(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 101247391 B
(45)授权公告日 2013.03.06

(21)申请号 200710173482.0
(22)申请日 2007.12.28
(73)专利权人 上海电力学院
地址 200090 上海市杨浦区平凉路2103号
(72)发明人 魏国强 何鹏飞 何光营
(74)专利代理机构 上海申汇专利代理有限公司 31001
代理人 吴宝根
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
US 2004003235 A1,2004.01.01,
李宁、吴耀华．基于X.509的双向认证框架．《计算机工程与应用》.2005,
何丽、蔡小刚、周利华．基于USBKey的X.509身份认证．《计算机与现代化》.2003,
苑明哲、王智、程尚军、于海斌．OPC技术在现场总线控制系统中的应用．《工业仪表与自动化装置》.2000,
审查员 曹娟

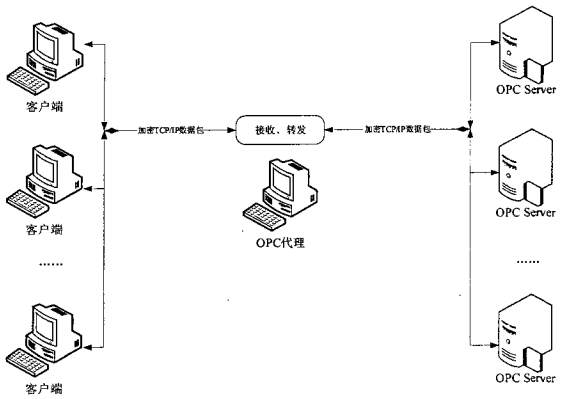
权利要求书 2 页 说明书 5 页 附图 3 页

(54)发明名称

OPC安全代理系统及其代理方法

(57)摘要

本发明公开一种OPC安全代理系统及其代理方法，涉及信息系统安全技术领域；所要解决的是OPC系统安全性的技术问题；该OPC安全代理系统，包括OPC安全代理服务器、至少一个分别连接OPC安全代理服务器的OPC客户端和至少一个分别连接OPC安全代理服务器的OPC服务器；其中作为安全网关，OPC安全代理服务器跨越用户内部具有不同安全性要求的内外网；该安全代理服务器采用Linux操作系统平台；所述安全代理服务器包括互相连接的基于USBkey的X.509身份认证及密钥交换模块、OPC请求权限验证及代理转发模块、数据加密模块。本发明公开具有能保持生产系统内外网间各种授权OPC透明访问的同时，满足较高的安全性隔离要求的特点。



CN 101247391 B

1. 一种用于过程控制的对象连接与嵌入 OPC 安全代理系统，其特征在于，包括 OPC 安全代理服务器、至少一个分别连接 OPC 安全代理服务器的 OPC 客户端和至少一个分别连接 OPC 安全代理服务器的 OPC 服务器；其中作为安全网关，OPC 安全代理服务器跨越用户内具有不同安全性要求的内外网；该 OPC 安全代理服务器采用 Linux 操作系统平台；所述 OPC 安全代理服务器包括互相连接的基于 USBkey 的 X.509 身份认证及密钥交换模块、OPC 请求权限验证及代理转发模块、数据加密模块。

2. 根据权利要求 1 所述的 OPC 安全代理系统，其特征在于，所述 OPC 安全代理服务器的基于 USBkey 的 X.509 身份认证及密钥交换模块设有一个符合 X.509 标准的证书授权及目录服务器用以签发和发布各使用者的数字证书；系统中每个用户使用基于 USB 接口的密钥载体 USBkey 产生和保存个人的私人密钥以及数字证书，在需要使用用户的私人密钥进行身份鉴别和签名时，整个过程在 USBkey 内完成。

3. 根据权利要求 1 所述的 OPC 安全代理系统，其特征在于，所述 OPC 安全代理系统使用 X.509 建议的三向鉴别实现用户和 OPC 安全代理服务器之间的身份鉴别和会话密钥交换。

4. 根据权利要求 1 所述的 OPC 安全代理系统，其特征在于，所述 OPC 安全代理系统在客户端采用基于 Windows 平台 Winsock 中“服务提供者接口”网络封包截获技术截获原 OPC 客户端发往 OPC 服务器的请求，并重定向至 OPC 安全代理服务器，即能通过 OPC 安全代理服务器透明地安全访问原有生产系统 OPC 服务器。

