(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 105407068 B
(45)授权公告日 2019.02.15

(21)申请号 201410307404.5

(22)申请日 2014.06.30

(65)同一申请的已公布的文献号
申请公布号 CN 105407068 A

(43)申请公布日 2016.03.16

(73)专利权人 优视科技有限公司
地址 100083 北京市海淀区成府路28号12层

(72)发明人 梁捷 何小鹏 杨伟

(74)专利代理机构 北京展翼知识产权代理事务所(特殊普通合伙) 11452
代理人 屠长存

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

(56)对比文件
CN 202679412 U,2013.01.16,
CN 101834875 A,2010.09.15,
CN 103179128 A,2013.06.26,
CN 103563335 A,2014.02.05,
CN 101141244 A,2008.03.12,
CN 101034981 A,2007.09.12,
US 2008046714 A1,2008.02.21,
CN 103139185 A,2013.06.05,

审查员 肖敬伟

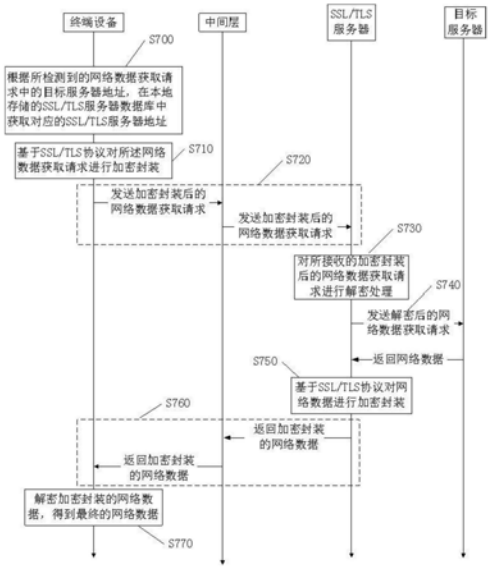
权利要求书3页 说明书10页 附图5页

(54)发明名称

网络数据获取方法、装置和系统

(57)摘要

本发明的网络数据获取方法、装置和系统，基于SSL/TLS协议对网络数据获取请求进行加密封装；之后经由中间层发送到SSL/TLS服务器，由SSL/TLS服务器解密处理后从目标服务器获取网络数据；然后将获取的网络数据基于SSL/TLS协议进行加密封装经由中间层返回给终端设备。本发明在终端设备与SSL/TLS服务器之间是通过密文的方式进行数据传输，而通过SSL/TLS服务器中转的方式获取网络数据，将能防止出现在访问不支持https协议的目标网站时的流量劫持现象。



CN 105407068 B

1.一种在终端设备侧执行的网络数据获取方法,包括:

根据所检测到的网络数据获取请求中的目标服务器地址,在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址,其中,所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表;

在获取到对应的SSL/TLS服务器地址后,基于SSL/TLS协议对所述网络数据获取请求进行加密封装;

将所述加密封装后的网络数据获取请求经由中间层发送到与SSL/TLS服务器地址对应的SSL/TLS服务器,以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数据;

依次经由所述SSL/TLS服务器和所述中间层,接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据。

2.如权利要求1所述的网络数据获取方法,其中,所述本地存储的SSL/TLS服务器数据库利用外部数据下发平台向所述终端设备下发的目标服务器地址与SSL/TLS服务器地址的对应关系表进行更新。

3.如权利要求2所述的网络数据获取方法,其中,所述目标服务器地址与SSL/TLS服务器地址的对应关系表由所述外部数据下发平台根据预先统计的网络数据获取请求劫持信息确定的。

4.如权利要求2所述的网络数据获取方法,其中,所述外部数据下发平台采用广播方式向所述终端设备下发所述目标服务器地址与SSL/TLS服务器地址的对应关系表。

5.如权利要求1所述的网络数据获取方法,其中,SSL/TLS服务器地址包括SSL/TLS服务器的IP地址或者SSL/TLS服务器的域名地址。

6.如权利要求5所述的网络数据获取方法,其中,当SSL/TLS服务器地址是SSL/TLS服务器的域名地址时,与终端设备进行数据传输的SSL/TLS服务器是根据终端设备的当前网络状态确定的。

7.一种网络数据获取方法,包括:

在终端设备侧,

根据所检测到的网络数据获取请求中的目标服务器地址,在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址,其中,所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表;

在获取到对应的SSL/TLS服务器地址后,基于SSL/TLS协议对所述网络数据获取请求进行加密封装;

将所述加密封装后的网络数据获取请求经由中间层发送到与SSL/TLS服务器地址对应的SSL/TLS服务器,以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数据;

依次经由所述SSL/TLS服务器和所述中间层,接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据;

以及

在SSL/TLS服务器侧,

对所接收的加密封装后的网络数据获取请求进行解密处理;

基于所述解密后的网络数据获取请求,从对应的目标服务器获取网络数据;

将所获取的网络数据基于SSL/TLS协议进行加密封装处理后,发送至终端设备。

8.一种设置于终端设备的网络数据获取装置,包括:

SSL/TLS服务器地址获取单元,用于根据所检测到的网络数据获取请求中的目标服务器地址,在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址,其中,所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表;

请求加密单元,用于在SSL/TLS服务器地址获取单元获取到对应的SSL/TLS服务器地址后,基于SSL/TLS协议对所述网络数据获取请求进行加密封装;

请求发送单元,用于将所述加密封装后的网络数据获取请求经由中间层发送到与SSL/TLS服务器地址对应的SSL/TLS服务器,以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数据;

网络数据接收单元,用于依次经由所述SSL/TLS服务器和所述中间层,接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据。

9.如权利要求8所述的网络数据获取装置,还包括,

数据更新单元,用于利用外部数据下发平台向所述终端设备下发的目标服务器地址与SSL/TLS服务器地址的对应关系表更新本地存储的SSL/TLS服务器数据库。

10.如权利要求8所述的网络数据获取装置,所述网络数据获取装置设置在终端设备。

11.一种网络数据获取装置,包括:设置于终端设备的SSL/TLS服务器地址获取单元、请求加密单元、请求发送单元、网络数据接收单元和设置于SSL/TLS服务器的解密单元、网络数据获取单元、网络数据加密单元和网络数据发送单元,

