Computer Science and Application 计算机科学与应用, 2018, 8(6), 1027-1033
Published Online June 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.86114

Hans汉斯

The Design and Analysis of Key Agreement Protocol in Space Information Network

Kelin Hao, Xiaokai Liu, Chao Wang, Shan Zhang

National Computer System Engineering Research Institute of China, Beijing
Email: 1486010567@qq.com

Received: Jun. 7th, 2018; accepted: Jun. 22nd 2018; published: Jun. 29th, 2018

Abstract

In order to meet the security and efficient communication requirements of nodes in space information network, a scheme of key agreement between nodes based on combined public key is proposed. The ground control center first completes the generation of the combination key based on identity and distributes it to the space nodes through a secure channel. When communication between different nodes is needed, after the two-way authentication is carried out, the two party nodes' session key is calculated by using their three secret values and the trusted public key information of the other nodes. The security properties of the protocol are analyzed, and compare the protocol and related protocols existing in the two aspects of security and performance. The comparison results show that this protocol not only has improved in terms of safety, and has higher computational efficiency.

Keywords

Space Information Network, Combined Public Key, Authentication, Agreement

空间网络中密钥协商协议的设计与分析

郝克林，刘笑凯，王　超，张　姗

华北计算机系统工程研究所，北京
Email: 1486010567@qq.com

收稿日期：2018年6月7日；录用日期：2018年6月22日；发布日期：2018年6月29日

摘　要

针对空间信息网络中节点间安全高效通信需求，本文利用组合公钥思想设计了一个节点间密钥协商协议。地面控制中心首先完成基于身份的组合密钥的生成，并通过安全通道分发至各空间节点。当各空间节点

文章引用: 郝克林, 刘笑凯, 王超, 张姗. 空间网络中密钥协商协议的设计与分析[J]. 计算机科学与应用, 2018, 8(6): 1027-1033. DOI: 10.12677/csa.2018.86114

间需要通信时，在进行双向身份认证后，利用本身的三个秘密值与对方节点的可信公钥信息计算得出两方节点的会话密钥。文章详细分析了协议自身的安全特性，并将协议和现有的相关协议在安全和性能两个方面进行比较。比较结果表明，本文设计的协议不仅在安全性方面有所提升，且具有更高的计算效率。

关键词

空间网络，组合公钥，认证，密钥协商

1. 引言

空间网络通信应用系统由具有空间通信能力的卫星节点、近地节点、地面通信系统及应用系统组成，是以在轨工作卫星组成的卫星星座作为主要转发节点的天、空、地一体化的网络系统[1]。我国目前空间信息领域的发展迅速，实现了空间系统自主安全运行的互联互通的星间链路，星地链路已经成为空间通信的发展趋势。

但是由于空间链路的开放性特征，节点之间进行通信时会遇到身份确认问题，例如，合法节点也许会遇到恶意节点假冒身份与其进行通信，并遭到其对自身信息的篡改、删除或窃取[2]。基于身份认证技术能判断出网络系统中的非法节点，确保通信数据均来自于合法的节点。这些年来，国内外学者已经提出多种多样的应用于空间网络的密钥协商方案，但早些年设计的密钥协商方案的安全性能并不完善，文献[3]设计的互相认证密钥协商方案，不能抵抗模仿攻击；文献[4]提出的方案不满足完美前向安全性，且使用的哈希方法效率很低；文献[5]提出的方案没有明确的密钥确认，用户无法验证其收到的密钥是否是对方生成的。

此外，空间网络拓扑结构呈现异构化、分层多域的特点，且节点系统计算，存储，能量资源有限，密钥协商协议要尽量减少传输花费及计算时间。针对以上空间网络系统中安全通信的特殊要求，本文提出了一个新的基于组合公钥的节点间认证密钥协商协议，首先对空间系统拓扑结构及协议的流程进行了详细的描述，随后分析了协议具有的安全特性，最后在安全性、传输花费和计算效率三个方面将新协议与已有的协议进行了比较与分析。

