深空网络的高效安全通信机制

任 方[1,2] 郑 东[2]
(西安邮电大学通信与信息工程学院 西安 710121)[1] (无线网络安全技术国家工程实验室 西安 710121)[2]

摘 要 安全的深空通信网络是实现深空探测的重要保证之一。研究了基于天基网的深空网络体系结构,给出了一种安全通信机制。该机制采用基于属性的公钥加密算法来实现安全的深空数据传输。深空节点为数据选择加密属性集,用户能够解密密文当且仅当该加密属性集满足用户持有的访问树。该方案中用户与深空节点之间无需进行身份认证,大大减少了信息交互次数,比较适用于深空网络通信,以弥补其数据传输代价高昂的缺陷。

关键词 深空网络,安全体系,通信,公钥密码学,属性
中图法分类号 TN915.08,TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.12.049

Efficient and Secure Communication Scheme for Deep Space Networks

REN Fang[1,2] ZHENG Dong[2]
(School of Telecommunication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)[1]
(National Engineering Laboratory for Wireless Security, Xi'an 710121, China)[2]

Abstract The secure deep space communication network is one of the most important aspects in deep space exploration. A deep space network architecture based on satellites networks was proposed and an efficient and secure communication scheme for this architecture was studied. In this scheme, the attribute-based encryption algorithms are used to achieve secure data transmission in deep space networks. The deep space node chooses a set of attributes for data to be transmitted and encrypts it with private keys corresponding to the attributes and a user can decrypt the cipher if and only if the attributes set satisfies the access tree user holds. There is no need for the node and the user to authenticate the identity of each other, so the numbers of information exchange are greatly reduced. The scheme is suitable for deep space networks in order to make up the deficiency of costly data transmission.

Keywords Deep space networks, Security systems, Communication, Public key cryptography, Attributes

1 引言

深空探测是在卫星应用和载人航天取得重大成就的基础上,利用深空探测器对更广阔的太阳系空间和宇宙空间进行的探测。其目的是利用空间资源探索太阳系和宇宙空间的起源和演化,为人类社会的可持续发展服务[1]。

相对于近地轨道航天器,深空探测器需要脱离地球引力场,对地球以外的天体开展空间探测。由于通信距离遥远,与近地通信相比,深空通信存在以下问题[2]:①巨大的信号衰减。以地面与GEO卫星通信的信号损失作为参考,通信距离到达月球时信号损失增加21.03dB,到达火星时增加80.94dB。②极大的通信时延。地面信号到达月球的单程时延为1.21s~1.35s,到达火星为19.807min~22.294min,实时通信已经变得不可行。③巨大的能量损耗。由于探测器体积有限,不能布置太大的天线,向地面发送数据时需要耗费大量的能量。鉴于深空通信存在以上问题,传统的实时通信模式已经不能应用于深空通信,而应该发展基于存储-转发模式的延时通信,不再追求高的数据传输率,而是尽可能提高数据的准确率和安全性。

由深空探测器、中继站、地面站、控制中心等构成的深空通信网络是整个深空探测任务成功的重要保证之一。文献[2]以月球探测为例分析了建立地面测控网(Command & Telemetry,C&T)的缺陷,指出地面建立的深空探测站只能保证短时间探测:中国本土建站至多可观测月球8小时,环月卫星4小时。该文提出可以利用若干GEO卫星组建天基网,卫星可以实现对地面的全球覆盖,同时作为地面站对探测器进行测控的中介。该模式可以实现对外层空间的全天候连续观测,鉴于当时的技术限制,该文未对此展开进一步叙述。

美国NASA-JPL等机构提出了建立星际互联网络(InterPlaNetary Internet,IPN)的设想,以解决深空探测和通信中的各种问题[3-8]。IPN设想是以深空中的大量骨干通信节点组成星际骨干网,进行星体探测的深空探测器通过骨干网传送数据,这样就缩短了通信距离,降低了通信时延。但由于星际网络拓扑不固定,深空部分与地面部分需采用不同的网

