(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2023 年 5 月 19 日 (19.05.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/083346 A1

(51) 国际专利分类号:
H04W 12/106 (2021.01) *H04W 12/03* (2021.01)
H04W 12/10 (2021.01)

(21) 国际申请号: PCT/CN2022/131721

(22) 国际申请日: 2022 年 11 月 14 日 (14.11.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111347750.2 2021年11月15日 (15.11.2021) CN

(71) 申请人: 大唐移动通信设备有限公司 (**DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.**) [CN/CN]; 中国北京市海淀区上地东路5号院1号楼1层, Beijing 100085 (CN)。

(72) 发明人: 周巍 (**ZHOU, Wei**); 中国北京市海淀区上地东路5号院1号楼1层, Beijing 100085 (CN)。
徐晖 (**XU, Hui**); 中国北京市海淀区上地东路5号院1号楼1层, Beijing 100085 (CN)。

(74) 代理人: 北京路浩知识产权代理有限公司 (**CN-KNOWHOW INTELLECTUAL PROPERTY AGENT LIMITED**); 中国北京市海淀区中关村大街11号9层965, Beijing 100086 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE,

(54) **Title:** SATELLITE COMMUNICATION SYSTEM, METHOD, AND APPARATUS, RECEIVER NETWORK ELEMENT, AND STORAGE MEDIUM

(54) **发明名称:** 卫星通信系统、方法、装置、接收方网元及存储介质

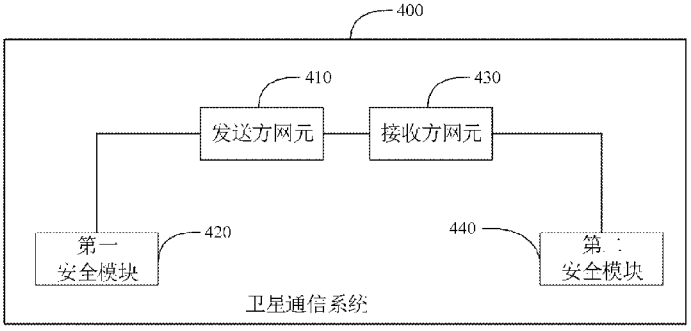

图 4

400 Satellite communication system
410 Sender network element
420 First security module
430 Receiver network element
440 Second security module

(57) **Abstract:** Embodiments of the present application provide a satellite communication system, comprising: a sender network element, a first security module, a receiver network element, and a second security module. The first security module is used for performing first security processing on a first data packet on the basis of a security policy to generate a second data packet having the data packet structure comprising a security field, and sending the second data packet to the sender network element; the second security module is used for performing second security processing on the second data packet on the basis of the security policy to obtain a third data packet comprising data of the first data packet, and sending the third data packet to the receiver network element; the sender network element is used for generating the first data packet and receiving the security policy sent from an SMF, sending same to the first security module to obtain the second data packet, and sending the second data packet to the receiver network element; the receiver network element is used for receiving the second data packet and obtaining the security policy, and sending the second data packet and the security policy to the second security module to obtain the third data packet. According to the embodiments of the present application, security related negotiation overhead is reduced, and the complexity in satellite communication management is reduced.

WO 2023/083346 A1

[见续页]

SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本公开实施例提供一种卫星通信系统，包括：发送方网元，第一安全模块、接收方网元和第二安全模块；第一安全模块用于基于安全策略对第一数据包进行第一安全处理生成数据包结构包含安全字段的第二数据包发送给发送方网元；第二安全模块用于基于安全策略对第二数据包进行第二安全处理获得包括第一数据包的数据的第三数据包发送给接收方网元；发送方网元用于生成第一数据包和接收SMF发送的安全策略，并发送给第一安全模块以获得第二数据包，并将第二数据包发送给接收方网元；接收方网元用于接收第二数据包并获取安全策略，将第二数据包和安全策略发送至第二安全模块以获取第三数据包。本公开实施例减少安全相关协商开销，降低卫星通信管理复杂度。

卫星通信系统、方法、装置、接收方网元及存储介质

相关申请的交叉引用

本申请要求于2021年11月15日提交的申请号为202111347750.2，发明名称为“卫星通信系统、方法、装置、接收方网元及存储介质”的中国专利申请的优先权，其通过引用方式全部并入本文。

技术领域

本公开涉及通信技术领域，尤其涉及一种卫星通信系统、方法、装置、接收方网元及存储介质。

背景技术

在通信系统中，从基站至核心网用户面功能(User Plane Function，UPF)对所有用户数据进行机密性和完整性保护时，可以不需要核心网络的干预或配置，因此，当前会话管理功能（Session ManagementFunction，SMF）下发给基站的安全策略不包含有基站与UPF之间的安全策略，并且SMF不向UPF下发任何安全策略，UPF也不处理任何与协议数据单元 (Protocol Data Unit，PDU)会话安全相关的内容。

而卫星的通信体制决定了承载网中的数据通信必须分为星间通信和星地通信2段。若直接应用传统的安全机制，目的卫星对信息的加密方式是未知的，无法对信息进行解密获得路由信息，进而无法确定下一跳的地址；若通信双方对信息的加密方式进行协商，复杂的密钥协商过程中通信资源高，卫星通信管理复杂。

发明内容

本公开实施例提供一种卫星通信系统、方法、装置、接收方网元及存储介质，用以解决现有技术中通信资源高，卫星通信管理复杂的缺陷，实现减少了安全相关协商的开销，降低了卫星通信管理的复杂度。

第一方面，本公开实施例提供一种卫星通信系统，包括:

发送方网元，所述发送方网元对应的第一安全模块、接收方网元、和所述接收方网元对应的第二安全模块，其中，所述发送方网元和所述接收方网元通过卫星承载网进行通信;

所述第一安全模块，用于接收所述发送方网元发送的第一数据包和所述卫星承载网的安全策略，并基于所述卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成第二数据包，所述第二数据包的数据包结构中包含安全字段，并将所述第二数据包发送给所述发送方网元;

所述第二安全模块，用于接收所述接收方网元发送的所述第二数据包，获取所述卫星承载网的安全策略，并基于所述卫星承载网的安全策略对所述第二数据包进行第二安全处理，获得第三数据包，所述第三数据包中包括所述第一数据包的数据，并将所述第三数据包发送给所述接收方网元;

所述发送方网元，用于生成所述第一数据包和接收会话管理功能SMF发送的所述卫星承载网的安全策略，并将所述第一数据包和所述卫星承载网的安全策略发送给所述第一安全模块，以获得所述第二数据包，并将所述第二数据包通过所述卫星承载网发送给所述接收方网元;

所述接收方网元，用于接收所述发送方网元通过所述卫星承载网发送的所述第二数据包，并获取所述卫星承载网的安全策略，并将所

述第二数据包和所述卫星承载网的安全策略发送至所述第二安全模块，以获取所述第三数据包。

可选地，根据本公开一个实施例的卫星通信系统，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

可选地，根据本公开一个实施例的卫星通信系统，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

可选地，根据本公开一个实施例的卫星通信系统，所述第一安全模块具体用于：接收所述发送方网元发送的第一数据包和所述卫星承载网的安全策略，基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第一数据包的第一安全处理，生成所述第二数据包，并将所述第二数据包发送给所述发送方网元。

可选地，根据本公开一个实施例的卫星通信系统，所述第二安全模块具体用于：接收所述接收方网元发送的所述第二数据包，基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第二数据包的第二安全处理，获得所述第三数据包，并将

所述第三数据包发送给所述接收方网元。

可选地，根据本公开一个实施例的卫星通信系统，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

可选地，根据本公开一个实施例的卫星通信系统，所述第一数据包的数据包结构包括 GTP-U 部分和安全字段部分，所述 GTP-U 部分包括目的网元 IP 地址部分，源网元 IP 地址部分，UDP 端口部分，GTP-U Header 部分，目的 IP 地址部分、源 IP 地址部分和 Payload 部分。

可选地，根据本公开一个实施例的卫星通信系统，处理所述第二数据包的协议层为卫星承载网数据传输协议栈中的安全层，所述安全层在 GTP-U 层与 PDU Layer 层之间。

可选地，根据本公开一个实施例的卫星通信系统，所述第一安全模块，具体用于以下至少一项：

若所述安全保护处理类型包括所述机密性保护处理，则对所述第一数据包的数据包结构中的所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，获得密文；

若所述安全保护处理类型包括所述完整性保护处理，则对所述第一数据包的数据包结构中的所述目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分、所述源 IP 地址部分和所述

Payload 部分进行完整性保护处理;

若所述安全保护处理类型包括所述机密性保护处理和所述完整性保护处理，则对所述第一数据包的数据包结构中的所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，获得密文，在所述机密性保护处理后，对所述第一数据包的数据包结构中的目的网元 IP 地址部分，所述源网元 IP 地址部分，所述 UDP 端口部分，所述 GTP-U Header 部分，所述安全字段部分，以及所述密文进行完整性保护。

可选地，根据本公开一个实施例的卫星通信系统，所述第二安全模块，具体用于以下至少一项:

若所述安全保护处理类型包括所述机密性保护处理，则对第二数据包的数据包结构中的密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分;

若所述安全保护处理类型包括所述完整性保护处理，则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分，所述源 IP 地址部分以及所述 Payload 部分进行完整性保护验证处理;

若所述安全保护处理类型包括所述机密性保护处理和所述完整性保护处理，则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、以及密文进行完整性保护验证处理，在所述完整性保护验证处理后，对所述密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分。

可选地，根据本公开一个实施例的卫星通信系统，所述第二数据包中的安全字段包含所述卫星承载网的安全策略，所述接收方网元获取的所述卫星承载网的安全策略是被携带在所述第二数据包中由所

述发送方网元发送至所述接收方网元的。

可选地，根据本公开一个实施例的卫星通信系统，所述 SMF 用于向所述发送方网元发送所述卫星承载网的安全策略。

可选地，根据本公开一个实施例的卫星通信系统，所述第二安全模块获取的所述卫星承载网的安全策略，是从所述第二数据包中的安全字段获取的。

可选地，根据本公开一个实施例的卫星通信系统，所述接收方网元获取的所述卫星承载网的安全策略是所述 SMF 发送给所述接收方网元的。

可选地，根据本公开一个实施例的卫星通信系统，所述 SMF 用于向所述发送方网元和所述接收方网元发送所述卫星承载网的安全策略。

可选地，根据本公开一个实施例的卫星通信系统，所述第二安全模块获取的所述卫星承载网的安全策略，是从所述接收方网元获取的。

可选地，根据本公开一个实施例的卫星通信系统，所述接收方网元还用于：在所述获取所述卫星承载网的安全策略之后，向所述第二安全模块发送所述卫星承载网的安全策略。

可选地，根据本公开一个实施例的卫星通信系统，所述卫星承载网的安全策略是所述 SMF 从安全管理实体获取的，所述安全管理实体包括统一数据管理功能 UDM。

第二方面，本公开实施例提供一种安全传输方法，应用于接收方网元，所述方法包括：

接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的；

将所述第二数据包发送至第二安全模块，以获取第三数据包，其

中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的；

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

可选地，根据本公开一个实施例的安全传输方法，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

可选地，根据本公开一个实施例的安全传输方法，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

可选地，根据本公开一个实施例的安全传输方法，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

可选地，根据本公开一个实施例的安全传输方法，所述第二数据

包中的安全字段包含所述卫星承载网的安全策略。

可选地，根据本公开一个实施例的安全传输方法，所述方法还包括：

接收 SMF 发送的所述卫星承载网的安全策略。

可选地，根据本公开一个实施例的安全传输方法，所述获取第三数据包之前，所述方法还包括：

向所述第二安全模块发送所述卫星承载网的安全策略。

第三方面，本公开实施例提供一种接收方网元，包括存储器，收发机，处理器：

存储器，用于存储计算机程序；收发机，用于在所述处理器的控制下收发数据；处理器，用于读取所述存储器中的计算机程序并执行以下操作：

接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的；

将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的；

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

可选地，根据本公开一个实施例的接收方网元，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

可选地，根据本公开一个实施例的接收方网元，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

可选地，根据本公开一个实施例的接收方网元，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

可选地，根据本公开一个实施例的接收方网元，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

可选地，根据本公开一个实施例的接收方网元，所述操作还包括：

接收 SMF 发送的所述卫星承载网的安全策略。

可选地，根据本公开一个实施例的接收方网元，所述获取第三数据包之前，所述操作还包括：

向所述第二安全模块发送所述卫星承载网的安全策略。

第四方面，本公开实施例提供一种安全传输装置，所述装置包括：

第一接收模块，用于接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略

经过第一安全处理后获得的；

第一发送模块，用于将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的；

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

第五方面，本公开实施例提供一种处理器可读存储介质，所述处理器可读存储介质存储有计算机程序，所述计算机程序用于使所述处理器执行第一方面所述的方法。

本公开实施例提供的卫星通信系统、方法、装置、接收方网元及存储介质，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

