信息隐藏中伪随机序列碰撞问题的算法改进

刘忠义 沈祥辰 倪绿林 许春根
(南京理工大学理学院 南京 210094)

摘 要 将秘密信息嵌入到有限大的载体图片的过程中,一般利用伪随机序列来选取要嵌入信息的像素点的位置。当秘密信息足够大时,伪随机数发生器产生的伪随机序列会重复出现,从而产生碰撞。如果选择跳过重复的位置,嵌入到有限大的载体图片中的秘密信息量将受限。因此,提出了一种改进算法,当伪随机数发生器产生的序列重复出现时,不跳过重复位置,正常进行嵌入操作,并将该重复位置上的操作过程以某种形式记录并保存;逆向提取时,通过密钥和该操作记录提取密文。该改进算法结合了密码学与信息隐藏技术,极大地扩展了嵌入到有限大的载体图片中的秘密信息的隐藏量,提高了信息隐藏过程的安全性。

关键词 图像处理,信息隐藏,密码学,流密码,伪随机变换,碰撞,安全性,信息隐藏量
中图法分类号 TP309 **文献标识码** A

Algorithm Improvement of Pseudo-random Sequence Collision in Information Hiding

LIU Zhong-yi SHEN Xiang-chen NI Lu-lin XU Chun-gen
(School of Science, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract In the process of embedding secret information into a limited large vector image, a pseudo-random sequence is generally used to select the position of the pixel to be embedded in the information. When the secret information is large enough, the pseudo-random number generated by the pseudo-random number generator would be repeated, thus resulting in collision. If we choose to skip all the duplicate locations, the amount of confidential information which had been embedded in a limited large vector image would be limited. Therefore, this paper proposed an improved algorithm. When the sequence generated by the pseudo-random number generator reoccurs, the repeated position will not be skipped and the embedded operation will be performed normally, and the operation process at the repeated position will be recorded and saved in some form. In reverse extraction, the key and this action record are used to extract the ciphertext. The improved algorithm, combined with cryptography and information hiding, greatly expands the amount of secret information hidden in a limited number of pictures and improves the security of information hiding.

Keywords Image processing, Information hiding, Cryptography, Stream cipher, Pseudo-random transform, Collusion, Security, Quantity of information hiding

1 引言

当下,信息安全和通讯安全的重要性与日俱增,信息安全领域的技术也越来越受到重视,其中密码学技术发展迅速,并且已经广泛应用于国防、军事、金融、商业等诸多领域。在这些领域中,人们需要通过公共信道传输机密信息,以保证所传输的机密信息的安全。由于在公共信道传输,任何攻击者都可以轻易截获传输的信息,因此发送方必须隐藏和加密传送的机密信息,信息隐藏技术由此诞生并得以迅速发展。

信息隐藏技术是指发送者将秘密信息嵌入到大量无关信息(即载体)中,并通过公共信道将秘密信息和载体同时传送给接收者,在传输过程中保证秘密信息的完整性的技术。

信息隐藏主要应用在需要安全保密通信的领域,发送者通常利用多媒体信息中的冗余空间携带隐蔽信息,并传递伪装后的秘密信息。信息隐藏技术还包括对隐藏信息的分析和检测。

替换技术是目前应用最广泛的信息隐藏方法,也是最直观的在载体中隐藏信息的方法。替换技术利用人的感官系统对物理随机噪声不敏感的特性,用秘密信息比特替换掉随机噪声,以隐藏秘密信息。实现替换技术最为常见的算法是最低有效位(LSB)算法。然而 LSB 算法中秘密信息的隐藏量十分受限,如何扩大载体中的信息隐藏量一直是研究的热点课题。

2 基本知识

表 1 包含本节用到的一些具有特殊含义的符号及其含

本文受江苏省自然科学基金(BK20141405),南京理工大学本科生科研训练项目及毕业设计重点课题项目立项资助。
刘忠义(1995-),男,硕士生,主要研究方向为信息安全与密码技术应用;**沈祥辰**(1996-),男,主要研究方向为数学与应用数学;**倪绿林**(1991-),男,硕士生,主要研究方向为信息安全与密码技术应用;**许春根**(1969-),男,博士,教授,CCF 会员,主要研究方向为信息安全与密码技术应用,E-mail:xuchung@njust.edu.cn(通信作者)。

