[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/02 (2006.01)
H04L 9/32 (2006.01)
H04Q 3/545 (2006.01)

[12] 发明专利说明书

专利号 ZL 03149989.9

[45] 授权公告日 2008 年 10 月 22 日

[11] 授权公告号 CN 100428748C

[22] 申请日 2003.8.1 [21] 申请号 03149989.9

[73] 专利权人 联想（北京）有限公司

地址 100085 北京市海淀区上地信息产业基地创业路 6 号

[72] 发明人 杨 燚 曲亚东 李 俊

[56] 参考文献

CN1359074A 2002.7.17

CN1318244A 2001.10.17

US6226689B1 2001.5.1

WO0146843A2 2001.6.28

P2P 技术的研究与应用. 陈姝等. 计算机工程与应用，第 13 期. 2002

SSL 与网络安全技术及其实现. 邬伟峰等. 中山大学学报论丛，第 22 卷第 1 期. 2002

用 Socket/Winsock 实现对等网络功能. 张敬峰. 软件世界，第 12 期. 1996

审查员 叶 峰

[74] 专利代理机构 北京德琦知识产权代理有限公司

代理人 张颖玲

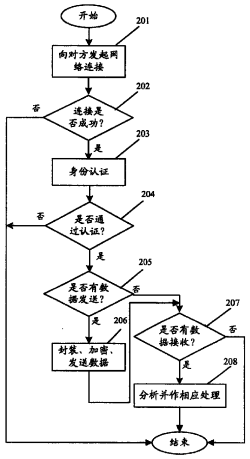
权利要求书 2 页 说明书 8 页 附图 3 页

[54] 发明名称

一种基于双重身份的多方通信方法

[57] 摘要

本发明公开了一种基于双重身份的多方通信方法，适用于一个以上通信设备在不对等连接情况下的互连互通，该方法包括：预先在每个通信设备中配置并存储当前通信设备的通信对象，以及与每个通信对象进行通信时当前通信设备的身份；每个通信设备根据所述配置要求实时监听与自身连接的所有通信对象，在判定有向自身发起的网络连接请求时，以服务器端的身份与发起网络连接请求的通信对象建立连接并与其进行交互；否则，继续进行监听；并且，每个通信设备也可以根据配置要求随时以客户端的身份向与自身连接的能提供服务的通信对象主动发起网络连接请求。该方法可使任意通信设备在不对等连接的多方通信情况下，能同时以服务器端和客户端的身份进行通信。



1、一种基于双重身份的多方通信方法，适用于一个以上通信设备在不对等连接情况下的互连互通，其特征在于，该方法包括：预先在每个通信设备中配置并存储当前通信设备的通信对象，以及与每个通信对象进行通信时当前通信设备的身份，为每个通信设备配置服务功能和/或请求服务功能；每个通信设备根据配置要求，实时以服务器的身份监听与自身连接的作为客户端的通信对象，判断是否有向自身发起的网络连接请求，如果有，则以服务器端的身份与发起网络连接请求的通信对象建立连接并与其进行交互；否则，继续进行监听；并且，每个通信设备根据所述配置要求，随时以客户端的身份向与自身连接的作为服务器的通信对象主动发起网络连接请求。

2、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：预先在每个通信设备中存储用于安全认证的数字证书。

3、根据权利要求 2 所述的方法，其特征在于，所述主动发起网络连接进一步包括：

a1. 发起方根据加密套接字协议层协议，向对方发送自身存储的数字证书，同时接收对方发来的数字证书，通信双方进行认证身份；

b1. 判断通信双方是否均通过身份认证，如果通过，则进行数据发送或接收，否则，结束当前网络连接流程。

4、根据权利要求 1 所述的方法，其特征在于，所述监听其他网络设备向自身发起的网络连接进一步包括：

a2. 监听方根据加密套接字协议层协议，接收向自身发起网络连接方发来的数字证书，对发起网络连接方进行身份认证，同时监听方向发起网络连接方发送自身存储的数字证书，请求对自身的身份进行认证；

b2. 判断通信双方是否均通过身份认证，如果通过，则进行数据发送或接收，否则，继续进行监听。

5、根据权利要求 3 或 4 所述的方法，其特征在于，所述的数据发送进一步

包括：将要发送的数据包进行封装，并采用自身存储的数字证书中的公共密钥对封装后的数据进行加密并发送。

6、根据权利要求 5 所述的方法，其特征在于，所述对数据包进行封装为：在要传输的数据包前顺序添加表示数据包类型的字段、表示数据包序号的字段以及表示数据包长度的字段。

