

(12) 发明专利

(10) 授权公告号 CN 101635727 B

(45) 授权公告日 2013.04.24

(21) 申请号 200910168074.5

US 20070071029 A1, 2007.03.29, 全文.

(22) 申请日 2009.08.24

L. Martini et al.. Pseudowire Setup and Maintenance Using the Label Distribution Protocol(LDP).《RFC4447》.2006, 参见第1,3,5节.

(73) 专利权人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
基地总部办公楼

审查员 杨柳

(72) 发明人 裴龑

(74) 专利代理机构 北京三友知识产权代理有限
公司 11127

代理人 任默闻

(51) Int. Cl.

H04L 29/06 (2006.01)

(56) 对比文件

CN 1909448 A, 2007.02.07, 参见说明书第5
页第1行 - 第9页最后一行、说明书附图1-2.

CN 101262301 A, 2008.09.10, 全文.

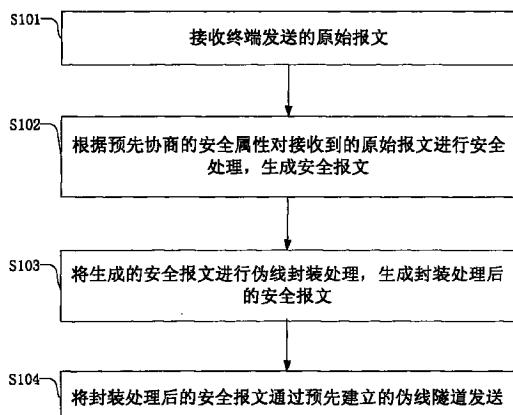
权利要求书3页 说明书7页 附图6页

(54) 发明名称

一种用于伪线网络的数据安全发送接收方
法、装置及系统

(57) 摘要

本发明是关于一种用于伪线网络的数据安全
发送接收方法、装置及系统。所述的数据安全发
送方法包括：接收终端发送的原始报文；根据预
先协商的安全属性对接收到的原始报文进行安
全处理，生成安全报文；将生成的安全报文进行
伪线封装处理，生成封装处理后的安全报文；将
封装处理后的安全报文通过预先建立的伪线隧
道发送。本发明克服了现有技术PW传输技术信息不
安全的问题，实现了在PW传输转发中的数据的安
全保护功能，解决在PW中传输数据进行安全保护处
理的技术空白，且不局限于IP/TCP报文，应用广
泛，可以对现有和以后可见的各种类型的报文进
行安全保护处理。



1. 一种用于伪线网络的数据安全发送方法,其特征在于,所述的方法包括:
接收终端发送的原始报文;

根据预先协商的安全属性对接收到的原始报文进行安全处理,生成安全报文;所述安全属性包括加解密属性、权限认证控制属性、时间限制属性以及防重放属性;所述安全处理包括:使用加密算法 MD5、SHA、3DES、AES 中的一种或多种对原始报文进行加密和鉴权处理;

将生成的安全报文进行伪线封装处理,生成封装处理后的安全报文;

将封装处理后的安全报文通过预先建立的伪线隧道发送;

在根据预先协商的安全属性对接收到的原始报文进行安全处理,生成安全报文前,所述的方法还包括通过协商建立所述的伪线隧道;

在通过协商建立伪线隧道时,通过协商得到所述的安全属性。

2. 如权利要求 1 所述的一种用于伪线网络的数据安全发送方法,其特征在于,所述的通过协商得到所述的安全属性包括:通过协商控制字字段,得到所述的安全属性。

3. 一种用于伪线网络的数据安全发送装置,其特征在于,所述的装置包括:

原始报文接收单元,用于接收终端发送的原始报文;

安全处理单元,用于根据预先协商的安全属性对接收到的原始报文进行安全处理,生成安全报文;所述安全属性包括加解密属性、权限认证控制属性、时间限制属性以及防重放属性;所述安全处理包括:使用加密算法 MD5、SHA、3DES、AES 中的一种或多种对原始报文进行加密和鉴权处理;

伪线封装单元,用于将生成的安全报文进行伪线封装处理,生成封装处理后的安全报文;

安全报文发送单元,用于将封装处理后的安全报文通过预先建立的伪线隧道发送;

伪线隧道建立单元,用于通过协商建立所述的伪线隧道;

安全属性协商单元,用于通过协商得到所述的安全属性。

4. 如权利要求 3 所述的一种用于伪线网络的数据安全发送装置,其特征在于,所述的安全属性协商单元包括:

控制字协商模块,用于通过协商控制字字段,得到所述的安全属性。

5. 一种用于伪线网络的数据安全接收方法,其特征在于,所述的方法包括:

通过协商建立伪线隧道,并在通过协商建立伪线隧道时,通过协商得到安全属性;所述安全属性包括加解密属性、权限认证控制属性、时间限制属性以及防重放属性;

通过预先建立的伪线隧道接收封装处理后的安全报文;其中,所述安全报文的生成过程包括:根据所述安全属性对接收到的原始报文进行安全处理,生成所述安全报文;所述安全处理包括:使用加密算法 MD5、SHA、3DES、AES 中的一种或多种对原始报文进行加密和鉴权处理;

将接收到的封装处理后的安全报文进行伪线解封装处理,生成解封装报文;

根据预先协商的安全属性对生成的解封装报文进行解安全处理,生成原始报文;

将生成的原始报文输出。

6. 如权利要求 5 所述的一种用于伪线网络的数据安全接收方法,其特征在于,所述的通过协商得到所述的安全属性包括:通过协商控制字字段,得到所述的安全属性。

7. 如权利要求 5 所述的一种用于伪线网络的数据安全接收方法,其特征在于,所述的

根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文包括：根据预先协商的安全属性对生成的解封装报文进行解密处理，生成原始报文。

