基于地理位置的蜂窝状密钥管理方案

孔贝贝，唐小虎
(西南交通大学 信息安全与国家计算网格实验室，成都 610031)

摘 要：无线传感器网络是由计算能力、存储能力、通信能力严格受限的传感器节点组成的，密钥管理是安全问题的基础，可以保证后续信息的保密性及认证性。采用蜂窝状网络划分方式对基于地理位置的密钥分配方案作了改进，改进后的方案相对原方案减少了传感器节点的存储量，具有更好的抗攻击能力，适用于大规模网络。

关键词：无线传感器网络；密钥分配；地理位置信息；蜂窝状划分；抗攻击能力
中图分类号：TP309.7 **文献标志码**：A **文章编号**：1001-3695(2010)04-1514-03
doi:10.3969/j.issn.1001-3695.2010.04.087

Improved key management scheme for wireless sensor networks using hexagon cells and deployment knowledge

KONG Bei-bei, TANG Xiao-hu
(Information Security & National Computation Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: WSN is consisted of low computation, low storage, low communication ability micro nodes, key management acts as the basic manner to assure security and authentication of information transported by nodes in WSN. An improved scheme making use of deploy knowledge based on random key predistribution had been made, adopting hexagon cells. The new scheme can use less memory, perform better with the same number of compromised nodes, and suit for large scale networks.

Key words: wireless sensor networks(WSN); key distribution; deployment knowledge; hexagon partition; attack resistant

0 引言

电子技术的发展使得微型智能系统得到了极大的发展，传感器节点也是微型智能系统的一种，有自己完整的硬件设备与软件系统。无线传感器网络是由大量的无线传感器节点采用无线通信方式构成的一种自组织网络，应用于民事及军事方面，它不仅面临着一般无线通信系统的安全威胁，同时由于WSN本身能力的限制还面临一些特殊的安全攻击。

加密与认证是WSN的安全通信的基本技术，由于传感器节点本身能力的限制，非对称加密算法，如RSA、ECC(椭圆曲线加密算法)，虽然已经在一些8位微控制器中实现[1]，但是算法所需节点的存储空间、计算能力、能耗较大，计算时间较长，因此低开销及高速度的对称加密算法，如RC系列算法，仍是WSN中采用的主流算法，而密钥分配又是加密及认证的基础。

1 一般密钥分配方式

WSN是一种无中心网络，不能采用基于KDC(key distribution center)的密钥分配措施，它有三种密钥预分配方式：

a) 预安装模型。最简单的方式给WSN中所有的节点相同的密钥，但这种方式如果一个节点被攻破，整个网络就会处于敌人的控制中，另外一种方式是一个有 N 个传感器节点的WSN，让每个传感器节点存储与其他的 $N-1$ 个节点的共享密钥，这种方式可以有效地抵抗攻击，保证节点之间数据传输的安全性，但整个网络的总存储量为 $N(N-1)/2$ 不适用于大规模网络，而且整个WSN中不是任意两个节点都需要直接通信，这种密钥分配方式会造成资源的严重浪费。

b) 确定预分配模型。节点通过预分配信息来计算与邻居节点的共同密钥，如Blom密钥分配方案的改进方案[2]、基于多项式的密钥分配方案[3]以及它的改进[4~6]，当超过门限值的秘钥信息被敌人获取后，整个网络被攻破的概率就会增大。

c) 随机预分配密钥模型。由Laurent等人[7]首先提出，基于随机连通图原理，首先生成一个密钥池，按照网络连通度的要求，每个节点从密钥池中随机选取一定数量的密钥进行存储，节点散布在目标区域后，可以形成一个安全连通网络。本文把这个方案作为基本方案(basic scheme)。Chan等人[8]在基本方案的基础上提出了q composite密钥分配方案，稍后Du等人[9]采用节点的位置分布信息提出一种基于网络的密钥分配方案(矩形方案)，相对于文献[7,8]有更好的抗攻击能力、减少了节点信息存储量且未增加节点间的通信量。

随机预分配密钥模型与确定预分配模型相比，不需要共享密钥的数学计算，在保证网络安全的同时减少了节点的计算能耗。本文采用蜂窝状结构以及节点的分布信息在Du的密钥分配方案基础上作出改进，仿真结果证明本方案不仅可以减少节点的存储量，而且具有更强的抗攻击能力。

2 基于地理位置的网络状密钥分配方案

2.1 基于地理位置的节点分布

首先对节点分布作一些假设：a) 整个网络中的节点都是

收稿日期：2009-08-20；修回日期：2009-09-25

作者简介：孔贝贝(1986-)，女，河南项城人，硕士研究生，主要研究方向为无线传感器网络安全(kongbeibei2329@126.com)；唐小虎(1972-)，男，教授，博导，主要研究方向为网络安全等.

