基于纠错码理论的群组认证

王 宏[1,2],李建华[1],赖成喆[3],曲 宁[2]
(1. 空军工程大学信息与导航学院,陕西西安 710077;
2. 国防科技大学信息通信学院,陕西西安 710106;3. 西安邮电大学,陕西西安 710121)

摘 要: 为解决群组认证中非法签名难以标定的问题,本文基于数字通信系统中的纠错码理论,提出了一个非适应性组合群组认证方案. 该方案首先根据纠错码理论构造认证节点分组算法,然后按照分组进行节点签名的批量认证,再对分组认证结果进行迭代,从而标定非法签名,最后进行了例证演示. 复杂度分析表明,针对 n 个签名(含有 r 个非法签名)进行非法者标定的问题,运用群组认证的标定次数远远小于逐一认证的 n 次,准确性演化结果表明当 r 远远小于 n 时,群组认证非法签名的标定成功概率接近于 1.

关键词: 群组认证; 组合分组测试; 纠错码
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2019)07-1393-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.07.001

Group Authentication Based on Error Correction Coding Theory

WANG Hong[1,2], LI Jian-hua[1], LAI Cheng-zhe[3], QU Ning[2]
(1. *Information and Navigation College, Air Force Engineering University, Xi'an, Shaanxi* 710077, *China*;
2. *Information and Communication College, National University of Defense Technology, Xi'an, Shaanxi* 710106, *China*;
3. *Xi'an University of Posts & Telecommunications, Xi'an, Shaanxi* 710121, *China*)

Abstract: Because it is difficult to identify bad signatures in group authentication schemes, the work is concerned with combinatorial group test based on error correction coding theory in digital communication system and a novel non-adaptive group authentication scheme is proposed. Firstly, the grouping algorithm of all nodes is proposed based on error correction coding theory; secondly, batch certification is implemented according to the groups; thirdly, bad signature is identified by iterative analyses; finally, an example is demonstrated. Complexity analyses show the identification times of the group authentication scheme of n signatures with r bad signatures is much less than n times of one-by-one authentication. Accuracy analyses show the probability of identification of the group authentication scheme is close to 1 when r is much less than n.

Key words: group authentication; combinatorial group test; error correction code

1 引言

在节点组网认证过程中,当存在大量节点合法性需要快速验证时,传统的逐一验证[1,2]往往比较耗费时间,群组认证通过聚合算法将 n 个节点的数字签名聚合生成一个固定长度的短签名,只需要验证这个短签名就可以批量确定所有签名是否合法[3~5],大大缩减了验证时间,有利于提高认证效率. 群组认证要求所验证的数字签名必须具有同态性[6,7]结构,基于模指数运算的数字签名就是比较常见的具有同态性的签名[6].

假设 $\boldsymbol{X}=(\sigma_1,\cdots,\sigma_n)$ 为待处理的一批签名,其中 $\sigma_i=m_i\parallel s_i; i=1,2,\cdots,n, m_i$ 为第 i 个消息,σ_i 为其对应的签名,p 为一个大素数,g 为乘法群 Z_p 的一个生成元. 如果通过检验

$$g^{m_i}\stackrel{?}{=}s_i(\mathrm{mod}p); i=1,\cdots,n \tag{1}$$

逐一检查所有签名的合法性,这个过程需要完成 n 个模指数运算. 由于模指数运算具有同态特征,可以将 n 个签名通过式(2)进行批量验证

$$g^{\sum_{i=1}^{n}m_i}\stackrel{?}{=}\prod_{i=1}^{n}s_i(\mathrm{mod}p) \tag{2}$$

这个过程只需要完成 1 个模指数运算,$n-1$ 个加法和 $n-1$ 个乘法运算. 相比较而言,模指数运算的消耗要远

收稿日期:2018-06-21;修回日期:2018-12-10;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61872293);陕西省创新人才推进计划-青年科技新星项目(No. 2017KJXX-47)

远大于加法和乘法运算,对比式(1)的逐一验证,式(2)的批量验证大大提高了验证效率.

有关群组认证的研究近年来已有很多文献[8~15],然而,这些方案都存在一个很大的缺陷,即难以抵抗拒绝服务攻击[16]. 当所有签名都为合法签名时,类似于式(2)的批量验证可以顺利通过;如果这一批签名中存在一个非法签名,则必定导致式(2)的检验失败,无法确认签名的合法性. 如果敌方始终释放非法签名干扰认证的进行,则无法进行正常的群组认证. 因此,当有非法者混入的情况下,保证群组认证的正常进行,并标定非法者,便成为群组认证亟待解决的问题. 当然,逐一进行签名验证也是一种解决办法,然而这需要较大的验证开销,能否找到一种检验次数较少又能标定非法签名的群组认证成为近年来的热点[17,18].

2 问题描述

群组认证(Group Authentication,GA)是组合数学中的组合分组测试(Combinatorial Group Test,CGT)理论[19]在认证方面的应用,它利用 CGT 理论对认证节点进行分组,并按分组对节点签名进行验证,标定非法者,从而实现以较少验证次数完成对所有签名的认证.

定义 1 (群组认证,GA):设 $\boldsymbol{X}$ 为所有节点签名的集合,$|\boldsymbol{X}|=n$,$\wp(\boldsymbol{X})$ 是 $\boldsymbol{X}$ 的幂集,$\mathcal{T}$ 为签名 $\boldsymbol{X}$ 的分组测试集合族,即 $\mathcal{T}\subseteq\wp(\boldsymbol{X})$. $\forall \boldsymbol{A}\subset\boldsymbol{X}$,$|\boldsymbol{A}|=r$,对于任意签名 $\sigma\notin\boldsymbol{A}$,则 $\exists \boldsymbol{B}\in\mathcal{T}$,满足 $\sigma\in\boldsymbol{B}$ 且 $\boldsymbol{A}\cap\boldsymbol{B}=\varnothing$,即通过对 $\boldsymbol{B}$ 中签名的验证,可以将 σ 从 $\boldsymbol{A}$ 剥离出来. 这种对所有签名 $\boldsymbol{X}$ 按照 $\mathcal{T}$ 进行分组测试的认证方法,称为群组认证,记作(n,r) - GA.

