(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102264065 A
(43)申请公布日 2011.11.30

(21)申请号 201010187361.3

(22)申请日 2010.05.27

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 王波 李静岚

(74)专利代理机构 北京派特恩知识产权代理事务所(普通合伙) 11270
代理人 张颖玲 蒋雅洁

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 24/00(2009.01)
H04W 76/02(2009.01)

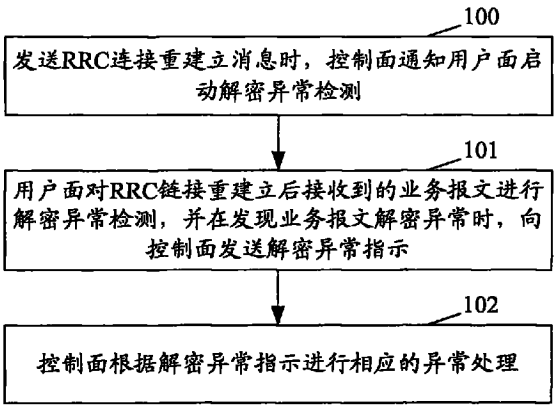
权利要求书 3 页 说明书 6 页 附图 4 页

(54)发明名称

一种实现接入层安全算法同步的方法及系统

(57)摘要

本发明公开了一种实现接入层安全算法同步的方法及系统，控制面发送RRC连接重建立消息时通知用户面启动解密异常检测；用户面对RRC连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示；控制面根据异常指示进行相应的异常处理。通过本发明方法，及时发现了RRC连接重建立时给UE配置的AS安全算法的异常，最大程度地避免了空口无效数据包对带宽的浪费，提高了异常恢复及时性，并进一步改善了切换前后的用户体验。



CN 102264065 A

1. 一种实现接入层安全算法保护的方法，其特征在于，包括：

发送 RRC 连接重建立消息时，控制面通知用户面启动解密异常检测；

用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示；

控制面根据解密异常指示进行相应的异常处理。

2. 根据权利要求 1 所述的方法，其特征在于，该方法还包括：预先设置检测计数器及其检测阈值；

如果所述解密异常检测次数达到检测阈值，或所述用户面已上报解密异常指示，所述用户面退出解密异常检测。

3. 根据权利要求 2 所述的方法，其特征在于，该方法还包括：预先设置异常计数器及其异常阈值；所述异常计数器用于统计所述解密异常检测发现业务报文解密异常次数；

如果所述异常计数器达到异常阈值，所述用户面上报解密异常指示，并退出解密异常检测。

4. 根据权利要求 3 所述的方法，其特征在于，所述异常计数器的异常阈值的取值小于或等于所述检测计数器的检测阈值。

5. 根据权利要求 1 所述的方法，其特征在于，预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

所述用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示具体包括：

所述用户面分组数据汇聚 PDCP 层收到所述控制面的通知，对 RRC 连接重建立后接收到的报文进行解密；

所述 PDCP 层对解密后的报文内容进行解析，并累加检测计数器；

在解密后的报文不符合 IP 协议时，累加异常计数器，并在异常计数器达到异常阈值时，用户面 PDCP 层向控制面发送解密异常指示，同时关闭解密异常检测。

6. 根据权利要求 1 所述的方法，其特征在于，预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

进行所述 RRC 连接重建立的演进节点 B eNB 及用户设备 UE 支持鲁棒性头压缩 ROHC；

所述用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示具体包括：

所述用户面分组数据汇聚 PDCP 层收到所述控制面的通知，对 RRC 连接重建立后接收到的报文进行解密；

所述 PDCP 层对解密后的报文进行 ROHC 解压缩，在解压缩成功时，解析解压缩后的报文内容，并累加检测计数器；

在解压失败或者经过解析所述解压缩后的报文不符合 IP 协议规则时，累加异常计数器，并在异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

