

天地一体化网络中基于预认证与群组管理的安全切换方案

洪佳楠¹, 李少华^{1,2}, 薛开平¹, 洪佩琳¹

(1.中国科学技术大学电子工程与信息科学系, 安徽 合肥 230026;

2.中国科学院信息工程研究所, 北京 100093)

摘要: 针对天地一体化网络中卫星节点高速移动过程的卫星接入点频繁切换问题, 利用卫星轨迹可预测的特点, 提出了基于组的多移动节点安全切换方案。该方案针对网络中卫星节点和地面移动节点的移动特性, 对多移动节点切换过程中的交互信息进行有效汇聚; 利用卫星节点运动轨迹可预测的特性, 提前通过安全上下文完成预认证与会话密钥协商。和已有方案相比, 所提切换方案在保证切换所必备的安全性的同时, 显著减小了切换延时以及认证和密钥协商过程中节点的通信、计算负担, 适用于卫星节点能量受限的天地一体化网络环境。

关键词: 天地一体化; 切换认证; 密钥协商; 群组管理

中图分类号: TV651.3

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00081

Pre-authentication and group management based secure handover for space-earth integration network

HONG Jia-nan¹, LI Shao-hua^{1,2}, XUE Kai-ping¹, HONG Pei-lin¹

(1. Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230026, China;

2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: In space-earth integration network, high-speed movement of space nodes brings in the problem of frequent satellite access router (SAR) handover. A group-based secure handover scheme for multiple mobility nodes (MN) utilizing satellite trajectory prediction was proposed. By using the movement features of the corresponding entities, an efficient aggregation mechanism for the interaction message occurred during the multi-MN handover was put forward. By using predictable satellite trajectory, authentication and session key agreement between new SAR and MN was accomplished beforehand with the secure context. Compared with existing schemes, the proposed scheme can provide necessary security features, lower the handover delay, and reduce the computation and communication overhead of mutual authentication and key agreement. The proposed scheme well suits the space-earth integration network, where the satellite node is energy constraint.

Key words: space-earth integration, handover and authentication, key agreement, aggregation in group

1 引言

随着航天技术和卫星通信技术的高速发展和

用户对通信需求的日益迫切, 将卫星通信融合到地面网络中已经成为学术界和工业界的重要趋势^[1]。这种天地一体化网络, 由地面网络、星地接入网

收稿日期: 2016-05-29; 修回日期: 2016-07-01。通信作者: 薛开平, kpxue@ustc.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61379129); 国家重点研发计划基金资助项目 (No.2016YFB0800301)

Foundation Items: The National Natural Science Foundation of China (No.61379129), The National Key Research and Development Plan of China(No.2016YFB0800301)

以及星际互联网组成, 该网络覆盖范围广、机动性强且通信链路不易受自然灾害、极端环境等外部作用的影响。

技术上, 与高轨同步卫星(GEO)相比低轨卫星(LEO), 在通信延时和信号衰落等方面, 具有不可替代的优势。为了满足天地一体化网络中日益增长的通信需求, 由LEO逐渐代替GEO作为卫星接入点来承载通信系统已成为不可阻挡的趋势。然而, LEO节点的高速移动性使地面移动节点在通过卫星接入网络时会更频繁地改变相应的卫星接入点。

一方面, 卫星节点的计算能力受限、星际链路的不稳定性和相对较高通信时延等因素, 使地面移动节点和卫星节点在切换过程中的重复接入认证成为系统的一大性能瓶颈。更迫切的是, 切换过程中通信的连续性需求, 使移动节点无法忍受接入认证过程引起的高时延。因此, 面向卫星接入点的轻量级、低延时的切换方案不断被提出^[2-5]。另一方面, 由于天地一体化网络的链路开放性, 导致它面临信息被窃取和干扰的威胁。移动节点的安全认证与接入是天地一体化网络中的第一道防线, 而在认证与接入地频繁交互过程中, 如何设计出在保证必要安全需求的同时, 避免复杂的认证过程和重复的密钥交换协议的切换方案, 是本文关注的焦点问题。

在天地一体化网络中, 许多研究都基于LEO轨迹预测技术提前完成地面节点与新卫星路由节点之间的切换认证和密钥交换协议^[6-8], 这是因为在该网络中, 绝大多数切换发生的原因来自LEO节点高速移动导致的节点覆盖范围的快速转移。例如, 在铱星系统中, 对于地面某一固定的节点, 单个LEO卫星节点的覆盖时间为8~11 min, 而每个点波束的覆盖范围为1~2 min^[8]。然而, 进一步研究可以发现, LEO有规律的高速移动, 除了轨迹可预测之外, 还有另一个不可忽视的特性, 即地面相邻的一组用户发生切换时具有极强的相似性: 相同的原始卫星接入点、相同的新卫星接入点以及相同的切换时间。以组的方式完成这类用户的汇聚式切换, 具有进一步降低切换延时并且减少节点运算、通信开销的潜力。就调研结果看, 目前尚未有基于这一特性而做的工作。

