基于Ad hoc网络的联合有效用户识别与信道安全编译码方法

张克楠 涂国防* 张 灿 陈德元
(中国科学院大学电子电气与通信工程学院 北京 100049)

摘 要：Ad hoc网络是一种无中心的自组织网络，由于用户能量受限当信噪比较低时有效用户识别的可靠性和信道安全性下降。该文针对这个问题提出一种联合有效用户识别与信道安全编译码方法。将发送用户的正交地址码与接收用户的伪随机地址码异或产生基于发送用户与接收用户的有效用户识别码。为提高信道安全性以信道安全码作为密钥加密有效用户识别码得到正交随机安全序列。为实现扩频并提高传输效率将发送数据以6 bit信息作为一个符号进行分组，将每个符号与一个正交随机安全序列对应。接收用户采用基于子空间的方法处理接收信号，通过建立判决模型识别有效用户。实验结果表明该方法与已有方法相比，当有效用户识别的漏警概率为10^{-3}时信噪比增益改善1.6 dB。

关键词：Ad hoc网络；联合编译码方法；有效用户识别；信道安全
中图分类号：TN918.91 **文献标识码**：A **文章编号**：1009-5896(2021)02-0380-08
DOI: 10.11999/JEIT190644

Joint Virtual User Identification and Channel Security En/Decoding Method for Ad hoc Networks

ZHANG Kenan TU Guofang ZHANG Can CHEN Deyuan
(*School of Electronic, Electrical and Communication Engineering, University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: Ad hoc network is a kind of self-organized network without center. The reliability of virtual user identification and channel security are reduced when SNR is low due to user energy limitation. In order to solve this problem, a joint virtual user identification and channel security en/decoding method is proposed in this paper. Transmitter-receiver-based virtual user identification code is generated by xoring the orthogonal address code of transmitter with the pseudo random address code of receiver and encrypted with channel security code as key to acquire orthogonal random secure sequence so as to improve channel security. In order to realize spread spectrum as well as improve transmission efficiency, transmitted data is divided into 6-bit symbols, each symbol is mapped with an orthogonal random secure sequence. Receivers adopt subspace-based method to process received data and establish a judgment model to identify virtual users. Simulation results indicate that the proposed method obtains 1.6 dB E_b/N_0 gains compared with existing methods when miss alarm rate of virtual user identification is 10^{-3}.

Key words: Ad hoc networks; Joint en/decoding method; Virtual user identification; Channel security

1 引言

Ad hoc网络是一种由电池供电的分布式自组织无线网络。用户能量受限引起了有效用户识别的可靠性和信道安全性问题。研究人员已经提出了许多有效用户识别方法。文献[1]使用基于发送用户的扩频码对数据包扩频，接收用户首先识别出活动用户，然后从数据包头部提取接收用户地址信息判断有效用户。该方法能耗较大同时安全性较弱。针对这个问题文献[2]构造了一种基于发送用户和接收用户的正交伪随机扩频码。通过使用该码字对数据包扩频，接收用户不需要从数据包头部提取接收用户地址信息就可以识别出有效用户从而降低能耗。但是当网络超负荷即用户数大于扩频码长度时该方法性能下降。为此文献[3]设计了一种适用于超负荷网络的扩频码，采用最大似然译码方法即可识别出有

收稿日期：2019-08-27；改回日期：2020-03-02；网络出版：2020-12-09
*通信作者： 涂国防 gft@ucas.ac.cn
基金项目：国家自然科学基金(61571416, 61271282)，中国科学院奖励基金(Y82901EA1)
Foundation Items: The National Natural Science Foundation of China (61571416, 61271282), The Award Foundation of Chinese Academy of Sciences (Y82901EA1)