7. 根据权利要求 1、5 或 7 所述的方法，其特征在于，如果在所述 RRC 连接重建立之前的切换时，有上行反传数据；

该方法还包括：在所述用户面 PDCP 层的上行重排序处理中进行报文匹配操作。

8. 根据权利要求 7 所述的方法，其特征在于，预先设置检测计数器及其检测阈值，异常

计数器及其异常阈值；

所述报文匹配操作具体包括：

所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

所述PDCP层将解密后的报文内容与所述上行反传数据进行IP头匹配，并累加检测计数器；

在IP头匹配失败时，累加异常计数器，并在异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

9. 一种实现接入层安全算法保护的系统，其特征在于，至少包括控制面和用户面，其中，

控制面，用于在发送RRC连接重建立消息时，控制面通知用户面启动解密异常检测；根据异常指示进行相应的异常处理；

用户面，用于对RRC连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示。

10. 根据权利要求9所述的系统，其特征在于，在所述用户面中预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

所述用户面，具体用于：

所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

所述PDCP层对解密后的报文内容进行解析，并累加检测计数器；

在解密后的报文不符合IP协议时，累加异常计数器，并在异常计数器达到异常阈值时，用户面PDCP层向控制面发送解密异常指示，同时关闭解密异常检测。

11. 根据权利要求9所述的系统，其特征在于，进行所述RRC连接重建立的演进节点BeNB及用户设备UE支持鲁棒性头压缩ROHC；在所述用户面中预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

所述用户面，具体用于：

所述用户面对RRC连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示具体包括：

所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

所述PDCP层对解密后的报文进行ROHC解压缩，在解压缩成功时，解析解压缩后的报文内容，并累加检测计数器；

在解压失败或者经过解析所述解压缩后的报文不符合IP协议规则时，累加异常计数器，并在异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

12. 根据权利要求9～11任一项所述的系统，其特征在于，在所述RRC连接重建立之前的切换时，有上行反传数据；

所述用户面还用于：PDCP层的上行重排序处理中进行报文匹配操作。

13. 根据权利要求12所述的系统，其特征在于，在所述用户面中预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

所述用户面具体用于：

所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

所述PDCP层将解密后的报文内容与所述上行反传数据进行IP头匹配，并累加检测计数器；

在IP头匹配失败时，累加异常计数器，并在异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

一种实现接入层安全算法同步的方法及系统

技术领域

[0001] 本发明涉及长期演进(LTE,Long Term Evolution)技术,尤指一种切换后发生RRC连接重建时,实现接入层安全算法同步的方法及系统。

背景技术

[0002] 目前,在长期演进(LTE,Long Term Evolution)系统中,由于演进节点B(eNB,E-UTRAN Node B)的地理位置和逻辑结构的高度分散化,运营商无法对eNB实行集中的安全控制,每个eNB都处于非安全区。

[0003] eNB需要根据各自的具体情况以及用户设备(UE,User Equipment)的安全能力,来选择适合自身的接入层(AS,Access Stratum)安全算法。AS安全算法选择的基本原则是:UE的安全能力信息通过信令流程发给eNB(比如:核心网在初始上下文建立请求消息中将UE的安全能力携带给eNB),eNB在自身及UE所支持的AS安全算法交集中,选择一个最高优先级的AS安全算法。当发生切换时,eNB需要根据上述原则更新AS安全算法,并通过空口消息将新的AS安全算法告知UE。

[0004] 每个eNB需要自行维护与UE之间的AS安全参数(包括算法和密钥)。显然,各eNB对AS安全算法的支持情况不一定相同。当发生跨eNB切换时,如果UE切换失败,那么,UE可能在目标侧eNB又发起无线资源控制(RRC)连接重建立(RRC connection re-establishment),此时,如果目标侧eNB不支持UE原来的AS安全算法,会造成AS安全算法不同步的问题,具体来讲:

[0005] 假设eNB 1支持的AS安全算法是eNB2不支持的,那么,当UE因为切换到eNB2失败(如切换时的RRC重配置未生效)而发生RRC连接重建立到eNB2时,如果UE不根据eNB2所支持的AS安全算法重新进行AS安全算法选择,而是仍使用原AS安全算法(即eNB1支持的AS安全算法)对RRC重建立完成消息进行完整性保护和加密的话,eNB2必定会因为不支持原AS安全算法而产生对该消息的解密和完整性校验的失败,最终导致UE切换后的接入失败,从而严重影响了用户的感受度。

