分布式 CA 下空间网络认证密钥安全度量方法

罗长远[①]　李　伟[①②]　李海林[①]　蹇　波[①]
[①](解放军信息工程大学电子技术学院　郑州　450004)
[②](解放军 63895 部队　孟州　454750)

摘　要：基于分布式 CA 的密钥管理策略解决了空间网络中不易实施集中式密钥管理的难题，但也给认证密钥的安全带来了新的威胁。该文在描述和分析空间网络中认证密钥的安全威胁的基础上，提出了一种度量认证密钥安全强度的方法。该方法可根据系统门限值、密钥更新周期等参数的设置情况，定量度量认证密钥的安全强度。通过分析系统门限值和密钥分量更新周期对安全强度的影响，给出了合理设置这两个网络安全参数的方法。

关键词：空间网络；分布式 CA；门限机制
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009-5896(2009)10-2316-05

Measurement Method for Space Networks Authenticated Key Security under Distributed CA

Luo Chang-yuan[①]　Li Wei[①②]　Li Hai-lin[①]　Jian Bo[①]
[①](*PLA Information Engineering University*, *Electronic Technology Institute*, *Zhengzhou* 450004, *China*)
[②](*The* 63895 *Unit of the Chinese People's Liberation Army*, *Mengzhou* 454750, *China*)

Abstract: The key management schemes bsaed on Distributed Certificate Authority resolve the difficulty to adopting concentrating key management in space networks, but result in some new threats of authenticated key. Based on discribing and analyzing the threats suffered by authenticated key of space networks, a measurement method for security intensity of authenticated key is proposed. The method can quantitatively measure the security intensity of authenticated key according to the setting of parameters, such as threshold value, key-update period etc. By analyzing the impact of threshold value and key-update period on authenticated key security, a method of setting the two networks security parameters reasonably is given.

Key words: Space networks; Distributed Certificate Authority (CA); Threshold mechanism

1　引言

空间网络是由卫星网络、临近空间网络和相关地面控制设施组成的一体化信息网络，在军事和民用领域都有着广泛的应用前景[1,2]。空间网络所处环境的高开放性和网络拓扑结构的动态性，使其所面临的安全形势异常严峻。传统地面网络的信息安全以 PKI (Public Key Infrastructure)技术为基础，采用集中式 CA(Certificate Authority)的方式来实施密钥管理和认证服务。在空间网络中，无法直接建立这样集中式的认证中心。首先，在动态变化的空间网络中，集中式的认证中心易导致单点失效和拒绝服务；其次，由于空间网络采用低带宽的无线信道作为通信链路，集中式的认证中心易造成网络拥塞和服务的延迟。为解决这些难题，文献[3]提出了在空间网络中实施基于分布式 CA 的密钥管理方案。基于分布式 CA 的密钥管理模型最早由 Zhou 与 Hass 等人提出并应用于了 Ad hoc 网络中[4]。现有的分布式 CA 密钥管理方案依据参与实现 CA 功能节点数目的不同，可分为局部分布式[5,6]和完全分布式[7,8]。这两类方案都利用 Shamir 等人提出的门限秘密共享算法[9]，将 CA 认证密钥共享给了多个服务节点，每个服务节点掌握一个认证密钥分量。多个(即门限个)服务节点联合即可恢复认证密钥，完成对其它节点的认证服务。因此，单个服务节点的失效不会引起整个认证中心的瘫痪；也避免了集中式认证中因数据流向过于集中而导致的拥塞和延迟现象。但这种共享认证密钥的做法也给密钥的安全带来了新的威胁。当攻击者在一定时间内掌握门限数个认证密钥分量即可重构系统认证密钥，从而对网络的安全构成严重的威胁。因此，需对分布式 CA 下空间网络认证密钥的安全强度做一个合理的评估和度量，给合理地布设空间网络提供依据。

本文在描述和分析系统安全威胁的基础上，提

2008-10-14 收到，2009-03-17 改回
国家 863 计划项目(2006AAJ124)资助课题

出了一种空间网络分布式 CA 认证密钥的安全度量方法。该方法可根据系统门限值、更新周期等参数的设置情况，定量度量系统对认证密钥安全的防护强度。通过分析参数对安全防护强度的影响，给出了相关参数的合理设置准则。