效用户。以上方法都是从扩频码构造的角度进行设计的，文献[4]提出一种基于随机集理论的方法，该方法虽然具有良好的性能，但是复杂度较高。针对这个问题文献[5]采用树搜索技术降低复杂度。与基于随机集理论的方法不同，文献[6]基于传统的概率论理论提出一种类似于维特比算法的幸存路径处理方法和两种基于粒子滤波的方法识别有效用户。与上述基于概率论的方法不同，文献[7]提出一种基于代数理论的确定性方法，通过设计一种具有良好互相关特性的协议序列使得用户仅根据信道活动信息就可以在一定延迟内识别出有效用户。文献[8]从协议设计的角度出发提出一种跨层方法，将媒体访问控制(Media Access Control, MAC)层SEEDEX协议[9]中的伪随机调度表用于物理层的有效用户识别。文献[10–12]针对5G应用场景大规模物联网(massive Machine Type of Communication, mMTC)中存在的有效用户识别问题开展研究。文献[10]提出一种基于压缩感知的方法识别有效用户。文献[11]在基于压缩感知方法的基础上引入期望传播算法降低有效用户识别的误判概率。文献[12]提出一种基于深度神经网络的有效用户识别方法，与基于压缩感知的方法相比有效降低了用户识别的误判概率。文献[13]与文献[14]针对5G非正交多址接入系统中存在的有效用户识别问题基于消息传递算法分别提出两种改进算法。文献[13]提出一种基于概率密度函数值门限判决的部分码字搜索消息传递算法，文献[14]在消息传递算法的基础上增加了对用户节点稳定性必要条件的判决。与原始消息传递算法相比两种改进算法有效降低了用户识别的误判概率。

以上介绍的方法均存在低信噪比情况下有效用户识别误判概率较高且没有考虑信道安全的问题。本文提出一种联合有效用户识别与信道安全编译码方法。发送用户产生基于发送用户与接收用户的有效用户识别码，为提高信道安全性以信道安全码作为密钥加密有效用户识别码得到正交随机安全序列，为实现扩频并提高传输效率将发送数据以6 bit为一个符号进行分组，将每个符号与一个正交随机安全序列对应。接收用户采用基于子空间的方法处理接收信号并建立判决模型识别有效用户。仿真结果表明该方法降低了有效用户识别的误判概率。

2　基于Ad hoc网络的联合编码方法

2.1　发送用户地址码和接收用户地址码

由于Ad hoc网络是分布式自组织网络，用户不经过中心节点相互之间直接通信。因此为实现有效用户识别给每个用户分配两个码字w和p，w称为发送用户地址码，p称为接收用户地址码。假设Ad hoc网络中用户不超过64个，选用长度为64 bit的沃尔什码作为发送用户地址码和长度为64 bit的M序列作为接收用户地址码。长度为64 bit的沃尔什码和M序列各有64个如表1和表2所示。表1和表2是存储在每个用户物理层的沃尔什码表和M序列表。沃尔什码表由哈达玛矩阵的行构成，M序列表由相同的生成多项式和不同的初始状态产生。

给每个用户编号，以用户编号作为表1和表2的索引。假设用户1给用户2发送数据，以用户1的编号查表1得到发送用户地址码w_1，以用户2的编号查表2得到接收用户地址码p_2，将w_1与p_2异或生成有效用户识别码v_{12}如式(1)所示，v_{12}的长度也是64 bit。v_{12}中包含用户2的接收用户地址码p_2从而避免用户2的地址信息在信道中传输，增强了用户2地址码的信道安全性；同时避免用户2从数据包头部提取接收用户地址信息识别有效用户，降低了用户2的能耗。

表 1　沃尔什码表

编号	沃尔什码
1	0110100110010110100101100110100110010110011010010110100110010110
2	0011001111001100110011000011001111001100001100110011001111001100
⋮	⋮
64	0110011001100110011001100110011001100110011001100110011001100110

表 2　M序列表

编号	M序列
1	1101111110101110001100111011000000111100100101010011010000100010
2	1011111101011100011001110110000001111001001010100110100001000101
⋮	⋮
64	0101101111110101110001100111011000000111100100101010011010000100

$$v_{12} = w_1 \oplus p_2 \tag{1}$$

由于沃尔什码具有式(2)所示的正交性，式中N_w表示码长，“+1”表示比特“0”，“–1”表示比特“1”。因此用沃尔什码标识发送用户可以使得同一符号间隔来自不同发送用户的信号之间彼此正交，增强了有效用户识别码的抗多址干扰性。

$$\frac{1}{N_w}\sum_{l=1}^{Nw} w_a(l)w_b(l) = \begin{cases} 1, a = b \\ 0, a \neq b \end{cases} \tag{2}$$

由于M序列具有较强的自相关性如式(3)所示，式中N_p表示码长，“+1”表示比特“0”，“–1”表示比特“1”。因此用M序列标识接收用户，增强了有效用户识别码的抗码间干扰性。

$$\frac{1}{N_p}\sum_{l=1}^{Np} p_a(l)p_a(l+m) = \begin{cases} 1, m = 0 \\ 0, m \neq 0 \end{cases} \tag{3}$$

