(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 104767781 B
(45)授权公告日 2018.09.04

(21)申请号 201410008131.4

(22)申请日 2014.01.08

(65)同一申请的已公布的文献号
申请公布号 CN 104767781 A

(43)申请公布日 2015.07.08

(73)专利权人 杭州迪普科技股份有限公司
地址 310051 浙江省杭州市滨江区通和路68号中财大厦6层

(72)发明人 姜跃

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 102130910 A,2011.07.20,
WO 02102020 A1,2002.12.19,
CN 101867558 A,2010.10.20,
US 7328267 B1,2008.02.05,
CN 102130910 A,2011.07.20,
JP 2005136684 A,2005.05.26,
WO 2004004272 A1,2004.01.08,
US 2007283429 A1,2007.12.06,

审查员 朱立峰

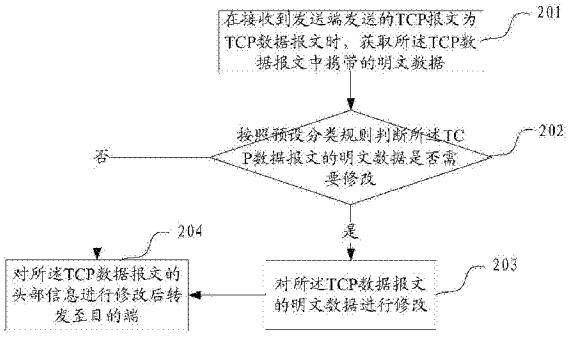
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种TCP代理装置以及方法

(57)摘要

本发明提供一种TCP代理装置以及方法，应用于建立TCP连接的发送端与目的端之间的网络设备上，其中该装置包括：数据获取模块，用于在接收到发送端发送的TCP报文为TCP数据报文时，获取所述TCP数据报文中携带的明文数据；报文判断模块，用于按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，如果是，内容处理模块对所述TCP数据报文的明文数据进行修改，并对所述TCP数据报文的头部信息进行修改后转发至目的端；如果否，对所述TCP数据报文的头部信息进行修改后转发至目的端。本发明减少了操作系统资源的消耗，大幅度提高了代理效率，在网络中相对核心位置上使用效果更佳。



CN 104767781 B

1.一种TCP代理装置，应用于建立TCP连接的发送端与目的端之间的网络设备上，其特征在于，所述装置包括：

数据获取模块，用于在接收到发送端发送的TCP报文为TCP数据报文时，获取所述TCP数据报文中携带的明文数据，其中，所述数据获取模块进一步用于接收到发送端发送的TCP数据报文时，先判断该报文携带的数据是否为SSL报文，如果不是，则确定该报文携带的数据为明文数据，转报文判断模块进行处理；如果是则进一步判断所述SSL报文是否为协议报文，如果是，则转SSL协议模块处理，否则确定该SSL报文为SSL数据报文，转SSL解密模块处理；

SSL解密模块，用于对SSL数据报文进行解密以获取报文的明文数据，并转报文判断模块进行处理；

SSL协议模块，用于按照SSL协议对SSL协议报文进行处理；

报文判断模块，用于按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，如果是，转内容处理模块进行处理，如果否，转头部处理模块进行处理；

内容处理模块，用于对所述TCP数据报文的明文数据进行修改，并转头部处理模块进行处理；

头部处理模块，用于对所述TCP数据报文的头部信息进行修改后转发至目的端。

2.如权利要求1所述的装置，其特征在于，还包括TCP协议模块，用于按照TCP协议对来自发送端的TCP协议报文进行处理；

所述数据获取模块进一步用于在接收到发送端发送的TCP报文为协议报文时，将该协议报文提交给TCP协议模块进行处理。

3.如权利要求1所述的装置，其特征在于，还包括：

数据加密模块，用于判断头部处理模块修改完成的TCP数据报文是否符合预设加密规则，如果是，对符合预设加密规则的报文进行加密后转发至目的端；否则将头部处理模块修改完成的TCP数据报文转发至目的端。

4.如权利要求1所述的装置，其特征在于，所述明文数据包括会话状态与报文特征，报文判断模块所述按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改具体包括：

