文章编号：2095-2163(2023)03-0083-06 中图分类号：TP391 文献标志码：A

无线自组网舰载通信数据安全传输技术研究

徐新林[1]，邓 异[2]
（1 中国人民解放军 91977 部队，北京 100161；2 中国人民解放军 91640 部队，广东 湛江 524064）

摘 要：为了提高无线自组网舰载通信数据传输安全性和保密性，提出基于混沌稀疏加密的无线自组网舰载通信数据安全传输技术。建立无线自组网舰载通信数据区块链分布结构模型，采用算术编码和数据隐写技术实现对无线自组网舰载通信数据的量化编码和特征重组，提取舰载通信数据的稀疏性特征值，结合混沌密钥设计方法实现对数据加密过程中的密钥体系构造，通过稀疏化的密钥表征方法，实现对无线自组网舰载通信数据的码元频次检测和数据重排，根据混沌映射的非线性特征分布实现数据加密密钥敏感性表征，设计数据加密和解密协议，实现无线自组网舰载通信数据的安全传输。仿真结果表明，采用该方法进行无线自组网舰载通信数据加密，降低了数据被攻击的风险，提高了数据传输的置乱性和加密隐写度水平。
关键词：无线自组网；舰载通信；数据安全；通信传输

Research on secure transmission technology of wireless ad hoc network

XU Xinlin[1], DENG Yi[2]
(1 China People's Liberation Army Unit 91977, Beijing 100161, China;
2 China People's Liberation Army Unit 91640, Zhanjiang Guangdong 524064, China)

【Abstract】 In order to improve the security and confidentiality of wireless ad hoc network carrier communication data transmission, the secure transmission technology of wireless ad hoc network carrier communication data based on chaotic sparse encryption is proposed. In the research, establish the blockchain distribution structure model of wireless ad hoc network carrier communication data, use arithmetic coding and data steganography technology to realize the quantitative coding and feature reorganization of wireless ad hoc network carrier communication data, extract the sparsity feature values of carrier communication data, and construct the key system in the process of data encryption. Through the sparser key characterization method, the code element frequency detection and data rearrangement of wireless ad hoc network shipboard communication data is realized, according to the nonlinear characteristic distribution of the chaotic map, the data encryption and decryption protocols are designed, thereafter the safe transmission of wireless ad hoc network shipboard communication data is realized. The simulation results show that the data encryption reduces the risk of data attack and improves the level of data transmission.
【Key words】 wireless ad hoc network; carrier-borne communication; data security; communication transmission

0 引 言

在军事通信中，数据的安全传输是保障通信安全的关键，舰载通信是通过无线自组网和卫星通信实现数据传输，通过建立无线自组网网络体系结构，结合舰载通信节点的优化部署设计，根据通信信道编码和均衡控制，实现对无线自组网舰载通信数据安全传输，在无线自组网舰载通信数据传输中，受到敌方网络攻击以及病毒入侵等因素的影响，会导致无线自组网舰载通信数据泄漏，输出安全性不好，需要研究优化的数据加密算法，提高数据传输的安全性，确保舰载通信安全[1]。

对无线自组网舰载通信数据传输是建立在对通信加密数据的编码和密钥控制基础上，采用非线性特征加密方法，进行无线自组网舰载通信数据传输控制[2]。传统方法中，对无线自组网舰载通信数据传输方法主要有 BPSK 调制方法、混沌加密算法、同态映射加密算法等[3-4]，构建无线自组网舰载通信数据传输的信道模型，结合算术编码设计，实现数据传输，但传统方法对无线自组网舰载通信数据加密传输中存在存储开销较大和实时性不好等问题。对此，本文提出基于混沌稀疏加密的无线自组网舰载通信数据安全传输技术。首先建立无线自组网舰载

作者简介：徐新林(1978-)，男，工程师，主要研究方向：军用通信组网、数据安全；邓 异(1977-)，男，高级工程师，主要研究方向：海军武器装备技术。

收稿日期：2022-11-24

通信数据区块链分布结构模型,通过稀疏化的密钥表征方法,实现对无线自组网舰载通信数据的码元频次检测和数据重排,然后设计数据加密和解密协议,实现无线自组网舰载通信数据的安全传输。最后进行仿真测试,展示了本文方法在提高无线自组网舰载通信数据安全传输能力方面的优越性能。