关于 CGT 理论的研究最早可以追溯到二战时期美军入伍士兵血样的梅毒检测,将一定数量的血液标本进行混合,然后对其进行检测,如果结果为阴性则表明这些标本没有被梅毒病菌感染,否则,说明这些标本中至少有一个被梅毒感染[6]. 后来,组合分组检测理论在工业、农业、医疗等方面有了进一步的应用. 在群组认证中,检测对象是签名的集合,记为$(\sigma_1,\cdots,\sigma_n)$,非法签名的集合记为 $\boldsymbol{K}$,个数记为 r,分组的个数记为 t,分组检测算法是签名验证算法,要检测的目的是确定非法的签名. 它的基本模型:假设有 n 个被验证的对象,它们的验证结果要么是合法,要么是非法,组合分组测试的根本问题就是通过巧妙地设计分组,通过尽可能少的验证次数完成对 $\boldsymbol{K}$ 中非法对象的标定.

按照过程的时序性要求,分组测试理论可以分为两种类型:适应性分组测试(Adaptive Group Test,AGT)和非适应性分组测试(Non-Adaptive Group Test,NAGT). 适应性测试算法的检测过程在时间上被分成具有先后次序的几个不同阶段,DCV[20,21](Divide-and-Conquer Verifiers)是最为著名的适应性检测算法,它将$(\sigma_1,\cdots,\sigma_n)$分成若干个分组,对分组进行检测,下一轮的检测过程由上一轮的检测结果给出,后面的检测取决于前面的检测结果;而非适应性测试要求事先确定检测过程,所有检测可以同步进行,有利于检测效率的提高,因此,本文主要考虑非适应性测试. 目前,有关非适应性分组测试的研究主要集中在分组设计方面[17~28],仍然存在一些不足之处,主要体现在 3 个方面:一是多数研究以析取矩阵(disjunctive and separable matrix)的构造为基础研究了分组理论,集中于分组设计,并没有对非法者身份进行甄别的算法[17,19~21];二是许多文献提出的组合分组检测方案,在方案设计前需要知道非法者的具体数量或数量的上界[17,20,21],这在实际应用中往往并不现实;三是多数组合分组检测方案仅能在包含一到两个非法者的情况下进行有效的身份识别[18,22~25],当两个以上非法者干扰认证时,则没有效果.

本文基于纠错码的分组测试理论,构建群组认证数学模型,提出一种群组认证方案,对签名进行分组验证,旨在快速标定非法签名,完成所有节点的认证.

3 群组认证方案

假设群组认证中即将进行的批量验证的签名为 $\boldsymbol{X}=(\sigma_1,\cdots,\sigma_n)$,向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\{0,1\}^n$ 表示 n 个要检测签名的状态,若合法,则 $x_j=0$;否则,$x_j=1$;$j=1,\cdots,n$. supp(·)表示 $\boldsymbol{x}$ 中非零元素的个数,根据上文则 $\mathrm{supp}(x)=|\boldsymbol{K}|=r$. 将 n 个签名分为 $t(t\ll n)$ 个不同的分组,记为 $\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_t$,检测结果记为 $\boldsymbol{y}^{\mathrm{T}}=(y_1,\cdots,y_t)\in\{0,1\}^t$,若检测合法,则 $y_j=0$;否则,$y_j=1$,$j=1,\cdots,t$. 签名和分组的对应关系可以由 t 行 n 列关联矩阵 $\boldsymbol{M}_{t\times n}$来表示,$\boldsymbol{M}$ 的行 $\boldsymbol{M}_{1\cdot},\boldsymbol{M}_{2\cdot},\cdots,\boldsymbol{M}_{t\cdot}$ 表示不同的分组,$\boldsymbol{M}$ 的列 $\boldsymbol{M}_{\cdot 1},\boldsymbol{M}_{\cdot 2},\cdots,\boldsymbol{M}_{\cdot n}$表示要检测的签名,$\boldsymbol{M}$ 中的元素 $m_{ij}\in\{0,1\}$,$1\le i\le t$,$1\le j\le n$. $m_{ij}=1$ 意味着签名 σ_j 属于第 i 个分组 $\boldsymbol{B}_i$,$m_{ij}=0$ 意味着签名 σ_j 不属于第 i 个分组 $\boldsymbol{B}_i$.

因此

$$\begin{aligned}\boldsymbol{y}&=\boldsymbol{M}\times\boldsymbol{x}^{\mathrm{T}}\\&=(\boldsymbol{M}_{\cdot 1}x_1+\boldsymbol{M}_{\cdot 2}x_2+\cdots+\boldsymbol{M}_{\cdot n}x_n)\end{aligned}\tag{3}$$

文中相关符号的定义如表 1 所示.

群组认证的最终目的是通过分组检测以最小的代价由 $\boldsymbol{y}$ 重构 n 个签名的合法状态向量 $\boldsymbol{x}$,记为 $D_M:\{0,1\}^t\to\{0,1\}^n$,使得重构的结果 $\hat{\boldsymbol{x}}=D_M(\boldsymbol{y})$ 满足 $\mathrm{set}(\hat{\boldsymbol{x}})\subseteq\mathrm{set}(\boldsymbol{x})$ 且 $|\mathrm{set}(\hat{\boldsymbol{x}})|\ge(1-\varepsilon)|\boldsymbol{K}|$,其中 set(·)表示对应的非零元素的集合,$0<\varepsilon<1$ 表示任意小的正数. 由于检验是通过分组做出的,总有可能做出错误的决策,当节点非法时可能接收其认证,称为“取伪”,记为 ε;相反地,当节点合

法时可能犯拒绝节点的错误,称为“弃真”错误. 为此,在确定分组方案时,应尽可能使犯两类错误的概率都较小. 通常当检验次数固定时,若犯“取伪”错误的概率减小,则犯“弃真”错误的概率往往增大,因此本文选择控制“取伪”错误的概率,使它不大于某个值.

表 1　相关符号的涵义

符号	意义
n	节点数
t	分组数
$\boldsymbol{S}$	合法节点的集合
$\boldsymbol{K}$	非法节点的集合
r	非法节点的个数
$\boldsymbol{M}$	关联矩阵
s	节点签名
X_j	第 j 个节点
$\boldsymbol{B}_i$	分组检测的第 i 个分组
$\boldsymbol{x}$	节点的状态
$\boldsymbol{y}$	分组检测的结果
$\hat{\boldsymbol{S}}$	$\hat{\boldsymbol{S}}:=\{X_j \mid m_{ij}=1 \text{ 且 } y_i=0\}$
supp(·)	非零元素的个数
set(·)	对应的非零元素的集合
$\hat{\cdot}$	估计量
$[n]$	$\{0,1,2,\cdots,n-1\}$
$\lvert\cdot\rvert$	集合中元素的个数
$\lceil\cdot\rceil$	向上取整

3.1　认证节点的分组

群组认证的首要问题是节点的分组设计,首先将签名进行分组,然后对每个分组进行检测,根据检测结果确定非法的签名. 关联矩阵 $\boldsymbol{M}_{t\times n}$ 是分组理论的数学模型,我们采用集合分割的概念描述构造过程.