所述SSL/TLS服务器地址获取单元,用于根据所检测到的网络数据获取请求中的目标服务器地址,在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址,其中,所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表;

所述请求加密单元,用于在SSL/TLS服务器地址获取单元获取到对应的SSL/TLS服务器地址后,基于SSL/TLS协议对所述网络数据获取请求进行加密封装;

所述请求发送单元,用于将所述加密封装后的网络数据获取请求经由中间层发送到与SSL/TLS服务器地址对应的SSL/TLS服务器,以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数据;

所述网络数据接收单元,用于依次经由所述SSL/TLS服务器和所述中间层,接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据;

所述解密单元,用于对经由所述中间层从所述终端设备接收的加密封装后的网络数据获取请求进行解密处理;

所述网络数据获取单元,用于基于所述解密后的网络数据获取请求,从对应的目标服务器获取网络数据;所述网络数据加密单元,将所获取的网络数据基于SSL/TLS协议进行加密封装处理;

所述网络数据发送单元,用于将加密封装处理后的所述网络数据发送发送至终端设备。

12.一种网络数据获取系统,包括:终端设备、中间层和SSL/TLS服务器,

所述终端设备,包括如权利要求8或9所述的网络数据获取装置;

所述SSL/TLS服务器,包括:

解密单元，用于对经由所述中间层从所述终端设备接收的加密封装后的网络数据获取请求进行解密处理；

网络数据获取单元，用于基于所述解密后的网络数据获取请求，从对应的目标服务器获取网络数据；

网络数据加密单元，将所获取的网络数据基于SSL/TLS协议进行加密封装处理；

网络数据发送单元，用于将加密封装处理后的所述网络数据经由所述中间层发送至终端设备。

13.如权利要求12所述的网络数据获取系统，还包括，外部数据下发平台；

所述外部数据下发平台，包括：

数据下发单元，用于向所述终端设备下发的目标服务器地址与SSL/TLS服务器地址的对应关系表；

数据统计单元，用于根据预先统计的网络数据获取请求劫持信息确定目标服务器地址与SSL/TLS服务器地址的对应关系表。

网络数据获取方法、装置和系统

技术领域

[0001] 本发明涉及移动通信技术领域，更为具体地，涉及网络数据获取方法、装置和系统。

背景技术

[0002] 目前网络传输的主流传输方式为http。而基于http协议进行网络传输的过程是是明文传输的，流量在途中可随心所欲的被控制。传统程序事先已下至本地，运行时只有通信流量；而在线使用的WebApp，流量里既有通信数据，又有程序的界面和代码，劫持简直轻而易举。所以在互联网及移动互联网不少的流量劫持。

[0003] 图1示出了正常访问目标网站的流程图。如图1所示，用户请求访问目标网站时，首先终端设备与目标网站建立基于http协议的连接，然后经由中间层向目标网站发送网络请求。目标网站根据接收的网络请求将所请求的网络数据经由中间层发送至终端设备。

[0004] 图2示出了访问目标网站遭劫持的流程图。如图2所示，用户请求访问目标网站时，首先终端设备与目标网站建立基于http协议的连接，然后经由中间层向目标网站发送网络请求，网络运营商或黑客在中间层使用流量旁路分析系统或网络嗅探系统，截获用户请求内容，然后跳转到伪造的网站地址中，或者将用户请求的网络数据抢先应答给终端设备。访问目标网站遭劫持会导致伪造的网站进行钓鱼式攻击或者植入频繁的非法广告弹窗或者向http的缓存投毒和非法恶意嗅探账号系统等。如果将用户请求的网络数据抢先应答给终端设备会导致终端设备获得的错误数据或者是非正版数据。中间层泛指除用户端及目标网站之间经过的所有网络节点，包括但不限于如用户的家用路由器、各级网络运营商的服务器、网络设备等。

[0005] 现有技术使用了SSL/TLS加密的数据进行网络传输很难以破解，更容易被修改。从实际情况来看SSL/TLS可以很好的解决流量劫持问题。但目前国内部署https的网站数量还是非常少。所以在访问不支持https协议的网站存在被运营商或者黑客劫持的现象。

发明内容

[0006] 鉴于上述问题，本发明的目的是提供一种网络数据获取方法、装置及系统，能解决访问不支持https协议的目标网站的流量劫持问题。

[0007] 根据本发明的一个方面，提供一种在终端设备侧执行的网络数据获取方法，包括：

[0008] 根据所检测到的网络数据获取请求中的目标服务器地址，在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址，其中，所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表；

[0009] 在获取到对应的SSL/TLS服务器地址后，基于SSL/TLS协议对所述网络数据获取请求进行加密封装；

[0010] 将所述加密封装后的网络数据获取请求经由中间层发送到与SSL/TLS服务器地址对应的SSL/TLS服务器，以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数

据；

[0011] 依次经由所述SSL/TLS服务器和所述中间层，接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据。

[0012] 其中，所述本地存储的SSL/TLS服务器数据库利用外部数据下发平台向所述终端设备下发的目标服务器地址与SSL/TLS服务器地址的对应关系表进行更新。

[0013] 其中，所述目标服务器地址与SSL/TLS服务器地址的对应关系表由所述外部数据下发平台根据预先统计的网络数据获取请求劫持信息确定的。

[0014] 其中，所述外部数据下发平台采用广播方式向所述终端设备下发所述目标服务器地址与SSL/TLS服务器地址的对应关系表。

[0015] 其中，SSL/TLS服务器地址包括SSL/TLS服务器的IP地址或者SSL/TLS服务器的域名地址。

[0016] 其中，当SSL/TLS服务器地址是SSL/TLS服务器的域名地址时，与终端设备进行数据传输的SSL/TLS服务器是根据终端设备的当前网络状态确定的。

[0017] 另一优选的本发明一种网络数据获取方法，包括：

[0018] 在终端设备侧，

[0019] 根据所检测到的网络数据获取请求中的目标服务器地址，在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址，其中，所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表；

