(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 106878378 B
(45)授权公告日 2020.02.21

(21)申请号 201611214700.6

(22)申请日 2016.12.26

(65)同一申请的已公布的文献号
申请公布号 CN 106878378 A

(43)申请公布日 2017.06.20

(73)专利权人 贵州银行股份有限公司
地址 550006 贵州省贵阳市观山湖区长岭北路贵阳国际会议展览中心SOHO区D1栋出版集团大厦三层

(72)发明人 冯六军 张晖 吴贤佳 臧晗

(74)专利代理机构 贵阳中新专利商标事务所 52100
代理人 李亮 程新敏

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

(56)对比文件
CN 102111378 A,2011.06.29,
CN 104050102 A,2014.09.17,
CN 103246547 A,2013.08.14,
CN 103002444 A,2013.03.27,
CN 104463670 A,2015.03.25,
CN 106453334 A,2017.02.22,
CN 105786611 A,2016.07.20,
CN 104378362 A,2015.02.25,

审查员 金星

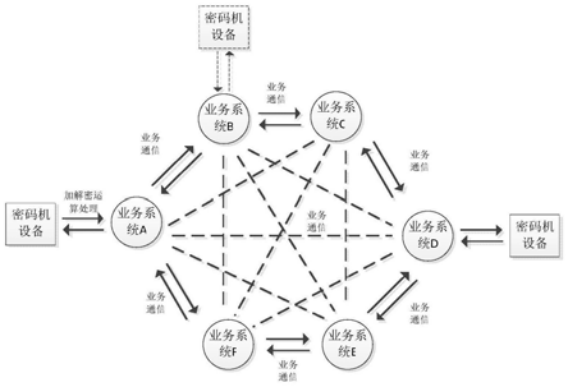
权利要求书1页 说明书4页 附图4页

(54)发明名称

网络通信管理中的散点处理方法

(57)摘要

本发明公开了一种网络通信管理中的散点处理方法，建立通信管理节点，通信管理节点集中保存了银行交易系统中所有系统的通信参数和业务功能，并提供通信参数获取接口；在业务系统客户端通过指定的通信参数获取接口从通信管理节点获取服务端通信参数后，将服务端通信参数保存在业务系统客户端的本地通信配置文件中，在进行通信交互时，业务系统客户端从本地通信配置文件中获取服务端通信参数与服务端进行通信；若通信失败，则向通信管理节点重新获取信息服务端通信参数。本发明使得银行业务系统客户端管理起来更为方便与灵活，减低系统集成成本，减低交易处理的事故风险，保障交易途径的安全性和保密性。



CN 106878378 B

1.一种网络通信管理中的散点处理方法,其特征在于:建立通信管理节点,通信管理节点集中保存了银行交易系统中所有系统的通信参数和业务功能,并提供通信参数获取接口;在业务系统客户端通过指定的通信参数获取接口从通信管理节点获取服务端通信参数后,将服务端通信参数保存在业务系统客户端的本地通信配置文件中,在进行通信交互时,业务系统客户端从本地通信配置文件中获取服务端通信参数与服务端进行通信;若通信失败,则向通信管理节点重新获取信息服务端通信参数。

2.根据权利要求1所述的网络通信管理中的散点处理方法,其特征在于:采用链路地址认证和功能权限认证方式对获取通信参数的业务系统客户端进行身份识别认证,具体实现方式如下:在通信管理节点中建立数据库预存数据,预存数据为允许访问的业务系统客户端的系统ID和链路IP,当通信管理节点收到业务系统客户端的通信参数获取请求报文时,先从报文中获取报文发起方的系统ID,并从链路中获取发起方的链路IP,然后再与数据库中的数据进行比对,比对通过,判断该系统请求的服务端实现的交易功能是否被允许,若允许,则下发服务端通信参数。

3.根据权利要求1所述的网络通信管理中的散点处理方法,其特征在于:当业务系统客户端需要将通信数据传输给服务端时,业务系统客户端先对通信数据进行MAC计算,然后拼装在通信报文中;服务端获取报文后,先对报文数据重新计算MAC,并与报文中的MAC数据进行验证,验证通过,则进行下一步处理。

4.根据权利要求1所述的网络通信管理中的散点处理方法,其特征在于:业务系统客户端和服务端先约定一把通信密钥,业务系统客户端使用该通信密钥对交易数据进行加密处理,服务端获取报文后,则使用通信密钥对交易数据进行解密处理。