到稿日期:2014-11-05 返修日期:2015-02-15 本文受国家自然科学基金(61272037,61472472),陕西省青年科技新星计划(2014KJXX-73),西安邮电大学青年教师科研基金(ZL2013-06)资助。
任 方(1981—),男,博士,讲师,主要研究方向为密码学与网络安全,E-mail:renfang_81@163.com;郑 东(1964—),男,博士,教授,主要研究方向为密码学与信息安全。

络技术，鉴于当前深空技术的发展水平，IPN 只能属于长远规划。

以卫星为主要节点的天基网中，目前路由技术已经相对成熟[9]，因此研究基于天基网的深空网络已经成为可能。本文给出了一种深空网络的体系结构，并为其建立了基本的安全通信机制。考虑到深空网络巨大的通信成本，本文采用的密码体系使用了基于属性的公钥加密机制。该机制具有信息交互次数少、无需目标节点身份认证、设置用户解密权限简单而灵活等优势，可以用于深空网络的安全通信。

2 深空通信的安全基础

2.1 安全基础

在深空通信中，由于数据发送需要消耗巨大的能量，因此我们希望探测器节点每次发送的探测数据都能够被成功接收。然而由于通信距离极为遥远，数据需要经中继节点中转，很容易发生数据包丢失。此外数据发送是以存储-转发的模式进行的，若中继节点被攻击者攻陷，则数据会发生泄漏或者遭到攻击者的恶意篡改。由于深空通信的资源非常珍贵，必须采用强有力的措施来实现安全的数据通信，同时尽量避免浪费通信资源。

传统端对端发送模式容易导致数据丢失，一旦数据链路出现断裂，数据发送将会失败。为减少数据包的丢失，深空通信可以采用单对多的数据发送模式，即探测器节点不指定单一的数据接收节点，而是由中继节点向多个可能的目标节点转发数据。这样，网络中始终存在多个数据包拷贝，可以减少由于链路故障导致的丢包。

深空通信可能存在以窃听为目的的被动攻击者或者以数据篡改为目的的主动攻击者，从安全的角度来看，必须采用密码机制来保证数据的完整性和保密性。由于深空网络是由多种类型的节点构成的异构式网络，采用公钥密码机制有利于进行网络扩展。但传统的基于证书和基于身份的公钥密码技术均存在一定的局限而不能应用于深空通信：

1)在基于证书的公钥密码机制[10]中，通信开始时需要节点双方交换公钥证书以验证身份，然后协商会话密钥，这将带来大量的信息交互，消耗大量的资源，在深空通信中是不可行的。

2)基于身份的公钥密码机制(Identity Based Encryption，IBE)[11-13]虽然可以省去身份验证带来的通信开销，但在深空通信单对多的数据发送模式下，由于数据存在多个数据接收者，IBE 机制无法使得多个接收者同时具备解密数据权限。

基于属性的公钥密码机制(Attribute Based Encryption，ABE)[14-19]能够有效解决单对多的数据发送模式下用户的解密权限问题。ABE 中用户持有的公钥是其自身具备的一组属性值，加密方为密文选择一定的属性值，用户能够解密密文当且仅当其自身的属性值与密文属性值满足一定条件。

Sahai 与 Waters 在文献[14]中给出了一种门限式的 ABE，用户能够解密密文当且仅当他所持有的属性达到预设的门限值。这是一种最简单的基于属性的公钥体制，不能满足复杂网络的需求。Goyal 和 Pandey 等人在文献[15]中提出的 KP-ABE 方案可以实现细粒度的用户访问控制。文献[16]提出的 CP-ABE 方案可应用于复杂系统的数据加密，更为灵活地指定用户解密权限。本文在现有 ABE 研究的基础上构建了一种适用于深空网络的高效加密方案，以实现深空通信的保密数据传输。

