(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 106452749 B
(45)授权公告日 2019.06.07

(21)申请号 201610906310.9

(22)申请日 2016.10.18

(65)同一申请的已公布的文献号
申请公布号 CN 106452749 A

(43)申请公布日 2017.02.22

(73)专利权人 北京骏逸通达信息服务有限公司
地址 100085 北京市海淀区知春路6号锦秋国际A座404室

(72)发明人 王雷 庄迅

(74)专利代理机构 北京高文律师事务所 11359
代理人 徐江华

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04W 12/02(2009.01)
H04W 84/06(2009.01)

(56)对比文件
CN 103684788 A,2014.03.26,
CN 1240547 A,2000.01.05,
US 2014351915 A1,2014.11.27,
US 6738902 B1,2004.05.18,
CN 103944878 A,2014.07.23,

审查员 张洁

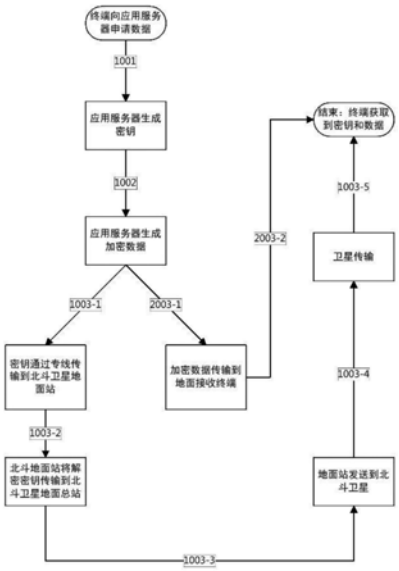
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种通过卫星通信进行密钥和数据分离传输的方法及系统

(57)摘要

本发明提供一种通过卫星通信进行密钥和数据分离传输的方法及系统，该技术在地面应用服务器和移动接收端使用双路由技术，使用卫星路由(如北斗)通信网络传输密钥，使用地面互联网路由传输加密数据。发送端和地面接收端通过卫星通信网络传递加密算法和交换密钥。本发明在物理链路层面进行分离传输，极大限度避免了传输中被同时窃取的可能性，从而解决传输安全问题。



CN 106452749 B

1.一种通过卫星通信进行密钥和数据分离传输的方法,包括下列步骤:

(1)应用服务器收到客户端的加密请求后生成密钥,利用该密钥对需要传输的数据进行加密;

(2)应用服务器采用双路由技术,实现了在数据包分发时将密钥包绑定空中路径、加密数据绑定地面路径,密钥路径设定密钥从应用服务器经专线,将密钥发送到北斗卫星地面站的服务器上,按卫星路由进行空中传输抵达地面移动接收端,加密数据路由设定加密数据从应用服务器通过地面互联网传输到地面移动接收端;

(3)卫星地面站服务器将密钥发送北斗地面卫星总站,卫星总站设定空间路由,将密钥传到空间卫星网络,密钥的空中传输路径由卫星系统决定;

(4)地面移动接收端使用卫星数据接收模块从卫星网络接收密钥,使用wifi或6G/5G/4G/3G模块从地面互联网获取加密数据,然后加解密模块用密钥对地面数据解密。

2.根据权利要求1所述的通过卫星通信进行密钥和数据分离传输的方法,其特征在于:所述地面接收端的设备上需要安装客户端软件或者集成SDK,所述客户端软件或集成SDK能够通过卫星网络获取密钥,并自动同步应用服务器的配置信息进行加解密操作。

3.根据权利要求1所述的通过卫星通信进行密钥和数据分离传输的方法,其特征在于:所述密钥和加密数据通过信密分离传输时,卫星网络和地面互联网使用TCP/IP传输协议分别传输密钥和加密数据。

4.根据权利要求1所述的通过卫星通信进行密钥和数据分离传输的方法,其特征在于:步骤(1)中,客户端通过本地卫星接收端向应用服务器发起数据申请请求,应用服务器接收到客户端的请求后,生成非对称密钥。