2. 认证密钥协商协议

2.1. 系统结构

空间网络通信系统拓扑结构如图 1 所示，由各类卫星节点，空中节点，和地面各类节点组成，能够完成空、天、地一体化通信网络贯通[7]。卫星作为其关键通信节点，通过星间链路与空间节点互相联系，利用星地通道与地面基站、近空节点、海上节点等有机结合，进行各类信息的接收、处理和传输[8]。

本系统包含一个公私钥对的计算与生成方案设计和密钥协商协议的设计。方案由地面控制中心[9]为各节点计算公钥和对应私钥，并在应用部署之前通过安全通道分发到位。当各类节点在空间网络中完成基础通信链路的搭建后，需要进行业务安全通信传输时，节点双方通过根据协议流程，协商产生本次通信使用的会话密钥[10]。

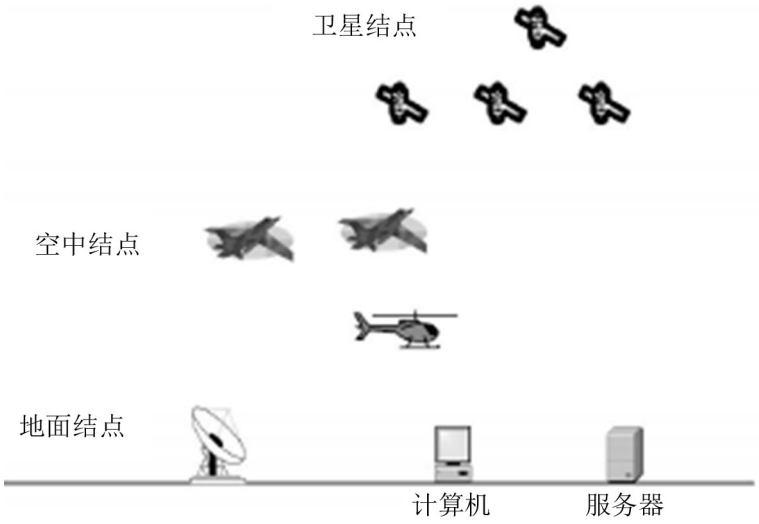

Figure 1. The topology of the space network system
图 1. 空间网络系统拓扑结构图

2.2. 系统初始化

地面控制中心作为整个系统，首先选择固定参数 $k(k>0)$，利用组合公钥的思想按照如下步骤生成系统初始化参数并向各节点公开：

1) 生成一个 k 比特的素数 p，选择阶为 q 的有限域 F_p。在 F_p 上选择两个数 $a,b\in F_p$，满足 $4a^3+27b^2\neq 0 \bmod p$，以 a,b 为参数，生成椭圆曲线：$E(a,b): y^2\equiv x^3+ax+b \bmod p$。

2) 在 $E(a,b)$ 上选择一个阶为素数 n 的基点 P，根据相应算法随机选取 $x_{ij}\in GF(p)$，其中 $1\le i\le m, 1\le j\le n, m\in Z^+, n\in Z^+$。构造 $m\times n$ 的私钥种子矩阵 X_{PR},有

$$X_{PR}=\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \tag{1}$$

根据已得到的 X_{PR} 生成对应的公钥种子矩阵 Y_{PR}，$y_{ij}=x_{ij}P$，$1\le i\le m, 1\le j\le n$，能够得出

$$Y_{PR}=\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & & \vdots \\ y_{m1} & y_{m2} & \cdots & y_{mn} \end{bmatrix} \tag{2}$$

3) 选择两个单向哈希数 $H_1:\{0,1\}^*\to Z_n^*; H_2:\{0,1\}^*\to Z_p^*$，完成系统初始化，向所有节点成员公开参数 $\{E(a,b), X_{PR}, Y_{Pk}, P, H_1, H_2\}$。