2.2 扩频与数据传输

每个用户的物理层还存储着一张信道安全码表如表3所示，信道安全码表由64个64 bit真随机序列组成[15]。将有效用户识别码v_{12}与表3中的信道安全码$z_c, (c = 1, 2, \cdots, 64)$逐个异或如式(4)所示，得到64 bit正交随机安全序列$s_{1,2,c}, (c = 1, 2, \cdots, 64)$，从而提高信道安全性。

将用户1的发送数据以6 bit为一组进行分组，将每组数据看作一个符号，共有64种符号，把每种符号与一个正交随机安全序列对应实现扩频如表4所示，扩频增益为64/6。采用这种扩频方式可以提高传输效率节省带宽。联合有效用户识别与信道安全编码方法如图1所示。

$$s_{1,2,c} = v_{12} \oplus z_c, \quad c = 1, 2, \cdots, 64 \tag{4}$$

每个用户在每个符号间隔处于“Listen”状态(简称“L”状态)或者“PossiblyTransmit”状态(简称“PT”状态)这两种状态之一。当用户处于“L”状态时，只能接收信号，不能发送信号；当用户处于“PT”状态时，不能接收信号，以一定概率发送信号。用二进制符号“1”表示“PT”状态，“0”表示“L”状态如图2所示。用户的状态由调度表控制，调度表由M序列生成器产生，所有用户使用相同的M序列生成多项式并以用户编号的二进制形式作为M序列生成器的初始状态产生调度表。各用户周期性地将初始状态的最右1位取反并循环右移1位作为新初始状态更新调度表。用户1生成所有用户的调度表，找到一个符号间隔使得用户1处于“PT”状态同时用户2处于“L”状态，如果此时网络中还有α个用户也处于“PT”状态，那么用户1就以概率$\min\{\gamma/(\alpha+1), 1\}$发送经过调制后的

表 3 信道安全码表

编号	信道安全码
1	100111011100011111111000101011001010101110100011010100010010100 0
⋮	⋮
64	010110001001010101100111011110010100100101100101001000101000 1001

表 4 正交随机安全序列表

6 bit符号	正交随机安全序列
000000	010010110000110100001001101001010100010011100000010100001111 1011
⋮	⋮
111111	100011100101111110010110011100001010011000100110001000110101 1010

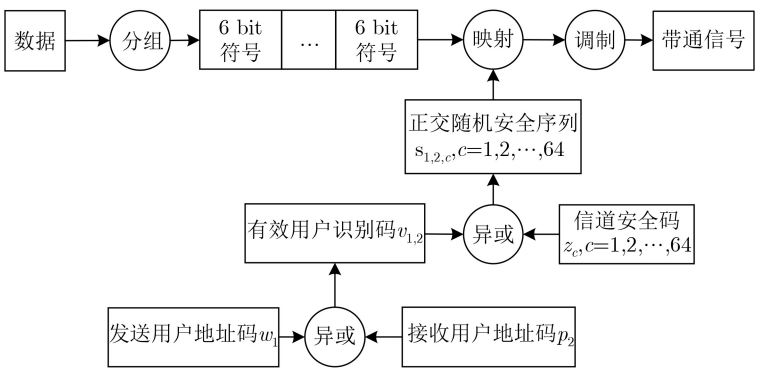

图 1 联合有效用户识别与信道安全编码方法

符号间隔	1	2	3	4	5	6	7	8	…
用户1调度表	0	1	1	0	0	0	1	0	…
用户2调度表	1	0	1	0	0	1	1	1	…
用户3调度表	1	0	0	0	1	1	1	0	…
…	…								

图 2 各用户调度表

正交随机安全序列。γ是一个可以调整的参数，当网络中吞吐量较大时$\gamma \approx 1.5$，当吞吐量较小时$\gamma \approx 2.5$[9]。采用调度表的方式协调各个用户的行为，可以避免网络拥堵，同时降低用户2的计算量从而降低能耗。