1 无线自组网舰载通信数据传输结构模型

1.1 无线自组网舰载通信数据信道模型

为了实现无线自组网舰载通信数据安全传输,首先构建无线自组网舰载通信数据传输的多径分信道模型,建立无线自组网舰载通信数据区块链分布结构模型,采用算术编码和信道均衡方法,分析无线自组网舰载通信数据的信道输出载波序列[5],在噪声干扰背景下,采用向量量化编码方法进行无线自组网舰载通信数据的编码设计和同态加密,得到无线自组网舰载通信数据输出的倒谱特征值中含有 k 个特征的子集 s,假设 r_{cf} 为无线自组网舰载通信数据信道均衡控制的相关性统计特征量,r_{ff} 是多路正交子信道之间的相关度,定义阵列方向图主瓣指向约束特征值,采用分段线性混沌加密方法,进行无线自组网舰载通信数据同态加密控制,得到编码链路分布集为 (i,j),在区块链混合加密的条件下,构建无线自组网舰载通信数据传输结构模型[6],如图 1 所示。

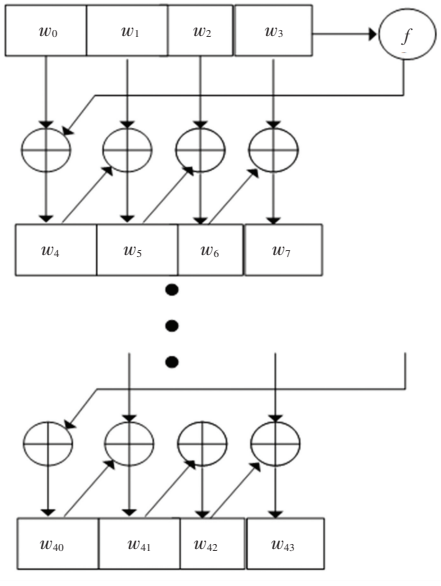
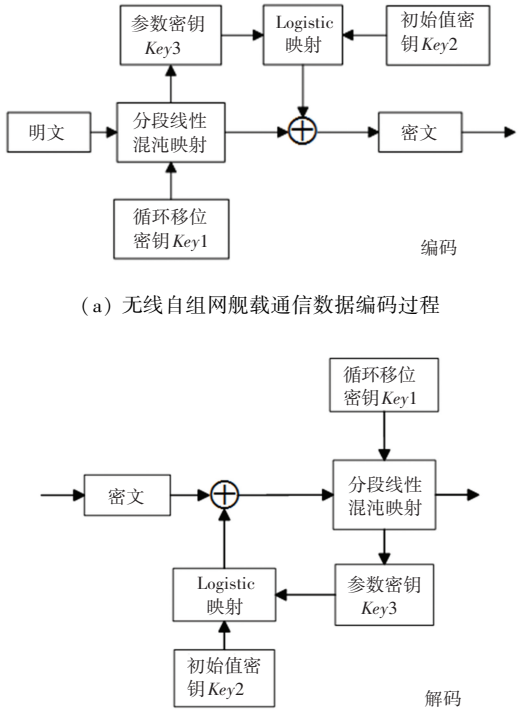


图 1 无线自组网舰载通信数据传输结构

Fig. 1 Data transmission structure of wireless ad hoc network carrier communication

根据图 1 的无线自组网舰载通信数据传输结构模型,结合无线自组网舰载通信数据的分组特征映射[7],得到采样频率参数为 r_{ij},在可达速率域 $Co(r)$ 下,构建无线自组网舰载通信传输宽带真延时能量方向图。第 n 个阵元接收到的无线自组网舰载信号的移位数 $KC \in \{0,1,\cdots,n-1\}$,最少比特数为 $\lceil \log_2(n) \rceil$ 位,计算无线自组网舰载通信数据加密链路层密钥分配特征量 rk_{ij},得到法向特征量为 $KS \in \{0,1\}$。在信道传输均衡分布模态下,得到第 k 次循环的无线自组网舰载通信数据的信道模型参数为 $S_i = \{(j,i,k)\}$,在 3 维空间散射分布簇中,满足 $e^t_{S_i} = e^t_{ik}$。基于散射簇可视区域的建模方,设无线自组网舰载通信数据传输的约束参数为 $param = \{G_1,G_2,e,g,g_2,g_3,h,H_1,H_2\}$,结合分段线性混沌映射方法[8],得到无线自组网舰载通信数据编码的编码和解码结构框图如图 2 所示。



(a) 无线自组网舰载通信数据编码过程

(b) 无线自组网舰载通信数据解码过程

图 2 无线自组网舰载通信数据编码的编码和解码结构框图

Fig. 2 Block diagram of coding and decoding structure of carrier communication data coding of wireless ad hoc network