[0006] 针对上述由于RRC连接重建立时均不进行AS安全算法更新,而导致的AS安全算法不同步的问题,通常,可以通过在eNB发给UE的RRC连接重建立消息中增加AS安全算法配置信元的方法来解决。但是,同时却引入了一个新的问题:新的AS安全算法配置只能通过RRC连接重建立消息发送给UE,而RRC连接重建立消息本身是不经过完整性保护的,因此,如果恶意攻击者将RRC连接重建立消息中携带的数据加密算法进行篡改,eNB和UE是不能及时发现的,这样,就会导致空口一段时间内存在大量的eNB无法解密的无效数据包,这样,不但浪费了空口资源,而且进一步严重影响了用户体验。

发明内容

[0007] 有鉴于此,本发明的主要目的在于提供一种实现接入层安全算法同步的方法及系统,能够及时发现RRC连接重建立时给UE配置的AS安全算法的异常,最大程度地避免空口

无效数据包对带宽的浪费，提高异常恢复及时性，从而进一步改善了切换前后的用户体验。

[0008] 为达到上述目的，本发明的技术方案是这样实现的：

[0009] 一种实现接入层安全算法保护的方法，包括：

[0010] 发送 RRC 连接重建立消息时，控制面通知用户面启动解密异常检测；

[0011] 用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示；

[0012] 控制面根据解密异常指示进行相应的异常处理。

[0013] 该方法还包括：预先设置检测计数器及其检测阈值；

[0014] 如果所述解密异常检测次数达到检测阈值，或所述用户面已上报解密异常指示，所述用户面退出解密异常检测。

[0015] 该方法还包括：预先设置异常计数器及其异常阈值；所述异常计数器用于统计所述解密异常检测发现业务报文解密异常次数；

[0016] 如果所述异常计数器达到异常阈值，所述用户面上报解密异常指示，并退出解密异常检测。

[0017] 所述异常计数器的异常阈值的取值小于或等于所述检测计数器的检测阈值。

[0018] 预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

[0019] 所述用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示具体包括：

[0020] 所述用户面分组数据汇聚 PDCP 层收到所述控制面的通知，对 RRC 连接重建立后接收到的报文进行解密；

[0021] 所述 PDCP 层对解密后的报文内容进行解析，并累加检测计数器；

[0022] 在解密后的报文不符合 IP 协议时，累加异常计数器，并在异常计数器达到异常阈值时，用户面 PDCP 层向控制面发送解密异常指示，同时关闭解密异常检测。

[0023] 预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

[0024] 进行所述 RRC 连接重建立的演进节点 B eNB 及用户设备 UE 支持鲁棒性头压缩 ROHC；

[0025] 所述用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示具体包括：

[0026] 所述用户面分组数据汇聚 PDCP 层收到所述控制面的通知，对 RRC 连接重建立后接收到的报文进行解密；

[0027] 所述 PDCP 层对解密后的报文进行 ROHC 解压缩，在解压缩成功时，解析解压缩后的报文内容，并累加检测计数器；

[0028] 在解压失败或者经过解析所述解压缩后的报文不符合 IP 协议规则时，累加异常计数器，并在异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

[0029] 如果在所述 RRC 连接重建立之前的切换时，有上行反传数据；

[0030] 该方法还包括：在所述用户面 PDCP 层的上行重排序处理中进行报文匹配操作。

[0031] 预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

[0032] 所述报文匹配操作具体包括：

[0033] 所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

[0034] 所述PDCP层将解密后的报文内容与所述上行反传数据进行IP头匹配，并累加检测计数器；

[0035] 在IP头匹配失败时，累加异常计数器，并在异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

[0036] 一种实现接入层安全算法保护的系统，至少包括控制面和用户面，其中，

[0037] 控制面，用于在发送RRC连接重建立消息时，控制面通知用户面启动解密异常检测；根据异常指示进行相应的异常处理；

[0038] 用户面，用于对RRC连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示。

[0039] 在所述用户面中预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

[0040] 所述用户面，具体用于：

[0041] 所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

[0042] 所述PDCP层对解密后的报文内容进行解析，并累加检测计数器；

[0043] 在解密后的报文不符合IP协议时，累加异常计数器，并在异常计数器达到异常阈值时，用户面PDCP层向控制面发送解密异常指示，同时关闭解密异常检测。

[0044] 进行所述RRC连接重建立的演进节点B eNB及用户设备UE支持鲁棒性头压缩ROHC；在所述用户面中预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