若明文数据的会话状态与报文特征符合所述预设分类规则，判断所述报文的明文内容需要修改；否则，判断所述报文的明文内容不需要修改。

5.如权利要求1所述的装置，其特征在于，所述头部处理模块具体用于：

对所述TCP数据报文的IP地址以及TCP序列号进行修改。

6.如权利要求1所述的装置，其特征在于，所述头部处理模块进一步用于：保存TCP数据报文的头部信息修改前与修改后的TCP序列号及对应关系；

在TCP数据报文转发出现异常时，在所述对应关系中查找与出现异常的TCP数据报文修改后的TCP序列号对应的修改前的TCP序列号；

通知发送端重传TCP序列号为所述修改前的TCP序列号的TCP数据报文。

7.一种TCP代理方法，应用于建立TCP连接的发送端与目的端之间的网络设备上，其特征在于，所述方法包括：

步骤A、在接收到发送端发送的TCP报文为TCP数据报文时，获取所述TCP数据报文携带

的明文数据；

所述步骤A进一步包括接收到发送端发送的TCP数据报文时，先判断该报文携带的数据是否为SSL报文，如果不是，则确定该报文携带的数据为明文数据，转步骤B进行处理；如果是则进一步判断所述SSL报文是否为协议报文，如果是，则转步骤A2处理，否则确定该SSL报文为SSL数据报文，转步骤A1处理；

步骤A1、对SSL数据报文进行解密以获取报文的明文数据，并转步骤B进行处理；

步骤A2、按照SSL协议对SSL协议报文进行处理；

步骤B、按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，如果是，转步骤C进行处理，如果否，转步骤D进行处理；

步骤C、对所述TCP数据报文的内容进行修改，并转步骤D进行处理；

步骤D、对所述TCP数据报文的头部信息进行修改处理后转发至目的端。

8.如权利要求7所述的方法，其特征在于，所述方法进一步包括：

步骤A3、按照TCP协议对来自发送端的TCP协议报文进行处理；

所述步骤A进一步包括在接收到发送端发送的TCP报文为协议报文时，将该协议报文提交给步骤A3进行处理。

9.如权利要求7所述的方法，其特征在于，还包括：

判断步骤D修改完成的TCP数据报文是否符合预设加密规则，如果是，对符合预设加密规则的报文进行加密后转发至目的端；否则将步骤D修改完成的TCP数据报文转发至目的端。

10.如权利要求7所述的方法，其特征在于，所述明文数据包括会话状态与报文特征，步骤B所述按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改具体包括：

若明文数据的会话状态与报文特征符合所述预设分类规则，判断所述报文的明文内容需要修改；否则，判断所述报文的明文内容不需要修改。

11.如权利要求7所述的方法，其特征在于，所述步骤D具体包括：

对所述TCP数据报文的IP地址以及TCP序列号进行修改。

12.如权利要求7所述的方法，其特征在于，所述步骤D进一步包括：

保存TCP数据报文的头部信息修改前与修改后的TCP序列号及对应关系；

在TCP数据报文转发出现异常时，在所述对应关系中查找与出现异常的TCP数据报文修改后的TCP序列号对应的修改前的TCP序列号；

通知发送端重传TCP序列号为所述修改前的TCP序列号的TCP数据报文。

一种TCP代理装置以及方法

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种TCP代理的装置以及方法。

背景技术

[0002] TCP代理是处理基于内容的网络业务常见的手段，其基本模型为在原本互通的TCP发送端与目的端之间加入代理端，使原本直接交互的两端分别与代理端进行交互，代理端起到一个“传话”的作用，同时根据业务的需要对两端交互的内容进行修改。其应用十分广泛，如：七层负载均衡、SSL加速、SSLVPN、内容审计、代理上网、连接复用、WEB缓存等。大部分基于内容处理的业务都可以使用TCP代理来实现。

[0003] 现有TCP代理多数是使用socket代理来处理基于内容的网络业务，在传输过程中socket代理充当的角色是两个终端，比如socket代理1以及socket代理2，其中socket代理1与socket代理2运行在同一代理程序中。socket代理1负责与客户端进行TCP连接，再提取接收到的报文数据发送给应用代理程序。之后socket代理2与服务器进行连接，代理程序使用socket代理2把之前从socket代理1获得的数据转发至服务器。在该传输系统中，socket代理的系统类似是两条完全独立的链接，所有数据报文通过应用代理程序进行中转。

