

基于非均匀分簇的 HWSN 密钥预分配方案的研究

黄慧娟,许 勇,张 海

(安徽师范大学 数学与计算机科学学院,安徽 芜湖 241003)

摘 要:密钥管理问题一直是无线传感器网络中的热点研究问题之一。针对传统的密钥预分配方案具有能量不均衡以及网络生存周期短的问题,文中设计了一种新的基于分簇结构的异构传感器网络的密钥预分配方案(New Clustering In Key Pre-distribution,NCIKP)。详细给出了簇首选择过程、非均匀分簇过程以及密钥预分配过程,在选择簇首时将同时考虑节点的能量消耗率、节点到基站的距离以及节点的邻接程度。通过仿真实验与分析,相较其他的密钥预分配方案,此方案较好地满足了异构传感器网络的安全和能耗需求。

关键词:异构传感器网络;非均匀分簇;密钥预分配;能量均衡

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2016)02-0077-05

doi:10.3969/j.issn.1673-629X.2016.02.018

Research on Key Pre-distribution Scheme for Heterogeneous Wireless Sensor Networks Based on Unequal Clustering

HUANG Hui-juan,XU Yong,ZHANG Hai

(College of Mathematics and Computer Science,Anhui Normal University,Wuhu 241003,China)

Abstract:The key management is always one of hot topics in wireless sensor network. For many traditional key pre-distribution scheme with energy imbalance and network short lifetime problem,a new cluster-based key pre-distribution scheme (New Clustering in Key Pre-distribution,NCIKP) for Heterogeneous Wireless Sensor Networks (HWSN) is proposed. The cluster head selection process,unequal clustering process and key pre-distribution process are given in detail. In the selection of cluster head,also consider node energy consumption rate,node distance to the base station and node adjacency degree. According to the simulation experiment,compared with other key pre-distribution scheme,it's better to meet the security and consumption demand for HWSN.

Key words:heterogeneous wireless sensor networks;unequal clustering;key pre-distribution;energy balance

0 引 言

随着无线传感器网络(Wireless Sensor Networks,WSN)^[1]的应用发展,WSN的安全通信日益受到关注。传感器节点通常被随机置于无人监听环境之中,易遭受窃听威胁,也容易被捕获和破坏,这使得一些常用加密体系中的密钥管理方法(如公钥加密体系)不再适用于传感器网络。目前,在WSN安全通信中,较为普遍使用的是密钥预分配方案^[2-9]。根据WSN构造形态,可将其分为异构传感器网络(Heterogeneous Wireless Sensor Networks,HWSN)和同构传感器网络。同构传感器网络的密钥预分配方案的研究已有很多成果^[3-6],相对而言,针对异构传感器网络的密钥预分配

方案^[8-9]还比较少。

文中主要关注异构传感器网络中的密钥预分配问题。因异构传感器网络中节点具有能量差异性,在进行密钥预分配过程中,若不进行节点能量的均衡与优化,则可能导致部分节点过早耗尽能量而失效。因此文中设计了一种新的基于分簇结构的异构传感器网络密钥预分配方案(New Clustering In Key Pre-distribution,NCIKP),采用二级网络结构,综合考虑节点的能量消耗率、节点到基站的距离以及节点的邻接程度选择簇首,用以均衡节点的能量消耗;同时,簇首节点通过竞争形成不同半径的簇,以防止“热区”的出现;在此基础上分别对簇首节点以及簇内节点进行密钥预

收稿日期:2015-04-03

修回日期:2015-07-08

网络出版时间:2016-01-04

基金项目:安徽省自然科学基金资助项目(11040606M137)

作者简介:黄慧娟(1990-),女,硕士研究生,研究方向为计算机网络与信息安全;许 勇,博士,教授,硕士生导师,研究方向为计算机网络与信息安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20160104.1608.078.html>