7、根据权利要求 6 所述的方法，其特征在于，所述的数据接收进一步包括：将接收到的数据包根据自身存储的数字证书中的公共密钥进行解密，然后从解密后的数据中解析出表示数据包类型的字段，根据数据包类型进行相应处理。

8、根据权利要求 6 所述的方法，其特征在于，所述数据包类型为报警信息、或系统状态信息、或通信配置文件数据、或系统日志文件数据、或规则文件数据、或升级包数据、或启动/停止/重启动/获取日志命令、或响应、或探测引擎配置文件数据、或规则屏蔽命令、或会话文件建立命令、或会话文件数据、或会话处理配置文件数据、或连接状态数据、或会话处理命令文件数据、流量统计数据、或地址解析协议欺骗配置文件数据、或拨号检测配置文件数据、或拨号检测列表文件数据、或流量统计配置文件数据、或防火墙联动配置文件、或防火墙联动密钥文件数据、或与控制台时钟同步命令、或报警代理配置文件数据。

9、根据权利要求 7 所述的方法，其特征在于，所述数据包类型为报警信息、或系统状态信息、或通信配置文件数据、或系统日志文件数据、或规则文件数据、或升级包数据、或启动/停止/重启动/获取日志命令、或响应、或探测引擎配置文件数据、或规则屏蔽命令、或会话文件建立命令、或会话文件数据、或会话处理配置文件数据、或连接状态数据、或会话处理命令文件数据、流量统计数据、或地址解析协议欺骗配置文件数据、或拨号检测配置文件数据、或拨号检测列表文件数据、或流量统计配置文件数据、或防火墙联动配置文件、或防火墙联动密钥文件数据、或与控制台时钟同步命令、或报警代理配置文件数据。

一种基于双重身份的多方通信方法

技术领域

本发明涉及计算机网络通信技术，具体地说，涉及一种基于双重身份的多方通信方法。

背景技术

目前，网络通信模式大都是客户端/服务器端模式，客户端和服务器端是不对等的，即服务器端不可能通过客户端和服务器端之间建立的通信连接向客户端提出服务请求，也就是说，服务器端只是提供服务，客户端只是提出服务请求。如果服务器端和客户端之间存在防火墙并且需要服务器端在内网，防火墙安全策略要求不允许外网用户访问内网，因此，如果采用现有的网络通信模式这种部署很难实现，尤其是需要同一解决方案满足不同的部署需求时，现有服务器端与客户端就更难实现了。

P2P（peer to peer）方式是一种对等连接通信模式，虽然 P2P 的通信模式打破了上述网络通信的模式，允许每个通信实体既充当客户端，又可以做服务器端，但 P2P 要求通信双方功能必须对等，并且通信时存在安全方面的问题，因此只是处于概念操作阶段。

并且，在现存的网络通信模式下，针对应用层的各种应用存在多种通信协议，分别实现不同的功能，例如：文件传输协议（FTP）传输文件；Telnet 协议远程登录；HTTP 协议浏览网页等等，但是不存在一种能支持所有这些功能的通信协议。

此外，现存的很多通信协议都是不安全的，虽然出现了 IP 层安全协议 IPSEC 和传输层安全协议加密套接字协议层（SSL）/传输层安全（TLS），但是实际部署在网络通信应用中的极其少，因此应用层协议不安全。在现有的这种

