

安全高效的空间信息网中群组密钥交换协议

钟焰涛, 马建峰

(西安电子科技大学 计算机网络与信息安全教育部重点实验室, 西安 710071)

摘要:为实现空间信息网中保密通信, 提出一个适用于空间信息网的群组密钥交换协议。协议充分考虑了空间信息网中结点的通信特点, 所有的卫星结点根据其所在的轨道划分为不同的簇。协议由簇内阶段、簇间阶段和密钥分发阶段组成, 每个结点均生成密钥贡献值并汇总至地面中心结点, 中心结点生成密钥并秘密发送给每个结点。证明了协议具有语义安全性, 进行了通信复杂度分析并利用NS2软件进行了仿真验证。结果表明: 相比其他协议, 本文协议在空间信息网中应用时具有较高的通信效率。

关键词:通信技术; 群组密钥交换; 可证明安全; 空间信息网; 语义安全性

中图分类号:TN918. 91 **文献标志码:**A **文章编号:**1671-5497(2012)01-0203-04

Efficient secure group key exchange protocol in space information networks

ZHONG Yan-tao, MA Jian-feng

(Key Laboratory of Computer Networks and Information Security, The Ministry of Education, Xidian University, Xi'an 710071, China)

Abstract: A group key exchange protocol was proposed to implement secure communication in space information networks. In this protocol, all satellite nodes in a space information network were divided into different clusters according to the orbits they belong to. The protocol was composed of intra-cluster phase, inter-cluster phase and key distribution phase. Each node generates a key contribution value and sends it to the center node on the ground. On receiving all the contribution values, the center node generates a group key and distributes the key to all nodes in a secure manner. The semantic security of the proposed protocol was proved. Communication complex analysis and NS2 simulation software were employed to evaluate the proposed protocol. Results show that the proposed protocol achieves higher efficiency than other related protocols.

Key words: communication; group key exchange; provable security; space information network; semantic security

空间信息网(Space information network, SIN)是以在轨运行的多颗卫星及卫星星座组为骨干的新型通信网络^[1], 具有覆盖面广、组网灵

活、建网快、不受地理环境限制等突出优点。使用群组密钥交换(Group key exchange, GKE)协议建立共享密钥, 并使用密钥加密通信是保证空间

收稿日期: 2010-08-29.

基金项目: 国家自然科学基金项目(60872041, 60573036, 60702059, 60503012); 国家自然科学基金重点项目(60633020).

作者简介: 钟焰涛(1980-), 男, 博士研究生。研究方向: 信息安全与密码学。E-mail: zhongyantao@126.com

信息网通信安全的重要手段。适用于空间信息网的密钥交换协议也逐渐成为近年来的研究热点^[2]。国内外学者已经提出了许多安全高效的方法实现传统网络中的GKE协议^[3-5]。然而,空间信息网中结点的高速运动、动态拓扑等突出特点使得这些GKE协议难以在空间信息网中得以有效应用。文献[6]提出一种基于集簇机制的空间信息网的GKE方案,但是该方案没有考虑在空间信息网中由于网络结点的移动性和拓扑的动态性导致簇内成员的动态变化。文献[7]提出一种通用组合安全的空间信息网中密钥交换方案,但该方案只考虑了两方密钥交换,没有考虑群组密钥交换的情形。文献[8]提出一个空间信息网中的密钥交换框架,但并未给出具体的GKE协议实现。

为了更好地解决空间信息网中的群组密钥交换问题,本文充分考虑空间信息网的特点,提出了一个新的GKE协议。协议采用基于簇的集中式密钥生成技术,根据空间信息网中卫星结点按照轨道分布的特点,将每根卫星轨道视为一个簇,由中心结点根据每个簇的簇内临时密钥生成群组密钥。对协议进行了安全性分析和通信效率分析,并使用NS2仿真工具进行了实验对比。

1 安全高效的群组密钥交换协议

1.1 系统初始假定和协议参数

假定存在适应性选择消息攻击下抗存在性伪造攻击的签名方案,且空间信息网中每个结点均有用于签名的公私钥对,网络中所有结点的公钥均公开。协议中使用的参数如下: k :系统安全参数; q :一个满足 $q = O(2^k)$ 的大素数; G :乘法循环群 Z_q^* ; g :群 G 的一个生成元; $H: \{0,1\}^* \rightarrow Z_q^*$:一个抗碰撞的安全单向哈希函数。