3　基于Ad hoc网络的联合译码方法

考虑一个有Q个用户的Ad hoc网络，用户通过加性高斯白噪声信道同步发送数据包。假设当前符号间隔有H个用户发送数据包，即当前符号间隔有H个活动用户。由于Ad hoc网络没有中心节点，各用户地位平等相互发送数据包，因此处于“L”状态的用户2可以接收到当前符号间隔网络中传输的所有数据包，对于用户2来说有效用户识别的目的就是从接收到的数据包中识别出发送给自己的数据包。用户2的接收信号可以表示为

$$r(t) = x(t) + n(t), t \in [0, T] \tag{5}$$

其中，T表示符号间隔，$n(t)$是加性高斯白噪声信号，$x(t)$是H个活动用户发送信号的叠加，可以表示为

$$x(t) = \sum_{h=1}^{H} y_h(t), t \in [0, T] \tag{6}$$

$y_h(t)$表示第h个活动用户的发送信号，它具有如下形式

$$y_h(t) = \sum_{l=0}^{N-1} {\beta_l}^h g(t - lT_c), t \in [0, T] \tag{7}$$

其中，${\beta_0}^h {\beta_1}^h \cdots {\beta_{N-1}}^h$是第$h$个活动用户发送的正交随机安全序列，长度$N$为64 bit，取值为$\pm 1$，“+1”表示比特“0”，“–1”表示比特“1”。$g(t)$是幅度归一化的持续时间为T_c的矩形脉冲，$T/T_c = N$。

将式(6)代入式(5)可得

$$r(t) = \sum_{h=1}^{H} y_h(t) + n(t), t \in [0, T] \tag{8}$$

用户2在一个符号间隔内对接收信号$r(t)$进行匹配滤波和采样得到接收向量$\boldsymbol{r} \in \mathrm{R}^N$，如式(9)所示

$$\boldsymbol{r} = \sum_{h=1}^{H} \boldsymbol{y}_h + \boldsymbol{n} \tag{9}$$

其中，$\boldsymbol{y}_h = \left[{\beta_0}^h \ {\beta_1}^h \cdots {\beta_{N-1}}^h \right]^{\mathrm{T}} \in \{\pm 1\}^{N \times 1}$表示第$h$个活动用户的发送向量，$\boldsymbol{n} \in \mathrm{R}^N$表示均值为零向量，协方差矩阵为$\sigma^2 \boldsymbol{I}_N$的加性高斯白噪声向量。

用户2对$\boldsymbol{r}$求相关得到协方差矩阵$\mathbf{CovR}$，如式(10)所示

$$\mathbf{CovR} = \mathrm{E}\{\boldsymbol{r}\boldsymbol{r}^{\mathrm{T}}\} \tag{10}$$

由于不同活动用户发送的正交随机安全序列相互正交，可得

$$\mathbf{CovR} = \sum_{h=1}^{H} \boldsymbol{y}_h {\boldsymbol{y}_h}^{\mathrm{T}} + \sigma^2 \boldsymbol{I}_N \tag{11}$$

令A表示$\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_H$组成的集合，令矩阵$\boldsymbol{S} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_H] \in \mathrm{R}^{N \times H}$则

$$\mathbf{CovR} = \boldsymbol{S}\boldsymbol{S}^{\mathrm{T}} + \sigma^2 \boldsymbol{I}_N \tag{12}$$

对$\mathbf{CovR}$做特征值分解如式(13)所示

$$\mathbf{CovR} = \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^{-1} \tag{13}$$

由于$\mathbf{CovR} = \mathbf{CovR}^{\mathrm{T}}$，所以$\boldsymbol{U}$是正交矩阵满足$\boldsymbol{U}^{\mathrm{T}} = \boldsymbol{U}^{-1}$，可得

$$\begin{aligned} \mathbf{CovR} &= \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^{\mathrm{T}} \\ &= \begin{bmatrix} \boldsymbol{U}_{\mathrm{s}} & \boldsymbol{U}_{\mathrm{n}} \end{bmatrix} \begin{bmatrix} \boldsymbol{\Lambda}_{\mathrm{s}} & 0 \\ 0 & \boldsymbol{\Lambda}_{\mathrm{n}} \end{bmatrix} \begin{bmatrix} {U_{\mathrm{s}}}^{\mathrm{T}} \\ {U_{\mathrm{n}}}^{\mathrm{T}} \end{bmatrix} \end{aligned} \tag{14}$$