通信现状下，绝大部分网络流量都是明文传输，黑客可以注入或窜改网络流量。通信双方没有通过严格认证，一些不法人员可以轻易连接到服务端。

发明内容

有鉴于此，本发明的主要目的在于提供一种基于双重身份的多方通信方法，使得任意通信设备在不对等连接的多方通信情况下，能同时以服务器端和客户端的身份进行通信。

本发明的另一目的是提高网络的通信安全，并以统一的通信协议控制各种网络功能的实现。

为达到上述目的，本发明的技术方案是这样实现的：

一种基于双重身份的多方通信方法，适用于一个以上通信设备在不对等连接情况下的互连互通，该方法包括：预先在每个通信设备中配置并存储当前通信设备的通信对象，以及与每个通信对象进行通信时当前通信设备的身份，为每个通信设备配置服务功能和/或请求服务功能；每个通信设备根据配置要求，实时以服务器的身份监听与自身连接的作为客户端的通信对象，判断是否有向自身发起的网络连接请求，如果有，则以服务器端的身份与发起网络连接请求的通信对象建立连接并与其进行交互；否则，继续进行监听；并且，每个通信设备根据所述配置要求，随时以客户端的身份向与自身连接的作为服务器的通信对象主动发起网络连接请求。

基于上述方案，在连接过程中，主动发起连接的通信设备作为客户端，监听连接请求的通信设备作为服务器端，每个通信设备根据配置需求可以在和与一些通信设备连接中时做客户端，同时在和与另一些通信设备连接时作为服务器端。连接建立之后，不管连接过程中该做通信设备自身是以什么样的身份出现，它根据配置要求既可以只做服务器端，又可以只做客户端，又还可以同时做服务器端和客户端。

该方法进一步包括：预先在每个通信设备中存储用于安全认证的数字证书。那么，所述主动发起网络连接进一步包括：

a1. 发起方根据加密套接字协议层协议，向对方发送自身存储的数字证书，

同时接收对方发来的数字证书，通信双方进行认证身份；

b1. 判断通信双方是否均通过身份认证，如果通过，则进行数据发送或接收，否则，结束当前网络连接流程。

所述监听其他网络设备向自身发起的网络连接进一步包括：

a2. 监听方根据加密套接字协议层协议，接收向自身发起网络连接方发来的数字证书，对发起网络连接方进行身份认证，同时监听方向发起网络连接方发送自身存储的数字证书，请求对自身的身份进行认证；

b2. 判断通信双方是否均通过身份认证，如果通过，则进行数据发送或接收，否则，继续进行监听。

基于步骤 a1、b1 和步骤 a2、b2 的方案，所述的数据发送进一步包括：将要发送的数据包进行封装，并采用自身存储的数字证书中的公共密钥对封装后的数据进行加密并发送。其中，所述对数据包进行封装为：在要传输的数据包前顺序添加表示数据包类型的字段、表示数据包序号的字段以及表示数据包长度的字段。那么，所述的数据接收进一步包括：将接收到的数据包根据自身存储的数字证书中的公共密钥进行解密，然后从解密后的数据中解析出表示数据包类型的字段，根据数据包类型进行相应处理。

上述方案中，所述数据包类型为报警信息、或系统状态信息、或通信配置文件数据、或系统日志文件数据、或规则文件数据、或升级包数据、或启动/停止/重启动/获取日志命令、或响应、或探测引擎配置文件数据、或规则屏蔽命令、或会话文件建立命令、或会话文件数据、或会话处理配置文件数据、或连接状态数据、或会话处理命令文件数据、流量统计数据、或地址解析协议欺骗配置文件数据、或拨号检测配置文件数据、或拨号检测列表文件数据、或流量统计配置文件数据、或防火墙联动配置文件、或防火墙联动密钥文件数据、或与控制台时钟同步命令、或报警代理配置文件数据。

因此，本发明所提供的基于双重身份的多方通信方法，在不对等连接的情况下进行多方通信时，同一个通信设备既能作为客户端，又能作为服务器端。

比如：预先已经设定通信设备 A 监听通信设备 B 的连接请求，通信设备 B 需要向通信设备 A 发起连接请求，本发明在实际应用中，可以根据需要让通信设备 A 扮演客户端的角色，主动向通信设备 B 发出服务请求；同样，通信设备 B 可以扮演服务器端的角色，接受通信设备 A 的服务请求。如此，就可以越过防火墙的障碍而不影响原来的防火墙安全策略，解决了服务器端在内网而防火墙安全策略又不允许外网用户访问内网的这种部署问题。

