文章编号:1004-9037(2014)06-0991-07

基于矩阵概率检验的 Zigbee 协议随机性检测方法

汤永利[1] 王 真[1] 张雯雯[1] 刘海峰[2] 郭玉翠[3]

(1.河南理工大学计算机科学与技术学院,焦作,454003; 2.北京信息安全测评中心,北京,100101;
3.北京邮电大学理学院,北京,100876)

摘要:随机性检测是研究密码算法基础理论的重要内容。为了有效测试与鉴别物联网系统中 Zigbee 协议采用密码算法的安全性,本文结合 Zigbee 网络的特点,在二元矩阵秩检验的基础上,对测试方式进行了合理的组织与划分,提出基于矩阵概率检验的 Zigbee 随机性检测方法,解决了二元矩阵秩检验单纯从线性相关性判断随机序列的片面性,并能有效地判断 Zigbee 协议是否实施了加密机制以及加密强度。仿真结果表明,该算法具有误差较小、可靠性高等特点,检测结果更具说服力,为物联网系统的信息安全测评提供理论和实践指导。

关键词:Zigbee 协议;矩阵概率检验;随机性测试

中图分类号:TP309 **文献标志码**:A

Randomness Tests Method of Zigbee Protocol Based on Matrix Probability Test

Tang Yongli[1], *Wang Zhen*[1], *Zhang Wenwen*[1], *Liu haifeng*[2], *Guo Yucui*[3]

(1. School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, 454003, China;
2. Beijing Information Security Test and Evaluation Center, Beijing, 100101, China;
3. School of Sciences, Beijing University of Posts and Telecommunications, Beijing, 100876, China)

Abstract: Randomness tests of cryptographic algorithm is analyzed. In order to test and identify Zigbee protocol security of cryptographic algorithm in the internet of things(IOT), test modes are organized and divided combining with the characteristics of Zigbee networks and binary matrix rank theory test, and randomness tests method of Zigbee protocol are proposed based on matrix probability test. The method solves the one-sidedness of binary matrix rank test to simply judge random sequence by linear correlation. It can determine whether the Zigbee protocol encryption mechanism and encryption strength are implemented or not. Simulation results show that this algorithm has less errors, and higher reliability, which is much more convincing. The proposed method provides theoretical and practical guidance for information security evaluation of IOT.

Key words: Zigbee protocol; matrix probability test; randomness tests

引 言

作为物联网的重要组成部分的 Zigbee 技术以其低功耗、低成本、低时延的明显优势,在工业控制、农业、环境科学等领域广泛应用,因此 Zigbee 技术的安全问题成为研究热点之一。由于 Zigbee 协议安全加密机制可选、加密算法自定义程度高、加密层级多样等特点,目前对 Zigbee 协议的安全性缺乏有效的检测。从计算复杂性和密码学角度讲,随机数是密码算法安全的根本。著名的密码学家 Bruce Schneider 曾说过,随机序列是谈论最少

基金项目:国家留学基金(201208410155)资助项目;国家自然科学基金(60973146、61300216)资助项目;河南省科技攻关重点(122102310309)资助项目;河南理工大学博士基金(B2011-058)资助项目;河南省科技厅基础与前沿技术研究(142300410147)资助项目。

收稿日期:2013-10-25;**修订日期**:2013-12-14

的密码学问题，但没有哪个问题比这个问题更重要[1]。在密码算法及认证协议算法中，都需要使用随机数序列作为密钥，并且随机性检测也是研究密码算法安全性的重要手段之一。因此，Zigbee 的随机性检测方法的研究对 Zigbee 技术及物联网系统的安全具有重要理论意义。

随机性与密码技术的安全性息息相关，根据密码算法产生序列的随机性可对密码算法的安全性进行评价。序列的随机性检测，实质上是检验其是否是真随机或与真随机的差距[2]。Bruce Schneier 认为一个随机序列应满足如下性质：(1)能通过所有正确的随机性测试；(2)具有不可预测性；(3)不能重复产生。