2　空间网络认证密钥安全度量方法

由以上分析可知，攻击者掌握的密钥分量达到门限个即可得到认证密钥。因此攻击者获得少于门限个密钥分量的概率可作为评估认证密钥安全强度的一个重要度量值。为了便于讨论，对系统做如下假设和定义。

(1)定义 n 为网络中的服务节点数，即系统存在的认证密钥分量数，k 为门限值，t 为节点持有当前密钥分量的时间，T 为系统对各服务节点密钥分量的更新周期；

(2)假设攻击者的攻击能力足够强，可同时对多个服务节点的密钥分量进行攻击，以期获得较大的成功率。攻击方式包括对节点进行欺骗干扰和监听节点的违规操作等，忽略通过破解密钥算法获取认证密钥的可能；

(3)称服务节点的密钥分量被攻击者获得这一事件为节点密钥分量失控，并假设每个服务节点的密钥分量失控概率分布相同。

下面在分析单节点密钥分量失控概率的基础上，给出空间网络认证密钥的安全强度度量方法。

2.1 单节点密钥分量失控概率

单节点密钥分量的失控是由服务节点的失误造成的，这种失误行为包括被攻击者欺骗以及节点自身的违规操作等。在实际网络中，单个服务节点的失误行为的发生具有以下特点：

(1)节点持有密钥分量的时间越长，失误的概率就越大，但失误不是必然的，即不存在节点绝对会失误的时间点。若用 $p(t)$ 表示单节点的失控概率分布函数，则有：$p(0)=0$，$p(\infty)=1$；

(2)攻击者无论选择何时开始攻击，获得成功的概率分布是相同的。即：在 t_1 时间内节点没有出现失误，将不会影响该节点再过 t_2 时间内的失误概率分布。用概率公式可将这一特点表示为 $P[t>t_1+t_2 \mid t>t_1]=P[t>t_2]$。

结合条件概率公式，上式可用 $p(t)$ 表示为：$1-p(t_1+t_2)=[1-p(t_1)]\cdot[1-p(t_2)]$。

令 $g(t)=1-p(t)$，显然有 $g(t_1+t_2)=g(t_1)\cdot g(t_2)$。结合 $g(0)=1-p(0)=1$，可得关于 $g(t)$ 的微分方程：

$$g(t)'=\lim_{\Delta t\to 0}\frac{g(t+\Delta t)-g(t)}{\Delta t}=\lim_{\Delta t\to 0}\frac{g(t)g(\Delta t)-g(t)}{\Delta t}$$
$$=\lim_{\Delta t\to 0}\frac{g(0+\Delta t)-g(0)}{\Delta t}g(t)=g(0)'g(t)$$

结合特点 1，解微分方程可得：$g(t)=e^{g'(0)t}=e^{-p'(0)t}$。令 $\lambda=p'(0)$，可得单节点密钥分量失控概率分布：$p(t)=1-e^{-\lambda t}$，$(0<t\le T)$。因此，单节点失控概率服从指数分布。令 $p_e=p(T)$，则有

$$p_e=1-e^{-\lambda T} \tag{1}$$

p_e 是在某个密钥分量更新之前，攻击者能够获得该密钥分量的最大概率。其中参数 λ 为初始时刻 $p(t)$ 的变化速率，与节点的安全设置有关，可由节点辨别欺骗的能力、安全操作手册的合理程度以及安全操作规程落实情况等因素来决定。因此是 λ 属于管理范畴的安全指标，本文不对 λ 的取值深入研究。后续分析将其当作常量，认为 p_e 的取值仅受分量更新周期 T 影响。

2.2 认证密钥安全防护强度度量

由于网络中各服务节点持有的密钥分量互不相同，且相互间没有任何联系，因此攻击者对 n 个节点分别攻击是一个相互独立的 n 重伯努利过程。用 $P(n,i)$ 表示攻击者同时攻击 n 个节点并能获得 i 次成功的概率，则有：$P(n,i)=C_n^i p(t)^i\left(1-p(t)\right)^{n-i}$。