本发明的通信方法采用统一的通信协议实现了利用 FTP 传输文件、Telnet 远程数据库访问和远程日志记录，解决了应用层中原有的一种通信协议只支持一种通信功能的问题。

本发明的通信方法用 SSL 作为传输层安全协议，对所有网络流量进行了加密，使得黑客无从下手；该协议要求对通信方进行身份认证，不法人员无法通过安全认证，从而提高了网络传输的安全可靠性。

附图说明

图 1 是本发明实现通信时通信设备间的关系示意图；

图 2 是通信设备作为客户端主动发起网络连接的流程示意图；

图 3 是通信设备作为服务器端监听其他网络设备向自身发起网络连接的流程示意图；

图 4 是本发明在实现入侵检测时的一实施例部署示意图。

具体实施方式

下面结合附图及具体实施例对本发明再作进一步详细的说明。

图 1 是本发明实现通信时通信设备间的关系示意图。如图 1 所示，通信设备 A 相对于通信设备 B 和 C 来说是客户端，而相对于通信设备 D 来说则是服务器端，可见，通信设备 A 既为客户端，又为服务器端。这里所说的客户端、服务器端是以谁发起网络连接而论的，实际上，发起连接的通信设备 A 对通信设备 B 和 C 也可以扮演服务器端，也就是说通信设备 B 和 C 可以向通信设备 A

发出服务请求，通信设备 A 会作为服务器端响应该服务请求。

在本发明中，所有设备间完成各种功能均采用统一的通信协议，即：设备间传输的数据采用统一的数据封装格式，本发明所定义的数据报文封装格式如表一所示：

Type	Seq_num	Length	Data

表 一

表一中，Type 表示数据包的类型，Seq_num 表示数据包的序号，Length 表示数据包长度，Data 就是数据包的内容。其中，Type 占用 2 个字节，类型包括：报警信息、系统状态信息、通信配置文件数据、系统日志文件数据、规则文件数据、升级包数据、启动/停止/重启动/获取日志命令、响应、探测引擎配置文件数据、规则屏蔽命令、会话文件建立命令、会话文件数据、会话处理配置文件数据、连接状态数据、会话处理命令文件数据、流量统计数据、地址解析协议（ARP）欺骗配置文件数据、拨号检测配置文件数据、拨号检测列表文件数据、流量统计配置文件数据、防火墙联动配置文件、防火墙联动密钥文件数据、与控制台时钟同步命令、报警代理配置文件数据；Seq_num 占用 4 个字节；Length 占用 4 个字节。

参见图 1 所示的通信设备之间的关系，以通信设备 A 向通信设备 B 发送数据为例，通信设备 A 按照表一所示的格式封装数据，然后将封装后的数据发送给通信设备 B；当通信设备 A 接收到通信设备 B 发送的数据时，查看该数据包中 Type 字段的值，得到该数据包的类型，然后进行相应的处理，即：根据数据类型保存文件、执行命令、与上层应用交互等。比如：类型为报警信息，就进行报警处理；类型为系统日志文件数据，则记录日志数据等等。因此，本发明实现了一种通信协议支持多种通信功能的目的，具体如何完成后续的处理，可采用现有技术的实现方案。

每个通信设备都要预先配置需要与其他哪些设备通信，并且预先配置与每个设备进行通信时采用的身份：做客户端还是服务器端。同时，需要在各通信

设备自身保存认证服务器端分配的数字证书，即用于鉴权的数字签名，以进行安全认证。每个通信设备根据实际需要，可以定制不同的服务功能和不同的请求服务功能。客户端设备与服务器端设备运行时，在主动发起网络连接的同时，会实时检测是否有其他设备向自身发起网络连接。

因此，本发明具体包括两个过程：主动发起网络连接的过程和监听其他设备向自身发起网络连接的过程。图 2 介绍了某个通信设备主动发起网络连接的过程，图 3 介绍了某个通信设备监听其他设备向自身发起网络连接的过程。

