分簇无线传感器网络中基于横截设计的对密钥建立方案

许　力　　章红艳　　沈金波
(福建师范大学网络安全与密码技术福建省高校重点实验室　福州　350007)

摘　要：由于节点能量有限、存贮空间小等特点，使传统的网络密钥管理方案受到挑战。该文基于横截设计、双变量多项式和门限机制，提出了适用于分簇结构传感器网络的对密钥建立方案和多路径密钥建立策略。该方案采用横截设计保证同簇内节点可以直接建立对密钥，而不同簇的节点可以基于门限机制构建多路径密钥。理论和实验分析表明，新方案在增强安全性、连通性和抗毁性的同时，有效地降低了通信量及密钥存储量等代价，并且具有良好的可扩展性。

关键词：密钥预分发；横截设计；双变量多项式；多路径密钥
中图分类号：TP393；TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)07-1600-06

Pair-wise Key Establishment Scheme Based on Transerval Design in Clustered Sensor Networks

Xu Li　　Zhang Hong-yan　　Shen Jin-bo
(*Key Lab of Network Security and Cryptology*, *Fujian Normal University*, *Fuzhou* 350007, *China*)

Abstract: Due to the limited energy, small storage room and so on, the traditional network key management scheme is challenged. Based on the transerval design，bivariable polynomial and threshold strategy, a new pairwise key establishment scheme and multi-path key construction strategy suit to clustered wireless sensor network is proposed. By this scheme and transerval design, the nodes in the same cluster can directly construct pair-wise key and the nodes in the different clusters can construct path key based on threshold strategy. Theory and simulation analysis indicate that the new scheme can not only increase the security, connectivity and vulnerability, but also decrease the communication overload and storage cost. The scalability is another good character.

Key words: Key pre-distribution; Transerval design; Bivariable polynomial; Multi-path key

1　引言

无线传感器网络(Wireless Sensor Networks, WSN)[1]集微机电技术、传感器技术、通信技术于一体，可广泛应用于教育、军事、医疗、交通等诸多领域，拥有巨大的应用潜力和商业价值，引起了国内外广泛的关注和研究。安全是WSN最基本的一项服务，特别当WSN部署在无人触及或容易受损或被俘获的环境时，保证WSN的安全性更是应该优先考虑的问题。以提供安全、可靠的保密通信为目标的密钥管理是WSN安全研究最为重要、最为基本的内容之一，它是安全路由、安全定位、安全数据融合及针对特定攻击的解决方案等的基础。

由于传感器网络的能量、计算能力和通信带宽等方面的限制，不宜采用公钥密码体制，应采用对称加密算法。在传统网络中使用的基于可信第三方的密钥分配协议也不适用于传感器网络。目前普遍认为可行的密钥分发机制是采用密钥预分发(Key Pre-distribution Scheme, KPS)。Eschenauer等人提出了一种随机密钥预分发方案RKPS[2]，网络节点在部署前，从密钥池中随机选取一定数目的密钥子集，称之为密钥链，子集的大小称为密钥链的长度。节点部署到指定区域后，通信双方在各自的密钥子集中寻找相同的密钥。在此方案基础上Chan等提出了q重随机密钥预分发方案q-RKPS[3]。两种方案不同之处为：前者方案每对节点只能找到一个共同密钥，而后一种方案中，每对节点可以找到至少q个共同密钥。Camtepe等提出了基于组合设计的对密钥预分发方案CDKDM[4]，此方案利用了组合设计理论中的区组设计技术，利用n阶的射影平面构造参数为$(n^2+n+1, n+1,1)$的对称平衡不完全区组设计，能支持n^2+n+1个节点的网络，每个节点的密钥链的长度为$n+1$，任意两个节点之间一定存在一个共同的密钥，其优点为，任意两个节点有共同密钥的概率为1，缺点在于密钥链的长度太长，当有一个节点被捕获时，破坏的链路为$1/n$。Deng等人提出了双变量多项式的对密钥建立方案[5]，利用双变量多项式的对称性，其优点是任意两个节点可以建立对密钥，缺点