目前，随机性测试有很多种类，George Marsaglia 提出了 DIEHARD 测试集[3]，但对序列长度均有较高要求，对样本数量较小的参考分布难以计算，应采用更严格的参考分布。NIST SP 800-22 规范[4]建议了 15 种用于随机性测试的统计检验方法，均是将假设机率 P_{-value} 值与显著性水平 α 进行比较给出序列是否随机的结论，但并未系统地讨论统计检验和随机本质的关系，也没有论证样本量和结论可信度的联系。文献[5]指出，游程检验并不能很好地反映随机性的本质特征。文献[6-8]对扑克检验及二元推导检验的参数集进行研究，为带参检测项目提供了优化方法和思路，但理论性过强难以指导操作，且以牺牲空间复杂度为前提，对资源受限的 Zigbee 系统并不适用。文献[9]将傅里叶变换检验的参考分布近似二项分布处理，对门限值和方差进行了优化，但仍存在一定的误差。文献[10]表明，块内频数检验和非叠加模式匹配检验虽具有较强的硬件可实现性，但对序列长度要求较高，测试耗时较长。文献[11-14]提出了新的随机性测试方法，但检验前提是被测网络采用的加密算法、加密结构已知，对加密算法未知或自定义的 Zigbee 系统并不适用。

同时，文献[15,16]表明，二元矩阵秩检验的淘汰能力较高，可以尽早淘汰不随机的序列。文献[10,17]表明，二元矩阵秩检验与 Lempel-Ziv 检验的检验方法相似。Lempel-Ziv 检验检测效果显著，被认为是可以包含频数检验、游程检验、其他压缩检验甚至频谱检验等，但 Lempel-Ziv 检验无法准确定义其分布函数的统计量，其适用性受到很大限制。可见，二元矩阵检验具有淘汰能力高、检测效果显著且适用性较广的特点，可提高测试效率。但进一步研究发现，二元矩阵秩检验涉及复杂的数学变换，硬件实现的资源开销大且检测速度较慢。当二元矩阵检验的构造矩阵全为满秩时的 P_{-value} 值甚至低于不全为满秩的 P_{-value}，该检验只能从线性相关性片面对序列是否随机做出判断，却无法对随机性的强弱做出判断。

综上所述，为了满足 Zigbee 协议随机性检测中对高效性、实时性的要求，本文在二元矩阵秩检验的基础上，为了有效解决二元矩阵秩检验单纯从线性相关性判断随机序列的片面性，结合 Zigbee 协议的特点，从硬件实现性开销及减少误差的角度出发，通过对矩阵元素随机性的概率进行研究，提出了基于矩阵概率检验算法，可有效判断被测序列是否加密及加密强度，实现对 Zigbee 协议数据传输的安全性检测。

1 基于矩阵概率检验的随机性检测算法

1.1 序列的划分方式和测试的组织方式

在对 Zigbee 进行随机性测试时，由于矩阵概率检验是通过考察矩阵的概率分布进行判断，概率分布是测量伪随机序列的不可预测性的一个非常重要的指标，在实际测试过程中，概率分布存在不稳定的性质。因此，为了使随机性测试更加高效、可靠，提出一种合理的测试组织方式，从而有效考察随机序列的稳定性。

频数检验是 NIST SP800-22 提出的最基本的检验方法，具有实现简单、区分度好、样本需求量小、计算快捷等优点，为了快速鉴别 Zigbee 网络是否采取加密传输，可利用此检验对序列进行先验检测。若样本未通过频数检验，即可认为序列是不随机的，不必再进行其他检验。通过频数检验之后，方可进行矩阵概率检验，对序列的随机性强度做出检验。

同时，NIST 分析研究了频数检验与矩阵检验的依赖关系，其结论是两者之间的依赖关系很小。文献[18,19]表明，频数检验与矩阵检验之间的相关度 $R=0.025<0.2$，二者存在着很小的依赖关系，相关性较小。因此，采用将两者结合的方式，不仅不会对测试结论产生相关性影响，而且会使测试更具说服力，更加高效。