5. 根据权利要求 1 所述的 OPC 安全代理系统，其特征在于，所述 OPC 安全代理系统的所有请求必须通过 OPC 安全代理服务器转发；在接收到客户端转发的 OPC 请求后，OPC 安全代理服务器对数据包解密并恢复客户端 OPC 请求，根据预设的访问权限与控制列表，确定该客户是否拥有相应 OPC 操作权限，决定代理或丢弃该 OPC 请求。

6. 一种权利要求 1 所述的 OPC 安全代理系统的代理方法，其特征在于，方法的流程包括：

1) 开始；

2) 建立访问规则列表；

3) 建立端口映射表；

4) 开始在命令端口监听；

5) 有新的连接请求？有则转至 6)；否则转至 9)；

6) 是否为合法用户？是则转至 7)；否则转至 8)；

7) 登记并返回可访问资源列表；转至 5)；

8) 拒绝连接；转至 5)；

9) 有新的访问请求？有则转至 10)；否则转至 5)；

10) 是否为合法用户？是则转至 12)；否则转至 11)；

11) 记录并拒绝访问；转至 5)；

12) 解密数据包；

13) 是否有权限？是则转至 15)；否则转至 14)；

14) 记录并拒绝访问；转至 5)；

15) 转发给服务器；

16) 等待服务器的响应；

17) 响应结果加密；

18) 返回给客户端；转至 5)。

OPC 安全代理系统及其代理方法

技术领域

[0001] 本发明涉及信息系统安全技术，特别是涉及一种能满足较高的安全性隔离要求的 OPC 安全代理系统及其代理方法的技术。

背景技术

[0002] OPC 规范概述：

[0003] 在电力系统控制领域，各种现场总线控制系统正在日益发挥着重要的作用。然而，由于可用于电力系统控制的现场总线系统种类繁多，其访问方式与接口均各不相同，致使电力控制各应用系统日益复杂，任何应用需要访问任一种现场总线系统都必须要按照该现场总线系统的规范开发一整套底层的驱动及通信模块，其控制模式如图 1 所示。

[0004] 对这样的控制方式，各控制系统的软硬件升级与维护都非常不便。为此，OPC(OLE for Process Control) 基金会提出了 OPC 标准体系，该标准体系基于 Microsoft 的 OLE/COM/DCOM 技术为基础，采用客户 / 服务器模式，基于 Windows 的客户端可以通过标准的 OPC 接口访问位于各控制系统的 OPC 服务器接口。采用这种模式，各现场控制系统厂商只需要开发一个标准的 OPC 服务器接口，即可屏蔽各种复杂的控制系统底层差异，为客户端提供统一的服务接口，而客户端通过标准的 OPC 接口就可以实现对异种控制系统的访问。OPC 提供了一系列的规范，在具体的实现过程中，用户可以根据需要使用相应的规范。其中数据访问规范提供给用户访问实时过程数据的方法；报警和事件规范提供了一种由服务器程序将现场的事件或报警通知客户程序的机制；历史数据存取规范用来提供用户存储的过程数据存档文件、数据库或远程终端设备中的历史以及分析这些历史过程数据的方法。OPC 规范很好的解决了客户端对异种控制系统的访问，在电力系统得到了广泛的应用。其控制访问模式如图 2 所示。

[0005] 在电力生产系统环境中，现场总线控制系统 (OPC 服务器端) 一般位于生产内网中，有很高的安全性要求，而部分 OPC 客户端系统则可能需要位于生产管理层外网，该网可能与外网相通。现有的 OPC 标准体系对跨接在两个安全性要求不同的网间运行并没有完整的安全性措施，此类应用将产生很大的安全性隐患。

[0006] 二、现有技术解决方案及缺陷

[0007] 为解决在安全性要求不同的内外网间在保证安全的情况下保持适当的信息互通要求，目前的常规做法是使用防火墙或隔离网闸。通用的防火墙只实现对 TCP 连接会话的控制，不提供强安全性的用户认证手段，一般只用于两个不同网络边界之间的访问控制。隔离网闸可以切断内外网的 TCP/IP 连接，提供很强的安全性隔离，但目前的隔离网闸都只提供诸如 Web 访问、FTP 文件传输、电子邮件收发等通用的网络服务，一般少有提供强安全用户认证手段，目前尚未见到有支持 OPC 协议的隔离网闸。