8. 一种用于伪线网络的数据安全接收装置，其特征在于，所述的装置包括：

安全报文接收单元，用于通过预先建立的伪线隧道接收封装处理后的安全报文；其中，所述安全报文的生成过程包括：根据安全属性对接收到的原始报文进行安全处理，生成所述安全报文；所述安全属性包括加解密属性、权限认证控制属性、时间限制属性以及防重放属性；所述安全处理包括：使用加密算法 MD5、SHA、3DES、AES 中的一种或多种对原始报文进行加密和鉴权处理；

解封装单元，用于将接收到的封装处理后的安全报文进行伪线解封装处理，生成解封装报文；

解安全处理单元，用于根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文；

原始报文发送单元，用于将生成的原始报文输出；

伪线隧道建立单元，用于通过协商建立所述的伪线隧道；

安全属性协商单元，用于通过协商得到所述的安全属性。

9. 如权利要求 8 所述的一种用于伪线网络的数据安全接收装置，其特征在于，所述的安全属性协商单元包括：

控制字协商模块，用于通过协商控制字字段，得到所述的安全属性。

10. 如权利要求 8 所述的一种用于伪线网络的数据安全接收装置，其特征在于，所述的解安全处理单元包括：

解密模块，用于根据预先协商的安全属性对生成的解封装报文进行解密处理，生成原始报文。

11. 一种用于伪线网络的数据安全收发方法，其特征在于，所述的方法包括：

接收终端发送的原始报文；

根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文；所述安全属性包括加解密属性、权限认证控制属性、时间限制属性以及防重放属性；所述安全处理包括：使用加密算法 MD5、SHA、3DES、AES 中的一种或多种对原始报文进行加密和鉴权处理；将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文；

将封装处理后的安全报文通过预先建立的伪线隧道发送；

通过预先建立的伪线隧道接收封装处理后的安全报文；

将接收到的封装处理后的安全报文进行伪线解封装处理，生成解封装报文；

根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文；

将生成的原始报文输出；

在根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文前，所述的方法还包括通过协商建立所述的伪线隧道，并在通过协商建立伪线隧道时，通过协商得到所述的安全属性。

12. 一种用于伪线网络的数据安全收发系统，其特征在于，所述的系统包括数据安全接收装置和数据安全发送装置，其中：

所述的数据安全发送装置包括：

原始报文接收单元,用于接收终端发送的原始报文;

安全处理单元,用于根据预先协商的安全属性对接收到的原始报文进行安全处理,生成安全报文;所述安全属性包括加解密属性、权限认证控制属性、时间限制属性以及防重放属性;所述安全处理包括:使用加密算法 MD5、SHA、3DES、AES 中的一种或多种对原始报文进行加密和鉴权处理;

伪线封装单元,用于将生成的安全报文进行伪线封装处理,生成封装处理后的安全报文;

安全报文发送单元,用于将封装处理后的安全报文通过预先建立的伪线隧道发送;

伪线隧道建立单元,用于通过协商建立所述的伪线隧道;

安全属性协商单元,用于通过协商得到所述的安全属性;

所述的数据安全接收装置包括:

安全报文接收单元,用于通过预先建立的伪线隧道接收封装处理后的安全报文;

解封装单元,用于将接收到的封装处理后的安全报文进行伪线解封装处理,生成解封装报文;

解安全处理单元,用于根据预先协商的安全属性对生成的解封装报文进行解安全处理,生成原始报文;

原始报文发送单元,用于将生成的原始报文输出。

一种用于伪线网络的数据安全发送接收方法、装置及系统

技术领域

[0001] 本发明是关于通信技术领域,具体来说是关于一种用于伪线网络的数据安全发送接收方法、装置及系统。

背景技术

[0002] 伪线(PW, Pseudo Wire)是在分组交换网络(PSN, Packet Switched Networks)中仿真ATM、帧中继、以太网、低速时分复用(TDM, Time Division Multiplexing)电路和同步光纤网(SONET, Synchronous Optical Network/同步数字体系(SDH, synchronous digital hierarchy)等业务的一种技术, PW通过在入口封装特定业务的(PDU, Protocol Data Unit),然后在入口和出口之间的路径或隧道上承载这些PDU,管理这些PDU的定时和顺序,来仿真其他业务的功能。

[0003] 随着网络安全问题日益严重,单靠设置密码已经无法保证数据在PW传输过程中的安全性。现在有的网络加密技术是IP Sec, IP Sec (Internet协议安全)是一个工业标准网络安全协议,为IP网络通信提供透明的安全服务,保护TCP/IP通信免遭窃听和篡改,可以有效抵御网络攻击。IP Sec采用端对端加密模式,发送方在数据传输前(即到达网线之前)对数据实施加密,在整个传输过程中,报文都是以密文方式传输,直到数据到达目的节点,才由接收端对其进行解密。

[0004] 对于PW传输技术来说,IP Sec只能保护IP/TCP通信,对于非IP/TCP报文无法实现加密传输,且IP Sec采用端到端处理,如果发送方和接收方有一方不支持IP Sec就不能实现安全保护功能。

发明内容

[0005] 为克服现有技术中存在的问题,本发明提供一种用于伪线网络的数据安全发送接收方法、装置及系统。

[0006] 本发明提供一种用于伪线网络的数据安全发送方法,所述的方法包括:接收终端发送的原始报文;根据预先协商的安全属性对接收到的原始报文进行安全处理,生成安全报文;将生成的安全报文进行伪线封装处理,生成封装处理后的安全报文;将封装处理后的安全报文通过预先建立的伪线隧道发送;在根据预先协商的安全属性对接收到的原始报文进行安全处理,生成安全报文前,所述的方法还包括通过协商建立所述的伪线隧道;在通过协商建立伪线隧道时,通过协商得到所述的安全属性。

[0007] 本发明还提供一种用于伪线网络的数据安全发送装置,所述的装置包括:原始报文接收单元,用于接收终端发送的原始报文;安全处理单元,用于根据预先协商的安全属性对接收到的原始报文进行安全处理,生成安全报文;伪线封装单元,用于将生成的安全报文进行伪线封装处理,生成封装处理后的安全报文;安全报文发送单元,用于将封装处理后的安全报文通过预先建立的伪线隧道发送;伪线隧道建立单元,用于通过协商建立所述的伪线隧道;安全属性协商单元,用于通过协商得到所述的安全属性。