2.3 密钥种子对的生成

现在，系统根据每个节点设备的用途及型号为他们确认唯一的 ID 号 $ID\in\{0,1\}^*$，同时创建 ID 链表来存储它们的 ID 信息，并根据节点 ID 按照下列步骤生成节点种子密钥对。

1) 根据公式 $H_1(ID)=h_1\cdots h_i\cdots h_n$，计算出节点的散列值，$h_i$ 是长度为 1 的二进制比特串，转化成十进制数为 a_i，容易知道 $i\in[l,n], a_i\in[0,m)$。

2) 从 2.2 中的 X_{PR} 矩阵中选出节点私钥种子 $SeedX_{ID}=\{x_{a_1,1},\cdots,x_{a_i,i},\cdots,x_{a_n,n}\}$，其中 $x_{a_i,i}$ 为私钥种子矩阵 X_{PR} 中第 a_i 行，第 i 列对应的值。

3) 从 2.2 节中的 Y_{PR} 中选取公钥种子 $SeedY_{ID}=\{y_{a_1,1},\cdots,y_{a_i,i},\cdots,y_{a_n,n}\}$，其中 $y_{a_i,i}$ 为 Y_{PR} 中第 a_j 行，第 j 列对应的值。

4) 将节点的公私钥种子对 $(SeedX_{ID},SeedY_{ID})$ 存储到对应节点，同时将自己的公钥 PK_{BS} 分发给所有的节点。

2.4. 节点密钥对的生成

1) 节点通过定位模块收集自己所在位置信息 LC_s 和当前时间 T_S，生成密钥参数 $KP_S=\{ID_S\|LC_S\|T_S\}$，其中 ID_S 是节点 S 的类型标识。

2) 计算密钥参数的散列值：$H_2(KP_S)=kp_{Si}\cdots kp_{Sj}\cdots kp_{Sn}$，其中 kp_{Si} 是 $H_2(KP_S)$ 的第 i 比特。

3) 结合节点 S 的公私钥种子对 $(SeedX_S,SeedY_S)$，计算得到节点 S 的私钥 d_S 和公钥 K_S，其中 $kp_{Si}\in H_2(d_S),x_{S_i i}\in SeedX_S,y_{s_i j}\in SeedY_S$，则有

$$d_S=\sum_{i=1}^{n}kp_{Si}x_{s_i i}\bmod p \tag{3}$$

$$K_S=\sum_{i=1}^{n}kp_{Si}y_{s_i i}\bmod p \tag{4}$$

4) 节点 S 保存自己的公私钥 (d_S,K_S)，结束密钥对生成阶段。

2.5. 密钥协商

当空间网内节点 U 和 S 需要建立通话时，完成互相认证并且协商生成一个会话密钥，设节点 U，S 的公钥，私钥分别是 (d_U,K_U)，(d_S,K_S)，协商密钥详细过程如下：

1) 节点 U 选择一个随机数 $u_1,u_2\in Z_n^*$，并且计算

$$\begin{cases}R_{u1}=u_1P,R_{u2}=u_2P\\h_1=H_1(ID_u\|R_{u1}\|R_{u2}\|T_u)\\Z_1=u_1+h_1d_u\bmod p\end{cases} \tag{5}$$

其中T_u是当前的时间戳，计算完成后，U 将 $M_1=\{ID_u,R_{u1},R_{u2},h_1,Z_1,T_u\}$ 发送给 S。

2) S 收到 M_1 后，首先验证 T_u 是否尚在有效范围内，如果 T_u 超出有效范围，S 向用户发送失败信息，停止本次协商。如果仍然有效，S 计算并验证等式 $Z_1P=R_{u1}+H_1(ID_u\|R_{u1}\|R_{u2}\|T_u)\cdot K_u$，如果验证等式正确，S 则生成随机数 $s_1,s_2\in Z_n^*$，时间戳 T_s 并计算下式，

$$\begin{cases}R_{s1}=s_1P,\ R_{s2}=s_2P\\h_2=H_2(ID_s\|R_{s1}\|R_{s2}\|T_s)\\Z_2=u_1+h_2\cdot d_s\bmod p\end{cases} \tag{6}$$

