一种基于身份的层次式空间网络组密钥管理方案

蒋自辉 雷凤宇
(解放军 75741 部队 广州 510510)

摘 要 随着航天技术、移动通信技术和网络技术的迅速发展以及信息化建设的逐渐深入,空间信息系统也在向着网络化的趋势加速发展,其应用前景受到了极大的关注,故其对安全的要求越来越高。文中提出的基于身份的空间网络组密钥管理方案 ID-GKM 中,采用分层分组式的组密钥管理机制,方案除了包括常有的组密钥生成分发、密钥更新外,还考虑了私钥更新。在私钥更新部分,采用 B&F 提出的基于身份的公钥加密机制,提出了适合空间网络的私钥更新机制。该方案能够适应空间网络的层次化架构,满足其对强扩展性、高可靠性等的要求。另外,针对地面终端节点与空间节点不同的特点,提出地面组管理的密钥更新应采用批量更新的方案,该方案结合使用了定期和基于队列更新的思想,且可以考虑采用基于代理重加密的组密钥管理方案来解决 LKH 方案中组密钥更新时对用户必须在线的要求。

关键词 分布式生成中心,签密,LKH
中图法分类号 TP393.08 **文献标识码** A

Identity-based Hierarchy Group Key Management of Space Network

JIANG Zi-hui LEI Feng-yu
(PLA 75741Troops, Guangzhou 510510, China)

Abstract With the gradual deepening of the information construction and the rapid development of space technology, mobile communication technology and network technology, spatial information system development also accelerates toward networking. Potential applications of special information network have gotten more concern, so its safety requirements are getting higher and higher. This paper proposed a identity-based group key management program(ID-GKM) for the entire space network, which uses the hierarchical-grouped group key management scheme. In addition to a common group key generating, distribution and updating, it also considered the part of the private key updating. Using the identity-based key encryption mechanism which is proposed by Boneh and Franklin, we proposed the private key update mechanism for space network. The program can adapt the hierarchical structure of the space network and meet the requirements of its strong scalability and high reliability. In addition, we concerned the difference of the ground terminal node and the nodes in space. This scheme uses the batch updating that is a combination of updating regularly and updating based on queue. And we can use the proxy re-encryption group key management scheme to solve the issue that the user must be online when group key is updating.

Keywords Distributed private key generation centre, Signcryption, LKH

1 引言

随着航天技术、移动通信技术和网络技术的迅速发展以及信息化建设的逐渐深入,空间信息系统也在向着网络化的趋势加速发展。不同轨道上多种类型的卫星、飞行器以及相应地面设施和用户终端,渐渐融合成为空天地一体化的综合信息网络,可以提供包括遥控、遥测、语音、图像、视频等多种不同类型的业务和应用。而空间信息网络的广阔的应用前景也使其得到了国内外学术界、工业界,特别是军方的高度关注和重视。

空间网络在军事应用领域发挥着极其重要的作用,是信息化战争的核心基础设施,因此,空间网络在安全性方面的要求远高于传统地面有线和无线网络。同时,网络安全技术是应对空间网络安全威胁和保障空间信息系统安全的技术基础,与空间网络其他技术的发展密不可分。在空天地一体化网络环境中,数据加密、完整性保护、身份认证等一系列的安全服务和具体安全机制的实施均需要密钥管理技术的支持,而空间网络的高动态性、异构性等特点则对密钥管理技术提出了更高的要求。现有的涉及到空间网络的密钥管理方案甚少从整个空间网络架构的角度去考虑总体的密钥管理问题,大部分方案都是直接针对卫星网络而提出的,且很大部分的方案是基于公钥证书提出的,可扩展性差。因此,从空间网络

本文受"973"项目(2009CB320403),国家自然科学基金(60832008,60832006)资助。
蒋自辉(1974-),男,硕士,工程师,主要研究方向为密码学、网络空间防御;雷凤宇(1980-),女,博士,高级工程师,主要研究方向为密码学、无线传感器网络、网络空间防御,E-mail:4485179@qq.com。

特点出发，设计适合总体架构并且满足安全性和空间网络性能要求的密钥管理方案，才能为其它安全机制的实施提供支持。

本文提出的基于身份的空间网络组密钥管理方案（Identity-based Group Key Management Program，ID-GKM），从整个空间网络结构出发，除了考虑组密钥生成分发、组密钥加入退出时的更新等内容外，还包括了适合空间网络节点的私钥更新机制。本方案采用 LKH 组密钥管理方案提高管理组的可扩展性，使用基于身份的多接收者签密机制来保证密钥分发的安全性，能够适应空间网络的层次化架构，满足其对强扩展性、高可靠性等的要求。针对地面层节点不同于空间节点的特点，提出了结合定期更新和基于队列更新思想的组密钥批量更新方案，另外，针对 LKH 方案中密钥更新时要求所有节点必须在线的问题，提出可采用基于代理重加密的组密钥管理方案来解决节点离线时的密钥更新问题。

本文第 2 节介绍国内外空间网络组密钥管理的相关研究工作；第 3 节提出组密钥管理模型；第 4 节从理论上分析了该方案的安全性以及性能开销；最后是总结。

2 相关工作

目前已有很多针对空间网络安全的密钥管理方案被提出。2005 年，Ayan Roy-Chowdhury 等人[4]针对卫星和地面混合网络的特点，在 LKH 方案的基础上提出了一种层次化的组密钥管理方法，缺点是没有考虑组通信中的用户的认证以及消息的完整性方面的问题。2006 年，Yavuz 等人[5]提出了一种基于 ECPVSS(Elliptic Curve Pintsov-Vanstone Signature Scheme)的安全协议，该协议主要使用椭圆曲线来保障分发过程中的安全。同年，文献[6]用相互独立的层次式的组密钥管理架构设计了 N 层卫星组播安全协议，其中采用了椭圆曲线密码体制和多接收者签密机制，可将组成员的加入及离开限制在一个层次内[1]，但没有考虑到 LEO 卫星相对于地面的快速运动而引起的组成员变化，且组密钥更新所需的开销较大。杨德明等人[7]于 2006 年提出了在空间网络中应用基于分布式 CA 的密钥管理方案，但若攻击者掌握门限认证的数个密钥分量仍可恢复出系统认证密钥。罗长远等人[8]于 2009 年在上述基于分布式 CA 的密钥管理策略的基础上，提出一种度量认证密钥安全强度的方法，重点分析了系统门限值和密钥分量更新周期，并对参数的设置规则给出了较为合理的方法。2007 年，Victor P. Hubenko Jr. 等人[9]提出了一个应用于 LEO 卫星系统的具有可伸缩性的安全组播架构，使用类似分簇的概念，建立了层次化的组播组，能减少组密钥更新的平均开销以及更新频率。但该方案只是一个架构设计，并没有设计具体的组密钥更新协议和方案。王宇等人于 2007 年，在构建多级多层的空间信息系统安全基础设施[10]中，提出建立层次性的公钥基础设施 PKI 的方案。2009 年，Tzung-Her Chen 等人在文献[11]中完全使用对称密钥管理体制，为移动卫星通信系统设计了一种“自认证”的认证机制，但这的扩展性不强。2010 年，罗长远等人[2]提出了空间网络的基于身份的分布式密钥管理方案，方案围绕构建的分布式密钥生成中心，考虑了私钥更新、主密钥分量更新和会话密钥协商等方面的策略问题，解决了空间网络中实施集中式密钥管理的难点及维护公钥证书的开销过大等问题，且有较好的扩展性。但这仅仅是针对空间网络中的卫星网络层提出的私钥更新方案，并非针对整个空间网络；彭长艳在文献[1]中对空间网络架构进行了详细的研究说明，提出了适合整个空间网络的组密钥管理方案，但没有考虑节点的私钥更新等其他问题。