分配。

仿真实验表明,该方案具有较好的安全性能,有效提高了网络能量利用率,延长了网络生存周期。

1 相关工作

密钥预分配一直是无线传感器网络安全研究领域的一个研究热点。对于同构无线传感网络,2003 年,Eschenauer 和 Gligor^[3]提出了最经典的 E-G 方案,其基本思想是:每个节点从一个大的密钥池中随机分配一些密钥来构成自己的密钥环,需要通信节点之间通过发现彼此密钥环中的公共部分来确定共享密钥,然后选择一个作为其会话密钥。该方案由于不需要任何先验信息,所以安全性一般;随后 Chan 等^[4]在 E-G 方案上进行改进,提出了 q -composite 方案,将 2 个节点之间共享密钥数提高到 q 个,增强了安全性;Du 等^[5]提出了一种根据节点部署信息的密钥预分配方案,有效提高了网络的连通性;2013 年,王小刚等^[6]提出了一种基于二次型的无线传感器网络密钥管理方案,该方案利用二次型正交对角化特性建立会话密钥,提高了安全性和可扩展性。

关于异构无线传感器网络,早在 2002 年,Duarte 等^[7]就指出了对比传统的同构无线传感器网络,异构传感器网络具有更长的生命周期和可测性。据此,马春光^[8]等于 2009 年提出了一种基于区域的异构无线传感器网络密钥预分配方案。该方案将网络监测范围划分为多个区域,同时将密钥池也划分为多个子密钥池,在一定程度上提高了相邻节点共享密钥的概率,但是密钥池的划分较为复杂;2010 年,马春光等^[9]又提出了一种基于按对平衡设计的异构无线传感器网络密钥预分配方案。该方案针对网络中节点的异构性,利用按对平衡设计构造了不同的节点密钥环,增加了网络的连通性,有效降低了网络的通信负载。但上述方案仅实现了安全的密钥预分配,没有考虑不同节点的能量差异性,在实际运行中,部分节点可能因能量过早耗尽而引起失效。

针对这个问题,研究者们给出一种分簇算法,通过合理构造分簇结构,将在实现安全通信的同时,也能达到均衡网络能量消耗及延长网络寿命的目的。经典的分簇算法有 LEACH^[10]、HEED^[11]等,但这些算法在选择簇首节点时随机性比较大,而且在能量节省方面也考虑不够;2007 年,陈贵海^[12]等提出一种非均匀分簇路由机制(EEUC)。该算法考虑到了节点剩余能量这一因素,实现了节点间的能量消耗平衡,但仍没有解决簇首节点选择时随机性较大的问题。2006 年,卿利等^[13]提出了一种异构传感器网络的分布式能量有效成簇算法(DEEC)。该算法将节点剩余能量作为选择

簇首节点的主要因素,并且给出了计算最优簇头公式以及优化簇头比例公式,可是该算法没有考虑到节点在网络中所处的位置,仅以节点剩余能量为依据,存在靠近基站的节点由于承担过多的任务而过早能量耗尽的问题。2014 年,刘唐等^[14]提出了一种异构传感器网络的分簇算法(DUBP)。该算法首先利用能耗因子进行动态分区,再利用 Floyd 算法计算节点的路径因子,随后进行分簇。算法在一定程度上延长了网络寿命,但仅考虑普通节点间的能量消耗,却未考虑到簇首间的能量均衡。

总体上说,现有的分簇算法存在的问题主要有两点:一是在簇首选择时考虑的因素不够全面,具有较大的随机性,存在部分节点过早能量耗尽的问题;二是鲜有考虑到簇首节点间的能量均衡,使得靠近基站的簇首不仅要承担本簇的数据融合任务,且要为其其他簇进行数据转发,即存在“热区”问题。

2 NCIKP 方案设计

通过对传统的密钥预分配方案的研究,针对其在进行安全通信时未能很好地实现节点能量均衡的问题,给出了一种解决方案,即设计了一种针对异构传感器网络的基于分簇结构的密钥预分配方案。

