改进的LEO卫星网络密钥管理协议

潘艳辉 王 韬 赵新杰 李 华
(军械工程学院计算机工程系 石家庄 050003)

摘 要 卫星网络密钥管理协议是实现网络节点间安全通信的前提。在分析卫星网络密钥管理协议特性的基础上,提出了分布式与集中式相结合的LEO卫星网络密钥建立方案,改进了密钥管理协议的分簇方式和密钥更新方法,并进行了分析和验证。该方法进一步增强了安全性,同时提高了密钥更新速度。

关键词 低轨道卫星网络,椭圆曲线密码,密钥管理,网络安全
中图法分类号 TP309 **文献标识码** A

Improved Key Management Protocol for LEO Satellite Network

PAN Yan-hui WANG Tao ZHAO Xin-jie LI Hua
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract Key management protocol is the base of secure communications between satellite network nodes. Character of key management protocol in the terms of satellite network environment was analyzed. A distributed key establishment scheme combined with centralized one was proposed for LEO satellite network. Then, an improved key management protocol was given with new clustered rekeying mathod. At the end, it was analyzed and checked. The result indicates that it could help to tighten security with shorter key updating period.

Keywords LEO satellite network, ECC, Key management, Network security

1 引言

针对卫星网络面临的安全威胁以及安全目标,目前在卫星网络安全问题上展开的研究主要有协议和加密机制的研究,其中加密机制是基础。密码学发展至今已形成了许多安全性很高的加解密算法。一般认为,在目前的技术水平下采用160~200位的椭圆曲线密码算法,其安全性已足够高,而160位长的椭圆曲线密码的安全性相当于1024位的RSA密码。由于椭圆曲线密码的密钥位数短,在硬件实现中电路的规模小、省电,因此,它特别适合在航空、航天、卫星及智能卡中应用[1]。

椭圆曲线密码能够用于保证消息的保密性。然而,在卫星网络通信环境中,还必须保证消息的完整性、真实性以及通信效率,这需要一套密钥管理机制来为卫星网络通信提供消息加密、认证以及密钥分配与更新功能。在相同安全强度要求下,椭圆曲线密码体制具有密钥长度短、算法速度快、占用内存少和抗攻击能力强等优点。文献[2,3]以椭圆曲线密码体制为基础,提出了适用于无线传感器网络(Wireless Sensor Network, WSN)的密钥管理协议。WSN是一种特殊的MANAT网络。文献[4]提出了借用MANAT网络的成果研究卫星网络的方法,由于卫星网络自身的特点,使得该协议无法直接满足卫星网络的安全性需求。为此,本文根据卫星网络的特点设计一种基于ECC、适用于卫星网络的密钥管理协议。

2 卫星网络与ECC椭圆曲线密码

2.1 卫星网络密钥管理协议特性分析

卫星网络具有节点暴露、广播时延长、可用带宽低、节点计算能力有限、误码率高等特点,相对于传统网络,卫星网络对密钥管理协议的要求更加严格。主要表现在以下几个方面:

(1)卫星网络节点布置在公开的空间环境中,卫星网络与地面网络相比更易受攻击和干扰,因此密钥管理协议应具有较高的安全性、可靠性和较好的抗DoS攻击能力;

(2)卫星网络的广播特性使得数据在网络传播过程中更容易遭受截获,因此应提高协议信息的保密性,降低对截获数据进行正确解密的可能性;

(3)卫星网络的传输时延较长,为了保证系统的运行效率,应尽量减少协议交互消息的传输,避免与第三方的实时交互;

(4)星上计算能力与存储资源有限,要求加解密算法对卫星节点计算与存储资源的需求较少;

(5)算法尽量采用非对称密钥体制,可在空间节点中预先注入私钥,认证时交换并验证公钥证书,在实现离线认证的同时提高系统的可靠性[5]。

2.2 椭圆曲线密码理论

根据卫星网络的特点及其对加解密算法的要求,如前所

到稿日期:2010-08-11 返修日期:2010-12-06 本文受国家自然科学基金项目(60772082)资助。
潘艳辉(1982-),女,博士生,主要研究方向为卫星网络路由,E-mail:yanhuipan@126.com。

述椭圆曲线密码是目前最符合卫星网络要求的加密算法。其优势是在安全强度相同的情况下，ECC 算法所需的密钥长度更短、算法速度更快、存储空间更小、效率更高，却没有减少密码分析的工作量[6]。以下对其作简要介绍。