由分析可知，空间网络组密钥管理已有很多框架和方案被提出，但甚少从整个空间网络架构的角度去考虑总体的密钥管理问题，大部分方案都是直接针对卫星网络而提出，且很大部分方案是基于公钥证书而提出的，扩展性较差。

3 基于身份的分层分组式组密钥管理方案 ID-GKM

3.1 设计思想

本文研究的空间网络主要由空间层、临近空间层和地面层共同组成，如图 1 所示，即有层次化的特性；同时它大规模的网络特性决定了其适合通过分组方式来将由于成员的加入和离开而造成的影响限制在较小的区域内。一般在有成员加入或退出时，都需要进行通信密钥的更新，如若进行分组管理，则一个小组内的成员的加入或退出引起的组密钥的更新只限制在该小组内，其他组却不用更新，从而避免了大范围的密钥更新带来的额外开销。因此，本文选择分层分组式的组密钥管理方案，能够满足空间网络中组播组的大规模、高动态、可扩展等对网络安全技术研究的挑战。本文研究的空间网络简化的架构如图 2 所示，其中，从上往下依次为空间层卫星节点、临近空间层节点和地面层节点。

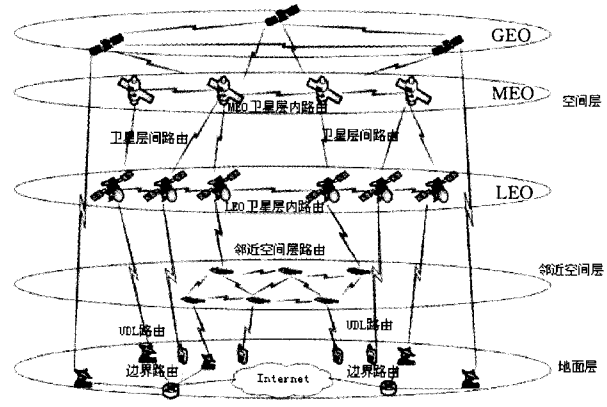

图 1 空间网络架构

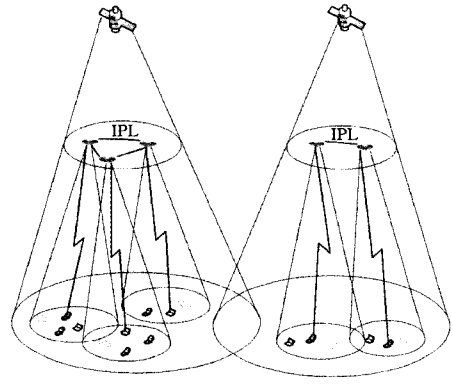

图 2 简化的空间架构

方案中，地面总控中心负责对整个系统架构进行管理，并对空间层的卫星节点进行管理；卫星节点负责对处于其覆盖范围内的临近空间平台进行管理并进行数据的通信；临近空

间网络节点对地面节点进行管理并提供数据通信。地面节点从临近空间节点处接收数据，可以考虑地面节点分组后直接由临近空间节点担任组管理者。但很多情况下，想要接收服务的地面节点相对临近空间节点来说是非常多的，即若地面终端节点直接接入临近空间网节点，则每个组中的成员数量将会非常大并且地面层节点加入或退出更加频繁；若每次密钥更新都由临近空间层节点直接负责，则将有很大的通信开销和资源浪费。因此，考虑将地面层节点进行分组，再由选定计算能力以及存储能力强的节点或者直接配置满足需要的节点作为地面组的组管理者与临近空间节点进行通信（此时，临近空间节点为组管理者，地面组管理者为其组成员），并负责对其对应的组进行管理和通信。这样可以保证地面组中成员加入或退出时，组密钥的更新不需要与临近空间层节点直接进行交互。

公钥一般主要用于实体认证、对称密钥协商等场合，常见的公钥体制为 PKI 和基于身份的密码体制。但相对于 PKI 来说，基于身份的密码体制不再需要存放公钥或者证书的目录；不再需要第三方的认证中心（CA）提供服务；验证者不论是确认实体的签名、执行公钥加密，还是进行会话密钥计算，都可以直接使用用户身份信息或者其变体作为公钥来使用，不再需要先验证其正确性再使用。空间网络中节点是运动的，若每次使用公钥之前都要先向固定的 CA 验证确认正确后才能使用，显然是不合适的，故本文的组密钥管理方案采用基于身份的密码体制。

3.2 ID-GKM 方案描述

本文的空间网络组密钥管理采用基于 LKH 的管理方案。在卫星节点与临近空间网络节点之间、临近空间节点与地面组管理者节点之间以及地面组管理者与组成员之间的组通信中，组管理者维护一棵逻辑密钥树，树的每个节点都有一个密钥，树的每个叶子节点对应一个组成员（组成员不包括组管理者）。组管理者负责生成分发组密钥，并在组成员加入或退出时或组密钥使用时间较长时更新密钥；每个组成员知道自己所在的叶子节点到根节点的路径上所有节点对应的密钥。逻辑密钥树只是逻辑上的，其中，除根节点外的非叶子节点实际上是不存在的。

本文空间网络组密钥管理方案主要包括组密钥管理系统的初始化、成员注册、组密钥的生成分发、新成员的加入、组成员退出和私钥更新等过程。本方案中采用的签密方案为 Yu 等人[3]提出的基于身份的多接收者签密机制。

3.2.1 系统初始化

给定安全参数 k，PKG 选择大素数 $q>2^k$，具有双线性对性质的超奇异椭圆曲线上的 q 阶群 G_1，有限域上的 q 阶乘法群 G_2，双线性对 $\hat{e}:G_1\times G_1\rightarrow G_2$，$P$ 为 G_1 的生成元。PKG 在 Z_q^* 上选择随机数 s 作为系统的主密钥，则系统公钥为 $P_{pub}=sP$。PKG 选择哈希函数 $H_0:\{0,1\}^*\rightarrow G_1^*$，$H_1:G_2\rightarrow\{0,1\}^*$，其中，$H_0$ 表示将代表节点身份表示的布尔串映射为 G_1 上的点，H_1 是用来将 G_2 上的点映射为可用作会话密钥的定长布尔串。PKG 保存主密钥 s，然后公开系统参数 $\langle G_1,G_2,\hat{e},P_{pub},P,H_0,H_1\rangle$。