用 P_T 表示在一个密钥更新周期 T 内，攻击者无法获取认证密钥(掌握的密钥分量数少于门限数)的概率。结合式 1 可得：

$$P_T=\sum_{i<k}P(n,i)=\sum_{i=0}^{k-1}C_n^i\left(1-e^{-\lambda T}\right)^i\left(e^{-\lambda T}\right)^{n-i} \tag{2}$$

P_T 反映了攻击者获得空间网络认证密钥的难易程度，表征了系统对分布式 CA 认证密钥的保护安全强度，P_T 的值越大认证密钥被攻击成功的概率就越小，系统对认证中心的密钥的保护就越强，网络就越安全。因此，式(2)可作为认证密钥安全强度的度量算式。

3　参数分析

在式(2)中，门限值和密钥分量更新周期是影响认证密钥安全强度的两个重要参数。如何调整这两个参数使系统达到最佳状态，则是网络建设者比较关心的问题。分析这两个参数与安全强度的关系，并给出最佳取值，对空间网络安全建设具有指导意义。

为便于讨论，将式(1)代入式(2)可得：

$$P_T=\sum_{i=0}^{k-1}C_n^i p_e^i(1-p_e)^{n-i} \tag{3}$$

由于 p_e 和 T 是一一映射关系，因此利用式(3)

可把考察 T 在 $(0,+\infty)$ 区间内对 P_T 的影响，转化到考察 p_e 在 $(0,1)$ 区间内对安全强度的影响情况，解决了不易对 T 全区间取值分析的困难。

3.1 门限值对安全强度的影响

为考察门限值 k 对 P_T 的影响，在图 1 中利用 Matlab 给出了 $n=100$， $p_e=0.3$ 时 P_T 关于 k 的变化曲线。为验证曲线趋势具有一般性，图 2 又给出了 $n=100$， p_e 分别为 0.1，0.2，0.3，0.5，0.7 时的 5 条曲线。由图 2 可看出各曲线的变化趋势基本一致。

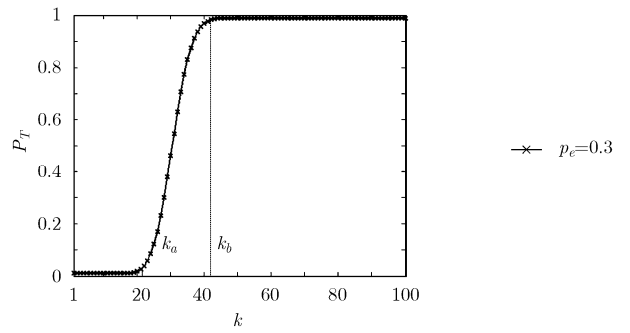

图 1 P_T 随 k 变化曲线

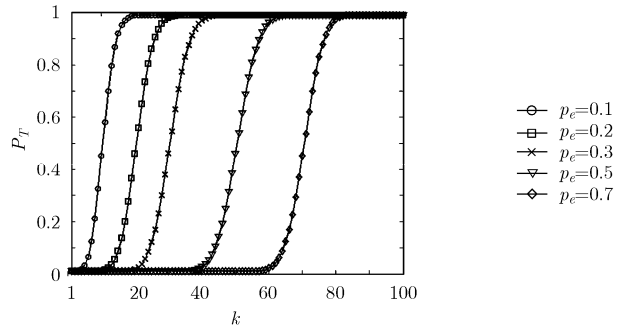

图 2 不同 p_e 值下 P_T 随 k 变化曲线

由图 1，图 2 可看出，P_T 关于 k 单调递增，但增加速度极不均匀，安全强度存在一个迅速增大的跳变区间。设跳变区间为 (k_a,k_b)，显然 k_b 即为最佳门限值。这是因为：$k=k_b$ 时，安全强度 P_T 取值接近 1；此时增大门限值并不会给安全强度明显的提升，反而会增加认证时的系统开销；而减小门限值则会带来安全强度的急剧下降。