附图说明

为了更清楚地说明本公开实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本公开实施例提供的卫星通信实体关系图；

图 2 是本公开实施例提供的 PDU 会话用户面协议栈的示意图;

图 3 是本公开实施例提供的星间路由数据包结构的示意图;

图 4 是本公开实施例提供的卫星通信系统的结构示意图;

图 5 是本公开实施例提供的数据安全传输方式的流程示意图;

图 6 是本公开实施例提供的卫星基站至 UPF 安全流程的示意图;

图 7 是本公开实施例提供的卫星基站至卫星基站安全流程的示意图;

图 8 是本公开实施例提供的 UPF 至卫星基站安全流程的示意图;

图 9 是本公开实施例提供的卫星通信用户面数据安全架构的示意图;

图 10 是本公开实施例提供的数据包结构示意图;

图 11 是本公开实施例提供的数据传输协议栈的示意图;

图 12 是本公开实施例提供的安全传输方法的流程示意图;

图 13 是本公开实施例提供的安全传输装置的结构示意图;

图 14 是本公开实施例提供的接收方网元的结构示意图。

具体实施方式

本公开实施例中术语“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

本公开实施例中术语“多个”是指两个或两个以上，其它量词与之类似。

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本公开一部分实施例，并不是全部的实施例。基于本公开中的实施例，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，

都属于本公开保护的范围。

本公开实施例提供了卫星通信系统，用以减少安全相关协商的开销，降低卫星通信管理的复杂度。

本公开实施例提供的技术方案可以适用于多种系统，尤其是5G系统。例如适用的系统可以是全球移动通讯（global system of mobile communication，GSM）系统、码分多址（code division multiple access，CDMA）系统、宽带码分多址（Wideband Code Division Multiple Access，WCDMA）通用分组无线业务（general packet radio service，GPRS）系统、长期演进（long term evolution，LTE）系统、LTE频分双工（frequency division duplex，FDD）系统、LTE时分双工（time division duplex，TDD）系统、高级长期演进（long term evolution advanced，LTE-A）系统、通用移动系统（universal mobile telecommunication system，UMTS）、全球互联微波接入（worldwide interoperability for microwave access，WiMAX）系统、5G新空口（New Radio, NR）系统等。这多种系统中均包括终端设备和网络设备。系统中还可以包括核心网部分，例如演进的分组系统（Evloved Packet System, EPS）、5G系统（5GS）等。

本公开实施例涉及的终端设备，可以是指向用户提供语音和/或数据连通性的设备，具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备等。在不同的系统中，终端设备的名称可能也不相同，例如在5G系统中，终端设备可以称为用户设备（User Equipment，UE）。无线终端设备可以经无线接入网（Radio Access Network, RAN）与一个或多个核心网（Core Network, CN）进行通信，无线终端设备可以是移动终端设备，如移动电话（或称为“蜂窝”电话）和具有移动终端设备的计算机，例如，可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，它们与无线接入网交换语言和/或数据。例如，个人通信业务（Personal Communication Service，

PCS）电话、无绳电话、会话发起协议（Session Initiated Protocol，SIP）话机、无线本地环路（Wireless Local Loop，WLL）站、个人数字助理（Personal Digital Assistant，PDA）等设备。无线终端设备也可以称为系统、订户单元（subscriber unit）、订户站（subscriber station），移动站（mobile station）、移动台（mobile）、远程站（remote station）、接入点（access point）、远程终端设备（remote terminal）、接入终端设备（access terminal）、用户终端设备（user terminal）、用户代理（user agent）、用户装置（user device），本公开实施例中并不限定。

本公开实施例涉及的网络设备，可以是基站，该基站可以包括多个为终端提供服务的小区。根据具体应用场合不同，基站又可以称为接入点，或者可以是接入网中在空中接口上通过一个或多个扇区与无线终端设备通信的设备，或者其它名称。网络设备可用于将收到的空中帧与网际协议（Internet Protocol，IP）分组进行相互更换，作为无线终端设备与接入网的其余部分之间的路由器，其中接入网的其余部分可包括网际协议（IP）通信网络。网络设备还可协调对空中接口的属性管理。例如，本公开实施例涉及的网络设备可以是全球移动通信系统（Global System for Mobile communications，GSM）或码分多址接入（Code Division Multiple Access，CDMA）中的网络设备（Base Transceiver Station，BTS），也可以是带宽码分多址接入（Wide-band Code Division Multiple Access，WCDMA）中的网络设备（NodeB），还可以是长期演进（long term evolution，LTE）系统中的演进型网络设备（evolutional Node B，eNB 或 e-NodeB）、5G 网络架构（next generation system）中的 5G 基站（gNB），也可以是家庭演进基站（Home evolved Node B，HeNB）、中继节点（relay node）、家庭基站（femto）、微微基站（pico）等，本公开实施例中并不限定。在一些网络结构中，网络设备可以包括集中单元（centralized unit，CU）节点和分布单元（distributed unit，DU）节点，集中单元和分布单元也可以地理上分

开布置。

首先对以下内容进行介绍:

（1）图 1 是本公开实施例提供的卫星通信实体关系图，如图 1 所示，基于 5G 技术的卫星通信系统，可以有以下 a)-b)共 2 种通信模式:

a）UE 数据通过核心网实现数据转发至目的地，也即数据出网业务。

b）UE 数据不通过核心网，直接由卫星实现数据转发至另一个 UE，也即卫星终端对终端（Terminal to Terminal，T2T）业务。

当实现数据安全传输时:

出网业务数据安全可分为: UE（起始）-卫星（起始），卫星（起始）-卫星（目的），和卫星（目的）-地面站/核心网等 3 段。

T2T 业务数据安全可分为: UE（起始）-卫星（起始），卫星（起始）-卫星（目的），和卫星（目的）-UE（目的）等 3 段。

（2）通信网络中 PDU 会话用户面协议栈;

图 2 是本公开实施例提供的 PDU 会话用户面协议栈的示意图，如图 2 所示。在通信系统中，UPF 通常使用通用无线分组业务隧道协议（General packet radio service Tunneling Protocol，GTP）隧道来实现。GTPtunnel endpoint identifier）隧道是双向的，由源互联网协议（Internet Protocol，IP）地址、目的 IP 地址、用户数据报协议（User Datagram Protocol，UDP）端口号、源 GTP 隧道端点标识（Tunnel Endpoint Identifier，TEID），目的 GTP TEID 来标识。

图 3 是本公开实施例提供的星间路由数据包结构的示意图，如图 3 所示，星间路由数据包包括:

UE 处理的数据包: 目的 IP 地址，源 IP 地址，有效载荷（Payload）;

网元处理的数据包（卫星基站 S-gNB 或 S-UPF/UPF）: 目的网元 IP 地址，源网元 IP 地址，GTP-U Header，UE 数据包;

星间路由数据包：L2 标签，卫星基站 S-gNB 或 UPF 处理的数据包。

（3）UE 用户面数据加密保护;

其中，用户面数据分以下两段:

空口部分的用户面数据保护：即 UE 至基站 gNB 的机密性和完整性保护。该空口安全基于网络 SMF 提供给 gNB 的安全策略决定是否开启，以及开启哪些安全功能。

基站 gNB 至核心网网元 UPF 的安全保护：该保护采用互联网安全协议（Internet Protocol Security，IPSec）安全机制。网络不提供针对特定 UE 的安全策略，也即对所有用户数据均提供安全保护。

针对出网业务的用户数据，S-gNB 与地面 UPF 建立 GTP-U 隧道，用户面数据将在 GTP-U 隧道里进行传输。用户面数据包格式如图 3 所示。L2 标签用于星间路由。网元 IP 地址主要用于网元之间的 GTP-U 隧道的路由。

典型的数据加密方式是采用 3 段加密方式: UE-卫星，卫星-卫星，卫星-陆地站。也就是说，分别进行 3 次加解密。其中，UE-卫星可通过已有的 UE-基站（S-gNB）安全机制实现；卫星-卫星可通过星间通信安全机制实现，也即，对 GTP-U 信息进行加密，并利用星间路由机制将信息路由至目的卫星；目的卫星对信息解密后获得 GTP-U 中的路由信息，据此确定下一跳的目的，然后将 GTP-U 数据再次加密，并发送至陆地站。这种方式的缺点是增加了卫星资源的消耗。

若实现以 PDU 会话为单位，按需开启卫星至陆地站之间的安全通信能力，则意味需要将 PDU 会话安全策略提供给卫星和陆地站，并在两者之间建立安全关联。卫星的通信体制决定了承载网中的数据通信必须分为星间通信和星地通信 2 段。若直接将 3 段安全机制中的后 2 段进行简单合并，则意味着数据到达目的卫星后，因 GTP-U 中的路由信息加密，目的卫星不能确定下一跳的地址。另外，5G 核心

网并没有至承载网网元陆地站的接口（陆地站对核心网是透明的），因此 PDU 会话安全策略不能提供给卫星陆地站。

为了克服上述缺陷，本公开实施例提出了一种卫星通信系统。

图 4 是本公开实施例提供的卫星通信系统的结构示意图，如图 4 所示，该系统 400 包括：发送方网元 410、所述发送方网元对应的第一安全模块 420、接收方网元 430、和所述接收方网元对应的第二安全模块 440，其中，所述发送方网元 410 和所述接收方网元 430 通过卫星承载网进行通信；其中：

所述第一安全模块 420 用于接收所述发送方网元发送的第一数据包和所述卫星承载网的安全策略，并基于所述卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成第二数据包，所述第二数据包的数据包结构中包含安全字段，并将所述第二数据包发送给所述发送方网元；

所述第二安全模块 440 用于接收所述接收方网元发送的所述第二数据包，获取所述卫星承载网的安全策略，并基于所述卫星承载网的安全策略对所述第二数据包进行第二安全处理，获得第三数据包，所述第三数据包中包括所述第一数据包的数据，并将所述第三数据包发送给所述接收方网元；

所述发送方网元 410 用于生成所述第一数据包和接收会话管理功能 SMF 发送的所述卫星承载网的安全策略，并将所述第一数据包和所述卫星承载网的安全策略发送给所述第一安全模块，以获得所述第二数据包，并将所述第二数据包通过所述卫星承载网发送给所述接收方网元；

所述接收方网元 430 用于接收所述发送方网元通过所述卫星承载网发送的所述第二数据包，并获取所述卫星承载网的安全策略，并将所述第二数据包和所述卫星承载网的安全策略发送至所述第二安全模块，以获取所述第三数据包。

具体地，若实现按需开启卫星承载网的安全通信能力，比如卫星至陆地站之间的安全通信能力，则意味需要将安全策略提供给卫星和陆地站，并在两者之间建立安全关联。因此，为了实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，本公开实施例对 SMF 功能进行了扩展，SMF 在为 UE 建立 PDU 会话时可以向与承载网的连接的发送方网元，提供卫星承载网的安全策略，应用于卫星承载网数据传输。

具体地，发送方网元可以首先生成第一数据包，第一数据包中包括发送方网元需要发送的数据；在发送方网元接收到卫星承载网的安全策略后，可以将第一数据包和卫星承载网的安全策略发送第一安全模块；

