自组网中一种基于填充设计的组密钥更新策略

陈建伟 许 力 黄丹芸
(福建师范大学网络安全与密码技术重点实验室 福州 350007)

摘 要：保证密钥安全分发和高效更新是目前自组网安全领域的一个研究热点。该文采用拉丁方构造正交阵列，快速实现 t 填充设计，在此基础上，将 t 填充设计的无覆盖集的族性质应用于密钥预分发，提高了自组网抵抗节点合谋的能力，增强了节点的共享密钥连接度，使得密钥的管理更加高效。该文对策略的安全性和有效性进行了详细的理论分析和数据分析。

关键词：自组网；组播；组密钥更新；填充设计；无覆盖集的族
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2008)08-2004-04

A t-Packing Designs Based Group Rekeying Scheme in Ad hoc Networks

Chen Jian-wei Xu Li Huang Dan-yun
(*Lab. of Network Security and Cryptology*, *Fujian Normal University*, *Fuzhou* 350007, *China*)

Abstract: Secure group key distribution and efficient rekeying is one of the most challenging security issues in Ad hoc networks at present. In this paper, Latin squares are used to construct orthogonal arrays, from which t-packing designs can be quickly obtained. Based on cover-free family properties, t-packing designs are adopted in key pre-distribution phase. The new scheme improves the collusion-resilience of the networks using the cover-free family properties, and enhances the key-sharing connectivity of nodes which makes key management more efficient. This paper also presents in depth theory and data analysis of the new scheme in terms of network security and efficiency.

Key words: Ad hoc network; Multicast; Group rekeying; Packing design; Cover-free family

1 引言

自组网(Ad hoc networks)是由移动节点组成的不需要固定基站并支持多跳的计算机通讯网络。组播作为自组网中许多应用的重要组成部分而成为研究的热点，它可以充分利用无线通讯的广播特性来加快信息的传播和改善移动节点的能量消耗。在组播中必须保证只有合法的成员才能够发送和接收组播数据，目前最有效的办法就是在组内使用组密钥来加密数据，只有合法的成员才能获得该组密钥。当组成员节点改变时，比如新的节点加入或者成员节点离开时，组密钥必须更新，以保证前向安全性和后向安全性。设计安全、及时和有效的组密钥更新策略是一个关键的问题。

现有的研究表明密钥预分发方案(Key Predistribution Scheme，KPS)提供了切实有效的密钥管理解决办法。KPS 的基本思想是：网络初始化时密钥分发中心(Key Distribution Center, KDC)从密钥集合 S 中为每个节点分发任一子集 $S_i(S_i \subset S)$，相邻节点发现或者计算各自集合间相同的密钥作为共享密钥。KPS 之所以更加适合自组网，一方面它利用对称密钥代替非对称密钥，可以减少计算量；另一方面，这种方式适合网络拓扑无法预知的场景，适应拓扑的变化。因此，采用 KPS 可以使得自组网密钥的管理更加高效。在自组网中开发基于 KPS 的策略需要考虑以下的因素：(1)连通性：节点在通讯范围内，要能够利用共享密钥和其他节点通讯；能够安全通讯的节点越多，连通性则越好。(2)抗合谋：当一定数量的节点被敌人捕获时，其他节点必须仍然是安全的，即：一定数量节点的合并不能够覆盖或者计算出其他合法的节点的密钥。

本文提出了基于填充设计的组密钥更新策略(t-Packing Design based Group Rekeying Scheme，PDGRS)。利用预分发密钥进行组密钥更新管理，采用组合设计中的填充设计进行密钥预分发，使得网络模型具有 CFF(Cover-Free Family)性质，能够提高自组网抗节点合谋的能力，同时由于策略更新了预分发的密钥，因此可以避免更多节点的合谋；增加了节点的共享密钥连接度，增强了共享密钥图的连通性，密钥的更新效率更高。