静止的,不具有移动性;b) 节点被投放在目标区域范围附近。一般情况下,在 WSN 中虽然不知道哪两个节点会是邻居(相互通信范围内),但节点所在区域是否是相邻的是可以知道的。

设 N 个传感器节点均匀分布在 $(X \times Y)$ m^2 大小的一个区域内,把这个区域划分成 $t \times n$ 个等大小的矩形区域,假设节点的目标投放区域为 $G_{ij}(1 \leq i \leq t,\ 1 \leq j \leq n)$,$G_{ij}$ 的质心为 (x_i, y_j)。节点在整个网络中是平均分布的,在目标区域 G_{ij} 中节点符合二维高斯分布,节点的概率密度函数如式(1)所示(σ 为高斯分布的标准偏差):

$$f(\text{node} \in G_{ij}) = \frac{1}{2\pi\sigma^2} e^{-[(x-x_i)^2+(y-y_j)^2]/2\sigma^2} = f(x-x_i, y-y_j) \quad (1)$$

每个节点被选入一个区域的概率是 $1/(t \times n)$,在整个 $(X \times Y)$ m^2 的区域内节点的概率分布函数如式(2)所示:

$$f(x, y) = \sum_{i=1}^{t}\sum_{j=1}^{n} \frac{1}{tn} f(\text{node} \in G_{ij}) \quad (2)$$

2.2　密钥分配过程

设用于整个 WSN 的密钥池的大小为 $|S|$,每个传感器节点可以存储 m 个密钥,一般认为 m 的上界为 200 个。整个密钥分配分为以下三步:

a) 密钥预分配。把整个密钥池 $|S|$ 划分成 $t \times n$ 个小的密钥池 $S_{ij}(1 \leq i \leq t,\ 1 \leq j \leq n)$,从每个小密钥池 S_{ij} 中随机选取 m 个密钥分配给区域 G_{ij} 中的每个传感器节点。

b) 共享密钥发现阶段。每个传感器节点存储的密钥 ID 号广播给周围邻居,邻居节点通过密钥的 ID 号找到相应的共享密钥,密钥的 ID 可以用明文的形式公布,但为了保障密钥信息的安全也可以采用 Merkle 谜语[2~9]的方式公布,每个节点预存储一个 α 值(挑战值),用自己拥有的密钥 K_i 加密 α 得到一组加密信息 E_{K_i},广播 $\langle \text{ID}_i, E_{K_i}(\alpha) \rangle$ 给邻居节点,邻居节点如果可以解密 $E_{K_i(\alpha)}$ 得到正确 α,表示与广播节点存在共享密钥 K_i,广播节点也可以通过这种方式知道与哪些邻居共享哪些密钥。

c) 路径密钥建立阶段。通过步骤 b) 整个网络建立起了一个安全连通图,即全网中两个节点间要么有共享密钥,要么可以通过有共享密钥的节点建立起联系。未能建立起共享密钥的节点 A、B 可以通过存在共享密钥的中间节点 C 进行密钥协商,由 C 生成 A、B 的通信密钥,并且用 K_{CA}、K_{CB} 把通信密钥加密后传输给 A、B,C 充当了 KDC 的角色。

