局化时按照UE开启退避计时器或者在拥塞控制对于所请求的APN活动时按照UE以及按照SSID开启退避计时器。

[0152] 提供了各个实施例，它们可以单独或组合使用。

[0153] 在一个实施例中，该TWAN被配置为：

[0154] -在退避计时器超时之前，拒绝或默默丢弃所接收的来自相同UE的任何后续请求或者来自相同UE的以相同SSID为目标的任何后续请求。

[0155] 在一个实施例中，该TWAN被配置为：

[0156] -基于该UE的MAC地址而检测来自相同的UE的请求以便在退避计时器超时之前拒绝或默默丢弃所接收的源自于相同UE的任何后续信令请求或者通过相同的所选择SSID而源自于相同UE的任何后续信令请求。

[0157] 在一个实施例中，该TWAN被配置为：

[0158] -通过发送回响应消息和/或通过释放WLAN关联而拒绝来自UE的任何后续请求或者通过相同的所选择SSID而来自该UE的任何后续请求。

[0159] 在一个实施例中，该TWAN被配置为：

[0160] -创建和维护用于该退避时间的持续时间的UE过载控制记录，其针对处于透明单连接模式的UE而包含UE的MAC地址、SSID、UE的IMSI和退避时间。

[0161] 在一个实施例中，该TWAN被配置为：

[0162] -在从UE接收到新的后续信令请求时，通过检查其是否具有针对相同UE的MAC地址和可能的SSID的过载控制记录来检查该TWAN是否需要退避该UE。

[0163] 在一个实施例中，该TWAN被配置为：

[0164] -从已经针对以该APN为目标的业务或者任何业务而对TWAN触发了过载控制的PDN网关PGW接收过载信息。

[0165] 在另一个方面，提供了一种用于针对EPC进行受信任WLAN访问的过载控制的方法，包括：

[0166] -当由于拥塞而针对认证和授权用户拒绝SCM模式的UE的请求时，网络以信号向UE通知退避时间，在拥塞控制针对APN活动时这可能仅能够应用于所请求的APN，

[0167] -在接收到该退避时间时，UE在该退避时间的持续时间内不发起新的请求或者针对拥塞APN的新的请求。

[0168] 在另一个方面，提供了一种用于针对EPC进行受信任WLAN访问的过载控制的方法，包括：

[0169] -当由于拥塞而针对认证和授权用户拒绝TSCM模式的UE的请求时，受信任WLAN访问网络TWAN在拥塞控制是全局化时按照UE开启退避计时器或者在拥塞控制对于所请求的APN活动时按照UE和SSID开启退避计时器。

[0170] 在一个实施例中，该方法包括：

[0171] -该受信任WAN访问网络TWAN在退避计时器超时之前，拒绝或默默丢弃所接收的来自相同UE或者来自相同UE的以该APN为目标的任何后续请求。

[0172] 本领域技术人员将会轻易认识到，以上所描述的各种方法的步骤能够由编程计算机来执行。这里，一些实施例还意在覆盖程序存储设备，例如数字数据存储媒体，其可以是机器或计算机可读的并且对机器可执行或计算机可执行的指令程序进行编码，其中所述指令执行以上所描述的所述方法的一些或全部步骤。该程序存储设备例如可以是数字存储器，磁性存储媒体—诸如磁盘和磁带，硬盘，或者光学可读数字数据存储媒体。实施例还意在覆盖被编程为执行以上所描述方法的所述步骤的计算机。