网络通信管理中的散点处理方法

技术领域

[0001] 本发明涉及计算机通讯技术领域，尤其是一种网络通信管理中的散点处理方法。

背景技术

[0002] 在金融行业中，银行部门都会部署多套业务系统处理各种类型的交易。随着交易类型和交易方式的不断增加，银行的业务系统数量也不断上升。业务系统完成一项交易处理必须要与行内外其他业务系统进行通信，由于银行业务系统数量较多，并且存在较为复杂的通信关系，业务系统如散乱的通信节点分布在网络中，如何管理这些业务系统的同通信参数和通信关系，成为银行运维人员一大难点。目前在运维管理中遇到如下的问题：

[0003] 1、单一的“集中式”网络部署存在不足

[0004] “集中式”网络部署是金融行业部门业务系统网络部署中常用的一种方式，有利于集中管理，但是这也伴随着一定的风险，若管理节点系统发生故障，则对行内业务交易造成大范围的影响。如图1-图2所示，所有业务系统的业务处理都必须把业务数据发送给“集中式管理系统”进行处理，而“集中式管理系统”调用“密码机设备”进行数据加解密运算后，再把交易数据发送给其他业务系统进行处理。“集中式管理系统”若发生故障，业务系统把交易数据发送给“集中式管理系统”进行处理时，由于“集中式管理系统”故障不能处理，导致业务系统交易失败。同时也会导致银行交易大面积“瘫痪”。

[0005] 2、总线结构部署成本高

[0006] 近年来，越来越多的银行采用“总线型架构”或正在向“总线结构”迁移，虽然“总线结构”具有互联简单，易管理等优点，但是部署时行内业务系统都要根据“总线系统”发布的统一接口进行改造，并且“总线系统”的开发难度较高，如此“总线型架构”的部署成本较高。

[0007] 3、通信参数不易修改

[0008] 参与网络通信的系统必须把与之关联的其他系统的通信参数保存在本系统的网络配置文件中，若这些网络配置文件是人为手工进行配置的，那么当网络中某一节点的通信参数进行修改时，与之关联的通信系统都必须进行手工修改，如此，改动量大，影响范围广，存在滞后性，影响业务交易效率。同时，由于配置文件散落在系统中的文件中，不可避免的存在漏改情况，严重时，会造成业务中断。

[0009] 4、存在系统伪造隐患

[0010] 由于业务系统的通信信息存在人为手工进行配置情况，所以银行生产系统通信信息存在泄漏风险，若通信信息泄露，非产出环境系统未经允许与生产环境系统进行通信，则导致生产事故的发生。

发明内容

[0011] 本发明的目的是：提供了一种网络通信管理中的散点处理方法，它能避免“集中式管理系统”中由于故障不能处理，而导致业务系统交易失败的问题，避免了了导致银行交易大面积“瘫痪”，同时提高了交易的安全性，以克服现有技术不足。

[0012] 本发明是这样实现的:网络通信管理中的散点处理方法,建立通信管理节点,通信管理节点集中保存了银行交易系统中所有系统的通信参数和业务功能,并提供通信参数获取接口;在业务系统客户端通过指定的通信参数获取接口从通信管理节点获取服务端通信参数后,将服务端通信参数保存在业务系统客户端的本地通信配置文件中,在进行通信交互时,业务系统客户端从本地通信配置文件中获取服务端通信参数与服务端进行通信;若通信失败,则向通信管理节点重新获取信息服务端通信参数。这样业务系统客户端的通信参数通过"分布式"的部署方式,保证了业务处理的独立性,避免了由于有节点系统故障而带来的交易停滞的问题,同时,通过"集中式"方式管理业务系统客户端的通信参数,使得通信参数的修改与添加显得更为灵活与方便。

[0013] 为了保障通信参数获取途径的安全性,防止位置系统非法获取通信参数,采用链路地址认证和功能权限认证方式对获取通信参数的业务系统客户端进行身份识别认证,具体实现方式如下:在通信管理节点中建立数据库预存数据,预存数据为允许访问的业务系统客户端的系统ID和链路IP,当通信管理节点收到业务系统客户端的通信参数获取请求报文时,先从报文中获取报文发起方的系统ID,并从链路中获取发起方的链路IP,然后再与数据库中的数据进行比对,比对通过,判断该系统请求的服务端实现的交易功能是否被允许,若允许,则下发服务端通讯参数。该认证方式提高了交易的保密性,避免特定的交易被第三方系统介入。

