(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 109039436 B
(45)授权公告日 2020.09.15

(21)申请号 201811234172.X

(22)申请日 2018.10.23

(65)同一申请的已公布的文献号
申请公布号 CN 109039436 A

(43)申请公布日 2018.12.18

(73)专利权人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 王利明 王建凯 宋晨

(74)专利代理机构 北京科迪生专利代理有限责任公司 11251
代理人 安丽 邓治平

(51)Int.Cl.
H04B 7/185(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04W 12/06(2009.01)
H04W 12/08(2009.01)

(56)对比文件
US 2008170536 A1,2008.07.17
US 5913164 A,1999.06.15
CN 101873652 A,2010.10.27
WO 2010051308 A1,2010.05.06
CN 103648132 A,2014.03.19

审查员 袁悦

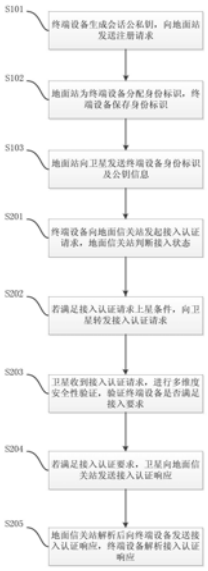
权利要求书3页 说明书13页 附图3页

(54)发明名称

一种卫星安全接入认证的方法及系统

(57)摘要

本发明公开了一种卫星安全接入认证方法及系统，包括：终端设备发起注册过程，地面站向终端设备分配身份标识，地面站向卫星发送终端设备身份信息，完成终端设备注册过程。终端设备发起接入认证请求，地面信关站判断接入状态，卫星收到接入认证请求，多维度验证后向终端设备发送接入认证响应，完成终端设备接入认证过程。当前连接卫星发生过顶时，地面信关站向新连接卫星发起接续认证请求，卫星收到接续认证请求，多维度验证后向地面信关站发送接续认证响应，完成终端设备接续认证过程。终端设备发起登出认证请求，地面信关站判断接入状态，卫星收到登出认证请求，多维度验证后向终端设备发送登出认证响应，完成终端设备登出认证过程。



CN 109039436 B

1.一种卫星安全接入认证方法,其特征在于,包括以下步骤:

S101:终端设备生成会话公私钥,并携带公钥及固有信息向地面站发送注册请求;

S102:所述地面站为所述终端设备分配身份标识,向所述终端设备发送注册响应,所述终端设备保存身份标识;

S103:所述地面站向卫星发送终端注册上注请求,卫星解析保存所述终端设备身份标识及所述公钥信息,完成所述终端设备注册;

S201:终端设备向地面信关站发送接入认证请求消息,所述地面信关站判断所述终端设备接入状态;

S202:若满足接入认证请求消息上星条件,所述地面信关站向卫星转发接入认证请求消息;

S203:所述卫星收到接入认证请求消息,进行多维度安全性验证,所述多维度安全性验证包括:接收到的接入认证请求消息中的终端设备信息是否已注册,所述接入认证请求消息中的校验位校验是否通过,以及所述接入认证请求消息中的时间戳是否在允许时间范围内,验证所述终端设备是否满足接入认证要求;

S204:若满足接入认证要求,计算所述终端设备接入失效时刻,所述卫星向所述地面信关站发送接入认证响应消息;

S205:所述地面信关站解析接入认证响应消息,获取所述终端接入失效时刻,向所述终端设备发送接入认证响应消息,所述终端设备解析接入认证响应消息,完成所述终端设备接入认证;

S301:地面信关站向新连接卫星发起接续认证请求,提供当前已接入终端设备列表;

S302:所述卫星收到接续认证请求,进行多维度安全性验证,所述多维度安全性验证包括:接收到的接续认证请求消息中的已接入终端设备列表包括的终端设备信息是否已注册,所述接续认证请求消息中的校验位校验是否通过,以及所述接续认证请求消息中的时间戳是否在允许时间范围内;验证所述已接入终端设备列表中设备是否满足接续认证要求;

S303:若满足接续认证要求,所述卫星向所述地面信关站发送接续认证响应消息;

S304:所述地面信关站解析接续认证响应消息,更新所述已接入终端设备列表,完成终端设备接续认证过程;

S401:终端设备向地面信关站发送登出认证请求消息,所述地面信关站判断所述终端设备接入状态;

S402:若满足登出认证请求消息上星条件,所述地面信关站向卫星转发登出认证请求消息;

S403:所述卫星收到登出认证请求消息,进行多维度安全性验证,所述多维度安全性验证包括:接收到的登出认证请求消息中的终端设备信息是否已注册,所述登出认证请求消息中的校验位校验是否通过,以及所述登出认证请求消息中的时间戳是否在允许时间范围内,验证所述终端设备是否满足登出认证要求;

S404:若满足登出认证要求,销毁所述终端设备接入状态,所述卫星向所述地面信关站发送登出认证响应消息;

S405:所述地面信关站解析登出认证响应消息,销毁所述终端设备接入状态,向所述终

端设备发送登出认证响应消息，所述终端设备解析登出认证响应消息，完成所述终端设备登出认证。

2.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S102中，所述地面站需要为所述终端设备分配唯一且尚未分配的身份标识；所述身份标识包括终端设备类型标识、归属域及终端设备识别码。

3.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S103中，所述终端注册上注请求消息至少包括以下一种类型：增加新注册终端设备的身份标识及公钥、或删除已注册终端设备的全部信息。

4.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S201中，所述终端设备向所述地面信关站发送接入认证请求消息中，至少包括：终端设备身份信息、发送时刻时间戳，以及采用安全策略生成的校验位；所述地面信关站收到所述接入认证请求消息后，根据所述接入认证请求消息中的终端设备身份信息判断所述终端设备接入状态，根据所述接入认证请求消息中的时间戳验证是否发生重放攻击。

5.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S202中，所述接入认证请求消息上星条件包括：所述终端设备尚未接入、以及所述接入认证请求消息不符合重放攻击的特征，所述重放攻击是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的。

6.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S204中，所述接入认证要求为通过所述多维度安全性验证，所述卫星向所述地面信关站发送接入认证响应消息中，至少包括：所述终端设备身份信息、所述终端设备接入失效时刻，以及所述终端设备接入结果。

7.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S205中，所述地面信关站需要保存所述终端设备的接入状态，所述地面信关站向所述终端设备发送接入认证响应消息中，至少包括：所述终端设备身份信息，以及所述终端设备接入结果。

8.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S301中，所述地面信关站向所述卫星发送接续认证请求消息中，至少包括：已接入终端设备列表、发送时刻时间戳，以及采用安全策略生成的校验位。

9.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S303中，所述接续认证要求为通过所述多维度安全性验证，所述卫星向所述地面信关站发送接续认证响应消息中，至少包括：通过验证的终端设备身份信息及接续失效时刻列表。

10.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S304中，所述地面信关站需要更新所述已接入终端设备列表中的终端设备接续失效时刻。

11.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S401中，所述终端设备向所述地面信关站发送登出认证请求消息中，至少包括：终端设备身份信息、发送时刻时间戳，以及采用安全策略生成的校验位；所述地面信关站收到所述登出认证请求消息后，根据所述登出认证请求消息中的终端设备身份信息判断所述终端设备接入状态，根据所述登出认证请求消息中的时间戳验证是否发生重放攻击。

12.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S402中，所述登出认证请求消息上星条件包括：所述终端设备已接入、以及所述登出认证请求消息不符合重