基于图 1 所示的通信设备间关系，以通信设备 A 向通信设备 B 发起网络连接为例，该过程中用 SSL 作为传输层安全协议，该 SSL 提供专门的应用程序接口（API），可通过 API 直接调用 SSL。如图 2 所示，通信设备 A 发起网络连接的过程包括如下步骤：

步骤 201~202：通信设备 A 以客户端的身份主动向通信设备 B 发起网络连接请求；然后，通信设备 A 判断主动连接是否成功，如果连接成功，则执行步骤 203，否则，结束当前网络连接流程。

步骤 203：根据 SSL 协议，通信设备 A 向通信设备 B 发送自身存储的数字证书，请求通信设备 B 认证身份；同时，通信设备 A 也要接收通信设备 B 发来的数字证书，认证通信设备 B 的身份是否合法。

步骤 204：判断通信设备 A 与通信设备 B 是否都通过对方的认证，如果通过对方认证，则执行步骤 205，否则，说明有通信设备可能不合法，结束当前网络连接流程。

步骤 205：判断是否有数据需要发送，如果需要发送数据，则执行步骤 206，否则，执行步骤 207；

步骤 206：通信设备 A 对要发送的数据按照表一所示的数据报文格式进行封装，然后根据自身存储的数字证书中的公共密钥对封装后的数据进行加密并发送。

步骤 207：判断是否有数据需要接收，如果需要接收数据，进行步骤 208；

否则，结束当前网络连接流程。

步骤 208：通信设备 A 根据自身存储的数字证书中的公共密钥，对接收到的数据进行解密，然后分析该收到的数据，解析出数据中的报文类型，根据报文类型作相应处理。例如：解析出报文类型是防火墙联动配置文件，则将该文件保存等等。

基于图 1 所示的通信设备间关系，以通信设备 A 监听其他设备发起网络连接为例，本实施例仍采用 SSL 作为传输层安全协议，如图 3 所示，通信设备 A 监听其他设备向自身发起网络连接的过程包括如下步骤：

步骤 301：通信设备 A 实时监听其他设备向自身发起的网络连接。

步骤 302：判断是否有网络连接请求，如果有请求，则执行步骤 303，否则，返回步骤 301 继续监听。

步骤 303：根据 SSL 协议，向监听到的发起网络连接的通信设备发送自身存储的数字证书，请求对方进行身份认证，同时接收对方设备发来的数字证书，认证对方设备的身份。

步骤 304：判断双方设备是否都通过认证，如果通过认证，则执行步骤 305，否则，返回步骤 301 继续监听。

步骤 305：判断是否有数据需要发送，如果需要发送数据，则执行步骤 306，否则进行步骤 307。

步骤 306：通信设备 A 对要发送的数据按照表一所示的数据报文格式进行封装，然后根据自身存储的数字证书中的公共密钥对封装后的数据进行加密并发送。

步骤 307：判断是否有数据需要接收，如果需要接收数据，执行步骤 308；否则，返回步骤 301 继续监听。

步骤 308：通信设备 A 根据自身存储的数字证书中的公共密钥，对接收到的数据解密，然后分析该接收到的数据，解析出数据中的报文类型，根据报文类型作相应处理。

图 4 是本发明在实现入侵检测时的一实施例部署示意图。在实现入侵检测时，会在网络中不同位置的通信设备上设置多个探测器和控制台，这些探测器和控制台根据部署需求扮演着不同的角色，即：客户端或服务器端。探测器可作为客户端将入侵报警信息、流量统计以及状态信息发送到指定的控制台，探测器也可以作为服务器端向控制台传输会话记录文件。同时，控制台可以作为客户端要求探测器通信程序发送日志文件，也可以作为服务器端把探测器的配置文件发送到指定探测器上，控制台还可以控制探测引擎的启动与停止。

