PKI技术在空间信息网中的应用

任 方 马建峰 钟焰涛
(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 介绍了空间信息网的结构,分析了其特点以及面临的安全威胁,提出了要达到的安全目标。将分层式PKI技术应用到空间信息网中,构建了一种多层次的CA模型,其达到了机密性、认证性、完整性、不可否认性等安全目标。

关键词 空间信息网,公钥基础设施,数字证书,签名
中图法分类号 TP393.08 **文献标识码** A

Application of PKI in Spatial Information Networks

REN Fang MA Jian-feng ZHONG Yan-tao
(Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)

Abstract The structure of spatial information networks was introduced in this paper, the characteristics and security threats were analyzed and the security goals were proposed. We applied the technology of hierarchical PKI to spatial information networks and constructed a model of multi-level CA. In this model, the security goals of confidentiality, authentication, integrity and non-repudiation were reached.

Keywords Spatial information networks, Public key infrastructure, Digital certificate, Signature

1 空间信息网

作为卫星网络(Satellite Networks)的进一步发展,空间信息网(Spatial Information Network, SIN)近年来得到了越来越多的关注。空间信息网是以由在轨运行的多颗卫星和卫星星座组成的卫星网络为骨干网络,辅以各种具有空间通信能力的航天飞机、空间站、载人飞船、高空平台以及地面站共同组成的网络系统。它能够把运行在不同轨道、执行不同任务的各类卫星和航天、航空设备以及地面站联系起来,为其建立通信链路。它具有组网灵活且速度快、网络覆盖面广、不受地理环境制约等突出的优点,可以为复杂的空间任务提供很好的集成通信服务。空间信息网的节点具有运行速度快、网络拓扑结构变化快等特点。

卫星网络作为一个比较成熟的网络体系已经得到深入的研究[4-8]。卫星网络可以提供全球覆盖,因此成为空间信息网的骨干网络。卫星按照其运行高度的不同一般可以分为三大类:静止地球轨道卫星GEO、中轨道卫星MEO以及低轨道卫星LEO[4]。GEO卫星相对于地球静止,高度为35786km,一般数量比较少。MEO卫星和LEO卫星运行速度较快、高度较低,分别为5000~20000km和2000km以下。单层卫星可以提供全球覆盖,但轨道越低,需要的卫星个数就越多,而较高轨道的卫星虽然可以用较少卫星实现全球覆盖,但是卫星负担又会变重,且对地面用户的功率要求更高,因此现在重点研究的是多层卫星网络,典型的就是GEO/MEO/LEO三层网络[4]。多层网络具有很多单层网络不具备的优点,如可以以很高的效率实现包含极地在内的全球覆盖、通信灵活性强、传输延迟较低等等。

航天器是在绕地球轨道或外层空间按受控飞行路线运行的载人飞行器。目前穿梭于天地之间、可供人类在太空生存的航天器有三种:载人飞船、空间站和航天飞机。随着空间技术的进一步发展,将来航天器的种类和数量会越来越多,它们之间需要下达各种指令或者进行数据传输,因此航天器的组网迫在眉睫。可以利用现有的成熟的卫星网络为依托,将航天器作为卫星网的接入节点。

高空平台(High Altitude Platform Station, HAPS)[9]是将无线基站安放在长时间停留在高空的飞行器上来提供通信的系统。HAPS基站处于距地面20km至50km的平流层中,保持相对静止,具有比地面无线通信系统更广的覆盖范围,可以实现用户的高移动性和高数据传输率。和卫星系统相比,HAPS具有低费用、较小时延、组建迅速、容纳用户数量大等特点,因此具有很大的发展潜力。未来的空间信息网将是一个包含由卫星和航天器所组成的天基网和HAPS组成的空基网的多样化的综合性通信网络,其作为地面有线和无线网络的有益补充,必将得到很大的发展。

2 公钥基础设施PKI

2.1 密码技术

为了保证网络中通信数据的安全,需要用到加密技术。传统的加密方案分为对称加密和公钥加密两大类,在对称加密方案中,通信双方使用同一个密钥k,发送方Alice用k对

到稿日期:2010-02-09 返修日期:2010-05-05 本文受国家自然科学基金(No. 60872041)资助。
任 方(1981-),男,博士生,主要研究方向为密码学与网络安全,E-mail:renfang_81@163.com;马建峰(1963-),男,教授,博士生导师,主要研究方向为密码学与无线网络安全。