[0008] 本发明还提供一种用于伪线网络的数据安全接收方法，所述的方法包括：通过协商建立所述的伪线隧道，并在通过协商建立伪线隧道时，通过协商得到所述的安全属性；通过预先建立的伪线隧道接收封装处理后的安全报文；将接收到的封装处理后的安全报文进行伪线解封装处理，生成解封装报文；根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文；将生成的原始报文输出。

[0009] 本发明还提供一种用于伪线网络的数据安全接收装置，所述的装置包括：安全报文接收单元，用于通过预先建立的伪线隧道接收封装处理后的安全报文；解封装单元，用于将接收到的封装处理后的安全报文进行伪线解封装处理，生成解封装报文；解安全处理单元，用于根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文；原始报文发送单元，用于将生成的原始报文输出；伪线隧道建立单元，用于通过协商建立所述的伪线隧道；安全属性协商单元，用于通过协商得到所述的安全属性。

[0010] 本发明还提供一种用于伪线网络的数据安全收发方法，所述的方法包括：接收终端发送的原始报文；根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文；将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文；将封装处理后的安全报文通过预先建立的伪线隧道发送；通过预先建立的伪线隧道接收封装处理后的安全报文；将接收到的封装处理后的安全报文进行伪线解封装处理，生成解封装报文；根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文；将生成的原始报文输出；在根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文前，所述的方法还包括通过协商建立所述的伪线隧道；在通过协商建立伪线隧道时，通过协商得到所述的安全属性。

[0011] 本发明还提供一种用于伪线网络的数据安全收发系统，所述的系统包括的数据安全接收装置和数据安全发送装置，所述的数据安全发送装置包括：原始报文接收单元，用于接收终端发送的原始报文；安全处理单元，用于根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文；伪线封装单元，用于将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文；安全报文发送单元，用于将封装处理后的安全报文通过预先建立的伪线隧道发送；所述的数据安全接收装置包括：安全报文接收单元，用于通过预先建立的伪线隧道接收封装处理后的安全报文；解封装单元，用于将接收到的封装处理后的安全报文进行伪线解封装处理，生成解封装报文；解安全处理单元，用于根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文；原始报文发送单元，用于将生成的原始报文输出；伪线隧道建立单元，用于通过协商建立所述的伪线隧道；安全属性协商单元，用于通过协商得到所述的安全属性。

[0012] 本发明克服了现有技术 PW 传输技术信息不安全的问题，实现了在 PW 传输转发中的数据的安全保护功能，解决在 PW 中传输数据进行安全保护处理的技术空白，且不局限于 IP/TCP 报文，应用广泛，可以对各种类型的报文进行安全保护处理。

附图说明

[0013] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，并不构成对本发明的限定。在附图中：

[0014] 图 1 是本发明实施例提供的一种用于伪线网络的数据安全发送方法流程图；

- [0015] 图 2 是典型 PW 组网结构图；
- [0016] 图 3 是本发明实施例提供的一种用于伪线网络的数据安全发送装置框图；
- [0017] 图 4 是本发明实施例提供的一种用于伪线网络的数据安全接收方法流程图；
- [0018] 图 5 是本发明实施例提供的一种用于伪线网络的数据安全接收装置框图；
- [0019] 图 6 是本发明实施例提供的一种用于伪线网络的数据安全收发方法流程图；
- [0020] 图 7 是本发明实施例提供的一种用于伪线网络的数据安全收发系统框图。

具体实施方式

[0021] 为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施方式和附图，对本发明做进一步详细说明。在此，本发明的示意性实施方式及其说明用于解释本发明，但并不作为对本发明的限定。

[0022] 本发明实施例提供一种用于伪线网络的数据安全发送接收方法、装置及系统，以下结合附图对本发明进行详细说明。

[0023] 在现在广泛使用的 PW 典型组网中，是没有做基于 PW 的安全保护技术对 PW 中传输的报文进行安全保护处理的，也就是说如果用户的报文是非保护状态下进入 PW 的，则在 PW 中传输时报文是不安全的，完全可以通过流量镜像等方法窃听到在 PW 中的报文，通过很简单的技术就可以剥离报文的 PW 传输封装，这样用户的原始报文就被非法获取了。

[0024] 基于现在没有基于 PW 的安全保护技术，我们提出了具有数据安全属性的 PW 网络。以下面的典型 PW 组网说明在 PW 建立时如何建立具有数据安全属性的 PW 网络。

[0025] 实施例 1

[0026] 图 1 是本发明实施例提供的一种用于伪线网络的数据安全发送方法流程图，如图 1 所示，所述的方法包括：

[0027] S101，接收终端发送的原始报文。

[0028] 在本发明实施例中，以典型 PW 组网说明在 PW 建立时如何建立具有数据安全属性的 PW 网络，图 2 是典型 PW 组网结构图，如图 2 所示，终端 201 通过配属链路 202 (AC, Attachment Circuit) 以及另一终端 204 的配属链路 203 建立与终端 204 的 PW 连接，其中，AC202 接收终端 201 发送的原始报文。

[0029] S102，根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文。所述对接收到的原始报文进行安全处理包括但不限于：使用 MD5 算法对报文进行加密或使用安全时间戳对报文生存时间进行限制等。

[0030] 在本发明实施例中，在步骤 S102 之前，AC202 和 AC203 可以通过协商建立一伪线隧道，并可以在建立伪线隧道的同时，通过协商得到安全属性，其中，安全属性包括但不限制加解密属性、权限认证控制属性、时间限制属性以及防重放属性等。在本发明实施例中，可以通过协商 CW (控制字, Control Word) 字段，得到安全属性。AC202 根据预先协商的安全属性对从终端 201 接收到的原始报文进行安全处理，生成安全报文。