本文针对高速LEO节点的轨迹可预测特性, 为相邻位置多地面移动节点提出高效、安全的组切换方案。通过对多个同时发生切换移动节点的切换操作进行有效汇聚, 本文方案显著降低了卫星接入点的通信、计算开销。此外, 基于预测的安全上下文提前转移机制, 能够显著降低切换过程带来的通信中断时间。

2 相关工作

由于网络环境存在极大的差异, 其他无线网络中的切换方案很难适用于卫星网络中, 因此, 针对卫星网络的节点移动和链路特性设计相应的切换和认证方案一直是研究天地一体化网络的重要问题之一。针对文献[2]总结的已有工作的切换方案以及卫星网络中水平切换的研究意义, 文献[3]给出基于阈值的优先级切换方案; 文献[4]提出软切换的方案机制。也有许多工作在提高切换时间的准确性方面提出相应机制^[5-7]。虽然这些工作并未提出安全上的相应保护机制, 但有效地减少了切换过程带来的延迟、能耗问题, 提高了卫星网络的服务质量。

为了保证切换过程的安全需求, 目前, 已有一些致力于安全切换的研究成果。文献[6, 7]都提出了安全切换的方案, 文献[8]指出之前的安全切换协议没有详细描述切换协议的执行过程, 给出了一种基于预认证的快速切换算法, 同时详细地展示了协议流程。文献[8]中使用了PKG(public key generator)^[9]体制来完成卫星网络中的密钥管理, 相对于公钥基础设施PKI, PKG可以有效降低非对称密钥在使用中的通信及计算开销^[10, 11]。2012年, 文献[12]提出基于双线性映射的切换认证方案, 该方案可有效抵御拒绝服务攻击, 认证开销小, 可为天地一体化网络中高效安全切换方案的设计提供参考。文献[13]总结了目前卫星网络的安全问题, 包括安全切换、安全传输、密钥管理、安全路由等方面。

切换时间的选择对于切换的准确性、通信的连续性以及系统的开销都有重要的决定作用, 这种选择一般使用切换决策算法来完成。传统的切换决策算法较多使用基于信号接收强度(RSS, received signal strength)的判断算法, 进一步地,

许多改进的切换决策算法不断被提出^[14,15]。文献[14]提出基于马尔可夫决策过程的自适应决策算法，其采用了RSS预测等来完成切换时间的选择；文献[15]提出一种基于Q学习的切换决策算法，该算法利用RSS、位置以及速度等信息，通过Q学习算法对切换时间进行预测。

进一步分析可以发现，上述针对卫星网络中的安全切换方案有一个共同点，即均只考虑单个用户在卫星接入点之间发生切换的场景。然而在天地一体化网络中，卫星的高速移动导致覆盖范围的转移是切换发生的主要原因，在这种情况下，该区域内所有用户需要同时迁移到新的卫星接入点。现有的针对单用户的切换方案无法很好地适应这种场景，因此进行多用户统一的安全无缝切换的研究十分必要。

3 网络和安全模型

3.1 网络结构和节点移动特性

本文研究地面移动节点通过卫星网络通信时的切换方案。这一过程主要考虑以下实体：移动节点MN、通信对端CN、原卫星接入点OSAR、新卫星接入点NSAR以及CN的卫星接入点CSAR。图1展示了网络结构中各实体的分布和相互关系。相对于卫星接入点SAR的高速移动，地面MN节点处于准静止状态。每个SAR都覆盖着一块通信区域，随着它的高速移动，通信区域也随之高速转移。如图1所示，虚方框所包围的MN原先通过OSAR接入网络，与各自的CN通信；由于卫星的高速运动，这一范围内的MN进入NSAR的覆盖范围，并即将脱离OSAR的覆盖范围。此时必须将这些MN的数据流从OSAR切换至NSAR以保证各自会话的连续性。

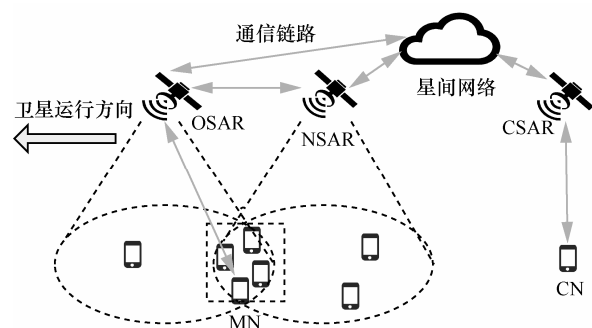


图1 天地一体化网络切换过程中的网络架构

与其他基于地面基站或AP的无线网络不同，天地一体化网络中的SAR节点能量受限，因此，依赖于大量计算或通信开销的切换算法无法部署在该网络中。此外，不稳定、长延时的链路使依赖于多次交互的切换认证方案带来的延迟问题在该网络中放大。综合来看，该网络亟需一套低计算/通信开销、低延迟的切换认证算法。