[0045] 所述用户面，具体用于：

[0046] 所述用户面对RRC连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示具体包括：

[0047] 所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

[0048] 所述PDCP层对解密后的报文进行ROHC解压缩，在解压缩成功时，解析解压缩后的报文内容，并累加检测计数器；

[0049] 在解压失败或者经过解析所述解压缩后的报文不符合IP协议规则时，累加异常计数器，并在异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

[0050] 在所述RRC连接重建立之前的切换时，有上行反传数据；

[0051] 所述用户面还用于：PDCP层的上行重排序处理中进行报文匹配操作。

[0052] 在所述用户面中预先设置检测计数器及其检测阈值，异常计数器及其异常阈值；

[0053] 所述用户面具体用于：

[0054] 所述用户面分组数据汇聚PDCP层收到所述控制面的通知，对RRC连接重建立后接收到的报文进行解密；

[0055] 所述PDCP层将解密后的报文内容与所述上行反传数据进行IP头匹配，并累加检测计数器；

[0056] 在IP头匹配失败时，累加异常计数器，并在异常计数器达到异常阈值，向控制面

发送解密异常指示，同时关闭解密异常检测。

[0057] 从上述本发明提供的技术方案可以看出，控制面发送 RRC 连接重建立消息时通知用户面启动解密异常检测；用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示；控制面根据异常指示进行相应的异常处理。通过本发明方法，及时发现了 RRC 连接重建立时给 UE 配置的 AS 安全算法的异常，最大程度地避免了空口无效数据包对带宽的浪费，提高了异常恢复及时性，从而进一步改善了切换前后的用户体验。本文将基站侧控制面简称为控制面，将基站侧用户面简称为用户面。

附图说明

[0058] 图 1 为本发明实现 AS 算法同步的流程示意图；

[0059] 图 2 为本发明实现 AS 安全算法同步的系统的组成结构示意图；

[0060] 图 3 为本发明实现 AS 算法同步的第一实施例的流程示意图

[0061] 图 4 为本发明实现 AS 算法同步的第二实施例的流程示意图；

[0062] 图 5 为本发明实现 AS 算法同步的第三实施例的流程示意图。

具体实施方式

[0063] 本文中所述的控制面和用户面分别指基站侧控制面和基站侧用户面。

[0064] 图 1 为本发明切换后发生 RRC 连接重建时，实现 AS 算法同步的流程示意图，如图 1 所示，包括以下步骤：

[0065] 步骤 100：发送 RRC 连接重建立消息时，控制面通知用户面启动解密异常检测。

[0066] 步骤 102：用户面对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示。

[0067] 本步骤中，对接收到的业务报文进行的解密异常检测属于本领域技术人员惯用技术手段，具体实现方法不用于限定本发明的保护范围，这里不再详述。

[0068] 本步骤中，进一步地，可以预先设置检测计数器及其检测阈值，如果解密异常检测次数达到检测阈值或用户面已上报解密异常指示，则用户面退出解密异常检测。

[0069] 进一步地，还可以预先设置异常计数器及其异常阈值，该异常计数器用于统计所述解密异常检测发现业务报文解密异常次数。如果异常计数器达到异常阈值，则用户面上报解密异常指示，并退出解密异常检测。

[0070] 这里，异常计数器的异常阈值的取值可以设置为：小于或等于检测计数器的检测阈值。

[0071] 步骤 103：控制面根据解密异常指示进行相应的异常处理。本步骤强调的是，控制面能根据用户面的异常指示，及时对异常情况进行相应处理，而如何进行处理不是本发明要保护的，也不用于限定本发明的保护范围。

[0072] 由于本发明在 RRC 连接重建立中，引入了用户面同步过程（即步骤 102），使得 eNB 和 UE 及时发现了 RRC 连接重建立时 UE 配置的 AS 安全算法的异常情况，最大程度地避免了空口无效数据包对带宽的浪费，提高了异常恢复及时性，从而进一步改善了切换前后的用户体验。