其中，$\boldsymbol{\Lambda} = \mathrm{diag}(\boldsymbol{\Lambda}_{\mathrm{s}}, \boldsymbol{\Lambda}_{\mathrm{n}}) = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_H, \sigma^2, \sigma^2, \cdots, \sigma^2)$由$\mathbf{CovR}$的$N$个特征值组成，$\boldsymbol{\Lambda}_{\mathrm{s}} = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_H)$，$\boldsymbol{\Lambda}_{\mathrm{n}} = \sigma^2 \boldsymbol{I}_{N-H}$，$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_H > \sigma^2$。$\boldsymbol{U} = \begin{bmatrix} \boldsymbol{U}_{\mathrm{s}} & \boldsymbol{U}_{\mathrm{n}} \end{bmatrix} \in \mathrm{R}^{N \times N}$由$\mathbf{CovR}$的$N$个标准正交特征向量组成，$\boldsymbol{U}_{\mathrm{s}} \in \mathrm{R}^{N \times H}$包含$H$个特征向量，与$\lambda_1, \lambda_2, \cdots, \lambda_H$一一对应。$\boldsymbol{U}_{\mathrm{n}} \in \mathrm{R}^{N \times (N-H)}$包含$N - H$个特征向量对应于$\sigma^2$。联立式(12)与式(14)可得

$$\boldsymbol{S}\boldsymbol{S}^{\mathrm{T}} = \boldsymbol{U}\left(\boldsymbol{\Lambda} - \sigma^2 \boldsymbol{I}_N\right)\boldsymbol{U}^{\mathrm{T}} \tag{15}$$

其中

$$\boldsymbol{\Lambda} - \sigma^2 \boldsymbol{I}_N = \begin{bmatrix} \boldsymbol{\Lambda}_{\mathrm{s}} - \sigma^2 \boldsymbol{I}_H & \boldsymbol{0}_{H \times (N-H)} \\ \boldsymbol{0}_{(N-H) \times H} & \boldsymbol{0}_{(N-H) \times (N-H)} \end{bmatrix} \tag{16}$$

将式(16)代入式(15)，可得

$$\boldsymbol{S}\boldsymbol{I}_H\boldsymbol{S}^{\mathrm{T}} = \boldsymbol{U}_{\mathrm{s}}(\boldsymbol{\Lambda}_{\mathrm{s}} - \sigma^2 \boldsymbol{I}_H){\boldsymbol{U}_{\mathrm{s}}}^{\mathrm{T}} \tag{17}$$

从式(17)可以看出，矩阵$\boldsymbol{S}$的列向量张成的空间，即集合A中正交随机安全序列张成的空间等效于$\boldsymbol{U}_{\mathrm{s}}$中特征向量张成的空间，即$\mathrm{range}(\boldsymbol{S}) = \mathrm{range}(\boldsymbol{U}_{\mathrm{s}})$，$\mathrm{range}(\boldsymbol{U}_{\mathrm{s}})$称为信号子空间。

用户2生成所有用户的调度表，检索所有用户调度表的当前符号间隔，得到处于“PT”状态的用户集合E。以用户2的接收用户地址码p_2与集合E中每个用户的发送用户地址码异或生成有效用户识别码集合，用该集合中的每个有效用户识别码与

表3中的信道安全码逐一异或生成正交随机安全序列集合B_2。

以集合A_2表示用户2的有效用户发送的正交随机安全序列，由于$A_2=A\cap B_2$，因此有效用户识别的目的就是从B_2中识别出属于A的序列。如果A_2不是空集，那么A_2中的正交随机安全序列属于range($\boldsymbol{S}$)。由于range($\boldsymbol{S}$) = range($\boldsymbol{U}_{\rm s}$)，那么A_2中的正交随机安全序列属于range($\boldsymbol{U}_{\rm s}$)。因此将B_2中的正交随机安全序列投影到$\boldsymbol{U}_{\rm s}$如式(18)所示，得到置信度$d_{i,2,c}$的集合D_2。

$$d_{i,2,c}=\left\|\boldsymbol{U}_{\rm s}{}^{\rm T}s_{i,2,c}\right\|^2=(\boldsymbol{U}_{\rm s}{}^{\rm T}s_{i,2,c})^{\rm T}(\boldsymbol{U}_{\rm s}{}^{\rm T}s_{i,2,c}),\quad s_{i,2,c}\in B_2 \tag{18}$$