[0031] S103，将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文。

[0032] 在本发明实施例中，AC202 将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文。

[0033] S104，将封装处理后的安全报文通过预先建立的伪线隧道发送。

[0034] 在本发明实施例中，AC202 还将封装处理后的安全报文通过预先建立的伪线隧道发送。

[0035] 在本发明的一实施例中，步骤 S102 可以包括：根据预先协商的安全属性对接收到的原始报文进行加密处理，使用 MD5、SHA、3DES、AES 等加密算法中的一种或多种对原始报文进行加密和鉴权处理，生成安全报文。

[0036] 本发明克服了现有技术 PW 传输技术信息不安全的问题，实现了在 PW 传输转发中的数据的安全保护功能，解决在 PW 中传输数据进行安全保护处理的技术空白，且不局限于 IP/TCP 报文，应用广泛，可以对现有和以后可见的各种类型的报文进行安全保护处理。

[0037] 实施例 2

[0038] 图 3 是本发明实施例提供的一种用于伪线网络的数据安全发送装置框图，如图 3 所示，所述的用于伪线网络的数据安全发送装置包括原始报文接收单元 301、安全处理单元 302、伪线封装单元 303 和安全报文发送单元 304，其中：

[0039] 原始报文接收单元 301，用于接收终端发送的原始报文。

[0040] 在本发明实施例中，结合图 2 所示，数据安全发送装置可以是 AC202，其中原始报文接收单元 301 用于接收终端 201 发送的原始报文。

[0041] 安全处理单元 302，用于根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文。

[0042] 在本发明实施例中，数据安全发送装置可以包括安全属性协商单元 306，安全属性协商单元 306 通过与 AC203 协商得到安全属性。安全处理单元 302 根据安全属性协商单元 306 协商的安全属性对从终端 201 接收到的原始报文进行安全处理，生成安全报文。在本发明的一实施例中，安全属性协商单元 306 可以包括 CW 协商模块，用于通过协商 CW 字段，得到安全属性。

[0043] 在本发明的一实施例中，安全处理单元 302 可以包括加密模块，用于根据预先协商的安全属性对接收到的原始报文进行加密处理，生成安全报文。

[0044] 伪线封装单元 303，用于将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文。

[0045] 在本发明实施例中，伪线封装单元 303 将安全处理单元 302 生成的安全报文进行伪线封装处理，生成封装处理后的安全报文。

[0046] 安全报文发送单元 304，用于将封装处理后的安全报文通过预先建立的伪线隧道发送。

[0047] 在本发明实施例中，数据安全发送装置还可以包括伪线隧道建立单元 305，伪线隧道建立单元 305 通过与 AC203 协商建立伪线隧道，安全报文发送单元 304 将伪线封装单元 303 封装处理后的安全报文通过伪线隧道建立单元 305 建立的伪线隧道发送给 AC203。

[0048] 本发明克服了现有技术 PW 传输技术信息不安全的问题，实现了在 PW 传输转发中的数据的安全保护功能，解决在 PW 中传输数据进行安全保护处理的技术空白，且不局限于 IP/TCP 报文，应用广泛，可以对现有和以后可见的各种类型的报文进行安全保护处理。

[0049] 实施例 3

[0050] 图 4 是本发明实施例提供的一种用于伪线网络的数据安全接收方法流程图，如图 4 所示，所述的方法包括：

[0051] S401,通过预先建立的伪线隧道接收封装处理后的安全报文。

[0052] 在本发明实施例中,在步骤S401通过预先建立的伪线隧道接收封装处理后的安全报文之前,所述的方法可以包括通过协商建立伪线隧道的步骤。结合图2所示,AC203与AC202通过协商建立伪线隧道,然后AC203通过建立的伪线隧道从AC202接收封装处理后的安全报文。

[0053] S402,将接收到的封装处理后的安全报文进行伪线解封装处理,生成解封装报文。

[0054] 在本发明实施例中,AC203将从AC202接收到的封装处理后的安全报文进行伪线解封装处理,生成解封装报文。

[0055] S403,根据预先协商的安全属性对生成的解封装报文进行解安全处理,生成原始报文。

[0056] 在本发明实施例中,在AC203与AC202通过协商建立伪线隧道的同时,AC203与AC202还可以通过协商得到安全属性,如可以通过协商CW字段得到安全属性。AC203根据预先协商的安全属性对生成的解封装报文进行解安全处理,生成原始报文。

[0057] S404,将生成的原始报文输出。

[0058] 在本发明实施例中,AC203将生成的原始报文输出至终端204。

[0059] 在本发明的一实施例中,步骤S403可以是根据预先协商的安全属性对生成的解封装报文进行解密处理,生成原始报文。

[0060] 本发明克服了现有技术PW传输技术信息不安全的问题,实现了在PW传输转发中的数据的安全保护功能,解决在PW中传输数据进行安全保护处理的技术空白,且不局限于IP/TCP报文,应用广泛,可以对现有和以后可见的各种类型的报文进行安全保护处理。

[0061] 实施例4

[0062] 图5是本发明实施例提供的一种用于伪线网络的数据安全接收装置框图,如图5所示,所述的装置包括:

[0063] 安全报文接收单元501,用于通过预先建立的伪线隧道接收封装处理后的安全报文。

[0064] 在本发明实施例中,结合图2所示,数据安全接收装置可以是AC203,其中安全报文接收单元501通过AC203预先建立的伪线隧道接收封装处理后的安全报文。在本发明实施例中,数据安全接收装置还可以包括伪线隧道建立单元505,用于使AC203与AC202通过协商建立伪线隧道。