要发送的信息 m 进行加密得到密文 c，将 c 通过不安全信道发送给接收方 Bob。Bob 接收到 c 后用 k 进行解密最终得到信息 m。在公钥加密方案中发送方 Alice 拥有两个密钥，分别称为公钥 pk 和私钥 sk，其中公钥对外公开。Alice 发送消息时用私钥 sk 加密信息，而 Bob 使用公钥 pk 进行解密。对称加密方案要求双方共享一个 k，这在现实中会遇到一些困难，比如远距离通信的双方如何在通信之前在不安全信道协商一个共同的 k？公钥密码方案的好处在于解密密钥 pk 可以公开，因此可以通过公共信道传送给接收方，它在现实中有着很广的应用范围。

网络安全的另一个重要方面是节点的身份认证，以保证通信的确是在合法预期的两个节点之间进行。以公钥加密技术为基础的数字证书可以实现节点的身份认证。网络中每一个合法节点拥有一份有效的数字证书来证明其身份，证书由网络中的可信中心颁发，其基本内容包含节点的身份信息和节点使用的公钥信息。两个节点需在通信时先验证对方的证书是否有效以完成身份认证。

数字证书需要可信中心进行签名以保证其有效性。数字签名技术可以提供数据完整性保护，可信中心使用自己的私钥对节点的证书进行签名，其它节点可以用可信中心的公钥进行证书验证[10]。

哈希函数 H()是一个单向函数，即给定消息 m 计算 $H(m)$是容易的，但是由 $H(m)$计算 m 却是计算上不可行的。$H()$可以将任意长度的消息压缩到固定长度的消息摘要。数字签名技术常常使用哈希函数来提高签名速度，此外哈希函数还可以破坏签名方案的同态结构，从而增加了签名的安全性[11]。

2.2 公钥基础设施

公钥基础设施(Public Key Infrastructure，PKI)指的是用公钥技术提供安全服务的成熟的基础设施。PKI 的主体包括证书机构 CA、数字证书库等。其中 CA 是系统的可信机构，也是整个 PKI 的核心部分。它是数字证书的颁发机关，在整个系统中具有权威的地位。证书库存储系统节点所有的合法证书，可供任意节点查询[2,3]。

CA 可以分为两类：集中式 CA 和分层式 CA。

1)集中式 CA：由单一的主体充当证书颁发机构，所有用户都信任该主体。

2)分层式 CA：存在多个层次的 CA。不同层的 CA 有不同的服务域，为该域内的用户颁发数字证书。

标准的分层式 CA 可以用树状结构来描述[1]。在这样的结构中，每一个节点代表一个用户，其数字证书由它的父节点发行。叶子节点代表的是最终的端用户，而非叶子节点充当的是不同级别 CA 的角色，树的根节点代表根 CA，它是整个系统的最高信任实体。如图 1 所示，C_0 表示根 CA，$C_{1,1}$ 和 $C_{1,2}$是两个二级 CA，B_i 表示端用户，箭头指向表示颁发证书。

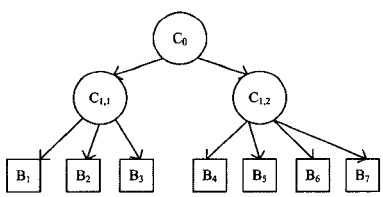

图 1 分层式 CA

一个 CA 的信任域包括它的所有子节点，即代表终端用户的叶子节点和若干(可能是零个)子 CA 节点。该信任域中的所有节点都信任该 CA。作为终端用户的叶子节点，它们的数字证书由各自的父节点也即最低一层的 CA 进行签署。而低级 CA 的数字证书由高一级的 CA 进行签署，由此层层上溯，最高的根 CA 是整个系统中最高的信任主体，它的证书是用自己的私钥签署的，其信任域包括整个系统。

终端用户进行通信之前需要验证数字证书。首先确认通信双方是否有共同的 CA，如果是则直接用该 CA 的公钥验证证书。如果不是，则向更高层的 CA 追溯，直至找到一个共同的 CA，然后依次验证连接该 CA 和用户节点的路径上所有节点的证书是否有效。如果该链上所有证书有效，则可说明终端用户持有的是合法的证书。例如图 1 中 B_1 和 B_5 要验证对方的证书，因为它们的上级 CA 并不相同，所以必须上溯到根 CA，因此要依次验证 B_1，$C_{1,1}$，C_0，$C_{1,2}$，B_5 的数字证书。

3 空间信息网的安全需求

3.1 空间信息网面临的安全威胁

由于空间信息网是一个开放式的网络，节点种类繁多，拓扑结构复杂多变，而且网络节点的加入和离开非常频繁且不可预测，网络很容易受到来自非法节点的安全威胁。一般来说空间信息网有可能受到以下种类的攻击：