[0014] 为了保障通信过程中的数据的正确性、完整性和保密性,本技术还采用了"MAC验证"方式。其原理如下:当业务系统客户端需要将通信数据传输给服务器端时,业务系统客户端先对通信数据进行MAC计算,然后拼装在通信报文中;服务端获取报文后,先对报文数据重新计算MAC,并与报文中的MAC数据进行验证,验证通过,则进行下一步处理。

[0015] 业务系统客户端和服务端先约定一把通信密钥,业务系统客户端使用该通信密钥对交易数据进行加密处理,服务端获取报文后,则使用通信密钥对交易数据进行解密处理。

[0016] 本发明采用"分布式"和"集中式"双结合的网络部署方式,以"分布式"为主,"集中式"为辅,设定一个"通信管理节点",该节点只实现唯一功能:集中保存了银行交易系统中所有业务系统客户端的通信参数和业务功能,并提供通信参数获取接口,让业务系统客户端系统获取服务端通信参数。交易数据的传送,则由业务系统客户端两两通信进行交互,不存在中间管理节点进行数据处理与转发。

[0017] 与现有的技术相比,本发明使得银行业务系统客户端管理起来更为方便与灵活,减低系统集成成本,减低交易处理的事故风险,保障交易途径的安全性和保密性。并且本发明原理简单,操作难度低,适用性广,使用效果好。

附图说明

[0018] 附图1-2为现有技术的工作原理流程示意图;

[0019] 附图3为本发明的分布式系统业务通信流程图;

[0020] 附图4为本发明的通信参数获取处理流程图;

[0021] 附图5为本发明的通信管理节点身份认证处理流程图;

[0022] 附图6为本发明的交易数据处理节点间处理流程图;

[0023] 附图7为本发明的通信管理节点对伪造系统识别处理流程;

[0024] 附图8为本发明的实施例的通信管理结构图。

具体实施方式

[0025] 下面结合附图对本发明作进一步的详细说明，但不作为对本发明的任何限制

[0026] 本发明的实施例：网络通信管理中的散点处理方法，申请人在贵州银行“通信管理平台”上进行测试。贵州银行行内60多套业务系统客户端的通信信息和业务功能统一登记在“通信管理平台”中(即通信管理节点)，通信管理节点统一提供系统登记接口和业务功能接口，让行内业务系统客户端调用。每新增一个服务端，该服务端则通过“通信管理平台”注册该系统的通信参数和功能，而业务系统客户端在调用服务功能接口前，也需在“通信管理平台”中登记其业务功能和通信参数，在调用功能接口时，功能接口内部则向服务器端发送报文获取服务端的通讯参数，并把通信参数保存在业务系统客户端的本地通信配置文件中，然后进行交易运行，并把交易信息直接发送给服务器端进行交易验证。

[0027] 如图3所示，各个业务系统客户端独立完成交易数据的处理，并直接发送给其它业务系统客户端。若其中一个节点发生故障，不会影响其它业务系统客户端的正常业务处理。

[0028] 如图4所示，服务端调用特定的接口，往“通信管理平台”注册本系统的IP地址和端口，业务系统客户端则通过报文方式向“通信管理平台”获取服务端的IP和端口，获取成功后，则与服务器端进行业务通信。

[0029] 如图6所示，两个业务系统先约定一把通信密钥，业务系统客户端(前端系统)使用该通信密钥对交易数据进行加密处理，并对通信报文进行MAC计算。服务端(后端业务系)统获取报文后，先进行MAC重新进行和验证，再使用通信密钥对交易数据进行解密处理。

[0030] 如图7所示，“通信管理平台”对伪造系统先进行报文MAC验证，即使验证成功，“通信管理平台”还会对伪造系统进行身份识别，通过身份识别处理，辨认出请求系统为伪造，返回错误信息。

[0031] 如图8所示，在应用系统规划时，要求核心系统，合作系统群，管理系统群实现渠道无关，通过通讯管理系统以及通讯和报文标准化，贵州银行生产系统无需部署渠道整合平台、应用整合平台产品。

[0032] 该方案在享受到SOA架构提供的优越性的同时，简化了生产系统的结构，是生产系统稳定运行的基础。对于这两个平台提供的具体功能，比如说统一认证等，可以部署独立的管理系统实现。