最后将 $M_2=\{R_{s1},R_{s2},h_2,Z_2,T_s\}$ 发送给用户 U。

3) 收到 M_2 后，U 验证 T_s 时间戳的值是否还在有效范围内，如果 T_s 过期，U 停止协商过程并向服务器 S 发送失败信息。如果 T_s 有效，U 验证等式 $Z_2P=R_{s1}+H_2(ID_s\|R_{s1}\|R_{s2}\|T_s)\cdot K_s$ 是否成立，若成立，U 确认与其通信的确实是 S，最后 U 计算

$$\begin{cases}K_{us}=u_1R_{s2}\\h_3=H_2(ID_u\|R_{u1}\|R_{s1}\|Z_2\|Z_1\|K_{us}\|T_s)\end{cases} \tag{7}$$

并将 $M_3=\{h_3\}$ 发送 S。

4) S 收到 M_3 后，计算 $K_{su}=s_2R_{u1}$，验证等式 $h_3=H_2\left(ID_u\|R_{u1}\|R_{s1}\|Z_2\|Z_1\|K_{su}\|T_s\right)$ 是否成立，若成立，S 确认以上信息来自一个合法节点 U。

5) U 和 S 分别计算会话密钥

$$\begin{aligned}SK_u&=H_2\left(ID_u\|ID_s\|R_{s1}\|R_{u1}\|Z_1\|Z_2\|K_{su}\|T_u\|T_s\right)\\SK_s&=H_2\left(ID_u\|ID_s\|R_{s1}\|R_{u1}\|Z_1\|Z_2\|K_{us}\|T_u\|T_s\right)\end{aligned}\tag{8}$$

容易得出，$K_{su}=u_1R_{s2}=u_1s_2P=s_2R_{u1}=K_{us}$. 因此：$SK_U=SK_s$。

所以，U 和 S 可以计算出相同的会话密钥。

3. 协议分析

3.1. 安全性分析

1) 已知会话密钥安全

会话密钥 SK_U,SK_s 的值是由一个单向哈希函数生成的，即它的值是均匀随机地分布在 $\{0,1\}^k$ 中的，因此每两个会话密钥的值之间都互不相关，也就是说当次会话的密钥值在敌人获得了一定信息后也是无法通过以前的会话密钥值推测得到。另外，会话密钥的 Z_1 和 Z_2 还各包含了一个随机数，每个随机数是临时的，每次会话都会重新生成。因此即使攻击者用某种方法获得了一些会话的秘密随机值，也不能从中推测出当前会话的随机值，从而计算得到当前的会话密钥。所以，本文协议满足已知会话密钥安全。

2) 前向安全性分析

假设 U 的私钥 d_u 和 S 的私钥 d_s 都被泄露，且攻击者截获了 U 与 S 之间传递的部分消息，从中获得了 ID_u,R_{u1},R_{u2} 和 R_{s1},R_{s2}，但是根据 ECDLP 问题，敌手并不能从 R_u 和 R_s 中计算得到 r_s 和 r_u，敌手就无法计算得到 $Z_1=u_1+h_1d_u \bmod p$，也不能直接计算出 $Z_2=u_1+h_2\cdot d_s \bmod p$。由 CDH 问题可知，敌手也不能从 $R_{u1}=r_{u1}P$ 和 $R_{s1}=r_{s1}P$ 中推测出 Z_2 的值。因此，假如 U 和 S 泄露了自身的私钥，先前通信使用的会话密钥的值也无法通过它们计算得到，所以该协议满足完美前向安全。