具体测试组织方式如下：

步骤 1：首先将 Zigbee 序列测试样本划分为组，定义每组样本的编号为 $1,2,3,\cdots,N$。

步骤 2：分别对每组样本进行频数检验，考察

被检验序列各部分的随机性。若样本未通过此检验，则测试结束；若通过此检验，可继续进行下一步。

步骤 3：采用累加测试的方式，依次逐一增加样本的数量（即每次增加一组样本，N 组的样本即整体序列）进行矩阵概率检验，考察被测序列随机性的平稳性，对 Zigbee 加密算法的随机强度做出验证。

需要说明的是，此方法是以频数检验为前提，首先测试被测序列的 0 码或 1 码的比例是否为 1/2；在被测序列 0 码较为平均的前提下，使用矩阵概率检验可进一步考察序列中 0 或 1 的分布是否为均匀随机分布。

由于实际测试过程采用了多序列测试策略，在评价随机序列性能好坏时，可采用 NIST SP800-22 提出的 $P_{-\text{value}}$ 值分布的均匀性方法来描述。具体方法是：选定由加密算法产生的若干个序列进行随机性测试，产生对应的 $P_{-\text{value}}$ 值集合，通过考察 $P_{-\text{value}}$ 值通过率及其分布特性对加密算法进行评价。由于 $P_{-\text{value}}$ 是 0 到 1 之间的实数，可将 0－1 等划分为 10 个区间，当序列个数足够多时，$P_{-\text{value}}$ 值应该平均分布在这 10 个区间。统计每个区间的频数，记为 V_i，则有 $V_1+V_2+\cdots V_{10}=h$（h 为序列个数），计算其统计量的卡方分布 $\chi^2=\sum_{i=1}^{10}\frac{(v_i-h/10)^2}{(h/10)}$，计算假设概率 $P_{-\text{valueT}}=\text{igamc}\left(\frac{9}{2},\frac{\chi^2}{2}\right)$，若 $P_{-\text{valueT}}>0.000\ 1$，则认为序列是符合均匀分布的，即随机性较好。

若 Zigbee 样本无法通过频数检验，则可认为随机性很差，该 Zigbee 网络未采取加密措施，数据很可能是明文传送的；若通过频数检验，且符合均匀分布特性，则表明该 Zigbee 网络的随机性较好，继续进行矩阵概率检验。

若样本未通过矩阵概率检验，则可以认为 Zigbee 网络实施的加密机制不够安全或根本未实施加密机制；若通过矩阵概率检验，即表明该 Zigbee 网络的随机性较平稳，可以认为该 Zigbee 网络实施了安全的加密机制。

1.2　基于矩阵概率的随机性检验算法

线性相关性检验是衡量序列随机性很重要的一个指标，在二元矩阵秩检验中，采用统计测试序列构造的方阵中满秩矩阵的数量 F_m，秩为 $m-1$ 的矩阵数量 F_{m-1}，通过考察矩阵的行与列的线性相关性来判断序列的随机性。但相对于传统信息系统而言，Zigbee 网络的丢包率较高[20]，数据包的缺失及获取数据的先后顺序都会对矩阵的秩产生较大的影响，从而使二元矩阵秩检验的结果不能够真实反映 Zigbee 序列的随机性。该检验方法并不完全适用于 Zigbee 网络，且 NIST 定义二元矩阵检验的方阵阶数为 32，此时方阵都表现为较低的线性相关性，且二元矩阵检验是通过 $P_{-\text{value}}$ 比较法进行判断。在某些情况下，二元矩阵检验可以给出序列非随机的结论，却可能无法检测出明显非随机的序列。

本文借鉴二元矩阵检验的思想，结合 Zigbee 的特点，从二元矩阵元素的随机性概率入手，通过检验新生成矩阵中 0 所占的比例是否接近在假设序列具有随机性条件下 P_c 的概率，提出基于矩阵概率检验的检测方法，从而对测试序列的随机性做出判断；且该方法是域值判断法，可直观看出期望值与理论值的差值大小，即随机性的强弱，误差小，可靠性高。