义，主要用于描述伪随机变换过程中的一些重要概念。

表 1　本节用到的符号

符号名	含义
$L(m)$	秘密信息的二进制长度
m_i	第 i 个秘密信息比特值
j_i	第 i 个秘密信息 $bite$ 嵌入的位置
$\{j_1,\cdots,j_{L(m)}\}$	嵌入位置序列的集合
$\{k_1,k_2,\cdots,k_{L(m)}\}$	伪随机数发生器产生的伪随机序列

2.1　BMP 图像(以真彩色图像为例)

作为常见的信息隐藏载体，BMP 图像的基本单元是像素，其中每英寸的像素数(PPI)表示分辨率的大小。BMP 图像采用 RGB 色彩模式，即每个像素点由三原色红(R)、绿(G)、蓝(B)叠加成色，真彩色图像中每个像素点占 3 个字节，每个的值用 8 位(1 字节)表示，RGB 色彩模式共有 $2^8=256$ 种颜色。由于人类感官系统的不敏感性，仅仅改变像素点字节的最低位或最低几位时，人眼无法察觉出颜色的变化。因此，改变 BMP 图像中任一像素点值的最低位或最低几位，对整个图像没有明显影响，用秘密信息替换掉这些不重要的像素点，就可以达到隐藏信息的目的。

LSB 算法就是将秘密信息嵌入到载体图像像素值的最低有效位(也称最不显著位)，改变最低有效位对整个载体图像的品质影响最小。

2.2　伪随机置换[1]

在将秘密信息嵌入到载体图像时，如果能得到全部载体的元素，那么就可以利用伪随机序列把秘密信息比特随机地分散在整个载体中。嵌入信息流程如下。

载体子集的选取：将伪随机数发生器产生的伪随机序列 $\{k_1,k_2,\cdots,k_{L(m)}\}$ 作为载体子集的位置索引序列，即 $\{j_1,\cdots,j_{L(m)}\}=\{k_1,\cdots,k_{L(m)}\}$。将第 i 个秘密信息隐藏在 j_i 的最低位。

嵌入信息：在载体图像中选择出的像素点组成的子集 $\{j_1,\cdots,j_{L(m)}\}$ 上执行替换操作，同时将 j_i 的最低比特位用 m_i ($m_i=0$ 或 1)替换。

提取过程：找到嵌入信息的伪装元素子集 $\{j_1,\cdots,j_{L(m)}\}$，并从中抽取最低比特位的信息，逆向排列后得到秘密信息。

2.3　碰撞问题

有限大的载体图片中可选择的像素点数量有限，生成的伪随机序列大小也有限，因此当秘密信息足够大时，伪随机数发生器产生的序列会重复出现，重复选取像素点的过程称为碰撞[1]，重复的像素点称为碰撞点。对于碰撞问题，一般的处理方法是跳过碰撞点，即发生碰撞时，跳过重复选取的像素点，直到不出现碰撞为止。该方法使得有限大的载体图片中最大隐藏信息量十分有限。

3　改进算法

3.1　算法原理

在有限大的载体图片中嵌入信息时，若出现碰撞，我们则不跳过碰撞点，而是正常嵌入隐藏信息，并同时记录在碰撞点嵌入信息的操作过程。其中发送方和接收方对载体图片上各像素点上信息的操作过程如下。

发送方：用数组记录像素点上嵌入的信息比特值与该点的最低有效位的“异或”值，存储在文件 A(钥匙文件)中并加密。嵌入完成后，通过公共信道发送伪装载体图片和伪随机数生成器种子密钥。

接收方：首先解密文件 A 和伪随机数发生器种子密钥，逆序提取出每一个点的信息。提取时，该像素点的最低有效位即为秘密信息；然后提取文件 A 中记录的像素点的操作信息与伪装载体在该点最低有效位的值(即这次提取的秘密信息)，取这两个值的“异或”，最后将“异或”值与该像素点的最低有效位替换。如此，像素点的值被还原到嵌入之前。