[0073] 图 2 为本发明实现 AS 安全算法同步的系统的组成结构示意图，如图 2 所示，至少包括控制面和用户面，其中，

[0074] 控制面，用于在发送 RRC 连接重建立消息时，控制面通知用户面启动解密异常检测；根据异常指示进行相应的异常处理。

[0075] 用户面，用于对 RRC 连接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示。

[0076] 下面结合实施例对本发明方法进行详细描述。以下实施例中涉及的解密处理，有可能是指 Null Algorithm 的空算法处理。

[0077] 图 3 为本发明实现 AS 算法同步的第一实施例的流程示意图，LTE 业务是基于 IP 的分组业务，因此，在第一实施例中，假设在分组数据汇聚层 (PDCP，Packet Data Convergence Protocol) 层对接收的分组报文进行异常分析处理，即对 PDCP 层解密后的接收报文进行异常分析，如图 3 所示，包括以下步骤：

[0078] 步骤 300：控制面发送 RRC 连接重建立消息并指示用户面 PDCP 层启动解密异常检测。

[0079] 步骤 301：PDCP 层对 RRC 连接重建立后接收到的报文进行解密。

[0080] 步骤 302：PDCP 层对解密后的报文内容进行解析，并累加检测计数器。

[0081] 在检测计数器达到预设检测阈值时，关闭解密异常检测。

[0082] 步骤 303：在解密后的报文不符合 IP 协议时，比如该报文的 IP 头已被破坏等，则累加异常计数器。

[0083] 在异常计数器达到异常阈值时，用户面 PDCP 层向控制面发送解密异常指示，同时关闭解密异常检测。

[0084] 步骤 304：控制面收到用户面的解密异常指示，进行相应异常处理。

[0085] 图 4 为本发明实现 AS 算法同步的第二实施例的流程示意图，第二实施例中，假设 eNB 及 UE 支持鲁棒性头压缩 (ROHC，RObust Header Compression) 功能，则可以在解压器 (Decompressor) 输出端进行解密异常检测，如图 4 所示，包括以下步骤：

[0086] 步骤 400：控制面发送 RRC 连接重建立消息并通知用户面 PDCP 层启动解密异常检测。

[0087] 步骤 401：PDCP 层对 RRC 连接重建立后接收到的报文进行解密。

[0088] 步骤 402：PDCP 层对解密后的报文进行 ROHC 解压缩。

[0089] 步骤 403：在解压缩成功时，进一步解析解压缩后的报文内容，并累加检测计数器。

[0090] 如果检测计数器达到检测阈值，则关闭解密异常检测。

[0091] 步骤 404：在解压失败或者经过解析该报文不符合 IP 协议规则时，累加异常计数器。

[0092] 如果异常计数器达到异常阈值，向控制面发送解密异常指示，同时关闭解密异常检测。

[0093] 步骤 405：控制面收到用户面的解密异常指示，进行相应异常处理。

[0094] 图 5 为本发明实现 AS 算法同步的第三实施例的流程示意图，如果 UE 发生切换时，有上行反传数据 (UL Data Forwarding)，那么，可以在 PDCP 层的上行重排序 (Reordering)

处理中进一步进行报文匹配操作。具体就是：将反传到目标侧的上行反传数据作为基准，将目标侧 RRC 连接重建立后接收到的报文与基准进行比对来进一步检测解密异常，如图 5 所示，包括以下步骤：

[0095] 步骤 500：控制面发送 RRC 链接重建立消息，并指示用户面 PDCP 层启动解密异常检测。

[0096] 步骤 501：PDCP 层对 RRC 连接重建立后接收到的报文进行解密。

[0097] 步骤 502：PDCP 层将解密后的报文内容与上行反传数据进行 IP 头匹配，并累加检测计数器。

[0098] 如果检测计数器达到检测阈值，则关闭解密异常检测。

[0099] 步骤 503：在 IP 头匹配失败时，累加异常计数器。

[0100] 如果异常计数器达到异常阈值，则用户面 PDCP 层向控制面发送解密异常指示，同时关闭解密异常检测。

[0101] 步骤 504：控制面收到用户面的解密异常指示，进行相应异常处理。

[0102] 图 5 所示的第三实施例可以与第一实施例结合使用，也可以与第二实施例结合使用，具体组合实现是本领域技术人员在获知本发明方法后容易实现的，这里不再详述。