假设忽略子空间估计误差。如果集合E中的用户i是用户2的有效用户，则集合B_2中由用户i生成的正交随机安全序列中必存在一个$s_{i,2,c}$同时属于集合B_2和集合A，那么它对应的$d_{i,2,c}$满足$d_{i,2,c}=N$。反之，如果用户i不是用户2的有效用户，则由用户i生成的正交随机安全序列属于集合B_2但不属于集合A，那么集合D_2中用户i的置信度服从$0\le d_{i,2,c}<N$, $c=1,2,\cdots,64$。在这种理想情况下，用户2根据式(18)的结果可以轻易地识别出有效用户。但是在实际情况下由于受到不可避免的子空间估计误差和信道噪声的影响，即使用户i是用户2的有效用户，它的置信度也服从$0\le d_{i,2,c}<N, c=1,2,\cdots,64$。

因此本文给出一个如式(19)所示的判决模型来区分有效用户与非有效用户，式中$d_{\rm th}$表示判决门限，它是一个经验值。通过将D_2中的置信度与$d_{\rm th}$进行比较，用户2识别出有效用户。

$$A_2=\{s_{i,2,c}|d_{i,2,c}\ge d_{\rm th}, s_{i,2,c}\in B_2, d_{i,2,c}\in D_2\} \tag{19}$$

如果判决之后D_2中所有的置信度都小于$d_{\rm th}$，说明用户2不存在有效用户，那么用户2丢弃接收信号不做后续处理；如果存在$d_{i,2,c}$满足$d_{i,2,c}\ge d_{\rm th}$，说明用户i是用户2的有效用户，如果用户i的置信度中存在多个不小于$d_{\rm th}$的置信度，那么以数值最大的置信度对应的正交随机安全序列为索引检索用户i的正交随机安全序列表得到用户i发送的6 bit符号。联合有效用户识别与信道安全译码方法如图3所示。

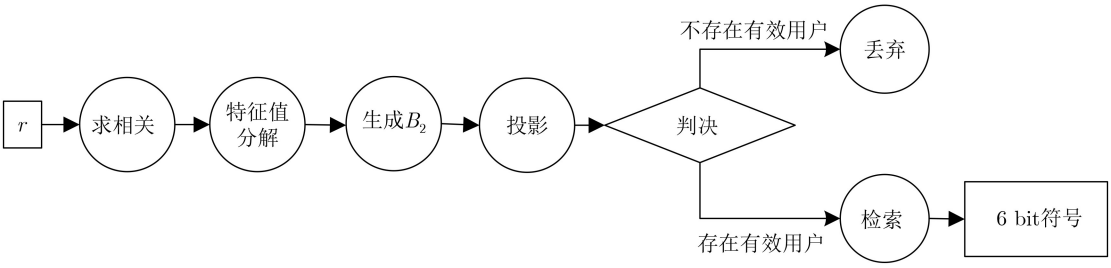

图 3 联合有效用户识别与信道安全译码方法

4 仿真实验与分析

为了验证联合有效用户识别与信道安全编译码方法的性能，采用Matlab2015软件进行仿真实验。采用随机生成的二进制符号作为数据包，实验参数如表5所示，Ad hoc网络结构如图4所示。所有用户保持静止在加性高斯白噪声信道上采用BPSK调制方式同步传输数据包。随机选择一个用户作为观测用户，观测用户在仿真实验中一直处于“L”状态，其他用户在每个符号间隔的状态由各自的调度表决定。处于“PT”状态的用户以相等概率发送数据，并随机选择一个处于“L”状态的用户作为接收用户。实验结果是经过1000次独立重复实验得到的平均值。