若方阵 $\boldsymbol{A}$ 和方阵 $\boldsymbol{B}$ 中符号 0 出现的概率分别为 P_a 和 P_b，令新生成的矩阵 $\boldsymbol{C}=\boldsymbol{AB}$，若 $\boldsymbol{A}$，$\boldsymbol{B}$ 中符号 0 是随机分布的，则 $\boldsymbol{C}$ 中符号 0 出现的概率为：$P_c=(P_a+P_b-P_aP_b)^m$，m 为方阵的阶。定义方阵 $\boldsymbol{C}$ 中的元素为 c_{ij}，方阵 $\boldsymbol{A}$ 中的元素为 a_{it}，方阵 $\boldsymbol{B}$ 中的元素为 b_{tj}。

证明：对于生成的方阵 $\boldsymbol{C}$，其中任一元素为 $c_{ij}=\sum_{t=1}^{m}a_{it}b_{tj}$。

方阵 $\boldsymbol{C}$ 中 0 出现的概率为

$$P_c=(c_{ij}=0)=\prod_{t=1}^{m}P(a_{it}=0 or b_{tj}=0)=$$

$$\prod_{t=1}^{m}\begin{pmatrix}P(a_{it}=1)\,P(b_{tj}=0)+\\P(a_{it}=0)\,P(b_{tj}=1)+\\P(a_{it}=0)\,P(b_{tj}=0)\end{pmatrix}=$$

$$\prod_{t=1}^{m}((1-P_a)P_b+P_a(1-P_b)+P_aP_b)=$$

$$\prod_{t=1}^{m}(P_a+P_b-P_aP_b)=(P_a+P_b-P_aP_b)^m$$

矩阵概率检验的算法如下：

步骤 1：将长度为 n 的 Zigbee 输出序列作为待测序列，依序将待测序列划分为 $\boldsymbol{M}=\left[\frac{n}{2}\right]$ 比特的不相交的区块，得到 2 个区块，剩余的 $n-2\times M$ 位将被舍弃。

步骤 2：分别将两个 M 比特的区块，构造为两个 $m\times m$ 的矩阵，定义为方阵 $\boldsymbol{A}$ 与方阵 $\boldsymbol{B}$，统计两

个方阵中 0 所占的比例，其中，$M=m^2$。

方阵 $\boldsymbol{A}$，$\boldsymbol{B}$ 中 0 所占的比例 P_a，P_b 分别为：

$$P_a=P(a_{it}=0)=\frac{\text{方阵 }\boldsymbol{A}\text{ 中 0 的数目}}{m^2}$$

$$P_b=P(b_{tj}=0)=\frac{\text{方阵 }\boldsymbol{B}\text{ 中 0 的数目}}{m^2}$$

为便于讨论，在元素个数为 m^2 的方阵中，可将方阵中的元素看为二元序列，记为 $\varepsilon_k(1\leqslant k\leqslant m^2)$。利用式(1)计算方阵中 0 所占的比例

$$P=1-\frac{\sum_{k=1}^{m^2}\varepsilon_k}{m^2}(1\leqslant k\leqslant m^2) \tag{1}$$

步骤 3：将方阵 $\boldsymbol{A}$ 与方阵 $\boldsymbol{B}$ 进行相乘运算，得到新生成的矩阵 $\boldsymbol{C}=\boldsymbol{AB}$。方阵 $\boldsymbol{C}$ 为 $c_{ij}=\sum_{t=1}^{m}a_{it}b_{tj}$。

方阵 $\boldsymbol{C}$ 中 0 码所占的统计比例 $P_{c(\text{obs})}$，$P_{c(\text{obs})}=P(a_{ij}=0)=\frac{\text{方阵 }\boldsymbol{C}\text{ 中 0 的数目}}{m^2}$。同理，采用式(1)计算。

步骤 4：对于统计的比例 P_a 和 P_b，计算对应的期望值 $P_c=(P_a+P_b-P_aP_b)^m$。理论上，当统计的概率值 $P_{c(\text{obs})}$ 与期望值 P_c 相等时，则认为序列通过此检验。

事实上，产生的每一个序列都与期望的结果完全相符不可能，也不全面。因此可引入统计学中的置信区间概念，当 $P_{c(\text{obs})}\in(P_c-3\sqrt{\alpha(1-\alpha)/h}$，$P_c+3\sqrt{\alpha(1-\alpha)/h})$区间时($\alpha$ 为显著性水平，h 为序列个数)，则认为序列通过该检验；反之，则未通过该检验。