1)窃听攻击。由于空间信息网使用无线链路进行连接，攻击者可以任意截获网络节点之间的所有数据流，造成信息泄漏。

2)伪造攻击。攻击者可以伪造成已存在的某合法节点与其他节点进行通信，造成保密消息泄漏。

3)恶意攻击。攻击者可以截获并且篡改合法用户之间的通信数据流，造成不可估量的严重后果。

3.2 空间信息网应该达到的安全目标

1)机密性：卫星节点之间、卫星与其它航天器以及 HAPS 之间、卫星与地面用户之间的数据通信不能泄露给非法用户，节点之间的路由信息也要求保密。

2)认证性：网络节点之间能够相互认证通信对方节点的身份，防止恶意节点进行伪装攻击。

3)完整性：卫星之间或者卫星与其它节点之间传输的数据不能被改动，这些改动包括传输错误或者恶意用户的篡改。

4)不可否认性：网络节点不能否认它所发送的数据，以此可以追踪发送错误数据的恶意的或者被攻陷的网络节点。

5)可用性：网络能够提供可靠的服务，避免拒绝服务攻击。

4 空间信息网安全解决方案

4.1 遵循的原则

由于空间信息网节点运动速度很快，导致节点之间的通信链路切换迅速、网络拓扑结构变化频繁，很难为任意两个用户之间建立长期的对称密钥，因此可以采用公钥和对称密钥相结合的方案来实现安全通信。即

1)使用对称密钥实现保密的数据通信。网络中两个节点通信时使用对称的会话密钥，一次会话使用一个对称密钥，通信结束则该会话密钥失效。

2)使用基于公钥密码的 PKI 技术实现网络通信双方的身份认证以及建立对称的会话密钥，此外还可以实现通信数据的完整性和不可否认性。

集中式 CA 是由系统中单一的实体充当 CA，此实体的安全性将成为整个系统安全的瓶颈，存在单点失效的问题。此外单一的 CA 负担过重，由运算能力有限的卫星来充当并不合适。如果将地面控制中心作为系统的 CA，则所有空间网络节点要频繁地与地面进行数据通信，降低了网络的通信效率，因此集中式 CA 并不适合空间信息网。作为空间信息网主干网的卫星网络是由三个层次的卫星构成的，因此可以将分层式的 CA 模型引入卫星网络，即由上层的卫星充当下层卫星的 CA，为其颁发证书。这样某个单独的 CA 失效只会影响它所服务的域，不会对整个网络有太大影响。

4.2 卫星网络 CA 模型的实现

4.2.1 卫星网体系结构

卫星网络部分包括 GEO 卫星层、MEO 卫星层、LEO 卫星层以及卫星地面站。其中地面站负责卫星网络节点的加入或者退出。卫星网络中有三种类型的双向连接[8]：星间链路(ISLs)、轨间链路(IOLs)和用户数据链路(UDLs)。其中同层卫星之间的通信使用星间链路，不同层卫星之间的通信使用轨间链路，而卫星与地面站之间的通信使用用户数据链路。

假定 MEO 层卫星全体与 LEO 层卫星全体可以分别提供全球覆盖，一颗 GEO 卫星的覆盖域指的是它所覆盖的所有 MEO 和 LEO 卫星全体。同样 MEO 卫星的覆盖域指的是它所覆盖的所有 LEO 卫星全体。GEO 卫星的覆盖域如图 2 所示，其中 G_0 代表一颗 GEO 卫星，M_0 表示它所覆盖的 MEO 卫星群组，其中单独的 MEO 卫星用编号 $M_{0,0}$，$M_{0,1}$ 等表示。$M_{0,0}$ 的覆盖域用 $L_{0,0}$ 表示，其中单独的 LEO 卫星用 $L_{0,0,0}$，$L_{0,0,1}$ 等表示。

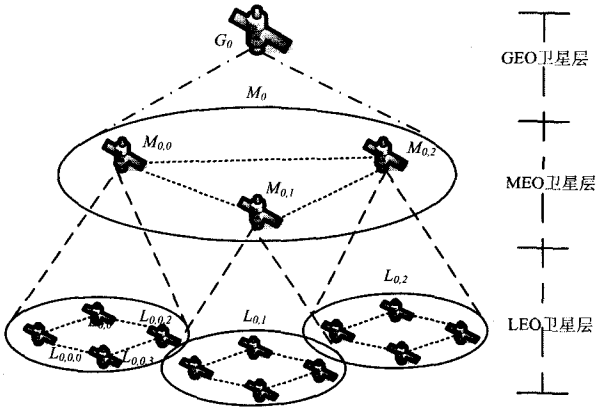

图 2 GEO/MEO/LEO 三层卫星网络图

4.2.2 安全模型

每颗卫星都有一对公/私钥，其中公钥用来加密消息和验证签名，私钥用来解密和签名。系统选择了一个哈希函数 $H(x)$，其在数字证书签名时使用。该函数对所有加入系统的节点公开。