1.2 协议概述

如图1所示,协议分为三个阶段:簇内阶段(I)、簇间阶段(II)、密钥分发阶段(III)。在簇内阶段,每个簇头结点发起簇内通信以生成一个簇内临时密钥;簇间阶段则由各簇头将该临时密钥汇总给中心结点;在密钥分发阶段,中心结点生成群组密钥后以“盲方式”将群组密钥传递给各簇头结点,各簇头结点以“盲方式”将群组密钥分发给各簇内结点。

协议中非簇头卫星结点仅需要与其邻近的一颗同轨道卫星通信,这样只需要非簇头卫星在轨

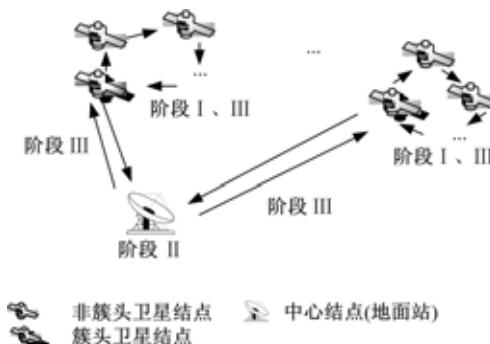


图1 协议的三个阶段

Fig. 1 Three stages of protocol

道中维持轨道内的相邻星间链路即可。而只占卫星总数小部分的簇头卫星则还需与地面站保持联系。总体而言,在协议执行中降低了维持星间链路、星地链路过程中卫星天线跟踪、定位的开销。

1.3 簇内阶段

(1)中心结点选择随机数 $r \in \{0,1\}^k$,并用其私钥对 r 签名得到签名值 δ ,发送 $r|\delta$ 给所有的簇头结点。注意随机值 r 用于标识协议会话,对 r 值的检查能够防止重放攻击。下面对协议的描述略去了每个步骤对 r 值的检查。

(2)假定一个簇中的所有结点按照在轨道内的位置依次为 U_1, U_2, \dots, U_m ,其中 U_1 为簇头。 U_1 收到中心结点发来的消息 $r|\delta$ 后,验证签名 δ 的正确性;若验证通过, U_1 设置 $E_1 = g$, GL_1 为空,用其私钥对 $r|E_1|GL_1$ 签名得到签名值 δ_1 ,并发送 $r|\delta_1|E_1|GL_1$ 给 U_2 。

(3)对于 $i = 2, \dots, m$,每个 U_i 依次执行下列步骤:收到来自 U_{i-1} 的消息 $r|\delta_{i-1}|E_{i-1}|GL_{i-1}$ 后,验证签名 δ_{i-1} 的正确性;若验证通过, U_i 选取随机值 $x_i \in \{0,1\}^k$,计算 $G_i = g^{x_i}$, $E_i = E_{i-1}^{x_i}$, $GL_i = GL_{i-1} | G_i$,用其私钥对 $r|E_i|GL_i$ 签名得到签名值 δ_i ,并发送 $r|\delta_i|E_i|GL_i$ 给结点 U_{i+1} 。该步骤中, U_m 的消息发送给簇头 U_1 。

(4) U_1 收到来自 U_m 的消息 $r|\delta_m|E_m|GL_m$ 后,验证签名 δ_m 的正确性;若验证通过, U_1 选择随机值 $x_1 \in \{0,1\}^k$,并计算簇内临时密钥为 $Intra-K = (E_m)^{x_1} = g^{x_1 x_2 \dots x_m}$,同时记录 GL_m 的值,即, G_2, \dots, G_m 。

1.4 簇间阶段

生成了簇内临时密钥的簇头结点进入簇间阶段,假定群组中共有 n 个簇,依次标记各簇头结点分别为 $U_{H1}, U_{H2}, \dots, U_{Hn}$ 。 U_{Hi} 持有的簇内临时密钥记为 $Intra-K_i$ 。

(1)对于 $i=1,2,\dots,n$,每个 U_{Hi} 计算 $g^{Inter-K_i}$,用其私钥对 $r|g^{Inter-K_i}$ 签名得到 δ_{Hi} ,并发送 $r|g^{Inter-K_i}|\delta_{Hi}$ 给中心结点。

(2)中心结点收到所有簇头结点发来的消息后,验证每个消息的签名值;若验证均通过,中心结点选择随机值 $K_r \in \{0,1\}^k$,计算 $FGK = H(g^{Inter-K_1} | g^{Inter-K_2} | \dots | g^{Inter-K_n} | K_r)$ 。对于 $i=1,2,\dots,n$,中心结点为每个 U_{Hi} 计算 $FGK_i = FGK \oplus (g^{Inter-K_i})^{K_r}$,用其私钥对消息签名得到 δ_{Gi} ,并发送 $r|g^{K_r}|FGK_i|\delta_{Gi}$ 给 U_{Hi} 。