5.根据权利要求1所述的通过卫星通信进行密钥和数据分离传输的方法,其特征在于:所述客户端发送数据请求时同时发送自身的卫星定位信息,能够指定数据解密的卫星定位范围,在接收数据和密钥后需要由应用服务器进行确认,解密数据前通过客户端软件或者集成SDK结合定位装置发送当时的卫星定位信息,由应用服务器判断是否在卫星定位范围内,超出则不予确认,符合则确认后进行解密。

6.根据权利要求4所述的通过卫星通信进行密钥和数据分离传输的方法,其特征在于:所述客户端能够首先在应用服务器进行信息登记,发起数据申请请求时由应用服务器对客户端采集的客户信息进行确认,然后判断是否发送数据,所述客户信息包括客户的指纹、面部识别、密码、终端设备信息或终端软件ID。

7.一种通过卫星通信进行密钥和数据分离传输的系统,其特征在于:包括应用服务器、密钥专线、接收端,所述应用服务器包括密钥生成模块、双路由算法分发模块,所述接收端包括卫星信号接收模块、解码模块、数据加密解密模块;所述双路由算法分发模块用于实现信密分离传输,密文数据按自定义路由走互联网通道,进行单独传输,跟密钥专线区分开;所述解码模块对卫星信号接收模块接收后的密钥信号实现数据解码,对通过地面互联网传输的加密数据进行数据解码;所述数据加密解密模块利用卫星传输的密钥对加密数据进行加解密。

8.根据权利要求7所述的通过卫星通信进行密钥和数据分离传输的系统,其特征在于:所述应用服务器还包括确认模块和信息检测模块,所述确认模块用于确认客户端的客户信息,包括指纹识别模块、实时面部识别模块;所述信息检测模块用于接收客户端的卫星定位

信息。

9.根据权利要求7所述的通过卫星通信进行密钥和数据分离传输的系统，其特征在于：所述解码模块匹配硬件厂商相应型号的硬件驱动程序，解密后的数据及密钥不以任何文件形式存储在本地，都储存在RAM中，减少被木马窃取的可能性，跟客户端软件之间通过运行在内存中的全局变量通信。

10.根据权利要求7所述的通过卫星通信进行密钥和数据分离传输的系统，其特征在于：所述密钥生成模块针对每个业务每次单独生成密钥，每笔业务的密钥都根据请求动态生成。

一种通过卫星通信进行密钥和数据分离传输的方法及系统

技术领域

[0001] 本发明涉及一种卫星网传输密钥和信密分离的方法，尤其是涉及一种通过卫星通信进行密钥和数据分离传输的方法及系统。

背景技术

[0002] 目前密钥和数据共同使用互联网链路传输，有在传输时同时泄露的风险。现有技术的缺点在于互联网是开放的数据链路，密钥和数据都使用互联网传输很容易被同时截取并解密。现有软件只能按单一路由原则进行数据传输，不能解决密钥和加密数据分别按空中地面两条路径的传输问题。

发明内容

[0003] 本发明提供了一种通过卫星通信进行密钥和数据分离传输的方法及系统，解决了密钥和数据都使用互联网传输很容易被同时截取并解密的问题，采用加密数据和密钥分开传输：A通道是互联网，传加密数据；B通道是卫星网，传密钥。在物理链路层面进行分离传输，极大限度避免了传输中为同时窃取的可能性，从而解决传输安全问题。其技术方案如下所述：

[0004] 一种通过卫星通信进行密钥和数据分离传输的方法，包括下列步骤：

[0005] (1)应用服务器收到客户端的加密请求后生成密钥，利用该密钥对需要传输的数据进行加密；

[0006] (2)应用服务器采用双路由技术，实现了在数据包分发时将密钥包绑定空中路径、加密数据绑定地面路径，所述密钥路径设定密钥从应用服务器经专线，将密钥发送到北斗卫星地面站的服务器上，按卫星路由进行空中传输抵达接收端，加密数据路由设定加密数据从应用服务器通过地面互联网传输到地面移动接收端；

[0007] (3)卫星地面站服务器将密钥发送北斗地面卫星总站，卫星总站设定空间路由，将密钥传到空间卫星网络，密钥的空中传输路径由卫星系统决定；

[0008] (4)客户端的地面接收端使用卫星数据接收模块从卫星网络接收密钥，使用wifi或6G/5G/4G/3G模块从地面互联网获取加密数据，然后加解密模块用密钥对地面数据解密。