2.1 基本假设

该方案假设共有 N 个传感器节点,随机分布在一个 $W * W$ 的正方形区域内,所有的节点是静止或者是微移动的,从而避免网络拓扑结构频繁改变。

表 1 为方案中的符号及其意义。

2.2 分簇

2.2.1 分簇准备

定义 1(节点到基站的距离):

$$d_{i,BS} = \partial \sqrt{\frac{K \times E_{BS}^{tran}}{E_{i,BS}^{rec}}} \quad (1)$$

其中, ∂ 表示距离—能量梯度 ($1 \leq \partial \leq 6$); K 表示一个常数; E_{BS}^{tran} 表示 BS 广播消息的信号强度; $E_{i,BS}^{rec}$ 表示节点 i 接收到 BS 发来消息时的信号强度^[15]。

定义 2(节点的邻接程度):与节点 i 之间的跳数不超过 2 跳的节点都是 i 的相邻节点。

$$N(i) = \{j \in S \mid i \neq j \wedge d(i,j) \leq 2\} \quad (2)$$

定义 3(节点的能量消耗率):

$$V(i) = \frac{E_{initial} - E_{current}}{r - 1} \quad (3)$$

定义 4(节点权值):

$$w(i) = d_{i,BS} * a + N(i) * b + v(i) * (1 - a - b) \quad (4)$$

2.2.2 簇首选择

(1) 阈值 $T(n)$ 的推导。

表1 方案中的符号及其意义

符号	意义
N	异构传感器网络的中传感器节点个数
W	节点所在正方形区域的边长
n	分簇结构中的分簇数
L	一个分簇中含有的节点数
CID	簇标识号
ID	节点标识号
$Ck_{i,BS}$	节点 i 与基站的会话密钥
i, j	传感器节点
$\varepsilon_{fs}, \varepsilon_{mp}$	发送节点的功耗系数
$K_{i,j} = K_{j,i}$	i, j 之间共享的密钥
s	密钥空间池
KID	密钥标识号
∂	随机数
$d(i, j)$	节点间的距离
w	节点权值
$E_{k_i}(\partial, CID)$	用密钥 k_i 加密 ∂ 和 CID
$d_{i,BS}$	节点 i 与基站的距离
CHK_i	簇首节点为 i 的簇的会话密钥
Hash	Hash 函数
r	轮询数
E_{total}	节点的初始能量
$E_{current}$	节点在第 r 轮中的剩余能量
α, b	权重因子(视具体应用环境而定)
P	节点成为簇首节点的概率

文献[13]提出计算优化簇头的公式:

$$k_{opt} = \frac{\sqrt{N}}{\sqrt{2\pi}} \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \frac{W}{d_{CH_BS}^2}$$

优化簇头比例为:

$$p_{opt} = \frac{k_{opt}}{N}$$

假设形成的簇共有 L 个节点,除去簇首节点,簇内还有 $L-1$ 个节点,则簇内节点到基站的平均距离可表示为:

$$D_{L_BS} = \frac{\sum_{j=1}^{L-1} d_{j_BS}}{L-1}$$

结合式(3)可推出簇内节点的平均损耗率为:

$$\bar{V}_L = \frac{\sum_{j=1}^{L-1} V(j)}{L-1}$$

结合式(2)可推出簇内节点的平均相邻节点数目为:

$$\bar{N} = \frac{\sum_{j=1}^{L-1} N_k(j)}{L-1}$$

综合上述分析,这里给出更适合异构传感器网络

的节点成为簇首节点的概率公式:

$$p_i' = p_{opt} \times \frac{d_{i,BS}}{D_{L_BS}} \times \frac{V_i}{V_L} \times \frac{N_k(i)}{\bar{N}} \tag{5}$$

