

两轮 SPN 结构安全性分析

龚 涛^{1,2}, 陈少真^{1,2}

(1. 解放军信息工程大学 四院, 郑州 450001; 2. 数学工程与先进计算国家重点实验室, 郑州 450001)

摘 要: 分析 2 种类型的 SPN 结构的安全性, 即 16 类最佳仿射等价 4×4 S 盒的代表元与上述 16 个代表元所在的置换等价类。对得到的具体两轮 SPN 结构, 通过最大差分可能概率(MEDP)、最大线性偏差可能概率(MELP)等指标进行刻画。分析结果表明, 利用置换等价类作为两轮 SPN 结构的混淆层, 相比仿射等价类代表元, 在 MELP 指标上没有明显差别, 而在 MEDP 指标上分布则更加集中, 抵抗差分攻击的能力更强。

关键词: SPN 结构; 仿射等价类; 置换等价类; 密码学; 安全性

中文引用格式: 龚 涛, 陈少真. 两轮 SPN 结构安全性分析[J]. 计算机工程, 2017, 43(11): 97-101.

英文引用格式: GONG Tao, CHEN Shaozhen. Security Analysis of Two Round SPN Structure [J]. Computer Engineering, 2017, 43(11): 97-101.

Security Analysis of Two Round SPN Structure

GONG Tao^{1,2}, CHEN Shaozhen^{1,2}

(1. Fourth Department, PLA Information Engineering University, Zhengzhou 450001, China;

2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

[Abstract] This paper analyzed two different ways of the security of SPN structure, 16 different optimal S-Boxes classified and permutation equivalence class whose representative elements are the 16 elements mentioned above. It evaluates the two different results by two cryptographic properties; Maximum Everage Differential Probabilities (MEDP), Maximum Everage Linear Hull Probabilities (MELP). Analysis results show that the permutation equivalence class as the confuse layers are more concentrated, which means has a better ability to resist differential attack than those constructed by using affine equivalence class in MEDP, while the other cryptographic properties make no difference in MELP.

[Key words] SPN structure; affine equivalence class; permutation equivalence class; cryptography; security

DOI: 10.3969/j.issn.1000-3428.2017.11.016

0 概述

差分分析和线性分析是针对迭代分组密码最著名的分析方法。任何新的密码体制在设计时, 都会重点考虑该密码在运用差分分析和线性分析时的具体情况。SPN 结构是密码设计中常用的结构, 该结构根据密码结构遵循扩散和混乱的原则, 扩散层采用数个 S 盒并置的结构, 混乱层采用线性置换来增加整个一轮 SPN 结构的复杂性。现在常用的密码体制, 如 AES, Crypton, Square 等采用的是 SPN 结构。

针对差分分析^[1-3]和线性分析^[4-5]的安全性的 2 个指标是最大差分可能概率(Maximum Everaged Differential Probabilities, MEDP)和最大线性偏差可能概率(Maximum Everaged Linear Hull Probabilities, MELP)。把整个两轮 SPN 结构看成是一个大的密

码结构, 在这个结构中, 最重要的就是选择混淆层的 S 盒以及较好的线性置换函数。根据选择 S 盒的不同, 相同的扩散层分析比较, 利用相同结构密码函数 2 个指标的不同情况。文献[6]根据仿射等价关系提出了 16 类最佳仿射等价类的 4×4 S 盒, 同一个等价类中 S 盒差分均匀度和非线性度都是一样的。文献[7]根据置换等价关系提出了置换等价类的 4×4 S 盒。在比较两轮 SPN 结构这 2 个指标情况的主要结果有: 文献[8]分析了选择不同的线性层对两轮 SPN 结构的差分均匀度和非线性度这 2 个密码学指标的情况; 文献[9]给出了更紧凑的 MEDP 和 MELP 的上界, 文献[10]证明在选取不同的仿射等价类的 S 盒作为混淆层, 得到的 2 个指标的上界是不一样的。