放攻击的特征，重放攻击是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的。

13.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S404中，所述登出认证要求为通过所述多维度安全性验证，所述卫星向所述地面信关站发送登出认证响应消息中，至少包括：所述终端设备身份信息、以及所述终端设备登出结果。

14.根据权利要求1所述的卫星安全接入认证方法，其特征在于：所述S405中，所述地面信关站需要清除所述终端设备的接入状态，所述地面信关站向所述终端设备发送登出认证响应消息中，至少包括：所述终端设备身份信息，以及所述终端设备登出结果。

15.一种卫星接入认证服务系统，其特征在于，包括：组网卫星、终端设备、地面信关站和地面站；组网卫星，指卫星网络中同一或不同轨道上多种类型的卫星系统；终端设备用于接收组网卫星提供的服务，与地面信关站之间进行通信，并通过地面信关站与卫星通信；地面信关站为一种中间可信设备，用于连接终端设备与组网卫星之间的通信；地面站用于为终端设备分配身份标识，向组网卫星上注终端设备身份信息；

所述组网卫星包括：安全接入模块，用于接收地面站发送的终端注册上注请求，以及接受地面信关站发送的接入认证请求消息、接续认证请求消息、登出认证请求消息，判断是否对接入认证请求消息、接续认证请求消息、登出认证请求消息进行响应以及向地面信关站发送接入认证响应消息、接续认证响应消息、登出认证响应消息；

所述终端设备包括安全注册模块、安全接入认证模块、安全接续认证模块和安全登出认证模块，其中：

所述安全注册模块，用于生成安全注册请求消息，解析安全注册响应消息，保存身份标识；

所述安全接入认证模块，用于生成安全接入认证请求消息，向地面信关站发送接入认证请求消息；

所述安全接续认证模块，用于生成安全接续认证请求消息，向地面信关站发送接续认证请求消息；

所述安全登出认证模块，用于生成安全登出认证请求消息，向地面信关站发送登出认证请求消息；

所述地面信关站包括安全接入认证代理模块、安全接续认证代理模块和安全登出认证代理模块，其中：

所述安全接入认证代理模块，用于判断终端设备是否具备向组网卫星请求接入网络的条件，以及转发接入认证响应消息；

所述安全接续认证代理模块，用于判断终端设备是否具备向组网卫星请求接续网络的条件，以及转发接续认证响应消息；

所述安全登出认证代理模块，用于判断终端设备是否具备向组网卫星请求登出网络的条件，以及转发登出认证响应消息；

所述地面站包括：安全注册模块，用于接收终端设备发送的安全注册请求消息，生成安全注册响应消息和终端注册上注请求消息，以及向终端设备发送安全注册响应消息、向组网卫星上注终端注册上注请求消息。

一种卫星安全接入认证的方法及系统

技术领域

[0001] 本发明属于网络安全技术领域，具体涉及一种卫星安全接入认证的方法及系统。

背景技术

[0002] 随着地面因特网的不断发展，利用卫星网络为全球任何地方任何用户提供网络服务，构筑“天地一体化网络”成为卫星网络发展的重要趋势。而卫星网络在很大程度上有别于传统地面网络。一方面，与传统地面网络相比，空间网络具有更强的开放性特点，这就使得安全性对天地一体化网络中的通信至关重要；另一方面，由于卫星的高速动态移动，为保证业务服务不中断，地面信关站需要在不同卫星间频繁地进行终端设备会话接续，整个过程对于终端设备而言是透明的。尤其是在终端接入这一特殊的通信场景下，系统更易受到诸如上下行接入消息窃听、消息篡改、消息重放等攻击的威胁。

[0003] 终端设备安全接入是指终端设备经过注册过程并获得合法身份标识后，可向卫星发起安全接入请求，该请求经过地面信关站判断后决定是否转发至卫星，卫星收到该请求后进行多维安全性验证，通过验证则准许该终端设备接入卫星网络。在这个过程中，地面信关站始终处于卫星的波束覆盖范围内从而可以与其保持通信，当卫星过顶后，便无法与地面信关站进行通信，因此，要保证卫星与地面信关站通信或卫星提供服务的连续性，同时保证对终端设备的透明性，需要地面信关站与新连接的卫星完成接续认证，即将地面信关站上保存的合法终端设备的接入状态同步到新连接的卫星上，从而保证服务的连续性。

[0004] 在终端接入方面，专利CN105490726A提出了一种可提高卫星系统安全性和保密性的远程卫星终端入网认证鉴权方法和系统。专利CN106850674A提出了一种在轨卫星身份认证方法，解决星地通信过程中双向认证的问题。这些研究成果通过设立网络管理系统或ECC双向认证来提高终端接入的安全性和鲁棒性，以保证卫星网络的正常运行。但上述方案均未考虑重放攻击的防御问题，以及接续和登出过程，默认终端设备为合法设备，同时，上述所有终端设备接入相关方案都需要终端用户与卫星接入点直接通信，不适用于无法与卫星直接通信的终端设备获取卫星服务的应用场景。

发明内容

[0005] 本发明技术解决问题：克服现有技术的不足，一种卫星安全接入认证的方法及系统，引入地面信关站作为可信设备，为终端用户以及卫星接入点之间建立可信关系提供桥梁，发生接入时，仅需完成轻量级的认证计算，即可保证终端用户接入网络的稳定性及安全性，在密集用户集体接入的场景下，依然能够保证信令开销小、带宽占用低、卫星资源消耗少、终端用户无感知的安全接入效果。同时，本方案能够适用于无法与卫星直接通信的终端设备接入卫星网络的场景。

[0006] 本发明实施例提供了一种卫星安全接入认证的方法，解决了未注册终端设备无法安全接入网络并使用卫星服务的问题。采用本发明实施例提供的方法，可以保证合法终端设备安全地接入卫星网络。

[0007] 本发明能够解决未注册终端设备无法安全接入网络并使用卫星服务的问题，保证终端用户接入网络的稳定性及安全性，以较小的卫星资源消耗、用户无感知的接入接续流程，安全地进行终端设备接入星地通信链路，同时，本发明能够应用于不能与卫星直接通信的终端设备接入卫星网络的场景。

[0008] 其具体技术方案如下：

[0009] 一种卫星安全接入认证的方法，包括以下步骤：

[0010] 终端设备生成会话公私钥，携带所述终端设备公钥及固有信息向地面站发送注册请求；

[0011] 所述地面站为所述终端设备分配身份标识，向所述终端设备发送注册响应，所述终端设备保存身份标识；

[0012] 所述地面站向卫星发送终端注册上注请求，所述卫星解析保存所述终端设备身份标识及公钥信息，完成所述终端设备注册；

[0013] 终端设备向地面信关站发送接入认证请求消息，所述地面信关站判断所述终端设备接入状态；

[0014] 若满足接入认证请求消息上星条件，所述地面信关站向卫星转发接入认证请求消息；

[0015] 所述卫星收到接入认证请求消息，进行多维度安全性验证，验证所述终端设备是否满足接入要求；

[0016] 若满足接入认证要求，计算所述终端设备接入失效时刻，所述卫星向所述地面信关站发送接入认证响应消息；

[0017] 所述地面信关站解析接入认证响应消息，获取所述终端接入失效时刻，向所述终端设备发送接入认证响应消息，所述终端设备解析接入认证响应消息，完成所述终端设备接入认证；