发明内容

[0008] 针对上述现有技术中存在的缺陷，本发明所要解决的技术问题是提供一种能保持

生产系统内外网间各种授权 OPC 透明访问的同时，满足较高的安全性隔离要求的，具有安全网关功能的 OPC 安全代理系统及其代理方法。

[0009] 为了解决上述技术问题，本发明所提供的一种 OPC 安全代理系统，其特征在于，包括 OPC 安全代理服务器、至少一个分别连接 OPC 安全代理服务器的 OPC 客户端和至少一个分别连接 OPC 安全代理服务器的 OPC 服务器；其中作为安全网关，OPC 安全代理服务器跨越用户内部具有不同安全性要求的内外网；是整个系统的关键；该安全代理服务器采用 Linux 操作系统平台并经过严格裁剪和重新编译，以确保系统不存在已知的安全漏洞；所述安全代理服务器包括互相连接的基于 USBkey 的 X.509 身份认证及密钥交换模块、OPC 请求权限验证及代理转发模块、数据加密模块等。

[0010] 进一步的，所述安全代理服务器的基于 USBkey 的 X.509 身份认证及密钥交换模块设有一个符合 X.509 标准的 CA 及目录服务器用以签发和发布各使用者的数字证书；系统中每个用户使用基于 USB 接口的密钥载体 USBkey 产生和保存个人的私人密钥以及数字证书，在需要使用用户的私人密钥进行身份鉴别和签名时，整个过程在 USBkey 内完成。其私人密钥一旦产生，就不可读、不可拆解、永不输出的保存在 USBkey 中，从物理上保证了私人密钥的安全，而 USBkey 则由 PIN 码保护。

[0011] 进一步的，所述 OPC 安全代理系统使用 X.509 建议的三向鉴别实现用户和安全代理服务器之间的身份鉴别和会话密钥交换。

[0012] 进一步的，所述 OPC 安全代理系统在客户端采用基于 Windows 平台 Winsock 中“服务提供者接口 (Service Provider Interface，SPI)”网络封包截获技术截获原 OPC 客户端发往 OPC 服务器的请求，并重定向至 OPC 安全代理服务器，不用修改原有 OPC 客户端程序，即可通过 OPC 安全代理服务器透明地安全访问原有生产系统 OPC 服务器。

[0013] 进一步的，所述 OPC 安全代理系统的所有请求必须通过 OPC 安全代理服务器转发；在接收到客户端转发的 OPC 请求后，OPC 安全代理服务器对数据包解密并恢复客户端 OPC 请求，根据预设的访问权限与控制列表，确定该客户是否拥有相应 OPC 操作权限，决定代理或丢弃该 OPC 请求。

[0014] 本发明所提供的一种 OPC 安全代理系统的代理方法，流程为：

[0015] 1) 开始；

[0016] 2) 建立访问规则列表；

[0017] 3) 建立端口映射表；

[0018] 4) 开始在命令端口监听；

[0019] 5) 有新的连接请求？有则转至 6)；否则转至 9)；

[0020] 6) 采用 X.509 协议判断用户是否为合法用户？是则转至 7)；否则转至 8)；

[0021] 7) 与客户端完成密钥交换，并返回可访问资源列表给客户端；转至 5)；

[0022] 8) 拒绝连接；转至 5)；

[0023] 9) 有新的访问请求？有则转至 10)；否则转至 5)；

[0024] 10) 是否为合法用户？是则转至 12)；否则转至 11)；

[0025] 11) 记录并拒绝访问；转至 5)；

[0026] 12) 解密数据包；

[0027] 13) 是否有权限？是则转至 15)；否则转至 14)；

[0028] 14) 记录并拒绝访问 ;转至 5) ;

[0029] 15) 转发给服务器 ;

[0030] 16) 等待服务器的响应 ;

[0031] 17) 响应结果加密 ;

[0032] 18) 返回给客户端 ;转至 5)。

[0033] 利用本发明提供的 OPC 安全代理系统及其代理方法,由于本发明使用基于 USBkey 的 X.509 安全身份认证、客户端网络封包截获、OPC 请求重定向及数据加密、OPC 代理与权限分析等技术,在不用修改原有 OPC 客户端与 OPC 服务器端程序即可保持生产系统内外网间各种授权 OPC 透明访问的同时,满足较高的安全性隔离要求。

附图说明

[0034] 图 1 是现有技术中无 OPC 的控制访问模式框图 ;

[0035] 图 2 是现有技术中 OPC 控制访问模式框图 ;