2.3　基于网格的密钥池划分过程

Du 等人采用基于网格状的划分如图 1 所示,大部分网格有 8 个邻居区域,每个区域的密钥池大小为 $|S_c|$。

设条件如下:

a) 区域 E 与水平、竖直邻居区域 B、H、D、F 有 $a|S_c|$」个共享密钥,$0 \leq a \leq 0.25$,a 为重叠因子。

b) 区域 E 与斜对角邻居区域 A、C、G、I 有 $b|S_c|$」个共享密钥,$0 \leq b \leq 0.25$,b 为重叠因子,$4a + 4b = 1$。

c) 非相邻区域之间没有共享密钥。

通过以上条件可以得出每个小密钥池的大小,如式(3):

$$|S_c| = \frac{|S|}{tn - (2tn - t - n)a - 2(tn - t - n + 1)b} \quad (3)$$

任意两个节点之间共享密钥的概率如式(4)所示,λ 为 1,a,b,0:

$$p(\lambda) = 1 - \frac{\sum_{i=0}^{\min(m,\ \lambda|S_c|)} \binom{\lambda|S_c|}{i}\binom{(1-\lambda)|S_c|}{m-i}\binom{|S_c|-i}{m}}{\binom{|S_c|^2}{m}} \quad (4)$$

3　蜂窝状密钥管理方案

本文采用蜂窝状结构对基于网格的密钥分配方案作了改进,改进方案减少了节点的存储量,提高了节点的抗攻击能力,而且采用区域化方式的密钥分配方案更加附合实际应用[10, 11]。

3.1　节点分布模型

基于地理位置的网格状密钥分配方案仅仅采用矩形方式对网络进行划分,在实际通信中节点的传输范围是圆形。在顶点到几何中心等距的多变形中,能够无重叠地覆盖某一区域的几何形状有正方形、等边三角形、正六边形。这几种形状中正六边形的面积最大。密钥池划分时,正方形的邻居区域为 8 个,等边三角形的邻居区域为 12 个,正六边形的邻居数为 6,正六边形邻居数所需要存储的邻居信息少。

本文借签文献[12,13]中的思想,把基于网格的方案与基于正六边形的方案进行对比。假设邻居区域的任意两个节点之间可以建立起通信,节点的通信距离为 R m(相邻区域的节点间的最远通信距离),采用正方形网格的区域划分方式与采用正六边形区域的划分方式比较如图 2 所示。

采用正方形结构进行划分,每个小正方形面积为 $R^2/8$,但采用正六边形结构进行划分每个正六边形的面积为 $3\sqrt{3}R^2/26$,在节点通信能力相同的情况下,采用正六边形结构进行划分的小区域的面积是采用正方形结构进行划分的 1.598 8 倍。

3.2　蜂窝状密钥预分配方案

本文采用的密钥分配过程与 2.2 节相同。

3.3　蜂窝状网络的密钥池划分

采用正六边形结构进行网络划分,每个正六边形与它的 6 个邻居的最远通信距离都相同,整个网络中每个正六边形的地位都平等,这与采用正方形结构划分不同。正方形结构划分中,每个正方形区域同 8 个邻居的最远通信距离不完全相同,在密钥池划分时相邻区域的覆盖因子分为两类 a 与 b,采用正六边形结构只用一种覆盖因子就可以了,本文假设每个正六边形与邻居区域有 $a|S_c|$」个共同的密钥,a 为覆盖因子。

采用与 2.1 节中正方形结构网络划分相同的划分方式,设正六边形结构的网络中也有 $t \times n$ 个等大小的正六边形,每个小区域 $G_{ij}(1 \leq i \leq t,\ 1 \leq j \leq n)$ 的划分如图 3 所示。设网络为 $(X \times Y)$ m^2,整个网络的密钥池为 S,网络被划分成了 $t \times n$ 个六边形。图 3 中 $t = 6$、$n = 5$。密钥分配的过程按照从左到右,从下到上的顺序进行:

(a) 首先从 S 中选出 $|S_c|$ 个密钥分配给第一个六边形 $G_{1,1}$,然后把这 $|S_c|$ 个密钥从密钥池 S 中剔除。

(b) 第一行的六边形区域 $G_{1,j}(j \in [2, t])$ 先从它左边的邻居 $G_{1,j-1}$ 的密钥池 $|S_c|$ 中选取 $a|S_c|$ 个密钥,然后再从剩余的密

钥池中选出 $w=(1-a)\ |S_c|$个密钥，由选出的这两部分密钥构成区域 $G_{1,j}$中的密钥池 $|S_c|$，每个区域选完密钥后，从密钥池 S 中剔除已经被选中的密钥。