[0018] 地面信关站向新连接卫星发起接续认证请求，提供当前已接入终端设备列表；

[0019] 所述卫星收到接续认证请求，进行多维度安全性验证，验证所述已接入终端设备列表中设备是否满足接续要求；

[0020] 若满足接续认证要求，所述卫星向所述地面信关站发送接续认证响应；

[0021] 所述地面信关站解析接续认证响应消息，更新所述已接入终端设备列表，完成终端设备接续认证过程；

[0022] 终端设备向地面信关站发送登出认证请求消息，所述地面信关站判断所述终端设备接入状态；

[0023] 若满足登出认证请求消息上星条件，所述地面信关站向卫星转发登出认证请求消息；

[0024] 所述卫星收到登出认证请求消息，进行多维度安全性验证，验证所述终端设备是否满足登出要求；

[0025] 若满足登出认证要求，销毁所述终端设备接入状态，所述卫星向所述地面信关站发送登出认证响应消息；

[0026] 所述地面信关站解析登出认证响应消息，销毁所述终端设备接入状态，向所述终端设备发送登出认证响应消息，所述终端设备解析登出认证响应消息，完成所述终端设备

登出认证。

[0027] 在终端设备发起的注册请求消息中，至少包括终端设备公钥信息及设备PIN码或IMEI码等固有信息，便于地面站在生成设备标识期间提升终端设备识别码的随机性。

[0028] 在终端设备发起的接入认证请求消息中，至少包括终端设备身份信息、发送时刻时间戳，以及采用一定安全策略生成的校验位。添加终端设备身份信息可以使卫星在本次接入认证过程中验证终端设备的合法身份。添加发送消息时刻的时间戳，目的是接收方对该时间进行有效性判断，可以有效防止重放攻击。校验位可以是发送方身份信息的校验或请求包完整性的校验等。

[0029] 在地面信关站发起的接续认证请求消息中，至少包括已接入终端设备列表、发送时刻时间戳，以及采用一定安全策略生成的校验位。添加已接入终端设备列表可以使卫星在本次接续认证过程中获知当前已接入终端设备的身份信息及会话失效时间。添加发送消息时刻的时间戳，目的是接收方对该时间进行有效性判断，可以有效防止重放攻击。校验位可以是发送方身份信息的校验或请求包完整性的校验等。

[0030] 在终端设备发起的登出认证请求消息中，至少包括终端设备身份信息、发送时刻时间戳，以及采用一定安全策略生成的校验位。添加终端设备身份信息可以使卫星在本次登出认证过程中验证终端设备的合法身份。添加发送消息时刻的时间戳，目的是接收方对该时间进行有效性判断，可以有效防止重放攻击。校验位可以是发送方身份信息的校验或请求包完整性的校验等。

[0031] 卫星收到地面信关站发来的接入认证请求消息后，判断是否进行接入认证响应的条件为：接入认证请求消息中的校验位校验通过以及消息中的时间戳在允许时间范围内；卫星收到地面信关站发来的接续认证请求消息后，判断是否进行接续认证响应的条件为：接续认证请求消息中的校验位校验通过以及消息中的时间戳在允许时间范围内；卫星收到地面信关站发来的登出认证请求消息后，判断是否进行登出认证响应的条件为：登出认证请求消息中的校验位校验通过以及消息中的时间戳在允许时间范围内。

[0032] 上述接入认证请求消息、接续认证请求消息和登出认证请求消息可以是经过特殊处理的内容，该特殊处理包括但不限于加密。

[0033] 卫星向地面信关站发送的接入认证响应消息中，至少包括接入认证响应结果、终端设备身份信息；卫星向地面信关站发送的接入认证响应消息中，至少包括接入认证响应结果、终端设备身份信息、发送时刻时间戳，以及采用一定安全策略生成的校验位；卫星向地面信关站发送的接入认证响应消息中，至少包括接入认证响应结果、终端设备身份信息、发送时刻时间戳，以及采用一定安全策略生成的校验位。

[0034] 上述接入认证响应消息、接续认证响应消息和登出认证响应消息可以是经过特殊处理的内容，该特殊处理包括但不限于加密。

[0035] 卫星收到地面信关站发送的接入认证请求消息、接续认证请求消息和登出认证请求消息后，进行的多维度安全性验证包括：

[0036] 接收到的地面信关站发送的接入认证请求消息中的校验位校验是否通过，以及该响应消息中的时间戳是否在允许时间范围内；

[0037] 接收到的地面信关站发送的接续认证请求消息中的校验位校验是否通过，以及该响应消息中的时间戳是否在允许时间范围内；

[0038] 接收到的地面信关站发送的登出认证请求消息中的校验位校验是否通过，以及该响应消息中的时间戳是否在允许时间范围内。

[0039] 接入认证完成后，终端设备与卫星间通过地面信关站建立安全通信，此时，卫星与地面信关站均知道上述终端设备身份信息以及会话失效时刻；接续认证完成后，已接入的终端设备与新连接到地面信关站的卫星间通过地面信关站建立安全通信；登出认证完成后，终端设备与卫星间的安全通信会被切断结束，终端无法继续使用卫星提供的服务。

[0040] 本发明的一种卫星接入认证服务系统，包括：组网卫星、终端设备、地面信关站和地面站；组网卫星，指卫星网络中同一或不同轨道上多种类型的卫星系统；

[0041] 终端设备用于接收组网卫星提供的服务，与地面信关站之间进行通信，并通过地面信关站与卫星通信；地面信关站为一种中间可信设备，用于连接终端设备与组网卫星之间的通信；地面站用于为终端设备分配身份标识，向组网卫星上注终端设备身份信息；

[0042] 所述组网卫星包括：安全接入模块，用于接收地面站发送的终端注册上注请求，以及接受地面信关站发送的接入认证请求消息、接续认证请求消息、登出认证请求消息，判断是否对接入认证请求消息、接续认证请求消息、登出认证请求消息进行响应以及向地面信关站发送接入认证响应消息、接续认证响应消息、登出认证响应消息，安全接入模块接收地面站的安全注册模块的终端注册上注请求；安全接入模块接收地面信关站的安全接入认证代理模块发送的接入认证请求消息，进行接入认证，地面信关站的安全接入认证代理模块接收安全接入模块发送的接入认证响应消息；安全接入模块接收地面信关站的安全接续认证代理模块发送的接续认证请求消息，进行接续认证，地面信关站的安全接续认证代理模块接收安全接入模块发送的接续认证响应消息；安全接入模块接收地面信关站的安全登出认证代理模块发送的登出认证请求消息，进行登出认证，地面信关站的安全登出认证代理模块接收安全登出模块发送的登出认证响应消息；

[0043] 所述终端设备包括安全注册模块、安全接入认证模块、安全接续认证模块和安全登出认证模块，其中：

[0044] 所述安全注册模块，用于生成安全注册请求消息，解析安全注册响应消息，保存身份标识，地面站的安全注册模块接收终端设备的安全注册模块发送的安全注册请求消息，完成注册后，终端设备的安全注册模块接收地面站的安全注册模块发送的安全注册响应消息；

[0045] 所述安全接入认证模块，用于生成安全接入认证请求消息，向地面信关站发送接入认证请求消息，地面信关站的安全接入认证代理模块接收安全接入认证模块发送的安全接入认证请求消息，安全接入认证模块接收地面信关站的安全接入认证代理模块发送的安全接入认证响应消息；