具体地，该第一安全模块在获取到第一数据包和卫星承载网的安全策略后，可以基于该卫星承载网的安全策略对第一数据包进行第一安全处理，生成第二数据包，所述第二数据包的数据包结构中包含安全字段，该安全字段可以为空或可以包括卫星承载网的安全策略；

具体地，该第一安全模块可以是一个与发送方网元通信连接的实体模块，也可以是一个可以实现上述功能的虚拟模块。

具体地，在第一安全模块生成第二数据包后，可以将所述第二数据包发送给所述发送方网元；发送方网元获取到第二数据包后，可以将第二数据包通过卫星承载网发送给接收方网元；

具体地，本公开实施例中，卫星承载网不参与数据的安全保护相关工作。

具体地，在发送方网元将第二数据包发送给接收方网元后，接收方网元可以将第二数据包发送至第二安全模块；

具体地，第二安全模块可以获取第二数据包，还可以获取卫星承载网的安全策略，则可以基于卫星承载网的安全策略，对第二数据包进行第二安全处理，可以获取第三数据，该第三数据包括第一数据中

的数据，即第二安全处理可以理解为对第一安全处理后的数据包的恢复处理。

具体地，本公开实施例通过发送方网元和接收方网元获取到的卫星承载网的安全策略，发送方网元通过第一安全模块基于该卫星承载网的安全策略对向卫星承载网发送的数据包进行第一安全处理，接收方网元通过第二安全模块基于该卫星承载网的安全策略对从承载网接收的数据包进行第二安全处理，即第二安全模块基于卫星承载网的安全策略可以直接确定如何对接收到的第二数据包进行安全处理，从而实现按需提供数据安全传输的能力。

具体地，本公开实施例提供的卫星通信系统可以实现上述流程的数据安全传输方式，使卫星承载网两端的网元不必进行密钥和安全策略协商，即可以对需要传输的数据进行机密性和/或完整性保护。

本公开实施例提供的卫星通信系统，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

可选地，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

具体地，在卫星系统中，由于卫星资源有限，需要按需对用户数据进行机密性和/或完整性保护。

可选地，第一安全处理可以包括机密性保护处理，相应的，第二

第二安全处理可以包括解密处理;

可选地，第一安全处理可以包括完整性保护处理，相应的，第二第二安全处理可以包括完整性保护验证处理;

可选地，第一安全处理可以包括机密性保护处理和完整性保护处理，相应的，第二安全处理可以包括解密处理和完整性保护验证处理。

可选地，所述卫星承载网的安全策略包括以下至少一项:

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

具体地，卫星承载网的安全策略可以包括以下任一项或任意多项:

数据安全策略信息，用于指示第一安全处理包括的安全保护处理类型，所述安全保护处理类型包括以下至少一项：所述机密性保护处理和所述完整性保护处理，即用于指示是否需要对第一数据处理进行机密性保护处理，以及是否对第一数据处理进行完整性保护处理;

或者，

算法信息，用于指示实现所述机密性保护处理的算法和实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和实现所述完整性保护处理的密钥。

可选地，所述第一安全模块具体用于：接收所述发送方网元发送的第一数据包和所述卫星承载网的安全策略，基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所

述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第一数据包的第一安全处理，生成所述第二数据包，并将所述第二数据包发送给所述发送方网元。

具体地，在第一安全模块基于卫星承载网的安全策略，对第一数据包进行第一安全处理，获得第二数据包时，可以基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第一数据包的第一安全处理，生成所述第二数据包。

可选地，所述第二安全模块具体用于：接收所述接收方网元发送的所述第二数据包，基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第二数据包的第二安全处理，获得所述第三数据包，并将所述第三数据包发送给所述接收方网元。

具体地，在第二安全模块基于卫星承载网的安全策略，对第二数据包进行第二安全处理，获得第三数据包时，可以基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第二数据包的第二安全处理，获得所述第三数据包。

具体地，图 5 是本公开实施例提供的数据安全传输方式的流程示意图，如图 5 所示，数据安全传输的流程包括如下步骤（1）-（6）：

（1）UE 请求建立 PDU 会话；

（2）SMF 依据 UE 的签约信息获取适用于该 PDU 会话的卫星承载网的安全策略，该卫星承载网的安全策略描述的信息可以包括承载网安全保护使用不同的算法和密钥信息；

（3）SMF 基于获取的适用于该 PDU 会话的承载网安全策略生成承载网用户面上行和下行数据安全策略，并将安全策略分别发送至 PDU 会话隧道中与承载网两端连接的第三代伙伴计划协议（3rd Generation Partnership Project，3GPP）网元，也即 S-gNB 和/或 UPF;

（4）数据发送时，发送方网元执行如下(a)-（c）所示的操作:

（a）生成欲发送至接收方网元的第一数据包;

（b）基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型;

（c）基于所述算法信息中与所述安全保护处理类型对应的算法，和所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第一数据包的第一安全处理，生成第二数据包;

（5）发送方网元将第二数据包发送至接收方网元;

（6）接收方网元执行如下(d)-（e）所示的操作:

（d）基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型;

（e）基于所述算法信息中与所述安全保护处理类型对应的算法，和所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第二数据包的第二安全处理，获得第三数据包。

可选地，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

具体地，本公开实施例中的卫星承载网两端的发送方网元和接收

方网元可以至少有一方网元为卫星基站；

可选地，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；

图 6 是本公开实施例提供的卫星基站至 UPF 安全流程的示意图，如图 6 所示，其中在步骤 1-步骤 3 为由空口用户面(User Plane，UP)安全。为实现卫星承载网部分按需提供数据安全传输，基于 SMF 提供的卫星承载网的安全策略，在步骤 4-步骤 5 实现对用户面数据（第一数据包）进行第一安全处理获得第二数据包，然后第二数据包在承载网上传输；在 UPF 处，经步骤 11 至步骤 12，对第二数据包进行第二安全处理，获得数据明文；随后由已有协议继续进行相关处理。

可选地，所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；

图 7 是本公开实施例提供的卫星基站至卫星基站安全流程的示意图，如图 7 所示，该流程适用于卫星通信环境下的 T2T（终端至终端）安全；其中在步骤 1-步骤 3 为由空口 UP 安全。为实现卫星承载网部分按需提供数据安全传输，基于 SMF 提供的卫星承载网的安全策略，在步骤 4-步骤 5 实现对用户面数据（第一数据包）进行第一安全处理获得第二数据包，然后第二数据包在承载网上传输；在接收方的卫星基站处，经步骤 11 至步骤 12，对第二数据包进行第二安全处理，获得数据明文；随后由已有协议继续进行相关处理。

可选地，所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

图 8 是本公开实施例提供的 UPF 至卫星基站安全流程的示意图，如图 8 所示，其中在步骤 1-步骤 2 为 UPF 对用户面数据（第一数据包）进行第一安全处理，获得第二数据包，然后在承载网上传输；在

卫星基站 S-gNB 处，经步骤 8 至步骤 9，对第二数据包进行第二安全处理，获得数据明文；随后由已有协议继续进行相关处理。

图 9 是本公开实施例提供的卫星通信用户面数据安全架构的示意图，以图 9 中的卫星通信用户面数据安全架构为例，如图 9 所示，卫星通信系统所应用的卫星通信用户面数据安全架构可以由如下功能实体或模块组成：

卫星基站（S-gNB）：卫星上实现基站功能的功能实体；

卫星 UPF（S-UPF）：卫星上实现 UPF 功能的实体；

星间通信功能：负责卫星间数据通信的功能实体；

星载安全功能模块：卫星上负责卫星承载网安全相关操作的功能实体或虚拟模块；

馈电通信功能：卫星上负责卫星与地面站（信关站）间数据通信的功能实体；

地面站（信关站）：地面上负责与卫星进行通信的实体。核心网通过信关站与卫星相连接，并进一步与 UE 相连接；

核心网或信关站中部署的 UPF；

与 UPF 连接的地面站安全功能模块：地面站负责卫星承载网安全相关操作的功能实体或虚拟模块；

SMF：负责承载网两端 3GPP 网元用户面安全策略的分发。

可选地，所述第一数据包的数据包结构包括 GTP-U 部分和安全字段部分，所述 GTP-U 部分包括目的网元 IP 地址部分，源网元 IP 地址部分，UDP 端口部分，GTP-U Header 部分，目的 IP 地址部分、源 IP 地址部分和 Payload 部分。

具体地，本公开实施例中对第一数据包进行第一安全保护处理获得第二数据包，通过在数据包结构中加入安全字段，对传统的 GTP-U 数据包结构进行扩展，提出了新的数据包结构。

图 10 是本公开实施例提供的数据包结构示意图，如图 10 所示，

第一数据包的数据包结构包括 GTP-U 部分和安全字段部分，所述 GTP-U 部分包括目的网元 IP 地址部分，源网元 IP 地址部分，UDP 端口部分，GTP-U Header 部分，目的 IP 地址部分、源 IP 地址部分和 Payload 部分。

可选地，处理所述第二数据包的协议层为卫星承载网数据传输协议栈中的安全层，所述安全层在 GTP-U 层与 PDU Layer 层之间。

具体地，为实现按需提供卫星通信承载网数据安全传输的能力和减少卫星承载网分段处理数据安全的负担和开销，本公开实施例对传输用户面（UP）数据的网元之间的数据传输协议进行了扩展，可以增加一个安全层，从而使承载网不必处理数据安全相关的事项。

图 11 是本公开实施例提供的数据传输协议栈的示意图，为实现承载网数据安全传输，对数据传输协议栈增加了一个安全层，该层在 GTP-U 层与 PDU Layer 层之间。新的协议栈如图 11 所示，该层可以由生成和处理第一数据包和/或第二数据包的卫星基站 S-gNB 和/或 UPF 处理。

可选地，所述第一安全模块，具体用于以下至少一项:

若所述安全保护处理类型包括所述机密性保护处理，则对所述第一数据包的数据包结构中的所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，获得密文;

若所述安全保护处理类型包括所述完整性保护处理，则对所述第一数据包的数据包结构中的所述目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行完整性保护处理;

若所述安全保护处理类型包括所述机密性保护处理和所述完整性保护处理，则对所述第一数据包的数据包结构中的所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，

获得密文，在所述机密性保护处理后，对所述第一数据包的数据包结构中的目的网元 IP 地址部分，所述源网元 IP 地址部分，所述 UDP 端口部分，所述 GTP-U Header 部分，所述安全字段部分，以及所述密文进行完整性保护。

具体地，如图 7 所示，L2 标签用于星间路由；目的网元 IP 地址和源网元 IP 地址用于 S-gNB 和 UPF 之间路由或者两个 S-gNB 之间的路由；IP 地址，源 IP 地址和 Payload 为 UE 承载，可被机密性保护即加密处理；除 L2 标签外的其他数据被完整性保护。

可选地，第一安全模块在对第一数据包进行第一安全处理时，若所述安全保护处理类型包括所述机密性保护处理，则在对第一数据包进行第一安全处理时，可以对所述第一数据包的数据包结构中的目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，即进行加密处理，获得密文；

可选地，第一安全模块在对第一数据包进行第一安全处理时，若所述安全保护处理类型包括所述完整性保护处理，则对第一数据包的数据包结构中的所述目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行完整性保护处理；

可选地，第一安全模块在对第一数据包进行第一安全处理时，若所述安全保护处理类型同时包括所述机密性保护处理和所述完整性保护处理，可以先执行机密性处理再执行完整性保护处理，则可以首先对所述第一数据包的数据包结构中的所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，获得密文；在所述机密性保护处理后，可以再对所述第一数据包的数据包结构中的目的网元 IP 地址部分，所述源网元 IP 地址部分，所述 UDP 端口部分，所述 GTP-U Header 部分，所述安全字段部分，以及机密性保

护处理时获得的密文进行完整性保护。

可选地，所述第二安全模块，具体用于以下至少一项:

若所述安全保护处理类型包括所述机密性保护处理，则对第二数据包的数据包结构中的密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分;

若所述安全保护处理类型包括所述完整性保护处理，则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分，所述源 IP 地址部分以及所述 Payload 部分进行完整性保护验证处理;