[0103] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

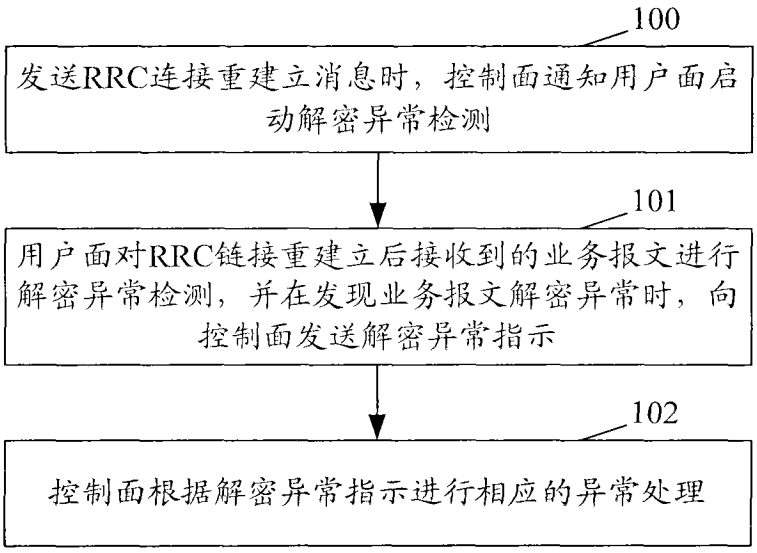

100
发送RRC连接重建立消息时，控制面通知用户面启动解密异常检测
101
用户面对RRC链接重建立后接收到的业务报文进行解密异常检测，并在发现业务报文解密异常时，向控制面发送解密异常指示
102
控制面根据解密异常指示进行相应的异常处理