[0046] 所述安全接续认证模块，用于生成安全接续认证请求消息，向地面信关站发送接续认证请求消息，地面信关站的安全接续认证代理模块接收安全接续认证模块发送的安全接续认证请求消息，安全接续认证模块接收地面信关站的安全接续认证代理模块发送的安全接续认证响应消息；

[0047] 所述安全登出认证模块，用于生成安全登出认证请求消息，向地面信关站发送登出认证请求消息，地面信关站的安全登出认证代理模块接收安全登出认证模块发送的安全登出认证请求消息，安全登出认证模块接收地面信关站的安全登出认证代理模块发送的安

全登出认证响应消息；

[0048] 所述地面信关站包括安全接入认证代理模块、安全接续认证代理模块和安全登出认证代理模块，其中：

[0049] 所述安全接入认证代理模块，用于判断终端设备是否具备向组网卫星请求接入网络的条件，以及转发接入认证响应消息，安全接入认证代理模块接收终端设备的安全接入认证模块发送的安全接入认证请求消息，终端设备的安全接入认证模块接收安全接入认证代理模块发送的安全接入认证响应消息，组网卫星的安全接入模块接收安全接入认证代理模块发送的接入认证请求消息，进行接入认证，安全接入认证代理模块接收组网卫星的安全接入模块发送的接入认证响应消息；

[0050] 所述安全接续认证代理模块，用于判断终端设备是否具备向组网卫星请求接续网络的条件，以及转发接续认证响应消息，安全接续认证代理模块接收终端设备的安全接续认证模块发送的安全接续认证请求消息，终端设备的安全接续认证模块接收安全接续认证代理模块发送的安全接续认证响应消息，组网卫星的安全接入模块接收安全接续认证代理模块发送的接续认证请求消息，进行接续认证，安全接续认证代理模块接收组网卫星的安全接续模块发送的接续认证响应消息；

[0051] 所述安全登出认证代理模块，用于判断终端设备是否具备向组网卫星请求登出网络的条件，以及转发登出认证响应消息；安全登出认证代理模块接收终端设备的安全登出认证模块发送的安全登出认证请求消息，终端设备的安全登出认证模块接收安全登出认证代理模块发送的安全登出认证响应消息，组网卫星的安全登出模块接收安全登出认证代理模块发送的登出认证请求消息，进行登出认证，安全登出认证代理模块接收组网卫星的安全登出模块发送的登出认证响应消息；

[0052] 所述地面站包括：安全注册模块，用于接收终端设备发送的安全注册请求消息，生成安全注册响应消息和终端注册上注请求消息，以及向终端设备发送安全注册响应消息、向组网卫星上注终端注册上注请求消息，地面站的安全注册模块接收终端设备的安全注册模块发送的安全注册请求消息，完成注册后，终端设备的安全注册模块接收地面站的安全注册模块发送的安全注册响应消息，组网卫星的安全接入模块接收安全注册模块的终端注册上注请求。

[0053] 本发明的有益效果在于：

[0054] (1)保证了组网卫星为已接入终端设备提供服务的连续性，以及接续过程的透明性。接续认证过程只在地面信关站与组网卫星间完成，不涉及最终接受服务的终端设备，终端设备对接续过程无感知，接续完成后，由新连接卫星代替过顶卫星继续提供服务，使得服务不会由于卫星过顶结束而被中断。

[0055] (2)保证了终端设备接入卫星过程的安全性。终端设备注册时，地面站为终端设备分配唯一的身份标识，将终端设备公钥及身份信息上注到卫星；终端设备发起安全接入认证过程与安全接入认证过程时，地面信关站与卫星的每一次通信过程双方都会进行身份校验等安全措施，可以有效避免中间人攻击，若中间人伪造身份与地面信关站或卫星进行通信，则无法通过校验，从而攻击失败；同时，每次通信过程都会对消息中的时间戳进行有效性验证，能够有效防止重放攻击。

[0056] (3)满足密集用户集体接续认证需求。现有的接续认证过程均在用户设备与卫星

之间直接进行切换，若用户设备过多，在切换频繁发生的情况下，会产生大量信令开销，极大消耗有限的卫星资源，同时显式的接续操作会影响用户体验，本发明接续过程只发生在卫星与地面信关站之间，而连接至地面信关站的终端设备可使用连续的卫星服务，因此，可以满足密集用户集体切换需求，并且对终端设备保持透明服务。

[0057] (4)满足无法与卫星直接通信的终端设备获取卫星服务的应用场景。现有终端设备接入认证方案均需由终端设备与卫星之间直接交换接入信令，本发明通过地面信关站作为中间可信设备建立终端设备与卫星间的数据通信，可以为终端设备提供卫星服务。

附图说明

[0058] 图1为本发明的一种卫星安全接入认证方法的流程图；

[0059] 图2为本发明的一种卫星安全接入认证方法的一部分流程图；

[0060] 图3为本发明的一种卫星安全接入认证方法的一部分流程图；

[0061] 图4为本发明的一种卫星安全接入认证服务系统的结构图。

具体实施方式

[0062] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0063] 本发明包括：终端设备发起注册过程，生成会话公私钥，向地面站发送注册请求，地面站为终端设备分配身份标识，终端设备保存身份标识，地面站向卫星发送终端设备身份标识及公钥信息，完成终端设备注册过程。终端设备向地面信关站发起接入认证请求，地面信关站判断接入状态；若满足接入认证请求上星条件，向卫星转发接入认证请求，卫星收到接入认证请求，进行多维度安全性验证，验证终端设备是否满足接入要求；若满足接入认证要求，卫星向地面信关站发送接入认证响应，地面信关站解析接入认证响应消息，获取终端接入失效时刻，向终端设备发送接入认证响应，终端设备解析接入认证响应，完成终端设备接入认证过程。当前连接卫星发生过顶时，地面信关站向新连接卫星发起接续认证请求，提供当前接入终端设备列表，卫星收到接续认证请求，进行多维度安全性验证，验证终端设备列表中设备是否满足接续要求；若满足接续认证要求，卫星向地面信关站发送接续认证响应，地面信关站解析接续认证响应消息，更新当前接入终端设备列表，完成终端设备接续认证过程。终端设备向地面信关站发起登出认证请求，地面信关站判断接入状态；若满足登出认证请求上星条件，向卫星转发登出认证请求，卫星收到登出认证请求，进行多维度安全性验证，验证终端设备是否满足登出要求；若满足登出认证要求，卫星向地面信关站发送登出认证响应，地面信关站解析登出认证响应消息，向终端设备发送登出认证响应，终端设备解析登出认证响应，完成终端设备登出认证过程。

[0064] 图1、2、3显示了本发明一种卫星安全过顶切换方法的一个实施例的流程图，主要包括以下步骤：

[0065] S101，终端设备生成会话公钥和私钥，分别为DEV_PubKEY和DEV_PriKEY，携带终端设备公钥DEV_PubKEY及设备固有信息向地面站发送注册请求；

[0066] S102,地面站为终端设备分配身份标识DEV_ID,向终端设备发送注册响应,终端设备保存身份标识;

[0067] S103,地面站向卫星发送终端注册上注请求,卫星解析保存终端设备身份标识DEV_ID及公钥信息DEV_PubKEY,完成终端设备注册;

[0068] S201,终端设备向地面信关站发送接入认证请求消息,地面信关站判断终端设备接入状态;

[0069] S202,若在步骤S201中,经判断满足接入认证请求消息上星条件,地面信关站向卫星转发接入认证请求消息;

[0070] S203,卫星收到接入认证请求消息,进行多维度安全性验证,验证终端设备是否满足接入要求;