2.2 基本工具

定义 1(访问结构) 设实体集合为$\{P_1,P_2,\cdots,P_n\}$，一个访问结构指的是实体幂集的一个非空子集 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\setminus\{\emptyset\}$，访问结构 A 中的集合称为授权子集，不在 A 中的集合称为非授权子集。

访问结构 A 称为单调的是指如果对任意的实体子集 B 和 C，如果有 $B\in A$ 且 $B\subseteq C$，则一定有 $C\in A$。在 ABE 方案中实体一般是属性值，故而访问结构 A 包含了授权的属性集。我们只关注单调的访问结构。

访问结构可以通过访问树来具体实现[15-18]。

定义 2(访问树) 一棵访问树 TR 中的每一个非叶子节点是一个门限门，叶子节点代表一个属性值。对于非叶子节点 n，用 num_n 表示该节点的孩子个数，k_n 表示该节点的门限值，显然有 $0<k_n\leqslant num_n$。

对于访问树定义以下函数：$parent(n)$表示非根节点 n 的父节点，$attr(n)$表示叶子节点的属性值。每一个非根节点在其父节点的孩子中有一个序列值，令 $I(n)$表示这个值，显然有 $0<I(n)\leqslant num_{parent(n)}$。

用 TR_n 表示以节点 n 为根节点的访问子树。对于一个属性集合 γ，我们称 γ 满足一棵访问树(记作 $TR_n(\gamma)=1$)指的是按照如下的递归定义：若 n 是叶子节点，则 $TR_n(\gamma)=1$ 当且仅当 $attr(n)\in\gamma$；若 n 不是叶子节点，则首先对于 n 的每一个孩子节点 x 计算 $TR_x(\gamma)$，然后计算 $TR_n(\gamma)$，$TR_n(\gamma)=1$ 当且仅当至少有 k_n 个 $TR_x(\gamma)=1$。

可以证明：若属性集合 γ 满足访问树 TR，则任意包含 γ 的属性集合必定也满足访问树 TR。因此满足访问树 TR 的所有属性集合全体必定是一个单调的访问结构。

定义 3(双线性映射) 设群 G_1 和 G_2 是两个素数阶的乘法循环群，$|G_1|=|G_2|=p$。用 g_1 和 g_2 分别表示 G_1 和 G_2 的生成元，e_1 和 e_2 为 G_1 和 G_2 的单位元。则称 $\varphi:G_1\times G_1\rightarrow G_2$ 为一个双线性映射是指 φ 具有以下特点：

①双线性：对于任意的 $u,v\in G_1$ 和 $a,b\in Z_p$，有 $\varphi(u^a,v^b)=\varphi(u,v)^{ab}$；

②非退化性：$\varphi(g,g)\neq e_2$。

我们称 G_1 是一个双线性群如果 G_1 中的群运算和双线性映射 $\varphi:G_1\times G_1\rightarrow G_2$ 可以有效进行计算。显然 φ 是对称的：$\varphi(g^a,g^b)=\varphi(g,g)^{ab}=\varphi(g^b,g^a)$。文献[12]给出了椭圆曲线上的具体的双线性映射。

定义 4(拉格朗日插值) 对于 $i\in Z_p$ 和集合 $W\subseteq Z_p$，定义拉格朗日系数：$\Delta_{i,W}(x)=\prod_{j\in W,j\neq i}\frac{x-j}{i-j}$。则对于一个 $d-1$ 次多项式 $p(x)$，若已知集合 W 包含 d 个数，且对于 W 中任意的 i 均已知 $p(i)$，则可以通过插值恢复出 $p(x)=\sum_{i\in W}p(i)\Delta_{i,W}(x)$。