[0009] 所述地面接收端的设备上需要安装客户端软件或者集成SDK，所述客户端软件或集成SDK能够通过卫星网络获取密钥，并自动同步服务器端的配置信息进行加解密操作。

[0010] 所述密钥和加密数据通过信密分离传输时，卫星网络和地面互联网使用TCP/IP传输协议分别传输密钥和加密数据。

[0011] 步骤(1)中，客户端通过本地卫星接收端向应用服务器发起数据申请请求，应用服务器接收到客户端的请求后，生成非对称密钥。

[0012] 所述客户端发送数据请求时同时发送自身的卫星定位信息，能够指定数据解密的卫星定位范围，在接收数据和密钥后需要由应用服务器进行确认，解密数据前通过客户端软件或者集成SDK结合定位装置发送当时的卫星定位信息，由应用服务器判断是否在卫星

定位范围内，超出则不予确认，符合则确认后进行解密。

[0013] 所述客户端能够首先在应用服务器进行信息登记，发起数据申请请求时由应用服务器对客户端采集的客户信息进行确认，然后判断是否发送数据，所述客户信息包括客户的指纹、面部识别、密码、终端设备信息或终端软件ID。

[0014] 一种通过卫星通信进行密钥和数据分离传输的系统，包括应用服务器、密钥专线、接收端，所述应用服务器包括密钥生成模块、双路由算法分发模块，所述接收端包括卫星信号接收模块、解码模块、数据加密解密模块；所述双路由算法分发模块用于实现信密分离传输，密文数据按自定义路由走互联网通道，进行单独传输，跟密钥专线区分开；所述解码模块对卫星信号接收模块接收后的密钥信号实现数据解码，对通过地面互联网传输的加密数据进行数据解码；所述数据加密解密模块利用卫星传输的密钥对加密数据进行加解密。

[0015] 所述应用服务器还包括确认模块和信息检测模块，所述确认模块用于确认客户端的客户信息，包括指纹识别模块、实时面部识别模块；所述信息检测模块用于接收客户端的卫星定位信息。

[0016] 所述解码模块匹配硬件厂商相应型号的硬件驱动程序，解密后的数据及密钥不以任何文件形式存储在本地，都储存在RAM中，减少被木马窃取的可能性，跟客户端软件之间通过全局变量通信。

[0017] 所述密钥生成模块针对每个业务每次单独生成密钥，每笔业务的密钥都根据请求动态生成，并根据需求将密钥生命期设置成极短，极大提高破解难度。

[0018] 本发明具有以下优点：

[0019] 1、因为利用卫星网络(如北斗)传输密钥，具备军用传输级别的链路安全；

[0020] 2、因为使用了双路由算法，所以加密数据和密钥可以沿地面和空中两种不同的路径传播；

[0021] 3、因为密钥和数据分别使用不同通道传输，所以加密数据和密钥同时被泄露的概率大幅度降低；

[0022] 4、因为地面接收端使用软件向卫星(如北斗)获取密钥，所以可以通过本系统的日志信息和位置记录进行逆向追踪，通过历史记录可追查到每台终端设备。

附图说明

[0023] 图1是本发明中北斗卫星进行密钥分离传输的实际步骤图；

[0024] 图2是本发明中涉及方法的实施例的流程示意图。

具体实施方式

[0025] 本发明提供的通过卫星通信进行密钥和数据分离传输的方法及系统，该技术在地面应用服务器和移动接收端使用双路由技术，使用卫星路由(如北斗)通信网络传输密钥，使用地面互联网路由传输加密数据。发送端和地面接收端通过卫星通信网络传递加密算法和交换密钥。

[0026] 如图1所示，具体传输流程如下所述：

[0027] 步骤A、应用服务器收到加密请求后使用常规方法生成密钥，利用该密钥对数据进行加密。

[0028] 步骤B、应用服务器根据独创双路由技术，实现了在数据包分发时将密钥包绑定空中路径、加密数据绑定地面路径。密钥路径设定密钥从应用服务器经专线，将密钥发送到北斗卫星地面站的服务器上，按卫星路由进行空中传输抵达接收端。加密数据路由设定加密数据从应用服务器通过地面互联网传输到地面移动接收端。