椭圆曲线密码是建立在有限域内由椭圆曲线上的一些点构成的交换群，离线对数问题是难解的。定义在 $GF(p)$ 上的椭圆曲线，设 p 是大于 3 的素数，且 $4a^3+27b^2\neq 0 \bmod p$，称曲线

$$y^2=x^3+ax+b, a,b\in GF(p) \tag{1}$$

为 $GF(p)$ 上的椭圆曲线[7]。相应地，一个椭圆曲线密码由下面的六元组描述：

$$T=\langle p,a,b,G,n,h\rangle \tag{2}$$

式中，n 为生成元 G 的阶，G 和 n 确定了循环子群 E_1；$h=|E|/n$，称为余因子，它将交换群 E 和循环子群联系起来。

用户的私钥定义为一个随机数 d：

$$d\in\{1,2,\cdots,n-1\} \tag{3}$$

用户的公钥定义为 Q 点：

$$Q=dG \tag{4}$$

3 LEO 卫星网络密钥管理协议

现有的卫星网络管理协议[8]依赖于地面认证中心(CA)，属于集中式管理方式，由地面测控站依次对每颗卫星进行密钥更新，容易遭受单点失效、DoS 攻击，且容易造成网络拥塞和服务的延迟。文献[9]的优点是提出了基于卫星运行轨道进行分簇的思想，降低了解决问题的规模，提高了处理效率，但仅就密钥更新算法进行了描述。文献[10]克服了依赖于地面认证的缺点，提出了分布式密钥管理协议，但该方案通过簇内每个节点依次计算并向下一个节点传递公钥份额的方式，增加了密钥建立时间。现有卫星网络密钥管理方案存在的共同缺点是建立在网络节点数固定、拓扑规则性前提假设基础之上的。但实际运行中可能会出现特殊情况，如卫星变轨机动、应急发射以及因自身原因或受到外界的干扰和攻击发生故障，都会造成网络拓扑出现无法预料的变化，特别是未来微小卫星的广泛应用更会造成组网节点数目的频繁增减[11]。在此基础上，本文从两个方面进行了改进，提出了运用 ECC 的半分布式 LEO 卫星网络密钥管理协议。本协议由 4 部分组成：初始化、密钥建立、密钥更新、会话密钥协商，其中密钥建立分为簇内密钥 KC 和簇首密钥 KH 的建立两种情况。KC 用于簇内成员共享，对交互消息进行加、解密；KH 用于簇首之间对交互消息进行加、解密。

3.1 初始化

按照文献[12]中的簇划分方法对卫星网络进行分簇，将节点数为 N 的网络划分为 d 个簇，用 $C(i,N_i,H_j)$ 表示第 i 个簇，其节点数为 N_i，簇首节点为 H_j，且 $i\in[1,d]$，$j\in[1,N]$，$N_1+N_2+\cdots+N_d=N$。

3.2 分布式簇间密钥建立

各簇首节点在 $Zr*$ 内随机选择自己的 ECC 私钥 S_i，由私钥生成簇间公钥份额 M_i。根据网络划分的簇数共需进行 d 步操作，把各簇首节点公钥份额组合成簇间公钥，并为各簇首节点生成密钥参数 C，运用文献[10]的方法进行计算，如式(5)和式(6)所示：

$$M_i=S_i*M_{i-1}=\prod_{t=1}^{i}S_tP \tag{5}$$

$$C_{i,k}=\begin{cases}M_{i-1}, k=i\\ S_i*C_{i-1,1\leqslant k\leqslant i}\end{cases}=\prod_{t=1}^{i}S_k^{-1}S_tP, \forall k\in[1,i] \tag{6}$$

区别在最后一步：最后一个簇首节点计算簇间公钥后，为各簇首节点计算其密钥参数，并向各簇首节点广播。

3.3 集中式簇内密钥建立

与地面 CA 方式不同，集中式簇内密钥建立方法用簇首节点存储簇内节点的公钥，实现集中式管理。由于选用 ECC 的密钥方案其密钥位较短，对有限的星上存储空间来说是可行的，其密钥建立过程分为以下 4 步：

第 1 步　$\forall V_i, i\in[1,N]$ 根据其私钥 S_i 计算其公钥 $P_i=S_i*G$；

第 2 步　$\forall H_j\rightarrow V_i, V_i\in C(i,N_i,H_j)$：$H_j$ 的公钥 P_H 和标识 ID；

第 3 步　$\forall V_i\rightarrow H_j, V_i\in C(i,N_i,H_j)$：$E(P_i,P_H)$ 和标识 ID；

第 4 步　$\forall H_j$ 执行 $D(P_i,P_H)$ 获得 V_i 的 P_i，并将其添加到密钥列表中存储，且有 $V_i\in C(i,N_i,H_j)$。