定义 2　对于任意 $\boldsymbol{A}\subset\boldsymbol{X}$, $\forall\sigma\in\boldsymbol{A}$,如果 $\exists\boldsymbol{B}\subset\boldsymbol{X}$,使得 $\boldsymbol{A}\cap\boldsymbol{B}=\{\sigma\}$,则称元素 σ 被集合 $\boldsymbol{B}$ 选取. 同理,元素 σ 被集合族 $\mathcal{F}\subseteq\mathcal{P}(\boldsymbol{X})$ 选取,意味着 σ 被集合族 $\mathcal{F}$ 中的至少一个子集选取.

定义 3　对于任意 $\boldsymbol{A}\subset\boldsymbol{X}$, $|\boldsymbol{A}|=r$,如果 $\boldsymbol{A}$ 中的每一个元素都被集合族 $\mathcal{F}\subseteq\mathcal{P}(\boldsymbol{X})$ 选取,则称 $\mathcal{F}$ 为 (n,r) 选取集合族(Selective Family),记作 $(n,r)-\mathrm{SF}$.

下面证明选取集合族 SF 和群组测试 GA 之间存在密切的关联.

定理 1　通过 $(n,r+1)-\mathrm{SF}$,可以构造一个 $(n,r)-\mathrm{GA}$;通过 $(n,r)-\mathrm{GA}$,可以构造一个 $(n,r+1)-\mathrm{SF}$.

证明　如果 $\mathcal{F}$ 为 $(n,r+1)-\mathrm{SF}$,意味着当 $x\in\boldsymbol{A}$ 时, $\exists\boldsymbol{B}\in\mathcal{F}$,使得 $\boldsymbol{A}\cap\boldsymbol{B}=\{\sigma\}$. 此时,令 $\boldsymbol{A}'=\boldsymbol{A}-\{\sigma\}$, $|\boldsymbol{A}'|=r$,则对于 $\sigma\notin\boldsymbol{A}'$, $\boldsymbol{B}\in\mathcal{F}$,且 $\boldsymbol{A}'\cap\boldsymbol{B}=\varnothing$,因此 $\mathcal{F}$ 为 $(n,r)-\mathrm{GA}$.

如果 $\mathcal{F}$ 为 $(n,r)-\mathrm{GA}$,意味着当 $\sigma\notin\boldsymbol{A}$, $|\boldsymbol{A}|=r$ 时, $\exists\boldsymbol{B}\in\mathcal{F}$,使得 $\sigma\in\boldsymbol{B}$ 且 $\boldsymbol{A}\cap\boldsymbol{B}=\varnothing$. 此时,令 $\boldsymbol{A}''=\boldsymbol{A}\cup\{\sigma\}$, $|\boldsymbol{A}''|=r+1$,则 $\sigma\in\boldsymbol{A}''$, $\boldsymbol{B}\in\mathcal{F}$, $\boldsymbol{A}''\cap\boldsymbol{B}=\{\sigma\}$,因此 $\mathcal{F}$ 为 $(n,r+1)-\mathrm{SF}$.　**证毕**

由定理 1 可知,只需通过 SF 便可以构造 GA,下面将给出 SF 的构造方法.

在数字通信系统中纠错码(Error Correction Codes, ECC)是进行差错控制的有效方法,利用添加冗余的方法对信息进行编码,以便于信息传输过程中发生错误时能够及时被发现,并得到纠正. 码长为 m,信息位数为 k,汉明距离为 d 的 q 元 ECC,记作 $(m,k,d)_q-\mathrm{ECC}$. 下面通过 ECC 来构造 SF,如算法 1 所示.

假设 $\mathcal{C}=\{c_1,\cdots,c_n\}$ 是 $(m,k,d)_q$ 的纠错码, $\mathcal{C}$ 对应的 SF 为 $\mathcal{F}(\mathcal{C})$,其中的元素为 $\boldsymbol{f}_{ij}=\{k\mid c_k[i]=j\}$, $i\in[m]$, $j\in[q]$, $k\in\{1,2,\cdots,n\}$, $n=q^k$.

算法 1　$\mathcal{F}(\mathcal{C})$ 的构造算法

```
输入:C = {c_1,…,c_n}
输出:F(C)
定义 F 为 m 行 q 列的矩阵;
for i ∈[m]
   for j ∈[q]
      for k ∈{1,2,…,n}
         if c_k[i] = =j
            将 k 加入 F(i,j);
         end if
      end
   end
end
```

下面证明算法 1 得到的 $\mathcal{F}$ 为 $(n,r)-\mathrm{SF}$.

定理 2　$\mathcal{C}=\{c_1,\cdots,c_n\}$ 是 $(m,k,d)_q$ 的纠错码,当 $m<q^{k-1}$ 时,由算法 1 得到的 $\mathcal{F}(\mathcal{C})$ 为 $(q^k,r)-\mathrm{SF}$.

证明　分组的个数小于节点的总数 $mq<q^k$,即 $m<q^{k-1}$. 令 $r=\left\lceil\frac{m}{m-d}\right\rceil$, $\forall k_1,\cdots,k_r\in\{1,2,\cdots,n\}$,我们证明集合 $\boldsymbol{K}=\{k_1,\cdots,k_r\}$ 是能被 $\mathcal{F}(\mathcal{C})$ 选取的,也就是 $\boldsymbol{K}$ 中的任何元素能被 $\mathcal{F}(\mathcal{C})$ 选取,因此,我们不妨证明 k_1 能被 $\mathcal{F}(\mathcal{C})$ 选取,即 $\exists\boldsymbol{B}\in\mathcal{F}(\mathcal{C})$,使得 $\boldsymbol{K}\cap\boldsymbol{B}=\{k_1\}$. 对于任意的 $j\neq1$,由于纠错码 $\mathcal{C}$ 的汉明距离为 d,满足 $c_{k_j}[i]=c_{k_1}[i]$ 的编码位置 i 最多为 $m-d$,则 $c_{k_1}[i]\in\{c_{k_2}[i],\cdots,c_{k_r}[i]\}$ 的编码位置 i 最多为 $(r-1)(m-d)<m$. 因此, $\exists i'\in[m]$,使得 $c_{k_1}[i']\notin\{c_{k_2}[i'],\cdots,$