2 数学背景及相关定义

无覆盖集的族(CFF)最早是 Kautz 和 Singleton[1]为了研究重迭编码(superimposed coding)而引入的，并逐步应用于

2007-01-09 收到，2007-10-29 改回
国家自然科学基金项目(60502047)和福建省教育厅科技项目(JB06093)资助课题

信息论、组合论、组测试(group testing)和防诬陷码等领域，其定义[2]如下：

定义 1　集合系统 (X,F) 称为是 $(r;d)$ 无覆盖集的族（$(r;d)$ -CFF），若对任何 r 个子集 $A_1,A_2,\cdots,A_r\in F$ 和任何其它子集 $B_0\in F$，则有 $\left|B_0\setminus\bigcup_{j=1}^{r}A_j\right|>d$。

定义 1 描述了当 $d\geq 0$ 时，B_0 至少有 d 个元素不被其他 r 个子集覆盖。利用组合设计可以构造 $(r;d)$-CFF，以下给出 t 填充设计(packing design)和其他相关的定义：

定义 2　一个 t-(v,k,λ) 填充设计是一个集合系统 (X,F)，其中 $|X|=v$，对 F 中的每个 $\boldsymbol{B}$，有 $|B|=k$，且 X 的每个 t-子集至多出现在 F 中的 λ 个区组中。

定义3　元素取自于符号集 S 的 $k\times v^t$ 阵列 $\boldsymbol{A}$ 称为符号个数为 $|S|=v$，强度为 t，指标为 λ 的正交阵列(对某个 t，$0\leqslant t\leqslant k$)，若 S 上的每个 t-向量恰好在 A 的每个 $t\times v^t$ 子阵列中出现 λ 次。该正交阵列用符号 $\mathrm{OA}_\lambda(t,k,v)$ 来表示。当 $\lambda=1$ 时，表示为 $\mathrm{OA}(t,k,v)$。

定义 4　以 1，2，…，n 为元素(也可用别的 n 个记号来代替)，而且每行以及每列中的元素又都互不相同的 n 阶方阵，叫做一个 n 阶拉丁方。

当 n 为素数或者素数幂时，可以得到 n–1 个 n 阶拉丁方完全组。

3　基于填充设计的组密钥更新策略

3.1 网络假设和基本思想

假设存在 N 个节点的自组网，节点间需要对称密钥来加密和传播组密钥，部署前每个节点基于填充设计预分发得到一串密钥 R，部署后相邻节点间通过安全共享密钥发现协议寻找密钥串中相同的密钥作为共享密钥并进行安全的通讯，当节点加入或者成员节点离开时，更新节点的组密钥以保证前向和后向安全性，同时更新节点的预分发密钥。

3.2 符号和映射

策略所用到的一些符号和相关约定如表 1 所示。

表 1 符号表示和约定

N	自组网节点个数	$H(x,y)$	密钥计算函数
n	邻居节点个数	$E_k(\mathrm{meg})$	用密钥 k 加密信息 meg
P	密钥池	$\{f_i\}$	伪随机函数簇
p	密钥池中的密钥	R_u	节点 u 的密钥串
q	素数或素数幂	m	节点的密钥个数

3.3 策略的描述

3.3.1 密钥预分发阶段　网络初始化时，在线组管理器生成含有 q 个密钥的密钥池 P，且和有限域 $\mathrm{GF}(q)$ 的元素一一对应，即 $P=\{p_i\mid i\in\mathrm{GF}(q)\}$，区组的元素个数 k，根据以下步骤构造填充设计：

(1)构造 n 阶正交拉丁方。

定理 1[3]　设 a 为 n 阶有限域 $\mathrm{GF}(n)$ 的一个元根，则有方阵

$$\boldsymbol{B}_{i+1}=\begin{pmatrix}0 & 1 & a & \cdots & a^{n-2}\\ a^i & 1+a^i & a+a^i & \cdots & a^{n-2}+a^i\\ a^{i+1} & 1+a^{i+1} & a+a^{i+1} & \cdots & a^{n-2}+a^{i+1}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ a^{i+n-2} & 1+a^{i+n-2} & a+a^{i+n-2} & \cdots & a^{n-2}+a^{i+n-2}\end{pmatrix}$$