3 深空网络的安全架构

3.1 深空网络的体系结构

本文所考察的深空网络由地面网、天基网和深空节点构成，如图 1 所示。

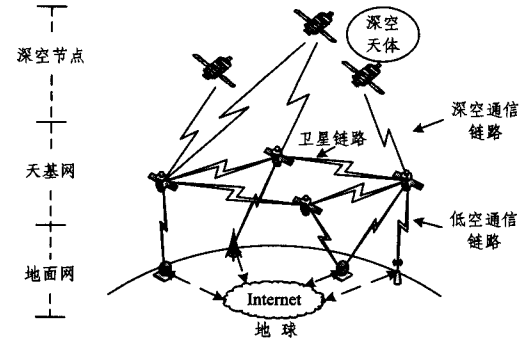

图 1　深空网络体系

地面网由设在地球上的深空观测站、地面控制中心以及地面通信网络所构成，主要功能是处理深空探测器发回的探测数据以及对探测器发送控制指令等。

天基网由可以覆盖全球的卫星网络构成，考虑到其主要与深空探测器进行数据通信，一般是由最高的 GEO 卫星群构成卫星网。卫星的运行有其固定的规律，地面的观测站可以预知卫星节点的位置和运行轨迹，能够计算出当前可以建立数据链路的卫星节点。卫星网能够实现对深空探测器全天候的观测和通信，接收探测器节点传回的数据并将控制指令转发给探测器节点。

深空节点包括各类深空探测器，比较典型的是月球探测器和火星探测器，以及以后可能出现的更多类型的探测器。深空探测器的运行规律是可以预先确定的，但往往不同于卫星节点具有一定的周期性。

通信链路包括低空通信和深空通信两类。低空通信是卫星网和地面网之间的通信，其通信距离较短，一般低于 4×10^7 m。深空通信链路是卫星网与深空节点进行通信的链路，其距离往往超过 10^8 m，远远大于低空通信的距离。

3.2　深空网络的安全机制

对应如上所述的深空网络体系，给出相应的安全通信机制。将各类深空探测器抽象为深空节点，其主要功能是完成探测数据的获取、加密以及发送任务；地面站抽象为用户节点，主要是接收并依据各自的解密权限解密数据；卫星为中继节点，负责转发针对深空节点的控制指令或者来自深空节点的加密数据。

安全机制采用基于属性的加密机制。系统初始化时地面控制中心根据深空节点所承担的探测任务和发送的探测数据为其分发一组属性值，同时为其生成相应的属性加密密钥。控制中心根据用户解密权限为其分发授权属性集，该属性集对应于一个单调的访问结构，可以用一棵访问树来描述。用户同时得到与授权属性集相对应的属性解密密钥。

深空节点采集探测数据，定期或者不定期地根据来自地面用户的数据请求指令将数据经中继节点发回给地面用户。根据需要发送的数据特点，深空节点在自己拥有的属性集中选择若干属性作为本次加密属性集，该集合中的属性决定了能够解密该数据的用户。深空节点用对应于该属性集的属性加密密钥对数据进行加密，然后将其发送给能够直接进行通信的中继节点。中继节点不对密文进行任何形式的改动，仅仅以存储-转发的模式将其发给覆盖范围内的地面用户。根据中继节点的覆盖范围和通信能力，该密文可能存在多个用户作为接收者。

根据解密权限的不同，用户从控制中心申请到对应于授权属性集的访问树以及相应的属性解密密钥。用户接收到来自中继节点的密文后，首先检验密文中包含的加密属性集。只有当密文对应的加密属性集满足用户持有的访问树，也即密文属性集包含于用户的授权属性集时，用户可以用属性解密密钥解密该数据。

4　方案的实现

4.1　符号与基本假设

设网络用户涉及到的所有属性为有限的 N 个，将其数量化后记作 $A=\{1,2,\cdots,N\}$。控制中心 BS 为每一个用户 U 确定其授权属性集，并指派一颗访问树 TR_U，该访问树标识了用户的实际解密能力。TR_U 的所有叶子所对应的属性集合记作 A_U，$A_U\subseteq A$。