[0020] 在获取到对应的SSL/TLS服务器地址后，基于SSL/TLS协议对所述网络数据获取请求进行加密封装；

[0021] 将所述加密封装后的网络数据获取请求发送到与SSL/TLS服务器地址对应的SSL/TLS服务器，以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数据；

[0022] 依次经由所述SSL/TLS服务器和所述中间层，接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据。

[0023] 以及

[0024] 在SSL/TLS服务器侧，

[0025] 对所接收的加密封装后的网络数据获取请求进行解密处理；

[0026] 基于所述解密后的网络数据获取请求，从对应的目标服务器获取网络数据；

[0027] 将所获取的网络数据进行基于SSL/TLS协议进行加密封装处理后，发送至终端设备。

[0028] 另一方面，本发明还提供一种网络数据获取装置，包括：

[0029] SSL/TLS服务器地址获取单元，用于根据所检测到的网络数据获取请求中的目标服务器地址，在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址，其中，所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表；

[0030] 请求加密单元，用于在SSL/TLS服务器地址获取单元获取到对应的SSL/TLS服务器地址后，基于SSL/TLS协议对所述网络数据获取请求进行加密封装；

[0031] 请求发送单元，用于将所述加密封装后的网络数据获取请求发送到与SSL/TLS服务器地址对应的SSL/TLS服务器，以供所述SSL/TLS服务器解密处理后从所述目标服务器获

取网络数据；

[0032] 网络数据接收单元，用于依次经由所述SSL/TLS服务器和所述中间层，接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据网络数据。

[0033] 其中，还包括，数据更新单元，用于利用外部数据下发平台向所述终端设备下发的目标服务器地址与SSL/TLS服务器地址的对应关系表跟新本地存储的SSL/TLS服务器数据库。

[0034] 优选的所述网络数据获取装置，所述网络数据获取装置设置在终端设备。

[0035] 另一方面，本发明还提供一种网络数据获取装置，包括：设置于终端设备的SSL/TLS服务器地址获取单元、请求加密单元、请求发送单元、网络数据接收单元和设置于SSL/TLS服务器的解密单元、网络数据获取单元、网络数据加密单元，

[0036] 所述SSL/TLS服务器地址获取单元，用于根据所检测到的网络数据获取请求中的目标服务器地址，在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址，其中，所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表；

[0037] 所述请求加密单元，用于在SSL/TLS服务器地址获取单元获取到对应的SSL/TLS服务器地址后，基于SSL/TLS协议对所述网络数据获取请求进行加密封装；

[0038] 所述请求发送单元，用于将所述加密封装后的网络数据获取请求发送到与SSL/TLS服务器地址对应的SSL/TLS服务器，以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数据；

[0039] 所述网络数据接收单元，用于依次经由所述SSL/TLS服务器和所述中间层，接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据网络数据。

[0040] 所述解密单元，用于对经由所述中间层从所述终端设备接收的加密封装后的网络数据获取请求进行解密处理；

[0041] 所述网络数据获取单元，用于基于所述解密后的网络数据获取请求，从对应的目标服务器获取网络数据；

[0042] 所述网络数据发送单元，将所获取的网络数据进行基于SSL/TLS协议进行加密封装处理后，发送至终端设备。

[0043] 另一方面，本发明还提供一种网络数据获取系统，包括：终端设备、中间层和SSL/TLS服务器，

[0044] 所述终端设备，包括前面所述的SSL/TLS服务器地址获取单元、请求加密单元、请求发送单元、网络数据接收单元和设置于SSL/TLS服务器的解密单元、网络数据获取单元、网络数据加密单元和或数据更新单元，用于利用外部数据下发平台向所述终端设备下发的目标服务器地址与SSL/TLS服务器地址的对应关系表跟新本地存储的SSL/TLS服务器数据库；

[0045] 所述SSL/TLS服务器，包括：

[0046] 解密单元，用于对经由所述中间层从所述终端设备接收的加密封装后的网络数据获取请求进行解密处理；

[0047] 网络数据获取单元，用于基于所述解密后的网络数据获取请求，从对应的目标服务器获取网络数据；

[0048] 网络数据加密单元，将所获取的网络数据进行基于SSL/TLS协议进行加密封装处理后经由所述中间层发送至终端设备。

[0049] 其中，还包括，外部数据下发平台；所述外部数据下发平台，包括：

[0050] 数据下发单元，用于向所述终端设备下发的目标服务器地址与SSL/TLS服务器地址的对应关系表；

[0051] 数据统计单元，用于根据预先统计的网络数据获取请求劫持信息确定目标服务器地址与SSL/TLS服务器地址的对应关系表。

[0052] 本发明的网络数据获取方法、装置和系统，基于SSL/TLS协议对网络数据获取请求进行加密封装；之后经由中间层发送到SSL/TLS服务器，由SSL/TLS服务器解密处理后从目标服务器获取网络数据；然后将获取的网络数据基于SSL/TLS协议进行加密封装经由中间层返回给终端设备。本发明在终端设备与SSL/TLS服务器之间是通过密文的方式进行数据传输，而通过SSL/TLS服务器中转的方式获取网络数据，将能防止出现在访问不支持https协议的目标网站时的流量劫持现象。

[0053] 为了实现上述以及相关目的，本发明的一个或多个方面包括后面将详细说明并在权利要求中特别指出的特征。下面的说明以及附图详细说明了本发明的某些示例性方面。然而，这些方面指示的仅仅是可使用本发明的原理的各种方式中的一些方式。此外，本发明旨在包括所有这些方面以及它们的等同物。

附图说明

[0054] 通过参考以下结合附图的说明及权利要求书的内容，并且随着对本发明的更全面理解，本发明的其它目的及结果将更加明白及易于理解。在附图中：

[0055] 图1示出了正常访问目标网站的流程图；

[0056] 图2示出了访问目标网站遭劫持的流程图；

[0057] 图3示出了根据本发明的实施例的网络数据获取系统的结构图；

[0058] 图4示出了网络数据获取系统10的实例图；

[0059] 图5示出了根据本发明的实施例的网络数据获取装置300的一个示例的框图；

[0060] 图6示出了根据本发明的网络数据获取系统10的SSL/TLS服务器40的一个示例的框图；

[0061] 图7示出了根据本发明的实施例的网络数据获取方法流程图；

[0062] 图8示出了根据本发明的另一实施例的网络数据获取系统的结构图；

[0063] 图9为图8的网络数据获取系统20的示例图；

[0064] 图10示出了外部数据下发平台的装置方框图。

[0065] 在所有附图中相同的标号指示相似或相应的特征或功能。

具体实施方式

[0066] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整的描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于