$c_{k_1}[i']\}$,也即 $\exists \boldsymbol{f}_{i'j} \in \mathcal{F}(\mathcal{C})$,$\boldsymbol{f}_{i'j}=\{k \mid c_k[i']=c_{k_1}[i']\}$,使得 $k_1 \in \boldsymbol{f}_{i'j}$,而 $k_j \notin \boldsymbol{f}_{i'j}, j=2,\cdots,r$. 令 $\boldsymbol{B}=\boldsymbol{f}_{i'j}$,则 $\boldsymbol{K}\cap\boldsymbol{B}=\{i_1\}$,$\mathcal{F}(\mathcal{C})$为$(q^k,r)-\mathrm{SF}$. **证毕**

如二进制线性分组码$(7,4)$:$\mathcal{C}=\{0000000,1000101,0100111,0010110,0001011,1100010,1010011,1001110,0110001,0101100,0011101,1110100,1101001,1011000,0111010,1111111\}$,根据算法可以得到$(16,2)-\mathrm{SF}$:

$\mathcal{F}(\mathcal{C})=\{$

$\{1,3,4,5,9,10,11,15\}$ $\{2,6,7,8,12,13,14,16\}$

$\{1,2,4,5,7,8,11,14\}$ $\{3,6,9,10,12,13,15,16\}$

$\{1,2,3,5,6,8,10,13\}$ $\{4,7,9,11,12,14,15,16\}$

$\{1,2,3,4,6,7,9,12\}$ $\{5,8,10,11,13,14,15,16\}$

$\{1,5,6,7,9,13,14,15\}$ $\{2,3,4,8,10,11,12,16\}$

$\{1,2,9,10,11,12,13,14\}$ $\{3,4,5,6,7,8,15,16\}$

$\{1,4,6,8,10,12,14,15\}$ $\{2,3,5,7,9,11,13,16\}$

$\}$

其对应的关联矩阵 $\boldsymbol{M}$ 为

$$\begin{bmatrix}
1&0&1&1&1&0&0&0&1&1&1&0&0&0&1&0\\
0&1&0&0&0&1&1&1&0&0&0&1&1&0&1&1\\
1&1&0&1&1&0&1&1&0&0&1&0&0&1&0&0\\
0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1\\
1&1&1&0&1&1&0&1&0&1&0&0&1&0&0&0\\
0&0&0&1&0&0&1&0&1&0&1&1&0&1&1&1\\
1&1&1&1&0&1&1&0&1&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
1&0&0&0&1&1&1&0&1&0&0&0&1&1&1&0\\
0&1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
1&1&0&0&0&0&0&0&1&1&1&1&1&1&0&0\\
0&0&1&1&1&1&1&1&0&0&0&0&0&0&1&1\\
1&0&0&1&0&1&0&1&0&1&0&1&0&1&1&0\\
0&1&1&0&1&0&1&0&1&0&1&0&1&0&0&1
\end{bmatrix}$$

3.2 群组认证的实施

按照分组方案,对认证节点的签名进行分组检验,所得结果为

$$\boldsymbol{y}=\begin{bmatrix}y_1\\ \vdots\\ y_t\end{bmatrix}=\boldsymbol{M}\odot\boldsymbol{x}\overset{\mathrm{def}}{=\!=}\begin{bmatrix}\boldsymbol{M}_1.\odot\boldsymbol{x}\\ \vdots\\ \mathrm{M}_t.\odot\boldsymbol{x}\end{bmatrix}=\begin{bmatrix}\vee_{j=1}^{n}(m_{1j}\wedge x_j)\\ \vdots\\ \vee_{j=1}^{n}(m_{tj}\wedge x_j)\end{bmatrix} \tag{4}$$

其中$\odot$表示一种特殊的向量运算,$\vee$表示“或”运算,$\wedge$表示“与”运算.

3.3 非法节点的标定

非法节点的标定,即通过式(4)中的 $\boldsymbol{y}$ 得到 $\boldsymbol{x}$,基本思路是首先对每个分组进行验证,由验证结果确定合法节点,利用算法 2 的排除算法,即不是合法节点便认定为可疑非法节点,然后对可疑非法节点集合进行进一步筛选,最终完成对非法节点的标定.

算法 2 利用排除法确定非法节点

输入:$\boldsymbol{y}=[y_1 \ \cdots \ y_t \ \bar{y}_1 \ \cdots \ \bar{y}_t]^{\mathrm{T}}$
输出:$\hat{\boldsymbol{K}}$
for $y_i \in \boldsymbol{y}$
  if $y_i == 0$
    for $j \in [n]$
      if $m_{ij} == 1$
        $\hat{\boldsymbol{S}}=\hat{\boldsymbol{S}}\cup X_j$
      end if
    end
  end if
end
$\hat{\boldsymbol{K}}:=\bar{\hat{\boldsymbol{S}}}$

显然 $\hat{\boldsymbol{S}}\subseteq\boldsymbol{S}$,即 $\boldsymbol{K}\subseteq\hat{\boldsymbol{K}}$,为进一步确定非法节点集合 $\hat{\boldsymbol{K}}$,采用迭代方式进行判断,首先在关联矩阵 $\boldsymbol{M}$ 中去掉合法节点所在列,记为 $\boldsymbol{M}'$,由于去除的是合法节点,不会改变分组认证结果,即 $\boldsymbol{M}'$ 所对应的检测结果仍为 $\boldsymbol{y}=[y_1 \ \cdots \ y_t]^{\mathrm{T}}$.