3.2.2 成员注册

组管理者负责对所有的组成员进行管理，所以想要加入组播组成为该组的合法成员的网络节点必须先向组管理者注册，注册的过程可以看成是新成员 U_i 和组管理者 GC 通过交互进行双向认证以后协商出新成员和组管理者之间的会话密钥 K_i 的过程。

用户 U_i 向组管理者 GC 发送的注册请求消息 reg-request 消息，包含新用户的自身标识；另外，用户 U_i 选择随机数 $a\in Z_q^*$，计算 $T_{U_i}=aP$；然后利用其自身私钥 S_{U_i} 和 GC 的公钥 Q_{GC} 对消息进行签密后发送给 GC，其内容为 $signcrypt_{U_i,GC}(reg\text{-}request_{U_i},ID_{U_i},T_{U_i})$。

GC 在接收到 U_i 发送的注册请求消息后，用自己的私钥 S_{GC} 和 U_i 的公钥 Q_{U_i}，进行解签密操作，从而得到请求消息的内容，然后通过验证消息的合法性来完成对请求节点的认证。之后，GC 便向 U_i 发送出对其注册请求的响应消息 reg-response。像 U_i 一样，GC 选择随机数 $b\in Z_q^*$，计算得到 $T_{GC}=bP$，并选择合适的时间 $time$ 来同时进行会话密钥的协商计算工作。利用自身私钥 S_{GC} 和 U_i 的公钥对消息进行签密，然后发送给请求者 U_i，内容如下：$signcrypt_{GC,U_i}(reg-response_{GC},T_{GC},time)$。

用户 U_i 接收到由 GC 发出的响应消息后，使用自身的私钥 S_{U_i} 和 GC 的公钥解签密得到消息内容，通过验证消息的合法性来完成对 GC 的认证。如此就完成了双向认证，此时，就可以通过交换得到的消息来计算共享密钥 K_i。若 U_i 解签密以后发现时间 $time$ 已过，则重新申请。

约定系统时间 $time$ 时刻，节点 U_i 和 GC 计算会话密钥，则会话密钥协商过程如下：GC 计算 $k_{U_i\rightarrow GC}=H_1(\hat{e}(bQ_{U_i},P_{pub}))\oplus H_1(\hat{e}(S_{GC},T_{U_i}))$，$U_i$ 计算 $k_{GC\rightarrow U_i}=H_1(\hat{e}(aQ_{GC},P_{pub}))\oplus H_1(\hat{e}(S_{U_i},T_{GC}))$。其中，考虑到公私钥的更新问题（详见 3.2.6 节的私钥更新），对 GC 而言，在 $time$ 时刻的 Q_{U_i} 计算过程为：

$$\left.\begin{aligned}&time_{U_i}=g(ID_{U_i})\\&k=\lfloor(time-time_{U_i})/w\rfloor\\&Q_{U_i}=H_0(ID_{U_i}\|phase_0+k+1)\end{aligned}\right\}$$

U_i 采用相同的办法计算 $time$ 时刻的 Q_{GC}。可以验证

$$\begin{aligned}K_i&=k_{U_i\rightarrow GC}\\&=H_1(\hat{e}(bQ_{U_i},P_{pub}))\oplus H_1(\hat{e}(S_{GC},T_{U_i}))\\&=H_1(\hat{e}(bQ_{U_i},sP))\oplus H_1(\hat{e}(S_{GC},aP))\\&=H_1(\hat{e}(sQ_{U_i},bP))\oplus H_1(\hat{e}(sQ_{GC},aP))\\&=H_1(\hat{e}(S_{U_i},bP))\oplus H_1(\hat{e}(aQ_{GC},P_{pub}))\\&=H_1(\hat{e}(S_{U_i},T_{GC}))\oplus H_1(\hat{e}(aQ_{GC},P_{pub}))\\&=k_{GC\rightarrow U_i}\end{aligned}$$

因此，双方都可得到共享密钥 K_i。

3.2.3 组密钥的生成分发

当组播组中的所有成员都成为组成员时，组管理者构造一棵逻辑树，将所有的组成员安排到叶子节点，生成所有非叶子节点对应的密钥，包括根节点所对应的组密钥。

以 8 个节点的二叉逻辑密钥树为例来介绍密钥树的初始化工作。组管理者生成二叉树以后，将该树结构广播给所有组成员。由于在注册阶段，GC 和所有组成员已协商得会话密钥，即已得到图 3 中的叶子节点对应的 K_i，GC 只要把非叶子节点的密钥分发给对应的叶子节点上的组成员，即完成密钥树的更新。

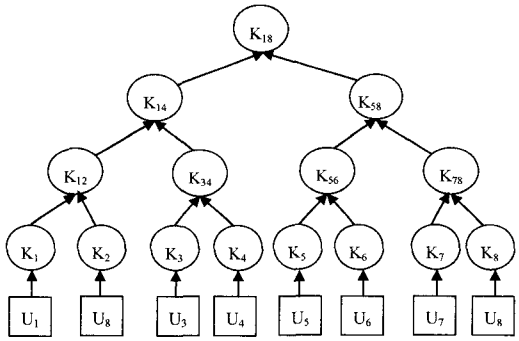

图 3　8 个组成元的 LKH 的密钥树形式

为了保证密钥的保密性、完整性、真实性等，采用基于身份的多接收者签密机制来完成密钥的安全分发。密钥的分发过程介绍如下：

(1)GC 将 K_{12} 签密得到的消息 $signcrypt_{GC,U_1,U_2}(K_{12})$ 发送至 U_1 和 U_2；将 K_{34} 签密后的消息 $signcrypt_{GC,U_3,U_4}(K_{34})$ 发送给 U_3 和 U_4；将 K_{56} 签密后得到的消息 $signcrypt_{GC,U_5,U_6}(K_{56})$ 发送给 U_5 和 U_6；将 K_{78} 签密后的得到的消息 $signcrypt_{GC,U_7,U_8}(K_{78})$ 发送给 U_7 和 U_8。

(2)GC 将 K_{14} 进行签密得到的 $signcrypt_{GC,U_1,U_2,U_3,U_4}(K_{14})$ 发送给组成员 U_1、U_2、U_3、U_4；将 K_{58} 签密得到的 $signcrypt_{GC,U_5,U_6,U_7,U_8}(K_{58})$ 发送给组成员 U_5、U_6、U_7、U_8。