[0029] 步骤C、卫星(如北斗)地面站服务器将密钥发送北斗地面卫星总站。

[0030] 步骤D、卫星(如北斗)总站设定空间路由，将密钥传到空间卫星网，密钥的空中传输路径由卫星系统决定。

[0031] 步骤E、地面接收端使用卫星数据接收模块从卫星网络接收密钥，使用wifi或6G/5G/4G/3G模块从地面互联网获取加密数据，然后加解密模块用密钥对地面数据解密。

[0032] 地面接收端设备上需要安装客户端软件或者集成SDK，该客户端软件(或SDK)可以通过卫星网络获取密钥，并自动同步服务器端的配置信息进行加解密操作。

[0033] 本发明的关键点在于：将密钥和加密数据分开传输，使用空中卫星网络传输密钥，应用服务器传输密钥和加密数据的时候使用双路由分离传输算法，加密数据通过地面互联网传输到接收方后，接收方再通过卫星下载密钥。

[0034] 为了保证数据安全，进一步的，所述客户端发送数据请求时同时发送自身的卫星定位信息，能够指定数据解密的卫星定位范围，在接收数据和密钥后需要由应用服务器进行确认，解密数据前通过客户端软件或者集成SDK结合定位装置发送当时的卫星定位信息，由应用服务器判断是否在卫星定位范围内，超出则不予确认，符合则确认后进行解密。

[0035] 所述客户端能够首先在应用服务器进行信息登记，发起数据申请请求时由应用服务器对客户端采集的客户信息进行确认，然后判断是否发送数据，所述客户信息包括客户的指纹、面部识别或密码。

[0036] 密钥和加密数据通过信密分离传输的方法，卫星网络和互联网使用TCP/IP传输协议分别传输密钥和加密数据。

[0037] 本方法涉及到的系统，包括应用服务器、密钥专线、接收端，所述应用服务器包括密钥生成模块、双路由算法分发模块，所述接收端包括卫星信号接收模块、解码模块、数据加密解密模块；所述应用服务器还包括确认模块和信息检测模块，所述确认模块用于确认客户端的客户信息，包括指纹识别模块、实时面部识别模块；所述信息检测模块用于接收客户端的卫星定位信息。

[0038] 数据和密钥会涉及到密钥通道、卫星网络和数据通道。

[0039] 密钥通道：

[0040] 数据专线连接卫星地面站，使用地面数据专线连接应用服务器和卫星地面站。特点是：应用服务器与卫星地面站之间用专线连接，实现链路安全。

[0041] 卫星网络：使用卫星网络连接地面站发送端和接收端。特点是：信密分离传输，密钥传输使用卫星网络传输，不走目前的互联网通道。

[0042] 数据通道：地面互联网传输加密后的数据通过地面互联网传输。特点是：信密分离传输，密文数据按自定义路由走互联网通道单独传输，跟密钥通道区分开。特点：传统方法使用相同通道传输密钥和加密数据，本方案将密钥和加密数据分别用各自独立通道传输，从物理链路层面增加了整体安全性。

[0043] 那么，接收端包括：

[0044] 卫星信号接收模块:此模块为通用卫星接收硬件电子模块,用于实现与通信卫星的物理网络连接。接收到卫星传送过来的密钥信号后,软件用于解码和组装数据。

[0045] 解码模块:匹配主要硬件厂商如MTK、北斗等相应型号的硬件驱动程序,对模块接收后实现数据解码。特点:解密后的数据及密钥不以任何文件形式存储在本地,都储存在RAM中,减少被木马窃取的可能性,跟客户端软件之间通过全局变量通信。

[0046] 数据加密解密模块:利用卫星传输的密钥对加密数据进行加解密。特点在于:软件通过通用卫星模块和互联网模块接收卫星端的密钥以及互联网的加密数据。

[0047] 发送端包括:

[0048] 密钥生成模块:针对每个业务每次单独生成密钥。特点在于一次一密,每笔业务的密钥都根据请求动态生成,软件将密钥生命期设置成极短,极大提高破解难度。

[0049] 双路由算法:为密钥和加密数据分别使用密钥路由和数据路由两种路径。双路由算法包含地面网络路由和卫星网络路由。数据路由指定加密数据的传输路径,其路径为地面互联网。密钥路由指定密钥在空中的传输路径,其路径为卫星网络。特点在于:打破传统单路由传输思路,首创为不同数据设定截然不同的两种路由同时传输,首创空中地面的双路由方法。

[0050] 下面以北斗卫星网络数据密钥分离传输实施为例,对本发明作进一步说明,但不作为对本发明的限定。

[0051] 如图2所示,下面就详细步骤进行一一说明:

[0052] 步骤1001(终端向应用服务器申请数据):通过本地卫星接收端向应用服务器发起数据申请请求。

[0053] 步骤1002(应用服务器生成密钥):应用服务器接收到客户端的请求后(如https请求),生成非对称密钥。

[0054] 步骤1003-1(应用服务器生成加密数据):应用服务器接收到客户端的请求后(如https请求),利用密钥对数据进行加密。

[0055] 步骤1003-2(密钥通过专线传输到北斗卫星地面站):密钥经过地面专线传输到北斗卫星地面站的服务器上。

[0056] 步骤1003-3(北斗地面站将解密密钥传输到北斗卫星地面总站):地面站服务器将密钥通过北斗地面网络传输到北斗卫星地面总站。

