# Ad hoc网络密钥预配置方案

张学锋[1]，刘 斌[2]，姜皇普[3]

(1. 邢台市广播电视大学教务处 河北 邢台 054000; 2. 建材职业技术学院信息机电系 河北 秦皇岛 066004;
3. 燕山大学信息科学与工程学院 河北 秦皇岛 066004)

【摘要】为了减少Ad hoc网络密钥管理方案对网络资源、节点资源的依赖，同时提高网络的安全性能，该文深入研究了传感器网络中基于多项式的密钥对预配置方案，将门限机制引用到密钥的传输过程当中，设计出一个应用于Ad hoc网络的高效密钥预配置方案：基于门限机制的密钥预配置方案。通过分析可以看出该方案有一些优良的特性，包括两节点间能以很高的概率成功建立密钥对、对入侵有较强的鲁棒性、高连通性、低通讯量。

关 键 词 Ad hoc网络; 二变量t度多项式; 密钥管理; 密钥预配置
中图分类号 TP393 文献标识码 A

# Threshold-Based Key Predistribution in Ad hoc Network

ZHANG Xue-feng[1]，LIU Bin[2]，JIANG Huang-pu[3]

(1. Educational Administration Office, Xingtai Radio & TV University Xingtai Hebei 054000;
2. Department of Information and Electricity, Vocational & Technical College of Building Materials Qinhuangdao Hebei 066004;
3. College of Information Science and Engineering, Yanshan University Qinghuangdao Hebei 066004)

**Abstract** To cut down the dependent of key management scheme on resource of networks, this paper deeply researches polynomial-based key predistribution in distribution sensor networks for reference and presents an efficient key predistribution scheme for Ad hoc networks, a threshold-based key predistribution scheme. The analysis in this paper indicates that this scheme has a number of good properties, such as high probability to establish pairwise keys, tolerance of node captures, and low communication overhead.

**Key words** Ad hoc networks; bivariate t-degree polynomial; key management; key predistribution

传统的比较流行的认证结构包括Kerberos、标准X.509和PKIX。在Kerberos、X.509、PKIX标准中两个认证实体通过一个全球可信的认证中心(CA)来实现相互间的认证[1]。虽然在一个有线网络里这种架构可以发挥很好的作用，但是在大规模的Ad hoc无线网络里却行不通，主要有以下几个原因。

集中式的解决方案通常扩展性不是很强。当那些CA服务器受到攻破或者机器瘫痪时，整个系统都不能用。频繁的结点移动引起频繁的相互认证，从而使得可扩展性的问题不能很好的解决，并且极有可能造成服务器周围的信道严重阻塞。高动态性使得路由要频繁的变化，从而使得实时的定位这些服务器和联系这些服务器变得非常繁琐。通过很容易出错的无线信道来进行的多跳通信经常出现很高的丢包率和平均延迟。层次性的CA服务器和服务器代理的很多变体[2]可以在一定程度上缓解上面的问题，但是不能解决随时随地服务的可用性和强壮性。

近年来，随着传感器[3]网络应用的日益广泛，很多传感器网络中的密钥管理方案也被提出来。文献[4]提出了基于概率的为建立成对的会话密钥的密钥预配置方案。该方案是在预配置时，让每个传感器随机地从一个密钥池里选取一定数量的密钥，这样任何两个传感器都以一定的概率来共享一个密钥，通过这个密钥来进行会话。文献[5]对文献[4]的方案进行了改进，提出了另外三个密钥预配置方案：$q$个密钥联合的密钥预配置方案；多路径的密钥加强方案和随机的成对密钥方案。文献[6]提出了两个成对的密钥预配置方案：随机的多项式的密钥方案和一个基于格的多项式密钥预配置方案。这些方案是基于多项式上的密钥预配置协议，通过采用多项式

收稿时间：2007 – 09 – 07
作者简介：张学锋(1967 – )男，硕士，副教授，主要从事计算机应用、数据库方面的研究；刘 斌(1973 – )，男，主要从事网络方面的研究；姜皇普(1982 – )，男，硕士，主要从事无线网络安全方面的研究.