在 LEACH 给出的阈值 $T(n)$ 计算公式的基础上进行改进,得到新的阈值计算公式:

$$T(i) = \begin{cases} \frac{p_i'}{1 - p_i'(r \bmod \frac{1}{p_i})} [\frac{d_{i,BS}}{D_{L_BS}} \times \frac{V(i)}{V_L} \times \frac{N_k(i)}{\bar{N}} + \\ (r \div \frac{1}{p}) (1 - \frac{d_{i,BS}}{D_{L_BS}} \times \frac{V(i)}{V_L} \times \frac{N_k(i)}{\bar{N}})] , i \in G \\ 0, \text{其他} \end{cases} \tag{6}$$

其中, G 为最近 $1/P$ 轮中还未当选簇首的节点的集合; r 为节点连续未当选簇首节点的轮数,一旦当选,将 r 重置为 0。

(2)簇首节点产生流程。

①通过节点与节点间、节点与基站间发送消息,每个节点分别算出自己到基站的距离、自己的邻接节点数、能量损耗速率即 $d_{i,BS}$, $N(i)$ 以及 $V(i)$ 。

②每个节点根据式(5)算出自己在本轮成为簇首的概率 p_i' 。

③节点根据式(6)计算成为簇首节点的概率门限阈值 $T(i)$ 。

④若 $p_i' < T(i)$,则节点 i 成为本轮的簇首节点,否则放弃成为簇首。

⑤其余节点在本轮竞争结束前都保持睡眠状态,在本轮竞选结束后,下一轮竞选按照上述四个步骤重复进行。

2.2.3 分簇形成

(1)簇半径计算公式。

文中采用文献[12]中节点的竞争半径公式:

$$R_i = (1 - C \frac{d_{max} - d(i,BS)}{d_{max} - d_{min}}) R_{max} \tag{7}$$

其中, d_{max} 为网络中节点距离基站 BS 的最远距离; d_{min} 为网络中节点距离基站 BS 的最近距离; C 为 0-1 之间的一个常数; R_{max} 为网络中允许的最大竞争半径。

(2)每轮非均匀成簇流程。

①节点计算自己成为簇首的概率 $p(i)$ 以及阈值 $T(i)$ 。

②如果满足 $p_i' < T(i)$,节点成为临时簇首节点。

③临时簇首节点广播自己的标识号 ID,竞争半径 R_i 以及权值 $w(i)$ 。

④若节点 j 收到 i 发送来的消息,便开始接下来的判断。

⑤若满足 $d(i, j) < R_j$ OR $d(i, j) < R_i$, j 便加入以 i 为临时簇首的簇。

⑥ i 检查是否本簇中所有节点的权值都小于自己的权值,若是,则广播一条消息 BEHEAD_MSG(ID) 给所有相邻的临时簇首节点,通知自己成为本轮簇首。

⑦若 i 收到本簇中节点 j 成为簇首的广播消息,则 i 必须放弃本轮簇首的机会,然后广播一条退出消息 QUIT_MSG(ID)。

⑧若 i 收到一条来自簇中 j 的退出请求消息 QUIT_MSG,则立刻将 j 从簇中删除。

⑨在每轮簇首节点竞争结束后,其余普通节点就从睡眠状态恢复过来,所有的簇首节点广播一条 CH_MSG 到全网,普通节点判断收到的来自不同簇首节点的消息,选择加入一个信号最强的簇中,然后给该簇首节点发送消息 JOIN_CH_MSG,通知其自己成为它的簇成员。此时该轮的成簇过程完成。

2.3 密钥预分配

此阶段包括四个部分:基站为簇首分配密钥、簇首为簇内节点分配密钥、同一簇内节点的通信、不同簇内节点的通信。

2.3.1 基站为簇首分配密钥

基站产生一个密钥池 S ,为每一个密钥分配一个唯一的编号 KID;在上面阶段通过竞争当选簇首的节点向 BS 发送 $Ck_{i,BS}(ID, d_{i,BS})$,告知基站自己成为了簇首;基站根据 $d_{i,BS}$ 来给簇分配一个唯一的编号 CID ($d_{i,BS}$ 越小, CID 越小);簇首节点广播消息 (CID, ID) 来发现自己的邻接簇,发送给基站自己邻接簇的 CID,让基站知道整个网络的簇首之间的相邻关系;基站根据簇首的邻接簇数目以及邻接簇已分配密钥的情况为每个簇分配一定的密钥,构成自己的密钥池。