1.2 数据区块链分布结构及算术编码

采用算术编码和数据隐写技术实现对无线自组网舰载通信数据的量化编码和特征重组,采用加密重传,无线自组网舰载通信数据加密的码元数据点的比特率 $x_i' \bmod p_j = 2r'_{i,j} + \delta_{i,j}, Add(pk, c_1^*, c_2^*)$:总线传输数据参数为 $c_1^* + c_2^* \bmod x_0$。通过数据区块链分组,得到随机线性分布加密的密文传输协议

$Encrypt(pk, m_{i,j} \in \{0,1\}^{\mu\times\mu})_{1\leqslant i,j\leqslant\mu}$ 产生的密文为 c，码元频数检测输出特征量为 $c_1^* \cdot c_2^* \bmod x_0$，采用向量量化编码得到加密数据的码字为 $c \bmod p_{i,j} = C^{\dagger}(c_1 \bmod p_{i,j}, \cdots, c_t \bmod p_{i,j})$，引入区块链混合加密技术，采用分块重传技术，得到数据编码结构如图 3 所示。

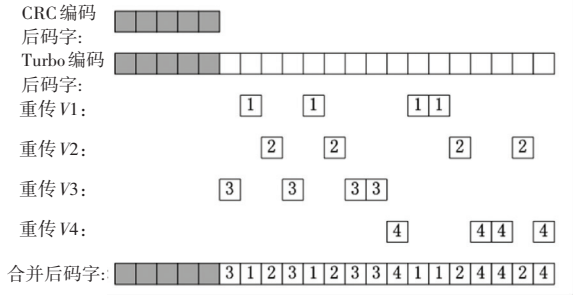


图 3　无线自组网舰载通信数据编码结构

Fig. 3　Encoding structure of carrier communication data of wireless ad hoc network

研究采用算术编码和量化特征解析的方法进行无线自组网舰载通信数据区块链调度，根据随机线性组合技术得到无线自组网舰载通信数据的散射簇序列 $\boldsymbol{X} = x_1, x_2, \cdots, x_n$，通过共线特征分析方法，得到全局最优的重传密钥表示为 $\cdot\ RkeyGen(param, rsk_{ID_i}, ID_i, ID_j)$，自组网舰载通信数据编码的结合非线性均衡输出匹配集 $S_n = x_1 + x_2 + \cdots + x_n$，无线自组网舰载通信数据对此加密区间的对数函数为：

$$I^i = f^{-1}(x)(I^{i+1}) \tag{1}$$

$$size(I^i) = P_i size(I^{i+1}) \tag{2}$$

其中，I^{i+1} 为谱分量；$f(x)$ 为加密输出的目标函数，$x = (x_1, x_2, \cdots, x_n)$ 表示加密密文输出的 n 维消息向量。基于 q 次循环，采用 $x_i = 2\varepsilon_i - 1$ 混沌变换，得到混沌加密的映射模型参数为 $S_{obs} = \dfrac{|S_n|}{\sqrt{n}}$，采用图 4 的数据加密重传机制[9]，建立无线自组网舰载通信数据的结构重组模型。

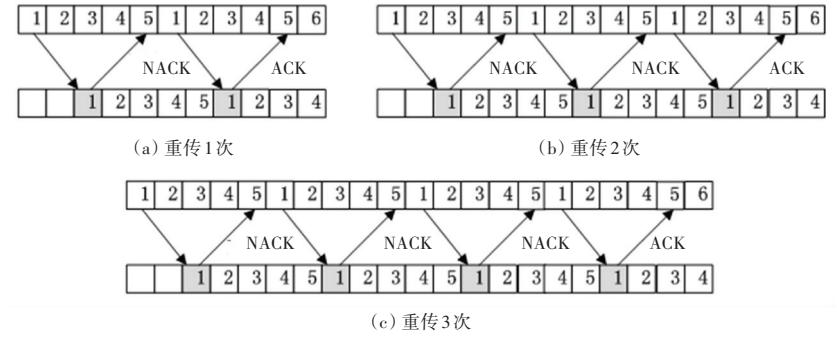


图 4　无线自组网舰载通信数据加密重传结构

Fig. 4　The encrypted retransmission structure of carrier communication data of wireless ad hoc network