密钥池加强了基础的基于多项式的密钥预配置方案，性能超出了原来的基本方案，但是这些方案都需要进行很复杂的计算。

以上方案在节点的存储量、网络的通讯量、安全性能方面存在很大差异。基于概率的密钥预配置方案中，节点在通讯过程中必须获得其他节点的密钥ID列表，当两节点间不存在共享密钥时，将会造成网络的通信量很大。基于格的多项式密钥与配置方案减少了节点的存储量和通信量，但是当节点间不共享密钥时，建立会话密钥的过程中存在很大的安全隐患，并且当节点相距条数越多，密钥被俘获的概率就越大。利用传感器网络的预配置方案可以设计出高连通性、高安全性、低通信量的Ad hoc网络密钥预配置方案。

密钥预配置方案是为了适应传感器网络的需要而提出的，它利用了传感器网络节点的高密度、可用资源极其有限、生存期短等特点，因此，将其直接应用到传统的Ad hoc会带来很多的弊端。(1) 传统的Ad hoc网络节点密度低，传感器网络的密钥预配置方案的应用会造成网络的低概率连通；(2) 受传感器资源的限制，这些预配置方案以牺牲安全性来减少对资源的占用，对于资源相对充裕的传统Ad hoc网络来说是不能接受的；(3) 以上方案都引入了中间节点，从而降低了密钥传输过程的安全性能。为了解决以上问题，本文在会话密钥的传输过程中引入了门限机制。

# 1　基于格的密钥预配置方案

## 1.1　t度多项

有限域$F_q$上产生二变量t度多项式定义为$f(x,y)=\sum_{i,j=0}^{t}a_{ij}x^i y^j$。这个多项式具有如下属性$f(x,y)=f(y,x)$。其中$q$是一个素数，它必须足够大，以容纳一个加密密钥。假设网络中的每一个节点都有一个全局ID，安装服务器为节点$a$($a$为节点ID)计算多项式$f(x,y)$的份额$f(a,y)$；为节点$b$($b$为节点$ID$)计算多项式$f(x,y)$的份额$f(b,y)$。$a$节点就可以通过在$b$点计算$f(a,y)$得到共享密钥$f(a,b)$，同样$b$节点也可以通过在$a$点计算$f(b,y)$得到共享密钥$f(b,a)$。这样每两个节点之间都可以建立会话密钥。

## 1.2　多项式网格

假设一网络有$N$个节点，基于格的密钥预配置方案如下：利用$2m$个二变量$t$度多项式$F=\{f_i^{\mathrm{r}}(x,y), f_i^{\mathrm{c}}(x,y)\}_{i=0,1,\cdots,m-1}$构造一个$m\times m$的二维格，其中$m>\lceil\sqrt{N}\rceil$，如图1所示。格中的每一行$i$都与一个多项式$f_i^{\mathrm{r}}(x,y)$相关联，每一列$i$都与一个多项式$f_i^{\mathrm{c}}(x,y)$相关联。安装服务器给网络中的每一个节点分配格中的一个交叉点。在坐标($i$，$j$)，安装服务器给相应传感器分配多项式$f_i^{\mathrm{r}}(x,y)$和$f_j^{\mathrm{c}}(x,y)$的份额。

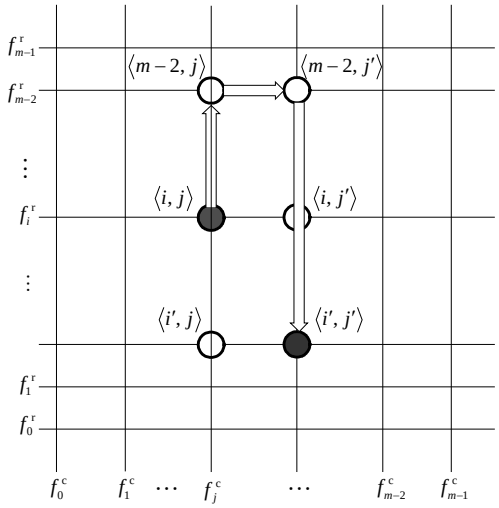


图1　格的示例

可以利用坐标($i$，$j$)表示节点ID。有时为了方便表示，令$l=\lceil\log_2 m\rceil$，这样任何横坐标、纵坐标都可以用$lb$的二进制位串表示，用$\langle r_i,c_j\rangle$表示节点的ID(其中$r_i$，$c_j$分别是节点ID的前$lb$和后$lb$)。