[0033] 上述实施的通信管理系统提供了对SOA架构的支持。由于XML交易报文的低效，目前大中型银行没有采用XML报文作为核心系统交易报文的例子。而贵州银行拟参考相关国际标准，选定高效的行内标准报文格式，作为全行所有系统间联机交易的标准接口。

[0034] 在报文标准确定后，贵州银行拟提供主流开发语言的标准通讯接口程序，实现系统间的相互访问功能。同时在标准通讯接口程序中集成相关安全管理功能。

[0035] 标准通讯接口程序通过访问通讯管理系统，可以获得其有权限访问的所有行内系统的通讯参数，从而实现相关系统的透明访问。

[0036] 在新产品、业务管理系统上线或者更新时，需要向通讯管理系统汇报通讯等相关参数，其他系统通过标准通讯接口程序自动获取相应参数，以便支撑交易执行。

[0037] 以上所述，仅是本发明的较佳实例而已，并非对本发明做任何形式上的限制，任何

未脱离本发明技术方案内容,依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰,均仍属于本发明技术方案的范围内。

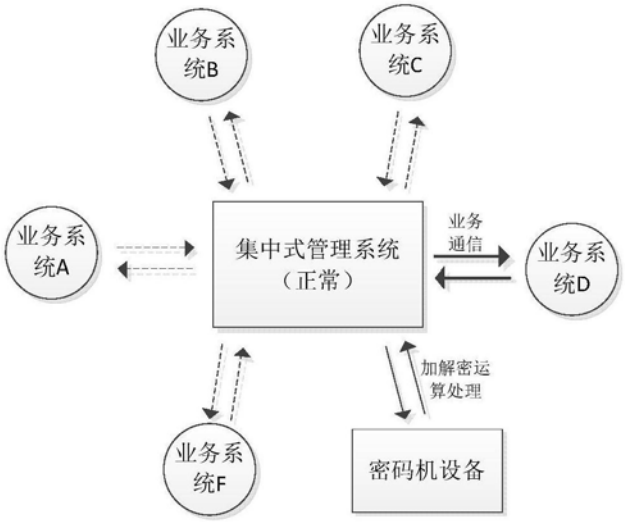

业务系统B
业务系统C
业务系统A
集中式管理系统（正常）
业务通信
业务系统D
加解密运算处理
业务系统F
密码机设备

图1