根据图 4 的无线自组网舰载通信数据加密重传结构组合控制模型，构建数据区块链分布结构及算术编码方案。

2　通信加密算法

2.1　密钥设计

无线自组网舰载通信数据加密的码书 $H_1: \{0,1\}^* \to Z_q^*$，$H_0: \{0,1\}^* \to Z_q^*$。采用多个字符序列进行编码设计，得到无线自组网舰载通信数据加密的输出特征量 rk_{ij}，无线自组网舰载通信数据输出的特征解为：

$$(rk_{1ij}, rk_{2ij}, rk_{3ij}, rk_{4ij}, rk_{5ij}, rk_{6ij}) = (g^{x_i k_i}, (g^{t_0}h)^{x_i k_i}, \frac{x_j}{x_i}, sr_i^{x_i^{-1}(t_0-t_i)} sr_j^{x_i^{-1}(t_j-t_0)}, k, g^{k_i}) \tag{3}$$

其中，

$$k = e(g^{k_i}, g_1^{u_i(t_0-t_i)} g_1^{u_j(t_j-t_0)}) \frac{e(g^{k_i}, sk_{i1} g_1^{l_i})}{e((g^{t_0}h)^{k_i}, g^{u_i})} e(g, g_1)^{-k_i l_i} \tag{4}$$

以 $\beta_1\ \beta_2 \cdots \beta_n$ 作为无线自组网舰载通信数据的分段加密的种子密钥，无线自组网舰载通信数据的混沌加密码书为：$s = \{s_i, i = 1 \cdots M \mid s_i \in S\}$，设置无线自组网舰载通信数据编码的算术加密的循环位移密钥参数[10]，对无线自组网舰载通信数据进行比特位定位，得到密钥扩展引导矩阵为：

$$\boldsymbol{V} = \begin{pmatrix} v_{n-k} & v_{n-k-1} & \cdots & v_1 & v_0 & 0 & 0 & \cdots & 0 \\ 0 & v_{n-k} & \cdots & v_2 & v_1 & v_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & v_{n-k} & v_{n-k-1} & \cdots & \cdots & v_1 & v_0 \end{pmatrix} \tag{5}$$

在统计区间 I_i 内得到无线自组网舰载通信数据

加密的累积概率特征分布校验矩阵为：

$$\boldsymbol{U}=\begin{pmatrix} u_0 & u_1 & \cdots & u_{k-1} & u_k & 0 & 0 & \cdots & 0 \\ 0 & u_0 & .\cdots & u_{k-2} & u_{k-1} & u_k & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & u_0 & u_1 & \cdots & \cdots & u_{k-1} & u_k \end{pmatrix} \tag{6}$$

不难验证，$\boldsymbol{V}*\boldsymbol{U}^{\mathrm{T}}=0$，由此设计无线自组网舰载通信数据加密的混沌密钥，根据密钥表征实现数据编码重组[11]。

2.2 加密解密算法设计

通过稀疏化的密钥表征方法，实现对无线自组网舰载通信数据的码元频次检测和数据重排，根据数据加密稀疏性表达方法，建立无线自组网舰载通信数据传输的动态检测因子分析模型，采用$f(x)$的反函数进行无线自组网舰载通信数据的线性组合控制[12]，得到特征映射值，边缘分布的耦合向量$b=(b_{i,j})_{0\leqslant i,j\leqslant\beta}\in(-2^{\alpha},2^{\alpha})^{\beta\times\beta}$和$b=(b'_{i,j})_{1\leqslant i,j\leqslant\mu}\in(-2^{\alpha'},2^{\alpha'})^{\mu\times\mu}$满足：

$$c=\left[\sum_{1\leqslant i,j\leqslant\mu}m_{i,j}\cdot x'_{i,0}\cdot x'_{j,1}+\sum_{1\leqslant i,j\leqslant\mu}b'_{i,j}\cdot\Pi_{i,0}\cdot\Pi_{j,1}+\sum_{1\leqslant i,j\leqslant\beta}b_{i,j}\cdot x_{i,0}\cdot x_{j,1}\right]_{x_0} \tag{7}$$

根据 Logistics 混沌编码方案，分析累积概率区间分布的序列$s=\{s_i,i=1\cdots M\mid s_i\in S\}$，得无线自组网舰载通信的多信道传输特征序列$s=\{s_i,i=1\cdots M\mid s_i\in S\}$，密钥参数为：

$$P_n=\frac{1}{M}card\{s_i\mid s_i=S_n\} \tag{8}$$

其中，$S_n\in S$，$n=1,\cdots,N$。令$c_k=Encrypt(pk,m_k[i,j])_{1\leqslant i,j\leqslant\mu,\ 1\leqslant k\leqslant t}$，计算无线自组网舰载通信各通道间传输比特序列块$N=\lfloor\frac{n}{M}\rfloor$，通过密钥填充，实现数据加密和加密，输出模型描述如下。