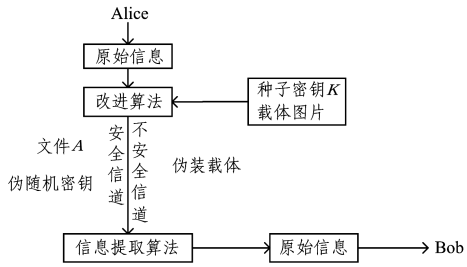


图 1　改进算法原理图

3.2　算法实现

表 2 是改进算法实现过程中使用到的一些量的符号及其意义，主要用来描述被操作的文件的属性和算法执行过程中的变量。

表 2　本节用到的符号

符号名	含义
A	存储操作信息的文件，即钥匙文件
BMP	载体图片名
$BMP(n)$	载体图片第 n 次嵌入位置的最低有效位(0 或 1)
$M(n)$	第 n 次嵌入的信息(0 或 1)
$T(n)$	第 n 次操作信息(0 或 1)
$bite[L(m)]$	顺序存储每次嵌入的操作信息 $T(n)$
$xulie[L(m)]$	顺序存储伪随机序列，即位置序列
$xinxi[L(m)]$	顺序存储所提取出的秘密信息 $bite$
K	生成伪随机序列的种子密钥
BMP'	伪装载体图片
$BMP'(n)$	伪装载体图片第 n 次提取位置的最低有效位(0 或 1)

3.2.1　嵌入

建立两个数组：int $bite[L(m)]$. $xulie[L(m)]$。

Step 1　由密钥 K 生成伪随机序列，并将该伪随机序列作为嵌入位置序列顺序存入数组 $xulie[L(m)]$中；

Step 2　$T(n)=BMP(xulie[n])\wedge M(n)$，即最低有效位与第 n 次嵌入的秘密信息的异或(0 或 1)；

Step 3　$BMP(xulie[n])=M(n)$，即嵌入过程执行替换操作；

Step 4　$bite[n]=T(n)$，即将操作信息存入数组 $bite[L(m)]$。

所有信息嵌入完成后生成伪装载体图片 BMP'，将数组 $bite[L(m)]$存入文件 A。

实验结果如图 2 所示。

(a)原始载体图片 BMP(嵌入前)　　(b)待隐藏的信息

图 2　嵌入前的预备文件

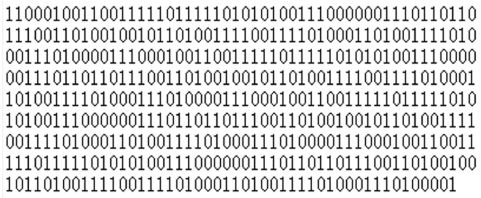
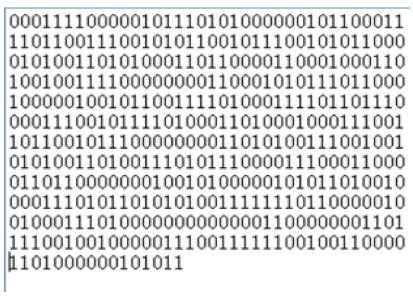


图 3 秘密信息的二进制码

(a)伪装载体图片(嵌入后)



(b)生成的文件 A

图 4 嵌入完成后生成的文件

比较图 2 和图 4,人眼无法分辨出嵌入秘密信息前后载体图片的改变。

比较图 2(b)和图 3,由于嵌入位置是伪随机选取的,不能由文件 A 和 BMP' 通过分析直接得出原始信息,因此原始信息的二进制码和生成的文件内容之间没有规律可言。

3.2.2 提取

建立两个数组:int $xulie[L(m)]$,$xinxi[L(m)]$。

Step 1 由密钥 K 生成伪随机序列,并按顺序将该序列存入数组 $xulie[L(m)]$。

Step 2 解密并提取文件 A 的信息 $bite[L(m)]$。

Step 3 由于碰撞点处存储多个信息,因此只能按伪随机序列的逆序提取,$xinxi[n]=BMP'(xulie[n])$,$n=L(m),\cdots,1$,因为嵌入执行替换操作,所以 $BMP'(xulie[n])$ 就是秘密信息第 n 次嵌入的信息。