## 1.3　密钥分配

对于每一个传感器节点，安装服务器选择一个空闲的交叉点($i$，$j$)，并将它分配给此节点。然后安装服务器将$\{\mathrm{ID}, f_i^{\mathrm{r}}(j,x), f_j^{\mathrm{c}}(i,x)\}$部署到传感器节点。如图1所示，两传感器节点如果共享多项式就可以通过计算得到多项式密钥。如果不存在共享多项式，可以通过其他节点进行密钥传递，从而建立会话密钥。

基于格的密钥预配置方案直接应用到Ad hoc网络，同样存在着上面提到的弊端。为了解决这些问题，本文给出了应用于传统Ad hoc网络的密钥预配置方案，称之为基于门限机制的密钥预配置方案。

# 2　基于门限机制的密钥预配置

基于门限机制的密钥预配置方案在进行多项式份额分配共享密钥发现时，所采用的方法与基于格的方案是相同的。但是，该方案在进行会话密钥的建立时，通过类似于按需路由中路由查询的方式获得多条密钥路径[7-8]，然后从返回的密钥路径中选择

*k*条作为密钥份额的传输路径。在会话密钥的传输过程当中加入了门限机制[9-11]，使密钥份额分别在*k*条不同的路径上传输，到达目的节点后重新恢复出会话密钥。

**2.1** 传输路径的获取

本方案的路径选择方案采用类似于Ad hoc网络中的按需路由[7-8]。设源节点想与目的节点进行通信，但是两节点间又不存在共享密钥。如图2所示，源节点*A*洪泛路径请求数据包(PathQuery，图中用实线箭头表示)。收到此包的节点首先判断自己是不是此包目的节点，如果是则判断此包中的路径是否符合选择标准，符合则将路径应答数据包(PathReply，图中用虚线箭头表示)按查询包中的路径反向返回，路径应答包中也包含了查询包中的路径信息。如果不是目的节点则转发此包，并将节点的身份标识加入到请求包的节点列表中。

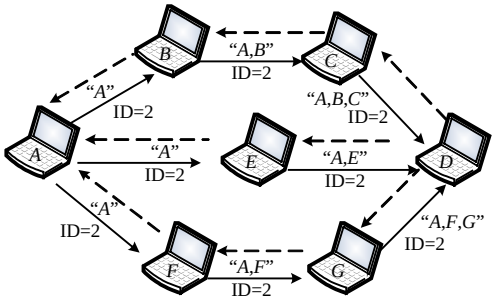
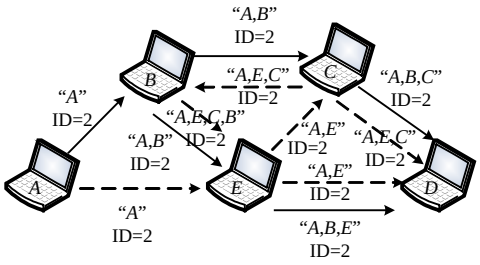