[0065] 解封装单元502,用于将接收到的封装处理后的安全报文进行伪线解封装处理,生成解封装报文。

[0066] 在本发明实施例中,解封装单元502将从AC202接收到的封装处理后的安全报文进行伪线解封装处理,生成解封装报文。

[0067] 解安全处理单元503,用于根据预先协商的安全属性对生成的解封装报文进行解安全处理,生成原始报文。

[0068] 在本发明实施例中,数据安全接收装置可以包括安全属性协商单元506,用于通过协商得到安全属性,安全属性协商单元506具体可以包括CW协商模块,可以通过协商CW字段得到安全属性。解安全处理单元503根据安全属性协商单元506预先协商的安全属性对解封装单元502生成的解封装报文进行解安全处理,生成原始报文。

[0069] 原始报文发送单元 504，用于将生成的原始报文输出。

[0070] 在本发明实施例中，原始报文发送单元 504 将解安全处理单元 503 生成的原始报文输出至终端 204。

[0071] 在本发明的一实施例中，解安全处理单元 503 可以包括解密模块，解密模块根据预先协商的解密属性对生成的解封装报文进行解密处理，生成原始报文。

[0072] 本发明克服了现有技术 PW 传输技术信息不安全的问题，实现了在 PW 传输转发中的数据的安全保护功能，解决在 PW 中传输数据进行安全保护处理的技术空白，且不局限于 IP/TCP 报文，应用广泛，可以对现有和以后可见的各种类型的报文进行安全保护处理。

[0073] 实施例 5

[0074] 图 6 是本发明实施例提供的一种用于伪线网络的数据安全收发方法流程图，如图 6 所示，所述的方法包括：

[0075] S601，接收终端发送的原始报文；

[0076] S602，根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文；

[0077] S603，将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文；

[0078] S604，将封装处理后的安全报文通过预先建立的伪线隧道发送；

[0079] S605，通过预先建立的伪线隧道接收封装处理后的安全报文；

[0080] S606，将接收到的封装处理后的安全报文进行伪线解封装处理，生成解封装报文；

[0081] S607，根据预先协商的安全属性对生成的解封装报文进行解安全处理，生成原始报文；

[0082] S608，将生成的原始报文输出。

[0083] 本发明克服了现有技术 PW 传输技术信息不安全的问题，实现了在 PW 传输转发中的数据的安全保护功能，解决在 PW 中传输数据进行安全保护处理的技术空白，且不局限于 IP/TCP 报文，应用广泛，可以对现有和以后可见的各种类型的报文进行安全保护处理。

[0084] 实施例 6

[0085] 图 7 是本发明实施例提供的一种用于伪线网络的数据安全收发系统框图，如图 6 所示，所述的系统包括的数据安全接收装置 701 和数据安全发送装置 702，其中：

[0086] 所述的数据安全发送装置 702 包括：

[0087] 原始报文接收单元 703，用于接收终端发送的原始报文；

[0088] 安全处理单元 704，用于根据预先协商的安全属性对接收到的原始报文进行安全处理，生成安全报文；

[0089] 伪线封装单元 705，用于将生成的安全报文进行伪线封装处理，生成封装处理后的安全报文；

[0090] 安全报文发送单元 706，用于将封装处理后的安全报文通过预先建立的伪线隧道发送；

[0091] 所述的数据安全接收装置 701 包括：

[0092] 安全报文接收单元 707，用于通过预先建立的伪线隧道接收封装处理后的安全报文；

[0093] 解封装单元 708,用于将接收到的封装处理后的安全报文进行伪线解封装处理,生成解封装报文;

[0094] 解安全处理单元 709,用于根据预先协商的安全属性对生成的解封装报文进行解安全处理,生成原始报文;

[0095] 原始报文发送单元 710,用于将生成的原始报文输出。

[0096] 本发明克服了现有技术 PW 传输技术信息不安全的问题,实现了在 PW 传输转发中的数据的安全保护功能,解决在 PW 中传输数据进行安全保护处理的技术空白,且不局限于 IP/TCP 报文,应用广泛,可以对现有和以后可见的各种类型的报文进行安全保护处理。

[0097] 以上所述的具体实施方式,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施方式而已,并不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,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