3) 密钥泄露模仿攻击

假设一个攻击者已获得 U 的私钥，那么它就可以成功的在会话中模仿 U，但他仍然不能模仿其他用户。因为要想成功地模仿另一个用户 U′，它就需向服务器发送正确的消息 $\{ID_u,R_{u1},R_{u2},h_1,Z_1,T_u\}$，其中的 $Z_1=u_1+H_1\left(ID_u\oplus R_{u2}\right)\cdot d_u$，要想发送的消息被验证成功，就需要知道 d_u,u_1 的值。根据 ECDLP 问题，仅根据 $R_{u1}=u_1\cdot P$，不能计算得到 u_1 的值，更无法计算出 d_u 的值，因此攻击者不能成功地模仿用户 U′。综上所述，本文协议满足无密钥泄露模仿攻击。

4) 未知密钥共享安全

在本文协议中，通信双方自身的身份信息都包含在他们之间传送的每条信息里，且都是用对方的公钥和身份信息对传输数据进行加密。如果第三方攻击者想对数据进行解密，攻击者必须知道通信双方的私钥，然而私钥只有真实的双方才知道。因此，本文协议具有未知密钥共享安全。

5) 非密钥控制

因为在会话密钥的协商设计计算中，使用的散列函数中不仅有通信双方的身份信息，还有用户自己每次产生的随机数，通过这些计算，产生的会话密钥都不是提前确定的值，具有单次不确定性。所以满足非密钥控制安全性。

6) 防重放攻击

在新协议中，节点间传送的每条信息中都带有时间戳，因此敌手不能通过重放攻击来获取合法的回应消息。

3.2. 性能分析

1) 安全性比较

通过对本文协议和前面提到的几个已有协议进行 3.1 章节的各类安全性分析，并对几个协议的分析结果进行了详细的比较，结果如表 1 所示。从表中的分析结果可看出，本文协议比其他协议能够抵抗更多的已有攻击，具有更高的安全性。

2) 传输花费比较

在两方通信过程中，传输消息的大小直接影响到传送的速度，消息越小，传输所花费的时间越小。比较本文设计协议与已有其他协议的传输花费消耗。此处我们做一个假设，协议中用到的椭圆曲线 $E(a,b)$ 的阶 q 为 256 比特的大素数，用户身份标识是 160 比特，hash 函数的大小是 256 比特，T_u 的长度是 16 比特。

在新协议的密钥协商阶段中，U 与 S 之间一共传输了三条信息，分别是 $\{ID_u, R_{u1}, R_{u2}, h_1, Z_1, T_u\}$，$\{R_{s1}, R_{s2}, h_2, Z_2, T_s\}$，$\{h_3\}$。其中 ID_u 是 U 的身份标识，长度是 160 比特，R_u 和 R_s 是随机数与 $E(a,b)$ 上一个点点乘结果，长度为 256 比特，h_1，h_2 和 h_3 是散列函数的输出结果，大小为 256 比特，T_u 和 T_s 是时间戳，大小为 16 比特。因此，新协议在密钥协商阶段的传输花费为 1168 比特。使用相同的方法计算出其他协议的传输花费，将四个已有协议的传输花费与本文的协议做比较，计算结果如表 2 所示。

从上表结果可以得出，本文协议的传输花费比文献[5]和文献[6]的协议小，这说明本文协议不仅在安全方面有所提升，且降低了传输花费。而文献[3]，文献[4]的传输花费较小，这是因为在他们的协议中，通信双方只传送了两条信息，然后双方计算会话密钥，没有多余的消息做密钥确认，所以不是一个严格安全的协议。

3) 计算效率比较

我们将本文协议与其他几个协议在计算效率方面做详细规范的比较。主要计算协商过程中，各步过

Table 1. Comparison of protocol security
表 1. 协议安全性比较

协议	密钥确认	抗模仿攻击	抗 KCI 攻击	前向安全
文献[3]	×	×	√	√
文献[4]	×	√	√	×
文献[5]	√	×	×	√
文献[6]	√	×	√	√
本文	√	√	√	√