2.3.2 簇首为簇内节点分配密钥

簇首生成本簇内的会话密钥 CHK,簇首节点从上面分配得到的密钥池中随机选择 r 个密钥分配给簇内节点,构成节点的密钥环,分配的密钥数不宜过多也不宜过少,过少会出现“孤立点”,从而导致通信困难;过多可能会造成单个节点被捕,整个网络瘫痪的危险。

2.3.3 同一簇内节点的通信

簇内节点 i 随机选择自己密钥环中的一个密钥来加密一个含有随机数和簇标识号的数据包,即 $E_{k_i}(\partial, CID)$,之后再用本簇内的会话密钥 CHK 来第二次加密,即 $E_{CHK}\{E_{k_i}(\partial, CID)\}$,随后在簇内广播,簇内其他节点 j 收到此消息后,用 CHK 来解密收到的消息,便得到 $E_{k_i}(\partial, CID)$,再从自己密钥环中取出一个密钥来加密 ∂ 和 CID,即 $E_{k_j}(\partial, CID)$ 。与收到的消息进行比较,若结果相同,即 $K_i = K_j$,此时便可取 $K_{i,j} = K_i = K_j$ 为簇内节点 i, j 的会话密钥。按此方法,在一定的时间过

后,簇内节点与其邻接节点便可找到它们之间的通信密钥了。若 2 个节点没有找到彼此的通信密钥,则需要簇内与其有通信密钥的节点作为中间节点,此时同一簇内的所有节点便可以建立起连接。

2.3.4 不同簇内节点的通信

为安全起见,规定不同簇内节点通信必须选择簇首节点作为中间节点。假设 2 个位于不同簇的节点 i, j 想要通信,它们分属的簇头分别为 C_1, C_2 ,若 2 个节点间有 k_1, k_2, \dots, k_L 个相同密钥,则利用 hash 函数计算,得到 $\text{hash}(k_1 \parallel k_2 \parallel \dots \parallel k_L)$,来作为二者的共享密钥 $K_{i,j}$,节点 i 用 $K_{i,j}$ 将要发送的数据进行加密,得到 $E_{K_{i,j}}(\text{数据})$,然后用 CHK_1 进行第二次加密,即把 $E_{\text{CHK}_1}\{E_{K_{i,j}}(\text{数据})\}$ 发送给 C_1 , C_1 用 CHK_1 解密,得到 $E_{K_{i,j}}(\text{数据})$; C_1 用其与 C_2 的密钥 K_{C_1, C_2} 加密 $E_{K_{i,j}}(\text{数据})$,随后发给 C_2 ; C_2 用 K_{C_1, C_2} 解密,然后用 CHK_2 加密得到 $E_{\text{CHK}_2}\{E_{K_{i,j}}(\text{数据})\}$,发给 j , j 随后两次解密得到原始数据,通信完成。

3 安全性分析及性能分析

3.1 安全性分析

在该方案中,簇首节点需要向基站注册自己的身份以及邻接簇情况,因此即使一个簇首被攻击者冒充,也会立即被基站检测出来;基站根据簇首邻接簇情况为其分配密钥,随后簇首再从自己的密钥池中随机取部分密钥分配给簇内节点,因此不同节点被分配到相同密钥的概率较低;在同一个簇内节点通信时,若采用以往算法中通过广播节点密钥来建立会话密钥的方法,则会增加被攻击的概率,因此该方案中同簇节点建立会话密钥时采用节点取自己的密钥来加密一个随机数和本簇标识号并与其他节点加密结果比较的方法,提高了安全性;此外该方案规定,在不同簇内节点通信时必须经过簇首节点的转发,进行二次加密,可以保证即使一个簇被攻击,也不会影响到其他簇的安全,且利用了 hash 函数的单向性,有效防止攻击者从单个节点的密钥来推算出节点间的通信密钥。