天地一体化网络中节点移动特性为理想切换认证方案的设计提供了参考，本文总结了3点有助于为无缝安全切换提供支持的节点移动特性。

1) 由于SAR高速运动，地面MN在网络架构中被认为是准静止状态。因此，绝大多数切换的发生可认为是由于SAR运动导致的覆盖范围的转移。

2) SAR的运动轨迹是可预测的。因此，与传统的无线网络相比，切换前NSAR节点的预测以及切换发生时间的预测更为准确。

3) 当覆盖范围变化时，在同一SAR的覆盖范围内，相邻位置的所有MN会同时发生切换，并且它们可选择相同的NSAR。因此，在SAR中可以以组的形式管理MN，并以高效的措施汇聚组内多MN的切换交互消息，能够进一步提高安全切换中的性能表现。

目前，许多针对卫星网络切换的研究考虑了卫星轨迹可预测的特性，提出了NSAR和MN之间的预认证机制^[8]或OSAR和NSAR上下文提前转移机制^[6]。然而，相邻位置MN同时切换的特性并没有被有效利用。因此，目前基于轨道预测的切换方案仅能在减少切换时间、保证会话连续性上做出突破，而无法在切换过程中为减少节点间的通信和计算开销提供支持。

3.2 安全需求

切换过程除了要保证MN与各自CN之间的会话连续性之外，开放的无线链路导致的安全问题同样不容忽视。为了实现安全的通信系统，接入和切换过程需要满足以下特性。

1) 双向认证：为了保证用户和卫星接入点之间的安全会话，两者的双向认证是前提和必要因素。有效的双向认证可以防止服务器的欺骗攻击和伪造用户攻击。

2) 会话机密性：为了防止会话被窃听，通信

数据和必要信令需要进行加密保护。

3) 后向安全性: 系统中原始会话(切换前)若被攻击, 其引起的安全问题不能影响新会话, 即切换之后地面移动节点和新卫星接入点之间的通信。

3.3 PKG 体制

在基于身份的密码系统中, PKG (private key generator) 作为可信方为系统中的实体产生并管理私钥。在 PKG 体制中, 实体的公开信息(如姓名、电子邮件地址等)即为其公钥, PKG 根据实体的公钥, 并通过秘密管理的系统主密钥为其产生私钥。系统中的任意实体也都可以轻松地获取到其他实体的公钥, 而无需额外进行公钥验证。相对于 PKI 体制中通过 CA 颁发证书的方式来保障公钥的安全获取和使用, PKG 显著降低了实体的计算和存储开销, 尤其在卫星网络环境下, 避免证书的传输、验证、存储等操作给卫星网络节点带来额外的开销十分必要, 因此, 近年来的一些卫星网络的方案中均使用 PKG 体制来进行密钥管理^[10,11]。

双线性配对是 PKG 体制中实现加密、签名和签密等一系列安全协议算法的重要工具, 下面简要介绍双向性配对的基本概念。

设 G_1 是由生成元 P 生成的加法循环群, 其阶为素数 p , G_2 为具有相同阶 p 的乘法循环群, 双线性配对是指具有如下 3 种性质的映射 $e: G_1 \times G_1 \rightarrow G_2$ 。

1) 双线性: 对所有 $P, Q \in G_1$, $a, b \in Z_p^*$, 有 $e(aP, bQ) = e(P, Q)^{ab}$ 。

2) 非退化性: 存在 $P, Q \in G_1$, 使 $e(P, Q) \neq 1_{G_2}$, 其中, 1_{G_2} 为 G_2 的单位元。

3) 可计算性: 对所有 $P, Q \in G_1$, 存在有效的计算 $e(P, Q)$ 的算法。

综合应用以上性质, 可以使双线性对在 PKG 体制中安全地进行加密、签名等操作。在本文所介绍的方案中, PKG 使用公开的系统参数 p 、 G_1 、 G_2 、 e 、 P 以及秘密掌握的主密钥 s 和公开公钥 sP 等, 结合各主体的身份公钥为其产生私钥并秘密地传送给各实体。并且, 在这体制下, 接入认证过程中的密钥协商既能实现 Diffie-Hellman 密钥交换协议所能实现的公开信道下统一会话密钥的