其中 $i=0,1,\cdots,n-2$，构成 n 阶正交拉丁方完全组。

(2)利用正交拉丁方构造正交阵列，这里的方法类似文献[3]。

(3)利用正交阵列构造填充设计。假设 $(y_0,y_1,\cdots,y_{k-1})$ 是正交阵列 $\mathrm{OA}(t,k,v)$ 中的一列，定义一个新的区组 B 为 $\{(0,y_0),(1,y_1),\cdots,(k-1,y_{k-1})\}$，则可以得到 t-$(kv,k,1)$ 填充设计。

然后，组管理器分发给每个节点以下信息：

信息 1　从填充设计的结果中，根据节点的 ID 选择其对应的区组 $B=\{(j,i)\mid j=0,1,2,\cdots q;i\in\mathrm{GF}(q)\}$，按照式(1)计算相应的密钥串 $R=\{k_j\mid j=0,1,\cdots q\}$ 并发给节点。

$$k_j=H(j,p_i),(j,i)\in B \tag{1}$$

信息 2　每个节点得到初始的组密钥 k_g。

3.3.2 共享密钥产生阶段　节点获得密钥串后，部署在不同的地理位置。邻居节点间利用安全共享密钥发现协议(Secure Shared Key Discovery，SSD)[4]寻找相同的密钥作为共享密钥。SSD 协议利用保密同态(Privacy Homomorphism，PH)加密算法来发现相邻节点的共享密钥，不泄漏其他密钥的信息。

3.3.3 节点离开阶段　设当前的组密钥为 k_g，当节点变化时，假设节点 u 离开组，R_u 中包含的密钥和组密钥 k_g 都是不安全的，为了保证后向安全性，采取以下步骤：

(1)组管理器从剩下的节点所包含的安全的密钥中选择 l 个密钥 $\{k_1,k_2,\cdots,k_l\}$，并生成新的组密钥 $k_g^{'}$，然后向所有节点广播消息：

$$\text{组管理器}\rightarrow *:\mathrm{ID}_u,\{E_{k_1}(k_g^{'}),E_{k_2}(k_g^{'}),\cdots,E_{k_l}(k_g^{'})\},f_{k_g^{'}}(0) \tag{2}$$

(2)拥有 $\{k_1,k_2,\cdots,k_l\}$ 中任何一个密钥的节点，都可以解密出新的组密钥 $k_g^{'}$；否则，可以通过共享密钥从邻居节点获得 $k_g^{'}$。而节点 u 不包含任何一个解密密钥因此无法得到 $k_g^{'}$，同时组管理广播的消息中包含了 u 的标识符 ID_u，也无法从邻居节点获得 $k_g^{'}$。

(3)每个节点 v 得到新的组密钥 $k_g^{'}$ 后，计算 $f_{k_g^{'}}(0)$ 并判断是否等于消息(2)中的 $f_{k_g^{'}}(0)$ 以验证组密钥的合法性。如果相等，则更新所有的 $k_i\in R_v$ 为 $k_i^{'}=f_{k_i}(0)$，若 $k_i\in R_u$，则更新为 $k_i^{'}=f_{k_i}(k_g^{'})$，新的密钥集合记为 $R_v^{'}$。

(4)节点更新成功后，删除旧的组密钥 k_g。

在步骤(1)中，组管理器选择的 l 个密钥可以是其附近大

部分节点所包含的安全密钥，作为新的组密钥的加密密钥。当节点的共享密钥连接度较高时(详细分析见 4.2 节)，组密钥能够快速分发给网络组成员节点。

4 安全与性能分析

4.1 安全分析

PDGRS 策略的安全性除了表现在前向和后向安全性之外，基于填充设计使得策略的数学模型具有 CFF 性质。

定理 2 若存在一个正交阵列 OA(t,k,v)，则存在含有 v^t 个区组的 t-$(kv, k, 1)$填充设计。

定理 3[2] 若存在一个有 b 个区组 t-$(v,k,1)$ 填充设计，则存在$(r;d)$-CFF(v,b)，这里 $r=\lfloor(k-d-1)/(t-1)\rfloor$。