3.2 性能分析

利用 Matlab 对文中分簇算法与 LEACH 和 EEUC 协议进行性能比较分析。采用文献[10]中提出的无线通信系统能量消耗模型来进行计算。

(1) 传送一个 1 bit 的数据包到距离 d 的节点需耗费的能量为:

$$E_{Tx}(l, d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2, & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4, & d \geq d_0 \end{cases}$$

(2) 接收一个 1 bit 字节的数据包需要的能量为:

$$E_{Rx}(l) = lE_{elec}$$

其中, E_{elec} 为发送节点和接收节点的功耗; $d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} = 87\text{ m}$ 进行数据融合所需能量 E_{DA} 。

表2 为仿真采用的参数表;图1 为仿真场景图。
表2 仿真参数表

参数	数值
区域范围($W * W$)	200 * 200
节点个数(N)	1 类节点 100 个,2 类节点 100 个
节点初始能量	1 类节点 1 J,2 类节点 2 J
P	0.05
E_{elec}	50 nJ/bit
ε_{fs}	10 pJ/(bit • m ²)
ε_{mp}	0.001 3 pJ/(bit • m ⁴)
E_{DA}	5 nJ/bit/signal
基站位置	(100 m,100 m)
数据包大小	1 类节点 2 000 bits 2 类节点 4 000 bits

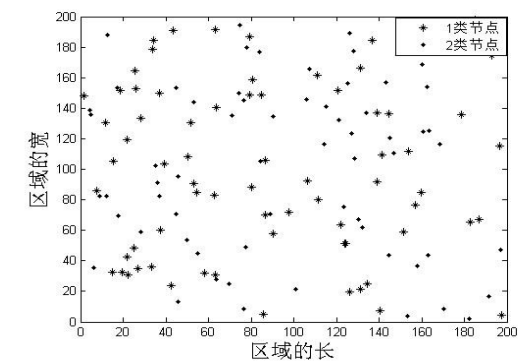


图1 200 个节点随机布于 200 m * 200 m 的区域
死亡节点个数和网络剩余能量随着进行的轮数变化情况比较见图 2 和图 3。

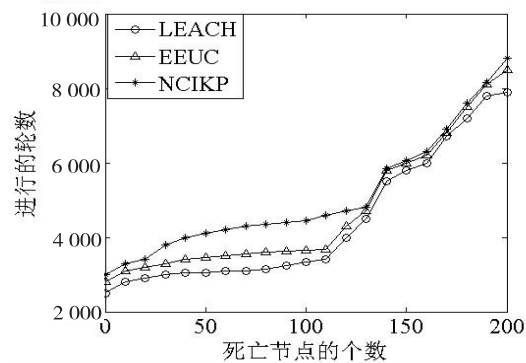


图2 死亡节点个数随着进行的轮数变化情况比较

4 结束语

文中设计了一种针对异构传感器网络的基于分簇结构的密钥预分配方案 (NCIKP)。在该方案中,首先给出了一种新的分簇算法,该算法可以有效地均衡节

点间的能量消耗;在密钥预分配过程中,将分别对簇首节点和簇内节点进行预分配,以降低节点被分配到相同密钥的概率;同一簇内节点在建立会话密钥时,只需随机取一个密钥加密一个随机数以及本簇标识号,并与其余节点加密结果相比较即可,避免了广播密钥带来的被攻击的风险;不同簇节点通信时,规定必须经过簇首节点的转发,进行二次加密,因此即使一个簇被攻击,也不会影响到其他簇的安全,此外还加入了 Hash 函数,利用其单向性来进一步提高网络的安全性。