如图 4 所示，公司的分部部署了两个探测器 5 和 6、一个控制台 3，其中探测器 6 处在一个关键网段，通过防火墙与控制台 1 进行通信，因为该探测器 6 不仅要向分部的控制台报告入侵事件，同时要向公司总部报告分部中关键网段出现的入侵事件。以探测器 6 为例，在具体应用中，控制台 3 作为客户端主动与探测器 6 建立连接，这时探测器 6 作为服务器端接收控制台 3 的请求；同时，由于在实际部署中，分部不允许外部访问，因此探测器 6 又作为客户端主动与控制台 1 建立连接。同理，对于分公司中的控制台 2，分公司中的所有探测器都分别作为客户端主动与控制台 2 建立连接，此时控制台 2 作为服务器端；同时，控制台 2 又会将收集到的报警通过与总部控制台 1 建立的连接发送给控制台 1，此种情况下控制台 2 扮演了探测器的角色，也就是说，此时控制台 2 作为客户端。

本发明可以支持网络中多个设备之间多方通信的实现，而且每个设备可以不同的身份与其它设备通信，不需要对等连接。总之以上所述，仅为本发明的较佳实施例而已，并非用来限定本发明的保护范围。

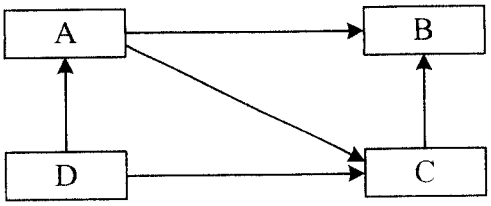

A
B
D
C

图 1

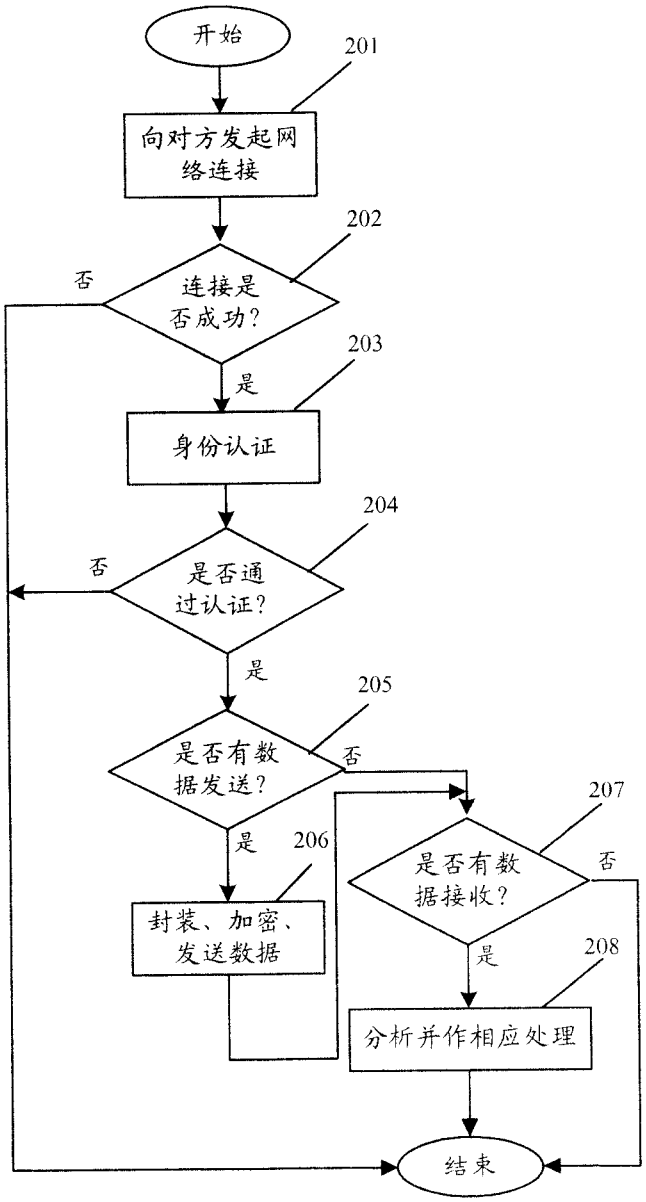

开始
201
向对方发起网络连接
202
连接是否成功?
否
是
203
身份认证
204
是否通过认证?
否
是
205
是否有数据发送?
否
是
206
封装、加密、发送数据
207
是否有数据接收?
否
是
208
分析并作相应处理
结束