2008-05-08 收到，2009-03-16 改回
国家自然科学基金(60502047)，福建省教育厅重点项目(JA07030)，福建省高等学校新世纪优秀人才支持基金(FM035)和福建省自然科学基金项目(2008J0014)资助课题

是密钥的抗毁性是苦于计算复杂度的代价。Farshid等人提出了多变量多项式密钥预分发方案[6],每个节点拥有唯一的n唯的ID，在此基础上，每个节点在部署之前存储多变量多项式的共享份额，节点部署之后，节点和在通信范围内的邻居节点通信，若他们之间的海明距离为1，则有n–1个共同密钥，而通信密钥为这n–1个密钥的组合。

我们认为[7],在传感器网络中研究 KPS 的策略，需要全面考虑以下的因素：

(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。

(3)节点数量：采用某种密钥预分发方案，网络最多能够支持多少个节点。

(4)存储量：由于网络节点资源的限制，节点的存储量有限，分发给节点的密钥量要小。

本文在Deng方案[5]的基础上，结合组合设计的思想，引入横截设计和双变量多项式密钥池，提出了基于横截设计的KPS方案TDKPS(Transerval Design based KPS), 该方案降低了对密钥建立的计算复杂度，增强了密钥的连通性，提高了安全性和抗毁性。

2　方案描述

无线传感器网络一般有两种拓扑结构：平面结构和分级结构。平面结构的网络中所有节点是对等的，原则上不存在瓶颈，所以比较健壮。但是，其最大的缺点就是网络规模受限，路由维护开销大，能耗也比较大。分级结构中网络被划分成簇，每个簇由一个簇头(也称锚节点)和多个簇成员组成，因此也称为分簇结构。簇头节点形成高一级的网络，负责簇间数据的收集和转发。采用簇结构可以减少传输产生的能量开销[8]，便于对簇内节点进行管理，有利于网络扩展。目前在无线传感器网络领域研究的拓扑结构主要都是基于分簇结构。

2.1 网络模型和假设

为了便于描述，我们假设传感器网络中共有n^2个节点，n为奇数。通过分簇算法把网络分成若干个簇，对每个簇成员进行标识。节点的身份用一个二维数组(i,j) $(0\le i,j\le n-1)$表示，其中i表示节点处于第i个簇，j表示节点是这个簇内的第j个节点。表 1 给出横截设计和密钥预分发的表示符和对应关系。

表 1 横截设计和密钥预分发映射关系

符号	横截设计	密钥预分发
v	元素的集合	密钥池
$\|v\|$	元素集合的大小	密钥池的大小
b	区组个数	网络中节点的个数
k	区组长度	节点拥有的多项式的个数
(x_i,x_j)	区组中的点	多项式的标识

2.2 密钥预分发阶段

密钥分发中心随机的选取有限域GF(q)上的次数为 t 的双变量多项式集合Γ 构成k个密钥空间，每个空间有n个多项式。为了区分这些多项式，每个多项式有一个唯一的标识(i',j')，$(0\le i'\le k-1,$ $0\le j'\le n-1)$，这里i'表示此多项式属于第几个多项式密钥空间，j'表示此多项式是密钥空间中的第几个多项式。

步骤 1　构造一个TD(k,1;n)设计。

定理 1　设 n 是素数，且$2\le k\le n$，则存在横截设计TD(k,1;n)。

设$X=\{0,1,2\cdots,K-1\}\times\mathbb{Z}_n$，对$0\le x\le k-1$，定义$H_x=\{x\}\times\mathbb{Z}_n$，$H=\{H_x:0\le x\le k-1\}$。

对任意的$(i,j)\in\mathbb{Z}_n\times\mathbb{Z}_n$，定义区组$B_{i,j}=\{(x,$ $xj+i \bmod n):0\le x\le k-1\}$，$B=\{B_{i,j}:(i,j)\in\mathbb{Z}_n$ $\times\mathbb{Z}_n\}$，则有$b=n^2,v=kn,r=n$。