(3)GC 将根节点对应密钥 K_{18} 签密后得到的消息 $signcrypt_{GC,U_1,U_2,U_3,U_4,U_5,U_6,U_7,U_8}(K_{18})$ 发送给所有组成员节点。

在上述密钥分发的过程中使用了基于身份的签密机制进行密钥的保护，之后就可以以广播或组播的方式进行发送，避免了为每个成员进行单播发送，可以减少组管理者与组成员的交互次数，节省通信开销。

3.2.4　新成员的加入

当有新成员想要加入时，需向组管理者发送成员注册请求，详见 3.3.2 小节成员注册。注册完成以后，新成员就正式成为组成员并获得和组管理者共享的会话密钥。而后，组管理者将新的组成员添加到密钥树中(此处，若密钥树不是满二叉树则直接将新成员节点加入叶子节点的位置即可；若密钥树已满，则分裂叶子节点创建新的位置给新节点)，并进行相应的密钥更新工作。现以 3.2.3 小节的 8 个组成员节点的满的二叉树为例来说明，设要加入的成员为 U_9，注册完成后得到的共享密钥为 K_9。组管理者将 U_9 加入到密钥树中后，树的形式如图 4 所示，并再次广播该树结构给所有组成员。

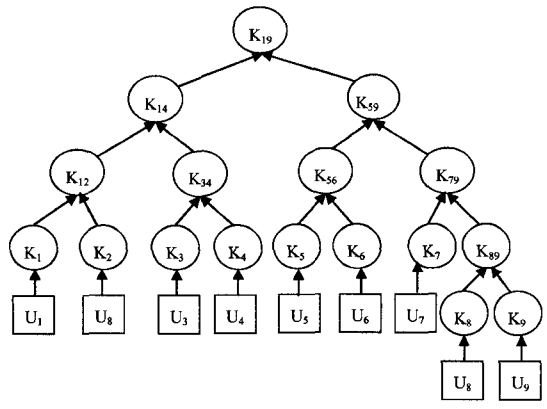

图 4　U_9 加入时的 LHK 密钥树状态图

如图 4 所示，需要更新的密钥为 K_{89}、K_{79}、K_{59}、K_{19}，其中 K_{19} 为组密钥。密钥更新过程描述如下：

(1)组管理者 GC 将 K_{89}、K_{79}、K_{59}、K_{19} 进行签密后得到的消息 $signcrypt_{GC,U_8,U_9}(K_{19},K_{59},K_{79},K_{89})$ 发送给 U_8 和新成员 U_9。

(2)组管理者 GC 将 K_{79}、K_{59}、K_{19} 签密后得到的消息 $signcrypt_{GC,U_7}(K_{19},K_{59},K_{79})$ 发送给组成员 U_7。

(3)组管理者 GC 将 K_{59}、K_{19} 签密后的消息 $signcrypt_{GC,U_5,U_6}(K_{19},K_{59})$ 发送给组成员 U_5、U_6。

(4)组管理者 GC 将 K_{19} 签密后的消息 $signcrypt_{GC,U_1,U_2,U_3,U_4}(K_{19})$ 发送给组成员 U_1、U_2、U_3、U_4。

到此，新成员加入时所需更新的密钥全部更新完成，已能保证之前通信消息的安全，即保证了组密钥的前向安全性。

3.2.5　组成员退出

组成员离开该组播组时，组管理员 GC 需要将其从逻辑密钥树中移除。为了避免已离开的成员获取后续的组密钥及组播数据，因此，组管理者 GC 必须将该节点知道的所有密钥进行更新。以 8 个组成员的满二叉树为例，设组成员 U_8 离开后逻辑密钥树如图 5 所示。

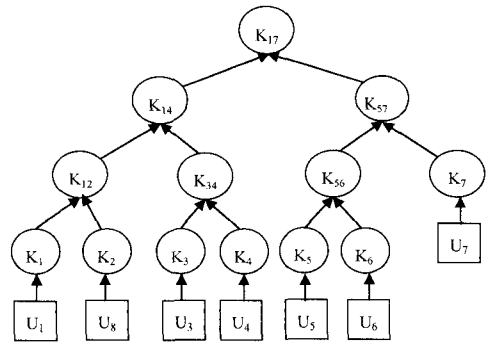

图 5　U_8 离开后的逻辑密钥树

组成员 U_8 离开后，GC 整理密钥树，选择将离开成员的位置删除，将更新后的密钥树通知给相应的组成员，然后进行密钥更新工作。

(1)组管理者 GC 将 K_{57}、K_{17} 进行签密得到的消息 $signcrypt_{GC,U_5,U_6,U_7}(K_{17},K_{57})$ 发送给组成员 U_5、U_6 和 U_7。

(2)将 K_{17} 进行签密得到的消息 $signcrypt_{GC,U_1,U_2,U_3,U_4}(K_{17})$ 发送给组成员 U_1、U_2、U_3、U_4。

组成员离开后的密钥更新可以保证组密钥的后向安全性。除了成员加入、退出时需要更新组密钥以外，组管理者也需要对组密钥进行定期更新，可见 3.2.3 节的组密钥的生成分发。

3.2.6　私钥更新

空间网络中的节点如卫星节点、临近空间节点等都将在空中长期存在，而节点私钥若长期不进行更新则会增加其被攻破的机率，为了保证节点私钥安全，需对节点私钥的进行定时更新。而地面节点的私钥更新可由地面的私钥生成器 PKG 来进行更新；卫星节点直接接收地面总控中心的调度和管理，则其私钥更新可由地面站直接进行更新；临近空间节点和空间层其他节点(指除卫星节点以外的节点)的私钥更新也必须要考虑，下面直接考虑临近空间节点(空间层其他节点类似)。

考虑到临近空间层的节点链路，这里考虑临近空间节点-

地面站间链路：若地面站在节点的覆盖范围之内，则可以直接通过该链路进行远程控制和高速数据通信；否则，就需要借助卫星网络为中继实现临近空间网络节点与地面站的交互，而私钥更新要与地面总 PKG 交互。另外，空间层的其他节点在不能直接与地面控制中心联系时通过卫星节点来与地面控制中心取得联系。因此，本方案考虑由卫星节点为临近空间节点进行定期的私钥更新。

空间网络中卫星节点的运动是有规律、有周期性，并且是可预知的。为了防止单点失效而导致的 PKG 瘫痪问题，可在卫星网络中采用分布式的私钥生成中心 PKGs 负责为临近空间层节点更新私钥，采用基于门限的密钥共享机制将 PKG 功能分布到不同的卫星服务节点上。

3.2.6.1 私钥更新方案设计

地面节点的私钥更新可由地面的私钥生成器 PKG 来进行更新；卫星节点直接接收地面总控中心的调度和管理，则其私钥更新可由地面站直接进行更新；临近空间节点的私钥则由卫星节点负责更新。