Step 4 $BMP'(xulie[n])=BMP'(xulie[n])\wedge bite[n]$,该操作使得该像素点的最低有效位还原为这次嵌入前的数值。若该像素点是碰撞点,则回到该点前一次嵌入的值,即该点前一次嵌入的秘密信息。

所有信息提取完成后,将秘密信息的 $bite$ 值(即数组 $xinxi[L(m)]$)还原即可得到嵌入的秘密信息。

(a)提取出的秘密信息 (b)还原出的原始载体图片

图 5 提取操作获得的文件

4 算法分析

4.1 改进算法的密码学原理

改进算法比原算法在加密后多出一个钥匙文件 A,下面来分析这个文件的特性。

表 3 列出了流密码定义中的一些基本概念的符号表示,并给出了它们的具体含义。

表 3 本节用到的符号

符号名	含义
x	明文信息
y	密文信息
z_i	第 i 次加密的密钥
$z=z_1z_2z_3\cdots z_n$	密钥流
$e_z(x)$	加密函数
$x=d_z(y)$	解密函数
z_0	初始密钥

改进算法从密码学的角度出发相当于实现了一次流密码[4],但又不仅仅局限于密码学,是密码学和信息隐藏的有机结合。而这个钥匙文件就是流密码加密后的秘密文件,它具有所使用的流密码的安全性。

根据流密码的理论,流密码就是用一个初始密钥 z_0 来生成第一个加密信息的密钥 z_1。第一次加密后由 z_1 生成第二个密钥 z_2。用 z_2 来加密第二个信息。由此循环就可以由初始密钥生成一个密钥流 $z=z_1z_2z_3\cdots z_n$。

改进算法的流密码原理如下。

明文信息 x:待隐藏的信息;

密文信息 y:文件 A;

初始密钥 z_0:伪随机序列生成器种子密钥 k;

生成密钥流的算法:由初始密钥 z_0 生成伪随机序列,再由伪随机序列找出嵌入位置序列,嵌入位置序列即为密钥流 $z=z_1z_2z_3\cdots z_n$;

加密函数 $e_z(x)$:嵌入操作被视为加密函数,包括原始载体图片。

解密函数 $x=d_z(y)$:提取操作被视为解密函数,包括伪装载体图片。

改进算法对载体图像的处理严格符合 LSB 信息隐藏的原理;伪装载体图像也是人眼无法察觉的,是可以在公共信道上传输的图片。因此它同时实现了信息隐藏和流密码,其流密码原理图如图 6 所示。

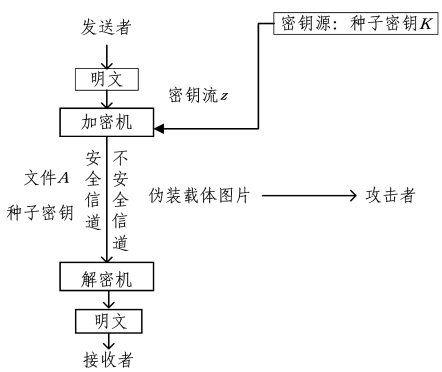


图 6 改进算法的流密码原理图

4.2 与传统伪随机变换法的比较

(1)隐藏量:传统伪随机变换法中,处理碰撞问题时,选择跳过碰撞点,这使得有限大的载体图片中的信息嵌入量极其有限。改进算法在处理碰撞问题时不跳过碰撞点,使得有限

大的载体图片可以隐藏任意大小的秘密信息，解决了 LSB 信息隐藏量不足的缺点。

表 4　改进算法与经典算法最大信息隐藏量的比较

算法	最大信息隐藏量
LSB	≤图片像素点数×3
伪随机变换	≤图片像素点数×3
改进算法	任意大

注：像素点数×3 是因为一个像素点有 R，G，B 3 个最低有效位

(2)解密条件：将伪装载体图像和文件 A 独立发送，其中文件 A 用密码学方法加密发送，伪随机数生成器种子密钥 k 由双方约定或加密发送，伪装载体在公共信道发送，则攻击者需同时满足以下条件才能破解信息：