(3)对于 $i=1,2,\dots,n$, U_{Hi} 在收到来自中心结点的消息后,验证签名的正确性;若验证通过, U_{Hi} 计算 $FGK = FGK_i \oplus (g^{K_r})^{Inter-K_i}$ 。

1.5 密钥分发阶段

密钥分发阶段在每个簇中独立执行,其作用是将生成密钥的材料分发给簇内各结点,使各结点能够生成最终的群组密钥。该阶段的描述中延续描述簇内阶段时使用的记号和参数。

(1)对于 $i=2,\dots,m$,簇头 U_1 计算 $GK_i = (G_i)^{FGK}$,用其私钥对 $r|GK_1|GK_2|\dots|GK_m$ 签名得到 δ'_1 ,并发送 $r|GK_1|GK_2|\dots|GK_m|\delta'_1$ 给簇内每个结点。

(2)对于 $i=2,\dots,m$,每个 U_i 收到 U_1 的消息后验证签名值的正确性,若验证通过,计算 $g^{FGK} = (GK_i)^{-1}_{x_i}$ 。群组密钥 GK 为 $GK = g^{FGK}$ 。

2 协议分析

2.1 安全性分析

群组密钥交换协议的语义安全性要求:群组外部攻击者即使能够捕获协议执行中所有的通信消息,也无法区分密钥值和密钥空间上的随机值。协议的安全性需要协议的三个阶段分别的安全性保证。安全性证明通过以下三个定理给出。

定理1 在簇内阶段,外部攻击者无法区分簇内临时密钥和簇内临时密钥空间上的随机值。

证明:簇内临时密钥为 $Intra-K = (E_n)^{x_1}$,其中 x_1 由簇头随机选择且从未公开,所以对外部攻击者而言,簇内临时密钥和簇内临时密钥空间上的随机值无法分辨。

定理2 在簇间阶段,外部攻击者无法区分 FGK 和 FGK 取值空间上的随机值。

证明:由于 $FGK = H(g^{Inter-K_1} | g^{Inter-K_2} | \dots | g^{Inter-K_n} | K_r)$,其中 K_r 为群组中心结点随机选取且从未公开,且 $Intra-K_1, Intra-K_2, \dots, Intra-K_n$

分别为各簇的簇内临时密钥。根据定理1,外部攻击者无法区分各簇的簇内临时密钥和随机值,同时,由于哈希函数 H 的抗碰撞性,外部攻击者无法区分 FGK 和 FGK 取值空间上的随机值。另一方面,也正是因为外部攻击者无法分辨 $Intra-K_i$ 和随机值, $FGK_i = FGK \oplus (g^{Inter-K_i})^{K_r}$ 的计算和传输也不能给外部攻击者在分辨 FGK 和随机值上提供任何帮助。

定理3 在密钥分发阶段,外部攻击者无法区分群组密钥 GK 和 GK 取值空间上的随机值。

证明:在密钥分发阶段,对于 $i=2,\dots,m$,外部攻击者能够收集的有关 $GK = g^{FGK} = (GK_i)^{-1}_{x_i}$ 的计算的信息仅有 $GK_i = (G_i)^{FGK}$ 和 $G_i = g^{x_i}$,如果攻击者能够从这些信息中分辨 GK 和 GK 取值空间上的随机值,则攻击者解决了Divisible-DDH问题^[9],这与Divisible-DDH假设^[9]相矛盾。

综合以上三个定理,本文群组密钥交换协议满足语义安全性。

2.2 通信效率分析

本协议充分考虑了空间信息网的组网特点,在空间信息网中具有较高的通信效率。表1为不同群组密钥交换协议完整执行一次所需的通信次数。在对比中假定空间信息网中共有 n 个卫星轨道面,每个轨道面有 m 颗卫星。由于空间信息网的结点间距大,传输延迟可达毫秒级,故协议所需的通信次数很好地反映了协议通信效率的高低。

表1 SIN 场景中各 GKE 协议的通信效率比较

Table 1 Comparison among GKE protocols in SIN scenario

群组密钥交换协议	所需通信次数
ACEKA ^[3]	$7mn - 6 - n$
R. Dutta 的协议 ^[4]	$4mn - n + 1$
Kim 的协议 ^[5]	$3mn$
本文协议	$2mn$

从表1中可看出,在空间信息网中应用时,本文协议所需要的通信次数和网络规模有关,并且与经典 GKE 协议相比,本文协议所需要的通信次数最少,具有很高的通信效率。

3 仿真结果

为进一步验证本文协议在空间信息网中的效率,使用 NS2 网络仿真软件(版本:2.30)将本文协议与 ACEKA^[3]、R. Dutta 的协议^[4]及 Kim 的协议^[5]在性能上进行仿真比较,并对密钥建立所需时间进行评估。