步骤 2　中心计算节点应该分配的多项式

对任意的节点$\mathrm{ID}_{ij}=(i,j)$，根据横截设计的构造方法计算出区组$B_{i,j}=\{(x,xj+i \bmod n):0\le x\le k-1\}$，区组中的点就是对应的多项式的标识。中心选取出区组$B_{i,j}$中相对应的多项式，并根据其ID_{ij}计算$f_{rc}(\mathrm{ID}_{ij},y)=\sum_{i=0}^{t-1}\sum_{j=0}^{t-1}a_{ij}x^iy^j=\sum_{j=0}^{t-1}b_jy^j$，其中$b_j=\sum_{i=0}^{t-1}a_{ij}x^i,0\le r\le n-1,0\le c\le n-1$。

步骤 3　中心将$f_{rc}(\mathrm{ID}_{ij},y)$分发给节点$\mathrm{ID}_{ij}$。每个节点接收到$k$个多项式。

2.3 共享密钥建立阶段

当节点获得相应的多项式后，判断节点之间是否有共享多项式。假设为节点$A(i_1,j_1)$和节点$B(i_2,$ $j_2)$，它们可以通过下面的步骤确定是否有公共的多项式，然后建立对密钥。

(1)如果$j_1=j_2$，则两节点没有共同的多项式；

(2)如果$i_1=i_2$，则两节点的共同多项式为$(i_1,0)$；

(3)如果 $j_1 \neq j_2$，则计算 $i' = \dfrac{i_2 - i_1}{j_1 - j_2} \bmod n$。如果 $0 \le i' \le k-1$，则两节点共同的多项式为 $(i', i' \cdot j + i \bmod n)$。如果 $i' \ge k$，则两节点没有共同的多项式。

2.4 路径密钥建立阶段

2.4.1 基于最短跳数的路径密钥建立方案 不同簇并且没有共同多项式的节点我们可以采用路径密钥的方式来建立它们的对密钥。

定理 2 网络中的任意两个节点，在密钥图中至多两跳就可以建立对密钥。

证明 设 X 和 A 是 TD$(k,1;n)$ 的点的集合和区组的集合。由此可知 $k \le n+1$。

当 $k = n+1$ 时，任意两个区组都相交。即，任意节点之间有共同的多项式可以直接建立对密钥；

当 $k < n+1$ 时，TD$(k,1;n)$ 有不相交的区组。设 B 和 B' 是两个不相交的区组，则对 $\forall x \in B, x' \in B'$，$x, x'$ 不属于同一组，存在唯一的区组 B^* 同时包含 x和x'。即存在区组 B^* 同时和 B， B' 相交。

因此，网络中的任意两个节点，在密钥图中至多两跳就可以建立对密钥。

定理 3 任意两个节点在密钥图上有 $k(k-1)$ 条密钥路径建立对密钥。

证明 由定理 2 可知对于两个区组中任意不属于同一组的点，都存在唯一区组同时包含这两个点，而区组长度为 k，因此，共有不属于同一组的点对 $k(k-1)$ 个。因此，与两个区组都相交的区组共有 $k(k-1)$ 个。即，任意两个没有对密钥的节点，可以通过这 $k(k-1)$ 个节点建立对密钥。

2.4.2 多路径密钥建立方案 在 E-G 方案中，两个相邻节点 A 和 B 所分配的密钥有可能被分配给其他的节点，若这些节点受损，则 A 和 B 之间的链路会受到安全威胁。

当节点 A 和节点 B 之间需要建立对密钥时，A 将对密钥 k_{AB} 通过秘密共享方案分成 m 份份额，并且寻找与 A 和 B 都有共享密钥的节点作为密钥路径上的节点，然后通过这些中间节点把 k_{AB} 的份额转发给节点 B，B 收到消息后利用门限方案恢复出 k_{AB}。设中间节点为 $C_1, C_2, \cdots, C_{k(k-1)}$，即 $\{C_i \,|\, C_i \cap A \neq \Phi, C_i \cap B \neq \Phi$， $i = 1,2,\cdots,k(k-1)\}$，与节点 A 和 B 都可以建立对密钥，对密钥记为 K_{AC_i} 和 K_{BC_i}，从中选择一部分节点作为路径密钥上的节点。对密钥建立的具体步骤如下：

步骤 1 节点 A 选择一个密钥 k_{AB}，并通过秘密共享方案分成 m 份。具体做法如下：

假定 p 是一个素数，共享的密钥 $k_{AB} \in Z_p$。

(1)节点 A 随机选择一个 $t-1$ 次多项式 $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \in Z_p[x]$，其中 $a_0 = k_{AB}$。