[0004] 然而由于使用socket代理需将socket代理1获取的数据发送到应用程序，处理完成后应用代理程序还要将数据发送到socket代理2，因此增加了操作系统资源的消耗以及报文在网络协议栈中的时间消耗，当并发数巨大时这无疑致命的打击。另一方面，使用socket代理还需要时刻监控socket的读写信号，这样对于没有读写信号的socket就相当于在做无用功，就算使用信号出发机制，也无法实现多CPU的异步处理，虽然对于普通系统这样的并发处理已经足够，但对于高端的网络设备来说这是远远不够的，因为高端的网络设备位于网络核心位置，其上的报文处理量十分巨大。

发明内容

[0005] 有鉴于此，本发明提供了一种TCP代理装置，应用于建立TCP连接的发送端与目的端之间的网络设备上，其中该装置包括：

[0006] 数据获取模块，用于在接收到发送端发送的TCP报文为TCP数据报文时，获取所述TCP数据报文中携带的明文数据；

[0007] 报文判断模块，用于按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，如果是，转内容处理模块进行处理，如果否，转头部处理模块进行处理；

[0008] 内容处理模块，用于对所述TCP数据报文的明文数据进行修改，并转头部处理模块进行处理；

[0009] 头部处理模块，用于对所述TCP数据报文的头部信息进行修改后转发至目的端。

[0010] 本发明还提供一种TCP代理方法，应用于建立TCP连接的发送端与目的端之间的网络设备上，其中该方法包括：

[0011] 步骤A、在接收到发送端发送的TCP报文为TCP数据报文时，获取所述TCP数据报文

携带的明文数据；

[0012] 步骤B、按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，如果是，转步骤C进行处理，如果否，转步骤D进行处理；

[0013] 步骤C、对所述TCP数据报文的内容进行修改，并转步骤D进行处理；

[0014] 步骤D、对所述TCP数据报文的头部信息进行修改处理后转发至目的端。

[0015] 本发明提供的TCP代理装置以及方法，对于接收到的需要修改内容的TCP数据报文根据其业务类型可直接进行修改，对于不需要修改内容的TCP数据报文则由TCP代理更改其头部信息后直接进行转发，无需将所有报文发送到应用代理程序，再由应用代理程序发送到网络层。由此可见，本发明实施例所提供的TCP代理减少了操作系统资源的消耗以及减少报文在网络协议栈中的时间消耗，大幅度提高了代理效率，在网络中相对核心位置上使用效果更佳。

附图说明

[0016] 图1是本发明实施例中TCP代理装置的结构示意图；

[0017] 图2是本发明实施例中TCP代理方法的流程框图；

[0018] 图3是本发明实施例中TCP代理方法的工作流程图。

具体实施方式

[0019] 本发明提供一种TCP代理装置以及方法，该TCP代理通过模拟客户端与服务器建立连接，然后再模拟服务器与客户端建立连接，在TCP连接建立之后，TCP代理则负责对客户端与服务器通信的报文数据进行修改以及转发。以下以发送端为客户端，目的端为服务器为例对本发明做进一步的阐述。

[0020] 请参考图1，本发明提供了一种TCP代理装置，应用于发送端与目的端之间的网络设备上，该装置的基本硬件环境包括CPU、内存、非易失性存储器以及其他硬件。该TCP代理装置可以理解为CPU读取非易失性存储器中对应的计算机程序在内存中运行所形成的，从本质上说其是一个逻辑装置。在本实施方式中，该装置在逻辑层面上包括：数据获取模块、报文判断模块、内容处理模块以及头部处理模块，请参考图2，该装置在运行过程中执行如下处理流程：包括：

[0021] 步骤201，数据获取模块在接收到发送端发送的TCP数据报文后，获取所述TCP数据报文中携带的明文数据；

[0022] 步骤202，报文判断模块按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，如果是，转步骤203进行处理，如果否，则转步骤204进行处理；

[0023] 步骤203，内容处理模块对所述TCP数据报文的内容进行修改，并转步骤204进行处理；

[0024] 步骤204，头部处理模块对所述TCP数据报文的头部信息进行修改处理后转发至目的端。

[0025] TCP协议用来提供可靠的连接服务，在客户端与服务器建立TCP连接时，TCP代理模拟客户端与服务器建立连接，然后再模拟服务器与客户端建立连接。经过三次握手建立连接之后，TCP代理与两侧的TCP连接就建立了。接下来TCP代理则负责对客户端与服务器通信