安全生成, 又可以抵御非授权实体的中间人攻击。

4 接入认证方案

在天地一体化网络中, 移动节点 MN 在获得网络服务之前, 首先需要通过某卫星接入点的认证并成功接入卫星网络。本节首先简单介绍 MN 和卫星接入点之间在接入认证过程中的方案; 之后, 介绍本方案中卫星节点对 MN 组的管理机制, 并详细介绍该机制中卫星接入点需要维护的 2 种数据表的内容和用途; 最后, 基于所提出的群组管理机制, 本文详细介绍涵盖预认证和切换 2 个阶段的多 MN 切换算法。

为了描述方便, 表 1 列举了文中所涉及到的重要相关实体的符号定义。

表 1 实体符号定义

符号	定义
MN (mobile node)	移动节点
CN (correspondent node)	通信对端
SAR (satellite access router)	卫星接入点
OSAR (original SAR)	原卫星接入点
NSAR (new SAR)	新卫星接入点
CSAR (correspondent SAR)	CN 的卫星接入点

4.1 MN 与 OSAR 之间的安全接入

在本文方案中, 当 MN 与 OSAR 进行双向认证时, 使用 PKG 体制分配、管理网络中各节点的密钥。在该体制中, PKG 作为全局可信第三方, 为每个节点(包括 SAR 和 MN)根据其公开的身份 ID 计算私钥, 并在初始化时安全地将私钥传递给各节点, 各节点秘密地存储私钥, 用于以后的加密或签名。此时, 每个节点的 ID 即为其公钥, 其他节点均可以安全且无需额外验证地使用该公钥。

本文方案利用文献[8]等使用的认证机制完成 MN 与 OSAR 之间的接入认证。大致的协商过程如下。

1) MN 随机选取 $a \in Z_p^*$, 并计算 aP 。其中 P 是基于椭圆曲线的加法群 G_1 中公开的生成元; p 为群的阶, 为素数。MN 秘密存储 a , 并将 aP 秘密地发送给 OSAR。

2) OSAR 随机选取 $b \in Z_p^*$, 计算 bP , 并秘密发送给 MN, 再利用 aP 、私钥 SK_{OSAR} 、MN 的公钥 PK_{MN} 以及 PKG 的公钥通过双线性映射计算出

会话密钥；MN 通过 bP 、私钥 SK_{MN} 、SAR 公钥 PK_{OSAR} 和 PKG 的公钥采用同样的方式计算出统一的会话密钥 $K_{MN-OSAR}$ 。

认证和密钥协商协议需要签名、加密或签密算法等机制来保护、抵御伪造用户（或接入点）攻击、中间人攻击等威胁。

在认证和密钥协商完成后，OSAR 还要为 MN 分配有效的网络地址。本方案通过子网号+主机号的形式为每个 MN 分配 IP，卫星接入点为同一地理区域内的 MN 分配一个子网号，再为该区域内的每个 MN 分配唯一的主机号，使用同一子网号的 MN 即在逻辑上形成了一个组，这个组的信息由 OSAR 维护和管理。

4.2 MN 组管理机制

根据对 MN 的定位信息，SAR 为位置上有特定联系的 MN 形成一个组进行管理。一个组内的 MN 地理位置相邻，当 SAR 的覆盖区域离开时，可以统一将组内用户的流量切换至新的接入点。与其他基于组的管理方式不同，在本文方案中，群组管理机制对 MN 是透明的。因此，MN 不需要为该机制做额外操作（如不需要为该组选择一个特定的 MN 作组管理员）。每个 SAR 维护 2 种表格来管理覆盖范围内的组。其中，表 2 维护 SAR 当前覆盖范围内的所有 MN 组。表 3 用于为每个组维护 MN 成员的信息。

表 2 组标识映射

组 ID	网络号	位置坐标	切换时间	NSAR
g_1	pre_1	L_1	t_1	SAR_1
g_2	pre_2	L_2	t_2	SAR_2
g_3	pre_3	L_3	t_3	SAR_3
...	...	...	...	...
g_i	pre_i	L_i	t_i	SAR_i
...	...	...	...	...
g_m	pre_m	L_m	t_m	SAR_m

表 2 记录了每个组的组标识 g_j ，组内 MN 的子网号 pre_j 作为该组每个 MN 的网络前缀。此外，计算所得的位置坐标 L_j 不仅可以管理组内 MN（MN 的离开和新 MN 的加入），还可用于协助预测该组 MN 切换的时间 t_j 以及 NSAR 的身份标识 SAR_j 。其中，该表还维护即将切换过来的 MN 组，在这种情况下，NSAR 身份标识对应的就是该

SAR 本身。当 OSAR 未选定 g_j 的切换方案时，表项中的切换时间和 NSAR 置空。

表 3 记录了一个组中所有的成员（用 MN_i 标识）的信息，包括成员的身份标识 ID_i 、成员在网络中的主机号 $HostID_i$ 、OSAR 与 MN_i 之间的会话密钥 K_{MN_i-OSAR} 以及用于协商会话密钥的参数 a_iP 。卫星接入点为每个组建立表 3 来管理组内的 MN 节点。