BS 为深空节点 D 分发一组属性值 A_D，深空节点根据探测数据的读取权限为每一次加密的数据分配一个加密属性集 $A_C\subseteq A_D$，该属性集标识了能够解密该密文的用户，即只有满足条件 $TR_U(A_C)=1$ 的用户 U 可以解密该密文。

假定 BS 和地面用户的计算能力比较强，能够承担较为复杂的公钥密码运算，而深空节点的计算能力一般较弱。此外假定 BS 是绝对安全的，用户可以通过安全信道在 BS 处申请授权属性集和对应的访问树。

4.2　具体算法实现

控制中心 BS 执行系统初始化算法，生成并保管系统私钥，然后为深空节点生成并分发加密密钥，为用户生成并分发解密密钥。深空节点执行加密算法，完成数据加密。中继节点只负责存储转发，不涉及对数据的任意修改。用户执行解密算法，完成数据解密。算法流程如图 2 所示。

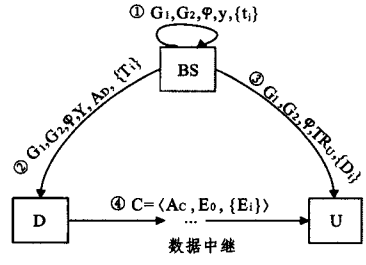

图 2　算法流程

4.2.1　初始化算法

1）控制中心 BS 首先生成系统环境参数：选取 p 阶的双线性群 G_1 和相应的群 G_2，用 g 表示 G_1 的生成元，$\varphi:G_1\times G_1\rightarrow G_2$ 是双线性映射。

2）BS 随机生成系统私钥 $y\in Z_p$，并为 A 中每一个属性随机地生成属性私钥 $t_i\in Z_p$，$i=1,2,\cdots N$。

步骤 1）中生成的系统环境参数需要向所有深空节点和用户公开，而步骤 2）中生成的私钥由 BS 秘密保管，在整个网络的生存期内可以定期更换系统私钥和属性私钥以保证安全性。

4.2.2　节点与用户的密钥生成

对于合法的深空节点 D，控制中心 BS 首先为其生成节点私钥 $Y=\varphi(g,g)^y$，然后根据该节点所探测的数据类型为其分发属性集 A_D 并生成加密密钥集 $\{T_i=g^{t_i}\mid i\in A_D\}$。BS 将 Y，A_D 和 $\{T_i\}$ 预装入节点 D。

对于用户 U，控制中心 BS 根据其数据解密权限为其分配一棵访问树 TR_U，并同时生成解密密钥集，具体步骤如下：

1)为 TR_U 中每一个非叶子节点 n 选择多项式 $q_n(x)$。首先为根节点 r 随机地秘密选取 k_r-1 次多项式 $q_r(x)$ 使得 $q_r(0)=y$，再按照自顶向下的顺序为其余子节点 n 选取 k_n-1 次多项式 $q_n(x)$ 使得 $q_n(0)=q_{parent(n)}(I(n))$。

2)对于 TR_U 的叶子节点 n，记 $i=attr(n)$，计算 $Q_i=q_{parent(n)}(I(n))$。

3)为用户分发解密密钥。对于每一个 $i\in A_U$，计算 $D_i=g^{\frac{Q_i}{t_i}}$。控制中心将解密密钥集 $\{D_i\mid i\in A_U\}$ 分发给用户 U。

4.2.3 *数据加密算法*

深空节点 D 根据数据请求指令，首先确定待加密的数据 $M\in G_2$，然后执行以下加密算法：

1)选择加密属性集 $A_C\subseteq A_D$，并选取一次性随机数 $s\in Z_p$；

2)计算 $E_0=MY^s$ 以及 $\{E_i=T_i^s\mid i\in A_C\}$；

3)将密文 $C=\langle A_C,E_0,\{E_i\mid i\in A_C\}\rangle$ 发给中继节点，由中继节点转发给用户。

4.2.4 *数据解密算法*

用户 U 接收到来自中继节点的密文 C 后取出其中的加密属性集 A_C 以及 $\{E_i,i\in A_C\}$，然后根据自己持有的访问树 TR_U，对其中的节点自底向上进行以下计算：