(2)节点 A 在 Z_p 中选择 m 个非零的、互不相同的元素 $x_1, x_2 \cdots x_m$，计算 $y_i = f(x_i)$，$1 \le i \le m$，$y_i\,(1 \le i \le m)$作为 $P_i\,(1 \le i \le m)$的秘密共享。

步骤 2 从 n 个中间节点中选择 m 个节点 C_i，并向 C_i 发送消息 $\{E_{K_{AC_i}}(x_i, y_i), A\}$；

步骤 3 节点 C_i 收到消息后解密消息 $D_{K_{AC_i}}(x_i, y_i)$，并向 B 发送消息 $\{E_{K_{BC_i}}((x_i, y_i), A), C_i\}$；

步骤 4 节点 B 收到消息后解密消息 $D_{K_{BC_i}}((x_i, y_i), A)$，得到 (x_i, y_i)。并利用收到的其他 $t-1$ 个消息恢复出 k_{AB}，$k_{AB} = f(0) = \sum_{s=1}^{t} y_{i_s} \cdot \prod_{\substack{j=1 \\ j \neq s}}^{t} \dfrac{-x_{i_j}}{x_{i_s} - x_{i_j}}$。

3 性能分析

3.1 密钥连通概率

以网络节点作为定点，以相邻节点间是否有共享密钥作为边的图，称为共享密钥图，节点的度称为共享密钥连接度。为了不出现孤立点，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：

$$d = \frac{N-1}{N}[\ln(N) - \ln(-\ln(p_c))]$$

图 1 描述了在不同的网络节点数的情况下，密钥图的连通性要达到 p_c 时，节点需要的最小的 d 的曲线图。当给出一定的分布密度的网络时，设 n' 为节点一跳通信范围内的邻居节点数，则节点需要的共享密钥连接概率为 $p_r = d / n'$。根据定义，TDKPS 方案中的平均密钥共享连接度为 $n(k-1)$，任意两个节点有共享密钥的概率为 $p_{\text{actural}} = k(n-1)/(n^2-1) = k/(n+1)$。

分簇结构下的网络应从两个角度考虑密钥连通性，一种是簇内密钥连通概率，一种是簇外密钥连

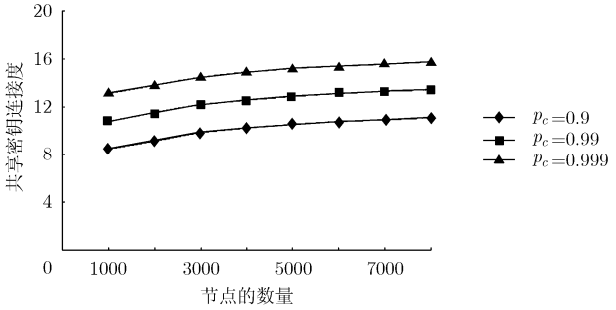


图 1 不同数量节点需要的节点连接度

通概率。簇内的所有节点之间都有共享的多项式因此都可以建立对密钥，即簇内密钥连通概率为 1。

定理 4　不在同一个簇的两个节点可以建立对密钥的概率为 $p_c=\frac{k-1}{n}$。

证明　由横截设计的定义知，区组中任意一点出现 n 次，区组长度为 k，因此，和某个区组相交的区组个数为 $k(n-1)$，而本簇中共有 n 个节点。因此，不同簇的两个节点可以建立对密钥的概率为 $p_c=\frac{k(n-1)-(n-1)}{n^2-n}=\frac{k-1}{n}$。即不同簇节点的密钥连通概率和节点拥有的多项式数量成正比。

我们对 TDKPS，E-G 和 PRKP[10]方案的实际密钥连通概率进行了比较，其中 $n=101$。如图 2，在 3 种方案密钥池的密钥量相同的情况下，随着节点密钥量的增加，TDKPS 方案的密钥连通概率更高。和其它两种方案相比，TDKPS 方案的密钥图的连通性更好。