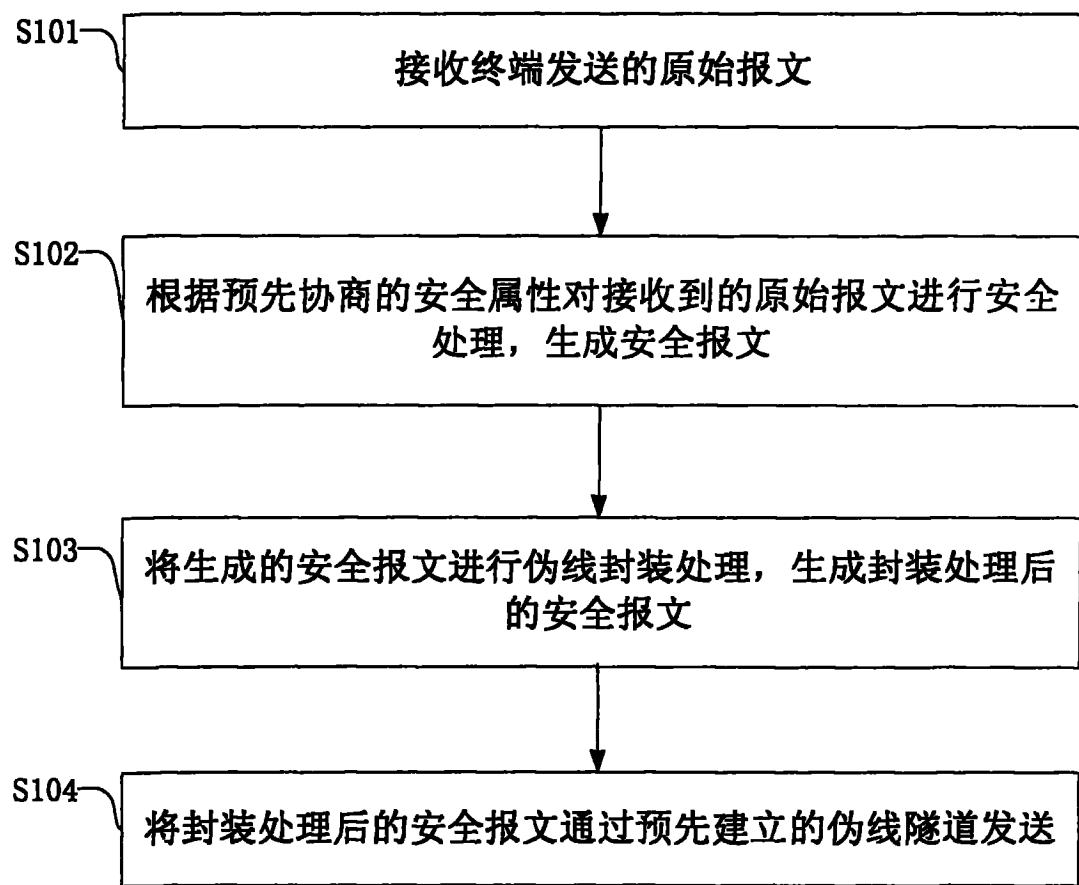


图 1

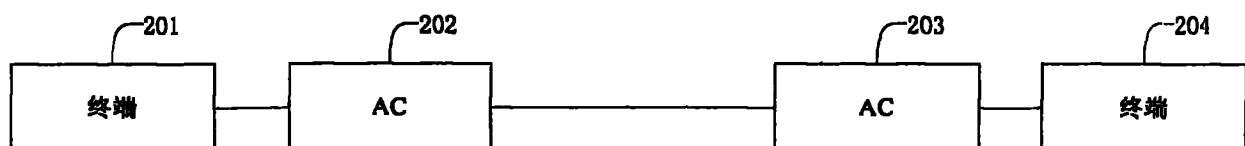


图 2