由于 k_b 是区分 P_T 增长“快”与“慢”的一个模糊值，确定 k_b 的取值需引入辅助判定条件。用 $\Delta p(k)$ 表示增加一个单位门限值系统安全强度的增量，其中 k 为增加前的门限值。引入辅助判定条件：当 $\Delta p(k)$ 小于某个给定的数值 δ 时，认为 P_T 随 k “变化缓慢”，则有：$\Delta p(k_b)=\delta$。由式(3)可得：

$$\Delta p(k)=C_n^k p_e^{\ k}\cdot(1-p_e)^{n-k} \tag{4}$$

$\Delta p(k)$ 与 k 的单调关系可由函数曲线来直观反映。图 3 给出了 $n=100$， $p_e=0.3$ 时，$\Delta p(k)$ 随 k 的变化曲线。

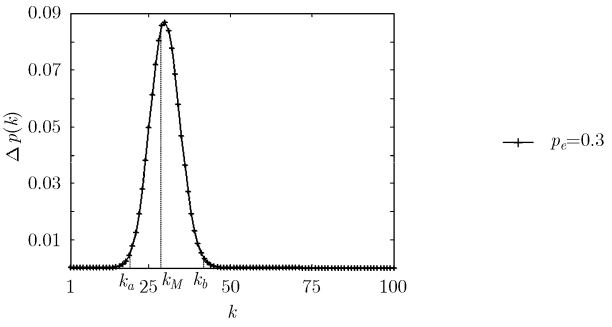

图 3 $\Delta p(k)$ 随 k 的变化曲线

若设 $k=k_M$ 时 $\Delta p(k)$ 取最大值，显然 $k_b\in(k_M,n)$。其中 k_M 可由下式求得：

$$\frac{\Delta p(k+1)}{\Delta p(k)}=\frac{n-k}{k+1}\cdot\frac{p_e}{1-p_e}=1 \tag{5}$$

这是因为：当 $\dfrac{\Delta p(k+1)}{\Delta p(k)}>1$ 时，$\Delta p(k)$ 随 k 的增大而增大；当 $\dfrac{\Delta p(k+1)}{\Delta p(k)}<1$ 时，$\Delta p(k)$ 随 k 的增大而减小。所以当 $\dfrac{\Delta p(k+1)}{\Delta p(k)}=1$ 时，$\Delta p(k)$ 最大。

由式(5)可得：$k_M=p_e(n+1)-1$。若 $p_e(n+1)-1$ 为非整数，则 k_M 为离 $p_e(n+1)-1$ 最近的两个整数中，使 $\Delta p(k)$ 较大的那个。因 $\Delta p(k)$ 在区间 (k_M,n) 上是单调的，结合 $\Delta p(k_b)=\delta$，在区间 (k_M,n) 内采取“折半查找”算法，可求得 k_b。

3.2 分量更新周期对安全强度的影响

T 对 P_T 的影响可通过 p_e 来反映。图 4 中给出了 $n=100$，$k=20$ 时 P_T 随 p_e 的变化曲线。同样为反映曲线趋势具有一般性，图 5 又给出了 $n=100$，k 分别为 20，30，40，50，60 时的 5 条曲线。由图 5 可看出，各曲线的变化趋势基本一致的，即这种趋势具有一般性。