本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0067] 本发明提供的一种网络数据获取方法、装置及系统，通过在存在流量劫持区域使用加密的数据传输，防止出现在访问不支持https协议的目标网站时的流量劫持问题。

[0068] 图3示出了根据本发明的实施例的网络数据获取系统的结构图。

[0069] 如3所示的网络数据获取系统10，包括终端设备30、SSL/TLS服务器40和中间层50。所述终端设备包括网络数据获取装置300。

[0070] 图4示出了网络数据获取系统10的实例图。

[0071] 图5示出了根据本发明的实施例的网络数据获取装置300的一个示例的框图。

[0072] 如图5所示，网络数据获取装置300包括：SSL/TLS服务器地址获取单元301、请求加密单元302、请求发送单元303、网络数据接收单元304。

[0073] SSL/TLS服务器地址获取单元301，用于根据所检测到的网络数据获取请求中的目标服务器地址，在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址，其中，所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表。网络数据获取请求包括获取网页数据的请求或者获取网络其它数据的请求，例如获取某个软件安装包的请求。

[0074] 目标服务器可以为用户请求访问的某个网页的服务器，也可能是用户请求获取某个数据时的服务器。例如获取某个软件安装包时，目标服务器就是提供该软件下载的服务器。

[0075] 请求加密单元302，用于在SSL/TLS服务器地址获取单元301获取到对应的SSL/TLS服务器地址后，基于SSL/TLS协议对所述网络数据获取请求进行加密封装。

[0076] 请求发送单元303，用于将所述加密封装后的网络数据获取请求发送到与SSL/TLS服务器地址对应的SSL/TLS服务器，以供所述SSL/TLS服务器解密处理后从所述目标服务器获取网络数据。

[0077] 请求发送单元303将加密封装后的网络数据获取请求发送到与SSL/TLS服务器地址对应的SSL/TLS服务器40之前，终端设备30的网络建立模块(图中未示出)与SSL/TLS服务器需要根据网络数据获取请求建立基于SSL/TLS协议的网络连接，在建立网络连接时，当SSL/TLS服务器地址为IP地址时，则直接与该IP地址对应的SSL/TLS服务器建立网络连接。当SSL/TLS服务器地址为SSL/TLS服务器的域名时，首先经过域名解析服务器对域名进行解析，解析出来的SSL/TLS服务器的IP地址可能有多个。在优选的实施例中是根据当前网络状态来选择终端设备进行数据传输的SSL/TLS服务器，域名解析服务器将该SSL/TLS服务器的IP地址返回给终端设备，终端设备与该IP地址对应的SSL/TLS服务器进行数据传输。在优选实施例中，域名解析服务器还通过CDN技术选择SSL/TLS服务器的IP地址返回给终端设备。

[0078] 当SSL/TLS服务器地址为SSL/TLS服务器的域名时，根据当前终端设备网络状态按照通过CDN技术选择SSL/TLS服务器，选择出最优的SSL/TLS服务器集群及网络线路使得网络数据传输速率更快。提高网络数据传输效率。

[0079] 网络数据接收单元304，用于依次经由所述SSL/TLS服务器40和所述中间层50，接收从目标服务器返回的由所述SSL/TLS服务器基于SSL/TLS协议进行加密封装处理后的网络数据。

[0080] 图6示出了根据本发明的网络数据获取系统10的SSL/TLS服务器40的一个示例的框图。

[0081] 如图6所示所述SSL/TLS服务器40包括解密单元401、网络数据获取单元402、网络数据加密单元403和网络数据发送单元404。

[0082] 解密单元401，用于对经由所述中间层从所述终端设备接收的加密封装后的网络数据获取请求进行解密处理。进行解密处理后的网络数据获取请求即相当于http协议的网络数据请求，SSL/TLS服务器与目标服务器之间通过http协议传输数据，SSL/TLS服务器与目标服务器之间是通过明文进行数据传输的。由于解密后的的网络数据请求是基于http协议的，所以这里获取网络数据的方式与普通的基于http协议获取网络数据的方式相同，这里不再赘述。

[0083] 网络数据获取单元402，用于基于所述解密后的网络数据获取请求，从对应的目标服务器获取网络数据。

[0084] 在优选的实施例中，还包括网络数据加密单元403，用于将所获取的网络数据进行基于SSL/TLS协议进行加密封装处理。由于之前终端设备与SSL/TLS服务器之间建立的网络是SSL/TLS协议的。所以返回的网络数据必须是通过SSL/TLS协议进行加密封装后的网络数据。

[0085] 网络数据发送单元404，用于将网络数据加密单元403进行加密封装处理后的网络数据经由中间层50，发送至终端设备30的网络数据接收单元304。

[0086] 图7示出了根据本发明的实施例的网络数据获取方法流程图。

[0087] 如图7所示，接收用户输入的网络数据获取请求后，执行步骤S700，终端设备根据所检测到的网络数据获取请求中的目标服务器地址，在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址。其中，所述SSL/TLS服务器数据库中存储有目标服务器地址与SSL/TLS服务器地址之间的对应关系表。

[0088] 网络数据获取请求包括获取网页数据的请求或者获取网络其它数据的请求，例如获取某个软件安装包的请求。

[0089] 目标服务器可以为用户请求访问的某个网页的服务器，也可能是用户请求获取某个数据时的服务器。例如获取某个软件安装包时，目标服务器就是提供该软件下载的服务器。