图 2

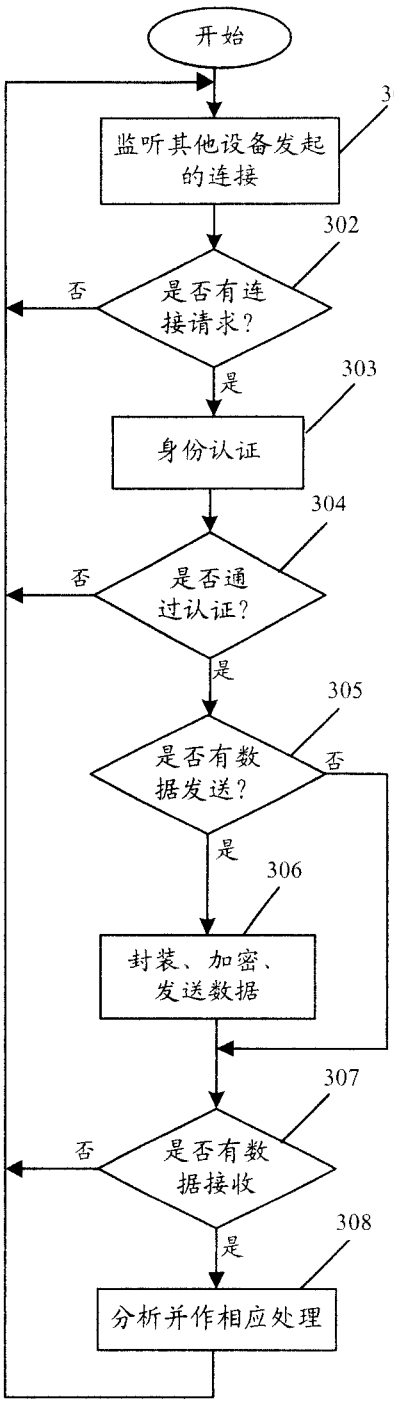

开始
301
监听其他设备发起的连接
302
是否有连接请求?
否
是
303
身份认证
304
是否通过认证?
否
是
305
是否有数据发送?
否
是
306
封装、加密、发送数据
307
是否有数据接收
否
是
308
分析并作相应处理

图 3

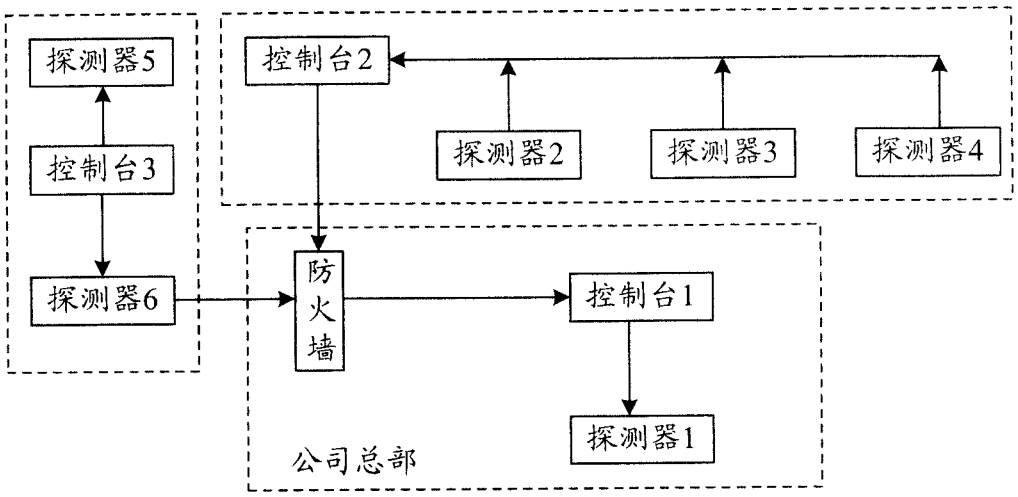


图 4