构造一个矩阵

$$\begin{aligned}\boldsymbol{U}&=[\boldsymbol{U}_1 \ \ \bar{\boldsymbol{U}}_1 \ \ \boldsymbol{U}_2 \ \ \bar{\boldsymbol{U}}_2]^{\mathrm{T}}\\&=\begin{bmatrix}b_1&b_2&\cdots&b_{n-1}&b_n\\ \bar{b}_1&\bar{b}_2&\cdots&\bar{b}_{n-1}&\bar{b}_n\\ b_{i_1}&b_{i_2}&\cdots&b_{i_{n-1}}&b_{i_n}\\ \bar{b}_{i_1}&\bar{b}_{i_2}&\cdots&\bar{b}_{i_{n-1}}&\bar{b}_{i_n}\end{bmatrix}\\&=[\boldsymbol{u}_1 \ \ \boldsymbol{u}_2 \ \ \cdots \ \ \boldsymbol{u}_{n-1} \ \ \boldsymbol{u}_n]\end{aligned} \tag{5}$$

其中 $b_i(i\in[n])$ 为整数 $i-1$ 的 L 比特长度二进制表示,$L=\lceil\log_2 n\rceil$,$\bar{b}_i$ 表示 b_i 的非,序列$(i_1,i_2,\cdots,i_n)$是来自$[n]$的随机排列,则

$$\boldsymbol{z}\overset{\mathrm{def}}{=\!=}\boldsymbol{y}\otimes\boldsymbol{U}=[z_1 \ \cdots \ z_t] \tag{6}$$

$$\boldsymbol{z}_k=\boldsymbol{y}\odot[\boldsymbol{u}_1 \ \ \boldsymbol{u}_2 \ \ \cdots \ \ \boldsymbol{u}_{n-1} \ \ \boldsymbol{u}_n]\overset{\mathrm{def}}{=\!=}\begin{bmatrix}z_k^1\\ z_k^2\\ z_k^3\\ z_k^4\end{bmatrix} \tag{7}$$

其中 $k=1,\cdots,t$. z_k^1、z_k^2、z_k^3 和 z_k^4 为长度为 L 的向量,显然,如果分组中仅含有一个非法节点,则 $\boldsymbol{z}_k(k=1,\cdots,t)$ 的汉明重量为 $2L$,因此,通过判断 $\boldsymbol{z}_k$ 的汉明重量,可以确定仅含有一个非法节点的分组,取其前 L 个比特,换算成十进制,便可以确定这个非法节点. 仅含有 1 个非法节点的分组被确定后,可以进一步确定是否含有 2 个非法节点. 设 $\boldsymbol{u}_{l_0}$ 被确定为一个非法向量,另一个 $\boldsymbol{u}_{l_1}$ 被认为是可疑对象,则

$$\begin{bmatrix}z_k^1\\ z_k^2\end{bmatrix}=\boldsymbol{u}_{l_0}\vee\boldsymbol{u}_{l_1}=\begin{bmatrix}b_{l_0}\vee b_{l_1}\\ \overline{b_{l_0}}\vee\overline{b_{l_1}}\end{bmatrix} \tag{8}$$

通过下面步骤确定 b_{l_1},如果 $b_{l_0,1}=0$,则 $b_{l_1,1}=z_{k,1}^1$,否则 $b_{l_1,1}=\overline{z_{k,1}^2}$,这样便可以确定 b_{l_1},同理可以由 z_k^3 和 z_k^4 确定另外一个数 l_2,当 $i_{l_1}=l_2$ 时,则可以确定 b_{l_1} 为非法节点,否则,说明 b_{l_1} 为非法节点的假设错误,应进行重新假定.

例如,若 $\boldsymbol{u}_1$ 为非法节点,假设与 $\boldsymbol{u}_1$ 处于第 k 个分组的 $\boldsymbol{u}_2$ 为非法节点,则

$$\boldsymbol{z}_k=\begin{bmatrix}z_k^1\\z_k^2\\z_k^3\\z_k^4\end{bmatrix}=\begin{bmatrix}b_1\\\bar{b}_1\\b_{i_1}\\\bar{b}_{i_1}\end{bmatrix}\vee\begin{bmatrix}b_2\\\bar{b}_2\\b_{i_2}\\\bar{b}_{i_2}\end{bmatrix}=\begin{bmatrix}b_1\vee b_2\\\bar{b}_1\vee\bar{b}_2\\b_{i_1}\vee b_{i_2}\\\bar{b}_{i_1}\vee\bar{b}_{i_2}\end{bmatrix}\tag{9}$$

如果 $b_{11}=0$,则 $\hat{b}_{21}=z_{k1}^1$;否则 $\hat{b}_{21}=\overline{z_{k1}^2}$. 类似地,可以得到 $\hat{\boldsymbol{u}}_2$ 的其余比特,若 $\hat{\boldsymbol{u}}_2=\boldsymbol{u}_2$,则证明假设成立;否则,假设错误,对其进行改变,再进行检验,直到确定,像这样经过多次迭代,便可以将非法节点的集合确定下来.

定理 3　在上述方案中,发生错误判决的概率不超过 $1/n$.

证明　在上述算法中,当某个 $\boldsymbol{u}_i$ 的 z_k^1 和 z_k^2 不属于假设的分组中,但却能通过 z_k^3 和 z_k^4 的验证 $i_{l_1}=l_2$,即做出错误判决,而 i_{l_1} 的取值独立,因此,做出错误判决的概率为 $1/n$.　**证毕**

3.4　举例

假设要对 8 个入网节点进行群组认证,其中有 3 个非法节点,分别是第 1、3 和 8 个节点,即 $\boldsymbol{x}=(1\ 0\ 1\ 0\ 0\ 0\ 0\ 1)$. 此时,$n=8$,$r=3$,$L=\log_2 n=3$,有

$$\boldsymbol{M}=\begin{bmatrix}0&1&0&1&1&0&1&0\\1&0&1&1&0&1&0&0\\0&1&0&0&0&1&1&0\\0&1&1&0&1&0&0&1\end{bmatrix}\tag{10}$$

即对 8 个节点的签名进行认证时,将其分为 4 个组:{2,4,5,7}、{1,3,4,6}、{1,2,6,7}和{2,3,5,8}.

此时

$$\boldsymbol{U}=\left[\begin{array}{cccccccc}0&0&0&0&1&1&1&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\\\hline1&1&1&1&0&0&0&0\\1&1&0&0&1&1&0&0\\1&0&1&0&1&0&1&0\\\hline1&0&0&1&1&0&0&1\\0&0&1&1&1&0&1&0\\0&1&1&1&0&0&0&1\\\hline0&1&1&0&0&1&1&0\\1&1&0&0&0&1&0&1\\1&0&0&0&1&1&1&0\end{array}\right]\tag{11}$$

则

$$\boldsymbol{y}=\boldsymbol{M}\odot\boldsymbol{x}=\begin{bmatrix}0&0&0&0&0&0&0&0\\1&0&1&0&0&0&0&0\\1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&1\end{bmatrix}=\begin{bmatrix}0\\\boldsymbol{u}_1\vee\boldsymbol{u}_3\\\boldsymbol{u}_1\\\boldsymbol{u}_3\vee\boldsymbol{u}_8\end{bmatrix}=\begin{bmatrix}0\\1\\1\\1\end{bmatrix}\tag{12}$$

通过分组检验,可知所有分组中都含有非法节点,但由于 $\boldsymbol{M}$ 满足(8,2)-GA,第 1 个分组检测为合法,可以确定{2,4,5,7}都是合法节点,其余的{1,3,6,8}不能确定.