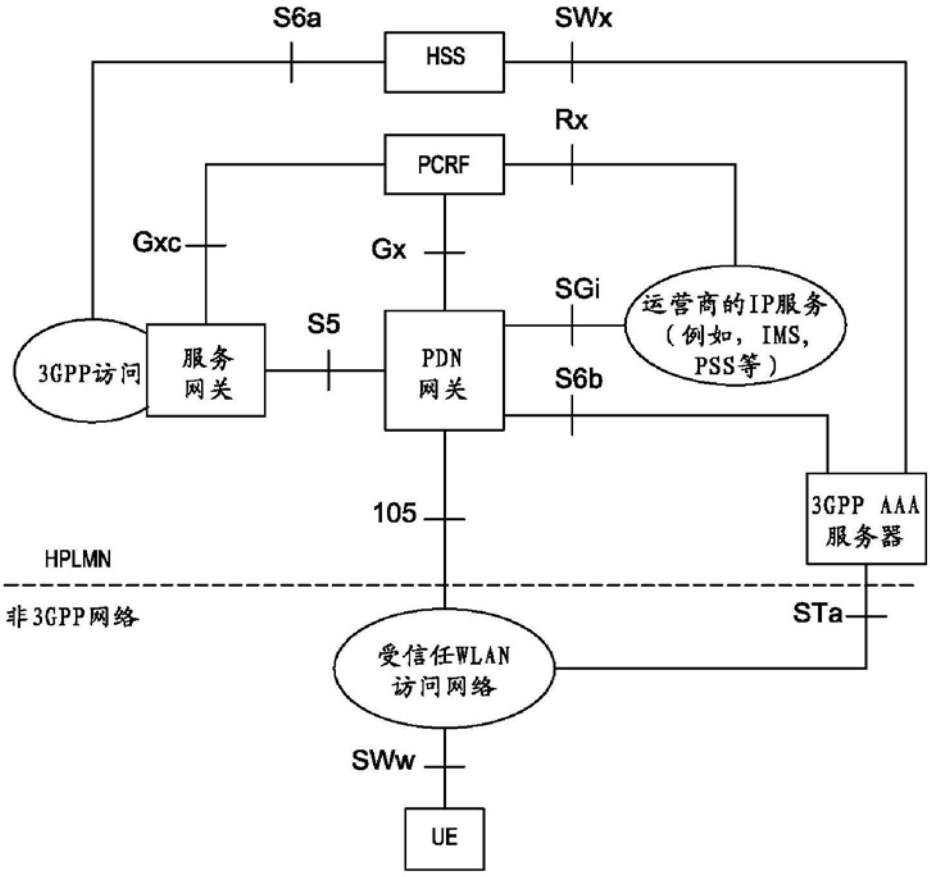

S6a
SWx
HSS
Rx
PCRF
Gxc
Gx
SGi
运营商的IP服务
（例如，IMS，
PSS等）
S5
3GPP访问
服务
网关
PDN
网关
S6b
105
3GPP AAA
服务器
HPLMN
非3GPP网络
STa
受信任WLAN
访问网络
SWw
UE