本文首先选用 16 类仿射 4×4 S 盒的代表元作

作者简介: 龚 涛(1992—), 男, 硕士研究生, 主研方向为分组密码; 陈少真, 教授、博士生导师。

收稿日期: 2016-10-19 **修回日期:** 2016-12-01 **E-mail:** 805814287@qq.com

为 SPN 结构的混淆层,并对构造得到的两轮 SPN 结构进行分析。然后采用上述 16 个代表元所在的置换等价类作为两轮 SPN 结构的混淆层,并利用 MEDP 和 MELP 等密码学指标进行刻画。最后分析比较两者在两类密码学指标上的区别,分析原因并给出结论。

1 SPN 结构

1.1 SPN 结构介绍

SPN 结构一般由密钥层、扩散层和混乱层三部分组成。混乱层由 n 个小规模的非线性置换组成,常用的就是小规模 S 盒,扩散层主要是线性变化,增加混乱层的复杂度,轮子密钥和轮输入做异或运算。特别地,ARIA^[11]、SERPENT^[12]、AES^[13] 等分组密码都采用此结构。典型的一轮 SPN 结构如图 1 所示。

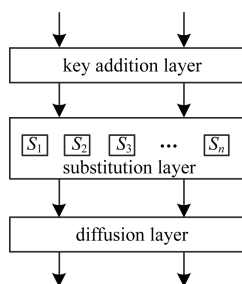


图 1 一轮 SPN 结构

在 r 轮 SPN 结构中,考虑到加解密算法的相似性,最后一轮的线性层通常省略。两轮 SPN 结构如图 2 所示。

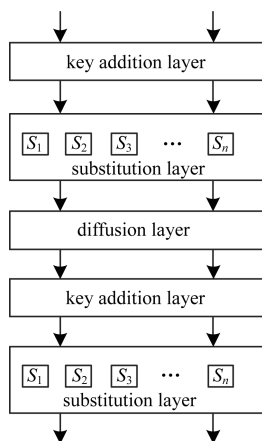


图 2 两轮 SPN 结构

1.2 SPN 结构密码学指标

SPN 结构密码学指标定义如下^[14-15]：

定义 1(最大差分可能概率^[9]) 令 $(E_k)_{k \in F_2^K}$ 是密钥规模 K 的 r 轮迭代密码,则:

$$EDP_r^E(a, b) = 2^{-k} \sum_{k \in F_2^K} \Pr_X[E_k(X) + E_k(X + a) = b]$$

称 $EDP_r^E(a, b)$ 为 r 轮差分 (a, b) 的期望概率, r 轮 SPN 结构的最大差分可能概率(MEDP)为:

$$MEDP_r^E = \max_{a \neq 0, b} EDP_r^E(a, b)$$

定义 2(最大线性偏差可能概率^[6]) 令 $(E_k)_{k \in F_2^K}$ 是密钥规模 K 、分组长度是 n 的 r 轮迭代密码,则:

$$EDP_r^E(u, v) = 2^{-2n-k} \sum_{k \in F_2^K} \left(\sum_{x \in F_2^n} (-1)^{u \cdot x + v \cdot E_k(x)} \right)^2$$

称 $EDP_r^E(a, b)$ 为 r 轮线性掩码 (u, v) 的线性偏差, r 轮 SPN 结构的最大线性偏差可能概率(MELP)为:

$$MELP_r^E = \max_{v \neq 0, u} ELP_r^E(u, v)$$

2 结构安全性分析

两轮 SPN 结构是分组密码中重要的结构,研究两轮抵抗差分攻击和线性攻击强弱对 S 盒的设计有重要作用。下文主要介绍两轮 SPN 结构选用不同 S 盒作为混淆层在相关差分分析和线性分析的密码学指标下的比较。