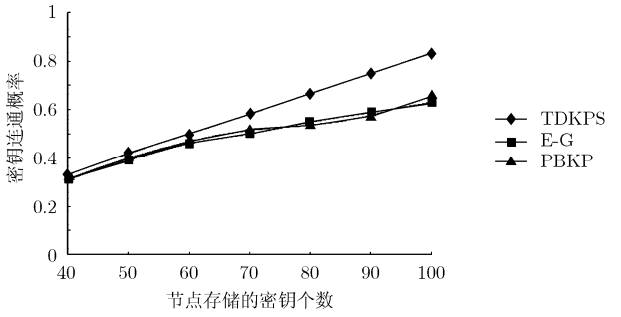


图 2 密钥连通概率比较

3.2 安全性分析

当一个节点和另一个节点建立对密钥时，若是同簇节点，之间一定共享一个多项式，因此，可以计算出对密钥。若非同簇节点，只通过 2.3 节的方法可以确定是否具有共同的多项式，若有则可以计算对密钥。通过此方法，节点只知道和其它节点共享哪个多项式，无法知道其它节点还拥有哪些多项式，因此，节点被捕获后，不会泄漏其它节点拥有多项式的情况。

传感器网络中共有 n^2 个节点，设有 N_x 个节点被捕获。由双变量多项式的性质可知，要恢复多项式至少于需要 t 个秘密份额。因此，当被捕获的节点的数目 N_x 小于 t 时无法恢复出任何一个双变量多项式，即所有的信息都不会泄漏。当被捕获节点的数目 N_x 大于 t 时，某个多项式泄漏的概率为 $p=1-\sum_{i=0}^{t-1}\frac{N_x!}{(N_x-i)!i!}\left(\frac{1}{n}\right)^i\left(1-\frac{1}{n}\right)^{N_x-i}$。

图 3 表明，随着被捕获的节点的数量增加密钥连通概率减小，在被捕获节点数量小于 6000 时，TDKPS 方案的连通概率较高，但是，当被捕获节点的数量继续增加时，TDKPS 方案的密钥连通概率小于 E-G 方案。也就是说，在一定的阈值内 TDKPS 方案优于 E-G 方案。图 4 表明当节点被捕获时 TDKPS 方案受影响的安全链路要比 E-G 方案少，比 PBKP 方案略少，因此 TDKPS 方案的抗毁性最佳。