的报文数据进行修改以及转发，类似一条连接。请参考图3，TCP代理的数据获取模块在接收到客户端发送的TCP报文后，若判断该TCP报文为TCP数据报文，则进一步获取所述TCP数据报文中携带的明文数据。

[0026] 在获取到该TCP数据报文的明文数据之后，报文判断模块按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，如果需要修改，则根据业务类型对该报文的内容进行修改，在修改完成后再转由头部处理模块对该TCP数据报文的头部信息进行修改，并将修改完成的报文根据其IP地址转发至指定的目的端；如果根据明文数据判断该TCP数据报文的内容不需要修改，则直接由头部处理模块对该TCP数据报文的头部信息进行修改，并将修改完成的报文根据其IP地址转发至指定的目的端。

[0027] 在本发明实施例中，TCP代理对于接收到的需要修改内容的TCP数据报文可根据其业务类型直接进行修改，对于不需要修改内容的TCP数据报文则由TCP代理更改其头部信息后直接进行转发，无需将所有报文发送到应用代理程序，再由应用程序发送到网络层。由此可见，本发明实施例所提供的TCP代理减少了操作系统资源的消耗以及减少报文在网络协议栈中的时间消耗，有效提高了代理效率。

[0028] 本发明优选地实施例中，该TCP代理装置还包括TCP协议模块，用于按照TCP协议对来自发送端的TCP协议报文进行处理。在接收到发送端发送的TCP报文后，若判断该TCP报文是TCP协议报文则由TCP协议模块根据TCP协议对其进行处理，并不转发至服务器。

[0029] 进一步地，本发明实施例提供的TCP代理还可完美兼容如SSL等上层安全协议。其中，该TCP代理装置还包括SSL解密模块，用于对SSL数据报文进行解密以获取报文的明文数据；以及SSL协议模块，用于按照SSL协议对SSL协议报文进行处理。

[0030] 具体地，在TCP连接建立后，数据获取模块接收的TCP报文有可能是进行加密的SSL报文(Secure Sockets Layer安全套接层协议层)。若接收到的报文为SSL报文时，则要进一步判断该SSL报文为SSL协议报文还是SSL数据报文，若该SSL报文为SSL协议报文，那么TCP代理按照SSL协议对SSL协议报文进行处理；若接收的SSL报文为SSL数据报文，那么则在实际的数据传输开始前，TCP代理分别模拟客户端与服务器对该SSL数据报文进行SSL握手、协商加密算法以及密钥交换等，以获取该报文的明文数据。通常在进行SSL握手过程中会产生一些协议报文，接收到该协议报文后仍按照协议对该报文直接处理，并不转发给服务器。

[0031] 对接收到的SSL报文解密得到明文数据后，按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改，若明文数据的会话状态与报文特征符合所述预设分类规则，判断所述报文的明文内容需要修改，则对该报文的数据内容进行修改，再由头部处理模块对其头部信息进行修改处理后转发至指定的目的端。在修改报文内容时，根据明文数据可以得知该报文是何种业务类型，并根据该业务类型对该报文的内容进行修改。

[0032] 示例性地，比如用户在访问公网时后台服务器出现短暂故障，用户的网页信息通常显示为“错误提示:403”等，然而为了增加页面显示的友好度，则需要针对这种HTTP403错误进行相应的处理，具体来说可以将用户访问的网页信息设置为“正在加载…”等友好信息，TCP代理根据该业务需要对接收到的TCP数据报文的内容进行修改；此时HTTP403错误就是一个预定的分类规则。当然开发人员可以根据用户的实际需要定义各种分类规则，命中分类规则的都需要进行相应的内容修改，而分类规则本身是可以千变万化的。

[0033] 另一方面，若按照报文分类规则根据该明文数据的会话状态与报文特征判断该报

文的明文数据不需要修改，或者对需要修改明文数据的报文修改完成后，由头部处理模块对该TCP数据报文的头部信息进行修改，该TCP数据报文的头部信息为IP地址以及TCP序列号。由于TCP代理相当于一个中继设备，接收到的TCP数据报文都要转发至目的端，因此TCP代理在接收到所有TCP数据报文后均要将其头部中的IP地址修改为目的端的IP地址，且相应修改TCP序列号后再进行转发。

[0034] 进一步地，为了保护敏感数据在传送过程中的安全，可以在客户端和服务器之间构造安全通道来进行数据传输，以给数据通讯提供安全支持。因此TCP代理在将报文转发至目的端之前可以根据报文交互协议判断该报文是否符合加密规则，并对符合加密规则的报文进行加密后转发至目的端。