2.1 两轮 SPN 结构安全性分析

SPN 结构中的 S 是指替换(Substitution), P 是指置换或更广泛的线性变化(Permutation)。SPN 结构是目前广泛使用的一种分组密码整体结构, AES, Serpent, ARIA 等分组密码都采用该结构。在这种密码结构的每一轮中,首先轮输入被作用一个由子密钥控制的逆函数 S,然后再作用一个置换(或一个可逆的线性变化)P。SPN 结构非常清晰, S 层一般被称为混淆层,主要起混淆作用。P 一般被称为扩散层,主要起扩散的作用。直观来看,先经过混淆层,再经过扩散层,就很接近 Shannon 所提出的混淆原则和扩散原则,而现代分组密码将混淆层和扩散层通过整体结构迭代多次,将会增强密码的混淆性和扩散性,使得密码的输入和输出之间的依赖关系更为复杂。和 Feistel 结构相比, SPN 结构可以得到更快的扩散。

在轮子密钥独立、均匀分布的假设下,密钥层对密码体制的活动 S 盒个数没有任何影响,从而略去密钥层的 SPN 结构与原有结构具有相同抵抗差分和线性分析的能力。因此,为了便于分析两轮 SPN 结构的安全性,不考虑每一轮的轮密钥,同时以差分分析为例做具体分析,线性分析类似。通过上述的假定,图 1 中的密钥加对活动 S 盒个数没有影响。下面定义一个新的结构,即 SDS 结构,如图 3 所示。

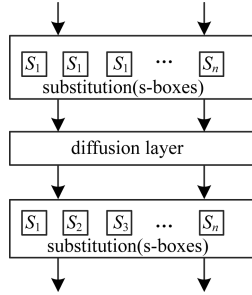


图 3 SDS 结构

SDS 结构中的扩散层即如图 3 中的 D 层,输入差分用 $\Delta x = x \oplus x^*$ 表示,那么输出差分就可以表示为 $\Delta y = y \oplus y^* = D(x) \oplus D(x^*)$,相应地输入输出线性掩码 Γx 和 Γy 可以类似表达。差分 and 线性最少活动 S 盒个数定义如下:

$$n_d(D) = \min_{\Delta x \neq 0} Hw(\Delta x) + Hw(\Delta y)$$

$$n_l(D) = \min_{\Gamma y \neq 0} Hw(\Gamma x) + Hw(\Gamma y)$$

如图 4 所示,具体分析 SDS 结构的差分攻击过程,线性攻击的过程类似。

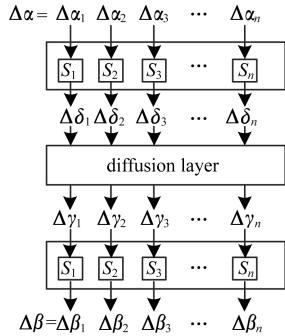


图 4 SDS 结构差分分析

考虑如图 4 所示的差分分析图,输入差分表示为 $\Delta\alpha = (\Delta\alpha_1, \Delta\alpha_2, \dots, \Delta\alpha_n)$,同样地,输出差分表示为 $\Delta\beta = (\Delta\beta_1, \Delta\beta_2, \dots, \Delta\beta_n)$,从而这一差分对的差分概率为:

$$DP(\Delta\alpha \rightarrow \Delta\beta) = \sum_{\Delta\delta_1, \Delta\delta_2, \dots, \Delta\delta_n} \left(\prod_{i=1}^n DP^{S_i}(\Delta\alpha_i \rightarrow \Delta\delta_i) \right) \left(\prod_{i=1}^n DP^{S_i}(\Delta\gamma_i \rightarrow \Delta\beta_i | \Delta\alpha) \right)$$