若所述安全保护处理类型包括所述机密性保护处理和所述完整性保护处理，则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、以及密文进行完整性保护验证处理，在所述完整性保护验证处理后，对密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分。

可选地，第二安全模块在对第二数据包进行第二安全处理时，若安全保护处理类型包括所述机密性保护处理，则对第二数据包的数据包结构中的密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分;

可选地，第二安全模块在对第二数据包进行第二安全处理时，若所述安全保护处理类型包括所述完整性保护处理，则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分，所述源 IP 地址部分以及所述 Payload 部分进行完整性保护验证处理;

可选地，第二安全模块在对第二数据包进行第二安全处理时，若

所述安全保护处理类型包括所述机密性保护处理和所述完整性保护处理，首先进行完整性保护验证处理，再进行解密处理；即首先则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、以及密文进行完整性保护验证处理，在所述完整性保护验证处理后，对所述密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分。

可选地，所述第二数据包中的安全字段包含所述卫星承载网的安全策略，所述接收方网元获取的所述卫星承载网的安全策略是被携带在所述第二数据包中由所述发送方网元发送至所述接收方网元的。

可选地，可以通过第二数据包中的安全字段直接携带卫星承载网的安全策略的方式使卫星承载网的安全策略传输至接收方网元。

具体地，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。这种方式需要对安全字段里的内容进行修改。

本公开实施例中，可以通过安全字段将密钥和安全策略（即卫星承载网的安全策略）集成至所传输的第二数据包中。接收方网元可以通过该安全字段确定如何对接收到的第二数据包进行安全处理，从而减少了安全相关协商的开销，降低了卫星通信管理的复杂度。

可选地，所述 SMF 用于向所述发送方网元发送所述卫星承载网的安全策略。

具体地，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。这种方式需要对安全字段里的内容进行修改。相应的，SMF 只需要将安全策略发送至数据的发送方即可。接收方网元可以依据第二数据包中包含的安全字段确定如何处理第二数据包中的安全数据。

可选地，所述第二安全模块获取的所述卫星承载网的安全策略，是从所述第二数据包中的安全字段获取的。

可选地，在第二数据包的安全字段中携带卫星承载网的安全策略

的情况下，接收方网元在向第二安全模块发送第二数据包后，第二安全模块可以直接从第二数据包的安全字段获取卫星承载网的安全策略。

可选地，所述接收方网元获取的所述卫星承载网的安全策略是所述 SMF 发送给所述接收方网元的。

具体地，第二数据包中的安全字段可以为空，即第二数据包中不携带卫星承载网的安全策略。因此不需要对第一数据包中的安全字段进行修改。相应的，SMF 需要将安全策略分发至数据的发送方和接收方，以便双方能够正确处理相关数据。

具体地，第二数据包中的安全字段也可以不为空，即第二数据包中也可以携带卫星承载网的安全策略。相应地，SMF 也可以将安全策略分发至数据的发送方和接收方，以便双方能够正确处理相关数据。

可选地，所述 SMF 用于向所述发送方网元和所述接收方网元发送所述卫星承载网的安全策略。

具体地，第二数据包中的安全字段可以为空，即第二数据包中不携带卫星承载网的安全策略。因此不需要对第一数据包中的安全字段进行修改。相应的，需要将安全策略分发至发送方网元和接收方网元，以便双方能够正确处理相关数据，且有效避免安全相关协商带来的资源浪费。

可选地，所述第二安全模块获取的所述卫星承载网的安全策略，是从所述接收方网元获取的。

可选地，在第二数据包的安全字段中不携带卫星承载网的安全策略的情况下，接收方网元在向第二安全模块发送第二数据包时，还可以向第二安全模块发送从 SMF 获取的卫星承载网的安全策略。

可选地，所述接收方网元还用于：在所述获取所述卫星承载网的安全策略之后，向所述第二安全模块发送所述卫星承载网的安全策略。

可选地，接收方网元在接收到从 SMF 发送的卫星承载网的安全

策略之后，可以向第二安全模块发送所述卫星承载网的安全策略，以使第二安全模块基于卫星承载网的安全策略对第二数据包进行第二安全处理。

可选地，所述卫星承载网的安全策略是所述 SMF 从安全管理实体获取的，所述安全管理实体包括统一数据管理功能 UDM。

具体地，安全管理实体包括 UDM 或其他可以生成卫星承载网的安全策略的网元;

具体地，SMF 可以预先从统一数据管理功能 UDM 或其他可以生成卫星承载网的安全策略的网元获取卫星承载网的安全策略。

本公开实施例提供的卫星通信系统，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

图 12 是本公开实施例提供的安全传输方法的流程示意图，该方法应用于接收方网元，如图 12 所示，该方法包括如下流程:

步骤 1200，接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的;

步骤 1210，将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略

经过第二安全处理后获得的;

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

具体地，若实现按需开启卫星承载网的安全通信能力，比如卫星至陆地站之间的安全通信能力，则意味需要将安全策略提供给卫星和陆地站，并在两者之间建立安全关联。因此，为了实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，本公开实施例对 SMF 功能进行了扩展，SMF 在为 UE 建立 PDU 会话时可以向与承载网的连接的发送方网元，提供卫星承载网的安全策略，应用于卫星承载网数据传输。

具体地，接收方网元可以接收发送方网元通过卫星承载网发送的第二数据包，其中，第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的;

具体地，由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得第二数据包的方式可以如下（1）-（3）所示:

（1）发送方网元可以首先生成第一数据包，第一数据包中包括发送方网元需要发送的数据; 在发送方网元接收到卫星承载网的安全策略后，可以将第一数据包和卫星承载网的安全策略发送第一安全模块;

（2）该第一安全模块在获取到第一数据包和卫星承载网的安全策略后，可以基于该卫星承载网的安全策略对第一数据包进行第一安全处理，生成第二数据包，所述第二数据包的数据包结构中包含安全字段，该安全字段可以为空或可以包括卫星承载网的安全策略;

该第一安全模块可以是一个与发送方网元通信连接的实体模块，也可以是一个可以实现上述功能的虚拟模块。

（3）在第一安全模块生成第二数据包后，可以将所述第二数据

包发送给所述发送方网元；发送方网元获取到第二数据包后，可以将第二数据包通过卫星承载网发送给接收方网元；

具体地，本公开实施例中，卫星承载网不参与数据的安全保护相关工作。

具体地，在接收方网元接收到第二数据包后，接收方网元可以将第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的；

具体地，由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得第三数据包的方式可以如下所示：

在接收方网元接收到第二数据包后，接收方网元可以将第二数据包发送至第二安全模块，第二安全模块可以获取第二数据包，还可以获取卫星承载网的安全策略，则可以基于卫星承载网的安全策略，对第二数据包进行第二安全处理，可以获取第三数据，该第三数据包括第一数据中的数据，即第二安全处理可以理解为对第一安全处理后的数据包的恢复处理。

其中，第二安全模块基于卫星承载网的安全策略，对第二数据包进行第二安全处理，获取第三数据的方式可以如下所示：

在第二安全模块基于卫星承载网的安全策略，对第二数据包进行第二安全处理，获得第三数据包时，可以基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第二数据包的第二安全处理，获得所述第三数据包。

具体地，本公开实施例通过发送方网元和接收方网元获取到的卫星承载网的安全策略，发送方网元通过第一安全模块基于该卫星承载

网的安全策略对向卫星承载网发送的数据包进行第一安全处理，接收方网元通过第二安全模块基于该卫星承载网的安全策略对从承载网接收的数据包进行第二安全处理，即第二安全模块基于卫星承载网的安全策略可以直接确定如何对接收到的第二数据包进行安全处理，从而实现按需提供数据安全传输的能力。

具体地，本公开实施例提供的卫星通信系统可以实现上述流程的数据安全传输方式，使卫星承载网两端的网元不必进行密钥和安全策略协商，即可以对需要传输的数据进行机密性和/或完整性保护。

本公开实施例提供的卫星通信方法，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

可选地，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

具体地，在卫星系统中，由于卫星资源有限，需要按需对用户数据进行机密性和/或完整性保护。

可选地，第一安全处理可以包括机密性保护处理，相应的，第二第二安全处理可以包括解密处理；

可选地，第一安全处理可以包括完整性保护处理，相应的，第二第二安全处理可以包括完整性保护验证处理；

可选地，第一安全处理可以包括机密性保护处理和完整性保护处

理，相应的，第二安全处理可以包括解密处理和完整性保护验证处理。

可选地，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

具体地，卫星承载网的安全策略可以包括以下任一项或任意多项：

数据安全策略信息，用于指示第一安全处理包括的安全保护处理类型，所述安全保护处理类型包括以下至少一项：所述机密性保护处理和所述完整性保护处理，即用于指示是否需要对第一数据处理进行机密性保护处理，以及是否对第一数据处理进行完整性保护处理；

或者，

算法信息，用于指示实现所述机密性保护处理的算法和实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和实现所述完整性保护处理的密钥。

可选地，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

具体地，本公开实施例中的卫星承载网两端的发送方网元和接收方网元可以至少有一方网元为卫星基站；

可选地，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；

如图 6 所示，其中在步骤 1-步骤 3 为由空口 UP 安全。为实现卫星承载网部分按需提供数据安全传输，基于 SMF 提供的卫星承载网的安全策略，在步骤 4-步骤 5 实现对用户面数据（第一数据包）进行第一安全处理获得第二数据包，然后第二数据包在承载网上传输；在 UPF 处，经步骤 11 至步骤 12，对第二数据包进行第二安全处理，获得数据明文；随后由已有协议继续进行相关处理。

可选地，所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；

如图 7 所示，该流程适用于卫星通信环境下的 T2T（终端至终端）安全；其中在步骤 1-步骤 3 为由空口 UP 安全。为实现卫星承载网部分按需提供数据安全传输，基于 SMF 提供的卫星承载网的安全策略，在步骤 4-步骤 5 实现对用户面数据（第一数据包）进行第一安全处理获得第二数据包，然后第二数据包在承载网上传输；在接收方的卫星基站处，经步骤 11 至步骤 12，对第二数据包进行第二安全处理，获得数据明文；随后由已有协议继续进行相关处理。

可选地，所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

如图 8 所示，其中在步骤 1-步骤 2 为 UPF 对用户面数据（第一数据包）进行第一安全处理，获得第二数据包，然后在承载网上传输；在卫星基站 S-gNB 处，经步骤 8 至步骤 9，对第二数据包进行第二安全处理，获得数据明文；随后由已有协议继续进行相关处理。

可选地，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

具体地，本公开实施例中对第一数据包进行第一安全保护处理获得第二数据包，通过在数据包结构中加入安全字段，对传统的 GTP-U 数据包结构进行扩展，提出了新的数据包结构。

如图 10 所示，第一数据包的数据包结构包括 GTP-U 部分和安全字段部分，所述 GTP-U 部分包括目的网元 IP 地址部分，源网元 IP 地址部分，UDP 端口部分，GTP-U Header 部分，目的 IP 地址部分、源 IP 地址部分和 Payload 部分。

可选地，处理所述第二数据包的协议层为卫星承载网数据传输协议栈中的安全层，所述安全层在 GTP-U 层与 PDU Layer 层之间。

具体地，为实现按需提供卫星通信承载网数据安全传输的能力和减少卫星承载网分段处理数据安全的负担和开销，本公开实施例对传输用户面（UP）数据的网元之间的数据传输协议进行了扩展，可以增加一个安全层，从而使承载网不必处理数据安全相关的事项。

为实现承载网数据安全传输，对数据传输协议栈增加了一个安全层，该层在 GTP-U 层与 PDU Layer 层之间。新的协议栈如图 11 所示，该层可以由生成和处理第一数据包和/或第二数据包的卫星基站 S-gNB 和/或 UPF 处理。

可选地，所述方法还包括:

接收 SMF 发送的所述卫星承载网的安全策略。

具体地，第二数据包中的安全字段可以为空，即第二数据包中不携带卫星承载网的安全策略。因此不需要对第一数据包中的安全字段进行修改。相应的，接收方网元可以接收 SMF 发送的所述卫星承载网的安全策略，即 SMF 需要将安全策略分发至数据的发送方和接收方，以便双方能够正确处理相关数据。