[0035] 具体地，本发明提供的TCP代理装置还包括数据加密模块，用于在将头部处理模块修改完成的TCP数据报文转发至目的端之前，判断该TCP数据报文是否符合预设加密规则，如果符合，对符合预设加密规则的报文进行加密后转发至目的端；否则将头部处理模块修改完成的TCP数据报文转发至目的端。

[0036] 该预设加密规则可以根据需要人为设定，比如该预设加密规则可以是：当数据获取模块接收到发送端发送的TCP数据报文为加密的报文时，那么该TCP数据报文则为符合预设加密规则的报文，若数据获取模块接收到发送端发送的TCP数据报文为明文数据报文，那么该TCP数据报文则为不符合预设加密规则的报文；或者该预设加密规则是：根据承载该TCP数据报文的协议来判断该报文是否符合加密规则，例如为Https(Hypertext Transfer Protocol Secure安全超文本传输协议)协议的报文；又或者该预设加密规则可以为：在数据获取模块接收到发送端发送的TCP数据报文虽为明文报文，但是根据承载该TCP数据报文的协议判断该报文符合加密规则时，仍判断该报文为符合加密规则的报文。在判断TCP数据报文为符合预设加密规则的报文后，由数据加密模块对该TCP数据报文进行加密，并将加密后的TCP数据报文转发至目的端。

[0037] 现有技术中，由于socket代理是把自己当成两个终端分别与客户端与服务器进行交互，因此若在TCP传输中出现中断的情况，就要对该TCP数据报文进行重传以及延迟ACK。然而使用socket代理进行重传以及延迟ACK等都需要定时器辅助实现，而在本发明实施例中TCP代理则相当于是一个中继设备，正是基于中继设备的特点，TCP代理可根据报文实时交互情况通过报文进行触发重传，不需要定时器来维护，也就无需自己来控制报文重传与ACK等。

[0038] 具体地，头部处理模块将头部信息修改完成后的TCP数据报文发送至目的端时，保存TCP数据报文进行修改前与修改后的TCP序列号，建立并保存其对应关系表项，该表项用于在重传异常报文时，便于知道需要给目的端重传哪个报文，因此在TCP数据报文发送成功后，即可删除该TCP数据报文在表项中的对应关系。在目的端接收报文出现异常时，TCP代理则根据该异常报文修改后的TCP序列号在该对应关系表项中查找与其对应的修改前的TCP序列号，通知发送端重传TCP序列号为该修改前的TCP序列号的TCP数据报文，目的端在接收到TCP数据报文时相应地发送ACK报文，TCP代理在接收到ACK报文后就向发送端转发ACK报文，并在重传完成后删除该TCP数据报文的TCP序列号对应关系。

[0039]

头部信息修改前的TCP序列号	头部信息修改后的TCP序列号

AAAA	BBBB
XXXX	YYYY

[0040] 表1

[0041] 表1为TCP数据报文进行头部信息修改前与修改后的TCP序列号对应关系表项，该表项仅为进一步理解本发明而举例说明。示例性地，如表1所述，若TCP代理接收到发送端发送的TCP数据报文的TCP序列号为XXXX，该TCP数据报文在经过头部信息修改后的TCP序列号为YYYY，若TCP代理在转发过程中出现异常，那么根据该异常报文修改后的TCP序列号YYYY在表1中查找与其对应的修改前的TCP序列号XXXX，通知发送端重传TCP序列号为XXXX的TCP数据报文，TCP代理再次进行修改，将序列号修改为YYYY，然后发送给目的端。目的端在成功接收到TCP数据报文时相应地发送ACK报文，TCP代理在接收到ACK报文，确定该报文是针对TCP序列号为YYYY报文的确认，然后就向发送端发送ACK报文，对TCP序列号为XXXX的报文进行确认，这样一来一次完整的重传就完成了。在该次重传完成后删除该TCP数据报文的TCP序列号对应关系。由此可见，本发明不需要自己控制异常报文的重传与ACK，也无需定时器来进行维护，可有效提高异常报文重传的效率。