图 1

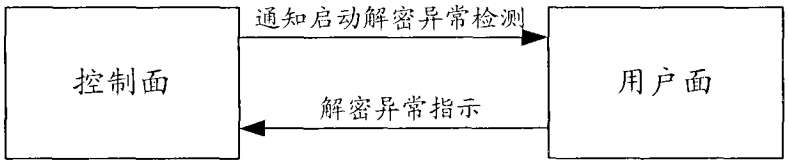

控制面
通知启动解密异常检测
解密异常指示
用户面

图 2

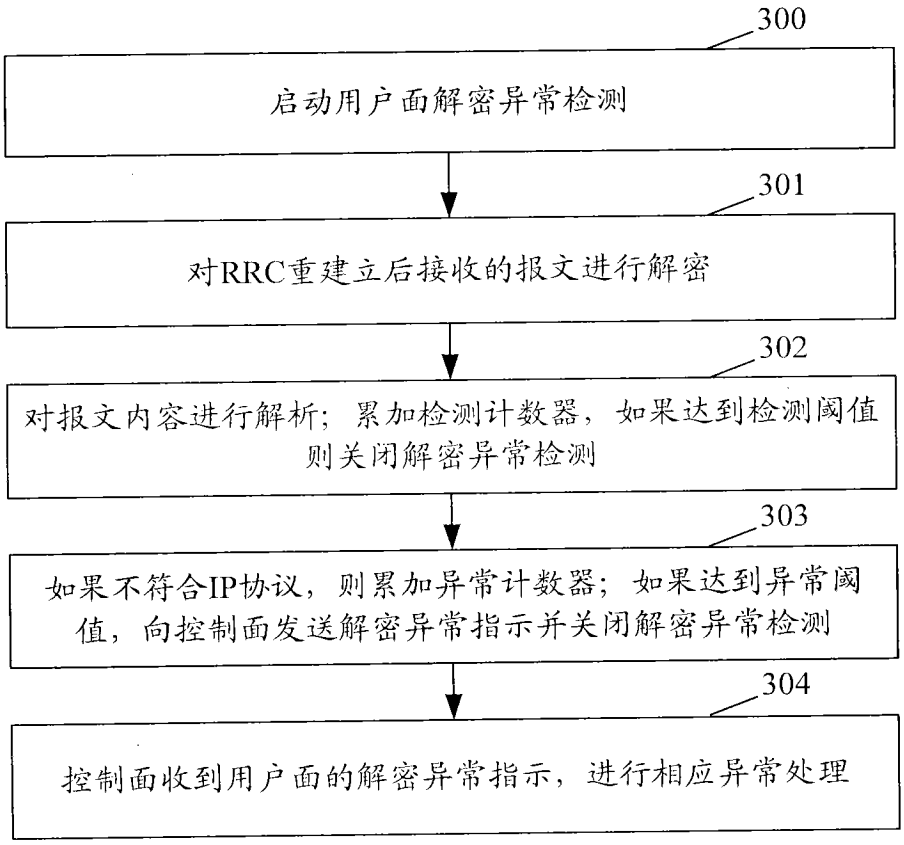

300
启动用户面解密异常检测
301
对RRC重建立后接收的报文进行解密
302
对报文内容进行解析；累加检测计数器，如果达到检测阈值则关闭解密异常检测
303
如果不符合IP协议，则累加异常计数器；如果达到异常阈值，向控制面发送解密异常指示并关闭解密异常检测
304
控制面收到用户面的解密异常指示，进行相应异常处理