本文的矩阵概率检验算法，通过考察生成矩阵随机分布的概率来判断原序列的随机性，减少大量复杂的数学运算，且硬件实现资源开销小，可满足 Zigbee 随机性检测过程中对资源有限和实时性的要求；且通过比较统计结果与期望值的偏差大小，不仅可以有效检测出非随机的序列，还可以检测出明显非随机的序列，使检测结果的误差更小，结果更准确，更适合于对 Zigbee 随机序列的检测。

2 仿真实验与分析

2.1 仿真环境

本文采用 MATLAB 软件进行仿真，分别选取 3 套不同厂家的 Zigbee 协议传输数据作为样本。其中，来自 A 单位的 Zigbee 设备，未采取和部署加密措施；来自 B 单位的 Zigbee 设备，在协议中采用了轻量级密码算法进行数据加密；C 单位的 Zigbee 设备，采用 AES CCM* 加密算法进行数据加密。

为更好地统计测试样本参数，保证实验结果的可比较性，实验选取同一节点、不同时刻数据载荷的同一位置(某字节)进行分析。具体随机性检测实验参数说明如下：

(1)样本容量：抽取 50 组 50 字节的样本序列，每一组样本序列从 50 个 Zigbee 有效载荷数据中各抽取 1 个字节，组成一个 50 字节的 Zigbee 序列。

(2)显著性水平：根据 NIST 标准检测标准的要求，显著性水平值设置为 0.01。

(3)样本起点、样本终点：在抽取样本时，实验对数据载荷的同一位置进行分析。

2.2 仿真实验及结论分析

(1)算法正确性验证：随机抽取 50 组样本数据，依次对每组数据进行矩阵概率检验和矩阵秩检验，测试样例见表 1。其中，序列个数 $h=50$，显著性水平 $\alpha=0.01$，统计值 $P_{c(\text{obs})}\in(P_c-0.042\,2$，$P_c+0.042\,2)$。

表 1 矩阵概率检验的准确性验证

Table 1 Accuracy verification of matrix probability test

矩阵概率检验			矩阵秩检验
期望值 P_c	统计值 $P_{c(\text{obs})}$	P_c 与 $P_{c(\text{obs})}$ 之差 P'	$P_{-\text{value}}$
0.031 4	0.02	0.011 4	0.481 3
0.063 2	0.081	0.017 8	0.741 9
0.081 3	0.053	0.028 3	0.085 2
0.073 3	0.039	0.034 3	0.423
0.084	0.051	0.033 0	0.328
0.039 9	0.065	0.025 1	0.539
0.092 4	0.05	0.042 4>0.042 2	0.006 2<0.01 (未通过检验)
0.067 3	0.037	0.030 3	0.235
0.038 8	0.089	0.050 2>0.042 2	0.002 7<0.01 (未通过检验)
0.024 7	0.09	0.065 3>0.042 2	0.008 3<0.01 (未通过检验)
0.081 5	0.01	0.071 5>0.042 2	0.000 773<0.01 (未通过检验)
0.016 6	0.078	0.061 4>0.042 2	0.000 158<0.01 (未通过检验)
⋮	⋮	⋮	⋮

通过数据分析，当矩阵概率检验的期望值与统计值的差值 P' 不在期望区间内时，矩阵秩检验的 $P_{-\text{value}}$ 值也小于 0.01，表明序列随机性很差；当 P' 在区间内时，矩阵秩检验的 $P_{-\text{value}}$ 值均大于 0.01，表明序列随机性较好。实验表明，矩阵概率检验与二元矩阵检验反映的随机性结论是一致的，矩阵概