[0071] S204,若在步骤S203中,经判断满足接入认证要求,计算终端设备接入失效时刻,卫星向地面信关站发送接入认证响应消息;

[0072] S205,地面信关站解析终端接入认证响应消息,获取接入失效时刻,向终端设备发送接入认证响应消息,终端设备解析接入认证响应消息,完成终端设备接入认证;

[0073] S301,地面信关站向新连接卫星发起接续认证请求,提供当前已接入终端设备列表;

[0074] S302,卫星收到接续认证请求,进行多维度安全性验证,验证已接入终端设备列表中设备是否满足接续要求;

[0075] S303,若在步骤S302中,经判断满足接续认证要求,卫星向地面信关站发送接续认证响应;

[0076] S304,地面信关站解析接续认证响应消息,更新已接入终端设备列表,完成终端设备接续认证过程;

[0077] S401,终端设备向地面信关站发送登出认证请求消息,地面信关站判断终端设备接入状态;

[0078] S402,若在步骤S401中,经判断满足登出认证请求消息上星条件,地面信关站向卫星转发登出认证请求消息;

[0079] S403,卫星收到登出认证请求消息,进行多维度安全性验证,验证终端设备是否满足登出要求;

[0080] S404,若在步骤S403中,经判断满足登出认证要求,销毁终端设备接入状态,卫星向地面信关站发送登出认证响应消息;

[0081] S405,地面信关站解析登出认证响应消息,销毁终端设备接入状态,向终端设备发送登出认证响应消息,终端设备解析登出认证响应消息,完成终端设备登出认证。

[0082] 具体来讲,本发明在步骤S101中,终端设备产生会话公私钥。本实施例中,采用ECC椭圆双曲线方法计算出公钥和私钥,分别为DEV_PubKEY和DEV_PriKEY,终端设备向地面站发送注册请求消息,该注册请求消息中,至少包括终端设备公钥DEV_PubKEY及设备固有信息等。

[0083] 在步骤S102中,地面站为终端设备分配身份标识。本实施例中,身份标识采用分段填充的方法生成,具体字段包括终端设备类型标识、归属域及终端设备识别码。身份标识中每个字段生成方法可以采用多种标准,包括但不限于随机数法,查表法,自增法等。

[0084] 在步骤S103中，地面站向卫星发送终端注册上注请求消息，该终端注册上注请求消息中，至少包括以下一种类型：增加终端设备信息、删除终端设备信息。本实施例中，增加终端设备信息类型指导卫星增加新注册终端设备的身份标识及公钥信息，删除终端设备信息类型指导卫星删除已注册终端设备的全部信息。

[0085] 在步骤S201中，终端设备向地面信关站发送接入认证请求消息，该接入认证请求消息中，至少包括终端设备身份信息、发送时刻时间戳，以及采用安全策略生成的校验位。本发明实施例中接入认证请求消息由两部分构成，分别为重要明文信息(终端设备身份信息、发送时刻时间戳)和校验位，生成校验位方式为终端设备使用私钥对接入认证请求中的重要明文信息部分进行签名，签名方法如下所示：

[0086] SIGN(Hash(DEV_ID|TimeStamp),DEV_PriKey)

[0087] 其中DEV_ID为终端设备身份信息，TimeStamp为时间戳，DEV_PriKey为终端设备私钥。采用散列函数，计算重要明文信息所产生的散列值，并对该散列值用终端设备的私钥进行签名。

[0088] 地面信关站收到接入认证请求消息后判断终端设备接入状态，判断的条件为：所述终端设备尚未接入、以及所述接入认证请求消息不符合重放攻击的特征。地面信关站中维护接入认证请求消息时间戳列表，记录每次终端设备发起的接入认证请求消息中的终端设备身份信息DEV_ID及时间戳TimeStamp，该列表的表项过期清除条件为：时间戳TimeStamp与当前时间的差值绝对值是否超过超时间隔Timeout_Interval，若超过则清除。

[0089] 具体在本发明实施例中，判断过程如下：

[0090] i.地面信关站收到终端设备发送的接入认证请求消息后，首先提取明文信息：终端设备身份信息DEV_ID，时间戳TimeStamp。

[0091] ii.接下来在已接入终端列表中查找终端设备身份信息DEV_ID，若查找成功，则说明该终端设备已经接入，无需再次接入，并结束接入流程。

[0092] iii.接下来在接入认证请求消息时间戳列表中查找时间戳TimeStamp，若查找成功，则说明该接入认证请求消息具有重放攻击特征，发出告警信息，并结束接入流程。

[0093] iv.以上验证均通过后，整个判断过程结束。

[0094] 若在步骤S201中判断结果为真，则进入步骤S202：

[0095] 地面信关站向卫星发送接入认证请求消息，该消息与终端设备发送给地面信关站的接入认证请求消息内容一致。该接入认证请求消息中，至少包括终端设备身份信息、发送时刻时间戳，以及采用安全策略生成的校验位。

[0096] 在步骤S203中，卫星收到接入认证请求消息，进行多维度安全性验证，验证终端设备是否满足接入要求，允许接入的条件为：

[0097] 卫星接收到的接入认证请求消息中的终端设备信息已注册，消息中的校验位校验通过，以及消息中的时间戳在允许时间范围内。

[0098] 具体在本实施例中，判断过程如下：

[0099] i.卫星收到地面信关站发送的接入认证请求消息后，首先提取明文信息：终端设备身份信息DEV_ID，时间戳TimeStamp。

[0100] ii.接下来提取明文信息中的时间戳TimeStamp，根据预设的有效时间范围，判断该时间戳是否在本次通信的有效时间内，若不在有效时间内，则无需进行后续验证，并结束

接入流程。

[0101] iii.接下来在已注册终端列表中查找终端设备身份信息DEV_ID,若查找不成功,则说明该终端设备尚未注册,无需进行后续验证,并结束接入流程。

[0102] iv.接下来在已接入终端列表中查找终端设备身份信息DEV_ID,若查找成功,则说明该终端设备已经接入,无需再次接入,并结束接入流程。

[0103] v.接下来将明文信息(终端设备身份信息DEV_ID,时间戳TimeStamp)采用与步骤S201中相同的散列函数,计算得到散列值2;

[0104] vi.接下来提取校验位,即数字签名SignMsg=SIGN(Hash(DEV_ID|TimeStamp),DEV_PriKey),其中SignMsg为提取到的数字签名信息,DEV_ID为终端设备身份信息,TimeStamp为时间戳,DEV_PriKey为终端设备私钥,卫星利用预先获取的终端设备的公钥DEV_PubKey,对来自终端设备的数字签名进行解签,方法如下:VERIFY(SignMsg,DEV_PubKey),其中SignMsg为提取到的数字签名信息,DEV_PubKey为终端设备的公钥,计算得到散列值3。

[0105] vii.比较散列值2和散列值3,若相等,则验证了数据的完整性和数据来源的真实性,校验位验证通过;

[0106] viii.若以上判断结果均为真,则整个判断过程结束,符合接入认证条件。

[0107] 若在步骤S203中判断结果为真,则进入步骤S204:

[0108] 卫星计算终端设备接入失效时刻,向已接入终端设备列表中添加当前终端设备的身份信息和接入失效时刻,卫星向地面信关站发送接入认证响应消息,该接入认证响应消息中,至少包括终端设备身份信息、终端设备接入失效时刻,以及终端设备接入结果。