[0057] 步骤1003-4(地面站发送到北斗卫星):北斗地面总站将密钥经过对空信号发送装置传递到接入卫星。

[0058] 步骤1003-5(卫星传输):密钥在北斗卫星网络间按北斗的卫星路由规则传输

[0059] 步骤2003-1(应用服务器生成加密数据):应用服务器接收到客户端的请求后(如https请求),利用密钥对数据进行加密。

[0060] 步骤2003-2(终端获取到密钥和数据):加密数据通过地面互联网传输到接收终端

[0061] 结束:地面接收终端获取到空中传输过来的密钥和地面传输过来的加密数据,客户端利用密钥对加密数据进行解密。

[0062] 以上所述的实施案例,只是本发明较优选的具体实施方式的一种,本领域的技术人员在本发明技术方案范围内进行的通常变化和替换都应包含在本发明的保护范围内。

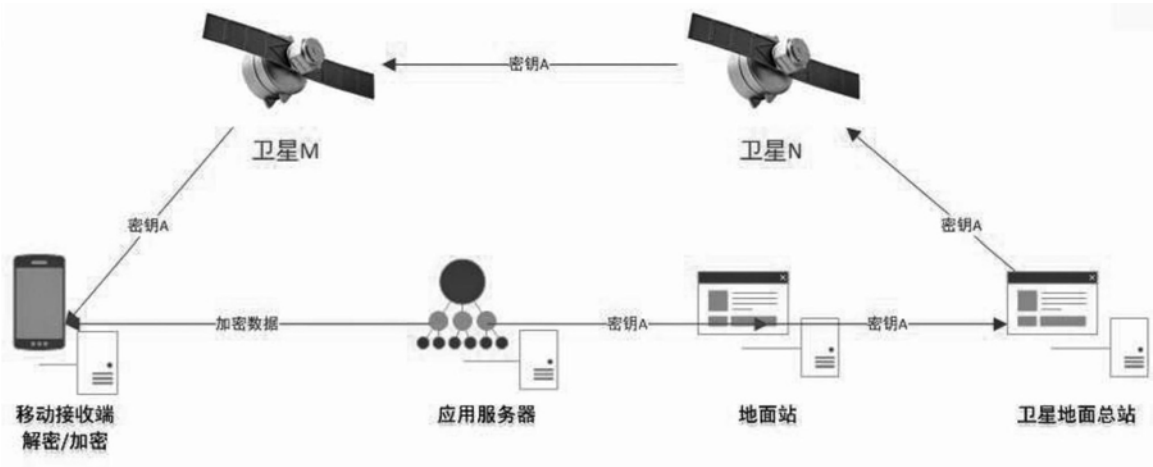


图1

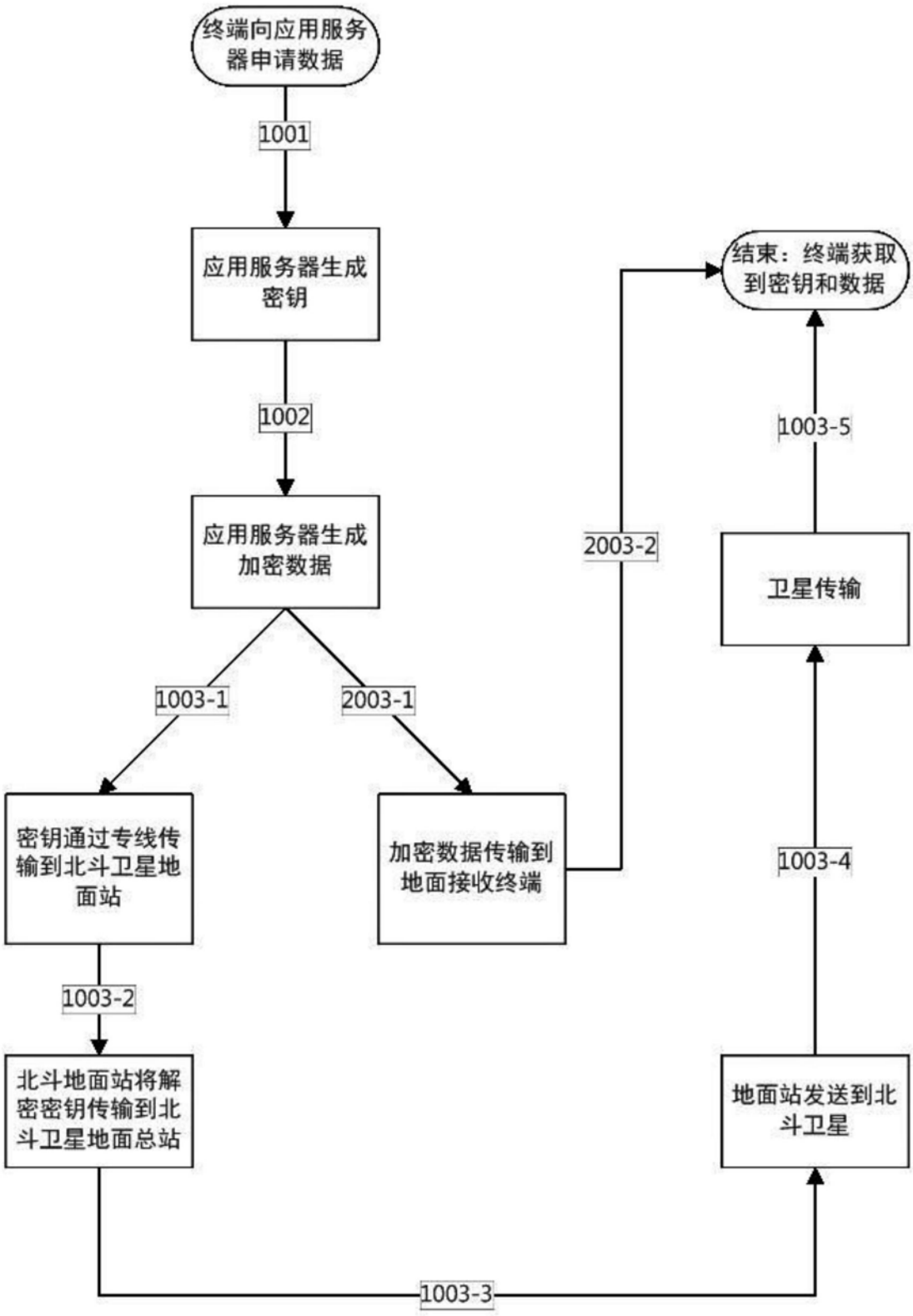

终端向应用服务器申请数据
1001
应用服务器生成密钥
1002
应用服务器生成加密数据
1003-1
2003-1
密钥通过专线传输到北斗卫星地面站
1003-2
北斗地面站将解密密钥传输到北斗卫星地面总站
1003-3
地面站发送到北斗卫星
1003-4
卫星传输
1003-5
结束：终端获取到密钥和数据
2003-2
加密数据传输到地面接收终端

图2