在 PDGRS 策略中，q 为素数或者素数幂，可以得到 q–1 个 q 阶拉丁方完全组。根据定义 1 和以上定理可以得到如下的推论：

推论 1 若 q 是一个素数或者素数幂，且 $t<q$，则存在正交阵列 OA(t,k,q)，因而存在含有 q^t 个区组的 t-$(kq, k, 1)$ 填充设计，所以存在 $\left(\left\lfloor\frac{k-d-1}{t-1}\right\rfloor,d\right)$-CFF$(qk,q^t)$，其中 $k\le q+1$。当 $k=q+1$ 时，即得到：$\left(\left\lfloor\frac{q-d}{t-1}\right\rfloor,d\right)$-CFF (q^2+q,q^t)。

推论 2 在 PDGRS 策略中，当合谋节点的个数不超过 r 个时，任何其他合法节点的密钥都无法被完全覆盖。

图 1 描绘了节点存储的密钥个数和抗合谋节点个数的关系曲线图。从图中可以观察到，和其他策略[5−8]不一样的是随着节点密钥量的增加，PDGRS 策略的抗合谋节点个数增加，并基本成正比。而在 GKMPAN 策略[8]中，在节点覆盖率 0.01%不变的情况下，随着节点存储的密钥个数的增加，抗合谋节点的个数越来越少。

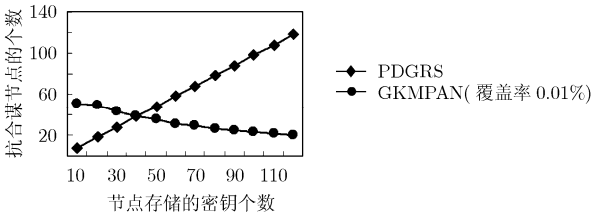

图 1 节点密钥数量和抗合谋节点个数关系图

此外，和其他策略[5−7]比较，PDGRS 策略的安全性更体现在，由于更新了预分发密钥，使得先后离开的节点无法累加合谋，只要保证两次更新之间合谋的节点数量不超过一定数量 r，则策略将保持较高的安全性。而大部分策略由于没有及时更新预分发密钥，一段时间后合谋的节点达到一定的数量时，策略的安全性将大大降低。

4.2 共享密钥连接度

以网络节点作为顶点，以相邻节点间是否有共享密钥作为边画出图，称为共享密钥图，节点的度称为共享密钥连接度。为了保证策略是高效的，组密钥能够快速分发给组成员节点，任何组成员节点都能够安全的收到其他组成员节点发出的信息，不出现孤立的情况，需要共享密钥图以较高的概率(称为全局连通性，记为 P_c)保持连通，Erdos 和 Renyi[9]表明了 P_c 和节点数量 N、节点共享密钥连接度 d 的关系：

$$d=\frac{(N-1)}{N}\left[\ln(N)-\ln\left(-\ln\left(P_c\right)\right)\right] \tag{3}$$

当给出一定的分布密度的网络时，设 n 为节点一跳通讯范围内的邻居节点数量，则节点需要的共享密钥连接概率(简称连接概率)为 $P_{\text{required}}=d/n$，即有 $d=P_{\text{required}}n$，可见增加 d 或者 p_{required} 都可以提高 P_c。

根据定义 2，PDGRS 策略中节点的平均共享密钥连接度为 bk/v，任意两个节点至少含有一个相同密钥的实际平均概率(称为实际连接概率)为

$$P_{\text{actual}}=\frac{bk/v-1}{b-1}\cdot k=\frac{k(bk-v)}{v(b-1)}=\frac{k}{q+1} \tag{4}$$