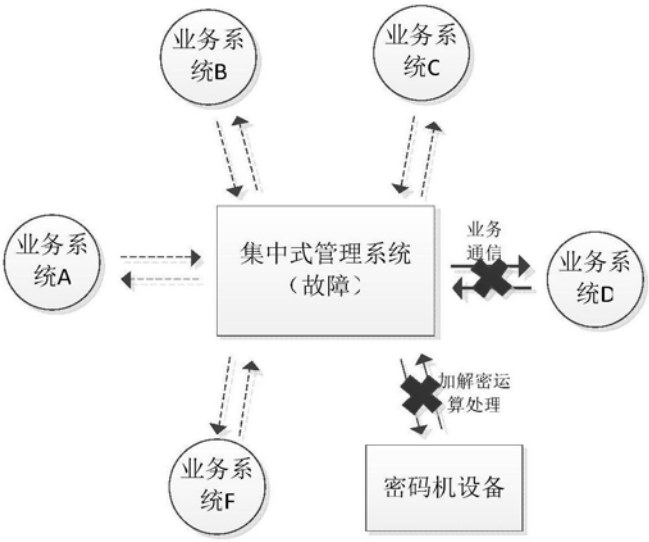

业务系统B
业务系统C
业务系统A
集中式管理系统（故障）
业务通信
业务系统D
加解密运算处理
业务系统F
密码机设备

图2

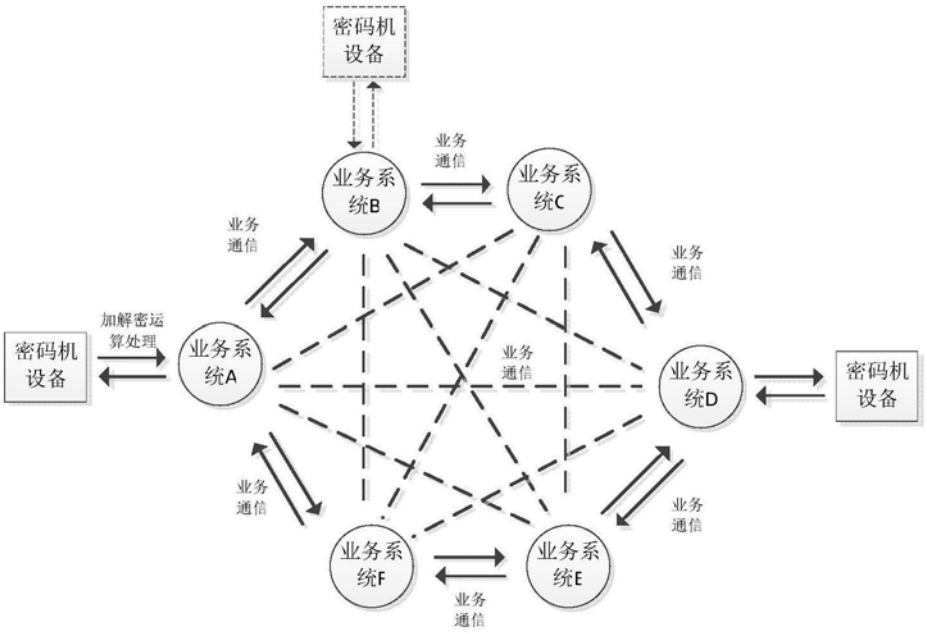

密码机设备
业务通信
业务系统B
业务系统C
业务通信
业务通信
业务通信
加解密运算处理
密码机设备
业务系统A
业务通信
业务系统D
密码机设备
业务通信
业务通信
业务系统F
业务系统E
业务通信

图3

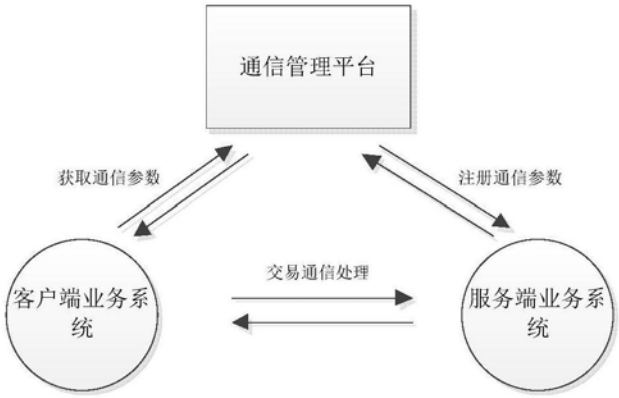

通信管理平台
获取通信参数
注册通信参数
客户端业务系统
交易通信处理
服务端业务系统

图4


拆解报文
报文MAC验证
获取请求系统ID和业务功能
获取链路IP
链路IP认证
系统功能认证
下发服务端通信参数

图5

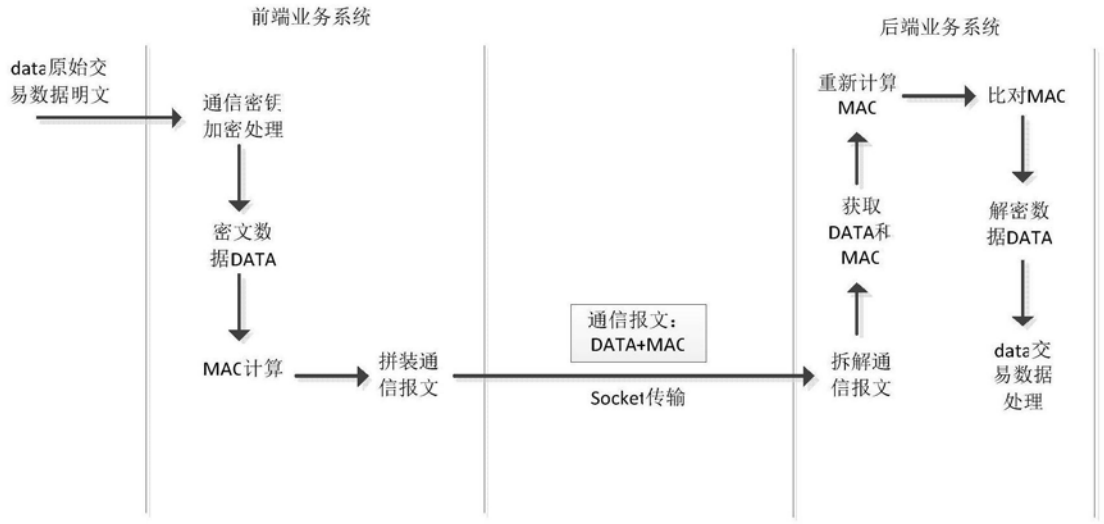

前端业务系统
后端业务系统
data原始交易数据明文
通信密钥加密处理
密文数据DATA
MAC计算
拼装通信报文
通信报文：DATA+MAC
Socket传输
拆解通信报文
获取DATA和MAC
重新计算MAC
比对MAC
解密数据DATA
data交易数据处理