因此

$$\boldsymbol{z}=\boldsymbol{y}\otimes\boldsymbol{U}=[\boldsymbol{z}_1\quad\cdots\quad\boldsymbol{z}_t]\tag{13}$$

其中

$$\boldsymbol{z}_1=(000000000000)^{\mathrm{T}}$$
$$\boldsymbol{z}_2=(010111111111)^{\mathrm{T}}$$
$$\boldsymbol{z}_3=(000111100011)^{\mathrm{T}}$$
$$\boldsymbol{z}_4=(111101111110)^{\mathrm{T}}$$

计算 $\boldsymbol{z}_1$、$\boldsymbol{z}_2$、$\boldsymbol{z}_3$ 和 $\boldsymbol{z}_4$ 的汉明重量,仅有 $\boldsymbol{z}_3$ 的汉明重量为 $2L=6$,因此,第 3 个分组只包括一个非法节点,取 $\boldsymbol{z}_3$ 的前 3 个比特(000),换算成十进制为 0,那么这个非法节点就是第 1 个节点,第 3 个分组除了第一个节点外,其余{2,6,7}都为合法节点,{3,8}不能确定;第 3 个节点包含在第 2、4 个分组,在第 2 个分组中,假设第 3 个节点为非法节点,那么 $\boldsymbol{z}_2=\boldsymbol{u}_1\vee\boldsymbol{u}_3$,而 $b_{11}=b_{12}=b_{13}=0$ 可知,取 $\boldsymbol{z}_2$ 的前 3 个比特,得到(010),换算成十进制结果为 2,则第 3 个节点为非法节点;同理,可以在下一轮确定第 8 个节点也是非法节点.

4　方案分析

上文提出的群组认证方案,即使在有非法节点混入合法节点对群体认证进行干扰时,仍旧可以通过本文算法对非法节点的进行标定,抵抗非法者对群组认证的拒绝服务攻击,下面针对本文提出的群组认证方案,进行可行性证明,并对算法的复杂度和准确性进行分析.

4.1　可行性证明

定理 4　如果关联矩阵对应一个分组测试集合族 $\mathcal{T}$,可以通过算法 2 分组检验确定合法节点,从而确定非法节点.

证明　分组测试时,如果分组中存在非法签名,则此组测试结果必定为 1,不能通过认证. 假设 σ_{j_0} 是一个合法签名,$\boldsymbol{D}$ 是非法签名的集合,则 $\sigma_{j_0}\notin\boldsymbol{D}$,由于关联矩

阵对应一个分组测试集合族 $\mathcal{T}$,可知必然存在 $\boldsymbol{S}\in\mathcal{T}$,使得 $\boldsymbol{\sigma}_{j_0}\in\boldsymbol{S}$ 且 $\boldsymbol{D}\cap\boldsymbol{S}=\varnothing$,因此以 $\boldsymbol{S}$ 所对应的签名作为一组进行检测,结果必定为0,可以确定 $\boldsymbol{\sigma}_{j_0}$ 为合法签名. 这样的过程重复进行 $|\mathcal{T}|$ 次,便能得到合法签名的集合.

证毕

4.2 复杂度分析

定理5 若 n 和 r 是正整数,则根据算法1在时间 $O(rn\ln n)$ 内可以构造 $O(r^2\ln n)$ 大小的 $\mathcal{T}(\mathcal{C})$.

证明 纠错码 $(m,k,d)_q$ 的汉明限为

$$\frac{k}{m}\leq 1-H_q\left(\frac{d}{2n}\right) \tag{14}$$

其中 $n=q^k$,$H_q(x)=-x\log_q x-(1-x)\log_q(1-x)$,则

$$k\leq m\left(1-H_q\left(\frac{d}{2n}\right)\right) \tag{15}$$

则

$$m=\frac{k}{1-H_q\left(\frac{d}{2n}\right)}=O(kr\ln r)=O(r\ln n) \tag{16}$$

所花费的时间为 $O(nm)=O(rn\ln n)$. $\mathcal{T}(\mathcal{C})$ 的元素个数为 $mq=O(r^2\ln n)$. **证毕**

4.3 准确性分析

算法2给出的 $\boldsymbol{S}$ 可能会将某些合法的节点错误地判断为非法节点. 在图1的例子中,合法节点包括第2、3、5和7个节点,然而利用关联矩阵进行的检测得到的结果 $\boldsymbol{y}=(1,1,0,1,0)$ 表明第3、5和7个节点合法,却不能证明第2个节点合法,按照算法2得到的合法节点的集合,可能会犯"弃真"错误. 相反地,在利用迭代算法确定非法签名时,可能会将某些非法节点漏掉,错误地判定为合法节点. 图1中的第4个节点为非法节点,由于 $y_4=1$,而第4分组中包含的第4、8个节点为非法节点,难以确定第4个节点是否合法,可能会犯"取伪"错误.

$$\begin{array}{c} \begin{array}{cccccccc} x_1 & \boxed{x_2} & \underline{x}_3 & \boxed{x_4} & \underline{x}_5 & x_6 & \underline{x}_7 & x_8 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \\ \boldsymbol{M}=\begin{array}{|cccccccc|c|c} \hline 1&0&0&0&0&0&0&1&1&y_1\\ 1&1&0&0&0&0&1&0&1&y_2\\ 0&0&1&0&1&0&1&0&0&y_3\\ 0&1&0&1&1&0&0&1&1&y_4\\ 0&0&0&0&0&0&1&0&0&y_5\\ \hline \end{array} \end{array}$$

图1 群组认证的举例

定理6 经过 $4LrC(\varepsilon)$,即 $4rC(\varepsilon)\log n$ 次检测,本文方案能以概率 $1-O(r/n)$ 确定至少 $(1-\varepsilon)r$ 个非法节点,其中 ε 为任意大于0的正整数,$C(\varepsilon)$ 和 ε 的对应关系如表2所示.