1)对于 TR_U 的叶子节点 n，令 $i=attr(n)$，计算

$$F_n=\begin{cases}\varphi(D_i,E_i), & i\in A_C\\ \perp, & i\notin A_C\end{cases}$$

2)对于非叶子节点 n，首先对其所有子节点 x 计算 F_x。如果至少有 k_n 个 $F_x\neq\perp$，则取这样的 k_n 个子节点组成集合 S_n，令 $j_x=I(x)$，$s_n=\{j_x,x\in S_n\}$，然后计算

$$F_n=\prod_{x\in S_n}F_x^{\Delta_{j_x,s_n}(0)}$$

若满足 $F_x\neq\perp$ 的子节点个数小于 k_n，则令 $F_n\neq\perp$。

当加密属性集 A_C 满足用户 U 所持有的访问树即 $TR_U(A_C)=1$ 时，容易看出对于 TR_U 的根节点 r 可以计算 $F_r\neq\perp$。以下证明 $F_r=Y^s$，这样用户 U 可以解密 $M=E_0/F_r$。

采用归纳法来证明 $F_r=Y^s$：对于 TR_U 的叶子节点 n，根据解密算法步骤 1)，有：

$$\begin{aligned}F_n&=\varphi(D_i,E_i)=\varphi(g^{\frac{Q_i}{t_i}},T_i^s)\\&=\varphi(g^{\frac{Q_i}{t_i}},g^{t_i\cdot s})=\varphi(g,g)^{sQ_i}\\&=\varphi(g,g)^{sq_{parent(n)}(I(n))}\end{aligned}$$

当 $TR_U(A_C)=1$ 时，TR_U 的任意非叶子节点 n 至少有 k_n 个子节点的 $F_x\neq\perp$，若对于这样的子节点都有 $F_x=\varphi(g,g)^{sq_{parent(x)}(I(x))}$，则可以计算：

$$\begin{aligned}F_n&=\prod_{x\in S_n}F_x^{\Delta_{j_x,s_n}(0)}\\&=\prod_{x\in S_n}(\varphi(g,g)^{sq_{parent(x)}(I(x))})^{\Delta_{j_x,s_n}(0)}\\&=\prod_{x\in S_n}\varphi(g,g)^{sq_n(j_x)\Delta_{j_x,s_n}(0)}\\&=\varphi(g,g)^{s\sum\limits_{x\in S_n}q_n(j_x)\Delta_{j_x,s_n}(0)}\\&=\varphi(g,g)^{sq_n(0)}\\&=\varphi(g,g)^{sq_{parent(n)}(I(n))}\end{aligned}$$

因此由归纳法原理，对于任意节点 n 均有：

$F_n=\varphi(g,g)^{sq_{parent(n)}(I(n))}$

特别地，当 $n=r$ 时有：

$F_r=\varphi(g,g)^{sq_r(0)}=\varphi(g,g)^{sy}=Y^s$

证明完毕。

5 性能分析

5.1 深空节点的开销

1)通信开销：初始化算法中，控制中心需要为深空节点一次性装载节点私钥和加密密钥集，为用户分配访问树和解密密钥集。此后除非控制中心由于安全原因更改系统私钥，不需要与节点和用户进行通信。网络中的用户、中继节点和深空节点之间均不需要进行身份认证，大大减少了数据交互次数。深空节点接收来自中继节点的数据请求指令，将待发送的数据进行加密后直接发往中继节点，发送的内容包括属性集合 A_C、群 G_2 中的 1 个元素 E_0 与群 G_1 中的 $|A_C|$ 个元素 $E_i,i\in A_C$。

2)计算开销：由于不需要进行身份认证，因此不存在认证带来的计算开销。深空节点发送数据时需要进行一组加密运算，其中包括 $|A_C|$ 次群 G_1 中的指数运算、1 次群 G_2 中的指数运算和 1 次乘法运算。控制中心和用户完成运算量较大的双线性映射的计算，深空节点的计算负担较小。