率检验可准确检测出序列的随机性。同时，矩阵概率检验可更直观地看出矩阵概率的期望值与统计值的差值，即加密算法的强弱。

(2)测试组织方式合理优越性验证：随机抽取 50 组样本序列，分别采用单个检验和逐次累加检验的方式进行，测试结果如下图 1 所示。

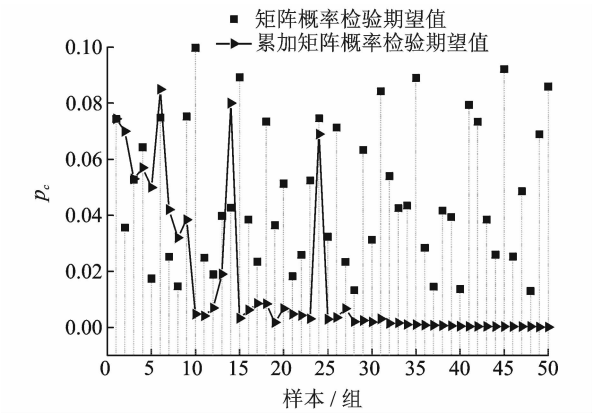

图 1　组织方式合理优越性验证

Fig. 1　Superiority verification of organizes and divides test modes

实验分析：采用单个样本组检验时，统计值 p_c 在 0～0.1 之间无规则分布；当采用逐次累加样本组检验时，可明显看出序列的平稳性在样本数为 6，14，24 时波动较大，随着样本组的增多，p_c 值逐渐趋于平稳。实验证明，在进行随机性测试时，采用逐次累加方式可更直观地考察序列的随机平稳性，可更合理地对随机性的强弱做出判断，此方法更加合理、优越。

(3)对 A 单位的未采取和部署加密措施的 Zigbee 设备，随机性测试结果如图 2 所示。

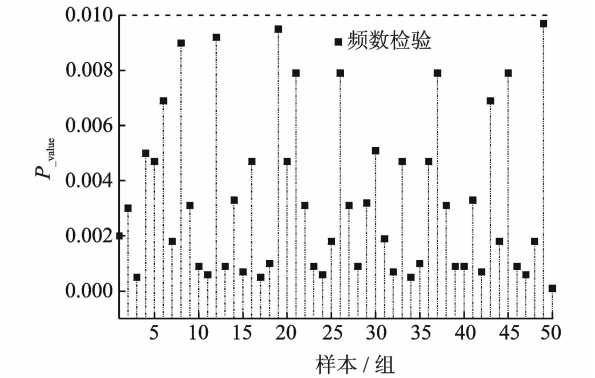

图 2　未采取加密措施

Fig. 2　Without encryption measures

实验结果分析：在此测试中，频数检验的 P_{-value} 均小于 0.01，样本无法通过该测试，测试结束，表明此样本的随机性很差，该网络的 Zigbee 数据很可能是明文传送的。随机性检测方法能够成功判断 Zigbee 协议数据是否经过加密传输。通过频数检验，可有效对未经加密传输的序列进行筛选，不必再进行后续检验即可对随机性做出判断，可显著提高测试效率。

(4)对 B 单位的采用改良后的 Zug 轻量级密码算法进行数据加密的 Zigbee 设备。其中，P_{-value} 表示频数检验的检测结果，p_c 表示矩阵概率检验的检测结果，随机性测试结果如图 3 所示。

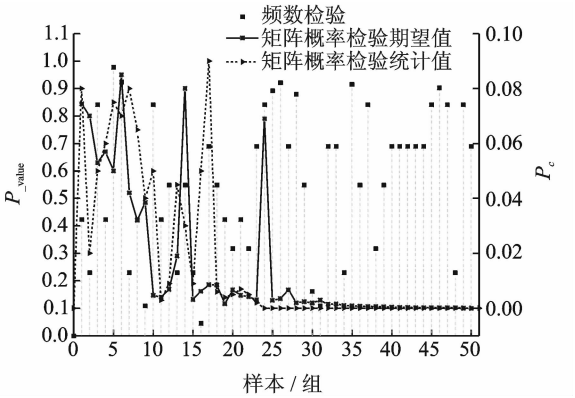

图 3　轻量级加密算法

Fig. 3　Lightweight encryption algorithms

实验分析如下，在此测试中，频数检验时，$P_{-value}>0.01$，且在 0～1 之间分布较为均匀，统计计算的概率值 $P_{-valueT}=0.018\ 7>0.000\ 1$；矩阵概率检验时，部分样本的统计值 p_c 与期望值的偏差较大，未能通过检验，样本的随机平稳性较差。实验显示该样本可以通过频数测试，未能通过矩阵概率检验，则认为样本随机性较好，随机平稳性即加密强度较差。对应的 Zigbee 协议实施了加密机制，但由于采用轻量级加密算法，存在加密强度不足的可能性。随机性检测方法能够判断 Zigbee 协议数据的是否加密传输及加密的强度。