Table 2. Cost comparison of protocol calculation
表 2. 协议计算花费比较

协议	传输花费	计算花费	
		U	S
文献[3]	1216 比特	4P + 2A + 4H	4P + 2A + H + 3h
文献[4]	1216 比特	3P + 2A + 5H	3P + 2A + H + 5h
文献[5]	1472 比特	3P + 3H	3P + 5H
文献[6]	1472 比特	3P + 4H	3P + 6H
本文	1168 比特	3P + 4H	3P + 5H

程中的计算复杂度和时间花费数，通过数字反映出协议的效率。为了简化分析，用下列符号来替换运算所需的时间。主要考虑以下几种运算时间：P：椭圆曲线加法群上的点乘运算时间 A：椭圆曲线上点加运算，H：哈希函数，h：单项哈希函数，M：MAC 函数。

密钥协商阶段，U 在第一步计算中包括两次点乘，一次散列函数运算，第三步计算中包括一次点乘和两次哈希运算，计算得出会话密钥时包括一次哈希运算，因此，U 花费时间为 3P + 4H；S 端在第二步计算包括三次点乘，和三次哈希，在第四步计算包括一次散列函数运算，最后计算会话密钥有一次哈希，所以，S 花费的时间为 3P + 5H。相同方法，计算其他几个协议花费的时间如表 2 所示。

由表 2 可以看出，本方案除了文献[5]，本文设计协议的计算耗费最小。但是文献[3]的协议不能抵抗用户模仿和 KCI 攻击；因此本文设计的协议不仅提高了安全特性，还降低了计算花费。

4. 结论

本文通过对空间网络结构的研究分析，针对其节点间安全高效传输的安全性要求，设计了一个两方认证密钥协商协议，并对协议的安全特性进行了一定的分析，证明了新协议的安全特性。并从安全性、传输花费，计算效率三个方面将协议与相关领域已有的其他四个协议进行了分析和比较。比较分析结果表明，本文提出的协议在空间网络通信协商方案中，对系统安全性进行了有效的保证，且一定程度上提高了计算效率，减小了传输花费。

参考文献

[1] 徐军华, 樊宏, 郝云芳. 安全高效的空间信息网中密钥管理方案[J]. 现代电子技术, 2011, 34(7): 81-84.

[2] 冯登国. 密码学原理与实践[M]. 北京: 电子工业出版社, 2016.

[3] Yang, J.H. and Chang, C.C. (2009) An ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem. *Computers & Security*, **28**, 138-143. https://doi.org/10.1016/j.cose.2008.11.008

[4] Yoon, E.J. and Yoo, K.Y. (2009) Robust Id-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC. 2009 *IEEE International Conference on Computational Science and Engineering* (*CSE*'09), Vancouver, BC, 29-31 August 2009, Vol. 2, 633-640. https://doi.org/10.1109/CSE.2009.363

[5] Chou, C.H., Tsai, K.Y. and Lu, C.R. (2013) Two ID-Based Authenticated Schemes with Key Agreement for Mobile Environments. *The Journal of Supercomputing*, **66**, 973-988. https://doi.org/10.1007/s11227-013-0962-3

[6] Farash, M.S. and Attari, M.A. (2014) A Secure and Efficient Identity-Based Authenticated Key Exchange Protocol for Mobile Client-Server Networks. *The Journal of Supercomputing*, **69**, 395-411. https://doi.org/10.1007/s11227-014-1170-5

[7] 周星, 刘军, 董春冻, 等. 基于身份的卫星网络密钥管理方案[J]. 计算机技术与发展, 2013, 23(11): 148-151.

[8] 刘毅. 基于椭圆曲线的无线传感器网络密钥管理方案的研究[D]: [硕士学位论文]. 北京: 北京邮电大学, 2014.

[9] 宋宁宁, 刘蕴络, 姚倩燕, 等. 基于隐秘映射组合公钥的云计算密钥管理方案[J]. 计算机应用研究, 2013, 30(9): 2759-2762.

[10] 赵秀凤. 认证及密钥协商协议设计与分析[D]: [博士学位论文]. 济南: 山东大学, 2012.