图1

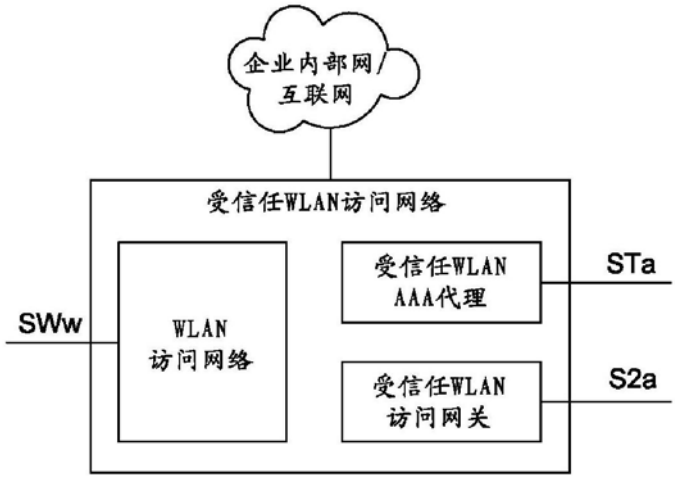

企业内部网/
互联网
受信任WLAN访问网络
受信任WLAN
AAA代理
STa
SWw
WLAN
访问网络
受信任WLAN
访问网关
S2a

图2

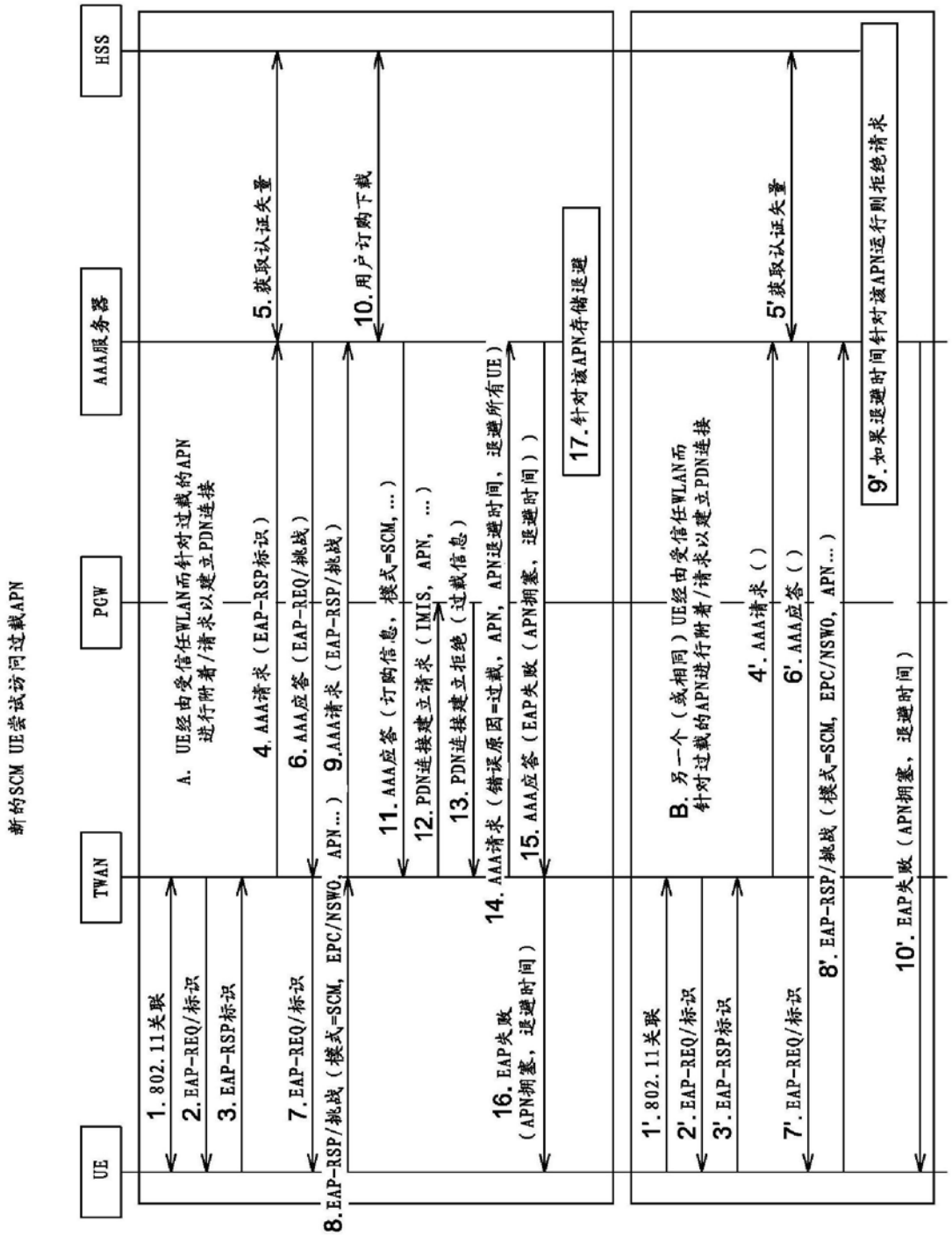

新的SCM UE尝试访问过载APN
UE
TWAN
PGW
AAA服务器
HSS
A. UE经由受信任WLAN而针对过载的APN进行附着/请求以建立PDN连接
B. 另一个（或相同）UE经由受信任WLAN而针对过载的APN进行附着/请求以建立PDN连接
1. 802.11关联
2. EAP-REQ/标识
3. EAP-RSP标识
4. AAA请求（EAP-RSP标识）
5. 获取认证矢量
6. AAA应答（EAP-REQ/挑战）
7. EAP-REQ/标识
8. EAP-RSP/挑战（模式=SCM, EPC/NSWO, APN...）
9. AAA请求（EAP-RSP/挑战）
10. 用户订购下载
11. AAA应答（订购信息，模式=SCM, ...）
12. PDN连接建立请求（IMIS, APN, ...）
13. PDN连接建立拒绝（过载信息）
14. AAA请求（错误原因=过载，APN，APN退避时间，退避所有UE）
15. AAA应答（EAP失败（APN拥塞，退避时间））
16. EAP失败（APN拥塞，退避时间）
17. 针对该APN存储退避
1'. 802.11关联
2'. EAP-REQ/标识
3'. EAP-RSP标识
4'. AAA请求（）
5'. 获取认证矢量
6'. AAA应答（）
7'. EAP-REQ/标识
8'. EAP-RSP/挑战（模式=SCM, EPC/NSWO, APN...）
9'. 如果退避时间针对该APN运行则拒绝请求
10'. EAP失败（APN拥塞，退避时间）