3.4 会话密钥协商

(1)簇间会话密钥

建立密钥协议后，各簇首节点得到其他节点的密钥参数，即可计算出两个簇首之间的会话密钥。

(2)簇内会话密钥

根据椭圆曲线的密钥交换协议[7]可知，$\forall V_i, V_j\in C(i,N_i,H_j), i,j\in[1,N]$，有 $P_i=S_i*G, P_j=S_j*G$。V_i, V_j 的会话密钥各为 $K=S_i*P_j$，$K=S_j*P_i$，而 $S_i*P_j=S_i*(S_j*G)=S_j*(S_i*G)=S_j*P_i$；$K$ 是椭圆曲线上的点。

3.5 密钥更新

密钥更新分为 3 种情况：周期性更新、簇首节点更新、簇内节点更新。以下分别进行描述。

(1) 周期性更新

对于周期性更新，虽然可以通过重新执行密钥建立协议来完成，但其网络运行过程中易遭受中间人攻击，因此本文对密钥更新方法进行了改进。在当前周期的末尾通过该周期的会话密钥传递下一周期的新密钥信息，实现密钥更新。密钥更新分为簇首密钥更新和簇内密钥更新两种情况，以下分别进行简述。

1) 簇首节点密钥更新的具体方法

第 1 步　簇首发起节点 H_1 按照式(5)和式(6)计算 M_1'，$C_{1,1}'$，执行 $H_1\rightarrow H_2$：$E(M_1', K_{12})$；

第 2 步　由于 $K_{12}=K_{21}$ 是 H_1 和 H_2 之间的会话密钥，故 H_2 执行 $D(M_1', K_{21})$ 可得 M_1'，并计算 M_2'，$C_{2,1}'$，$C_{2,2}'$，执行 $H_2\rightarrow H_3$：$E(M_1', K_{23})$；

⋮

第 i 步　节点 H_i 执行 $D(M_{i-1}', K_{i,i-1})$ 得 M_{i-1}'，计算 M_i'，$C_{i,k}'$，执行 $H_i\rightarrow H_{i+1}$：$E(M_i', K_{i(i+1)})$；

⋮

第 d 步　节点 H_d 执行 $D(M_{d-1}', K_{d,d-1})$ 得 M_{d-1}'，计算 M_d'，$C_{d,k}'$，并向簇首节点广播新密钥参数。

2)簇内密钥更新的具体方法

第1步　$\forall V_i, i\in[1,N]$按照密钥建立协议中的方法根据其新私钥计算 P_i'；

第2步　$\forall H_j\rightarrow V_i, V_i\in C(i,N_i,H_j)$：$E(P_H', P_H)$和标识 ID；

第3步　$\forall V_i\rightarrow H_j, V_i\in C(i,N_i,H_j)$：执行 $D(P_H', P_H)$后，计算并传递 $E(E(P_i', P_i), P_H')$和标识 ID；

第4步　$\forall H_j$ 分别用 P_H'，P_i 解密获得 P_i'，并更新 V_i 对应密钥列表项的值 P_i 为 P_i'，且 $V_i\in C(i,N_i,H_j)$。

新周期起始时刻各簇首节点通过新密钥参数计算相互之间通信的对等密钥 K_{ij}'，完成簇首密钥更新。

(2) 簇首节点更新

当有新的簇首节点加入时，需先按照式(5)和式(6)计算新簇头节点的密钥份额和簇间密钥，然后按照集中式密钥建立方法建立该簇首节点所在簇的簇内密钥。由于簇间相互独立，因此其余簇内节点不受影响。簇首节点退出时，按照簇管理方法必然会生成新的簇首节点，新簇首节点生成后按照簇首节点加入的方法更新密钥。

(3) 簇内节点更新

小卫星节点作为簇内节点加入和退出网络而引起的密钥更新过程比较简单，因为其不会影响簇首节点的密钥份额，也不会影响其他节点的密钥计算。这种情况的密钥更新分别对应于其所在簇簇首节点密钥列表中一条记录的增加和删除。

4　协议分析

4.1　安全性分析

多种文献表明，基于 ECC 密钥管理协议建立在椭圆曲线离散对数难题之上具有较高的安全性。本文在文献[10]的基础上改进了周期性密钥更新方式，采用在上一周期结束前通过该周期的会话密钥传递下一周期密钥信息的方式，进一步提高了安全性。