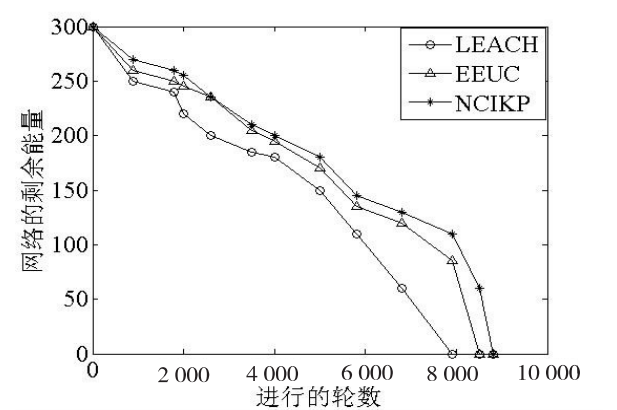


图3 网络剩余能量随着进行的轮数变化情况比较
通过仿真实验表明,该方案具有较强的安全性,此外获得了更好的能量利用率以及更长的网络生命周期。
方案暂未考虑到异构传感器网络中节点的移动性这一问题,此外如何降低节点的计算和存储开销也将是下一步工作研究的重点。

参考文献:

[1] 苏金树,郭文忠,余朝龙,等. 负载均衡感知的无线传感器网络容错分簇算法[J]. 计算机学报,2014,37(2):446-456.

[2] 孙力娟,魏 静,郭 剑,等. 面向异构无线传感器网络的节点调度算法[J]. 电子学报,2014,42(10):1907-1912.

[3] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor network[C]//Proc of 9th ACM conf on computer and communication security. Washtington,DC, USA: ACM,2002;41-47.

[4] Chan H, Perrig A, Song D. Random key pre-distribution scheme for sensor networks[C]//Proceedings of IEEE 2003 symposium on security and privacy. Berkeley, CA, USA: IEEE,2003;197-210.

[5] Du W,Deng J,Han Y. A key management scheme for wireless sensor networks using deployment knowledge[C]//Proceedings of IEEE INFOCOM'04. Hong Kong, China:IEEE,2004;586-597.

[6] 王小刚,石为人,周 伟,等. 一种基于二次型的无线传感

表 4 文中算法与文献[7]算法的比较

攻击类型	文中算法	文献[7]算法
JPEG 压缩(60% 压缩比)	0.997 0	0.990 7
JPEG 压缩(40% 压缩比)	0.994 5	0.941 6
JPEG 压缩(20% 压缩比)	0.991 8	0.806 2
高斯噪声(0.004)	0.986 4	0.817 7
椒盐噪声(0.01)	0.989 3	0.932 0
中值滤波(3×3)	0.996 2	0.945 7

的盲水印算法不但具有较好的保真度,对于各种攻击也具有较强的鲁棒性。

将来的主要工作在于研究嵌入位的不同选择对于实验结果的影响,以找到更加有效的方法来实现水印的嵌入。

参考文献:

[1] 薛胜男,陈秀宏. 基于混沌加密和 SVD 的数字图像水印算法[J]. 计算机工程,2012,38(19):107-110.

[2] 熊祥光,王 力. 一种改进的 DWT-SVD 域参考水印方案[J]. 计算机工程与应用,2014,50(7):75-79.

[3] 朱 光,张军亮. 基于 SVD 和小波包分解的自适应鲁棒水印算法[J]. 计算机应用研究,2013,30(4):1230-1233.

[4] 雷 蕾,郭树旭,王 雷. 基于小波变换的 SVD 数字图像水印算法研究[J]. 计算机仿真,2013,30(9):169-172.

[5] 陈 军,张 伟,杨华千,等. 一种基于小波变换和神经网络的数字水印算法[J]. 计算机科学,2011,38(6):142-144.

[6] 张秋余,李 凯,袁占亨. 基于混沌和 SVD-DWT 的稳健数字图像水印算法[J]. 计算机应用研究,2010,27(2):718-720.