[0090] 本步骤中SSL/TLS服务器地址包括SSL/TLS服务器的IP地址或者SSL/TLS服务器的域名地址。

[0091] 当SSL/TLS服务器地址是SSL/TLS服务器的域名地址时，还需要通过域名解析服务器对该域名进行解析，获取SSL/TLS服务器的IP地址。

[0092] 在获取到对应的SSL/TLS服务器地址后，执行步骤S710，终端设备基于SSL/TLS协议对所述网络数据获取请求进行加密封装。本步骤就相当于原来为http协议的网络数据获取请求通过SSL/TLS协议进行加密封装后转换成基于https协议的请求网络数据获取请求，但是由于目标服务器不支持https，所以需要设置SSL/TLS服务器对https进行解密以得到http协议的网络数据获取请求。原来http协议的直接由终端设备直接与目标服务器连接获取网络数据获取方式转换成由SSL/TLS服务器中转的方式获取网络数据。即在网络数据获取请求中加入SSL/TLS服务器的地址来实现SSL/TLS服务器中转的方式获取网络数据。

[0093] 完成S710后，执行S720，终端设备经由中间层将所述加密封装后的网络数据获取请求发送到与SSL/TLS服务器地址对应的SSL/TLS服务器。

[0094] 在执行步骤S720之前，终端设备与SSL/TLS服务器之间需要根据网络数据获取请求建立基于SSL/TLS协议的网络连接。在建立网络连接时，当SSL/TLS服务器地址为IP地址时，则直接与该IP地址对应的SSL/TLS服务器建立网络连接。当SSL/TLS服务器地址为SSL/TLS服务器的域名时，首先要经过域名解析服务器对域名进行解析，解析出来的SSL/TLS服务器的IP地址可能有多个。在优选的实施例中是根据当前网络状态来选择终端设备进行数据传输的SSL/TLS服务器，域名解析服务器将该SSL/TLS服务器的IP地址返回给终端设备，终端设备与该IP地址对应的SSL/TLS服务器进行数据传输。在优选实施例中，域名解析服务器还通过CDN技术选择SSL/TLS服务器的IP地址返回给终端设备。

[0095] 当SSL/TLS服务器地址为SSL/TLS服务器的域名时，根据当前终端设备网络状态按照通过CDN技术选择SSL/TLS服务器，能够选择出最优的SSL/TLS服务器集群及网络线路使得网络数据传输速率更快。提高网络数据传输效率。

[0096] SSL/TLS服务器接收到加密封装后的网络数据获取请求后，执行S730，SSL/TLS服务器对所接收的加密封装后的网络数据获取请求进行解密处理。进行解密处理后的网络数据获取请求即相当于http协议的网络数据请求，SSL/TLS服务器与目标服务器之间通过http协议传输数据，SSL/TLS服务器与目标服务器之间是通过明文进行数据传输的。

[0097] 完成S730后，执行S740，SSL/TLS服务器发送解密后的网络数据获取请求至目标服务器。由于解密后的的网络数据请求是基于http协议的，所以这里获取网络数据的方式与普通的基于http协议获取网络数据的方式相同，不再赘述。

[0098] 目标服务器接收到网络数据获取请求后，返回网络数据给SSL/TLS服务器。SSL/TLS服务器基于SSL/TLS协议对网络数据进行加密封装(S750)。之后SSL/TLS服务器将加密封装的网络数据经由中间层返回给终端设备(S760)。由于之前终端设备与SSL/TLS服务器之间建立的网络是SSL/TLS协议的。所以返回的网络数据必须是通过SSL/TLS协议进行加密封装后的网络数据。

[0099] 终端设备收到加密封装后的网络数据后，执行S770，解密加密封装的网络数据，得到最终的网络数据。

[0100] 本实施例的网络数据获取方法，通过在终端设备对网络获取请求进行基于SSL/TLS协议的加密封装，然后由SSL/TLS服务器进行解密，之后基于解密后的网络获取请求去目标服务器获取网络数据，在获取到网络数据后，对网络数据进行基于SSL/TLS协议的加密封装后返回给终端设备，终端设备对加密封装后的网络数据进行解密得到最终的数据。本实施例在终端设备与SSL/TLS服务器之间是通过密文的方式进行数据传输，而通过SSL/TLS服务器中转的方式获取网络数据，将能防止出现在访问不支持https协议的目标网站时的流量劫持现象。

[0101] 本发明还提供网络数据获取装置在如图5所示的网络数据获取装置300的基础上增加了解密单元401、网络数据获取单元402、网络数据加密单元403和网络数据发送单元404。

[0102] 所述解密单元401、网络数据获取单元402、网络数据加密单元403和网络数据发送单元404与前一实施例的工作方式和作用相同，这里不再赘述。

[0103] 图8示出了根据本发明的另一实施例的网络数据获取系统的结构图。

[0104] 图9为图8的网络数据获取系统20的示例图。

[0105] 如图8所示的网络数据获取系统20在图3所示的网络数据获取系统10的基础上增加了外部数据下发平台60。

[0106] 图10示出了外部数据下发平台的装置方框图。

[0107] 如图10所示的外部数据下发平台60，包括：

[0108] 数据统计单元601，用于根据预先统计的网络数据获取请求劫持信息确定目标服务器地址与SSL/TLS服务器地址的对应关系表。

[0109] 其中SSL/TLS服务器地址包括SSL/TLS服务器的IP地址或者SSL/TLS服务器的域名地址。当SSL/TLS服务器地址是SSL/TLS服务器的域名地址时，还需要通过域名解析服务器对该域名进行解析，获取SSL/TLS服务器的IP地址。

[0110] 数据下发单元602，用于向所述终端设备30下发的目标服务器地址与SSL/TLS服务器地址的对应关系表。外部数据下发平台60的数据统计单元601通过统计发现某些地区的用户存在流量被劫持的现象，就记录这些用户所在地区以及这些用户请求访问的目标服务器信息，目标服务器信息可能包含目标服务器的地址等信息，然后根据这些信息分配SSL/TLS服务器地址。然后生成目标服务器地址与SSL/TLS服务器地址的对应关系。

[0111] 由在优选实施例中所述外部数据下发平台60的数据下发单元602采用广播方式向所述终端设备30下发所述目标服务器地址与SSL/TLS服务器地址的对应关系表。

[0112] 优选实施例中终端设备30还包括数据更新单元(图中未示出)，用于利用外部数据下发平台60向所述终端设备30下发的目标服务器地址与SSL/TLS服务器地址的对应关系表跟新本地存储的SSL/TLS服务器数据库。