4.2　性能分析

因为卫星网络信息传输过程中传播距离远，时延较长，所以总时延主要取决于消息传输时延，也即消息传播经历的跳数。各簇首节点到其簇内各个节点消息传播的距离，以跳数 H 来表示：

$$H=\sum_{i=1}^{N} hop(v_i) \tag{7}$$

式中，N 为节点总数，hop 函数用于求节点 V_i 到其所在簇簇首的跳数。通过簇首节点到其簇内节点的跳数之和可分析密钥更新速度。

以 Iridium 为例将 LEO 骨干卫星网络划分为 6 个簇，根据式(7)分别计算文献[9]的跳数 H_1 和本文方法所得的跳数 H_2：

$H_1=(1+2+3+4+5)*2*6=180$

$H_2=(1*4+2*5+3*2)*4+(1*4+2*4)*2=104$

二者都是将 Iridium 网络划分为 6 个簇，显然本文方法进一步降低了密钥更新的平均时延，更新速度更快。

结束语　卫星网络自身的特点使其比传统网络的安全问题更加复杂，而密钥管理是实现卫星网络安全通信的基本保障。本文分析了卫星网络密钥管理的安全性需求，对 LEO 卫星网络密钥管理协议进行了改进；提出了分布式和集中式相结合的密钥建立方法，既实现了密钥管理不依赖于地面 CA 的效果，也降低了广播密钥信息的额外通信量；引入了更合理的卫星网络分簇方法，提高了密钥更新速度；完善了密钥更新方法，增强了密钥管理协议的安全性。

参 考 文 献

[1] 张焕国，王张宜. 密码学引论(第二版)[M]. 武汉：武汉大学出版社，2009

[2] 蹇波，郭永辉，罗长远，等. 基于 ECC 的无线传感器网络密钥管理协议[J]. 计算机工程，2010，36(3)：142-144

[3] 宗家然，王阳阳. 椭圆曲线在 WSN 密钥管理中的应用[J]. 电脑知识与技术，2010，6(4)：828-830

[4] 李喆，李冬妮，王光兴. LEO/MEO 卫星网络中运用自组网思想的动态路由算法[J]. 通信学报，2005，26(5)：50-57

[5] 吴举，杜学绘，钱雁斌. 改进的空间网络密钥交换协议[J]. 计算机工程，2009，35(18)：113-115

[6] 蔡晓秋，张建中. 基于椭圆曲线的多银行电子现金系统[J]. 计算机应用研究，2007(5)：14-15

[7] Kumar K，Begum J N，Sumathy V. A Novel Approach towards Cost Effective Region-based Group Key Agreement Protocol for Ad-hoc Networks Using Elliptic Curve Cryptography[J]. Int. J. Communications，Network and System Sciences，2010，3：369-379

[8] 纪豫宣，马恒太，郑刚，等. 卫星网络密钥管理模型设计与仿真[J]. 系统仿真学报，2009，21(13)：4153-4158

[9] 张志强，张永健，王宇，等. 低轨卫星网络中基于轨道分簇的密钥更新算法[J]. 电子与信息学报，2010，32(3)：687-692

[10] 闫少阁，苏锦海. 基于椭圆曲线的分布式密钥建立协议[J]. 计算机工程与应用，2009，45(1)：113-115

[11] 李喆，刘军. 卫星网络安全路由研究[J]. 通信学报，2006，27(8)：113-119

[12] 李冬妮，张大坤. 卫星网络中多因素均衡的分簇算法[J]. 北京理工大学学报，2008，28(1)：62-65

(上接第 72 页)

[5] 郑丕谔，马艳华. RBF 神经网络的递阶遗传训练新方法[J]. 控制与决策，2000，15(2)：165-168

[6] Honeynet Project. Know Your Enemy：Statistics. 2001 [EB/OL]. http://old.honeynet.org/papers/stats/

[7] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报，2006，17(4)：885-897

[8] 任伟，蒋兴浩，孙锬锋. 基于 RBF 神经网络的网络安全态势预测方法[J]. 计算机工程与应用，2006，31：136-138，144

[9] Wang Hui-qiang，Lai Ji-bao，Wu Xiao. A Quantitative Forecast Method of Network-Secuity-Situation-Based on the BP Neural-Network with Genetic Algorithm[C] // Second International Multisymposium on Computer and Computational Sciences. 2007，65：374-380