[0042] 综上所述，本发明提供的TCP代理对于接收到的协议报文可直接处理，对于数据报文则无需上送应用代理程序，对于部分需要修改内容的报文，根据其业务类型可直接进行修改后再转发至目的端，同样也无需发送到应用代理程序，再由应用代理程序发送到网络层。此外，在优选的方式中，本发明所提供的TCP代理还可以完美的兼容SSL等上层协议，且通过直接转发的形式将报文转发至目的端，不需要再经过复杂的网络协议栈，在多核CPU高并发条件的运行环境下，本发明的对整体代理效率提升的效果将越为明显。

[0043] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

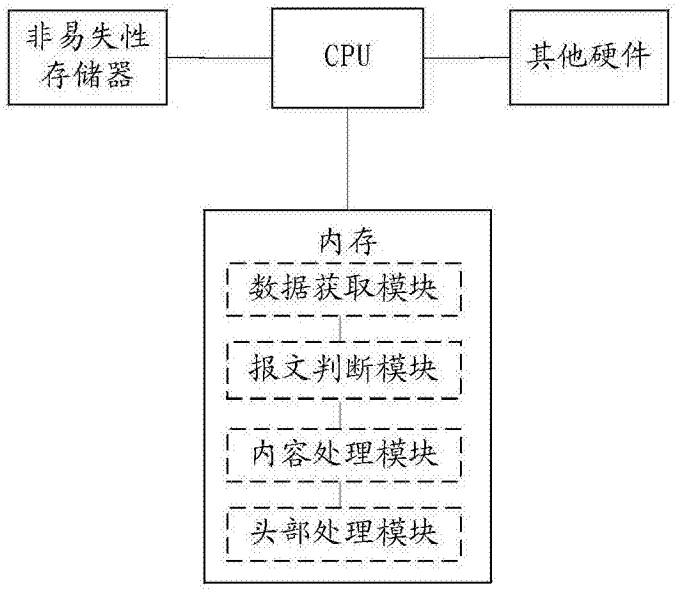

非易失性存储器
CPU
其他硬件
内存
数据获取模块
报文判断模块
内容处理模块
头部处理模块

图1

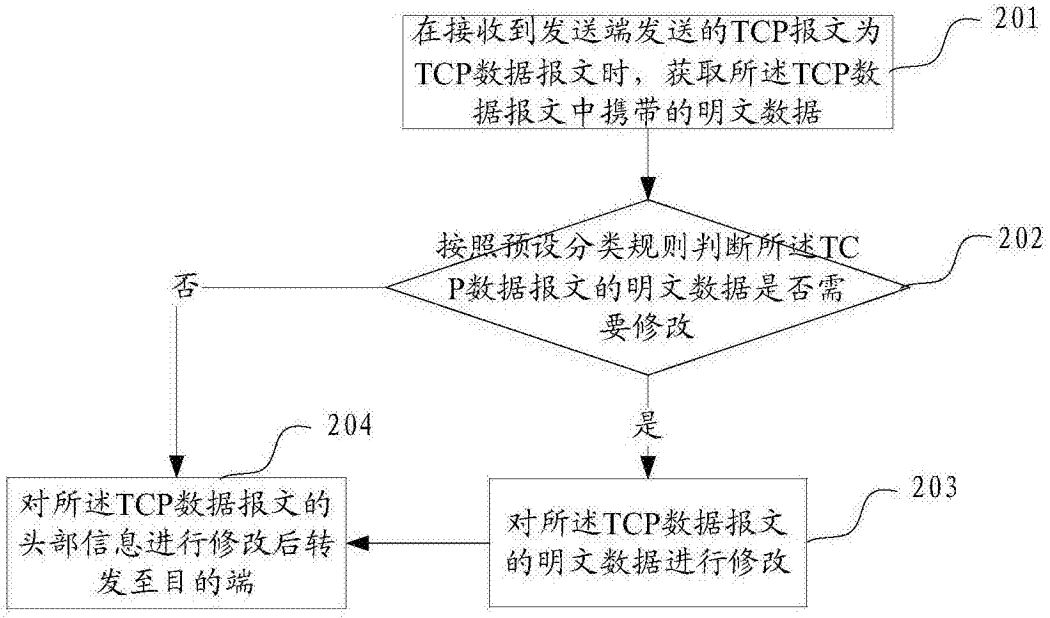

在接收到发送端发送的TCP报文为TCP数据报文时，获取所述TCP数据报文中携带的明文数据
201
按照预设分类规则判断所述TCP数据报文的明文数据是否需要修改
202
否
是
对所述TCP数据报文的头部信息进行修改后转发至目的端
204
对所述TCP数据报文的明文数据进行修改
203