图6

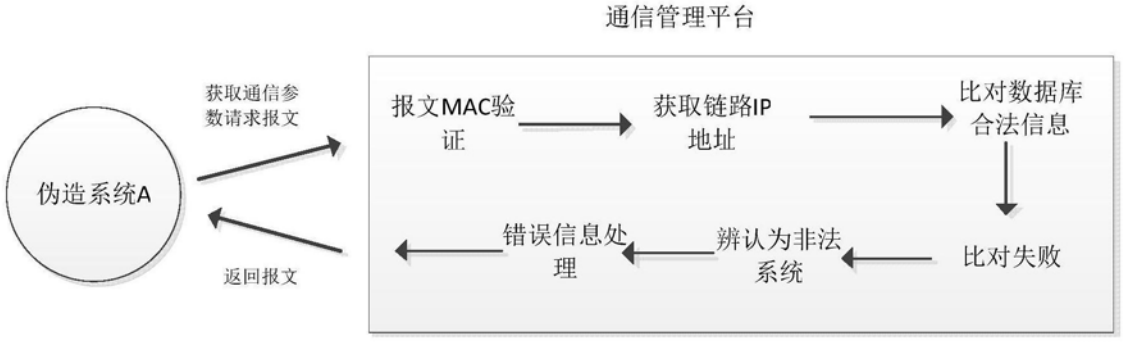

通信管理平台
伪造系统A
获取通信参数请求报文
返回报文
报文MAC验证
获取链路IP地址
比对数据库合法信息
比对失败
辨认为非法系统
错误信息处理

图7

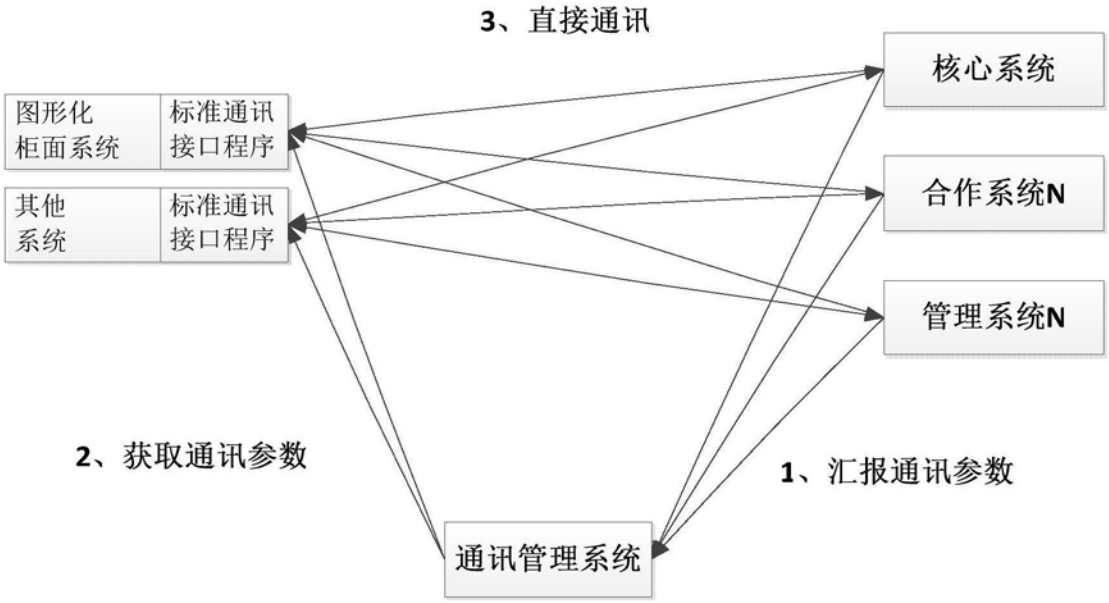

3、直接通讯
核心系统
图形化
柜面系统
标准通讯
接口程序
合作系统N
其他
系统
标准通讯
接口程序
管理系统N
2、获取通讯参数
1、汇报通讯参数
通讯管理系统

图8