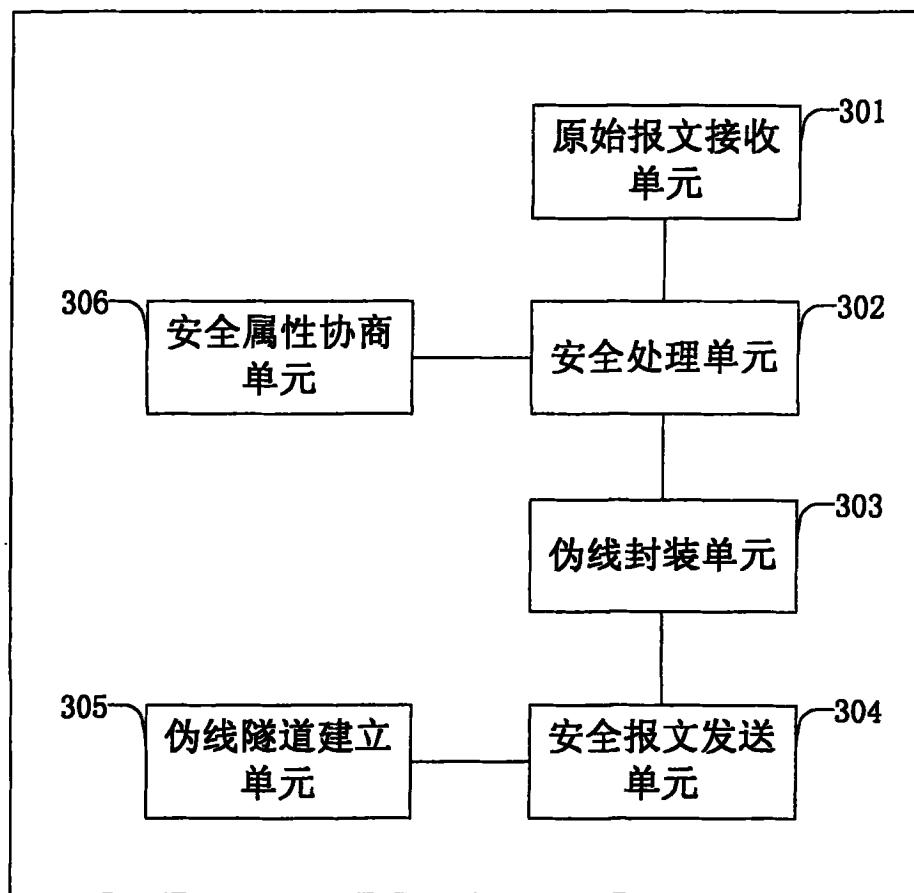


图 3

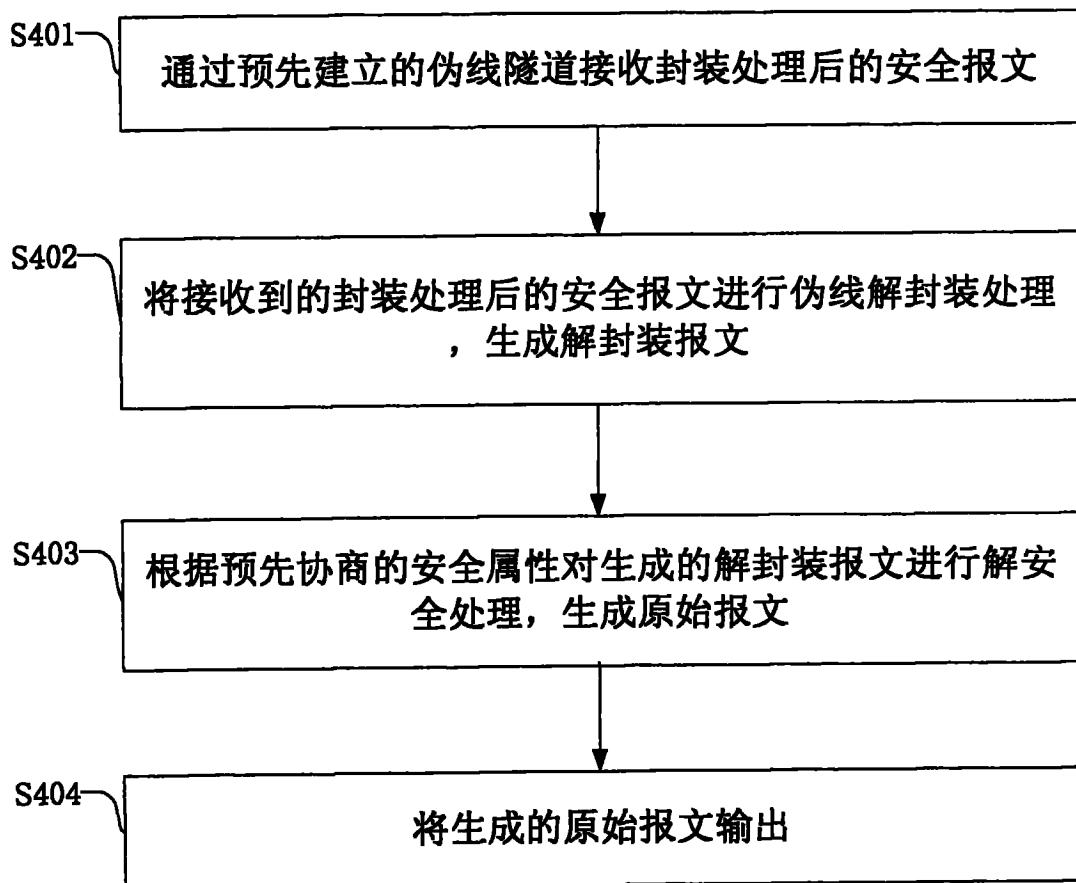


图 4

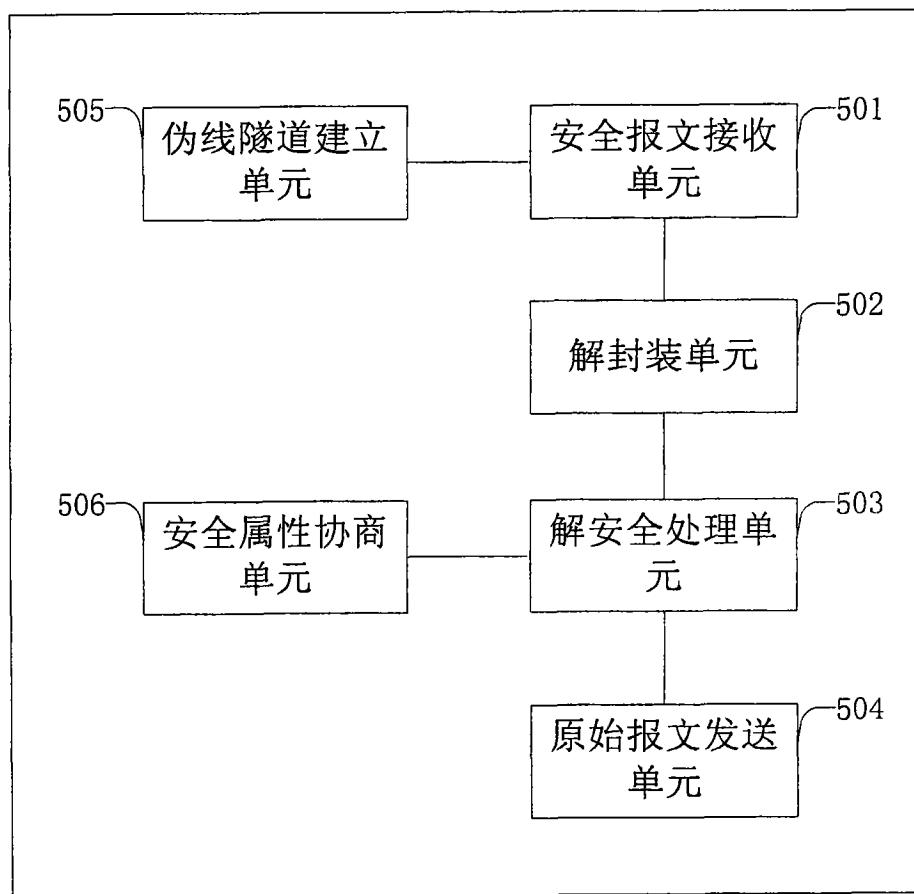