(5)对 C 单位采用 Zigbee 协议默认的 AES CCM* 加密算法进行数据加密的 Zigbee 设备，随机性测试结果如图 4。

实验分析如下，频数检验时，$P_{-value}>0.01$，且在 0－1 之间分布较为均匀，统计计算的概率值 $P_{-valueT}=0.029\ 6>0.000\ 1$。矩阵概率检验时，样本的统计值 p_c 与期望值基本吻合，均通过矩阵概率检验。实验表明，该样本既可以通过频数检验，又可以通过矩阵概率检验，认为样本随机性较好，随机平稳性即加密强度也较好。对应的 Zigbee 网

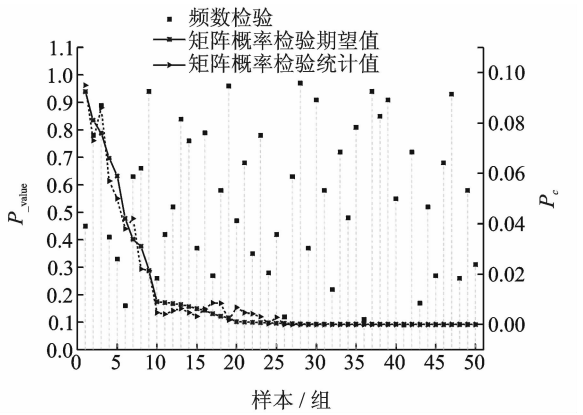

图 4 AES CCM* 加密算法

Fig. 4 AES CCM* encryption algorithms

络实施了加密机制，且密文的安全性也很高，采用 AES CMM* 加密模式 Zigbee 协议具有较好的保密性。随机性检测方法能够准确判断 Zigbee 协议数据是否加密传输及判断加密强度。

3 结束语

本文从密码算法安全性的角度出发，对 Zigbee 协议的随机性进行研究，提出了基于矩阵概率检验的 Zigbee 协议随机性检测算法、测试序列的划分及测试组织方式，采用合理科学的评价方法，使其具有理论保证。通过仿真实验，验证该算法具有检测误差小，可靠性高的优点；同时，该算法具有较强的硬件可实现性，并且可以对随机性的强弱做出有效判断，满足 Zigbee 系统对于实时性、可靠性的检测要求。本文提出的测试方法与思路局限于在 Zigbee 系统的安全性检测中适用，对于是否适用于其他类型的无线传感网的安全测评还有待验证。

因此，本课题下一步的工作重点将深入研究 WIFI、蓝牙等无线传感网的安全检测方法，为物联网感知层的信息安全测评提供更为系统完善的理论基础和可操作的指导方法。

参考文献：

[1] Schneier B. Secrets and lies: digital security in networked world [M]. New York: Jone Wiley and Sons, 2000:85-101.

[2] Ryabko B Y, Fionov A N, Monarev V A, et al. Using information theory approach to randomness testing[M]. Berlin: Springer, 2006:261-272.

[3] Marsaglia G. Diehard battery of tests of randomness [EB/OL]. http:// stat. fsu. edu/geo/diehard. html. 1995-12-09.

[4] National Institute of Standards and Technology. NIST SP 800-22. A statistical test suite for random and pseudorandom number generators for cryptographic applications[S]. U S Department of Commerce, 2010.

[5] 石竑松，张翀斌，杨永生，等. 随机性检测及其片面性[J]. 清华大学学报：自然科学版，2011，51(10)：1359-1363.
Shi Hongsong, Zhang Chongbin, Yang Yongsheng, et al. On the randomness test and its incompleteness [J]. J Tsinghua Univ: Sci & Tech, 2011, 51(10): 1359-1363.

[6] Chen Hua, Fan Limin. How to choose proper parameter values for poker test[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2008, 25(5):631-638.