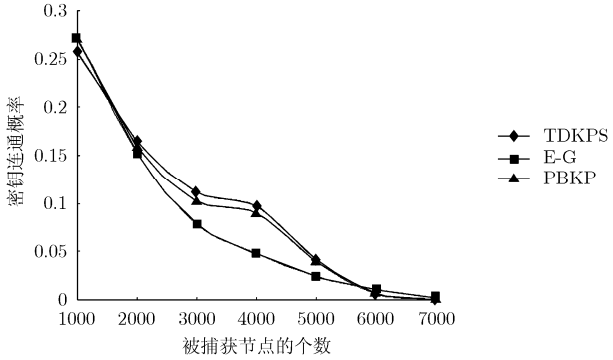


图 3 被捕获节点和密钥连通概率的关系图

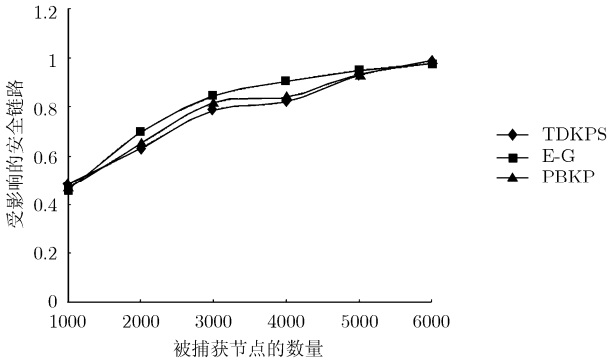


图 4 抗毁性分析与比较

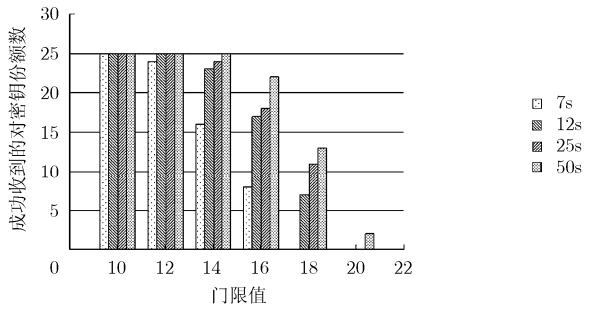
3.3 多路径密钥建立方案分析

我们利用 NS2 来进行仿真实验，取 n=23，假设网络当中恶意节点占整个网络的 5%，恶意节点可能不转发数据包或者丢弃包，但不篡改信息。我们对同一个场景进行仿真，取 100 次仿真结果数据求平均值。具体参数设置如表 2 所示。

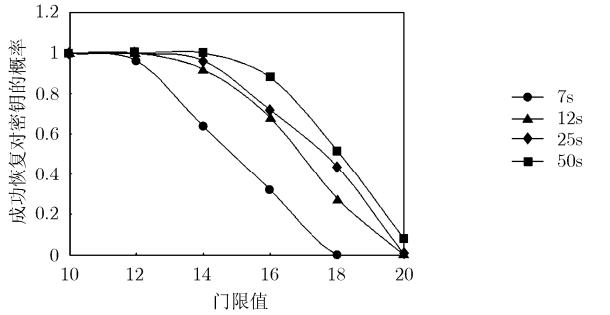
表 2 模拟参数设置

参数	含义	缺省值
Tx-range	无线传输距离	500 m
Length	区域长度	Sqrt(num*3.14*500*500/14)
Width	区域宽度	Sqrt(num*3.14*500*500/14)
k	门限值的取值	10 12 14 16 18
T_w	收到门限个值的最大有效时间	50 s

3.3.1 门限值对成功恢复对密钥的影响 由秘密共享方案的性质可知，秘密共享份额越多密钥就越安全。但是当门限值 t 较大时，需要很多的中间节点转发，这会增大通信代价和能量消耗。而且中间恶意节点的丢包使目标节点在有限时间内收到 t 个份额的概率就会降低，延时增大。由图 5 可以看出，当门限值较小时，成功恢复对密钥的概率较大同时所耗时间却较少，随着门限值的增大，在有效时间内成功恢复出门限值的概率降低且即使能够恢复出对密钥，所消耗的时间也大大的增加。



(a)成功收到的对密钥份额



(b)基于门限值的成功恢复对密钥概率

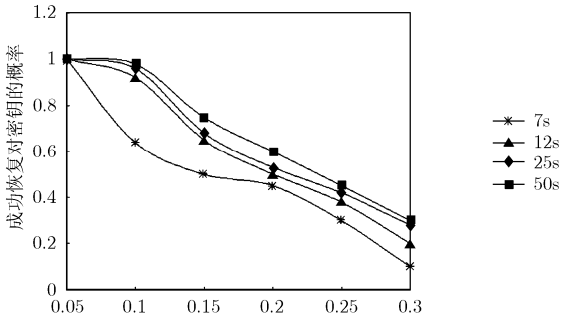
图 5 门限值与成功恢复密钥的概率的关系图

3.3.2 对中间节点的攻击对成功恢复对密钥的影响

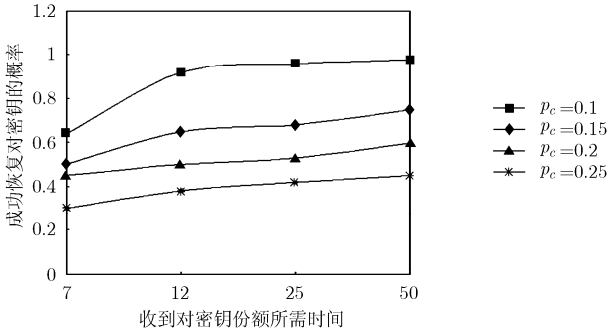
中间节点是否是恶意节点，对能否快速成功的恢复对密钥有很大的影响。由图 6(a)可以看出，当中间节点中恶意节点的个数增加时成功恢复对密钥的概率随着减小，当恶意节点的个数达到 30%时，成功恢复对密钥的概率下降到 10%。图 6(b)中可以看出随着恶意节点的数量不断增多，收到份额的时间也随着增加，并且成功恢复对密钥的概率减小。由此可见，节点是否是恶意节点对成功恢复出对密钥产生巨大的影响。因此，可以采取有效的策略[11]选择一些可信度较高的节点作为中间节点。中间节点的选择还可以通过对节点的可信度、位置、能量等因素综合起来考虑，选择出最适合的节点。