为了使得共享密钥图以较高的概率 (P_c) 保持连通，必须要 $P_{\text{actual}}\ge P_{\text{required}}$。由式(4)观察到，在 q 不变时，通过增加节点的密钥量 k 可以提高节点间的实际连接概率。当 k=q+1 时，P_{actual}=1，即任意两个节点至少含有一个相同的密钥。

对 PDGRS 和 GKMPAN 策略中节点的实际连接概率进行了比较(图 2)，取有限域 GF(113)，在两种策略密钥池的密钥量相同的情况下，随着节点密钥量的增加，PDGRS 策略的连接概率更高，可见，和 GKMPAN 策略比较，PDGRS 的共享密钥图的连通性更强。

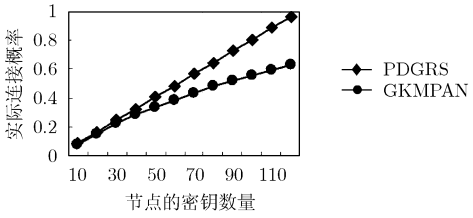

图 2 节点密钥数量和连接概率的关系图

然而，节点的连接概率受到存储量的限制，因此在存储量有限的情况下，可通过直接增加共享密钥连接度 d 来提高 P_c。在 PDGRS 策略中，节点通过已经和自己建立共享密钥的节点在二跳通讯范围内和其它更多的节点建立共享密钥。

5 结束语

本文的重点在于研究如何进行自组网中开放、重要的组密钥的更新。采用拉丁方构造 t 填充设计，基于 t 填充设计预先分发密钥，并利用共享密钥作为组密钥更新的加密密钥。分析表明策略的数学模型取得 CFF 性质，满足前向和后向安全性，抗合谋性和连接度都随着节点的密钥量的增加而提高，同时，由于更新了预分发密钥，策略的安全性得到

了进一步加强。

参 考 文 献

[1] Wagner D. Cryptanalysis of an Algebraic Privacy Homomorphism. in ISC2003, Lecture Notes in Comput. Sci., Vol. 2851, Springer-Verlag, Berlin, 2003: 234–239.

[2] Li P C, van Rees G H J, and Wei R. Constructions of 2-cover-free families and related separating hash families. J. of Combinatorial Designs, Published Online, 2006, 14: 423–440.

[3] Yang Z X. Construction of Orthogonal Arrays. Jinan: Shandong People Press, 1978: 110–128.

[4] Chan A C-F. Distributed symmetric key management for mobile ad hoc networks. IEEE INFOCOM, 2004, 4: 2414–2424.

[5] Chan H, Perrig A, and Song D. Random key pre-distribution schemes for sensor networks. IEEE Symposium on Security and Privacy, Berkeley, 2003: 197–213.

[6] Du W, Deng J, Han Y S, and Varshney P K. A pairwise key pre-distribution scheme for wireless sensor networks. Proc. of the 10th ACM conf. on Computer and communications Security, Washington, ACM Press, 2003: 42–51.

[7] Sung Jin Choi and Hee Yong Youn. An efficient key pre-distribution scheme for secure distributed sensor networks. EUC 2005 workshops, LNCS 3823, Berlin, Springer-Verlag, 2005: 1088–1097.

[8] Zhu S, Setia S, Xu S, and Jajodia S. GKMPAN: An efficient group rekeying scheme for secure multicast in Ad-hoc networks. In Proc. of International Conference on Mobile and Ubiquitous Systems: Networking and Services, Boston, 2004: 42–51.

[9] Erdos P and Renyi A. On Random Graphs I. Publications mathematicae, Debrecen, 1959: 290–297.

陈建伟：　男，1980 年生，硕士生，研究方向为无线 Ad hoc 网络、网络与信息安全.

许　力：　男，1970 年生，博士，副教授，主要研究方向为无线网络与移动计算、网络与信息安全.

黄丹芸：　女，1983 年生，硕士生，研究方向为组合数学.