2.2 具体两轮 SPN 结构指标分析

文献[6]对 4 比特 S 盒进行分类,给出了 16 个最佳仿射等价类,如表 1 所示,其中,表 1 中列出的都是每一类的代表元。文献[7]根据类似定义给出了所有置换等价类(两者的区别在于仿射等价类用的是可逆矩阵,而置换等价类利用的是置换矩阵)。本文采用图 4 的 SDS 结构,同时 $n=4$,即混淆层有 4 个 4×4 的 S 盒,随机选取一个性质较好的扩散层。首先利用所有 16 个仿射等价类的代表元作为 SPN

结构中混淆层的 S 盒,来构成两轮 SPN 结构,之后对新构成的结构进行密码学指标刻画,以此来衡量新结构抵抗差分和线性攻击的强弱。

表 1 16 类最佳 S 盒

类	代表元
G_0	0,1,2,13,4,7,15,6,8,11,12,9,3,14,10,5
G_1	0,1,2,13,4,7,15,6,8,11,14,3,5,9,10,12
G_2	0,1,2,13,4,7,15,6,8,11,14,3,10,12,5,9
G_3	0,1,2,13,4,7,15,6,8,12,5,3,10,14,11,9
G_4	0,1,2,13,4,7,15,6,8,12,9,11,10,14,5,3
G_5	0,1,2,13,4,7,15,6,8,12,11,9,10,14,3,5
G_6	0,1,2,13,4,7,15,6,8,12,11,9,10,14,5,3
G_7	0,1,2,13,4,7,15,6,8,12,14,11,10,9,3,5
G_8	0,1,2,13,4,7,15,6,8,14,9,5,10,11,3,12
G_9	0,1,2,13,4,7,15,6,8,14,11,3,5,9,10,12
G_{10}	0,1,2,13,4,7,15,6,8,14,11,5,10,9,3,12
G_{11}	0,1,2,13,4,7,15,6,8,14,11,10,5,9,12,3
G_{12}	0,1,2,13,4,7,15,6,8,14,11,10,9,3,12,5
G_{13}	0,1,2,13,4,7,15,6,8,14,12,9,5,11,10,3
G_{14}	0,1,2,13,4,7,15,6,8,14,12,11,3,9,5,10
G_{15}	0,1,2,13,4,7,15,6,8,14,12,11,9,3,10,5

本文第 1 种类型的构造选择 16 类最佳仿射等价 4 比特 S 盒的代表元作为混淆层,选定 4 个 S 盒变换三者的位置所构造出来的大 S 盒是相同的,从而每个位置有 16 种情况,总共有 2^{16} 种不同的 S 盒产生。所有 2^{16} 个的 MEDP 结果如表 2 所示。

表 2 仿射等价类代表元情况的 MEDP

MEDP	个数	所占比例/%
1.1×2^{-8}	334	0.510
1.5×2^{-8}	918	1.400
5.5×2^{-9}	6 560	10.010
4.5×2^{-9}	51 702	78.890
7.5×2^{-9}	2 720	4.150
2.3×2^{-9}	3 276	5.010
1.01×2^{-9}	26	0.013

新结构的两轮 SP 结构 MEDP 都是 4.5×2^{-9} ,只有少部分是 1.1×2^{-8} , 1.5×2^{-8} , 5.5×2^{-9} , 7.5×2^{-9} , 2.3×2^{-9} 或 1.01×2^{-9} 。这说明利用两轮 SP 结构和 16 类最佳 4 比特 S 盒的代表元来构造的新结构,无法保证将 4 比特 S 盒上好的密码学性质传递下来。结果比较分散,不是很集中。

根据大 S 盒线性度的情况,分析全部 65 536 个两轮 SP 结构,利用上文中 MELP 的定义编程实现,结果是只要 4 个 S 盒取自 16 类最佳 S 盒的代表元,那么这样构造出来的两轮 SP 结构的 MELP 都