4 结束语

本文的研究重点在于在分簇结构下如何进行密钥预分发，把分簇和横截设计很好的结合在一起，提出了基于横截设计的密钥预分发方案，通过理论分析表明在相同的传感器网络规模和存储相同数量的多项式的情况下，新方案有较高的密钥连通概率。实验表明，当受损节点较少时，抗毁性优于 E-G 方案和 PBKP 方案，但是当受损节点超过一定的阈值时，本方案的链路受损数量比 E-G 方案大。同时，本文在预分发密钥的基础上提出了两种路径密钥建立方案。并进行了详细的试验分析，对该领域的后续研究提供了一些借鉴。



(a)基于恶意节点个数的密钥恢复概率



(b)基于收到密钥时间的密钥恢复概率

图 6 恶意节点的百分比对成功恢复对密钥的影响

参 考 文 献

[1] Akyildiz F, Su W, Sankarasubra maniam Y, and Cayirci E. Wireless sensor network: A survey. *Computer Networks*, 2002, 38(4): 393–422.

[2] Eschenauer L and Gligor V. A key management scheme distributed sensor network. Proceeding of the 9th ACM Conference on Computer and Communications Security, Washington. New York: ACM Press, 2002: 41–47.

[3] Chan H and Perrig A, *et al*.. Random key predistribution schemes for sensor networks. Proceeding of the 2003 IEEE Symposium on Security and Privacy, Berkeley, California. IEEE Computer Society, 2003: 197–213.

[4] Camtepe S A and Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. Proceeding of 9th European Symposium On Research in Computer Security, Berlin. Springer-Verlag, 2004: 293–308.

[5] Hongmei Deng and Anindo Mukherjee, *et al*.. Threshold and identity-based key management and authentication for wireless ad hoc networks. Porceeding of international conference on information technology: coding and computing(ITCC'04), Washington. IEEE Computer Society, 2004, 2: 107–111 .

[6] Farshid delgosha and Faramarz fekri. Threshold key-establishment in distributed sensor networks using a multivariate scheme. Proceeding of 25th IEEE International Conference on Compute Communications, Barcelona, Catalunya, Spain. April, 2006: 1–12.

[7] Chen Jiangwei, Xu Li, and Mu Yi. A new group Rekeying scheme based on t-packing designs for Ad hoc networks. Proceeding of the 2nd international conference on Scalable information systems, Suzhou, China, ACM Press, 2007, 304: 110–115.

[8] 许力, 郑宝玉. MANET 环境下基于能量保护的路由策略及其研究进展. 电子与信息学报, 2005, 27(5): 827–834.
Xu Li and Zheng Bao-yu. Surey of energy conservation based routing strategy in MANET. *Journal of Electronics & Information Technology*, 2005, 27(5): 827–834.

[9] Erdos P and Renyi A. On random graph. Published in Mathematics. Debrecen. Hungary, 6. 1959: 290–297.

[10] Liu D and Ning P. Establishing pairwise keys in distributed sensor networks. Proceeding of the 10th ACM Conference on Computer and Communications Security, Washington. New York: ACM Press, 2003: 52–61.

[11] 章静, 许力, 黄榕宁. 自组网中基于可信度的分簇策略. 第二届中国可信计算与信息安全学术会议, 中国石家庄. 武汉大学学报(理学版), 2006, 52(S1): 1–4.
Zhang Jing, Xu Li, and Huang Rong-ning. Trust evaluation-based clustering algorithm in an ad hoc network. Proceeding of 2nd China Trusted Computing and Information Security Conference, Shijiazhuang, China. *Journal Wuhan University*(*Natural Science Edition*), 2006, 52(S1): 1–4.

许　力：　男，1970 年生，博士，教授，主要研究方向为无线网络与移动计算、网络安全和网络优化等.