表2 $C(\varepsilon)$ 和 ε 的对应关系表

ε	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}	10^{-9}	10^{-10}
C	5	6.7	8.3	9.2	10.8	12.3	13.3
d	6	8	10	11	13	15	16

证明 首先将需要认证的节点进行分组,每个分组中含有若干节点,假设共有 t 个分组,n 个需要认证的节点,当 $t=5$,$n=13$ 时,其对应关系如图2所示,如分组 $\boldsymbol{B}_1$ 中包含节点 $\{X_1,X_4,X_7,X_{13}\}$. 假设 n 个节点中包括 r 个非法节点,在群组认证进行分组时,每个节点平均出现在 d 个分组中,每个分组中平均含有 dr/t 个非法节点,即分组节点的度为 $\lambda=dr/t$,则分组节点的度是个随机变量,接近参数为 λ 的泊松分布,度分布函数为

$$\rho(x)=\sum_{i=1}^{\infty}\rho_i x^{i-1} \tag{17}$$

其中 $\rho_i=\frac{i}{\lambda}P\{\text{节点度为}\ i\}=\frac{i}{\lambda}e^{-\lambda}\frac{\lambda^i}{i!}=e^{-\lambda}\frac{\lambda^{i-1}}{(i-1)!}$,

那么

$$\rho(x)=e^{-\lambda(1-\lambda)} \tag{18}$$

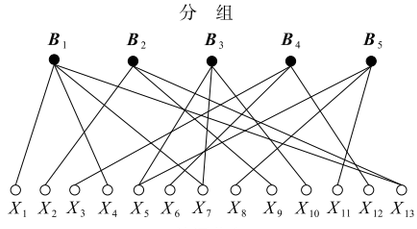

图2 认证节点的分组情况

在3.3节的每一轮迭代过程中,D_1 表示分组中仅含有一个非法节点,D_2 表示分组中包含两个非法节点,P_j 表示在第 j 轮迭代后仍有非法节点不能确定的概率. 在第 $j+1$ 轮迭代中,D_1 和 D_2 被确定的概率为 $\rho_1+\rho_2(1-P_j)$,其中 $\rho_1=e^{-\lambda}$,$\rho_2=\lambda e^{-\lambda}$,因此

$$P_{j+1}=[1-\rho_1-\rho_2(1-P_j)]^{d-1} \tag{19}$$

令 $\varepsilon=\lim_{j\to\infty}P_j$,则

$$\varepsilon\approx(1-\rho_1-\rho_2)^{d-1}=(1-e^{-\lambda}-\lambda e^{-\lambda})^{d-1} \tag{20}$$

如图3所示,当 $\lambda=1.2$,$d=16$ 时,以

$$\gamma(P)=[1-\rho_1-\rho_2(1-P)]^{d-1} \tag{21}$$

为迭代公式,从 $P_1=1$ 开始,即从 (P_1,P_1) 划条竖线,经过一次迭代到达 $(P_1,\gamma(P_1))=(P_1,P_2)$,再从 (P_1,P_2) 划条横线,到达 (P_2,P_2),经过第二次迭代到达 $(P_2,\gamma(P_2))=(P_2,P_3)$,如此继续下去,直到 $\gamma(P_j)$ 收敛到 $\varepsilon=(1-e^{-\lambda}-\lambda e^{-\lambda})^{d-1}\approx 10^{-10}$. 分析可知,$\lambda$ 和 d 是 ε 的函数,以检验次数最少作为目标函数构造模型如下

$$\begin{aligned}&\min\ t=\frac{rd}{\lambda}\\ &\text{s.t.}\quad (d-1)\log(1-e^{-\lambda}-\lambda e^{-\lambda})=\log\varepsilon\end{aligned} \tag{22}$$

若上述模型的最优解为 $\lambda^*(\varepsilon)$ 和 $d^*(\varepsilon)$,令 $C(\varepsilon)=\frac{t}{r}=\frac{d^*}{\lambda^*}$,则 $t_{\min}=C(\varepsilon)r$. 每个分组包括 $4L$ 次检验,则 t 个分组共需要进行 $4LrC(\varepsilon)$ 次检验. $\varepsilon=\lim_{j\to\infty}P_j$ 表示经

过数轮迭代后仍有非法节点不能确定的概率,则 $4LrC(\varepsilon)$ 次检验确定 $(1-\varepsilon)r$ 个非法节点. 由定理 3 得知,每个非法节点的确定,产生误判的概率为 $1/n$,则在 $O(r)$ 次检验中,产生误判的概率为 $O(r/n)$,当 $n\to\infty$ 时,误判的概率趋于 0.

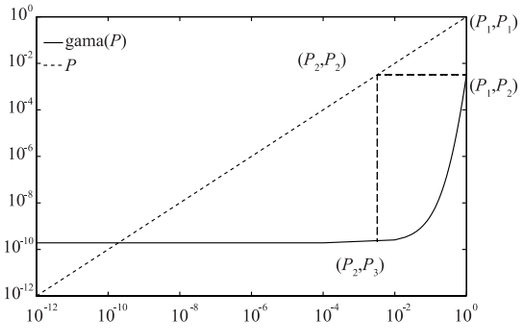

图3　迭代演化过程中$\gamma(P)$与P关系图

5　结论及下一步工作

为了在群组认证中抵抗拒绝服务攻击,并标定非法者,本文基于纠错码理论提出了一种群组认证方案. 该方案以分组组合检测理论为指导,通过合理的分组设计,包含有 r 个非法节点的 $n(r\ll n)$ 个节点的群组认证方案的时间复杂度为 $O(rn\ln n)$,能在 $4rC(\varepsilon)\log_2 n$ 次检测后以概率 $1-O(r/n)$ 确定 $(1-\varepsilon)r$ 个非法节点. 关于群组认证还有许多开放性问题[13,14,22],下一步将研究基于纠错码理论的群组认证次数的优化问题.

参考文献

[1] 李中献,詹榜华,杨义先. 认证理论与技术的发展[J]. 电子学报,1999,27(1):98 – 102.
LI Zhong-xian, ZHAN Bang-hua, YANG Yi-xian. A survey of identification and authentication[J]. Acta Electronica Sinica, 1999, 27(1): 98 – 102. (in Chinese)

[2] 刘冬,陈晶,杜瑞颖,等. 基于情景感知的低交互移动双因素认证系统[J]. 电子学报,2018,46(5):1056 – 1061.
LIU Dong, CHEN Jing, DU Rui-ying, et al. A low interaction mobile two-factor authentication system based on context awareness[J]. Acta Electronica Sinica, 2018, 46(5): 1056 – 1061. (in Chinese)

[3] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[J]. Advances in Cryptology-Eurocrypt, 2003, 2656(1): 416 – 432.