[0113] 如图7、图8所示的CD服务器即外部数据下发平台60与终端设备30连接。

[0114] 本实施例中所述目标服务器地址与SSL/TLS服务器地址的对应关系表由所述外部数据下发平台数据统计单元601根据预先统计的网络数据获取请求劫持信息确定的。且SSL/TLS服务器与终端设备之间的中间层是存在网络数据获取请求劫持风险的中间层，而SSL/TLS服务器去目标服务器获取网络数据时，SSL/TLS服务器与目标服务器之间也存在中间层。优选实施例中选择安全地区的SSL/TLS服务器进行网络数据获取，即选择不存在劫持风险的SSL/TLS服务器获取网络数据，使得SSL/TLS服务器与目标服务器之间的中间层网络是数据传输不存在劫持风险的中间层网络。即SSL/TLS服务器布局在未受污染的网络区域中。即在通过外部数据下发平台的统计的未受污染的网络区域中布局SSL/TLS服务器。

[0115] 外部数据下发平台60的数据统计单元601通过统计发现某些地区的用户存在流量被劫持的现象，就记录这些用户所在地区以及这些用户请求访问的目标服务器信息，目标服务器信息可能包含目标服务器的地址等信息，然后根据这些信息分配SSL/TLS服务器地址。之后生成目标服务器地址与SSL/TLS服务器地址的对应关系表。例如外部数据下发平台的数据统计单元通过统计发现广州用户访问新浪时存在被劫持的现象，就选择一个布局在武汉的SSL/TLS服务器集群作为SSL/TLS服务器，生成一条新浪网服务器地址与武汉的SSL/TLS服务器集群地址的对应关系表。具体可以是新浪域名与武汉的SSL/TLS服务器集群的域名对应关系表。

[0116] 之后外部数据下发平台60的数据下发单元602将目标服务器地址与SSL/TLS服务

器地址的对应关系表通过广播的形式发送至终端设备30。

[0117] 终端设备30本地存储的SSL/TLS服务器数据库利用外部数据下发平台使用广播的形式向所述终端设备30下发的目标服务器地址与SSL/TLS服务器地址的对应关系表进行更新。

[0118] 终端设备30接收用户输入的网络数据获取请求后，终端设备30的SSL/TLS服务器地址获取单元301根据网络数据获取请求中请求的目标服务器地址去目标服务器地址与SSL/TLS服务器地址的对应关系表查找SSL/TLS服务器地址，当在目标服务器地址与SSL/TLS服务器地址的对应关系表中能查询到对应的与SSL/TLS服务器地址时。则由请求加密单元302终端设备30的将普通的基于http协议的网络数据获取请求通过SSL/TLS协议进行加密封装。变成基于https协议的网络数据获取请求。然后由终端设备30的网络建立模块(图中未示出)在终端设备30与SSL/TLS服务器40之间建立基于https协议的网络连接。再由终端设备30的请求发送单元303将加密封装后的网络数据获取请求经由中间层50发送到与SSL/TLS服务器地址对应的SSL/TLS服务器40。SSL/TLS服务器40收到所述请求后，由解密单元401对其进行解密，之后网络数据获取单元402按照解密后的网络数据获取请求从所述目标服务器获取网络数据。

[0119] 收到目标服务器返回的网络数据后，SSL/TLS服务器40的网络数据加密单元403基于SSL/TLS协议对所述网络数据进行加密封装。然后网络数据发送单元404经由中间层50将所述加密封装后的网络数据返回给终端设备30。终端设备30对加密封装的网络数据进行解密得到最终的网络数据。

[0120] 本实施例的网络数据获取系统，通过在终端设备对网络获取请求进行基于SSL/TLS协议的加密封装，然后由SSL/TLS服务器进行解密，之后基于解密后的网络获取请求去目标服务器获取网络数据，在获取到网络数据后，对网络数据进行基于SSL/TLS协议的加密封装后返回给终端设备，终端设备对加密封装后的网络数据进行解密得到最终的数据。本实施例在终端设备与SSL/TLS服务器之间是通过密文的方式进行数据传输，而通过SSL/TLS服务器中转的方式获取网络数据，将能防止出现在访问不支持https协议的目标网站时的流量劫持现象。

[0121] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0122] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0123] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0124] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0125] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[0126] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)或处理器(processor)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0127] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