图 3

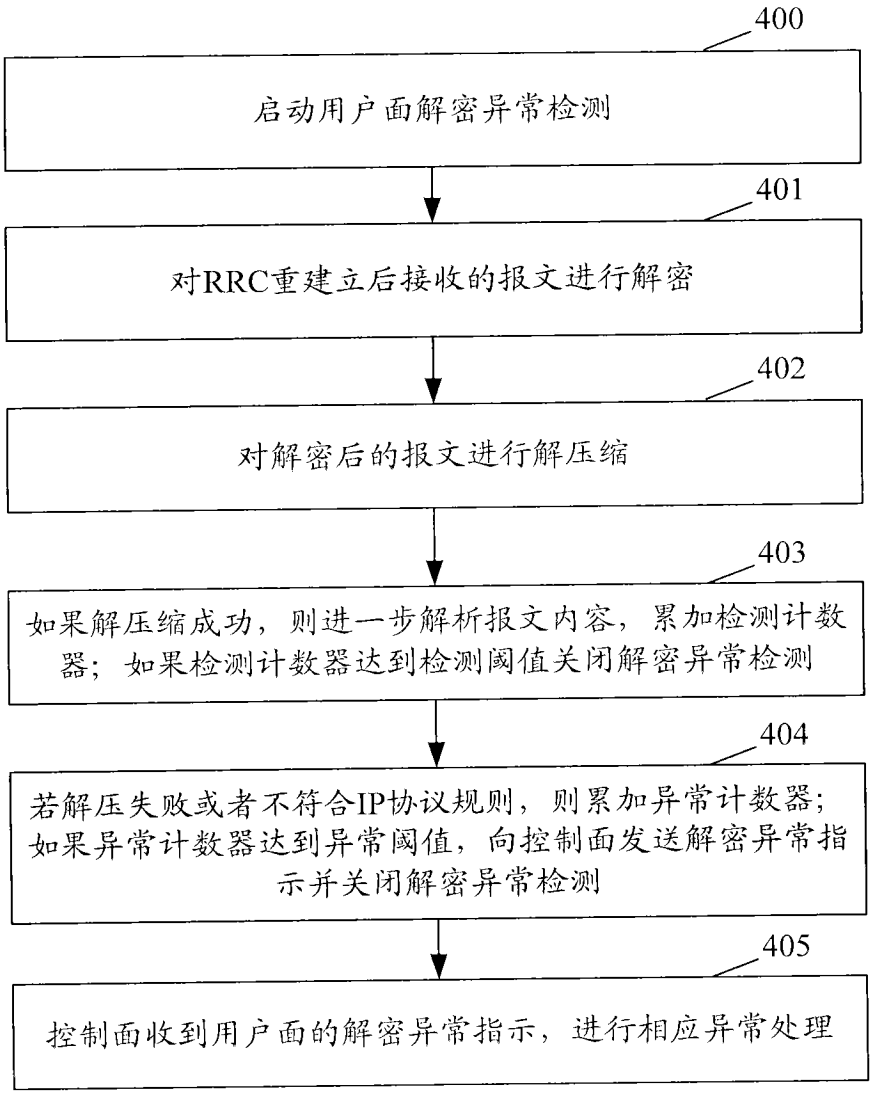

400
启动用户面解密异常检测
401
对RRC重建立后接收的报文进行解密
402
对解密后的报文进行解压缩
403
如果解压缩成功，则进一步解析报文内容，累加检测计数器；如果检测计数器达到检测阈值关闭解密异常检测
404
若解压失败或者不符合IP协议规则，则累加异常计数器；如果异常计数器达到异常阈值，向控制面发送解密异常指示并关闭解密异常检测
405
控制面收到用户面的解密异常指示，进行相应异常处理

图 4

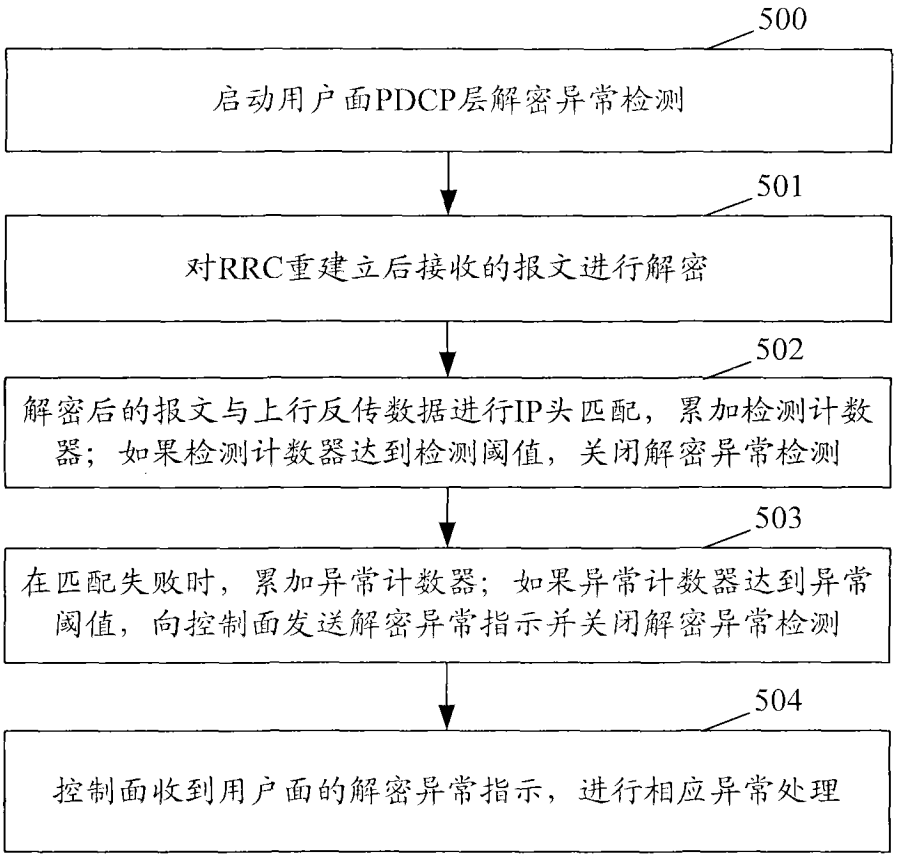

500
启动用户面PDCP层解密异常检测
501
对RRC重建立后接收的报文进行解密
502
解密后的报文与上行反传数据进行IP头匹配，累加检测计数器；如果检测计数器达到检测阈值，关闭解密异常检测
503
在匹配失败时，累加异常计数器；如果异常计数器达到异常阈值，向控制面发送解密异常指示并关闭解密异常检测
504
控制面收到用户面的解密异常指示，进行相应异常处理

图 5