1)截取伪装载体(不易察觉)；

2)取得种子密钥 k(k 用于生成索引序列，由双方约定或者加密发送)；

3)截取文件 A 并且破译(加密发送)；

4)将文件 A 和伪装载体正确匹配(有可能截获不同秘钥 k 加密的不同秘密信息的钥匙文件 A)。

传统的伪随机变换法只要满足条件 1)和条件 2)就能被完全破译，安全性极低。改进后的算法切实解决了该缺点，极大地提高了信息隐藏过程的安全性。

(3)算法复杂度：假设一次替换操作的时间复杂度为 O(1)，则传统算法的时间复杂度为 O(n)。改进算法除了要执行替换操作，每一步还要执行“异或”操作和存入数组。这两步和替换操作的算法复杂度相同，因此改进算法的算法复杂度为 3O(n)。两者的算法时间复杂度在同一个量级上。

4.3　安全性分析

(1)若攻击者在没有文件 A，只有嵌入位置序列(即拥有伪随机数发生器种子密钥)和伪装载体的情况下尝试破解信息。类似于密码学中加密方案的安全性条件，我们假设伪装的安全性不依赖于嵌入过程所使用的算法的安全性，而是依赖于伪装载体的不可感知性和伪随机序列的安全性。

我们可以认为攻击者在知道索引序列的情况下，可以根据伪装载体像素最低有效位的值解出非碰撞点和碰撞点的表层(该点最后一次)隐藏信息。但是没有文件 A，攻击者无法在提取后恢复出图片这次隐藏之前的状态。因此他如果尝试解出碰撞点的下一个信息，每次都会有两种可能的结果。

设一次嵌入完成后，图片上有 n 处碰撞点，每个碰撞点平均碰撞了 m 次，则该点有 $m+1$ 次信息嵌入(只嵌入一次不称为碰撞)。但攻击者能解出表层的信息，因此每个碰撞点有 m 次嵌入的信息解不出来。假设攻击者对这些解不出来的信息进行穷举法搜索，那么他将面临一个基数为 2^{mn} 的所有可能明文组成的空间。因此，在伪随机数发生器种子密钥和伪装载体不能保证安全传输的情况下，原始信息大小一定时，应选取更小的载体图片来隐藏信息以获取更大的安全性。

而传统 LSB 方法在上述假设下是可以被完全破译的。这就相当于传统算法把信息隐藏在载体的“表面”，而改进算法则将更多的信息隐藏在载体“表面”之下。

(2)当秘密信息量足够大时，图片的每一个像素点几乎都会被选取，但这并不影响伪随机选取像素点位置的初衷。因为图片的统计特性与秘密信息的统计特性不同，伪随机选取像素点就是为了伪装载体的各个部分的统计特性相同。若像素点全部被选取，则显然图片各个部分的统计特性是一样的。

(3)一个载体图片可被选择的嵌入位置数是固定的。当待嵌入的秘密信息足够大时，载体图片会出现很多碰撞点，而且每个碰撞点碰撞的次数可能也很大，即在一个碰撞点嵌入了大量的数据信息。其安全性问题可以分为以下两种情况：

1)伪装载体图像被攻击，即某嵌入点的最低有效位被篡改。为了应对这种攻击，可以把碰撞点某次嵌入后的最低有效位作为纠正码存于文件 B 中，用于纠正载体图片在该点的最低有效位的值。即在碰撞点，每隔固定嵌入次数就设置一个纠错位，用于检验当前最低有效位是否正确并纠正错误。这样，如果对秘密信息进行纠错编码，那么只要碰撞点提取错误的次数足够小就能进行纠错。