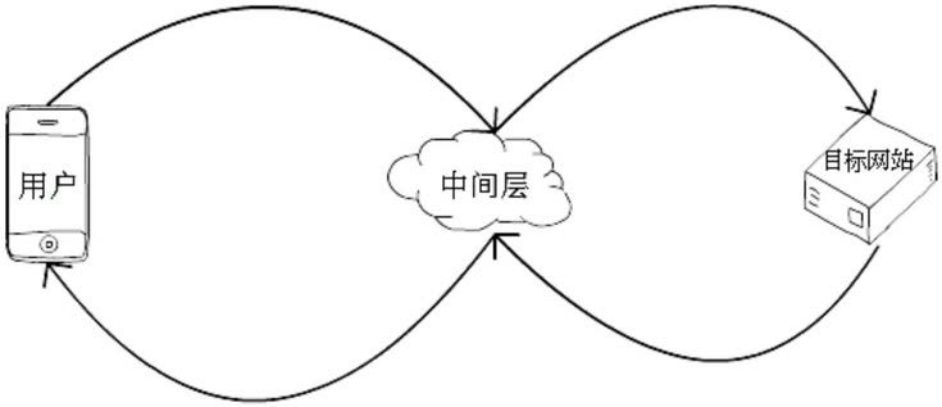

用户
中间层
目标网站

图1

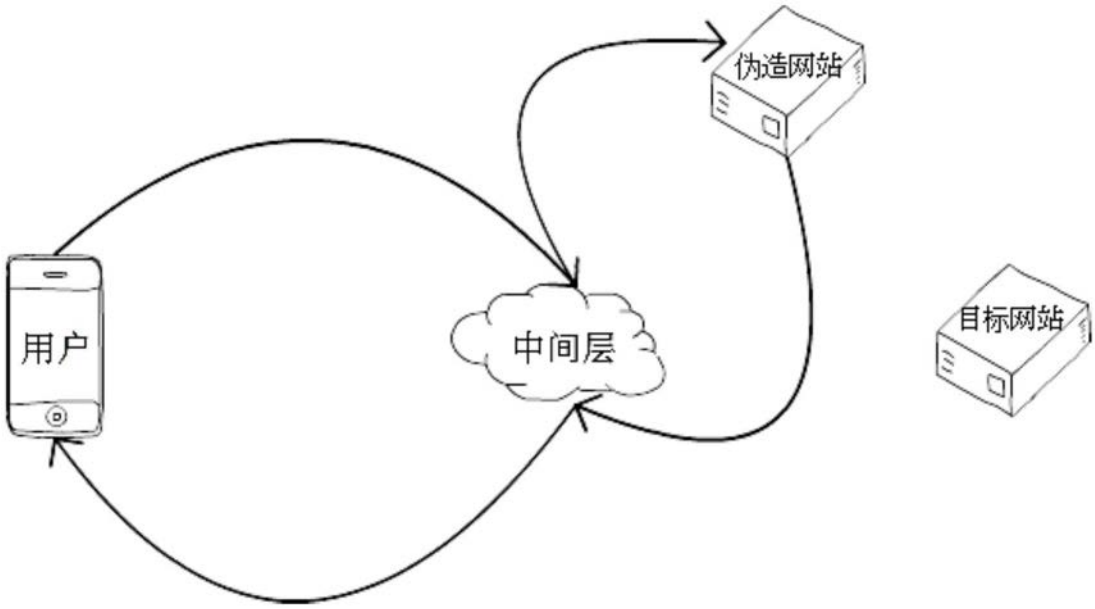

伪造网站
用户
中间层
目标网站

图2

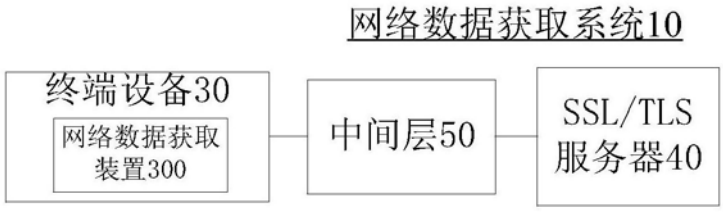

网络数据获取系统10
终端设备30
网络数据获取装置300
中间层50
SSL/TLS服务器40

图3

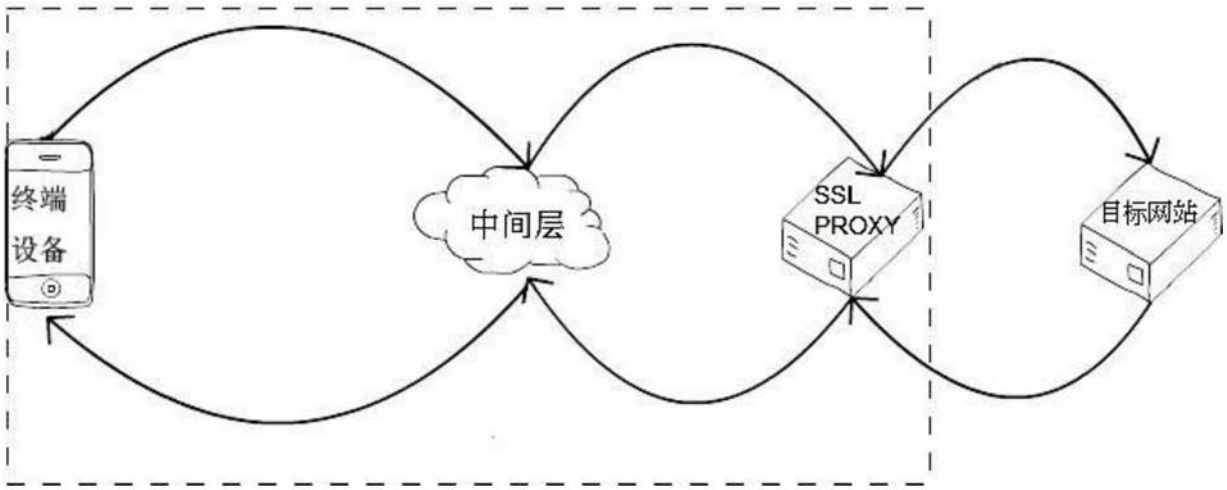

终端
设备
中间层
SSL
PROXY
目标网站

图4


网络数据获取装置
300
请求发送
单元303
请求加密
单元302
SSL/TLS服务器
地址获取单元301
网络数据接
收单元304

图5


SSL/TLS服务器40
解密单元401
网络数据获取单元402
网络数据加密单元403
网络数据发送单元404

图6

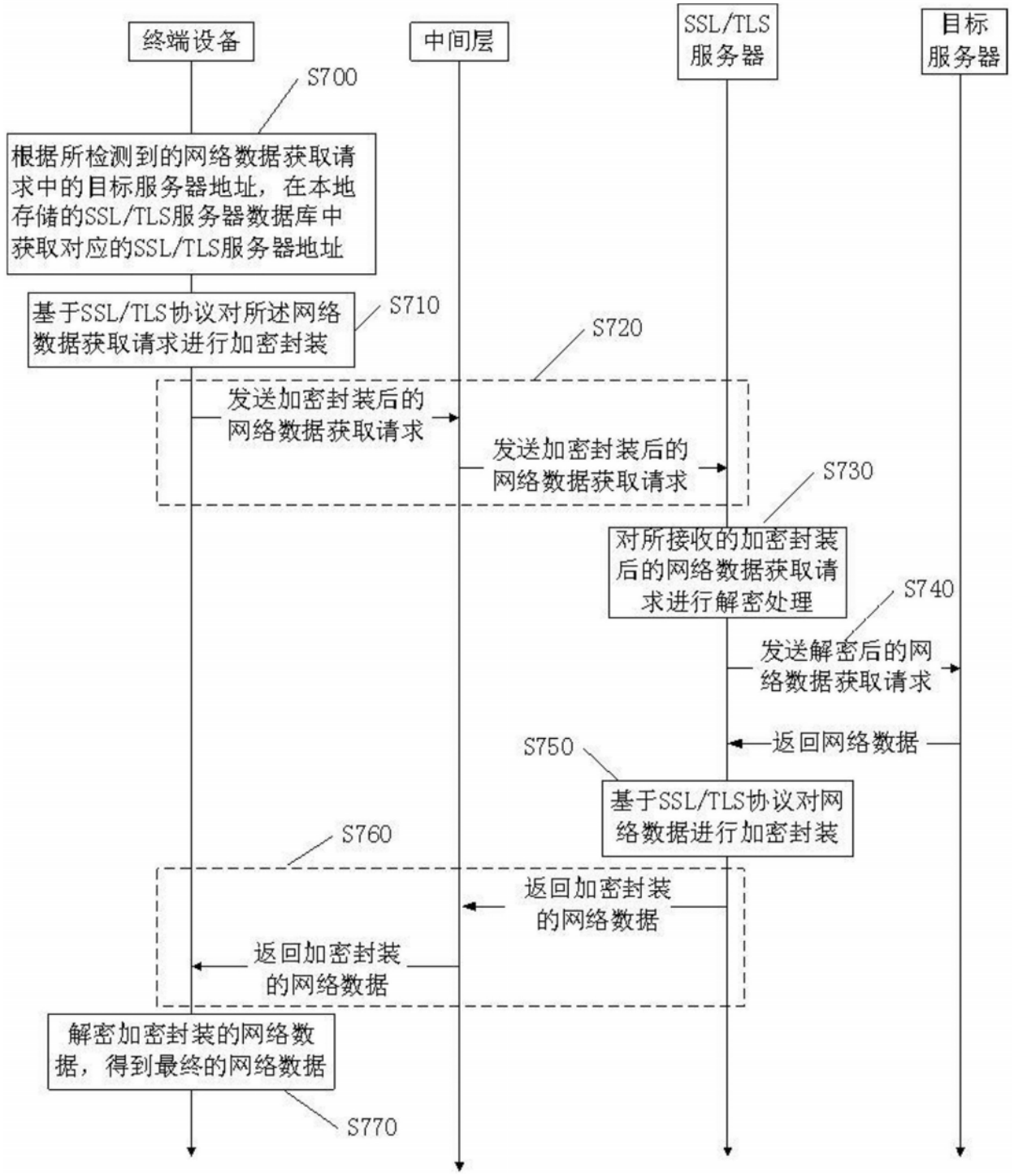

终端设备
中间层
SSL/TLS 服务器
目标 服务器
S700