具体地，第二数据包中的安全字段也可以不为空，即第二数据包

中也可以携带卫星承载网的安全策略。相应的，接收方网元可以接收SMF发送的所述卫星承载网的安全策略，即SMF也可以将安全策略分发至数据的发送方和接收方，以便双方能够正确处理相关数据。

可选地，所述获取第三数据包之前，所述方法还包括:

向所述第二安全模块发送所述卫星承载网的安全策略。

可选地，接收方网元在接收到从SMF发送的卫星承载网的安全策略之后，可以向第二安全模块发送所述卫星承载网的安全策略，以使第二安全模块基于卫星承载网的安全策略对第二数据包进行第二安全处理。

本公开实施例提供的卫星通信系统、方法、装置、接收方网元及存储介质，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

图13是本公开实施例提供的安全传输装置的结构示意图，如图13所示，该装置包括:

第一接收模块1310，用于接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于SMF提供的卫星承载网的安全策略经过第一安全处理后获得的;

第一发送模块1320，用于将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网

的安全策略经过第二安全处理后获得的；

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

其中，安全传输装置可以通过第一接收模块1310接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于SMF提供的卫星承载网的安全策略经过第一安全处理后获得的；然后可以通过发送模块1320将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的。

可选地，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

可选地，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

可选地，所述发送方网元为卫星基站S-gNB，所述接收方网元为用户面功能UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

可选地，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

可选地，所述装置还包括：

第二接收模块，用于接收 SMF 发送的所述卫星承载网的安全策略。

可选地，所述装置还包括：

第二发送模块，用于在所述获取第三数据包之前，向所述第二安全模块发送所述卫星承载网的安全策略。

本公开实施例提供的卫星通信装置，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

需要说明的是，本公开实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。另外，在本公开各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的

产品销售或使用时，可以存储在一个处理器可读取存储介质中。基于这样的理解，本公开的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本公开各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory ，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

在此需要说明的是，本发明实施例提供的上述装置，能够实现上述方法实施例所实现的所有方法步骤，且能够达到相同的技术效果，在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

图 14 是本公开实施例提供的接收方网元的结构示意图，如图 14 所示，所述接收方网元包括存储器 1420，收发机 1400，处理器 1410，其中包括存储器，收发机，处理器：

存储器 1420，用于存储计算机程序；收发机，用于在所述处理器 1410 的控制下收发数据；处理器 1410，用于读取所述存储器中 1420 的计算机程序并执行以下操作：

接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的；

将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的；

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

本公开实施例提供的接收方网元，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

可选地，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

可选地，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

可选地，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

可选地，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

可选地，处理器 1410 还用于:

接收 SMF 发送的所述卫星承载网的安全策略。

可选地，处理器 1410 还用于:

在所述获取第三数据包之前，向所述第二安全模块发送所述卫星承载网的安全策略。

本公开实施例提供的接收方网元，通过第一安全模块基于发送方网元拥有的卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成数据包结构中包含安全字段的第二数据包，并由发送方网元将其发送至接收方网元，接收方网元接收到第二数据包后，可以通过第二安全模块，基于获取到的卫星承载网的安全策略对第二数据包进行第二安全处理，获取包含第一数据包的数据的第三数据包，进而实现承载网两端的网元不必进行密钥和安全策略协商即可以对需要传输的数据进行保护，减少安全相关协商的开销，降低卫星通信管理的复杂度。

具体地，收发机 1400，用于在处理器 1410 的控制下接收和发送数据。

其中，在图 14 中，总线架构可以包括任意数量的互联的总线和桥，具体由处理器 1410 代表的一个或多个处理器和存储器 1420 代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机 1400 可以是多个元件，即包括发送机和接收机，提

供用于在传输介质上与各种其他装置通信的单元，这些传输介质包括无线信道、有线信道、光缆等传输介质。处理器 1410 负责管理总线架构和通常的处理，存储器 1420 可以存储处理器 1410 在执行操作时所使用的数据。

处理器 1410 可以是中央处理器（Central Processing Unit, CPU）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field－Programmable Gate Array，FPGA）或复杂可编程逻辑器件（Complex Programmable Logic Device，CPLD），处理器也可以采用多核架构。

在此需要说明的是，本公开实施例提供的上述接收方网元，能够实现上述执行主体为接收方网元的方法实施例所实现的所有方法步骤，且能够达到相同的技术效果，在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

另一方面，本公开实施例还提供一种处理器可读存储介质，所述处理器可读存储介质存储有计算机程序，所述计算机程序用于使所述处理器执行上述各实施例提供的方法，包括:

接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的;

将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的;

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

所述处理器可读存储介质可以是处理器能够存取的任何可用介

质或数据存储设备，包括但不限于磁性存储器（例如软盘、硬盘、磁带、磁光盘（MO）等）、光学存储器（例如CD、DVD、BD、HVD等）、以及半导体存储器（例如ROM、EPROM、EEPROM、非易失性存储器（NAND FLASH）、固态硬盘（SSD））等。

本领域内的技术人员应明白，本公开的实施例可提供为方法、系统、或计算机程序产品。因此，本公开可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本公开可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

本公开是参照根据本公开实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机可执行指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机可执行指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些处理器可执行指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的处理器可读存储器中，使得存储在该处理器可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些处理器可执行指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方

框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本公开进行各种改动和变型而不脱离本公开的精神和范围。这样，倘若本公开的这些修改和变型属于本公开权利要求及其等同技术的范围之内，则本公开也意图包含这些改动和变型在内。

权 利 要 求 书

1、一种卫星通信系统，其特征在于，包括：发送方网元，所述发送方网元对应的第一安全模块、接收方网元、和所述接收方网元对应的第二安全模块，其中，所述发送方网元和所述接收方网元通过卫星承载网进行通信；

所述第一安全模块，用于接收所述发送方网元发送的第一数据包和所述卫星承载网的安全策略，并基于所述卫星承载网的安全策略对所述第一数据包进行第一安全处理，生成第二数据包，所述第二数据包的数据包结构中包含安全字段，并将所述第二数据包发送给所述发送方网元；

所述第二安全模块，用于接收所述接收方网元发送的所述第二数据包，获取所述卫星承载网的安全策略，并基于所述卫星承载网的安全策略对所述第二数据包进行第二安全处理，获得第三数据包，所述第三数据包中包括所述第一数据包的数据，并将所述第三数据包发送给所述接收方网元；

所述发送方网元，用于生成所述第一数据包和接收会话管理功能SMF发送的所述卫星承载网的安全策略，并将所述第一数据包和所述卫星承载网的安全策略发送给所述第一安全模块，以获得所述第二数据包，并将所述第二数据包通过所述卫星承载网发送给所述接收方网元；

所述接收方网元，用于接收所述发送方网元通过所述卫星承载网发送的所述第二数据包，并将所述第二数据包发送至所述第二安全模块，以获取所述第三数据包。

2、根据权利要求1所述的卫星通信系统，其特征在于，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

3、根据权利要求 2 所述的卫星通信系统，其特征在于，所述卫星承载网的安全策略包括以下至少一项:

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

4、根据权利要求 3 所述的卫星通信系统，其特征在于，所述第一安全模块具体用于: 接收所述发送方网元发送的第一数据包和所述卫星承载网的安全策略，基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第一数据包的第一安全处理，生成所述第二数据包，并将所述第二数据包发送给所述发送方网元。

5、根据权利要求 3 所述的卫星通信系统，其特征在于，所述第二安全模块具体用于: 接收所述接收方网元发送的所述第二数据包，基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型，并基于所述算法信息中与所述安全保护处理类型对应的算法，以及所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第二数据包的第二安全处理，获得所述第三数据包，并将所述第三数据包发送给所述接收方网元。

6、根据权利要求 1-5 任一项所述的卫星通信系统，其特征在于，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为

地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

7、根据权利要求 3-5 任一项所述的卫星通信系统，其特征在于，所述第一数据包的数据包结构包括 GTP-U 部分和安全字段部分，所述 GTP-U 部分包括目的网元 IP 地址部分，源网元 IP 地址部分，UDP 端口部分，GTP-U Header 部分，目的 IP 地址部分、源 IP 地址部分和 Payload 部分。

8、根据权利要求 7 所述的卫星通信系统，其特征在于，处理所述第二数据包的协议层为卫星承载网数据传输协议栈中的安全层，所述安全层在 GTP-U 层与 PDU Layer 层之间。

9、根据权利要求 7 所述的卫星通信系统，其特征在于，所述第一安全模块，具体用于以下至少一项：

若所述安全保护处理类型包括所述机密性保护处理，则对所述第一数据包的数据包结构中的所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，获得密文；

若所述安全保护处理类型包括所述完整性保护处理，则对所述第一数据包的数据包结构中的所述目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行完整性保护处理；

若所述安全保护处理类型包括所述机密性保护处理和所述完整性保护处理，则对所述第一数据包的数据包结构中的所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分进行机密性保护处理，

获得密文，在所述机密性保护处理后，对所述第一数据包的数据包结构中的目的网元 IP 地址部分，所述源网元 IP 地址部分，所述 UDP 端口部分，所述 GTP-U Header 部分，所述安全字段部分，以及所述密文进行完整性保护。

10、根据权利要求 7 所述的卫星通信系统，其特征在于，所述第二安全模块，具体用于以下至少一项:

若所述安全保护处理类型包括所述机密性保护处理，则对第二数据包的数据包结构中的密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分;

若所述安全保护处理类型包括所述完整性保护处理，则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、所述目的 IP 地址部分，所述源 IP 地址部分以及所述 Payload 部分进行完整性保护验证处理;

若所述安全保护处理类型包括所述机密性保护处理和所述完整性保护处理，则对第二数据包的数据包结构中的目的网元 IP 地址部分、所述源网元 IP 地址部分、所述 UDP 端口部分、所述 GTP-U Header 部分、所述安全字段部分、以及密文进行完整性保护验证处理，在所述完整性保护验证处理后，对所述密文进行解密处理，获得所述目的 IP 地址部分、所述源 IP 地址部分和所述 Payload 部分。

11、根据权利要求 1-5 任一项或 8-10 任一项所述的卫星通信系统，其特征在于，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

12、根据权利要求 11 所述的卫星通信系统，其特征在于，所述 SMF 用于向所述发送方网元发送所述卫星承载网的安全策略。

13、根据权利要求 11 所述的卫星通信系统，其特征在于，所述第二安全模块获取的所述卫星承载网的安全策略，是从所述第二数据

包中的安全字段获取的。

14、根据权利要求1-5任一项或8-10任一项所述的卫星通信系统，其特征在于，所述接收方网元还用于接收所述SMF发送的所述卫星承载网的安全策略。

15、根据权利要求14所述的卫星通信系统，其特征在于，所述SMF用于向所述发送方网元和所述接收方网元发送所述卫星承载网的安全策略。

16、根据权利要求14所述的卫星通信系统，其特征在于，所述第二安全模块获取的所述卫星承载网的安全策略，是从所述接收方网元获取的。

17、根据权利要求16所述的卫星通信系统，其特征在于，所述接收方网元还用于：在所述获取所述卫星承载网的安全策略之后，向所述第二安全模块发送所述卫星承载网的安全策略。

18、根据权利要求12或15所述的卫星通信系统，其特征在于，所述卫星承载网的安全策略是所述SMF从安全管理实体获取的，所述安全管理实体包括统一数据管理功能UDM。

19、一种安全传输方法，其特征在于，应用于接收方网元，所述方法包括：

接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于SMF提供的卫星承载网的安全策略经过第一安全处理后获得的；

将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的；

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进

行通信。

20、根据权利要求 19 所述的安全传输方法，其特征在于，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

21、根据权利要求 20 所述的安全传输方法，其特征在于，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

22、根据权利要求 19-21 任一项所述的安全传输方法，其特征在于，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

23、根据权利要求 19-21 任一项所述的安全传输方法，其特征在于，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