[0036] 图 3 是本发明实施例 OPC 安全代理系统构架图 ;

[0037] 图 4 是本发明实施例 OPC 安全代理服务器的工作流程框图。

具体实施方式

[0038] 以下结合附图说明对本发明的实施例作进一步详细描述,但本实施例并不用于限制本发明,凡是采用本发明的相似结构及其相似变化,均应列入本发明的保护范围。

[0039] 如图 3 所示,本发明实施例所提供的一种 OPC 安全代理系统,包括 OPC 安全代理服务器、多个分别连接 OPC 安全代理服务器的 OPC 客户端和多个分别连接 OPC 安全代理服务器的 OPC 服务器 ;其中 OPC 安全代理服务器跨越企业内具有不同安全性要求的内外网,担当了一个安全网关的角色,是整个系统的关键。该安全代理服务器采用 Linux 操作系统平台并经过严格裁剪和重新编译,以确保系统不存在已知的安全漏洞。整个安全代理服务器由互相连接的基于 USBkey 的 X.509 身份认证及密钥交换模块、OPC 请求权限验证及代理转发模块、数据加密模块等组成。

[0040] 如图 4 所示,本发明的 OPC 安全代理系统的代理方法,即服务器的工作流程为 :

[0041] 1) 开始 ;

[0042] 2) 建立访问规则列表 ;

[0043] 3) 建立端口映射表 ;

[0044] 4) 开始在命令端口监听 ;

[0045] 5) 有新的连接请求 ? 有则转至 6) ;否则转至 9) ;

[0046] 6) 采用 X.509 协议判断用户是否为合法用户 ? 是则转至 7) ;否则转至 8) ;

[0047] 7) 与客户端完成密钥交换,并返回可访问资源列表给客户端 ;转至 5) ;

[0048] 8) 拒绝连接 ;转至 5) ;

[0049] 9) 有新的访问请求 ? 有则转至 10) ;否则转至 5) ;

[0050] 10) 是否为合法用户 ? 是则转至 12) ;否则转至 11) ;

[0051] 11) 记录并拒绝访问 ;转至 5) ;

[0052] 12) 解密数据包 ;

[0053] 13) 是否有权限？是则转至 15) ;否则转至 14) ;

[0054] 14) 记录并拒绝访问 ;转至 5) ;

[0055] 15) 转发给服务器 ;

[0056] 16) 等待服务器的响应 ;

[0057] 17) 响应结果加密 ;

[0058] 18) 返回给客户端 ;转至 5)。

[0059] 本发明的 OPC 安全代理系统中，安全代理服务器设有基于 USBkey 的 X.509 身份认证及密钥交换模块。用户身份认证是保证整个系统安全的关键，其功能包括客户端对使用者的身份确认及安全代理服务器对客户端的身份认证。本系统采用了基于 PKI 体系结构的 X.509 数字证书作为用户认证的标识。PKI(Public KeyInfrastructure) 是目前广泛采用的基于公开密钥算法实现数字签名、身份鉴别与密钥交换的基础技术构架，通过 X.509 数字证书的颁发、鉴别、更新、撤销等行为来管理、鉴别网络实体的身份。在该体系结构中，一个可信任的证书发布方 CA 对每个人的身份以某种方式予以确认，并向其颁布符合 X.509 标准格式的数字证书，证书包含有该用户的唯一标识、公开密钥信息、序列号、有效时间、颁布者 (即 CA) 的标识等要素，并由 CA 数字签名，以保证证书的完整性和可鉴别性。证书保持在 CA 的目录服务器上可以由任何人查阅，同时目录上还保持一份证书撤销表，使 CA 可以随时应要求而撤销某张证书。

[0060] 本发明的 OPC 安全代理系统建立了一个符合 X.509 标准的 CA 及目录服务器用以签发和发布各使用者的数字证书。为了保持系统的高安全性，系统中每个用户使用基于 USB 接口的密钥载体 USBkey 产生和保存个人的私人密钥以及数字证书，在需要使用用户的私人密钥进行身份鉴别和签名时，整个过程在 USBkey 内完成，其私人密钥一旦产生，就不可读、不可拆解、永不输出的保存在 USBkey 中，从物理上保证了私人密钥的安全，而 USBkey 则由 PIN 码保护。