[7] 范丽敏，冯登国，陈华. 随机性检测参数选择研究[J]. 通信学报，2009，30(1)：1-6.
Fan Limin, Feng Dengguo, Chen Hua. On the parameter selection of randomness test[J]. Journal on Communications, 2009, 30(1):1-6.

[8] 范丽敏，冯登国，许囡囡. 二元推导随机性检测的优化实现[J]. 计算机工程，2008，34(19)：20-22.
Fan Limin, Feng Dengguo, Xu Nannan. Optimization implementation of binary derivation randomness test[J]. Computer Engineering, 2008, 34(19):20-22.

[9] Kim S J, Umeno K, Hasegawa A. Corrections of the NIST statistical test suite for randomness[EB/OL]. http://arXiv:nlin. CD/0401040vl. 2004-01-07.

[10] 胡俭勇，苏锦海. 一种随机性实时检测方案[J]. 计算机工程，2009，35(9)：136-139.
Hu Jianyong, Su Jinhai. Scheme for real time test of randomness[J]. Computer Engineering, 2009, 35(9):136-139.

[11] 陈华. 密码算法的安全性检测及关键组件的设计[D]. 北京：中国科学院软件研究所，2005.
Chen Hua. Security test on cryptographic algorithms and design of key cryptographic components[D]. Beijing: Institute of Software Chinese Academy of Sciences, 2005.

[12] 陈华，冯登国，范丽敏. 一种关于分组密码的新的统计检测方法[J]. 计算机学报，2009，32(4)：595-601.
Chen Hua, Feng Dengguo, Fan Limin. A new statistical test on block ciphers[J]. Chinese Journal of Computers, 2009, 32(4):595-601.

[13] 范丽敏，冯登国，陈华. 对 3 个流密码及其组件的随机

性检测分析[J]. 高技术通讯，2007，17(2)：16-19.
Fan Limin, Feng Dengguo, Chen Hua. Analysis on randomness testing of three stream ciphers and their components[J]. High Technology Letters, 2007, 17(2): 16-19.

[14] Qi S, Xu M, Zheng N. A malware variant detection method based on byte randomness test[J]. Journal of Computers, 2013, 8(10): 2469-2477.

[15] 于亦舟，欧海文. 串行检验比较于传统的随机性检验方法的优越性[J]. 通信学报，2007，28(6)：20-23.
Yu Yizhou, Ou Haiwen. Serial test is superior to the traditional sequences random tests[J]. Journal on Communications, 2007, 28(6): 20-23.

[16] 黄佳琳，来学嘉. 随机性测试的淘汰能力和相关性[J]. 信息安全与通信保密，2009，(10)：43-46.
Huang Jialin, Lai Xuejia. Eliminating ability and correlation of random statistical tests[J]. Information Security and Communications Privacy, 2009, (10): 43-46.

[17] Blum L, Blum M, Shun M. A Simple unpredictable pseudorandom number generator[J]. SIAM Journal on Computing, 1986, 15(2): 364-383.

[18] 范丽敏，冯登国，陈华. 基于熵的随机性检测相关性研究[J]. 软件学报，2009，20(7)：1967-1976.
Fan Limin, Feng Dengguo, Chen Hua. Study on the correlation between randomness tests based on entropy[J]. Journal of Software, 2009, 20(7): 1967-1976.

[19] Fan Limin, Chen Hua, Gao Si. Information security applications[M]. Switzerland: Springer International Publishing, 2014: 52-62.

[20] 胡爱群，李古月. 无线通信物理层安全方法综述[J]. 数据采集与处理，2014，29(3)：341-350.
Hu Aiqun, Li Guyue. Physical layer security in wireless communication: A survey[J]. Journal of Data Acquisition and Processing, 2014, 29(3): 341-350.

作者简介：汤永利(1972-)，男，副教授，研究方向：信息安全、密码学，E-mail：yltang@hpu.edu.cn；王真(1988-)，女，硕士生，研究方向：网络与信息安全、物联网安全；张雯雯(1982-)，女，硕士生，研究方向：网络安全；刘海峰(1975-)，男，副研究员，研究方向：信息安全、等级测评；郭玉翠(1962-)，女，教授，研究方向：微分方程。