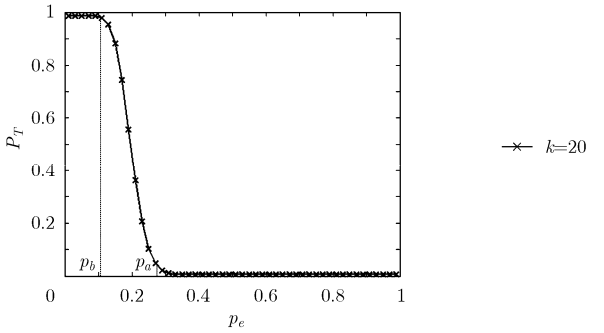

图 4 P_T 随 p_e 的变化曲线

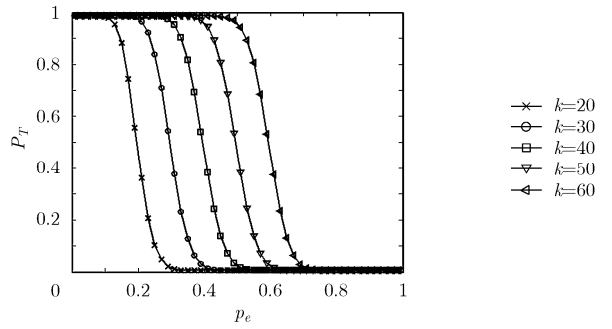

图 5 不同 k 值下 P_T 随 p_e 变化曲线

由图 4，图 5 可看出，P_T 关于 p_e 单调递减，减小速度也不均匀，安全强度存在一个迅速下降的跳变区间。设跳变区间为 (p_a, p_b)，若 $p_e = p_a$ 时 T 取值为 T_a，则 T_a 是最佳密钥分量更新周期。这是因为：$p_e = p_a$ 时，安全强度 P_T 取值接近 1；此时缩短更新周期(降低 p_e)不会使安全强度明显的提升，反而加大了密钥更新的频繁度，增加了系统开销；而延长更新周期(增大 p_e)则会使安全强度的急剧下降。

同样 p_a 也是一个区分 P_T 变化是否“迅速”的模糊值。因此，确定 p_a 的取值也需借助额外的判定条件。由于 p_e 是连续变量，不可像门限值那样通过安全强度增量来分析 P_T 随 p_e 的变化。定义 $\partial P_T(p_e)$ 为 P_T 关于 p_e 的 1 阶偏导函数，可通过 $\partial P_T(p_e)$ 来衡量 P_T 随 p_e 的变化速度。为了便于对 p_e 求导，可把式(3)中 $(1-p_e)^{n-i}$ 项展开，可得

$$P_T = \sum_{i=0}^{k-1} C_n^i \sum_{j=0}^{n-k} C_{n-i}^j (-1)^j \cdot {p_e}^{i+j} \tag{6}$$

式(4)是 P_T 关于 p_e 的 n 次多项式，易得

$$\partial P_T(p_e) = \sum_{i=0}^{k-1} C_n^i \sum_{j=0}^{n-i} C_{n-i}^j (-1)^j \cdot (i+j) {p_e}^{i+j-1} \tag{7}$$

图 6 为 $n=100, k=20$ 时，$\partial P_T(p_e)$ 随 p_e 的变化曲线。由图可看出 $\partial P_T(p_e)$ 有最小值。而 p_a 应处于最小值左侧。

为确定 p_a，引入判定条件：当 $|\partial P_T(p_e)|$ 小于某个给定的值 ε 时，称 P_T 随 p_e “变化缓慢”。则有：

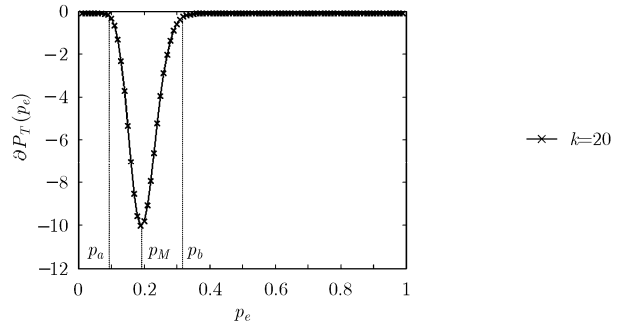

图 6 $\partial P_T(p_e)$ 随 p_e 的变化

$$\left|\partial P_T(p_a)\right| = \varepsilon \tag{8}$$

若 $p_e = p_M$ 时，$\partial P_T(p_e)$ 取得最小值。则 p_M 是 P_T 的 2 阶偏导函数的零点，即 P_T 的 2 阶偏导函数所确定的一元 $n-2$ 次方程的实根。方程解析式如式(9)所示，这个方程是可解的，解法不再赘述。

$$\sum_{i=0}^{k-1} C_n^i \sum_{j=0}^{n-i} C_{n-i}^j (-1)^j \cdot (i+j) \cdot (i+j-1) {p_e}^{i+j-2} = 0 \tag{9}$$