[0109] 在步骤S205中,地面信关站解析终端接入认证响应消息,获取接入失效时刻,向已接入终端设备列表中添加当前终端设备的身份信息和接入失效时刻,向终端设备发送接入认证响应消息,该接入认证响应消息中,至少包括终端设备身份信息,以及终端设备接入结果。终端设备解析接入认证响应消息,获取接入认证结果。至此,完成终端设备接入认证。

[0110] 接入认证完成后,终端设备与卫星间通过地面信关站进行安全通信,此时,卫星与地面信关站均知道已连接的终端设备信息以及接入状态,地面信关站根据接入状态为终端设备提供数据包上星转发服务。

[0111] 在步骤S301中,地面信关站向卫星发送接续认证请求消息,该接续认证请求消息中,至少包括已接入终端设备列表、发送时刻时间戳,以及采用安全策略生成的校验位。本发明实施例中接续认证请求消息由两部分构成,分别为重要明文信息(已接入终端设备列表、发送时刻时间戳)和校验位,生成校验位方式为地面信关站使用私钥对接续认证请求中的重要明文信息部分进行签名,签名方法如下所示:

[0112] SIGN(Hash(DEV_AccList|TimeStamp),FI_PriKey)

[0113] 其中DEV_AccList为已接入终端设备列表,TimeStamp为时间戳,FI_PriKey为地面信关站私钥。采用散列函数,计算重要明文信息所产生的散列值,并对该散列值用地面信关站的私钥进行签名。

[0114] 在步骤S302中,卫星收到接续认证请求消息,进行多维度安全性验证,验证已接入终端设备列表中设备是否满足接续要求,允许接续的条件为:

[0115] 卫星接收到的接续认证请求消息中已接入终端设备列表内的终端设备信息已注

册,消息中的校验位校验通过,以及消息中的时间戳在允许时间范围内。

[0116] 具体在本实施例中,判断过程如下:

[0117] i.卫星收到地面信关站发送的接续认证请求消息后,首先提取明文信息:已接入终端设备列表DEV_AccList,时间戳TimeStamp。

[0118] ii.接下来提取明文信息中的时间戳TimeStamp,根据预设的有效时间范围,判断该时间戳是否在本次通信的有效时间内,若不在有效时间内,则无需进行后续验证,并结束接续流程。

[0119] iii.接下来在已注册终端列表中逐一查找已接入终端设备列表DEV_AccList中的终端设备身份信息DEV_ID,若单次查找不成功,则说明该终端设备尚未注册,继续进行后项查找,若查找均不成功,则无需进行后续验证,并结束接续流程。

[0120] iv.接下来将明文信息(已接入终端设备列表DEV_AccList,时间戳TimeStamp)采用与步骤S301中相同的散列函数,计算得到散列值4。

[0121] v.接下来提取校验位,即数字签名SignMsg=SIGN(Hash(DEV_AccList|TimeStamp),FI_PriKey),其中SignMsg为提取到的数字签名信息,DEV_AccList为已接入终端设备列表,TimeStamp为时间戳,FI_PriKey为地面信关站私钥,卫星利用预先获取的地面信关站的公钥FI_PubKey,对来自地面信关站的数字签名进行解签,方法如下:VERIFY(SignMsg,FI_PubKey),其中SignMsg为提取到的数字签名信息,FI_PubKey为地面信关站的公钥,计算得到散列值5。

[0122] vii.比较散列值4和散列值5,若相等,则验证了数据的完整性和数据来源的真实性,校验位验证通过。

[0123] viii.若以上判断结果均为真,则整个判断过程结束,符合接续认证条件。

[0124] 若在步骤S302中判断结果为真,则进入步骤S303:

[0125] 卫星计算通过验证的终端设备的接续失效时刻,向已接入终端设备列表中添加通过验证的终端设备的身份信息和接续失效时刻,卫星向地面信关站发送接续认证响应消息,该接续认证响应消息中,至少包括通过验证的终端设备身份信息、通过验证的终端设备接续失效时刻,以及接续认证结果。

[0126] 在步骤S304中,地面信关站解析终端接续认证响应消息,获取接续认证结果、通过验证的终端设备身份信息、通过验证的终端设备接续失效时刻,向已接入终端设备列表中更新通过验证的终端设备身份信息和接续失效时刻。至此,完成终端设备接续认证。

[0127] 接续认证完成后,终端设备与新连接的卫星间可继续通过地面信关站进行安全通信,此时,新连接的卫星与地面信关站均知道已连接的终端设备信息以及接续状态,地面信关站根据接续状态为终端设备提供数据包上星转发服务。

[0128] 在步骤S401中,终端设备向地面信关站发送登出认证请求消息,该登出认证请求消息中,至少包括终端设备身份信息、发送时刻时间戳,以及采用安全策略生成的校验位。本发明实施例中登出认证请求消息由两部分构成,分别为重要明文信息(终端设备身份信息、发送时刻时间戳)和校验位,生成校验位方式为终端设备使用私钥对登出认证请求中的重要明文信息部分进行签名,签名方法如下所示:

[0129] SIGN(Hash(DEV_ID|TimeStamp),DEV_PriKey)

[0130] 其中DEV_ID为终端设备身份信息,TimeStamp为时间戳,DEV_PriKey为终端设备私

钥。采用散列函数，计算重要明文信息所产生的散列值，并对该散列值用终端设备的私钥进行签名。

[0131] 地面信关站收到登出认证请求消息后判断终端设备接入状态，判断的条件为：所述终端设备是否接入、以及所述登出认证请求消息不符合重放攻击的特征。地面信关站中维护登出认证请求消息时间戳列表，记录每次终端设备发起的登出认证请求消息中的终端设备身份信息DEV_ID及时间戳TimeStamp，该列表的表项过期清除条件为：时间戳TimeStamp与当前时间的差值绝对值是否超过超时间隔Timeout_Interval，若超过则清除。

[0132] 具体在本发明实施例中，判断过程如下：

[0133] i.地面信关站收到终端设备发送的登出认证请求消息后，首先提取明文信息：终端设备身份信息DEV_ID，时间戳TimeStamp。

[0134] ii.接下来在已接入终端列表中查找终端设备身份信息DEV_ID，若查找不成功，则说明该终端设备尚未接入，无需进行登出，并结束登出流程。

[0135] iii.接下来在登出认证请求消息时间戳列表中查找时间戳TimeStamp，若查找成功，则说明该登出认证请求消息具有重放攻击特征，发出告警信息，并结束登出流程。

[0136] iv.以上验证均通过后，整个判断过程结束。

[0137] 若在步骤S401中判断结果为真，则进入步骤S402：

[0138] 地面信关站向卫星发送登出认证请求消息，该消息与终端设备发送给地面信关站的登出认证请求消息内容一致。该登出认证请求消息中，至少包括终端设备身份信息、发送时刻时间戳，以及采用安全策略生成的校验位。

[0139] 在步骤S403中，卫星收到登出认证请求消息，进行多维度安全性验证，验证终端设备是否满足登出要求，允许登出的条件为：

[0140] 卫星接收到的登出认证请求消息中的终端设备信息已注册并已接入，消息中的校验位校验通过，以及消息中的时间戳在允许时间范围内。

[0141] 具体在本实施例中，判断过程如下：

[0142] i.卫星收到地面信关站发送的登出认证请求消息后，首先提取明文信息：终端设备身份信息DEV_ID，时间戳TimeStamp。

[0143] ii.接下来提取明文信息中的时间戳TimeStamp，根据预设的有效时间范围，判断该时间戳是否在本次通信的有效时间内，若不在有效时间内，则无需进行后续验证，并结束登出流程。