(c) 区域 $G_{i,j}(i\in[1,t-1],j\in[2,n])$ 先从已经分配了密钥的邻居中都选出 $a\ |S_c|$个密钥，再从密钥池 S 中选出剩余的密钥，选取的过程与步骤(b)相同，当 $i=1$ 时，$w=(1-a)\ |S_c|$；当 $2\leq i<t$ 时，如果 i 为偶数 $w=(1-4a)\ |S_c|$，如果 i 为奇数 $w=(1-2a)\ |S_c|$；如果 i 为 t 时，$w=(1-3a)\ |S_c|$。图 3 中每个区域中的值为比例系数 $w/|S_c|$。

3.4 密钥池 $|S_c|$的计算

整个密钥池的大小为 $|S|$，每个小区域中有 $|S_c|$个密钥，根据图 3 可以得出 $|S_c|$与 $|S|$的关系，每个正六边形区域内的系数 $\times|S_c|$求和得到密钥池 $|S|$的大小，$|S_c|$的大小如式(5)所示：

$$|S_c|=\frac{|S|}{tn-a(3tn-2t-2n+1)} \tag{5}$$

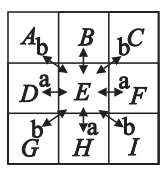

图1 邻居区域共享密钥分布图

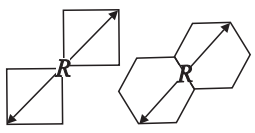

图2 相同通信能力的WSN中邻居区域划分

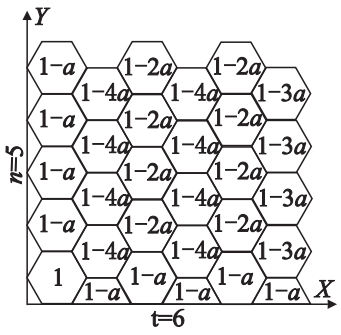

图3 正六边形网络密钥池分配图

假设 $|S|=100\ 000$，$t=n=10$，覆盖因子 $a=b=0.125$，采用正方形方式进行区域划分时 $|S_c|=1746$，采用正六边形结构进行划分时 $|S_c|=1\ 484$。选用相同的覆盖因子、相同的总密钥池大小，网络采用蜂窝状结构划分比采用正方形状结构划分时，$|S_c|$变小了；如果节点中存储相同数目的密钥个数，蜂窝状结构网络节点可以有更高的连通概率，3.5 节会有详细过程。

在区域个数相同的情况下，每个正方形区域与六边形区域内密钥池大小 $|S_c|$如表 1 所示。

3.5 本地连通概率

本地连通概率是指由存在共享密钥的节点之间建立起安全网络连通图的概率，与式(4)的表示相同。用 $B(n_i,n_j)$ 表示节点 n_i 与 n_j 之间至少存在一个共享密钥的概率，$A(n_i,n_j)$ 表示节点 n_i 与 n_j 节点在相邻区域的概率，本地连通概率的计算式为

$$Pr(\text{local connectivity})=Pr(B(n_i,n_j)\ |A(n_i,n_j))=\frac{Pr(B(n_i,n_j)\text{ and }A(n_i,n_j))}{Pr(A(n_i,n_j))} \tag{6}$$

本地连通概率也等于 1 - Pr(2 个节点之间无共享密钥)，利用式(1)可以得到：

$$Pr(B(n_i,n_j)\text{ and }A(n_i,n_j))=\int_{x=0}^{X}\int_{y=0}^{Y}\sum_{j\in\text{group}}\sum_{i\in\text{group}}f_R(d_{jZ}\,|n_j\in\text{group }j)\cdot g(d_{iZ}\,|n_i\in\text{group }i)\,p(\lambda)\,\mathrm{d}x\mathrm{d}y \tag{7}$$

$$Pr(A(n_i,n_j))=\int_{x=0}^{X}\int_{y=0}^{Y}\sum_{j\in\text{group}}\sum_{i\in\text{group}}f_R(d_{jZ}\,|n_j\in\text{group }j)\cdot g(d_{iZ}\,|n_i\in\text{group }i)\,\mathrm{d}x\mathrm{d}y \tag{8}$$