[4] YANAI N. On the tightness of deterministic identity-based signatures[A]. Proceedings of the Fourth International Symposium on Computing and Networking[C]. Hiroshima, Japan: IEEE, 2017. 168 – 173.

[5] 张玉磊,周冬瑞,李臣意,等. 高效的无证书广义指定验证者聚合签名方案[J]. 通信学报,2015,36(2):48 – 55.
ZHANG Yulei, ZHOU Dongrui, LI Chenyi, et al. Certificateless-based efficient aggregate signature scheme with universal designated verifier[J]. Journal on Communications, 2015, 36(2): 48 – 55. (in Chinese)

[6] PASTUSZAK J, MICHATEK D, PIEPRZYK J, et al. Identification of bad signatures in batches[A]. Proceedings of the International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography[C]. Imai: Springer-Verlag, 2000. 28 – 45.

[7] 李顺东,王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报,2013,41(4):798 – 803.
LI Shun-dong, WANG Dao-shun. Efficient secure multiparty computation based on homomorphic encryption[J]. Acta Electronica Sinica, 2013, 41(4): 798 – 803. (in Chinese)

[8] GENTRY C, RAMZAN Z. Identity-based aggregate signatures[A]. Proceedings of the International Conference on Theory and Practice of Public-Key Cryptography[C]. New York: Springer-Verlag, 2006. 257 – 273.

[9] SHEN Li-min, MA Jian-feng, LIU Xi-meng, et al. A secure and efficient ID-based aggregate signature scheme for wireless sensor networks[J]. IEEE Internet of Things Journal, 2017, 4(2): 546 – 553.

[10] IWASAKI T, YANAI N, INAMURA M, et al. Tightly-secure identity-based structured aggregate signature scheme under the computational Diffie-Hellman assumption[A]. Proceedings of the International Conference on Advanced Information Networking and Applications[C]. Crans-Montana, Switzerland: IEEE, 2016. 669 – 676.

[11] 庞辽军. 秘密共享技术及其应用研究[D]. 西安:西安电子科技大学,2006. 116 – 130.
PANG Liao-jun. Secret Sharing Technology and Its Applications[D]. Xi'an Shannxi: Xidian University, 2006. 116 – 130. (in Chinese)

[12] HARN L. Group authentication[J]. IEEE Transactions on Computers, 2013, 62(9): 1893 – 1898.

[13] LI S, DOH I, CHAE K. A group authentication scheme based on Lagrange interpolation polynomial[A]. Proceedings of the International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing[C]. Blumenau, Brazil: IEEE, 2016. 386 – 391.

[14] MIAO F, JIANG H, JI Y, et al. Asynchronous group authentication[J]. Chinese Journal of Electronics, 2017, 26(4): 820 – 826.

[15] 季洋洋,苗付友,蒋辉文. 简单的异步(t,m,n)组认证方案[J]. 计算机工程与应用,2016,52(15):8 – 12.
JI Yang-yang, MIAO Fu-you, JIANG Hui-wen. Simple asynchronous (t,m,n) group authentication[J]. Computer Engineering and Applications, 2016, 52(15): 8 – 12. (in

Chinese)
[16] LIU Qiang, YIN Jian-ping, LEUNG V C M, et al. FADE: forwarding assessment based detection of collaborative grey hole attacks in WMNs [J]. IEEE Transactions on Wireless Communications, 2013, 12(10): 5124 – 5136.
[17] PASTUSZAK J, PIEPRZYK J, SEBERRY, J. Codes identifying bad signatures in batches [J]. Lecture Notes in Computer Science, 2000, 1977: 143 – 154.
[18] ZAVERUCHA G M, STINSON D R. Group testing and batch verification [A]. Proceedings of the International Conference on Information Theoretic Security LNCS5973 [C]. Berlin, Germany: Springer-Verlag, 2009. 140 – 157.
[19] DU D, HWANG F K, HWANG F. Combinatorial Group Testing and Its Applications [M]. [S. L.]: World Scientific, 2000.
[20] PASTUSZAK J, MICHALEK D, PIEPRZYK J, et al. Identification of bad signatures in batches [A]. Proceedings of the International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography [C]. Imai: Springer, Heidelberg, 2000. 28 – 45.
[21] CHEN J, YUAN Q, XUE G, et al. Game-theory-based batch identification of invalid signatures in wireless mobile networks [A]. Proceedings of the IEEE Conference on Computer Communications [C]. Washington DC, USA: IEEE Computer Society, 2015. 262 – 270.
[22] ALDRIDGE M, BALDASSINI L, JOHNSON O. Group testing algorithms: bounds and simulation [J]. IEEE Transactions on Information Theory, 2013, 59(6): 7 – 16.
[23] CHAN C L, JAGGI S, SALIGRAMA V, et al. Non-adaptive group testing: explicit bonds and novel algorithms [A]. Proceedings of the IEEE International Symposium on Information Theory [C]. Cambridge, MA, USA: IEEE, 2012. 1837 – 1841.
[24] SHANGGUAN C, GE G. New bounds on the number of tests for disjunct matrices [J]. IEEE Transactions on Information Theory, 2016, 62(12): 7518 – 7521.
[25] LEE K, PEDARSANI R, RAMCHANDRAN K. Saffron: a fast, efficient, and robust framework for group testing based on sparse-graph codes [A]. Proceedings of the IEEE International Symposium on Information Theory [C]. Barcelona, Spain: IEEE, 2016. 2873 – 2877.
[26] BUI T V, KURIBAYASHI M, ECHIZEN I. Non-adaptive group testing framework based on concatenation code [J]. IEEE Transactions on Information Theory, 2017, 63(5): 1 – 12.
[27] BUI T V, KOJIMA T, KURIBAYASHI M, et al. Efficient (nonrandom) construction and decoding of non-adaptive group testing [J]. IEEE Transactions on Information Theory, 2018, 64(11): 1 – 15.
[28] PORAT E, ROTHSCHILD A. Explicit Non-Adaptive Combinatorial Group Testing Schemes [M]. Germany: Springer Berlin Heidelberg, 2008. 7982 – 7989.

作者简介

王 宏 男, 1979 年 9 月出生, 陕西澄城人. 讲师、博士研究生, 研究方向为信息安全、装备作战使用与保障.
E-mail: whongger2017@163.com

李建华 男, 1965 年 10 月出生, 陕西白水人. 博士、教授、博士生导师, 研究方向为装备作战使用与保障.
E-mail: kgdljh@163.com