[0061] 本发明的 OPC 安全代理系统使用 X.509 建议的三向鉴别实现用户和安全代理服务器之间的身份鉴别和会话密钥交换。三向鉴别实现了客户与安全代理服务器之间相互的鉴别并且完成客户与安全服务器之间本次会话所使用对称密钥的交换，同时可以避免由于鉴别双方因时钟误差可能导致的中间人重放攻击。

[0062] 客户端网络封包截获、OPC 请求重定向及数据加密 :

[0063] 本发明的 OPC 安全代理系统在客户端采用基于 Windows 平台 Winsock 中“服务提供者接口 (Service Provider Interface,SPI)”网络封包截获技术截获原 OPC 客户端发往 OPC 服务器的请求，并重定向至 OPC 安全代理服务器，不用修改原有 OPC 客户端程序，即可通过 OPC 安全代理服务器透明地安全访问原有生产系统 OPC 服务器。为保证传输安全，本发明可选三重 DES 或 AES 对称加密算法，采用密文反馈 (CBC) 方式对所传输报文加密，可以有效防止重放攻击。

[0064] OPC 代理与权限分析 :

[0065] 为了隔离内网和外网，所有请求必须通过 OPC 安全代理服务器转发。在接收到客户端转发的 OPC 请求后，OPC 安全代理服务器对数据包解密并恢复客户端 OPC 请求，根据预设的访问权限与控制列表，确定该客户是否拥有相应 OPC 操作权限，决定代理或丢弃该 OPC 请求。如果为合法 OPC 请求，则由 OPC 代理模块向目标 OPC 服务器代理发送该请求，并按需