在空间网络中，卫星网络节点、临近空间网络节点等动态节点在空间中所处的位置不同，与地面中心之间的无线链路的通信质量和安全性也有着较大的差别。因此，地面控制中心的安全视界为离地面中心相对较近、通信链路良好、安全威胁小的空间区域，其中卫星节点的运动是有规律、有周期、可预知且分布均匀的，就是说部分卫星节点会周期性地运行到地面中心的安全视界内[2]。私钥更新方案的思路描述如下：

如前文所述，地面控制中心会配置一个集中的私钥生成中心 PKG，节点想要进入空间网络需由该 PKG 认证身份并生成初始私钥；

选择若干卫星节点组成空间中在线的私钥生成中心 PKGs，选取在一定时间间隔内至少出现在地面 PKG 安全视界内一次的卫星节点。这些卫星节点在进入网络时，由 PKG 为每一个节点分配一个主密钥分量，门限数个 PKGs 节点联合可提供私钥更新在线服务；

网络运行阶段中，PKGs 运行到地面中心的安全视界内时，PKG 负责为其提供主密钥分量更新服务。

3.2.6.2 私钥更新方案描述

用 ID 表示网络节点身份标识空间，对于任意节点 A，其身份标识 $id_A \in ID$。方案采用 B&F 提出的基于双线性对的 IBE 体制。方案实施中，门限值和密钥分量的更新周期的选择可参照文献[8]中给出的度量方案来进行计算。

1. 系统初始化

地面总 PKG 做如下操作：

(1)选取系统参数。PKG 选择大素数 q，q 阶的循环加法群 G_1 和 q 阶乘法群 G_2，双线性对 $\hat{e}: G_1 \times G_1 \to G_2$，$P$ 为 G_1 的生成元。PKG 在 Z_q^* 上选择随机数 s 作为系统的主密钥，则系统公钥为 $P_{pub}=sP$。选择哈希函数：$H_0: \{0,1\}^* \to G_1$，$H_1: G_2 \to \{0,1\}^*$，$H_2: \{0,1\}^* \to Z_q^*$，$H_3: G_1 \to Z_q^*$。其中，H_0 表示将代表节点身份表示的布尔串映射为 G_1 上的点，H_1 用来将 G_2 上的点映射为可用作会话密钥的定长布尔串，H_2 将布尔串(为消息或者身份标识)映射为 Z_q^* 上的整数，H_3 将 G_1 上的点映射为 Z_q^* 上的整数。

(2)选取 PKGs 节点。选择 n 个符合要求的卫星节点组成 PKGs 节点集合 Ω，初始主密钥的共享多项式：$f(x)=(s+\sum_{i=1}^{t-1} a_i x^i) \bmod q$(其中 $a_i \in Z_q^*$，t 为门限数)。对于 Ω 中的节点 V，PKG 为其生成初始的主密钥分量 $s_V=f(H_2(id_V)) \bmod q$ 和资格验证参数：$S_V=s_V sQ_{PKG}$，其中 $Q_{PKG} \in G_1$ 为 PKG 的公钥。t 个 PKGs 节点的 S_V 可以重构 $f(x)$，然后计算 $f(0)=s$ 恢复出主密钥，S_V 用于向其他节点证明自己拥有合法的 s_V，以及所签发的私钥分量的正确性。

(3)计算初始公私钥对。设置一个与节点更新次数相关的非零字符串 $phase$，用于生成节点在不同时间段内的公钥。初始时刻取 $phase=phase_0$，并向所有成员公开。成员节点 x 的初始公私钥对为 $\langle Q_x, S_x \rangle = \langle H_0(id_x \| phase), sH_0(id_x \| phase) \rangle$，其中 $\|$ 表示字符串拼接。在网络运行阶段，节点每次更新公私钥前取 $phase=phase+1$，然后计算新的公私钥对。

(4)节点私钥更新周期 w。空间网络中不同层次的节点特性不同，决定了应为其设置不同的更新周期，即 $w=\{w_V, w_A, w_G\}$(其中 w_V 为卫星节点的更新周期，w_A 为临近空间节点的更新周期，w_G 为地面节点的更新周期)，一般情况下，若未分开说明则用 w 统一表示更新周期。为避免请求更新的节点过于集中造成网络拥塞，节点私钥更新采用分批更新。若将节点分成 m 次更新，PKG 设置一个首次更新时间集合 $T_u=\{iw/m, i=1,2,\cdots,m\}$，定义映射 $g: ID \to T_u$，要求可以根据节点的身份将所有节点均匀地映射到 T_u。对于成员 x，在系统时间 $time_x=g(id_x)$ 时第一次申请密钥更新，之后每隔 w 时间申请一次密钥更新。公开更新周期 w，集合 T_u 和映射函数 g。

初始化完成，公开的参数包括

$\{P, P_{pub}, \hat{e}, G_1, G_2, H_0, H_1, H_2, H_3, Q_{PKG}, phase_0, w, g, T_u\}$。

2. 临近空间节点私钥更新

若在时刻 $time$，节点 x 需要将公私钥对 $\langle Q_x, S_x \rangle$ 更新为 $\langle Q_{x\_new}, S_{x\_new} \rangle$，其中 $time_x$ 为节点 x 的首次更新时间，k 为已完成的更新次数，则新公钥为 Q_{x_new}：

$$\left.\begin{aligned} &time_x=g(id_x)\\ &k=\lfloor (time-time_x)/w_A \rfloor\\ &Q_{x\_new}=H_0(id_x \| phase_0+k+1) \end{aligned}\right\}$$

私钥更新过程如下：

节点 x 选取随机数 $r_x \in Z_q^*$，计算 $R_x=r_x P$，$sig_x=r_x Q_x \hat{+} S_x$($\hat{+}$ 为 G_1 上的加法)，向网络广播私钥更新请求信息 $REQ_{update}(Q_{x\_new}, R_x, sig_x, id_x)$。

PKGs 收到请求消息后检验请求节点是否为已退出节点，若是，则算法结束；若为网络中现有节点，则验证 $\hat{e}(sig_x, P)=\hat{e}(Q_x, P_{pub} \hat{+} R_x)$，验证不成立则算法结束，否则继续执行。

PKGs 节点 V 使用其主密钥分量 s_V 计算节点 x 的新的私钥分量 $M_V=s_V Q_{x\_new}$，并生成资格验证参数 $h_V=s_V P_{pub}$，选择 $r_V \in Z_q^*$，对私钥分量加密 $u=M_V \hat{+} r_V R_x$，生成辅助解密参数 $R_V=r_V P$，向节点 x 返回应答消息 $RES_{update}=\{h_V, S_V, R_V, u\}$。