24、根据权利要求 19-21 任一项所述的安全传输方法，其特征在于，所述方法还包括：

接收 SMF 发送的所述卫星承载网的安全策略。

25、根据权利要求 24 所述的安全传输方法，其特征在于，所述获取第三数据包之前，所述方法还包括:

向所述第二安全模块发送所述卫星承载网的安全策略。

26、一种接收方网元，包括存储器，收发机，处理器:

存储器，用于存储计算机程序；收发机，用于在所述处理器的控制下收发数据；处理器，用于读取所述存储器中的计算机程序并执行以下操作:

接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的;

将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的;

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

27、根据权利要求 26 所述的接收方网元，其特征在于，所述第一安全处理包括以下至少一项: 机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项: 解密处理和完整性保护验证处理。

28、根据权利要求 27 所述的接收方网元，其特征在于，所述卫星承载网的安全策略包括以下至少一项:

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

29、根据权利要求 26-28 任一项所述的接收方网元，其特征在于，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

30、根据权利要求 26-28 任一项所述的接收方网元，其特征在于，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

31、根据权利要求 26-28 任一项所述的接收方网元，其特征在于，所述操作还包括：

接收 SMF 发送的所述卫星承载网的安全策略。

32、根据权利要求 31 所述的接收方网元，其特征在于，所述获取第三数据包之前，所述操作还包括：

向所述第二安全模块发送所述卫星承载网的安全策略。

33、一种安全传输装置，其特征在于，所述装置包括：

第一接收模块，用于接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于 SMF 提供的卫星承载网的安全策略经过第一安全处理后获得的；

第一发送模块，用于将所述第二数据包发送至第二安全模块，以

获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的；

其中，所述发送方网元和所述接收方网元通过所述卫星承载网进行通信。

34、根据权利要求 33 所述的安全传输装置，其特征在于，所述第一安全处理包括以下至少一项：机密性保护处理和完整性保护处理，所述第二安全处理包括以下至少一项：解密处理和完整性保护验证处理。

35、根据权利要求 34 所述的安全传输装置，其特征在于，所述卫星承载网的安全策略包括以下至少一项：

数据安全策略信息，所述数据安全策略信息用于指示所述第一安全处理包括的安全保护处理类型，其中所述安全保护处理类型包括所述机密性保护处理和/或所述完整性保护处理；或

算法信息，所述算法信息用于指示实现所述机密性保护处理的算法和/或实现所述完整性保护处理的算法；或

密钥信息，所述密钥信息用于指示实现所述机密性保护处理的密钥和/或实现所述完整性保护处理的密钥。

36、根据权利要求 33-35 任一项所述的安全传输装置，其特征在于，所述发送方网元为卫星基站 S-gNB，所述接收方网元为用户面功能 UPF，所述第一安全模块为星载安全功能模块，所述第二安全模块为地面站安全功能模块；或

所述发送方网元和所述接收方网元均为卫星基站 S-gNB，所述第一安全模块和所述第二安全模块均为星载安全功能模块；或

所述发送方网元为用户面功能 UPF，所述接收方网元为卫星基站 S-gNB，所述第一安全模块为地面站安全功能模块，所述第二安全模块为星载安全功能模块。

37、根据权利要求 33-35 任一项所述的安全传输装置，其特征在于，所述第二数据包中的安全字段包含所述卫星承载网的安全策略。

38、根据权利要求 33-35 任一项所述的安全传输装置，其特征在于，所述装置还包括:

第二接收模块，用于接收 SMF 发送的所述卫星承载网的安全策略。

39、根据权利要求 38 所述的安全传输装置，其特征在于，所述获取第三数据包之前，所述装置还包括:

第二发送模块，用于向所述第二安全模块发送所述卫星承载网的安全策略。

40、一种处理器可读存储介质，其特征在于，所述处理器可读存储介质存储有计算机程序，所述计算机程序用于使所述处理器执行权利要求 19 至 25 任一项所述的方法。

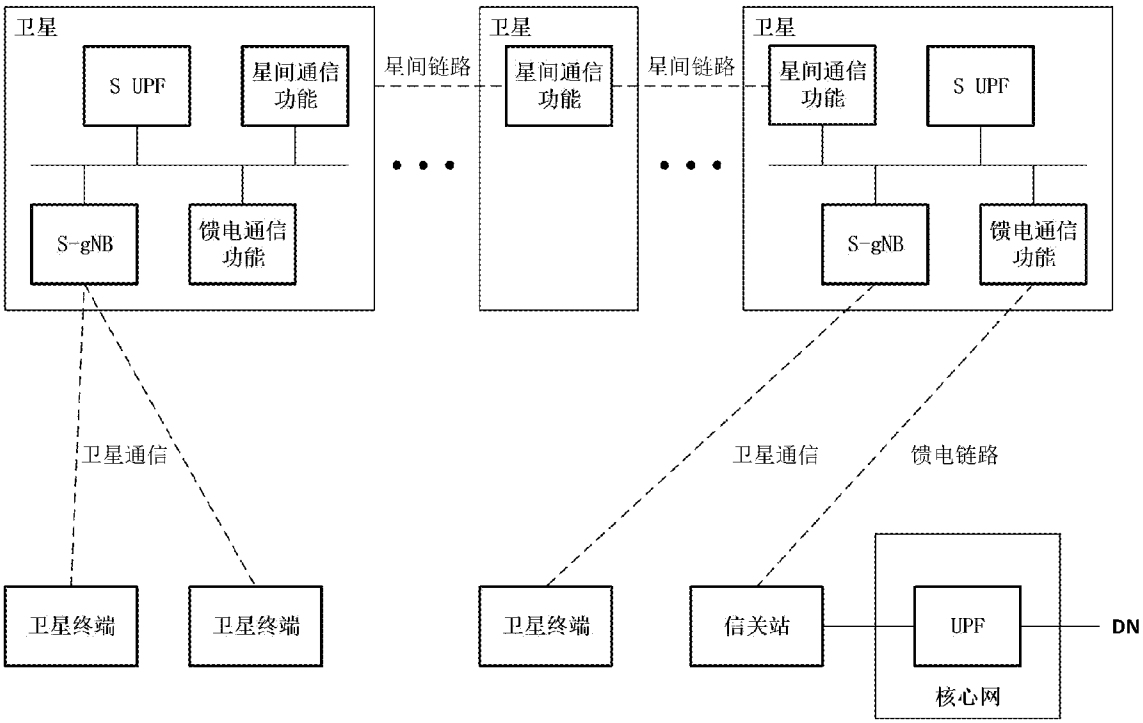

图 1

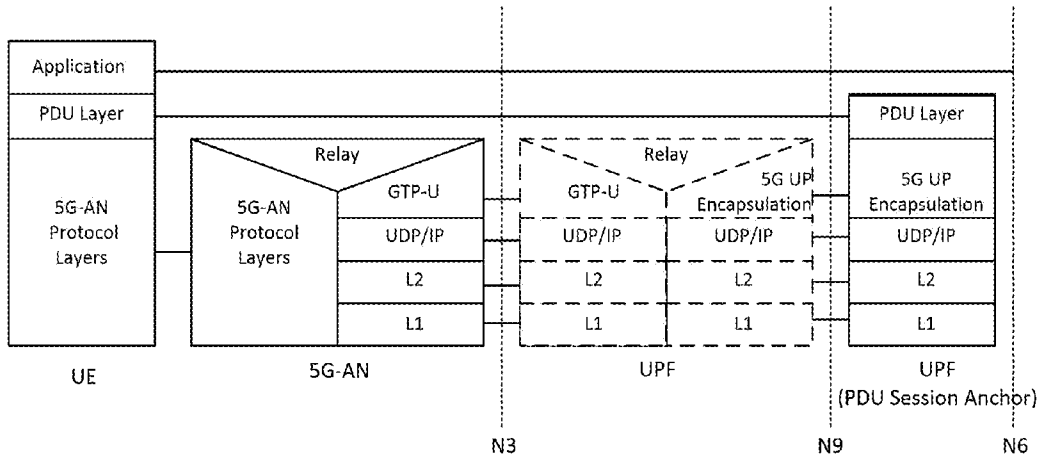

图 2

L2 标签	目的网元IP地址	源网元IP地址	UDP端口	GTP-U Header	目的IP地址	源IP地址	Payload

图 3

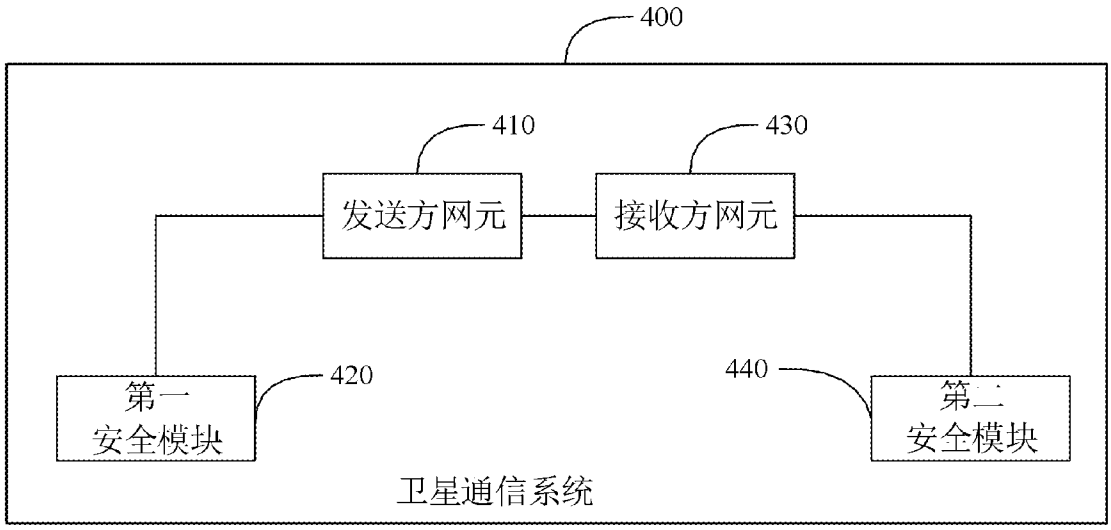
400
410
发送方网元
430
接收方网元
第一
安全模块
420
440
第二
安全模块
卫星通信系统

图 4

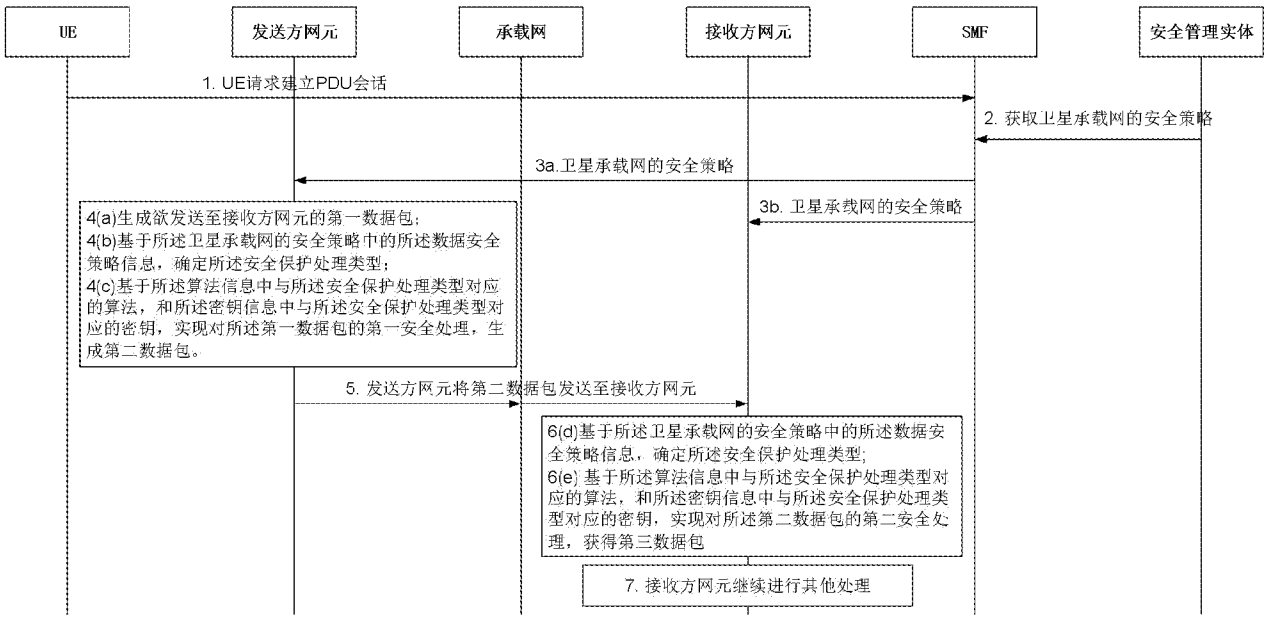
UE
发送方网元
承载网
接收方网元
SMF
安全管理实体
1. UE请求建立PDU会话
2. 获取卫星承载网的安全策略
3a.卫星承载网的安全策略
3b. 卫星承载网的安全策略
4(a)生成欲发送至接收方网元的第一数据包;
4(b)基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型;
4(c)基于所述算法信息中与所述安全保护处理类型对应的算法，和所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第一数据包的第一安全处理，生成第二数据包。
5. 发送方网元将第二数据包发送至接收方网元
6(d)基于所述卫星承载网的安全策略中的所述数据安全策略信息，确定所述安全保护处理类型;
6(e) 基于所述算法信息中与所述安全保护处理类型对应的算法，和所述密钥信息中与所述安全保护处理类型对应的密钥，实现对所述第二数据包的第二安全处理，获得第三数据包
7. 接收方网元继续进行其他处理