是 2^{-4} 。

第 2 种类型的构造混淆层选用的 S 盒是置换等价类的 S 盒。文献[7]根据前已有类似的定义给出了置换等价类,即满足 $S_2(x) = B(S_1(A(x) + a)) + b$, 其中, A, B 是置换矩阵, a, b 是定义在 F_2 上的 4 维向量, $S_1(x)$ 和 $S_2(x)$ 是 S 盒, $S_1(x)$ 和 $S_2(x)$ 就属于同一个置换等价类。类似于 $A(x) + b$ 的结构就是一个置换, 4×4 的置换矩阵共有 24 个, 定义在 F_2 上的 4 维向量共有 16 个, 从而不同的置换共有 $24 \times 16 = 384$ 个。

置换等价类一共有 142 090 700 类, 本文主要考察了仿射等价类的代表元所在的 16 个置换等价类中的元素作为混淆层。因此, 接下来在选择混淆层 4×4 的 S 盒时, 同样利用仿射等价类的分类结果, 考察 16 个代表元所在置换等价类 S 盒的表现。以仿射等价类所给出的 16 个代表元中的每一个所在的置换等价类元素作为第 2 种构造两轮 SPN 结构的混淆层。置换等价类的定义式中包含 2 个置换变换, 即内置换和外置换。这里, 在具体做实验的过程中, 考虑的是外置换。也就是说, 每一个代表元所在的置换等价类有 384 个元素。在每一类所有 384 个元素中, 任取 4 个作为上述两轮 SP 结构的混淆层, 之后考察具体两轮 SPN 结构的 MEDP 和 MELP 这 2 个密码学指标。

所有 16 个代表元的 MELP 都和第 1 种情况相同。由于篇幅原因, 不能把所有 16 种代表元所在置换等价类的指标分布表都列出, 表 3 是以 16 类仿射等价类中的第 1 个代表元所做的 MEDP 指标情况。其他 15 个代表元的指标分布类似于表 3 的分布情况, 相较于上述第 1 种情况, 利用置换等价类作为混淆层的 MEDP 分布更加集中。同时结果分布更趋向于高值, 即第 2 种方式构造的两轮 SPN 结构有更强的能力抵抗差分攻击, 在实际构造密码体制时更适合采用。

表 3 置换等价类的 MEDP

差分均匀度	代表元个数	所占比例/%
1.0×2^{-8}	110 890 686	0.51
1.5×2^{-9}	304 405 808	1.40
4.5×2^{-9}	20 425 629 657	93.94
7.5×2^{-9}	902 345 785	4.15

3 2 种不同 S 盒差异的分析比较

上文列出了 2 种不同方式构造的两轮 SPN 结构在 MEDP, MELP 这 2 种指标的具体情况。2 种方式构造结果的 MEDP 都是 2^{-4} 。它们在 MEDP 方面差

异较大, 两者的最佳 MEDP 指标都是 1.0×2^{-8} , 但是利用置换等价类元素作为两轮 SP 结构的混淆层得到两轮 SPN 结构的情形分布更加集中, 93.94% 的 MEDP 是 4.5×2^{-9} , 0.51% 的 MEDP 是 1.0×2^{-8} , 1.4% 的 MEDP 是 1.5×2^{-9} , 4.15% 的 MEDP 是 7.5×2^{-9} ; 而利用仿射等价类代表元作为两轮 SPN 结构的混淆层构造得到的两轮 SP 结构, 78.89% 的 MEDP 是 4.5×2^{-9} , 0.51% 的 MEDP 是 1.1×2^{-8} , 1.4% 的 MEDP 是 1.5×2^{-8} , 10.01% 的 MEDP 是 5.5×2^{-9} , 5.01% 的 MEDP 是 7.3×2^{-9} , 0.013% 的 MEDP 是 1.01×2^{-9} , 4.15% 的 MEDP 是 7.5×2^{-9} 。为了更直观地反映 2 种方式构造两轮 SPN 结构密码学指标的差异性, 2 种方式的 MEDP 如图 5、图 6 所示。本文的构造分析对在实际利用 SPN 结构构造密码体制具有一定的借鉴意义。当混淆层任意选用置换等价类的 S 盒时, SPN 结构抵抗差分攻击和线性攻击的能力较为类似, 不会出现很大的差异。同时 MEDP 绝大多数趋于高值, 即抵抗差分攻击的能力更强, 构造得到的密码体制相应地也会越安全。但是当混淆层任意选择仿射等价类的 S 盒时, 由于 MEDP 指标趋于分散, 分布不集中, SPN 结构抵抗差分攻击的能力会出现较大程度的差异。