节点 x 收到 PKGs 节点 V 回应的更新应答消息后，验证 $\hat{e}(h_V, Q_{PKG}) = \hat{e}(P, S_V)$ 是否成立，若不成立，则丢弃该消息；若成立，则通过 $u \hat{-} r_x R_V = u \hat{-} r_x r_V P = u \hat{-} r_V R_x = s_V Q_{x\_new} = M_V$（其中 $\hat{-}$ 为 $\hat{+}$ 的逆元）解密消息，得到 PKGs 节点 V 签发的私钥分量。验证 $\hat{e}(M_V, P_{pub}) = \hat{e}(Q_{x\_new}, h_V)$ 是否成立，若成立，则接收 M_V；否则，丢弃该节点 V 签发的私钥部分 M_V。

节点 x 在收到 t 个通过验证的解密消息后，利用 Lagrange 插值法来重构得到新的私钥：$S_{x\_new} = \sum_{v \in \Lambda} \lambda_V(0) M_V = \sum_{v \in \Lambda} \lambda_V(0) s_V Q_{x\_new} = sQ_{x\_new}$，其中 Λ 为 t 个通过验证的 PKGs 节点集合，$\lambda_V(0)$ 为插值系数。

3. PKGs 主密钥分量的更新

门限密钥共享方案中，攻击者若掌握门限的数个密钥分量，则可以重构出主密钥，造成主密钥泄露。为了防止该情况出现，各 PKGs 节点的主密钥分量也需要进行周期性更新。

假设 $f(x)$ 为当前系统的主密钥共享多项式，地面总 PKG 随机选取次数为 $k-1$ 且常数项为 0 的多项式：$\xi(x) = (\sum_{i=1}^{t-1} b_i x^i) \bmod q, b_i \in Z_q^*$，生成下一周期的密钥共享多项式：$f(x)_{new} = f(x) + \xi(x)$。因 $\xi(0) = 0$，新的多项式仍满足 $f(0) = s$，也就是说，多项式形式已变但主密钥仍然不变。考虑到更新耗时问题，可以使得 PKG 在空闲时利用 $f(x)_{new}$ 为各 PKGs 节点进行预计算，得出下一周期的各 PKGs 对应的主密钥分量 s_V 和验证参数 $S_V = s_V sQ_{PKG}$。具体的主密钥更新步骤如下：

(1) PKGs 节点 V 运行到 PKG 的安全视界内时，选取随机数 $r_V \in Z_q^*$，计算 $R_V = r_V P$，$sig_V = r_V Q_V \hat{+} S_V$，然后向总 PKG 发送更新请求 $RES_{update} = \{R_V, sig_V, id_V\}$。

(2)PKG 收到请求消息后，检查节点 V 是否为已退出节点，是则结束，否则验证等式 $\hat{e}(sig_V, P) = \hat{e}(Q_V, P_{pub} + R_V)$ 是否成立。若不成立，则结束；若成立，则继续。

(3)PKG 选取随机数 $r_P \in Z_q^*$，计算 $v = (H_3(r_P R_V) + s_V) \bmod q, R_P = r_P P$，然后向节点 V 返回更新应答消息 $RES_{update} = \{R_P, v, S_V\}$。

(4)收到应答消息后，利用 R_P、v 和仅由自己掌握的 r_V 来计算新的主密钥分量：$s_V = (v - H_3(r_V R_P)) \bmod q = (v - H_3(r_V r_P P)) \bmod q = (v - H_3(r_P R_V)) \bmod q$。

(5)验证 $\hat{e}(S_V, P) = \hat{e}(s_V Q_{PKG}, P_{pub})$，若成立，则存储 S_V 和 s_V；不成立，则丢弃，重新提出申请。

4. 卫星节点和地面节点的私钥更新

在空间网络中，除了考虑临近空间节点的私钥更新外，还需考虑地面节点、卫星节点的私钥更新，其私钥更新直接由地面 PKG 直接完成，而公钥的更新同以上方案。

(1)公钥计算。若在时刻 $time$，节点 x（这里的节点 x 指地面节点和卫星节点，我们在这里共同考虑，因为他们都可以直接与地面 PKG 直接联系）需要将公私钥对 $\langle Q_x, S_x \rangle$ 更新为 $\langle Q_{x\_new}, S_{x\_new} \rangle$，其中 $time_x$ 为节点 x 的首次更新时间，k 为已完成的更新次数，则新公钥为 Q_{x_new}：

$$\left.\begin{aligned} time_x &= g(id_x) \\ k &= \lfloor (time - time_x)/w \rfloor \\ Q_{x\_new} &= H_0(id_x \| phase_0 + k + 1) \end{aligned}\right\}$$

其中，w 代表 w_V 和 w_G。

(2)私钥生成及分发。PKG 为节点 x 生成新的私钥：$S_{x\_new} = sQ_{x\_new}$，将私钥签密后得到的消息 $signcrypt_{PKG,x}(S_{x\_new})$ 发送给节点 x，然后节点 x 经过解签密得到更新后的私钥。

3.3 针对地面层节点的改进

在一个较大型的动态组播组中，成员的加入、退出会很频繁，若随着节点的频繁加入或退出而频繁地更新组密钥是不明智的。一般在空间网络的实际应用中，卫星节点、临近空间节点、地面组管理者的存在是相对稳定的，而地面层的用户终端节点的加入或退出则非常频繁。很多情况下，提供给地面终端的很多服务对实时安全的要求并不严格，即一个节点的加入可能让其稍作等候或者离开的节点在短时间内仍可以接收到通信数据，这些延迟都是可以接收的。为了提高密钥更新效率，考虑组密钥的批量更新，通过牺牲部分前向、后向安全性来减少密钥更新所必需的花销。

批量更新的方案一般有两种：1)固定周期的批量更新；2)基于队列机制的批量密钥更新。固定周期批量更新即每隔一个时间周期更新一次组密钥，忽略了组成员关系变化的动态性。即使没有组成员的关系变化，组密钥也是需要定期更新的。

这里考虑将两个方法相结合使用。

首先，设定一个较长的时间间隔 interval 作为组密钥定期更新的时间间隔和较短时间间隔 s_interval，为管理组设置两个密钥更新定时器。在每次密钥更新完成之后，组管理者便激活密钥更新定时器，定时器 1 表示无成员关系变化时的组密钥定时更新，初始值为 interval；定时器 2 表示有成员关系变化时的组密钥更新，初始值为 s_interval。

其次，建一个合适的队列，利用队列数据结构存放加入和退出请求，根据队列的性质，队首的请求即为更新间隔内的第一个请求。思路：

- 若定时器 2 为非 0 但队列已满，则触发组管理者处理所有更新请求，两个定时器都置为初始值；
- 若定时器 2 已为 0 且队列非空，则触发组管理者处理队列中请求，两个定时器都置初始值；
- 若定时器 2 为 0 但队列为空，则定时器 2 置为 s_interval；
- 若定时器 1 已为 0，则触动组管理者的更新整个组的密钥，之后定时器都置初始值。循环往复。