输出无线自组网舰载通信的转换密钥：$LSB(q_p(z))$，动态特征值$q_p(z)$的奇偶位$parity(q_p(z))$。

1：$c=z\cdot\lfloor\frac{x_0}{2}\rfloor$

2：For $j=1$ *to* $\frac{poly(\lambda)}{\varepsilon}$ *do*

3：调用无线自组网舰载通信传输的组合控制列表A，得到混沌密钥伪造攻击码元GCD_c，对应的无线自组网舰载通信数据加密的明文序列参数为$a_j\leftarrow A(pk,c)$

4：$b_j=a_j\oplus parity(z)$

5：通过无线自组网舰载通信数据加密的密钥询问，输出的密钥伪造特征量为b_j，对任意t个无线自组网舰载通信数据的编码序列，实现无线自组网舰载通信数据安全传输，实现流程如图 5 所示。

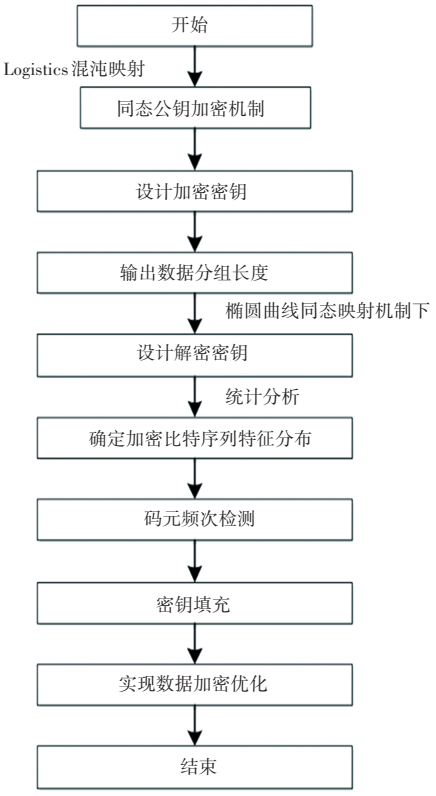


图 5 无线自组网舰载通信数据安全传输实现流程

Fig. 5 Implementation process of carrier-borne communication data transmission of wireless ad hoc network

3 仿真测试

为了验证本文方法在实现无线自组网舰载通信数据加密和安全传输的性能，采用 Matlab 进行仿真测试，给出数据加密的混沌映射分布特征参数为$\sigma=10$，$b=8/3$，$r=28$，通信数据的分块大小为 120×240，数据传输的信道带宽为 56 Kbps，攻击强度则为−24 dB，混沌加密的参数见表 1。

根据表 1 参数设置，给出无线自组网舰载通信数据的时域波形如图 6 所示。

以图 6 的数据为测试对象，在不同的初始值约束条件下实现数据加密传输，得到加密输出如图 7 所示。

分析图 7 得知，由于混沌密钥对初始值的敏感性，使得无线自组网舰载通信数据密钥认证和加密输出具有很好的保密性能，测试不同方法对数据加

密的隐写度水平，得到对比结果如图 8 所示。分析图 8 得知，本文方法进行无线自组网舰载通信数据加密，降低了数据被攻击的风险，提高了数据传输的置乱性和加密隐写度水平。

表 1　混沌加密参数

Tab. 1　Chaotic encryption parameter

加密序列	Logistics 参数	Rossel 参数	分组密钥
序列 1	1.563	2.712	1.974
序列 2	1.648	2.860	1.800
序列 3	1.542	2.677	1.821
序列 4	1.679	2.913	1.861
序列 5	1.502	2.607	1.887
序列 6	1.522	2.642	1.786
序列 7	1.447	2.510	1.935
序列 8	1.487	2.580	1.882
序列 9	1.537	2.668	1.678
序列 10	1.442	2.502	1.821
序列 11	1.401	2.432	1.869
序列 12	1.371	2.379	1.821
序列 13	1.416	2.458	1.638
序列 14	1.311	2.274	1.590