表 3 组 MN 映射

ID	主机号	会话密钥	密钥协商参数
ID_1	$HostID_1$	K_{MN_1-OSAR}	a_1P
ID_2	$HostID_2$	K_{MN_2-OSAR}	a_2P
ID_3	$HostID_3$	K_{MN_3-OSAR}	a_3P
...	...	...	...
ID_i	$HostID_i$	K_{MN_i-OSAR}	a_iP
...	...	...	...
ID_n	$HostID_n$	K_{MN_n-OSAR}	a_nP

在不同的情况下，表 2 和表 3 的内容均会有一些的变化，包括条目内容的修改、条目的增加或删除等，这些变化主要发生在以下情况。

1) 当新的 MN 节点加入时，如果它的地理位置属于某个已有分组 g_j ，则 OSAR 不需要改变表 2，只需要在对应分组的表 3 中新增记录 MN 的 ID、主机号、会话密钥以及密钥协商参数的条目。

2) 当已经接入的 MN 节点需要更新会话密钥时，该 MN 节点与 OSAR 执行与接入认证相似的过程完成会话密钥的更新，而新的会话密钥和密钥协商参数则在表 3 中进行更新。

3) 当检测到某一分组的 MN 节点即将发生切换时，OSAR 根据预测判断该 MN 组即将发生切换的时间以及 NSAR，并将该 MN 组所有节点在表 2 中的切换时间以及 NSAR 信息进行相应更新。此时，表 3 的相关条目不发生变化。

4) 当某个或某些 MN 节点成功切换至 NSAR 或与 OSAR 断开连接时，OSAR 将分组对应的条目在表 2 中删除，并清空该组对应的表 3。

4.3 基于组的多 MN 切换算法

本文将切换过程分为 2 个阶段：预认证阶段与切换阶段。在预认证阶段中，OSAR 将上下文信息传递给 NSAR；并且通过 OSAR 的中继，组内每个成员 MN 与未来的新卫星接入点 NSAR 之

间提前实现双向认证、地址更新和密钥协商。预认证阶段完成后,组内 MN 节点进入 NSAR 覆盖范围后开始进入切换阶段,完成 MN 的流量迁移。图 2 根据 2 个阶段描绘了切换过程中各实体间的信息交互。

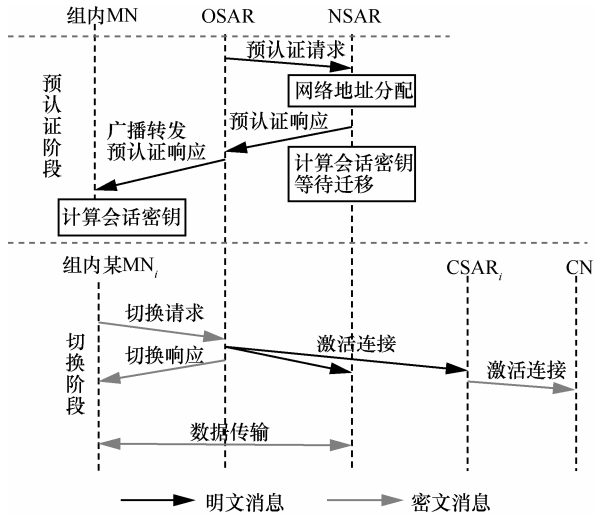


图2 迁移方案中各实体间通信流程

4.3.1 预认证阶段

OSAR 根据网络环境的预测,确定切换的时间、NSAR 以及发生切换的 MN 组,当这些信息确定之后,OSAR 在表 2 中将该分组的所有 MN 节点对应记录的切换时间及 NSAR 进行更新。本文方案在切换过程发生前,组内所有 MN 均还处在 OSAR 服务覆盖范围时,通过 OSAR 将组内 MN 的上下文提前转移至 NSAR,并提前完成所有 MN 与 NSAR 的双向认证、密钥协商以及地址分配。

OSAR 为组选择最佳 NSAR,通过星间链路发送预认证请求消息给 NSAR。预认证请求消息 PR 包括切换组内所有 MN 的身份 (ID_i)、主机号 ($HostID_i$) 和 aP 。 PR 需要 OSAR 私钥签名。OSAR 发往 NSAR 的消息格式如下。

$$Message = \{PR = \{\forall MN_i \in g_j : ID_i, HostID_i, a_iP\} \parallel Sign_{OSAR}(PR)\}$$