[0144] iii.接下来在已注册终端列表中查找终端设备身份信息DEV_ID，若查找不成功，则说明该终端设备尚未注册，无需进行后续验证，并结束登出流程。

[0145] iv.接下来在已接入终端列表中查找终端设备身份信息DEV_ID，若查找不成功，则说明该终端设备尚未接入，无需进行后续验证，并结束登出流程。

[0146] v.接下来将明文信息(终端设备身份信息DEV_ID，时间戳TimeStamp)采用与步骤S401中相同的散列函数，计算得到散列值6。

[0147] vi.接下来提取校验位，即数字签名SignMsg＝SIGN(Hash(DEV_ID|TimeStamp)，DEV_PriKey)，其中SignMsg为提取到的数字签名信息，DEV_ID为终端设备身份信息，TimeStamp为时间戳，DEV_PriKey为终端设备私钥，卫星利用预先获取的终端设备的公钥DEV_PubKey，对来自终端设备的数字签名进行解签，方法如下：VERIFY(SignMsg，DEV_

PubKey)，其中SignMsg为提取到的数字签名信息，DEV_PubKey为终端设备的公钥，计算得到散列值7。

[0148] vii.比较散列值6和散列值7，若相等，则验证了数据的完整性和数据来源的真实性，校验位验证通过。

[0149] viii.若以上判断结果均为真，则整个判断过程结束，符合登出认证条件。

[0150] 若在步骤S403中判断结果为真，则进入步骤S404：

[0151] 卫星清除已接入终端设备列表中当前终端设备的接入状态，卫星向地面信关站发送登出认证响应消息，该登出认证响应消息中，至少包括终端设备身份信息，以及终端设备登出结果。

[0152] 在步骤S405中，地面信关站解析终端登出认证响应消息，清除该终端设备的接入状态，向终端设备发送登出认证响应消息，该登出认证响应消息中，至少包括终端设备身份信息，以及终端设备登出结果。终端设备解析登出认证响应消息，获取登出认证结果。至此，完成终端设备登出认证。

[0153] 登出认证完成后，终端设备与卫星间断开安全通信连接，地面信关站将无法为该终端设备提供数据包上星转发服务。

[0154] 在本发明实施例技术方案基础上，如图4所示，本发明实施例提供一种卫星安全接入认证的系统，该系统包括四个实体，终端设备、地面信关站、组网卫星及地面站。

[0155] 该系统包括安全接入认证模块、安全接续认证模块、安全登出认证模块、安全注册模块、安全接入认证代理模块、安全接续认证代理模块、安全登出认证代理模块、安全接入模块和安全注册模块。

[0156] 图4中S501为安全接入认证模块，部署在终端设备中，用于生成安全接入认证请求消息，向地面信关站发送接入认证请求消息。

[0157] S502为安全接续认证模块，部署在终端设备中，用于生成安全接续认证请求消息，向地面信关站发送接续认证请求消息。

[0158] S503为安全登出认证模块，部署在终端设备中，用于生成安全登出认证请求消息，向地面信关站发送登出认证请求消息。

[0159] S504为安全注册模块，部署在终端设备中，用于生成安全注册请求消息，解析安全注册响应消息，保存身份标识。

[0160] S601为安全接入认证代理模块，部署在地面信关站中，用于判断终端设备是否具备向组网卫星请求接入网络的条件，以及转发接入认证响应消息。

[0161] S602为安全接续认证代理模块，部署在地面信关站中，用于判断终端设备是否具备向组网卫星请求接续网络的条件，以及转发接续认证响应消息。

[0162] S603为安全登出认证代理模块，部署在地面信关站中，用于判断终端设备是否具备向组网卫星请求登出网络的条件，以及转发登出认证响应消息。

[0163] S701为安全接入模块，部署在组网卫星中，用于接收地面站发送的终端注册上注请求，以及接受地面信关站发送的接入认证请求消息、接续认证请求消息、登出认证请求消息，判断是否对接入认证请求消息、接续认证请求消息、登出认证请求消息进行响应以及向地面信关站发送接入认证响应消息、接续认证响应消息、登出认证响应消息。

[0164] S801为安全注册模块，部署在地面站中，用于接收终端设备发送的安全注册请求

消息，生成安全注册响应消息和终端注册上注请求消息，以及向终端设备发送安全注册响应消息、向组网卫星上注终端注册上注请求消息。

[0165] 总之，本发明能够解决未注册终端设备无法安全接入网络并使用卫星服务的问题，保证终端用户接入网络的稳定性及安全性，以较小的卫星资源消耗、用户无感知的接入接续流程，安全地进行终端设备接入星地通信链路，同时，本发明能够应用于不能与卫星直接通信的终端设备接入卫星网络的场景。

[0166] 提供以上实施例仅仅是为了描述本发明的目的，而并非要限制本发明的范围。本发明的范围由所附权利要求限定。不脱离本发明的精神和原理而做出的各种等同替换和修改，均应涵盖在本发明的范围之内。

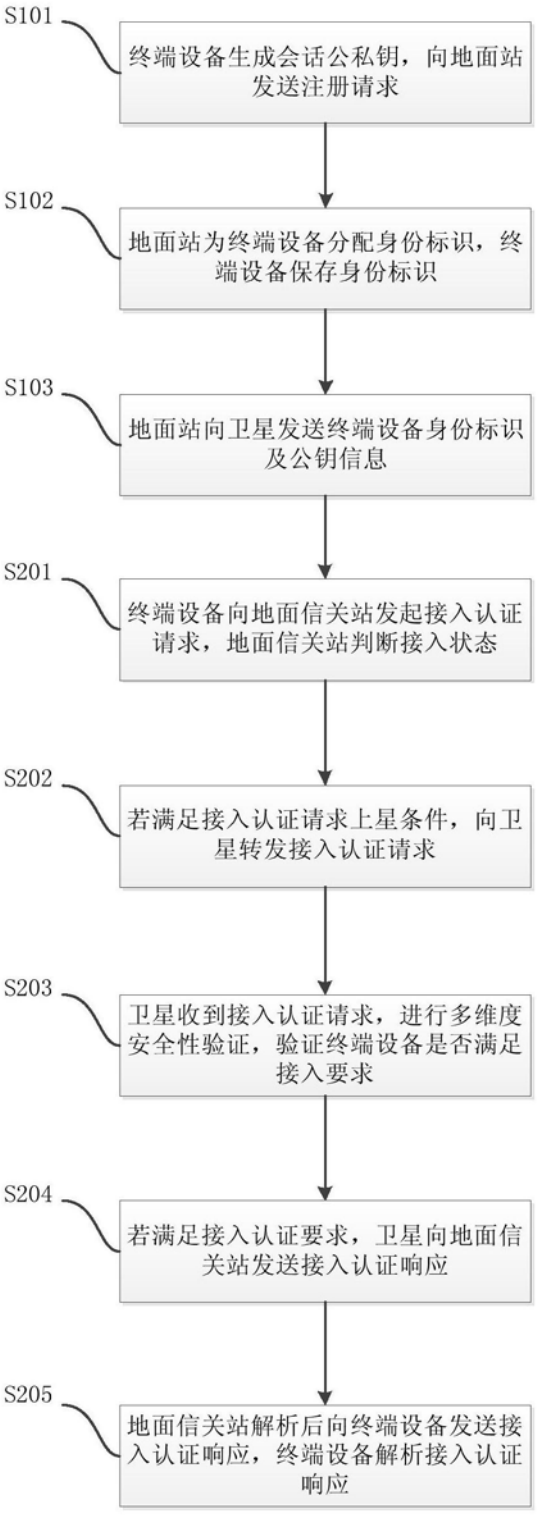

S101
终端设备生成会话公私钥，向地面站发送注册请求
S102
地面站为终端设备分配身份标识，终端设备保存身份标识
S103
地面站向卫星发送终端设备身份标识及公钥信息
S201
终端设备向地面信关站发起接入认证请求，地面信关站判断接入状态
S202
若满足接入认证请求上星条件，向卫星转发接入认证请求
S203
卫星收到接入认证请求，进行多维度安全性验证，验证终端设备是否满足接入要求
S204
若满足接入认证要求，卫星向地面信关站发送接入认证响应
S205
地面信关站解析后向终端设备发送接入认证响应，终端设备解析接入认证响应