图 5

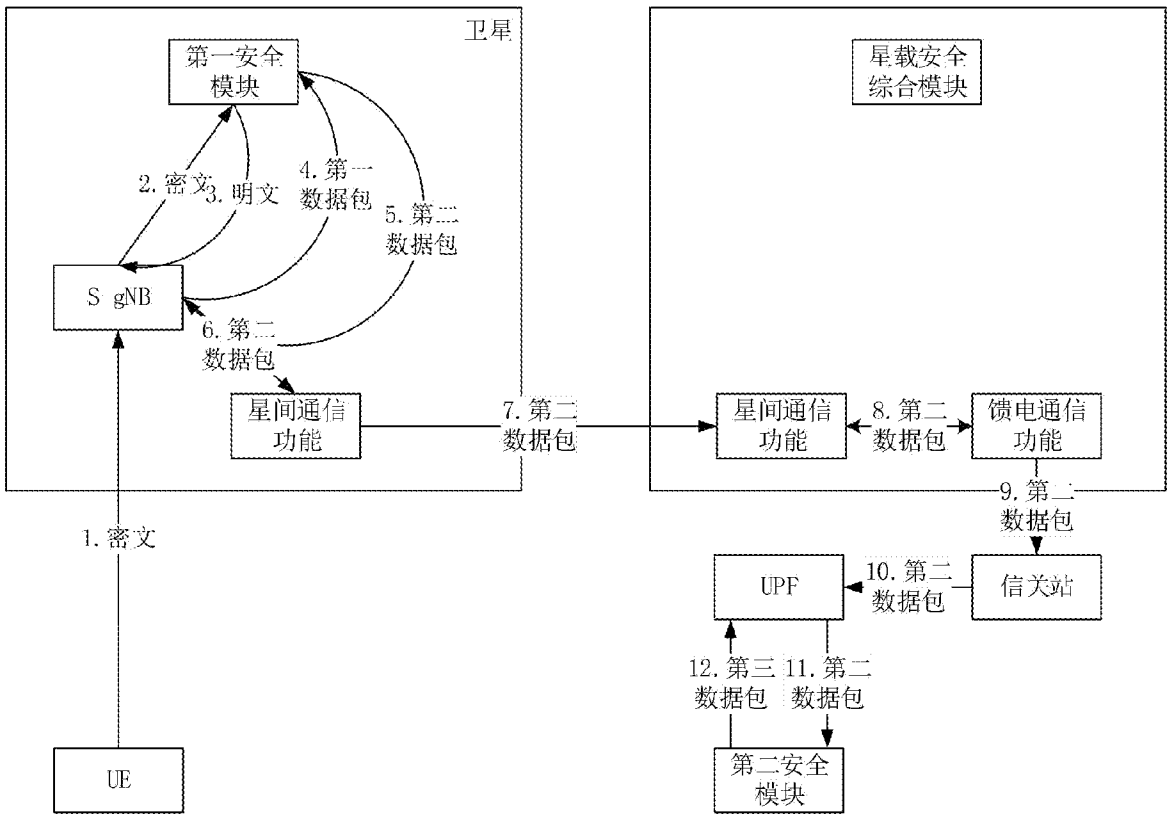
卫星
第一安全模块
2. 密文
3. 明文
4. 第一数据包
5. 第二数据包
S gNB
6. 第二数据包
星间通信功能
7. 第二数据包
星载安全综合模块
星间通信功能
8. 第二数据包
馈电通信功能
9. 第二数据包
1. 密文
UPF
10. 第二数据包
信关站
12. 第三数据包
11. 第二数据包
第二安全模块
UE

图 6

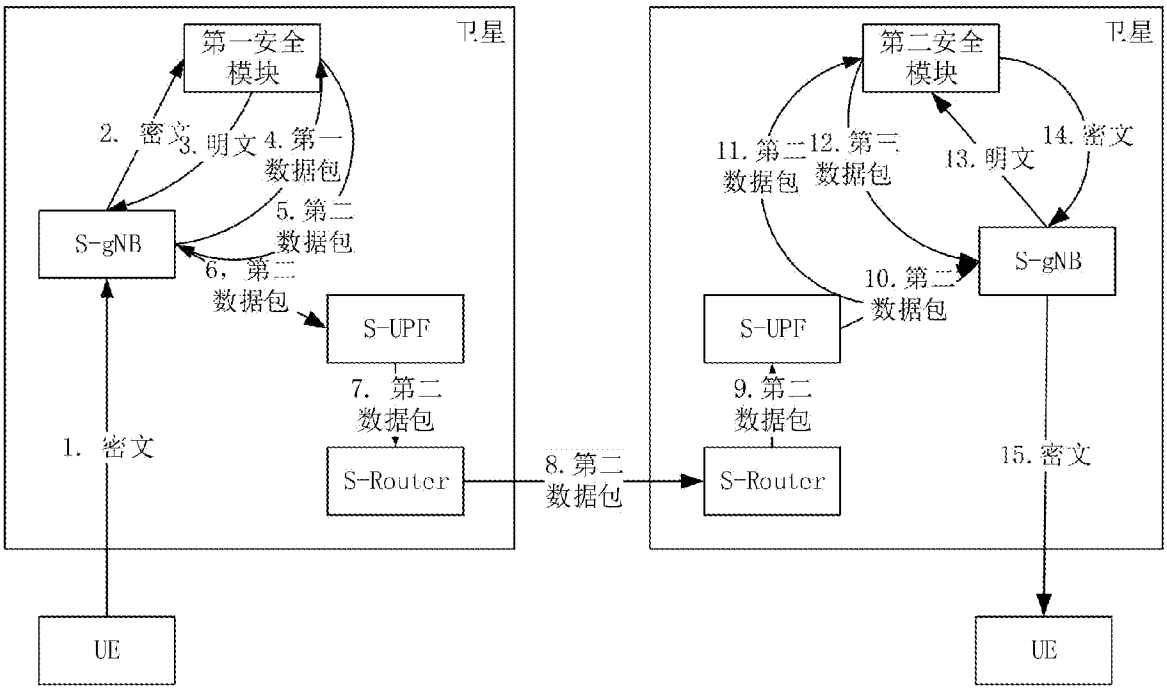
卫星
第一安全模块
2. 密文
3. 明文
4. 第一数据包
5. 第二数据包
S-gNB
6. 第二数据包
S-UPF
7. 第二数据包
1. 密文
S-Router
8. 第二数据包
卫星
第二安全模块
11. 第二数据包
12. 第三数据包
13. 明文
14. 密文
S-gNB
10. 第二数据包
S-UPF
9. 第二数据包
S-Router
15. 密文
UE
UE

图 7

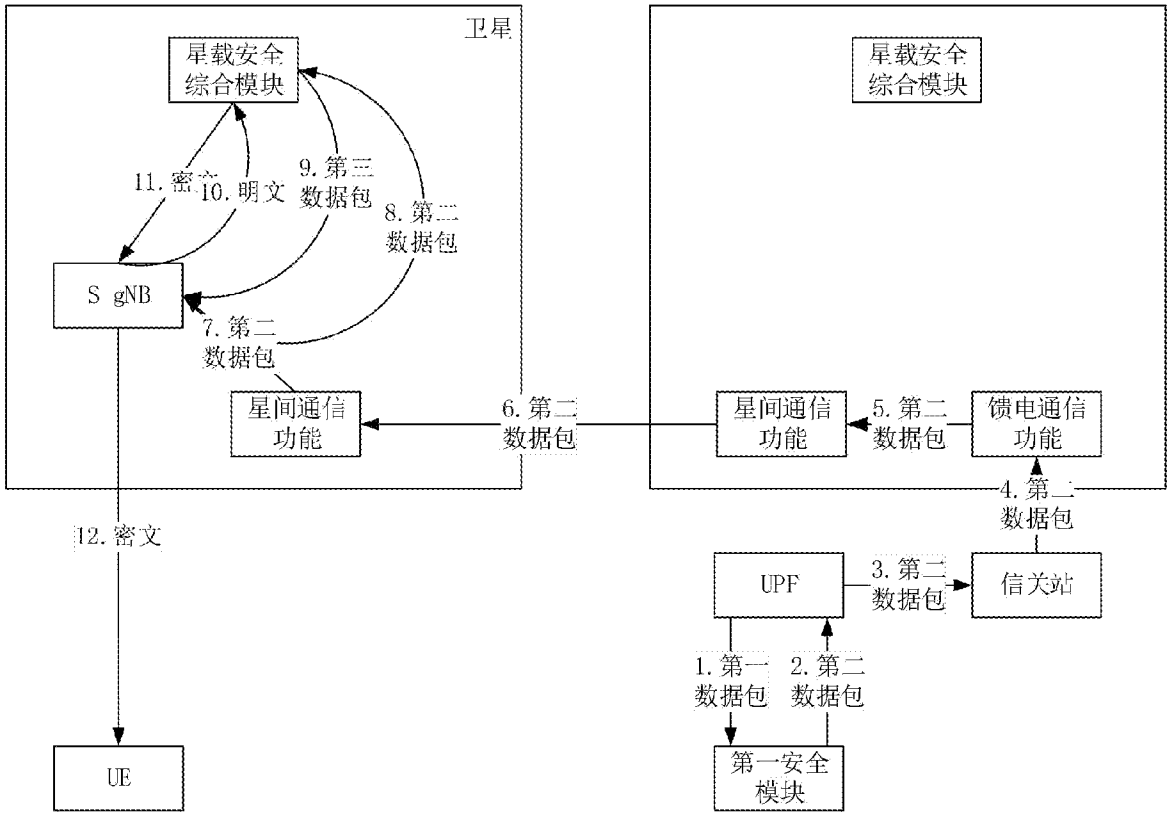
卫星
星载安全综合模块
星载安全综合模块
11. 密文
10. 明文
9. 第三数据包
8. 第二数据包
S gNB
7. 第二数据包
星间通信功能
6. 第二数据包
星间通信功能
5. 第二数据包
馈电通信功能
4. 第二数据包
12. 密文
UPF
3. 第二数据包
信关站
1. 第一数据包
2. 第二数据包
UE
第一安全模块