组密钥的批量更新不仅减少了组管理者的计算开销，也节省了通信带宽。而为了提高方案的安全性，可对成员退出的情况作区别对待，对于被强制退出的成员，采用单个即时处理；自动退出的成员的情况数量多且发生频繁，因其对安全的威胁较小，故可采用批量密钥更新的方法进行处理。

另外，在一般的组密钥管理方案中，如本文采用的 LKH 方案中，组密钥更新时要求所有组成员都必须在线。一般卫星网络节点和临近空间节点有高可靠性等保证，地面组管理者一般要求时时在线，只是地面终端节点可靠性不高，用户维护意识不强，且对其在线离线的要求也并不严格。若节点离线期间进行了组密钥更新，则离线节点就会错过更新的组密钥。因此，可以考虑采用基于代理重加密的组密钥管理方案[12]来解决节点离线时的组密钥更新问题。

4 ID-GKM 方案分析

本文从安全性和性能两个角度来对方案进行分析。

4.1 安全性分析

本方案是基于身份的密码体制提出的，其安全性已有充分的证明。在基于身份密码体制安全的前提下考虑本文提出方案的安全性和正确性。

成员注册过程中，会话密钥协商的安全。会话密钥协商所需的数据由双方签密以后发送，可以防止被篡改，解签密的过程也执行了认证，只要双方的私钥未泄露，则会话密钥必然是安全的。

密钥生成分发协议的安全。组密钥由组管理者随机选取，就算得到部分也无法通过其得到其他组密钥。分发阶段采用了基于身份的多接收者签密方案对密钥分发进行保护，之后指定接收者才可以解签密得到密钥。组成员收到消息后先进行认证再接收密钥，可保证收到的密钥的安全性(真实性和有效性)。

密钥更新过程的安全。组密钥更新过程中，采用了基于身份的多接收者签密方案对密钥进行保护，保证了消息的真实性，因可以进行源认证，验证消息来自于组管理者；保证了消息的保密性，因只有指定接收者才可以解密消息；可使消息满足完整性和不可否认性，确保消息没有被篡改，并且组管理者不能否定发出该消息。

密钥更新的前向后向安全。成员加入、离开时都会对组密钥以及逻辑密钥树进行更新。使得新加入的成员得不到其加入前的组密钥，无法解密以前传输的消息，保证了前向安全。退出的成员无法得到新的组密钥，即无法解密出其退出组以后的组消息，保证了后向安全性。另外，批量更新会牺牲一部分的前向、后向安全来提高更新的效率，但只会用在对消息的实时安全要求不高的情况下，此时密钥更新仍是安全的。

私钥更新的安全。经分析可知，攻击者想要通过已知信息得到系统主密钥要解决离散对数问题和判定双线性 DH 问题。一般情况下，认为离散对数问题和判定双线性 DH 问题都无法以不可忽略的概率在多项式时间 PPT 内解决，因此，攻击者通过公开参数计算或者窃听消息来重构主密钥是不可实现的。攻击者若试图获取到门限个主密钥分量来重构主密钥，本身就是很困难的。而本文提出的主密钥分量采用周期性更新机制，主密钥分量的更新周期和门限值的选择参考文献[21]给出的度量方法计算得到，可使得攻击者重构主密钥的概率可忽略。即方案可保证系统主密钥的安全，另外，经分析私钥和主密钥分量的更新均可以确保机密性和认证性。

4.2 性能分析

性能分析主要从存储开销、通信开销和计算开销 3 个方面来进行。本文组密钥管理方案的性能分析，假设逻辑密钥树为平衡树。

首先，ID-GKM 存储开销为：各组成员所存储的密钥数量等于其对应的叶子节点到根节点的路径上所有节点数目，即树的高度 $h=\log_d N+1$(其中，d 为密钥树的出度，N 为树中叶子节点的数目)。而组管理者存储的密钥数量为逻辑密钥树中所有节点所对应的密钥数，即$(d^h-1)/(d-1)=(dN-1)/(d-1)$。除了组密钥及其辅助密钥以外，每个节点还需要存储自身的公私钥对和基于身份密码机制的公开参数，但这部分开销对组员来说是固定的，不会随着规模的扩大而增加。

其次，组密钥管理算法的通信开销从组密钥的分发、成员加入时的密钥更新和组成员离开时的密钥更新这 3 个过程来进行分析。

如表 1 所列，本方案中采用基于身份的多接受者签密机制来分发密钥，因此没有单播消息，减小了通信开销。并且其成员加入退出时的通信开销较 LKH 方案也较小。

表 1 组密钥分发以及组成员加入或离开时密钥更新的通信开销

通信开销	单播次数	组播次数	消息总量
组密钥分发	0	$(N-1)/(d-1)$	$(N-1)/(d-1)$
组成员加入	0	h	h
组成员退出	0	h−1	h−1

最后，考虑其计算开销。组密钥管理中的计算开销主要是由密钥分发和密钥更新过程中消息处理的密码学算法开销组成，本方案的计算开销主要在于组管理者对消息签密的开销和节点对消息解签密的计算开销，设方案中签密、解签密的开销为 S、U。成员加入退出时，将组成员节点分为请求节点和非请求节点。计算开销如表 2 所列。

表 2 组密钥分发以及组成员加入或离开时密钥更新的计算开销

节点		组密钥分发	成员加入	成员退出
组管理者		$S(N-1)/(d-1)$	Sh	$S(h-1)$
组成员	请求节点	$(h-1)U$	U	0
	非请求节点		U	U

由于基于身份的公钥签密、解签密的开销远大于对称密钥的加解密开销，因此本文提出的方案的开销将会大于 LKH。但组密钥分发只发生在刚分组时或者定期更新组密钥时，一般更看重成员加入或退出时密钥更新的计算开销。在有成员加入或退出时：对组管理者来说，本方案的计算次数较小，但使用的签密机制的开销较大，所以总的计算开销仍然较大；对申请加入的节点，仅一次解签密操作，与密钥树无关；对非请求节点，无论是成员加入还是退出，开销仍为一次解签密操作。因此，组成员数量越多，本方案的计算优势越大。

结束语 针对整个空间网络架构中空间层、临近空间层和地面层节点，提出了适合空间网络的组密钥管理方案，该方案除了常用的组密钥生成分发、密钥更新外，还考虑了私钥更新。在私钥更新部分采用 B&F 提出的基于身份的公钥加密机制，提出了适合空间网络的私钥更新机制。本组密钥管理方案中，采用 LKH 组密钥管理方案提高管理组的可扩展性，使用基于身份的多接收者签密机制来保证密钥分发的安全性。该方案能够适应空间网络的层次化架构，满足其对强扩展性、高可靠性等的要求。另外，针对地面终端节点和空间节点的不同，对地面层节点的密钥管理做了改进。但空间网络系统庞大，本文只是一个整体的框架方案，具体实施中仍有很多细节需要考虑，比如不同域应由不同的 PKG 进行管理等。