图1

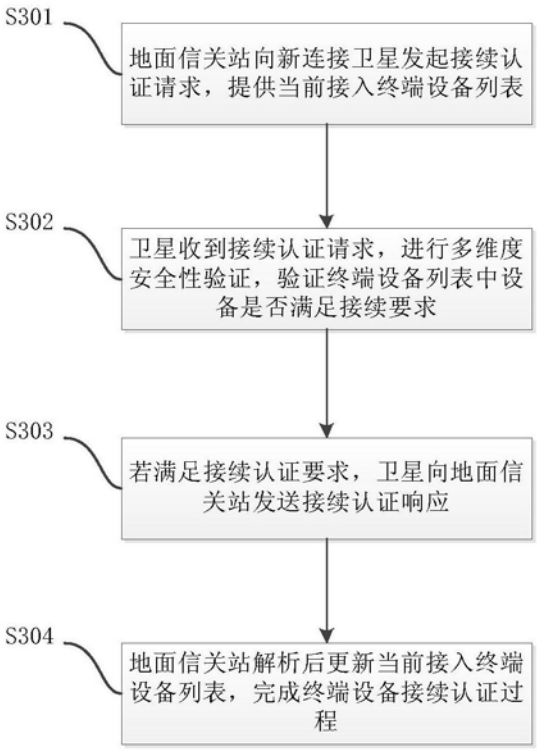

S301
地面信关站向新连接卫星发起接续认证请求，提供当前接入终端设备列表
S302
卫星收到接续认证请求，进行多维度安全性验证，验证终端设备列表中设备是否满足接续要求
S303
若满足接续认证要求，卫星向地面信关站发送接续认证响应
S304
地面信关站解析后更新当前接入终端设备列表，完成终端设备接续认证过程

图2

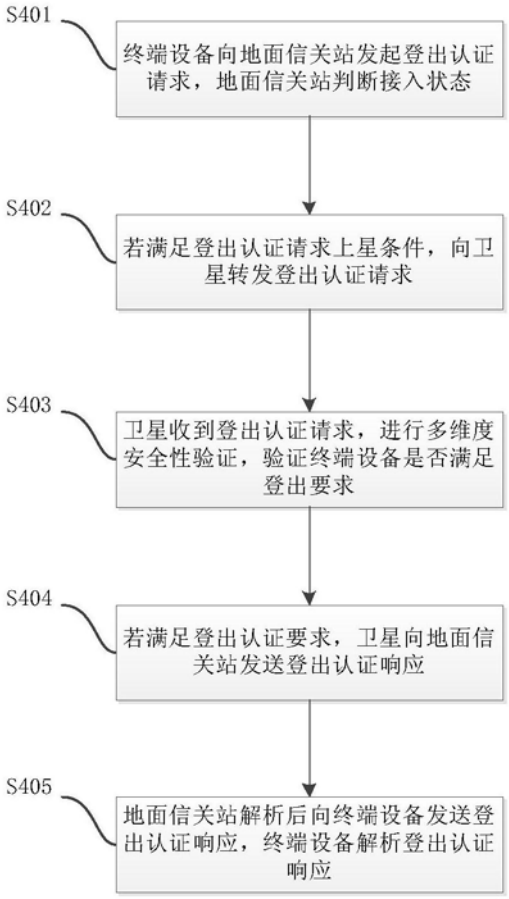

S401
终端设备向地面信关站发起登出认证请求，地面信关站判断接入状态
S402
若满足登出认证请求上星条件，向卫星转发登出认证请求
S403
卫星收到登出认证请求，进行多维度安全性验证，验证终端设备是否满足登出要求
S404
若满足登出认证要求，卫星向地面信关站发送登出认证响应
S405
地面信关站解析后向终端设备发送登出认证响应，终端设备解析登出认证响应

图3

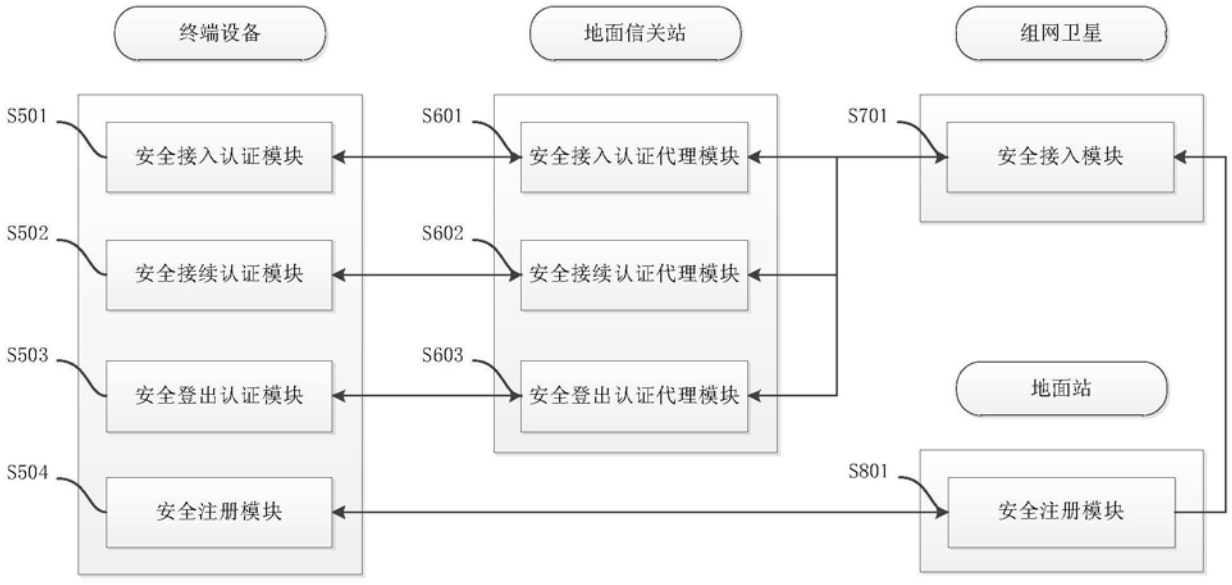

终端设备
地面信关站
组网卫星
S501
安全接入认证模块
S601
安全接入认证代理模块
S701
安全接入模块
S502
安全接续认证模块
S602
安全接续认证代理模块
S503
安全登出认证模块
S603
安全登出认证代理模块
地面站
S504
安全注册模块
S801
安全注册模块

图4