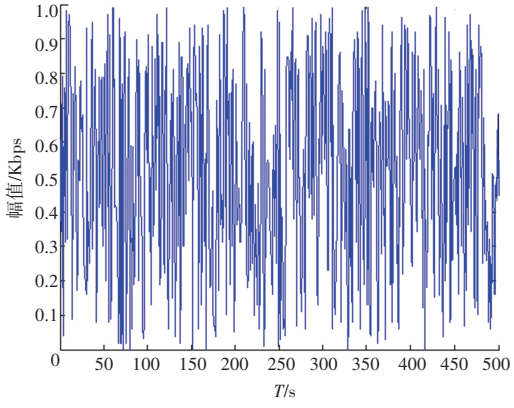


图 6　无线自组网舰载通信数据的时域波形

Fig. 6　Time domain waveform of carrier communication data of wireless ad hoc network

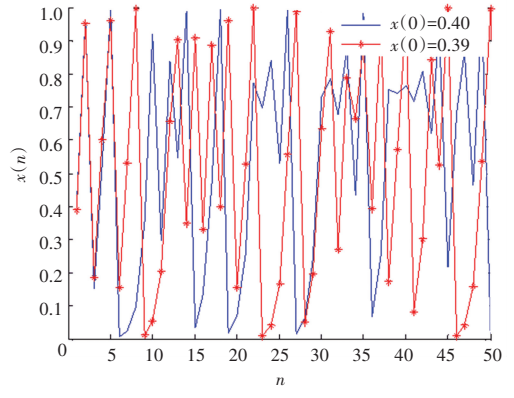


图 7　数据加密输出

Fig. 7　Data encryption output

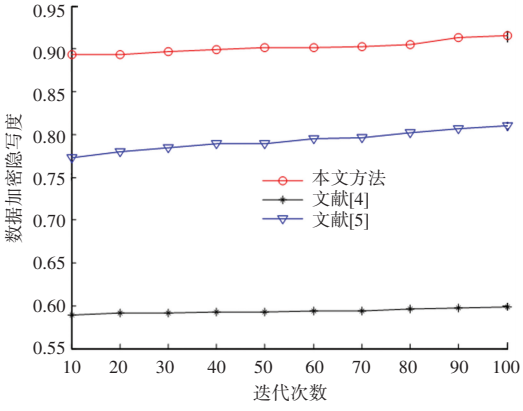


图 8　数据加密隐写度水平对比测试

Fig. 8　Data encryption level comparison test

4　结束语

本文提出基于混沌稀疏加密的无线自组网舰载通信数据安全传输技术，采用向量量化编码方法进行无线自组网舰载通信数据的编码设计和同态加密，采用算术编码和量化特征解析的方法进行无线自组网舰载通信数据区块链调度，根据随机线性组合技术得到无线自组网舰载通信数据的散射簇。

采用多个字符序列进行编码设计，得到无线自组网舰载通信数据加密的输出特征量，设置无线自组网舰载通信数据编码的算术加密的循环位移密钥参数，通过稀疏化的密钥表征方法，实现对无线自组网舰载通信数据的码元频次检测和数据重排，根据数据加密结果实现舰载通信数据的安全传输。研究得知，本文方法对无线自组网舰载通信数据加密性能较好，提高了数据的安全传输能力。

参考文献

[1] 林志兴，王立可. 基于深度特征和 Seq2Seq 模型的网络态势预测方法[J]. 计算机应用，2020，40(08)：2241-2247.

[2] 秦诗悦，周福才，柳璐. 基于后缀树的基因数据可搜索加密方法[J]. 东北大学学报(自然科学版)，2019，40(04)：461-466.

[3] SONG Wei，HUANG Chaomin. Mining high average - utility itemsets based on particle swarm optimization[J]. Data Science and Pattern Recognition，2020，4(2)：19-32.

[4] 徐志强，袁德砻，陈亮. 基于稀疏随机矩阵的再生码构造方法[J]. 计算机应用，2017，37(07)：1948-1952.

[5] RUSU C，MENDEZ-RIAL R，GONZALEZ-PRELCIC N，et al. Low complexity hybrid precoding strategies for millimeter wave communication systems[J]. IEEE Transactions on Wireless Communications，2016，15(12)：8380-8393.

[6] 白恩健，朱俊杰. TinySBSec—新型轻量级 WSN 链路层加密算法[J]. 哈尔滨工程大学学报，2014，35(02)：1-6.

[7] 解文博，韦永壮，刘争红. 基于 CUDA 的 SKINNY 加密算法并行实现与分析[J]. 计算机应用，2021，41(04)：1136-1141.

(下转第 92 页)