[7] 叶 闯,沈益青,李 豪,等. 基于人类视觉特性(HVS)的

离散小波变换(DWT)数字水印算法[J]. 浙江大学学报:理学版,2013,40(2):152-155.

[8] 季 燕. 基于 DCT 的自适应盲数字水印[J]. 计算机科学,2013,40(7):129-130.

[9] 廖 斌,任美玲,徐俊刚. 一种基于压缩感知的盲数字水印算法[J]. 计算机应用与软件,2014,31(2):307-311.

[10] Ho A T S,Shen J,Chow A K K,et al. Robust digital image-in-image watermarking algorithm using the fast Hadamard transform[C]//Proceedings of the international symposium on circuit and system 2003. [s. l.]:IEEE,2003:826-829.

[11] Saryazdi S,Nezamabadi-Pour H. A blind digital watermark in Hadamard domain[C]//Proceedings of world academy of science,engineering and technology. [s. l.]:[s. n.],2005:498-502.

[12] 李红丽,赖惠成. 基于哈达玛变换和奇异分解的四个彩色图像水印算法[J]. 计算机应用,2010,30(11):3025-3027.

[13] Niu Shaozhang,Niu Xinxin,Yang Yixian. Digital watermarking algorithm based on LU decomposition[J]. Journal of Electronics &Information Technology,2005,26(10):1620-1625.

[14] 王树梅,赵卫东,王志成. 一种基于 LU 的小波域自适应数字水印算法[J]. 微电子学与计算机,2008,25(12):76-79.

(上接第 81 页)

器网络密钥管理方案[J]. 电子学报,2013,41(2):214-219.

[7] Duarte-Meloe J,Liu M Y. Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks[C]//Proceedings of IEEE GLOBEC-OM. Taipei:IEEE,2002:21-25.

[8] 马春光,尚治国,王慧强. 基于区域的异构无线传感器网络密钥管理[J]. 通信学报,2009,30(5):74-81.

[9] 马春光,张秉政,孙 原,等. 基于按对平衡设计的异构无线传感器网络密钥预分配方案[J]. 通信学报,2010,31(1):37-43.

[10] Heinzelman W,Chandrakasan A,Balakrishan H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications,2002,1(4):660-670.

[11] Younis O,Fahrmy S. Heed:a hybird,energy-efficient,distributed clustering approach for ad-hoc sensor networks[J]. IEEE Trans on Mobile Computing,2004,3(4):660-669.


[12] 李成法,陈贵海,叶 懋,等. 一种基于非均匀分簇的无线传感器网络路由协议[J]. 计算机学报,2007,30(1):27-36.

[13] Qing Li,Zhu Qingxin,Wang Mingwen. A distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks[J]. Journal of Software,2006,17(3):1282-1291.

[14] 刘 唐,孙彦清. 基于负载均衡和最短路径的异构无线传感器网络成簇算法[J]. 计算机科学,2014,41(10):169-172.

[15] 刘 唐,汪小芬,杨 进. 基于相对距离的多级能量异构传感器网络成簇算法[J]. 计算机科学,2012,39(8):119-121.

基于非均匀分簇的HWSN密钥预分配方案的研究

作者：[黄慧娟](#)，[许勇](#)，[张海](#)，[HUANG Hui-juan](#)，[XU Yong](#)，[ZHANG Hai](#)
作者单位：[安徽师范大学 数学与计算机科学学院, 安徽 芜湖, 241003](#)
刊名：[计算机技术与发展](#)
英文刊名：
年，卷(期)：2016 (2)

引用本文格式：[黄慧娟](#). [许勇](#). [张海](#). [HUANG Hui-juan](#). [XU Yong](#). [ZHANG Hai](#) [基于非均匀分簇的HWSN密钥预分配方案的研究](#)[期刊论文]-[计算机技术与发展](#) 2016 (2)