NSAR 收到预认证请求后,利用 OSAR 公钥验证。若验证通过,为新的组分配一个子网号 pre_j' ,并随机选择 $b \in Z_p^*$,计算 bP ,并将 pre_j' 和 bP 发送至 NSAR。预认证响应消息同样需要 NSAR 签名,如下所示。

$$\{pre_j' \parallel bP \parallel Sign_{NSAR}(pre_j' \parallel bP)\}$$

针对每个 MN_i , NSAR 计算会话密钥

$$K_{MN_i-NSAR} = ba_iP = a_i bP \quad (1)$$

之后,NSAR 新建组标识 g_j' ,并将 g_j' 、 pre_j'

以及该组的地理位置信息、切换时间和 NSAR 的 ID 插入表 2,其中,NSAR 的 ID 即该 NSAR 本身。NSAR 为 g_j' 新建表 3,记录和维护每个 MN 的 ID、主机号、 aP 以及新计算的会话密钥 $K_{MN-NSAR}$ 。

OSAR 收到预认证响应后,使用 NSAR 的公钥验证签名,验证通过后,为子网号为 pre_j 的节点以广播的形式转发预认证响应消息。

此时, g_j 中的所有 MN_i 都会收到该预认证响应消息。 MN_i 使用 NSAR 的公钥验证签名有效性,若验证通过,通过在接入 OSAR 中选择的随机数 a_i 以及响应消息中的 bP ,计算 MN_i 与 NSAR 之间的会话密钥

$$K_{MN_i-NSAR} = a_i bP = ba_iP \quad (2)$$

可以看到,NSAR 与 MN_i 各自计算所得的会话密钥是一致的,并且组内每个节点之间的会话密钥相互独立。因此,NSAR 和组内所有 MN 之间的密钥协商过程顺利完成。

4.3.2 切换阶段

当 MN_i 从 OSAR 的覆盖范围进入到 NSAR 的覆盖范围后,接收到 NSAR 发出的广播消息, MN_i 根据比较 OSAR 和 NSAR 的信号强度等相关信息,同时结合表 2 中的切换时间记录,来选择确切的切换时间。在切换之前, MN 向 OSAR 发送切换请求消息。OSAR 收到请求后,返回响应消息。2 个消息均使用 K_{MN_i-OSAR} 密钥加密。

OSAR 随后通过星间网络向 CSAR 发送激活连接消息,告知 MN_i 新的通信地址 ($pre_j' + HostID_i$)。CSAR 将该地址转告给 CN_i 。

上述 2 个激活连接消息分别需要 OSAR 和 CSAR 私钥签名。

OSAR 同时向 NSAR 发出激活连接消息,使其完成与 MN_i 的连接,为 MN_i 与 CN_i 之间的通信提供服务,其中, MN_i 与 NSAR 之间的通信使用 K_{MN_i-NSAR} 进行加密保护。

上述步骤完成之后,OSAR 与 MN_i 的连接即断开,OSAR 将该 MN 组所对应的表 2 相关条目

和表 3 删除，来释放该 MN 组占用的资源。

5 安全与性能分析

5.1 安全分析

本文所提切换方案能有效抵御已知的攻击手段，保证切换过程的必要安全需求。接下来从双向认证、会话机密性和后向安全性 3 个方面分析本文方案的安全性。

5.1.1 双向认证

本文方案中，预认证请求算法是由 OSAR 根据当前网络环境发送至 NSAR，并由 NSAR 做出响应。以接入认证时 MN 与 OSAR 之间已经完成双向认证为前提，由于预认证请求消息和响应消息由 OSAR 和 NSAR 各自的私钥进行签名，其他实体在没有私钥的情况下无法伪造消息。

在这种情况下，未与卫星接入点完成双向认证的 MN 无法进入预认证过程，除非它与 OSAR 或 NSAR 中任意一个完成认证。而预认证响应中的签名保证了 NSAR 的有效性。因此，本文方案能成功抵御恶意用户伪造 MN 或伪造 SAR。

5.1.2 会话机密性

会话机密性主要通过会话密钥的安全性来保证。因此，本文主要考虑 $K_{MN-NSAR}$ 协商过程的安全性。

本文方案在切换过程中的密钥协商过程是基于椭圆曲线的 DH (Diffie-Hellman) 密钥交换算法。基于 DH 困难假设，任何攻击者在仅知道 P 、 aP 和 bP 情况下无法计算出 abP 。因此，在本文方案中，密钥协商过程可在公开信道传输，而任何除 NSAR 和 MN 以外的其他实体都无法计算出会话密钥 $K_{MN-NSAR}$ ，包括 OSAR 和组内其他 MN 节点。