表 5 仿真实验参数

实验参数	取值
数据包长度PL	1200 bit
正交随机安全序列长度N	64 bit
符号间隔T	2×10^{-6}s

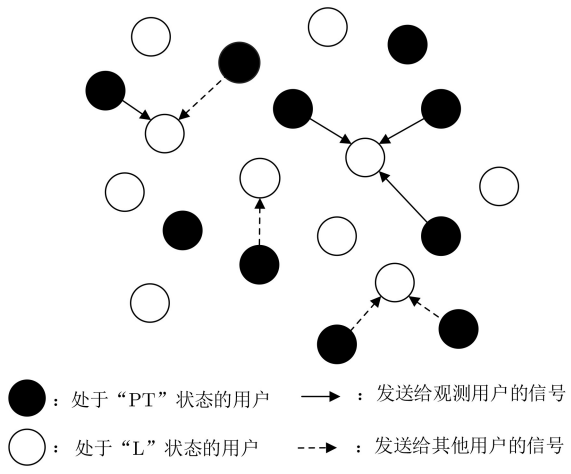

图 4 Ad hoc网络结构

4.1 判决门限d_{th}的选择

图5展示了用户数Q固定为20的条件下，E_{b}/N_0分别取-5 dB, -3 dB, -1 dB, 4 dB时有效用户与非有效用户置信度分布的变化规律。从图中可以看出随着E_{b}/N_0不断增大，有效用户的置信度与非有效用户的置信度的区分越来越明显，因此只需考察E_{b}/N_0最差的情况下判决门限的选择，适合$E_{\text{b}}/N_0 = -5$ dB条件下的判决门限同样适合于$E_{\text{b}}/N_0 = -4.5$ dB $\sim$ 4 dB的无线环境，所以判决门限d_{th}的选择对无线环境具有良好的适应性。

图6展示了E_{b}/N_0固定为-5 dB的条件下，用户数Q分别取20, 24, 28, 32时有效用户识别的漏警概率和虚警概率与判决门限d_{th}的关系曲线。从图6中可见随着d_{th}增大，漏警概率上升，虚警概率下降。不同用户数的情况下曲线的走势基本一致，因此判决门限d_{th}的选择对用户数目具有良好的适应性。

综合图5和图6的实验结果在$E_{\text{b}}/N_0 = -5$ dB, $Q = 20$的条件下决定判决门限d_{th}的取值。为了在漏警概率和虚警概率之间做一个平衡，将d_{th}设置为22。

4.2 误判概率的比较

比较本文方法与文献[6]和文献[7]中方法有效用户识别的误判概率。有效用户识别的误判概率包括漏警概率和虚警概率。漏警概率表示用户是有效用户而判为非有效用户的概率，虚警概率表示用户是非有效用户而判为有效用户的概率。文献[6]提出的3种方法分别称为顺序重要性采样-最优(Sequential Importance Sampling-OPTimal, SIS-OPT)，顺序重要性采样-线性滤波器(Sequential Importance Sampling-Linear Filter, SIS-LF)和幸存路径处理(Per-Survivor Processing, PSP)。文献[7]提出的方法称为用户可检测序列(User Detectable Sequence, UDS)。