要加密后向客户端转发应答数据。

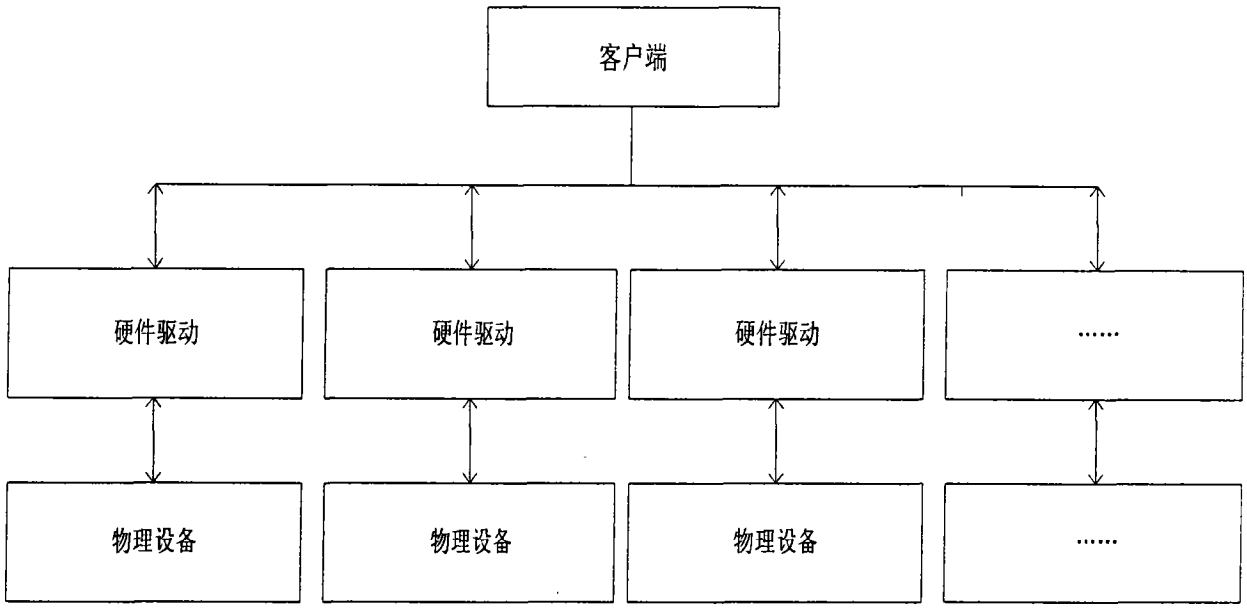


图 1

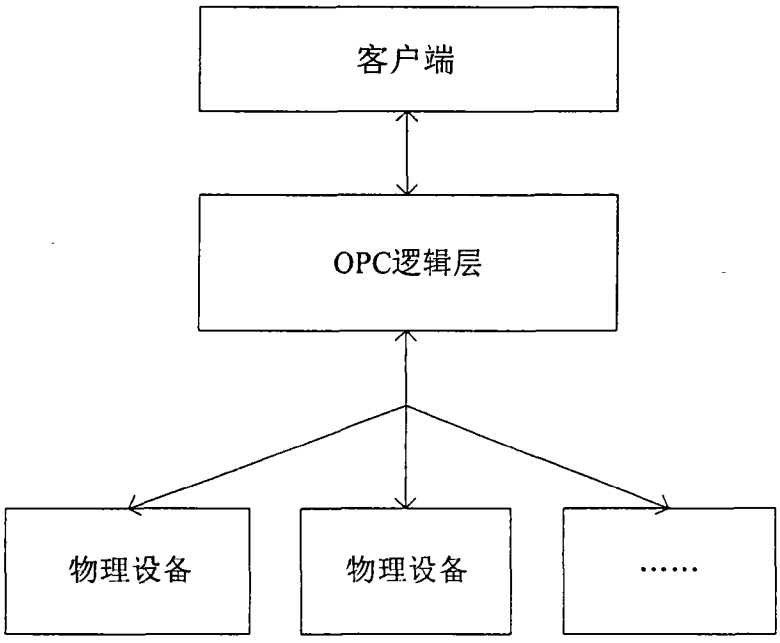


图 2

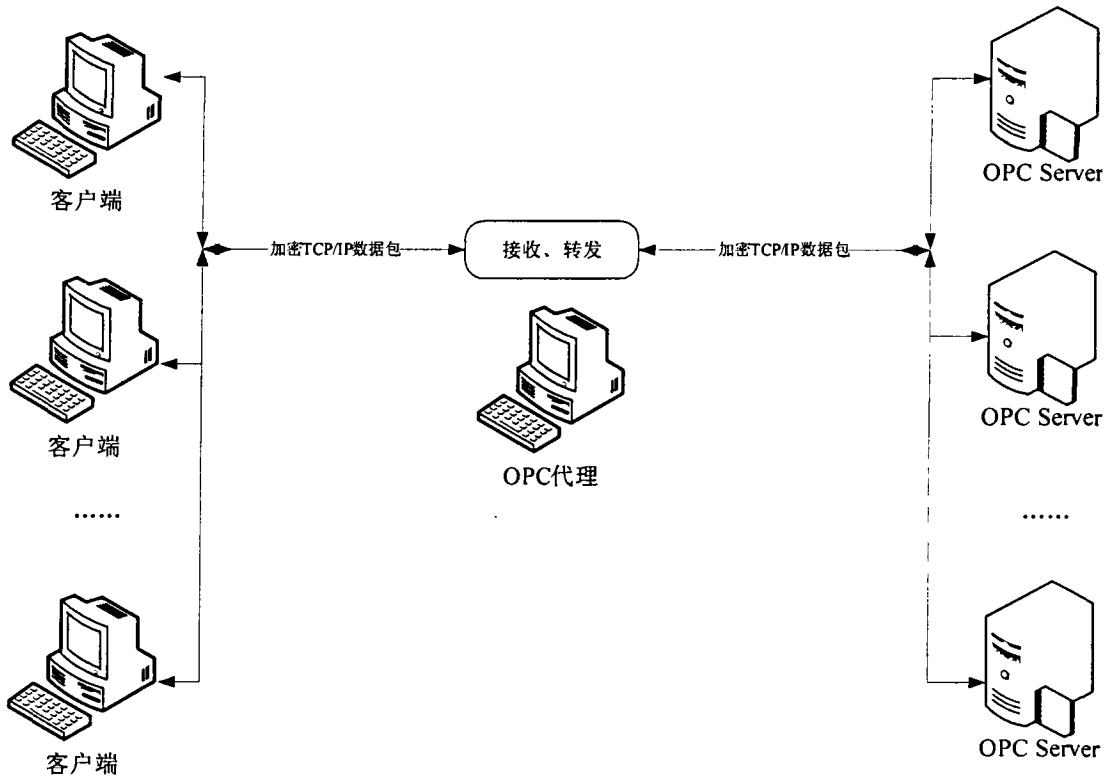

客户端
客户端
.....
客户端
加密TCP/IP数据包
接收、转发
加密TCP/IP数据包
OPC代理
OPC Server
OPC Server
.....
OPC Server