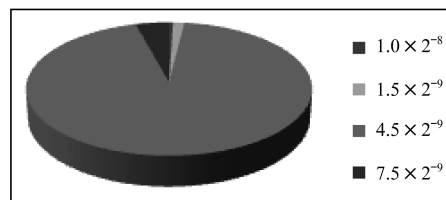


图 5 仿射等价类代表元情况的 MEDP

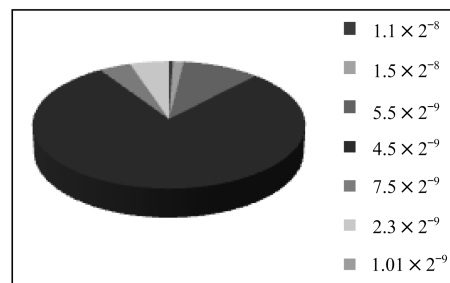


图 6 置换等价类的 MEDP

4 结束语

本文首先选用文献[1]提出的 16 类 4×4 S 盒的代表元和文献[3]提出的置换等价类中 16 个代表元所在的置换等价类, 分别作为两轮 SPN 结构的混淆层构造得到具体的两轮 SPN 结构。然后对所有生成的结果, 通过 MEDP, MELP 指标进行刻画。分析结果表明, 在 MEDP 指标上, 利用置换等价类作为混

淆层构造的结果,比 16 个仿射等价类代表元作为混淆层同等情况下构造得到的结果要好。但是由于本文方法构造的两轮 SP 结构的分组长度、密钥长度等都只有 16 bit,在实际构造分组密码体制时用现有的计算水平较容易被穷举攻击。寻找合适的 S 盒作为混淆层以及较好的线性层来设计两轮 SPN 结构,将是下一步的研究工作。