假如 $|S|=100\ 000$，$t=n=10$，$a=b=0.125$，图 4 为本地连通概率与每个节点存储密钥个数 m 的关系，设每个节点最多可以储存 200 个节点，基本方案为文献[7]中提出的方案，矩形方案为文献[9]中提出的方案。

从图 4 中可以得知本文方案的本地连通概率最高，当每个节点都存储 100 个密钥时，基本方案的连通概率是 0.095，采用正方形结构划分时本地连通概率是 0.513 8，采用本文方案时本地连通概率是 0.572。

表1 密钥池 $|S_c|$的大小

覆盖因子a	矩形方案	本文方案
$a=b=0.125$	1 746	1 484
$a=b=0.105$	1 560	1 377
$a=b=0.085$	1 409	1 285
$a=b=0.065$	1 285	1 204
$a=b=0.045$	1 181	1 133
$a=b=0.025$	1 150	1 069

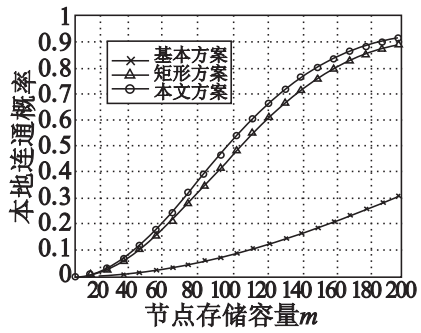

图4 本地连通概率与节点密钥存储量m的关系图

3.6 节点抗攻击能力

假设敌手捕获了某个节点，可以获得这个节点的所有密钥，敌手通过获得的密钥后续对整个网络的通信进行一定的破坏。

设整个网络中共有 x 个节点被捕获，m 为节点中存储密钥的个数，当一个节点被攻破后网络中剩余的节点与被攻破节点之间没有共享密钥的概率为 $1-m/|S|$；x 个节点被攻破后网络中其他节点不会被破坏的概率为：$(1-m/|S|)^x$；后续网络通信被破坏的概率为 $1-(1-m/|S|)^x$。

如果本地连通概率为 0.33，基本方案要求节点存储 200 个密钥，正方形划分方式要求节点存储 75 个密钥，本文方案中节点需存储 69 个密钥，图 5 为被攻破传感器节点的个数与对网络后续通信破坏的关系图，从图中可以看出本文方案具有更好的抗攻击能力。

当本地连通度为 0.5 时，基本方案需要存储 263 个密钥，正方形方案每个传感器节点需要存储 99 个密钥，本文方案需要存储 91 个密钥，如图 6 所示。

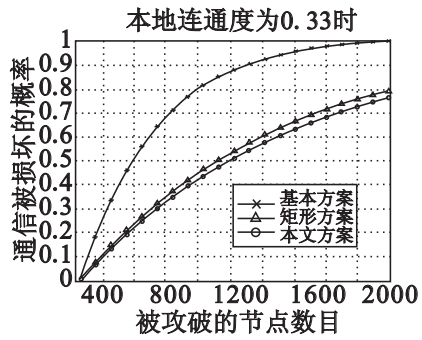

图5 p=0.33时被捕获节点数目与网络通信被破坏程度关系

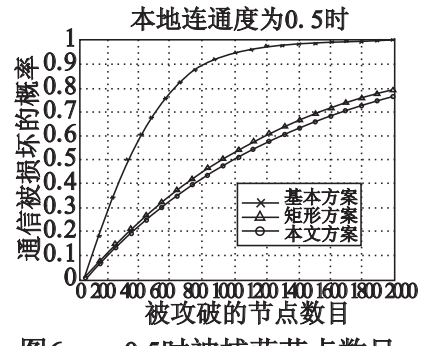

图6 p=0.5时被捕获节点数目与网络通信被破坏程度关系

矩形网格划分方式[9]比基本的基于图论的密钥分配模型以及改进模型 q-composite 模型[8]，在相同的网络连通概率的情况下具有更好的抗攻击能力，本文方案比文献[9]中方案抗攻击能力更强。