图 3

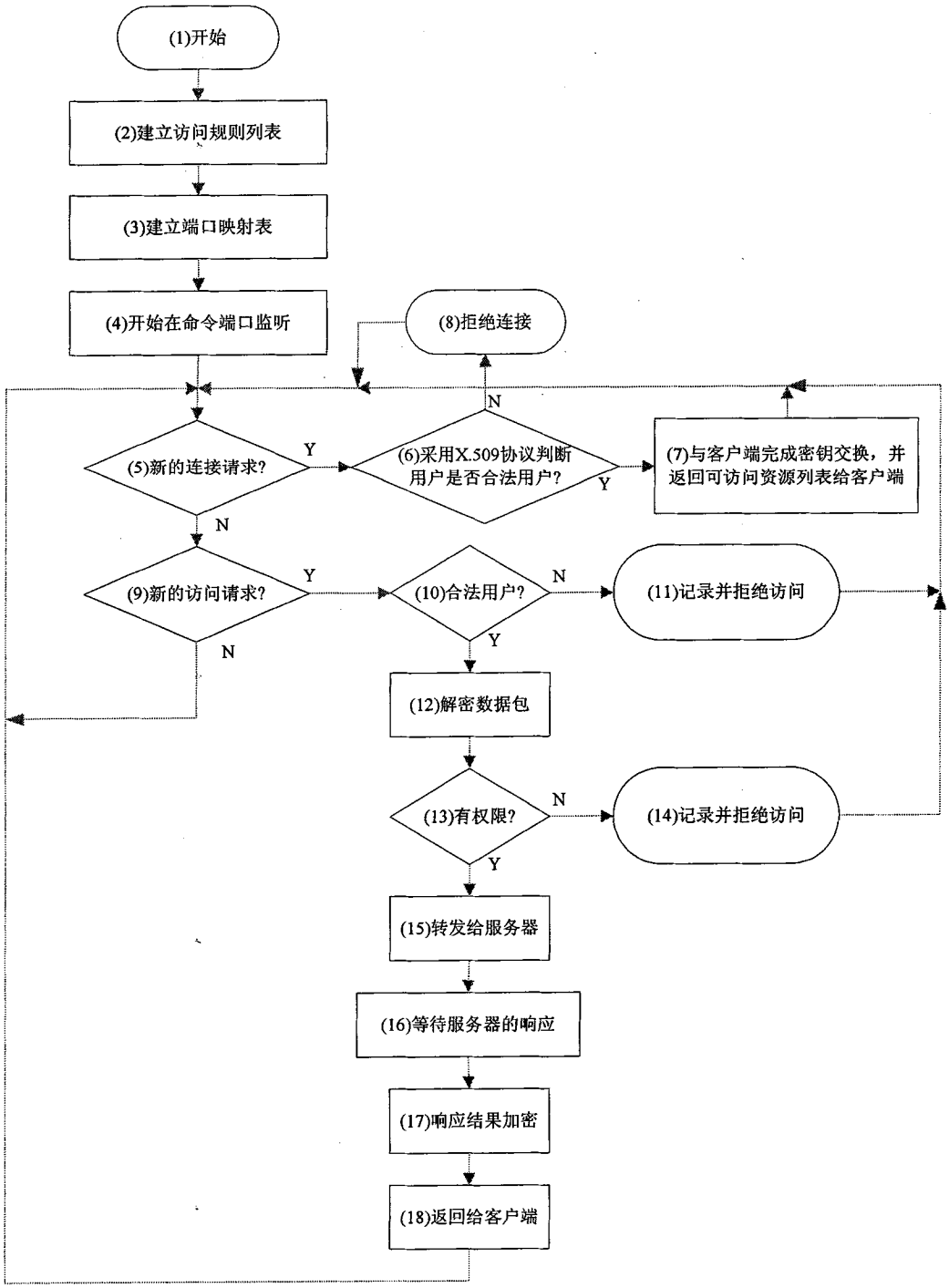

(1)开始
(2)建立访问规则列表
(3)建立端口映射表
(4)开始在命令端口监听
(8)拒绝连接
(5)新的连接请求?
Y
(6)采用X.509协议判断用户是否合法用户?
N
Y
(7)与客户端完成密钥交换，并返回可访问资源列表给客户端
N
(9)新的访问请求?
Y
(10)合法用户?
N
(11)记录并拒绝访问
N
Y
(12)解密数据包
(13)有权限?
N
(14)记录并拒绝访问
Y
(15)转发给服务器
(16)等待服务器的响应
(17)响应结果加密
(18)返回给客户端

图 4