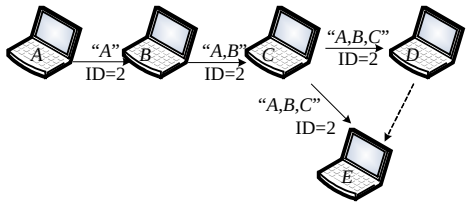

图2 获取传输路径

2.1.1 路径请求数据包洪泛规则

在路径请求数据包的洪泛过程中，节点应当按照一定的规则来广播路径请求数据包，否则将会对网络造成广播风暴。但是按照普通的广播协议，当节点收到某个节点的广播信息后，就不再对同一节点的同一个广播数据包进行处理。这样就会造成路径的遗漏，导致无法搜索到足够的密钥传输路径。本文方案的路径请求数据包的洪泛标准主要有两条：(1) 如果接收的路径请求数据包中的节点列表中不包含自身则转发数据包；(2) 路径请求数据包必须在生存期(TTL>0)，否则不转发。如图3中所示，节点对同一个源节点*A*的同一个路径请求数据包，节点*E*总共转发了两次，节点*E*每次都判断请求包中的节点列表中是否包含自身，如果不包含自身则转发，包含自身则抛弃。图3中，假如设定路径请求包的生存期为3，则节点*D*不再为源节点*A*转发路径请求数据包，因为数据包已经不在生存期内，图中用虚线标示。




a. 节点列表限制




b. 数据包生命期限制

图3 洪泛标准

2.1.2 路径的选择准则

定义 关键节点定义为路径中加密解密密钥份额的节点。

如图4所示，节点*A*用与*C*的共享密钥 $E_{K_C}$ 加密Packet得到 $E_{K_C}$(Packet)。*C*收到 $E_{K_C}$(Packet) 后解密得到Packet，然后将Packet用与E的共享密钥 $E_{K_C}$ 加密得到 $E_{K_E}$(Packet)。*E*收到 $E_{K_C}$(Packet)后解密得到Packet。图中*C*为关键节点，而*B*、*D*只是传输加密后的数据包，并不参与数据包的加密解密操作，所以不是关键节点。

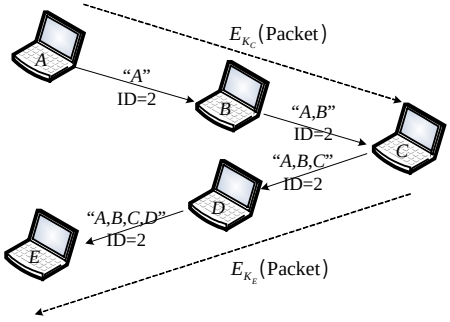



图4 关键节点

从路径获取过程中所获得的路径，并不是每一条都适合用来传输密钥份额，以必须从返回的路径中选择合适的路径。所以存在一个路径的选择标准：(1) 关键节点不重合。即任何两条路径的关键节点都不重合；(2) 路径的长度(物理跳数)在规定的范围内。

在基于格的密钥预配置方案中，只有相邻的共享密钥的节点才能进行直接的通讯，这种方式用在节点密度较小的Ad hoc网络中会造成网络的低概率连通。在路径的选择过程中引入关键节点的概念后，

使得节点的所有邻居节点都可以作为通信的下一跳，从而增加了网络连通的概率。

### 2.2　密钥传输过程

(1) 假设$P$是一个大素数，共享密钥$k \in K = Z_p$。源节点随机选择一个$t$–1次多项式$h(x) = (a_{t-1}x^{t-1} + \cdots + a_1 x + a_0) \bmod p$，其中$a_0 = k, a_1, a_2 \cdots, a_{t-1} \in Z_p$；在$Z_p$中选择$n$个非零的、互不相同的元素$x_1, x_2 \cdots, x_n$，计算$y_i = h_i(x_i)$，$1 \le i \le n$。其中$a_0, a_1, \cdots, a_{t-1}$是非公开的，$p, x_1, x_2, \cdots, x_n$是公开的，$y_i$是要被作为密钥份额传送的。

(2) 源节点将$y_i$通过$k$条密钥传输路径传送。如果$n = k$，则在每个路径上传送一个密钥份额；如果$n > k$，则在某些有优势的路径中传送多个密钥份额，或者是在$k$条路径上传送平均数量的密钥份额。

(3) 目的节点收到$t$个共享$y_s$ $(1 \le s \le t)$，从拉格朗日多项式重构的$h(x)$为：

$$h(x) = \sum_{s=1}^{t} y_s \prod_{j=1, j \ne s}^{t} \frac{x - x_j}{x_s - x_j}$$

通过计算获得密钥为：

$$k = h(0) = \sum_{s=1}^{t} y_s \prod_{j=1, j \ne s}^{t} \frac{-x_j}{x_s - x_j}$$