参 考 文 献

[1] 彭长艳. 空间网络安全关键技术研究[D]. 长沙：国防科学技术大学，2010

[2] 罗长远，李伟，邢洪智，等. 空间网络中基于身份的分布式密钥管理研究[J]. 电子与信息学报，2010，32(1)：183-188

[3] Yu Yong，Yang Bo，Huang Xin-yi，et al. Efficient Identity-Based

Signcryption Scheme for Multiple Receivers[C]//Proceedings of the 4th International Conference on Autonomic and Trusted Computing, ATCZOO7, Lecture Notes in Computer Science 4610. HongKong, China, 2007: 13-21

[4] Ayan R-C, Baras J S, Hadjitheodosious M, et al. Security Issues in Hybrid Networks with a Satellite Component [J]. IEEE Wireless Communications, 2005, 12(6): 50-61

[5] Yavuz A A, Alagozl F, Anarim E. A New Satellite Multicast Security Protocol Based on Elliptic Curve Signatures [C]// 2nd Information and Communication Technologies, 2006 (ICTTA '06). 2006

[6] Yavuz A A, Alagozl F, Anarim E. NAMEPS: N-Tier Satellite Multicast Security Protocol Based on Signcryption Schemes [C]// Proceedings of the 49th Annual IEEE Global Telecommunications Conference (Globecom2006). San Francisco, California, USA, 2006: 1-6

[7] 杨德明，慕德俊，许钟. Ad hoc 空间网络密钥管理与认证方案[J]. 通信学报，2006，27(8)：104-107

[8] 罗长远，李伟，李海林，等. 分布式 CA 下空间网络认证密钥安全度量方法[J]. 电子与信息学报，2009，31(10)：2316-2320

[9] Victor P, Hubenko J, Raines R A, et al. Improving Satellite Multicast Security Scalability by Reducing Rekeying Requirements [J]. IEEE Network, 2007, 21(4): 51-56

[10] 王宇，卢昱，吴忠旺，等. 构建多级多层的空间信息系统安全基础设施[J]. 宇航学报，2007，28(5)：1081-1085

[11] Chen T-H, Lee W-B, ai H-B. A Self-Verification Authentication Mechanism for Mobile Satellite Communication Systems [J]. Computers and Electrical Engineering, 2009, 35(1): 41-48

[12] Chen Yi-ruei, Tygar J D, Tzeng W-G. Secure Group Key Management Using Uni-Directional Proxy Re-Encryption Schemes [C]// IEEE INFOCOM 2011: The 30th IEEE International Conference on Computer Communications. 2011

（上接第 312 页）

的电力噪声功率下，新算法的均方误差比经典算法小很多。这说明，新算法对数据分组起点的检测准确性比经典算法高。

表 1 新算法及经典算法检测误差

	$n_0=-10$dB		$n_0=-30$dB	
	新算法	经典算法	新算法	经典算法
最大检测值	1257	1570	1005	1014
最小检测值	812	317	807	613
均值	979	967	994	981
均方误差	14.55	43.34	6.73	21.93

图 7 为 n_0 为－30dB～－10dB 的条件下，两种算法 100 个数据分组的检测起点均值比较，在－10dB 时，新算法的均值为 979，而经典算法为 967，经典算法比新算法的均值大；在－30dB时，新算法的均值均值为 994，而经典算法的为 981，同样经典算法比新算法的均值高。所以从图 7 中可以看出，多个数据分组检测起点求平均后，检测结果更逼近真实起点，并且新算法比经典算法更准确，在低信噪比环境中依然适用。

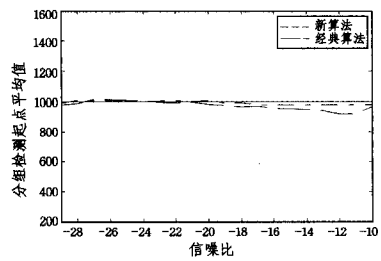

图 7 两种算法检测起点均值比较

结束语 发展智能电网要求高速的电力线通信技术，OFDM 技术作为一种高速、可靠的多载波通信技术，在智能电网中的地位日益重要。G3 标准 OFDM 技术因为具有 ROBO 的通信模式及高的频带利用率，所以被选来研究下行分组检测算法。G3-PLC 协议帧具有 8 个 256 采样周期的完全相同前导，用来进行数据分组检测。经典的分组检测算法采用延时相关算法，对当前 D 个接收数据和延迟的 D 个接收数据做相关，因为之前假定的高斯白噪声的非相关性，在出现信号之前，接收信号的延时相关值很小，当两个滑动窗完全进入前导数据后，延时相关值出现突变，利用预先设定的门限即可检测出数据分组的到来。但是在电力环境下，由于噪声具有非高斯性，这种变化不是很明显，检测结果具有较大的误差。通过对不同功率电力噪声条件下，延时相关值的比较，对经典算法进行改进，先将延时相关值利用微分器进行锐化处理，再利用设定的门限进行分组起点的检测。通过性能评测可知，新算法能够提高分组检测的准确度。

参 考 文 献

[1] Hoch M. Comparison of PLC G3 and PRIME [C]//IEEE International Symposium on Power Line Communications and its Applications. May 2011: 165-169

[2] International Electrotechnical Commission. Distribution automation using distribution line carrier systems: SN EN 61334-6[S]. IEC, 2000

[3] Hooijen O G. A channel model for the residential power circuit used as a digital communications medium[J]. IEEE Transactions on Electromagnetic Compatibility, 1998, 40(4): 331-336

[4] Mathias G, Rapp M, Dostert K. Power line channel characteristics and their effect on communication system design[J]. IEEE Communications Magazine, 2004, 27(1): 78-86

[5] Zimmermann M, Dostert K. A multipath model for the power line channel[J]. IEEE Transactions on Communication, 2002, 50(4): 555-559

[6] Zimmermann M, Dostert K. Analysis and modeling of impulsive noise in broad-band powerline communications[J]. IEEE Transactions on Electromagnetic Compatibility, 2002, 44(1): 249-258

[7] Zhai Ming-yue. Measurements and channel characteristics of LV power line communications networks in China[C]//IEEE International Symposium on Power Line Communications and Its Applications. 2006: 212-216

[8] ERDF. PLC G3 Physical Layer Specification [OL]. http://www.erdfdistribution.fr/medias/Linky/PLC_G3_Physical_Layer_Specification.pdf

[9] 胡景明，郭道省，王辉. 高阶调制 APSK 信号载波同步算法[J]. 计算机科学，2013，40(6A)：239-242

[10] 张进，赵文栋，彭来献，等. 相对误差受限的数据流流量测量算法[J]. 计算机科学，2013，40(6)：80-83