2)文件 A 被攻击，某些位置的操作信息被修改。这样会导致碰撞点某一次提取失败。在这次错误提取后，最低有效位恢复错误，导致之后的碰撞信息提取错误。如情形 1)，可以在碰撞点每隔几次嵌入就把最低有效位作为纠正码存入文件 B，用于纠正某次错误提取后的最低有效位的值。

这样接收者可以用文件 A 来提取，在提取过程中用文件 B 来纠错，以增加提取出的信息的准确率。

(4)如果伪装载体没有受损，那么此算法最终可以恢复图片的原始状态。接收者可以通过比较原始图片和恢复出的图片的最低有效位来判断是否被攻击和串改。

(5)由于能最终恢复出原始载体，我们可以使用同一个原始载体先后嵌入 n 个秘密信息文件。若要提取出全部 n 个秘密信息文件，则必须正确地以秘密信息文件嵌入时的反序来提取。如果攻击者不能获取嵌入顺序，那么他将面临 $n!$ 种可能的结果。

(6)由 4.1 节的分析可知，种子密钥 k 的安全性在改进算法中起着重要作用，因此应侧重种子密钥 k 的安全性保证。

结束语　改进算法是对在碰撞点操作的改进，对嵌入时的数学算法没有做定性要求，因此其他对 LSB 的一些嵌入算法上的改进对本文的改进算法也同样适用。如文献[3]提出，可以通过随机地修改像素值的 LSB，打破 LSB 替换算法的值对关系，使得安全性有了质的提高，其对本文的改进算法也同样适用。

载体可隐藏的信息量不受载体图片大小的制约，可以隐藏任意大的信息。因此，改进算法实现了比传统方法更高的安全性。改进算法的安全性不仅仅依靠隐藏的不可感知性，而且依赖于流密码的安全性，将密码学和信息隐藏自然地结合在一起。

参 考 文 献

[1] AL-DMOUR H, AL-ANI A. Quality optimized medical image information hiding algorithm that employs edge detection and data coding[J]. Comput Methods Programs Biomed, 2016, 127: 24-43.

[2] YUE X, ZHOU C, XING Y P, et al. Improved LSB Algorithm of Image Hiding Based on Randomness[J]. Applied Mechanics & Materials, 2015, 733: 926-930.

[3] JUNEJA M, SANDHU P S. Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images[J]. In-

dian Journal of Applied Research,2011,3(5):118-120.
[4] 钮心忻. 信息隐藏与数字水印[M]. 北京:北京邮电大学出版社,2004.
[5] 马文姬,张煜林. 传统 LSB 图像隐藏算法的优化研究[J]. 电子产品世界,2016,23(9):61-63.
[6] 陈铭,张茹,刘凡凡,等. 基于区域相关性的 LSB 匹配隐写分析[J]. 通信学报,2010,31(3):1-11.
[7] STINSON D R. Cryptography Theory and Practice (Third Edition)[M]. 北京:电子工业出版社,2009.
[8] 柏森,朱桂斌,曹玉强. 信息隐藏算法及应用[M]. 北京:北京国防工业出版社,2015.
[9] 刘洁. 信息隐藏技术及应用[J]. 现代情报,2004,24(6):204-205.
[10] 奚玲,平西建,张涛. 基于相邻灰度值对互补嵌入的 LSB 匹配隐写改进算法[J]. 计算机科学,2010,37(9):101-104.
[11] 郭立甫,高媛,王嘉祯. 图像 LSB 密写的信息隐藏量分析[J]. 计算机工程,2008,34(4):157-161.

(上接第 319 页)

将影响节点后续的充电请求情况,如果对某一节点在充电时分配的能量较少,该节点会很快再次发起充能请求,导致 MC 不得不频繁访问该节点,从而无形中增大了 MC 的移动距离。此外,因为 HEE 相比 NJNP 和 ESync 增加了对节点剩余能量的估计,同时考虑了节点在等待充电过程中的能耗,从而增大了可分配给节点的能量的上限值,进而提高了移动充电的整体能效。