考虑到 DH 密钥交换算法存在中间人攻击的

威胁，本方案的密钥协商消息分别由 OSAR 和 NSAR 进行签名。由于任何其他实体均无法伪造出合法签名，因此仅有 OSAR 具有实施中间人攻击的可能。然而，OSAR 仅能伪造出 MN 的 $a'P$ ，无法伪造 $b'P$ 。因此，OSAR 通过成为 NSAR 和 MN 之间的中间人获利。

5.1.3 后向安全性

后向安全性主要通过会话密钥的独立性来保持。当恶意用户获得了某次 MN 与 OSAR 之间的会话密钥 $K_{MN-OSAR}$ 后发生切换过程。而 MN 与 NSAR 之间的会话密钥 $K_{MN-NSAR}$ 并不是由 $K_{MN-OSAR}$ 派生所得。由于参与会话密钥计算的随机数 a 秘密保存在 MN 中，因此，对某次会话的攻击不会影响之后会话的安全性。

5.2 性能分析

本文方案通过基于群组管理的多用户切换机制，可以有效地优化卫星接入点和移动节点的通信及计算性能；通过预认证与会话密钥协商的提前处理保证了切换过程中会话的连续性。

从通信和计算 2 个方面的开销来分析本文方案的性能，并与文献[6,8]进行对比。需要指出的是，对比方案在卫星轨迹预测、链路切换上的操作是一致的，只在预认证上存在差异。因此，表 4 的对比数据只衡量预认证阶段中的开销。

5.2.1 通信开销

文献[8]方案在切换时，需要每个 MN 都与 OSAR 单独交互，且 OSAR 也需要向每个 MN 单独返回响应信息，多个待切换 MN 之间无法进行汇聚；并且 OSAR 与 NSAR 之间需要为每个待切换 MN 往返上下文转移信息和其他相关信令。因此，OSAR 和 MN 之间、OSAR 和 NSAR 之间的通信开销随着待切换 MN 的数量线性增长。文献[6]方案虽然不需要 MN 向 OSAR 发送消息，但

表 4 相关工作性能分析与对比 (组内 MN 个数设为 N)

方案	通信开销 (次数×数据分组大小)				会话密钥协商算法	会话密钥信息传递保护机制	会话密钥计算开销		
	N 个 MN 到 OSAR	OSAR 到 N 个 MN	OSAR 到 NSAR	NSAR 到 OSAR			单个 MN	OSAR	NSAR
文献[8]方案	$N \times 1$	$N \times 1$	$N \times 1$	$N \times 1$	双线性映射类 DH 密钥交换	签名	2 次乘法运算 + 2 次双线性运算	0	$2N$ 次乘法运算 + $2N$ 次双线性运算
文献[6]方案	0	$N \times 1$	$N \times 1$	$N \times 1$	基于密钥派生秘密信道传输	签密	0	N 次伪随机数生成	0
本文方案	0	1×1	$1 \times N$	1×1	椭圆曲线 DH 密钥交换	签名	1 次乘法运算	0	$1+N$ 次乘法运算

OSAR 仍然需要向所有 MN 单独发送消息,且 OSAR 与 NSAR 也需要为每个 MN 往返相关信令。

本文方案中,切换请求由 OSAR 发起,且 MN 与 NSAR 之间密钥协商中使用的 aP 复用了 MN 与 OSAR 之间的信息,因此,省去了 MN 向 OSAR 的通信。本文方案的地址分配方式和密钥协商机制使 OSAR 只需要广播统一的新子网号和 bP 就可以完成所有 MN 的地址更新和密钥协商,这显著降低了 OSAR 与 MN 之间的通信开销;同时,这种高效的信令汇聚机制也降低了 NSAR 到 OSAR 的通信量。而从 OSAR 向 NSAR 需要传递的数据量看,汇聚机制的作用没有其他链路上的明显,但减少的通信次数在一定程度上提高了切换效率。

5.2.2 计算开销

文献[8]方案使用基于双线性映射的类 DH 密钥交换来完成密钥协商,这一过程中可使用签名来保障会话密钥协商信息的可认证性(原方案使用签密方式)。文献[6]方案使用密钥派生的方法来生成新的会话密钥,虽然在计算上开销降低,但是传输时必须使用签密的方式防止传输的会话密钥被窃取,且 OSAR 能够得到 NSAR 与 MN 的会话密钥,从这 2 个角度看,该方案在机密性上弱于其他对比方案。

本文方案采用的是基于椭圆曲线的 DH 密钥交换,与文献[6]方案相比,本文方案的协商信息可在公开信道上传输,因此只需要签名机制保证信息的可认证;与文献[8]方案相比,椭圆曲线上的乘法计算开销远低于双线性映射。

通过以上性能分析可以得出,本文方案在切换过程中采用的多 MN 汇聚机制可以有效地减轻 MN 与 NSAR 的通信及计算负担,可以更好地支持多 MN 统一切换的场景。