图 8

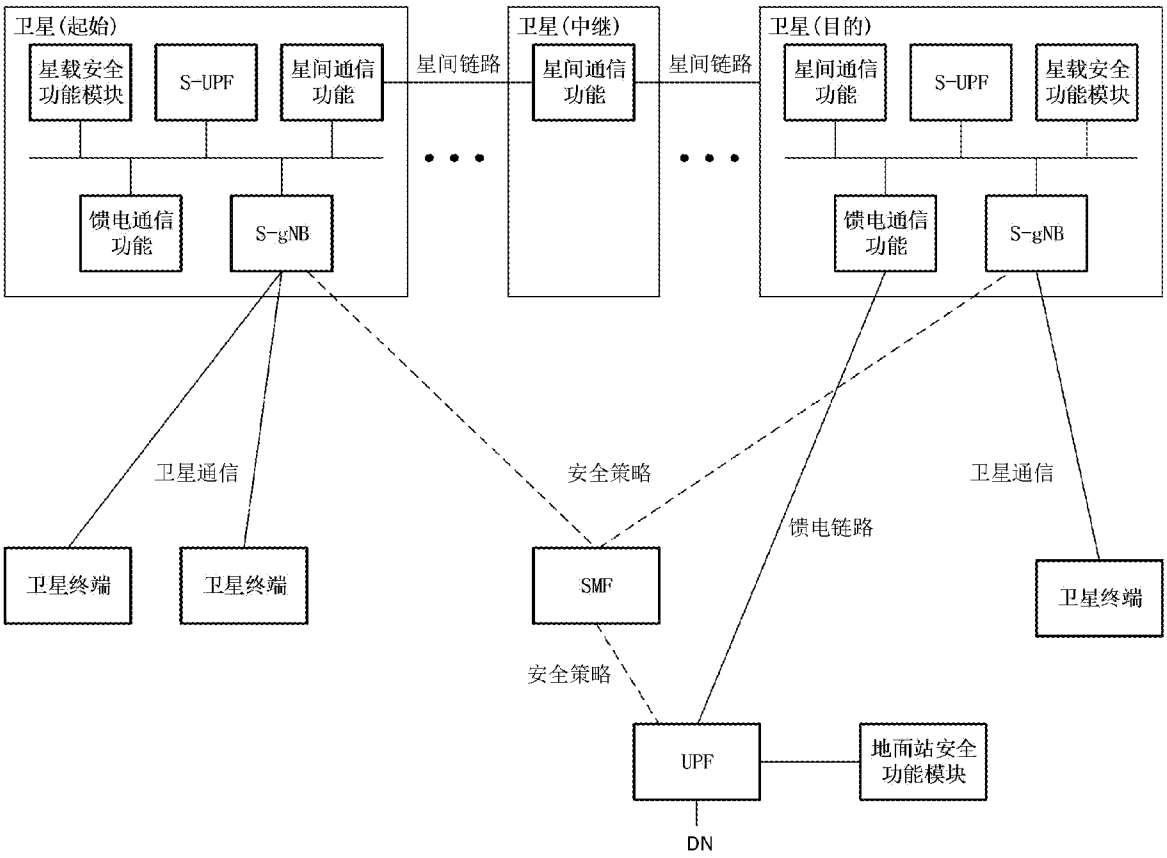

图 9

L2 标签	目的网元IP地址	源网元IP地址	UDP端口	GTP-U Header	安全字段	目的IP地址	源IP地址	Payload

图 10

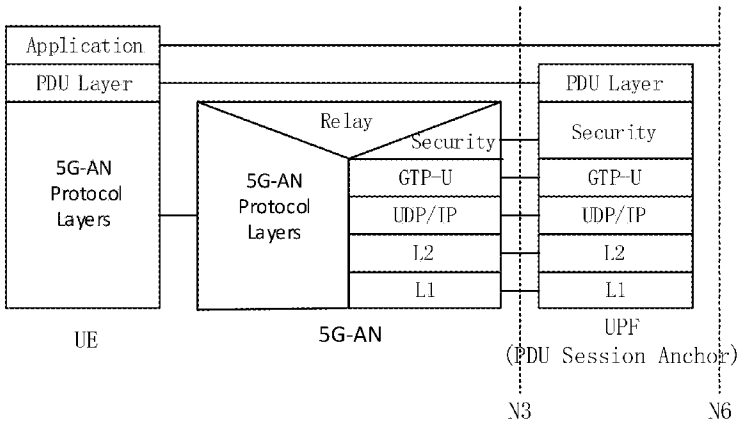

图 11

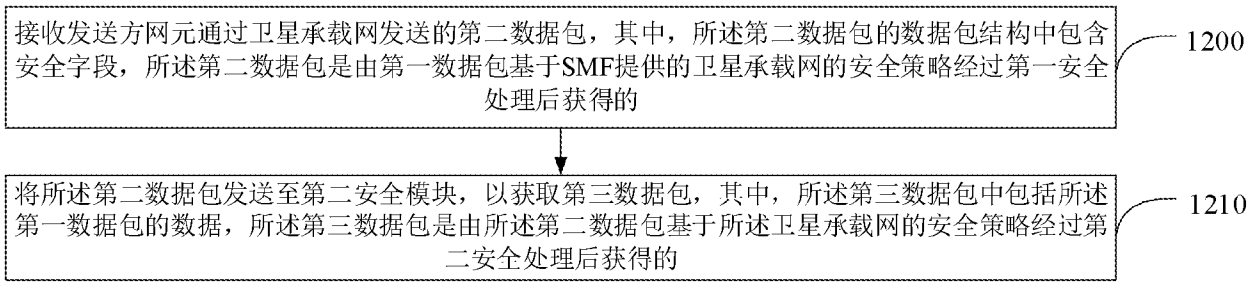
接收发送方网元通过卫星承载网发送的第二数据包，其中，所述第二数据包的数据包结构中包含安全字段，所述第二数据包是由第一数据包基于SMF提供的卫星承载网的安全策略经过第一安全处理后获得的
1200
将所述第二数据包发送至第二安全模块，以获取第三数据包，其中，所述第三数据包中包括所述第一数据包的数据，所述第三数据包是由所述第二数据包基于所述卫星承载网的安全策略经过第二安全处理后获得的
1210

图 12

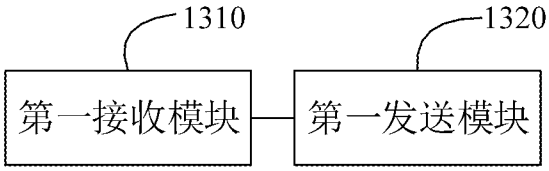
1310
1320
第一接收模块
第一发送模块

图 13

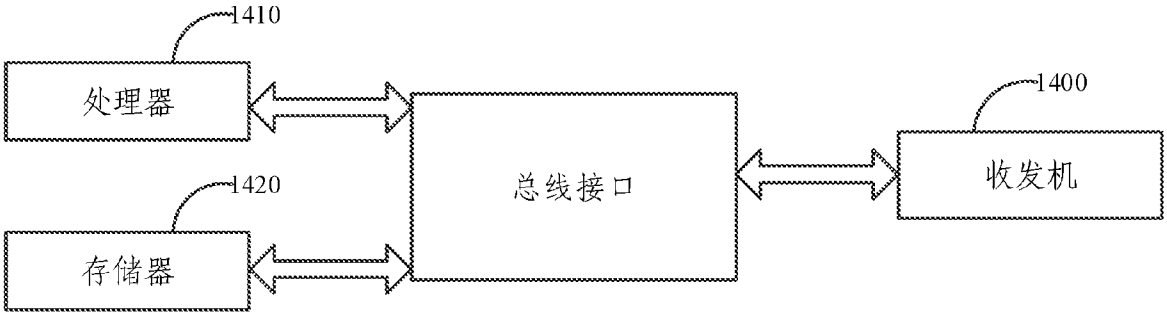
1410
处理器
1420
存储器
总线接口
1400
收发机

图 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/131721

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/106(2021.01)i;H04W12/10(2021.01)i;H04W12/03(2021.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W12/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; DWPI; USTXT; EPTXT; WOTXT; IEEE; 3GPP: 安全, 策略, 会话管理, 机密, 加密, 完整性, 卫星, 基站, 地面站, 信关站, 用户面, encrypt, integrity, policy, satellite, SMF, UPF, session mangement, user platform, secur +, S-gNB, gNB, ground, gatway, generation NodeB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 110912854 A (HUAWEI TECHNOLOGIES CO., LTD.) 24 March 2020 (2020-03-24) description, paragraphs 0036-0172	1-40
A	CN 102917333 A (SPACE STAR TECHNOLOGY CO., LTD.) 06 February 2013 (2013-02-06) entire document	1-40
A	CN 112689287 A (APPLE INC.) 20 April 2021 (2021-04-20) entire document	1-40
A	CN 113328783 A (GUANGZHOU IPLOOK TECHNOLOGIES CO., LTD.) 31 August 2021 (2021-08-31) entire document	1-40
A	CN 113519147 A (LENOVO (SINGAPORE) PTE. LTD.) 19 October 2021 (2021-10-19) entire document	1-40
A	US 2021051005 A1 (LENOVO (SINGAPORE) PTE. LTD.) 18 February 2021 (2021-02-18) entire document	1-40

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 February 2023	**10 February 2023**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/131721

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110912854	A	24 March 2020	US	2021185538	A1	17 June 2021
				EP	3820198	A1	12 May 2021
				EP	3820198	A4	08 September 2021
				WO	2020052416	A1	19 March 2020
				CN	110912854	B	23 March 2021
CN	102917333	A	06 February 2013	CN	102917333	B	23 September 2015
CN	112689287	A	20 April 2021	EP	3800857	A2	07 April 2021
				EP	3800857	A3	02 June 2021
				US	2021105687	A1	08 April 2021
				US	2021105847	A1	08 April 2021
CN	113328783	A	31 August 2021	None			
CN	113519147	A	19 October 2021	EP	3935810	A1	12 January 2022
				WO	2020183236	A1	17 September 2020
				US	2020288320	A1	10 September 2020
				US	11457360	B2	27 September 2022
US	2021051005	A1	18 February 2021	WO	2021033022	A1	25 February 2021

国际检索报告

国际申请号
PCT/CN2022/131721

A. 主题的分类

H04W12/106(2021.01)i;H04W12/10(2021.01)i;H04W12/03(2021.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W12/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;CNKI;VEN;DWPI;USTXT;EPTXT;WOTXT;IEEE;3GPP:安全,策略,会话管理,机密,加密,完整性,卫星,基站,地面站,信关站,用户面, encrypt,integrity,policy,satellite,SMF,UPF,session mangement,user platform,secur+,S-gNB,gNB,ground,gatway,generation NodeB

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 110912854 A (华为技术有限公司) 2020年3月24日 (2020-03-24) 说明书第0036-0172段	1-40
A	CN 102917333 A (航天恒星科技有限公司) 2013年2月6日 (2013-02-06) 全文	1-40
A	CN 112689287 A (苹果公司) 2021年4月20日 (2021-04-20) 全文	1-40
A	CN 113328783 A (广州爱浦路网络技术有限公司) 2021年8月31日 (2021-08-31) 全文	1-40
A	CN 113519147 A (联想（新加坡）私人有限公司) 2021年10月19日 (2021-10-19) 全文	1-40
A	US 2021051005 A1 (LENOVO (SINGAPORE) PTE. LTD.) 2021年2月18日 (2021-02-18) 全文	1-40

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"D" 申请人在国际申请中引证的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2023年2月9日	2023年2月10日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

张长梅

电话号码 (+86) 028-62969223

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/131721

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	110912854	A	2020年3月24日	US	2021185538	A1	2021年6月17日
				EP	3820198	A1	2021年5月12日
				EP	3820198	A4	2021年9月8日
				WO	2020052416	A1	2020年3月19日
				CN	110912854	B	2021年3月23日
CN	102917333	A	2013年2月6日	CN	102917333	B	2015年9月23日
CN	112689287	A	2021年4月20日	EP	3800857	A2	2021年4月7日
				EP	3800857	A3	2021年6月2日
				US	2021105687	A1	2021年4月8日
				US	2021105847	A1	2021年4月8日
CN	113328783	A	2021年8月31日		无		
CN	113519147	A	2021年10月19日	EP	3935810	A1	2022年1月12日
				WO	2020183236	A1	2020年9月17日
				US	2020288320	A1	2020年9月10日
				US	11457360	B2	2022年9月27日
US	2021051005	A1	2021年2月18日	WO	2021033022	A1	2021年2月25日