图3

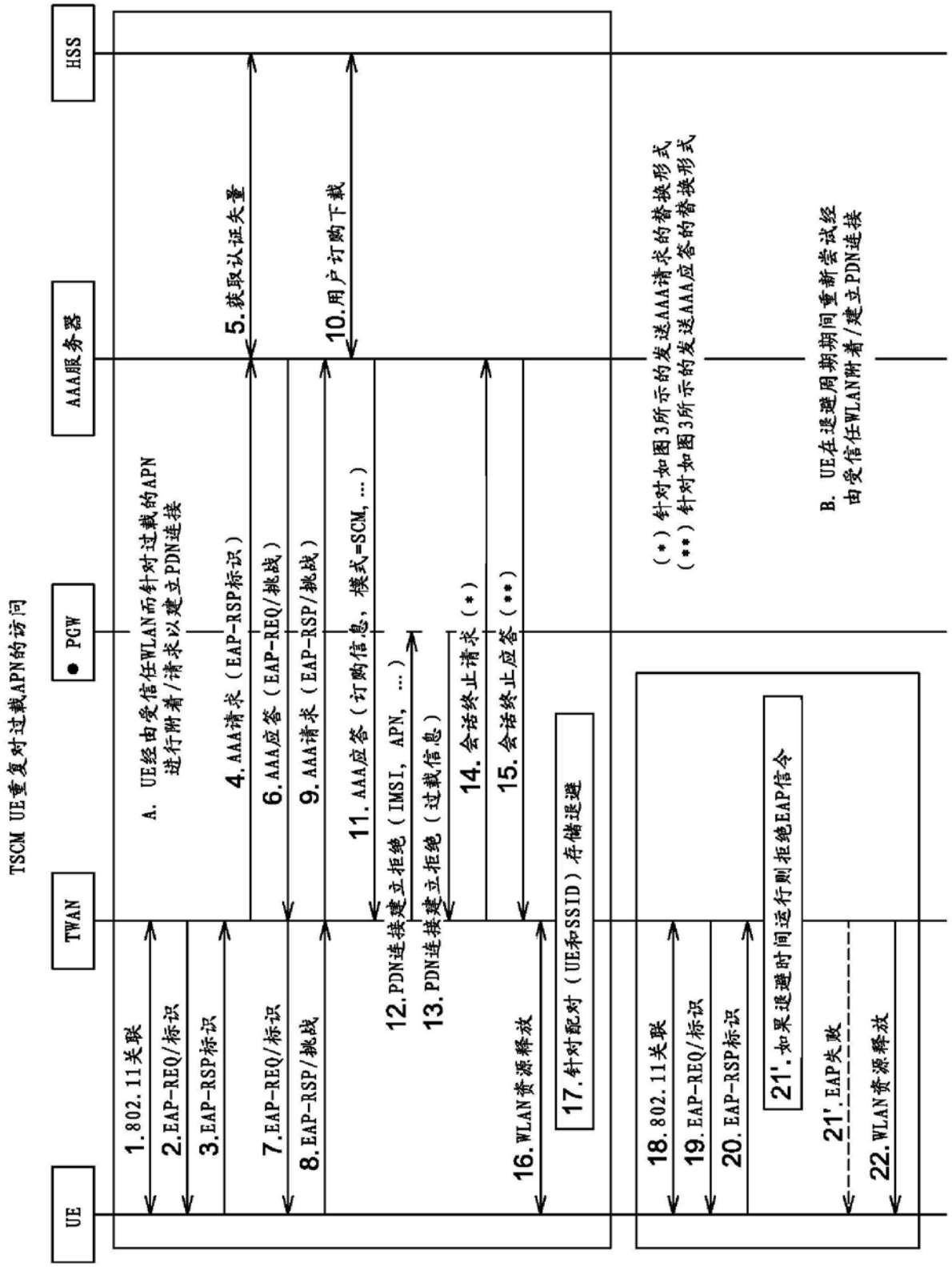

TSCM UE重复对过载APN的访问
UE
TWAN
PGW
AAA服务器
HSS
A. UE经由受信任WLAN而针对过载的APN进行附着/请求以建立PDN连接
1.802.11关联
2.EAP-REQ/标识
3.EAP-RSP标识
4.AAA请求（EAP-RSP标识）
5.获取认证矢量
6.AAA应答（EAP-REQ/挑战）
7.EAP-REQ/标识
8.EAP-RSP/挑战
9.AAA请求（EAP-RSP/挑战）
10.用户订购下载
11.AAA应答（订购信息，模式=SCM，…）
12.PDN连接建立拒绝（IMSI，APN，…）
13.PDN连接建立拒绝（过载信息）
14.会话终止请求（*）
15.会话终止应答（**）
16.WLAN资源释放
17.针对配对（UE和SSID）存储退避
（*）针对如图3所示的发送AAA请求的替换形式
（**）针对如图3所示的发送AAA应答的替换形式
B. UE在退避周期期间重新尝试经由受信任WLAN附着/建立PDN连接
18.802.11关联
19.EAP-REQ/标识
20.EAP-RSP标识
21'.如果退避时间运行则拒绝EAP信令
21'.EAP失败
22.WLAN资源释放

图4