图2

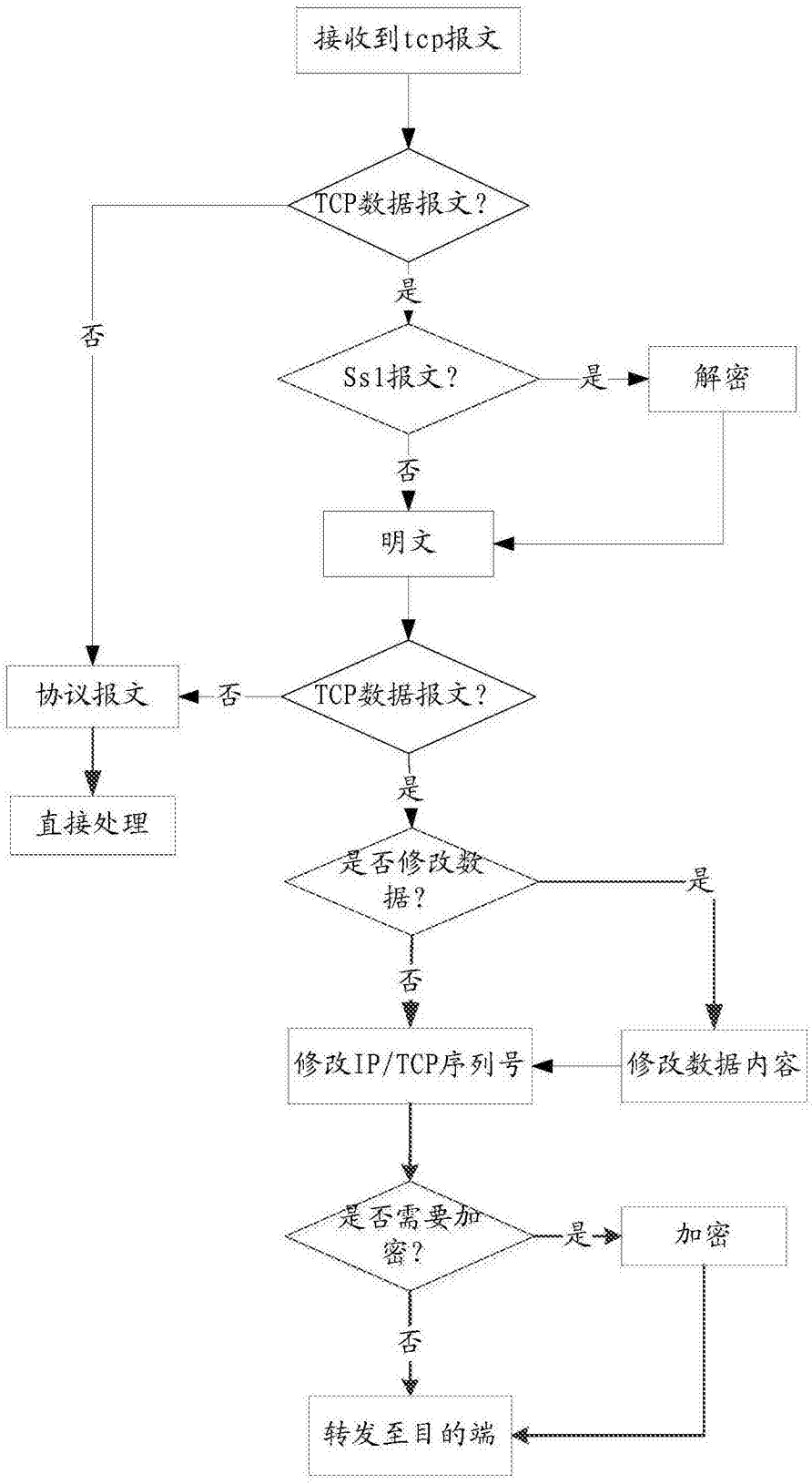

接收到tcp报文
TCP数据报文?
是
否
Ssl报文?
是
解密
否
明文
协议报文
否
TCP数据报文?
直接处理
是
是否修改数据?
是
否
修改IP/TCP序列号
修改数据内容
是否需要加密?
是
加密
否
转发至目的端

图3