6 结束语

本文针对卫星网络中移动节点水平切换的问题,利用多个移动节点地理位置相近的特点,采用基于组的节点管理方式,提出多移动节点安全切换方案。通过对组内多移动节点的汇聚处理,本文方案在通信及计算 2 个方面很好地减少了卫星接入点和移动节点的负担;双向认证和密钥交换的预处理保证了切换过程中通信的连续性。本

文的性能和安全评估显示:本文方案在通信、计算方面与已有方案相比具有明显的优势,并且双向认证性、会话机密性及后向安全性保证了切换过程及新会话的安全,适用于 LEO 等高速移动的卫星网络中,移动节点区域分布的情形。

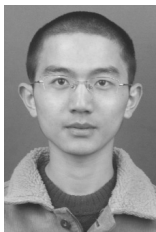
参考文献:

- [1] 沈荣骏. 我国天地一体化航天互联网构想[J]. 中国工程科学, 2006, 8(10): 19-30.
SHEN R J. Some thoughts of chinaese integrated space-ground network system[J]. Engineering Science, 2006, 8(10): 19-30
- [2] CHOWDHURY P K, ATIQUZZAMAN M, IVANCIC W D. Handover schemes in satellite networks: state-of-the-art and future research directions[J]. IEEE Communications Surveys and Tutorials, 2006, 8(4): 2-14.
- [3] DING D, MA D T, WEI J B. A threshold-based handover prioritization scheme in LEO satellite networks[C]//International Conference on Wireless Communications, Networking and Mobile Computing, IEEE. c2008: 1-6.
- [4] BARROS G, VIEIRA J, GANHÃO F, et al. A soft-handover scheme for LEO satellite networks[C]//IEEE 78th Vehicular Technology Conference (VTC). c2013: 1-5.
- [5] PAPAPETROU E, PAVLIDOU F N. Analytic study of doppler-based handover management in LEO satellite systems[J]. IEEE transactions on aerospace and electronic systems, 2005, 41(3): 830-839.
- [6] 徐国愚, 陈性元, 杜学绘. 一种新的基于上下文传递的临近空间安全切换机制[J]. 计算机科学, 2013, 40(4): 160-163.
XU G Y, CHEN X Y, DU X H. New near space security handoff scheme based on context transfer[J]. Computer Science, 2013, 40(4): 160-163.
- [7] 孟梦, 陈性元, 徐国愚, 等. 一种安全高效的 LEO 卫星网络任意点切换方案[J]. 计算机工程, 2015, 41(3): 1-6.
MENG M, CHEN X Y, XU G Y, et al. A secure and efficient LEO satellite network switching scheme at any point[J]. Computer Engineering, 2015, 41(3): 1-6.
- [8] 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.
PENG C Y. Research on key security technologies in space networks[D]. Changsha: National University of Defense Technology, 2010.
- [9] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Workshop on the Theory and Application of Cryptographic Techniques, Berlin Heidelberg. c1984: 47-53.
- [10] LUO C Y, LI W X, HONG Z. Research on identity-based distributed key management in space network[J]. Journal of Electronics and Information Technology, 2010, 32(1): 183-188.
- [11] ZHEFU Y, HAIGANG Z, ZHAOFENG W. Key management scheme based on certificateless cryptography for satellite networks[C]//The 2nd International Conference on Consumer Electron-

ics, Communications and Networks (CECNet). c2012: 1100-1103.

- [12] HE D, CHEN C, CHAN S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications, 2012, 11(1): 48-53.
- [13] JIANG C, WANG X, WANG J, et al. Security in space information networks[J]. IEEE Communications Magazine, 2015, 53(8): 82-88.
- [14] CHANG B J, CHEN J F, HSIEH C H, et al. Markov decision process-based adaptive vertical handoff with RSS prediction in heterogeneous wireless networks[C]//IEEE Wireless Communications and Networking Conference. c2009: 1-6.
- [15] 熊丹妮, 李屹. 星地融合网络中基于 Q 学习的切换算法研究[J]. 通信学报, 2015, 36(9): 252-258.
- XIONG D N, LI Y. Q-learning based handoff algorithm for satellite system with ancillary terrestrial component[J]. Journal on Communications, 2015, 36(9): 252-258

作者简介:



洪佳楠 (1989-), 男, 浙江宁波人, 中国科学技术大学博士生, 主要研究方向为网络安全协议设计与分析。



李少华 (1994-), 男, 安徽蚌埠人, 中国科学技术大学硕士生, 主要研究方向为信息与系统安全。



薛开平 (1980-), 男, 江苏东台人, 中国科学技术大学副教授, 主要研究方向为下一代网络体系结构与网络安全。



洪佩琳 (1961-), 女, 浙江宁波人, 中国科学技术大学教授, 主要研究方向为下一代网络体系结构与网络安全。