4 结束语

本文在文献[9]的基础上提出了蜂窝状网络划分的密钥管理方案，在没有增加任何附加的假设条件的情况下，本方案的网络覆盖面积是原始方案的 1.598 8 倍，相同安全连通概率的情况下，本文方案需要更少的节点存储量，拥有更高的抗攻击能力。

(下转第 1520 页)

历序列值的相关性。这是因为在对特征点进行遍历时,各特征点以均等的概率被历经,因此即使在匹配特征点数较少时,也能解算出高相关的遍历序列值(表 1 的检测结果也说明了这一点)。显然,改进后的方法可减少约一半的计算量。

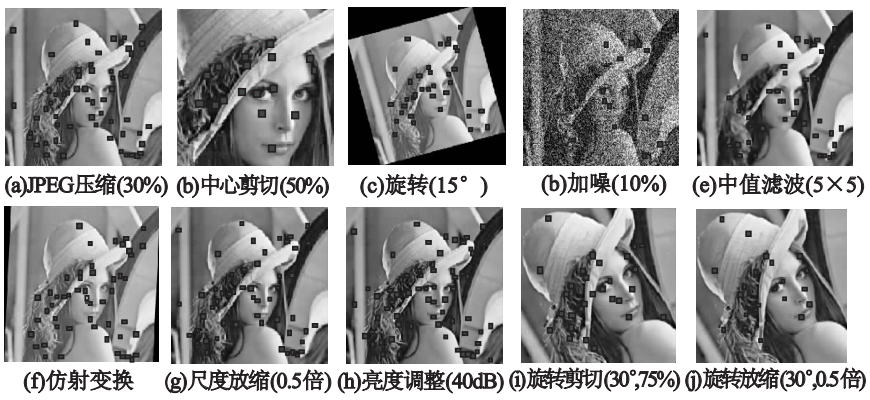

图5 Lena图像经不同图像操作处理后的效果图
(含SIFT匹配特征点分布)

表1 SIFT特征、DCT域以及高阶累积量水印算法对图5中各图像的水印检测结果

图像序号	图像操作描述	SIFT特征点数	匹配特征点数	相似性检测水平		
				SIFT	DCT域	高阶累积量
图5(a)	JPEG压缩(30%)	500	60	0.998 9	0.872 1	0.910 2
图5(b)	剪切(50%)	141	17	1.000 0	**0.046 5**	0.291 3
图5(c)	旋转(15°)	418	36	0.822 8	**0.073 0**	0.209 7
图5(d)	加噪(10%)	457	21	0.988 8	0.182 1	0.611 9
图5(e)	中值滤波(5×5)	195	48	0.984 6	0.290 7	0.594 2
图5(f)	仿射变换	384	51	0.993 8	0.190 3	0.692 7
图5(g)	尺度放缩(0.5倍)	112	53	0.999 5	0.843 2	0.915 7
图5(h)	亮度调整(40dB)	354	66	1.000 0	0.907 1	0.937 2
图5(i)	旋转并剪切(30°,75%)	259	29	0.710 1	**0.037 2**	**0·084 9**
图5(j)	旋转并放缩(30°,0.5倍)	447	23	0.553 4	**0.058 1**	**0·104 5**

注:表1中粗体表示水印检测不通过。

4 结束语

本文给出一种基于图像特征提取算子——SIFT 算子构建数字图像零水印的新算法,相比于其他提取重要系数或特征的零水印算法,SIFT 算子更能有效地提取出表征原图像作品的局部信息特征,而且这些局部特征信息能在常见的压缩、剪切、旋转、加噪、滤波等操作下保持一定的稳定性,因此,基于 SIFT 特征的水印信息更能有效地惟一表征原图像作品。同时,提出的匹配特征点随机遍历方法能将图像的局部特征信息以及局部特征之间的关联信息转换为一维序列,方便算法自动判别待检测图像是否包含已注册的水印信息,避免了依据匹配特征点个数或比例进行判别的不准确性。仿真实例也表明了基于 SIFT 特征的图像零水印算法具有较好的鲁棒特性和抗攻击特性。在计算性能上,针对在特征点匹配过程中需要对特征点距离反复计算的问题,给出了一种改进的匹配方法,该方法可将水印检测时的匹配计算量减少约一半。

参考文献:

[1] 杨义先,钮心忻. 多媒体信息伪装综论[J]. 通信学报, 2002, 23(5): 32-38.