G_0 卫星的证书由地面站签署，同时它又是自己所覆盖的所有卫星节点的局部根 CA。MEO 层的 $M_{0,0}$，$M_{0,1}$ 等卫星节点的数字证书由 G_0 用它的私钥签署，$M_{0,0}$ 又充当它所覆盖的 LEO 卫星群组的 CA，为它们颁发证书。

卫星节点的公钥证书包含以下内容：卫星节点的 ID 号、公钥、证书签署时间、证书吊销时间。比如对于如上所示的 MEO 卫星节点 $M_{0,0}$，原始证书格式如下

$$cert_{M_{0,0}} = \langle ID_{M_{0,0}}, pk_{M_{0,0}}, T_{sign}, T_{expire} \rangle$$

此证书经由覆盖它的卫星 G_0 的私钥签署生效。

当两颗卫星需要进行身份认证时，它们首先确定是否在同一个高层卫星的覆盖域内，如果是，则它们有共同的 CA，可以直接验证证书的有效性。如果不是，则需要认证充当对方局部根 CA 的 GEO 卫星。比如 $M_{0,0}$ 和 $M_{0,1}$ 卫星的证书是由同一个 $CA(G_0)$ 签署的，它们可以直接相互认证。如果另一颗 GEO 卫星 G_1 所覆盖的卫星 $M_{1,1}$ 要和 $M_{0,0}$ 通信，由于它们有着不同的局部根 CA，因此必须要确定 G_0 和 G_1 是否持有合法的证书。这就需要用到地面站的公钥以完成 $M_{1,1}$-G_1-地面站-G_0-$M_{0,0}$ 这一证书链的验证。

我们假定地面站是安全的。由于卫星运行轨道是确定的，地面站可以预知所有卫星运行的轨迹，当有新的卫星需要加入网络时，由地面站根据当前卫星运行情况确定该卫星加入的是哪一个域，它将通知该域的 CA 以完成接入认证。

4.3 其它节点的接入

各种类型的航天器以及 HAPS 是空间信息网的重要组成部分，由于它们的运行没有固定的规律可以遵循，因此可以作为卫星网络的接入节点。对于这一类节点可以选择临近的卫星作为自己的 CA，由该卫星为其颁发数字证书。航天器运行时基本上处于和卫星同样的高度，因此它可以选择最近的卫星作为其运行时的 CA，由地面站通过安全的渠道通知该 CA 即可完成网络接入。而 HAPS 运行位置介于卫星和地面之间，它可以选择低层的 LEO 卫星作为其 CA。同样接入认证需要通过安全的地面站进行。

结束语 空间信息网作为地面有线网络和无线网络之外的又一具有广阔发展前景的网络，其安全性有着非常重要的地位。本文通过分析空间信息网的特点，提出了空间信息网的安全需求和面临的安全威胁，将 PKI 技术引入空间信息网，为网络节点的安全数据传输和身份认证构建了一种多层次的 CA 模型。在这种模型下，网络中的任意节点可以通过验证对方的数字证书实现身份认证，建立保密的会话密钥，从而实现安全的数据通信。

参 考 文 献

[1] ITU-T. ITU-T Recommendation X.509 ITU-T. August 2005

[2] 金晓耿，郭巍，金亿平，等. PKI 中的证书和发证机构[J]. 计算机科学，1999，26(7)：83-86

[3] 李彦，王柯柯. 基于 PKI 技术的认证中心研究[J]. 计算机科学，2006，33(2)：110-111

[4] Akyildiz I F，Ekici E，Bender M D. MLSR：a novel routing algorithm for multilayered satellite IP networks[J]. IEEE/ACM Transactions on Networking，2002，10(3)：411-424

[5] Ercetin O，Ball M O，Tassiulas L. Next generation satellite systems for aeronautical communications[J]. Int. J. Satell. Commun. Network，2004，22：157-179

[6] Hu Yurong，Li V O K. Satellite-based Internet：a tutorial[J]. IEEE Communications Magazine，2001，39(3)：154-162

[7] Cruickshank H S. A security system for satellite networks[C]// Fifth International Conference on Satellite Systems for Mobile Communications and Navigation. 1996：187-190

[8] Chen Chao，Ekici E，Akyildiz I F. Satellite grouping and routing protocol for LEO/MEO satellite IP networks[C]// Proc. of the 5th ACM International Workshop on Wireless Mobile Multimedia. 2002：109-116

[9] Aragon-Zavala A. High-Altitude Platforms for Wireless Communications[M]. A John Wiley and Sons，Ltd，Publication，2008

[10] 毛文波. 现代密码学理论与实践[M]. 北京：电子工业出版社，2004

[11] 冯登国，裴定一. 密码学导引[M]. 北京：科学出版社，1999