在区间 $(0, p_M)$ 内，结合 $|\partial P_T(p_a)| = \varepsilon$，采取“折半查找”算法可求得 p_a。由式(1)，可用 p_a 计算得到最佳更新周期 T_a：

$$T_a = \frac{1}{\lambda} \ln \frac{1}{1-p_a} \tag{10}$$

4　结束语

基于分布式 CA 的密钥管理策略解决了空间网络中不易实施集中式密钥管理的难题，但也给认证密钥的安全带来了新的威胁。本文在对空间网络分布式 CA 认证密钥所受到的安全威胁进行了数学描述和分析的基础上，给出了一种定量度量认证密钥安全强度的方法，并分析了两个重要的网络安全参数——系统门限值和密钥分量更新周期对网络安全强度的影响。通过分析发现，两参数对网络安全强度的影响都是不均匀的，安全强度随着安全参数的变化存在跳变现象；在某些参数取值下，网络安全性能极差。这种不均匀性反映出合理设置网络安全参数的重要性。通过分析，最后给出了合理设置门限值和密钥分量更新周期的方法，这对指导空间网络安全建设有着重要意义。

参 考 文 献

[1] 徐志博, 马恒太. 一种用于卫星网络安全认证的协议设计与仿真[J]. 计算机工程与应用, 2007, 43(17): 130–132.
Xu Zhi-bo and Ma Heng-tai. Design and simulation of security authentication protocol for satellite network [J]. *Computer Engineering and Applications*, 2007, 43(17): 130–132.

[2] 唐志华. 基于临近空间的目标探测及宽带通信[J]. 无线电工程, 2007, 37(11): 28–30.
Tang Zhi-hua. Target acquisition and broadband communications based on near-space vehicles [J]. *Radio Engineering of China*. 2007, 37(11): 28–30.

[3] 杨德明, 慕德俊, 许钟. Ad hoc 空间网络密钥管理与认证方案[J]. 通信学报. 2006, 27(8): 104–107.
Yang De-ming, Mu De-jun, and Xu Zhong. Novel key management and authentication scheme for Ad hoc space networks [J]. *Journal on Communications*, 2006, 27(8): 104–107.

[4] Zhou L and Hass Z J. Securing Ad hoc networks [J]. *IEEE*

Networks, 1999, 13(6): 24–30.

[5] Wu B, Wu J, and Fernandez E B, *et al*.. Secure and efficient key management in mobile Ad hoc networks[C]. Proc of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05). Denver: IEEE Computer Society. 2005: 288–295.

[6] Dong Y, Wing G, and Sui A, *et al*.. Providing distributed certificate authority service in mobile ad hoc networks[C]. Proc of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks. Athens: IEEE Computer Society, 2005: 149–156.

[7] 曾萍, 陈瑞利, 方勇. 基于自认证公钥的全分布式移动 Ad hoc 网络密钥管理方案[J]. 计算机应用研究, 2008, 25(6): 1779–1782.
Zeng Ping, Chen Rui-li, and Fang Yong. Fully-distributed key management scheme based on self-certified public key for mobile Ad hoc network [J]. *Application Research of Computers*, 2008, 25(6): 1779–1782.

[8] Luo H Y, Zerfos P, and Kong J, *et al*.. Self-securing Ad hoc Networks[C]. Proc of the Seventh IEEE Symposium on Computers and Communications (ISCC'02). IEEE Computer Society, 2002: 567–574.

[9] Shamir A. How to share a secret [J]. *Communications of the ACM*, 1979, 22(11): 6l2–6l3.

罗长远： 男，1973 年生，博士，副教授，硕士生导师，研究方向为装备工程、无线通信系统安全.

李 伟： 男，1980 年生，硕士生，助理工程师，研究方向为空间信息网络安全.

李海林： 男，1981 年生，讲师，研究方向为无线通信安全.

蹇 波： 男，1982 年生，硕士生，研究方向为无线传感器网络安全.