3)存储开销：深空节点只需要存储群 G_2 中的元素 Y 和 G_1 中的属性密钥集 $\{T_i\}$，不需要存储额外的用户证书或者身份信息。

根据以上对深空节点通信开销、计算开销、存储开销的分析，本方案可以极大减少深空节点的各类开销，是一种高效的通信机制。

5.2 安全性分析

1)机密性：本文方案中，深空网络中传送的数据为 $C=\langle A_C,E_0,\{E_i\mid i\in A_C\}\rangle$，其中 A_C 是公开的属性集，$E_0=MY^s$ 和 $E_i=T_i^s$ 分别是由深空节点 D 根据其私钥 Y、T_i 和一次性随机数 s 以及明文信息 M 计算得到的，那么：

①对于非深空节点来说，Y、T_i 和 s 均是保密的，因此此类节点无法计算 M；

②若某深空节点 D' 被攻击者攻陷，成为恶意的深空节点，它知道 Y 和 T_i，但是想要计算一次性随机数 s 则需要解离散对数问题，这是一个计算困难问题，因此 Y^s 和 M 仍然无法计算。

此外，深空节点每次发送数据时可以根据数据的特点为其选择不同的加密属性集 A_C，以方便而灵活地改变可读取该数据的用户群组，适应不同的应用需求。

2)认证性：本方案不需要对请求数据的用户节点进行身份认证，这在很大程度上减轻了通信与计算负担，但是本方案依然能够实现对用户的认证。这主要体现在：控制中心 BS 为每一个用户 U 确定其授权属性集，指派一棵标识其实际解密能力的访问树，并同时生成解密密钥集。用户 U 能够解密某密文 C 当且仅当 $TR_U(A_C)=1$，即密文属性集满足用户持有的访问树，这实际上是一种对用户解密能力的隐性认证。

3)匿名性：本方案中用户节点 U 解密数据 C 的依据是其授权属性集和 BS 分配给它的访问树，用户无需向中继节点和深空节点认证自己的真实身份，这就可以实现深空网络数据的匿名性访问。

（下转第 267 页）

2011,28(9):3201-3205
Zhang Chao-qun, Zheng Jian-guo, Wang Xiang. Application Overview of research on bee colony algorithms[J]. Research of Computers,2011,28(9):3201-3205
[13] Gao Wei-feng, Liu San-yang. Improved artificial bee colony algorithm for global optimization[J]. Information Processing Letters,2011,111(17):871-882
[14] 王翔,李志勇,许国艺,等. 基于混沌局部搜索算子的人工蜂群算法[J]. 计算机应用,2012,32(4):1033-1036,1040
Wang Xiang, LI Zhi-yong, Xu Guo-yi, et al. Artificial bee colony algorithm based on chaos search operator [J]. Journal of Computer Applications,2012,32(4):1033-1036,1040
[15] Karaboga D, Basturk B. A powerful and efficient algorithm for numerical function optimization: Artificial Bee Colony (ABC) algorithm [J]. Journal of Global Optimization,2007,39(3):459-471

(上接第 232 页)

结束语 开展深空探测对于人类文明具有重大的意义,由深空节点、中继节点、地面用户和控制中心等构成的深空网络是开展深空探测的重要形式。深空通信与近地通信的不同之处于在于巨大的信号衰减、通信时延和能量损耗,因此传统的即时通信不能适用于深空通信,需要为其研究全新的通信形式,这其中包括安全通信的机制。

本文提出了一个高效的适用于深空网络的安全通信机制,该机制中深空节点采用基于属性的加密算法加密数据,用户持有与其授权属性集相对应的访问树。深空节点加密数据时为密文选择一组加密属性,用户能够解密数据当且仅当密文的属性能够满足用户的访问树。这是一种不需要进行用户认证的、高效的安全通信机制,深空节点还可以为密文选择不同的属性以满足不同的安全性需求,能够灵活更改或限制用户解密能力。进一步的研究工作可以选择更高效的属性加密方案以满足更高的要求。