在仿真场景中,假定每根卫星轨道等距离均匀分布6颗卫星,为说明仿真结果的有效性,仿真实验中通过逐渐增加卫星轨道实现网络规模的逐渐增大,并在不同网络规模下分析密钥交换协议的效率。仿真参数的取值如下:卫星数/轨道为6;卫星高度为1400 km;轨道倾角为86°;轨道类型为极轨道。

图2对比了不同网络规模情况下四种GKE协议建立密钥所需的时间。由图2可知,在不同网络规模下,本文协议建立一个密钥所需的时间比另三个协议均较少;另一方面,随着网络规模增大,本文协议建立密钥所需时间的增长率比其他三个协议更小,保持了较高的通信效率,完全可以达到空间信息网对密钥交换协议的要求。

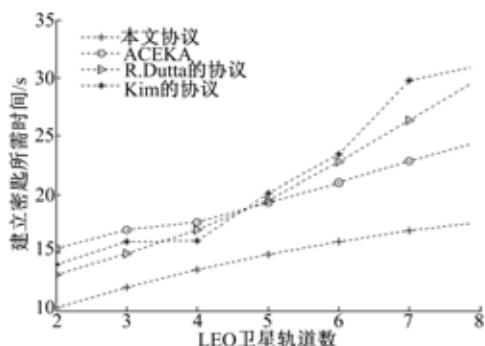


图2 不同GKE协议建立密钥所需的时间对比

Fig. 2 Comparison of time required to establish session key for different GKE protocols

4 结束语

根据空间信息网结点距离远、通信延时大及空间信息网中卫星根据轨道分布的特点,提出一个基于轨道分簇的群组密钥交换协议。协议中密钥的建立分为三个阶段:簇内阶段、簇间阶段和密钥分发阶段。每个结点均对密钥有贡献值,密钥交换过程通过加入盲因子的方式保证安全性。安全性分析表明,协议具有针对外部攻击者的语义安全性。通信效率的理论分析和仿真实验均表明:与其他协议相比,本文协议在空间信息网中应用时具有最高的通信效率。

参考文献:

- [1] 刘小跃,马建峰,钟焰涛,等. 空间信息网安全组网新架构[J]. 网络安全技术与应用, 2009, 6(6):13-15.
- [2] Liu Xiao-yue, Ma Jian-feng, Zhong Yan-tao, et al. New construction for secure networking of space information networks[J]. Network Security Technology and Application, 2009, 6(6):13-15.
- [3] 王宇,卢均,吴忠望,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.
- [4] Wang Yu, Lu Jun, Wu Zhong-wang, et al. Constructing multi-level and multi-layer security infrastructure of space information system[J]. Journal of Astronautics, 2007, 28(5): 1081-1085.
- [5] Shi H, He M, Qin Z. Authenticated and communication efficient group key agreement for clustered ad hoc networks[C]// Proceedings of Chinese-American Networking Symposium, Chicago, USA, 2006: 73-89.
- [6] Dutta R, Barua R, Sarkar P. Provably secure authenticated tree based group key agreement[C]// Proceedings of the 6th International Conference on Information and Communications Security, Malaga, Spain, 2004: 92-104.
- [7] Kim S, Ahn T, Oh H. An efficient hierarchical group key management protocol for a ubiquitous computing environment[C]// Proceedings of Computational Science and Its Applications, Glasgow, UK: Springer, 2006: 388-395.
- [8] 王宇,卢均,吴忠望. 空间信息网络的组密钥管理[J]. 宇航学报, 2006, 27 (3):553-555.
- [9] Wang Yu, Lu Jun, Wu Zhong-wang. Multicast key management of space information network[J]. Journal of Astronautics, 2006, 27(3): 553-555.
- [10] 冯涛,马建峰. UC安全的移动卫星通信系统认证密钥交换协议[J]. 宇航学报, 2008, 29(6):1959-1964.
- [11] Feng Tao, Ma Jian-feng. The universally composable security authentication and key exchange protocol for mobile satellite communication systems[J]. Journal of Astronautics, 2008, 29(6):1959-1964.
- [12] Wang K, Zhao Z W, Yao L. An agile reconfigurable key distribution scheme in space information network[C]// Proceedings of Second IEEE Conference on Industrial Electronics and Applications, Harbin, China, 2007:2742-2747.
- [13] Bao F, Deng R H, Zhu H. Variations of Diffie-Hellman problem[C]// Proceedings of the 5th Conference on Information and Communications Security, Huhehaote, China, 2003:301-312.