## 3　性能分析

### 3.1　网络连通的概率

假设网络中每个节点的邻居节点数为$n$，基于格的密钥预配置方案中，每个节点可以直接通讯的节点数约为$\frac{2n}{m}$。在本文的方案引入了关键节点的概念后，$n$个节点都可以作为直接通信节点，从而增加了网络连通的概率。

### 3.2　对网络攻击的抵御能力

对于一个有$N$个节点、$2m$个多项式的网络，其中$m > \lceil \sqrt{N} \rceil$。假设节点已经被俘获的概率为$P$，则某多项式有$i$个多项式份额泄漏的概率为$P(i) = \frac{m!}{i!(m-i)!} P^i (1-P)^{m-i}$，该多项式被破解的概率为$P_C = 1 - \sum_{i=0}^{t} P(i)$。为了计算方便，假设密钥的传输路径是$k$条；密钥传输路径的平均跳数为3，则该路径已被破解的概率$P_L = 1 - (1 - P_C)^3$，该密钥能够安全建立的概率$T = 1 - (P_L)^k$。图5表明随着被俘节点比例的增大，两节点能成功地建立密钥对的概率会降低，但是，基于门限机制的方案中这种概率降低的幅度较小。

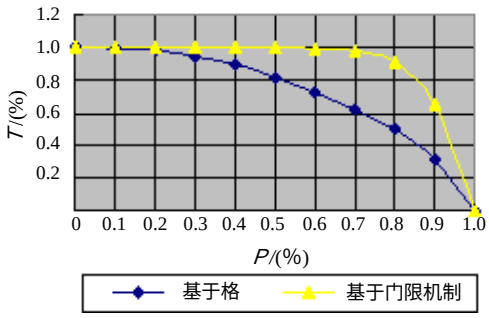



图5　节点被俘比例$P$与成功建立会话密钥的概率$T$

## 4　结 束 语

本文提出了一种应用了秘密共享机制的Ad hoc网络的密钥预配置方案。在密钥的传送过程中引入秘密共享机制，提高了密钥传输地安全性。相对于基于证书的预配置方案，该方案可以减少网络安全性能对网络资源的依赖性。同时，其安全性能相对传感器网络又有很大提高。

## 参　考　文　献

[1] 赵　刚. Ad hoc网络当中的密钥管理[D]. 上海: 上海交通大学, 2005.

[2] PERLMAN R. An overview of PKI trust models[J]. IEEE Network, 1999, 13(6): 38-43.

[3] 任丰原, 黄海宁, 林　闯. 无线传感器网络[J]. 软件学报, 2003, 14(7): 1282-1291.

[4] ESCHENAUER L, GLIGOR D. A key-management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. USA: ACM, 2002: 41-47.

[5] CHAN H, PERRIG A, Song D. Random key pre-distribution schemes for sensor networks[C]//IEEE Symposium on Security and Privacy. Berkeley, California, USA: IEEE, 2003:197-213.

[6] LIU D, NING P. Establishing pairwise keys in distributed sensor networks[C]// Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: Association for Computing Machinery Press, 2003: 52-61.

[7] 刘　军, 郭　伟, 肖百龙, 等. 移动自组网基于路径维持概率的按需路由协议[J]. 软件学报, 2007, 18(3): 693-701.

[8] 陈　晶, 崔国华, 洪　亮, 等. 一种Ad hoc网络中的安全匿名按需路由协议[J]. 计算机科学, 2007, 34(1): 29-33.

[9] MIYAZAKI K, TAKARAGI K. A threshold digital signature scheme for a smart card based system[J]. IEICE Trans on Fundamentals, 2001, 84 (1): 205-213.

[10] CHANG T Y, YANG C C, HWANG M S. A threshold signautre scheme for group communications without a shared distribution center[J]. Future Generation Computer Systems, 2005, 20(6): 1013-1021.

[11] 刘蓬涛, 李大兴. 基于Lagrange插值多项式的门限方案的实现[J]. 计算机工程与应用, 2005, 41(36): 117-119.

编　辑　税　红