[2] BARNI M, BARTOLINI F. Data hiding for fighting piracy[J]. IEEE Trans on Signal Processing, 2004(3): 28-39.

[3] 温泉,孙锬锋,王树勋. 基于零水印的数字水印技术研究[C]//全国第三届信息隐藏学术研讨会论文集. 西安: 西安电子科技大学出版社, 2001.

[4] 温泉,孙锬锋,王树勋. 零水印的概念与应用[J]. 电子学报, 2003, 31(2): 214 216.

[5] 向华,曹汉强,伍凯宁,等. 一种基于混沌调制的零水印算法[J]. 中国图象图形学报, 2006, 11(5): 720-724.

[6] LOWE D G. Distinctive image features from scale invariant keypoints [J]. International Journal of Computer Vision, 2004(1): 91-110.

[7] PHAM V Q, MIYAKI T, YAMASAKI T, *et al*. Geometrically invariant object-based watermarking using SIFT Feature[C]// Proc of ICIP. San Antonio: IEEE Signal Proccessing Society, 2007: 473-476.

[8] PETITCOLAS F A P. Watermarking schemes evaluation[J]. IEEE Transaction on Signal Processing, 2000, 17(5): 58-64.

[9] [EB. OL]. http://www.petitcolas.net/fabien/software/StirMarkBenchmark_4_0_129.zip.

(上接第 1516 页)

参考文献:

[1] 裴庆祺,沈玉龙,马建峰. 无线传感器网络安全技术综述[J]. 通信学报, 2007, 28(8): 113-122

[2] DU Wen-liang, DENG Jing, *et al*. A pairwise key pre-distribution scheme for wireless sensor networks[C]// Proc of the 10th ACM Conf on Computer and Communications Security. New York: ACM Press, 2003: 42-51.

[3] LIU D, NING P. Establishing pairwise keys in distribution sensor networks[C]// Proc of the 10th ACM Conf on Computer and Communications Security. New York: ACM Press, 2003: 52-61.

[4] LIU D, NING P. Location-based pairwise key establishments for static sensor networks[C]// Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks. New York: ACM Press, 2003: 72-82.

[5] FARSHID D, FARAMARZ F. Key pre-distribution in wireless sensor networks using multivariate polynomials[C]// Proc of the 2nd Annual IEEE Communications Society Conf Sensor and Ad hoc Communications and Networks. 2005: 118-129

[6] KIM J M, HAN Y J, PARK S H, *et al*. N-dimensional grid-based key predistribution in wireless sensor networks[C]// Proc of Computational Science and Its Applications. 2007: 1107-1120

[7] ESCHENAUER L, GLIGOR D V. A key management scheme for distributed sensor networks[C]// Proc of the 9th ACM Conf on Computer and Communications Security. New York: ACM Press, 2002: 41-47.

[8] CHAN Hao wen, ADRIAN P, DAWN S. Random key predistribution schemes for sensor networks[C]// Proc of IEEE Symp on Security and Privacy. Washington DC: IEEE Computer Society, 2003: 197-213

[9] DU Wen liang, DENG Jing, HAN Y S, *et al*. A key management scheme for wireless sensor networks using deployment knowledge [C]// Proc of IEEE INFOCOM. Hong Kong: IEEE Computer Society, 2004: 72-82.

[10] LIU Dong gang, NING Peng, DU Wen liang. Group-based key predistribution in wireless sensor networks[C]// Proc of the 4th ACM Workshop on Wireless Security. New York: ACM, 2005: 11-20.

[11] LIU Dong gang, NING Peng, DU Wen liang. Group-based key predistribution for wireless sensor networks[C]// Proc of the ACM Transactions on Sensor Networks (TOSN). New York: ACM, 2008: 1-30.

[12] XU Ya, HEIDEMANN J, ESTRIN D. Geography-informed energy conservation for Ad hoc routing[C]// Proc of the 7th Annual International Conference on Mobile Computing and Networking. New York: ACM Press, 2001: 70 84.

[13] YU Zhen, GUAN Yong. A robust group-based key management scheme for wireless sensor networks [C]// Proc of Wireless Communications and Networking Conference. 2005: 1915-1920