参 考 文 献

[1] 欧阳自远,李春来,邹永廖,等. 深空探测的进展与我国深空探测的发展战略[J]. 中国航天,2002(12):28-32
Ouyang Z Y, Li C L, Zou Y L, et al. Advances in deep space exploration and the development strategy of China's deep space exploration [J]. Aerospace China,2002(12):28-32
[2] 姜昌,黄宇民,胡勇. 研究与开发天基深空通信跟踪(C&T)网的倡议[J]. 飞行器测控学报,1999,18(4):28-37
Jiang C, Huang Y M, Hu Y. An initiative of research and development of space-based communications and tracking(C&T) network [J]. Journal of Spacecraft TT&C Technology, 1999, 18(4):28-37
[3] Hooke A. The interplanetary internet [J]. Communication of the ACM,2001,44(9):38-40
[4] Akyildiz I F, Akan Ö B, Chen C, et al. Interplanetary internet: state-of-the-art and research challenges [J]. Computer Networks,2003,43(2):75-112
[5] Bhasin K, Hayden J L. Space Internet architecture and technologies for NASA enterprises [J]. International Journal of Satellite Communications,2002,20(5):311-332
[6] Mukherjee J, Ramamurthy B. Communication technologies and architectures for space network and interplanetary internet [J]. IEEE Communications Surveys & Tutorials,2013,15(2):881-897
[7] Sodnik Z, Furch B, Lutz H. Optical intersatellite communication [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2010,16(5):1051-1057
[8] Marchese M. Interplanetary and pervasive communications [J]. IEEE Aerospace and Electronic Systems Magazine,2011,26(2):12-18
[9] 林闯,董扬威,单志广. 基于 DTN 的空间网络互联服务研究综述[J]. 计算机研究与发展,2014,51(5):931-943
Lin C, Dong Y W, Shan Z G. Research on space internetworking service based on DTN [J]. Journal of Computer Research and Development,2014,51(5):931-943
[10] Wenbo M. Modern cryptography: theory and practice [M]. Prentice Hall PTR,2004
[11] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology-Crypto'84. Berlin: Springer-Verlag,1984:47-53
[12] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C] // Advances in Cryptology-Crypto 2001. Berlin: Springer-Verlag,2001:213-229
[13] 郝云芳,吴静,王立炜. Boneh-Boyen_1 基于身份加密体制的安全密钥分发[J]. 计算机科学,2012,39(Z6):35-37
Hao Y F, Wu J, Wang L W. Secure key issuing for Boneh-Boyen$_1$ identity-based encryption [J]. Computer Science, 2012, 39(Z6):35-37
[14] Sahai A, Waters B. Fuzzy identity based encryption[C]// Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer-Verlag,2005:457-473
[15] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C] // ACM conference on Computer and Communications Security. Alexandria, USA: ACM Press,2006:89-98
[16] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]// Proceedings of IEEE Symposium on Security and Privacy. Oakland, USA: IEEE Computer Society, 2007:321-334
[17] Lewko A, Waters B. Decentralizing attributed-based encryption [C] // Advances in Cryptology-EUROCRYPT 2011. Berlin: Springer-Verlag,2011:568-588
[18] Zhang Guo-yan, Liu Lei, Liu Yang. An attribute-based encryption scheme secure against malicious KGC[C]// IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Liverpool, UK: IEEE Computer Society,2012:1376-1380
[19] 陈燕俐,杜英杰,杨庚. 一种高效的基于属性的认证密钥协商协议[J]. 计算机科学,2014,41(4):150-154,177
Chen Y L, Du Y J, Yang G. Efficient attribute based authenticated key agreement protocol [J]. Computer Science,2014,41(4):150-154,177