参考文献

- [1] BIHAM E, SHAMIR A. Differential Cryptanalysis of DES-like Cryptosystems[C]//Proceedings of Advances in Cryptology-CRYPTO'90. Berlin, Germany: Springer-Verlag, 1990:2-21.
- [2] BIHAM E, SHAMIR A. Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer [C]//Proceedings of Advanced in Cryptology-CRYPTO'91. Berlin, Germany: Springer-Verlag, 1991:156-171.
- [3] BIHAM E. On Matsui's Linear Cryptanalysis [C]//Proceedings of Advanced in Cryptology-EUROCRYPT'94. Berlin, Germany: Springer-Verlag, 1994:341-355.
- [4] MATSUI M. Linear Cryptoanalysis Method for DES Cipher[C]//Proceedings of Cryptology-EUROCRYPT'93. Berlin, Germany: Springer-Verlag, 1993:386-397.
- [5] MATSUI M. The First Experimental Cryptanalysis of DES [C]//Proceedings of Advanced in Cryptology-CRYPTO'94. Berlin, Germany: Springer-Verlag, 1994:1-11.
- [6] LEANDER G, POSCHMANN A. On the Classification of 4 Bit S-boxes [C]//Proceedings of WAIFI'07. Berlin, Germany: Springer-Verlag, 2007:159-176.
- [7] SAARINEN M J O. Cryptographic Analysis of all 4×4 -bit Sboxes [C]//Proceedings of SAC'11. Berlin, Germany: Springer-Verlag, 2011:118.
- [8] HONG S, LEE S, LIM J, et al. Provable Security Against Differential and Linear Cryptanalysis for the SPN Structure [C]//Proceedings of FSE'00. Berlin, Germany: Springer-Verlag, 2001:273-283.
- [9] PARK S, SUNG S H, LEE S, et al. Improving Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES [C]//Proceedings of FSE'03. Berlin, Germany: Springer-Verlag, 2003:247-260.
- [10] CANTEAUT A, ROUE J. On the Behaviors of Affine Equivalent Sboxes Regarding Differential and Linear Attacks [C]//Proceedings of Advances in Cryptology-Eurocrypt'15. Berlin, Germany: Springer-Verlag, 2015:45-74.
- [11] KEON D, KIM J, PARK S, et al. New Block Cipher: ARIA [C]//Proceedings of ICISC'03. Berlin, Germany: Springer-Verlag, 2003:432-445.
- [12] ANDERSON R, BIHAM E, KNUDSEN L. Serpent: A Proposal for the Advanced Encryption Standard [C]//Proceedings of AES'98. Berlin, Germany: Springer-Verlag, 1998:1-23.
- [13] DAEMEN J, RIJMEN V. The Design of Rijndael: AES-the Advanced Encryption Standard [M]. [S. l.]: Springer Science & Business Media, 2013.
- [14] 屈龙江, 付绍静, 李超. 密码函数安全性指标的研究进展[J]. 密码学报, 2014, 1(6):578-588.
- [15] 李超, 屈龙江, 周悦. 密码函数的安全性指标分析[M]. 北京: 科学出版社, 2011.

编辑 索书志

(上接第 96 页)

- [7] ERKAY U, FATIH S, KEMAL A, et al. Distributed Connectivity Restoration in Underwater Acoustic Sensor Networks via Depth Adjustment [C]//Proceedings of 2015 IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2015:6357-6362.
- [8] JORGIĆ M, STOJIMENOVÉ I, HAUSPIE M, et al. Localized Algorithms for Detection of Critical Nodes and Links for Connectivity in Ad Hoc Networks [C]//Proceedings of Mediterranean Ad Hoc Networking Workshop. Washington D. C., USA: IEEE Press, 2004:12.
- [9] HUANG J, SUN L, WEI X et al. Redundancy Model and Boundary Effects Based Coverage-enhancing Algorithm for 3D Underwater Sensor Networks [J]. International Journal of Distributed Sensor Networks, 2014, 2014(1):1-12.
- [10] 蒋鹏, 陈峰. 基于冗余节点休眠和分阶段唤醒策略的传感器网络三维覆盖控制方法[J]. 电子与信息学报, 2009, 31(12):2807-2812.
- [11] CARRICK D, MAREK D, IULIU V, et al. Autonomous Depth Adjustment for Underwater Sensor Networks: Design and Applications [J]. IEEE/ASME Transactions on Mechatronics, 2012, 17(1):16-24.
- [12] OVALIADIS K, SAVAGE N, KANAKARIS V. Energy Efficiency in Underwater Sensor Networks: A Research Review [J]. Journal of Engineering Science and Technology Review, 2010, 3(1):151-156.
- [13] GOYAL D, CAFFERY J. Partitioning Avoidance in Mobile Ad Hoc Networks Using Network Survivability Concepts [C]//Proceedings of the 7th International Symposium on Computers and Communications. Washington D. C., USA: IEEE Press, 2002:553-558.
- [14] SU R, VENKATESAN R, LI C. An Energy-efficient Asynchronous Wake-up Scheme for Underwater Acoustic Sensor Networks [J]. Wireless Communications and Mobile Computing, 2016, 16(9):1158-1172.
- [15] 李莉, 杨丽娟, 李钢, 等. 基于 Aqua-Sim 的水声传感器网络 MAC 层协议分析[J]. 传感器与微系统, 2015, 34(5):52-54.

编辑 金胡考