图 5

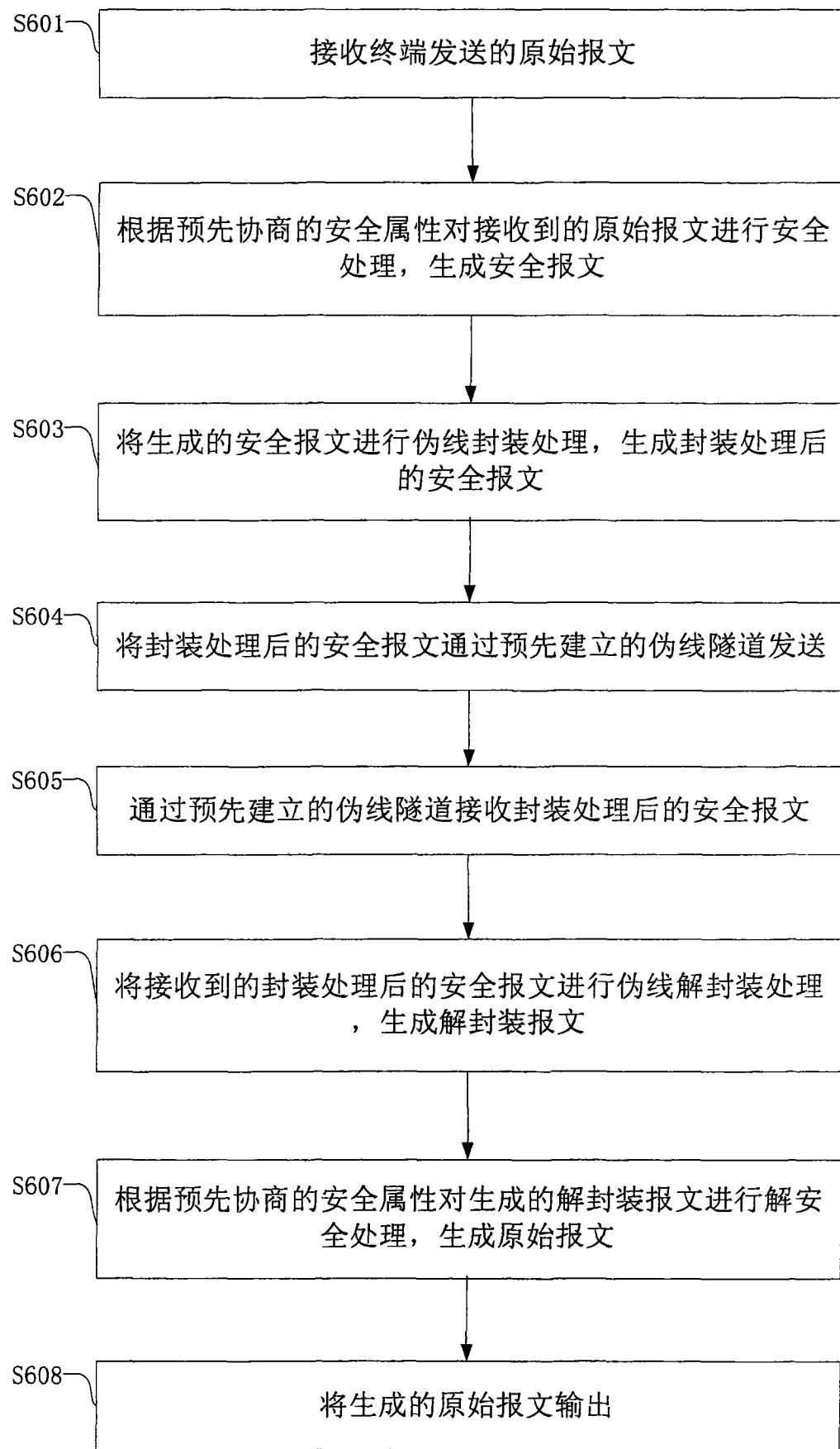


图 6

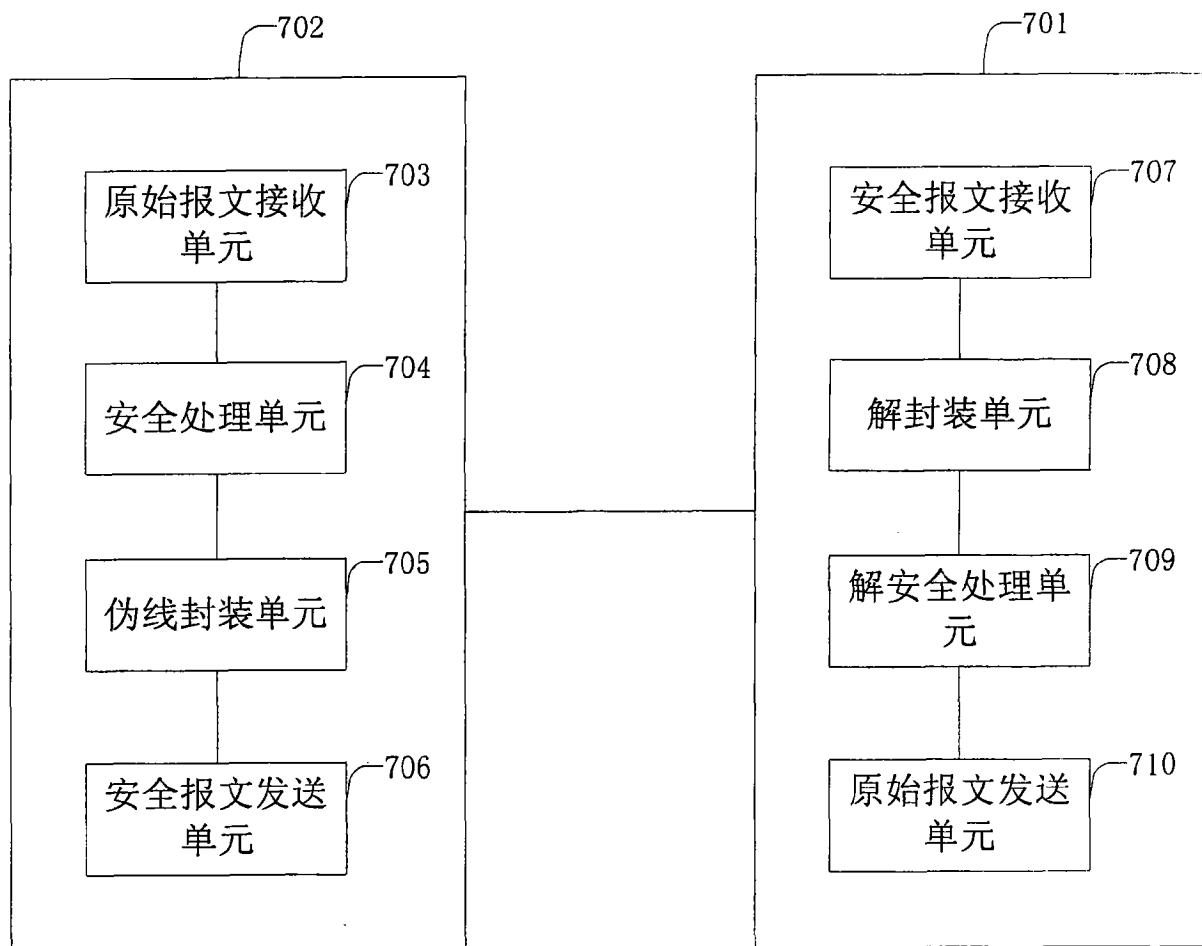


图 7