根据所检测到的网络数据获取请求中的目标服务器地址，在本地存储的SSL/TLS服务器数据库中获取对应的SSL/TLS服务器地址
S710
基于SSL/TLS协议对所述网络数据获取请求进行加密封装
S720
发送加密封装后的网络数据获取请求
发送加密封装后的网络数据获取请求
S730
对所接收的加密封装后的网络数据获取请求进行解密处理
S740
发送解密后的网络数据获取请求
返回网络数据
S750
基于SSL/TLS协议对网络数据进行加密封装
S760
返回加密封装的网络数据
返回加密封装的网络数据
解密加密封装的网络数据，得到最终的网络数据
S770

图7

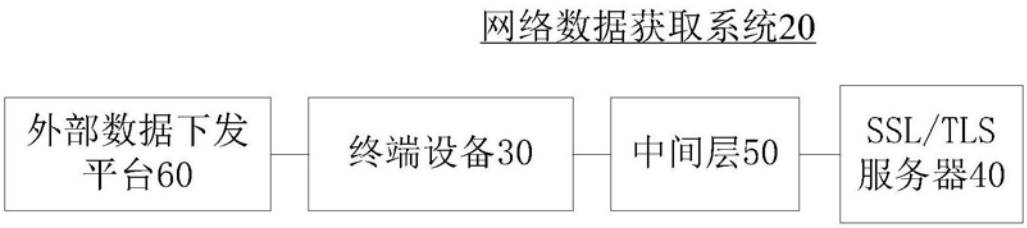

网络数据获取系统20
外部数据下发平台60
终端设备30
中间层50
SSL/TLS服务器40

图8

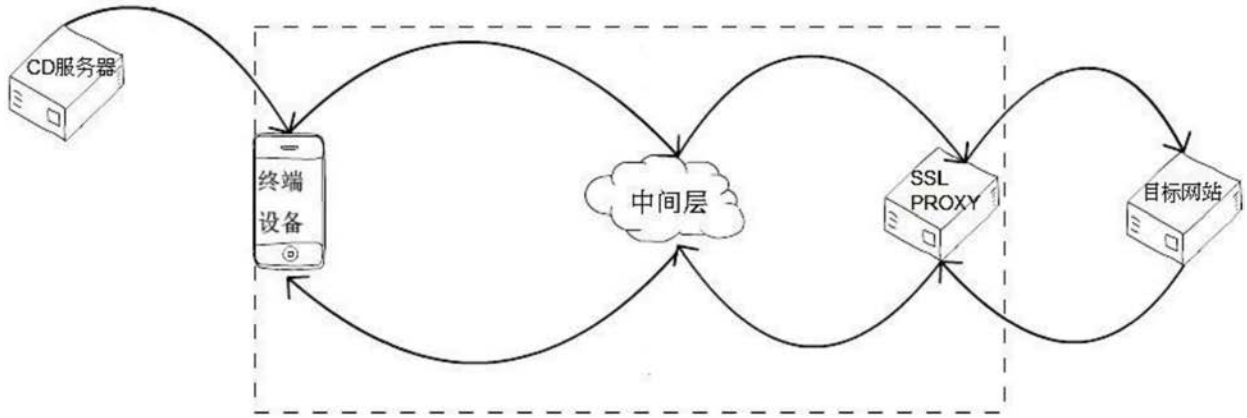

CD服务器
终端设备
中间层
SSL PROXY
目标网站

图9

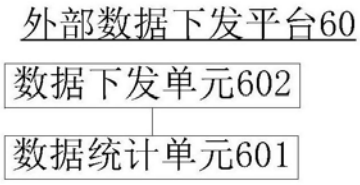

外部数据下发平台60
数据下发单元602
数据统计单元601

图10