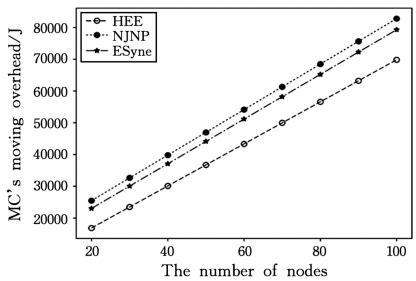


图 7 不同节点个数下 MC 的移动开销

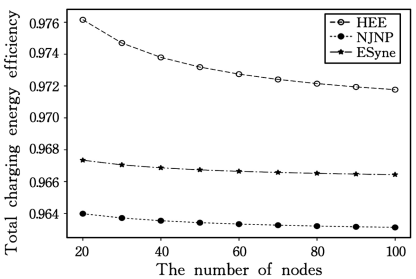


图 8 不同节点个数下的充电总能效

结束语 本文研究了 WRSN 中的移动充电问题,提出一种高能效的移动充电策略 HEE,通过节点剩余能量预测模型使节点能够在预计到自身剩余能量低于阈值时就发送充电请求,同时综合考虑了节点间距离与节点剩余能量来规划 MC 的移动路径,使更低剩余能量且距离更近的节点能够优先得到充电,并使用遗传算法进行求解。在求得的带权路径的基础上,将移动充电的能量分配问题转化为线性规划,使所有节点的充电量总和最大化。仿真结果显示,HEE 通过合适的路径规划与能量分配,降低了 MC 的移动开销,有着更高的移动充电能效,可保证 WRSN 长期稳定地工作。

参 考 文 献

[1] KURS A, KARALIS A, MOFFATT R, et al. Wireless power transfer via strongly coupled magnetic resonances [J]. Science, 2007,317(5834):83-86.
[2] KURS A, MOFFATT R, SOLJAČIĆ M. Simultaneous mid-range power transfer to multiple devices [J]. Applied Physics Letters, 2010,96(4):044102.
[3] SHI Y, XIE L, HOU Y T, et al. On renewable sensor networks with wireless energy transfer[C]// INFOCOM, 2011 Proceedings IEEE. IEEE, 2012:1350-1358.
[4] XIE L, SHI Y, HOU Y T, et al. Multi-node wireless energy charging in sensor networks [J]. IEEE/ACM Transactions on Networking, 2015, 23(2):437-450.
[5] SHU Y, YOUSEFI H, CHENG P, et al. Near-optimal Velocity Control for Mobile Charging in Wireless Rechargeable Sensor Networks [J]. IEEE Transactions on Mobile Computing, 2016, 15(7):1699-1713.
[6] HE L, KONG L, GU Y, et al. Evaluating the On-Demand Mobile Charging in Wireless Sensor Networks [J]. IEEE Transactions on Mobile Computing, 2015, 14(9):1861-1875.
[7] FU L, HE L, CHENG P, et al. ESync: Energy Synchronized Mobile Charging in Rechargeable Wireless Sensor Networks [J]. IEEE Transactions on Vehicular Technology, 2016, 65(9): 7415-7431.
[8] KHELLADI L, DJENOURI D, ROSSI M, et al. Efficient on-demand multi-node charging techniques for wireless sensor networks [J]. Computer Communications, 2017, 101:44-56.
[9] SHU Y, SHU Y, CHENG P, et al. TOC: Localizing Wireless Rechargeable Sensors with Time of Charge [J]. ACM Transactions on Sensor Networks (TOSN), 2015, 11(3):44-66.
[10] CHANG Z, WU X, WANG W, et al. Localization in Wireless Rechargeable Sensor Networks Using Mobile Directional Charger [C]// IEEE Global Communications Conference. IEEE, 2015:1-6.
[11] XU W, LIANG W, JIA X, et al. Maximizing Sensor Lifetime in a Rechargeable Sensor Network via Partial Energy Charging on Sensors [C]// IEEE International Conference on Sensing, Communication, and Networking. IEEE, 2016:1-9.
[12] WANG C, LI J, YE F, et al. A Mobile Data Gathering Framework for Wireless Rechargeable Sensor Networks with Vehicle Movement Costs and Capacity Constraints [J]. IEEE Transactions on Computers, 2016, 65(8):2411-2417.