图7和图8分别比较在$Q = 20$的场景下，本文方法与文献[6]、文献[7]方法在不同E_{b}/N_0下的漏警概

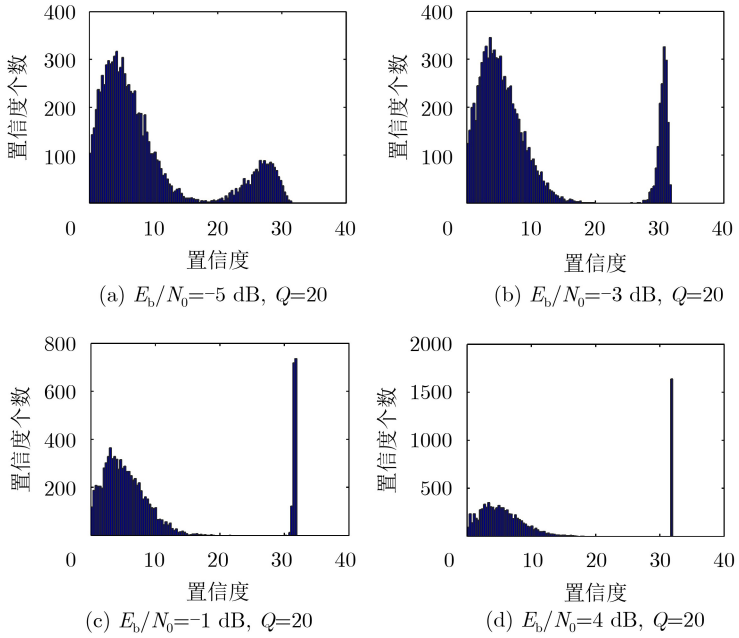

图 5 置信度直方图

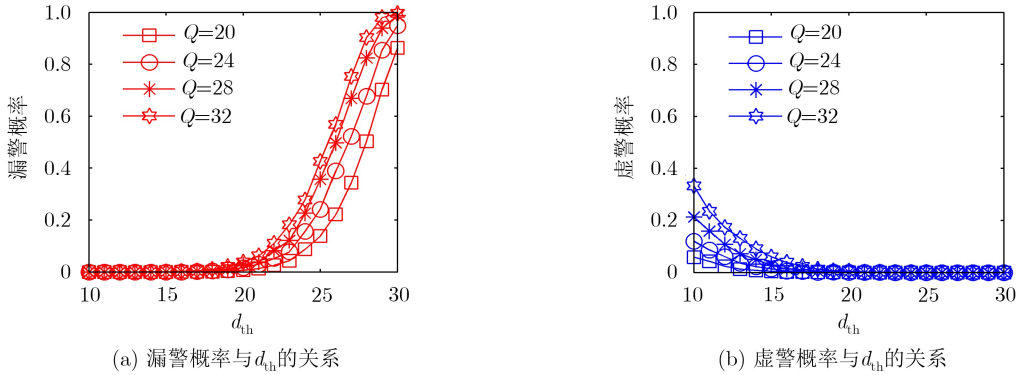

图 6 $E_{\text{b}}/N_0 = -5$ dB, $Q = 20, 24, 28, 32$时本文方法的漏警概率，虚警概率与d_{th}的关系

率和虚警概率。从图7中可见UDS的漏警概率性能在低信噪比区间较差，这是由于该方法在理想条件下设计。当漏警概率为10^{-3}时本文方法与其他4种方法相比获得至少1.6 dB信噪比增益。从图8可见本文方法的虚警概率曲线与UDS的虚警概率曲线完全重合，在全部信噪比区间都为0。

图9和图10分别比较在$E_b/N_0=-5$ dB的场景下，本文方法与文献[6]、文献[7]方法在不同用户数Q下的漏警概率和虚警概率。从图9可见当$Q\le 8$时，UDS的漏警概率性能与本文方法的漏警概率性能很接近，两者的差距随着Q的增加逐渐扩大。从图10可见本文方法的虚警概率曲线与UDS的虚警概率曲线又一次完全重合，在全部Q区间都为0，与图8展现出的性能一致。

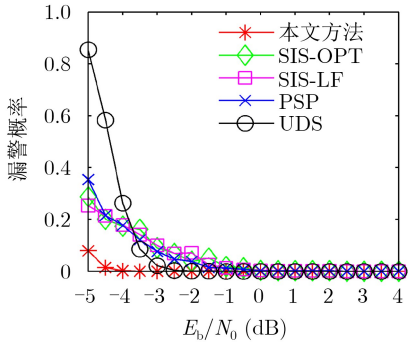

图 7 $Q=20$时不同E_b/N_0下5种方法的漏警概率

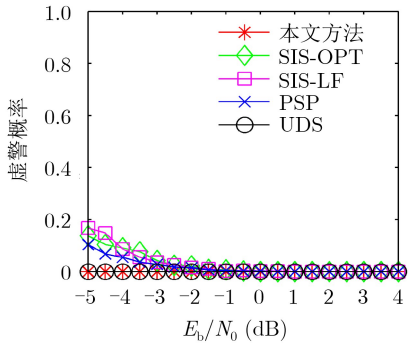

图 8 $Q=20$时不同E_b/N_0下5种方法的虚警概率

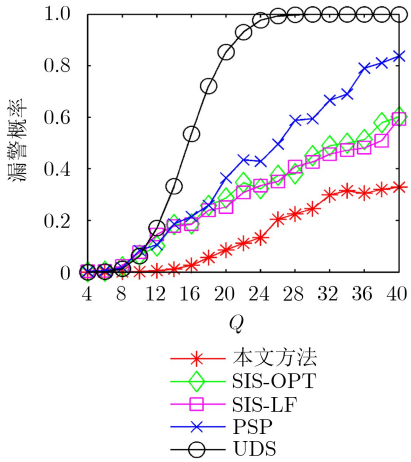

图 9 $E_b/N_0=-5$ dB时不同Q下5种方法的漏警概率

从图7—图10可以看出本文方法的性能是5种方法中最好的，尤其在无线环境较恶劣和用户数较多的情况下优势更明显。这是由于正交随机安全序列的特性使得本文方法可以有效对抗多址干扰和码间干扰。

4.3 复杂度分析

本文对联合有效用户识别与信道安全编译码方法的复杂度进行分析。为简化分析假设乘法、加法、比较等基本运算的复杂度都相同，设为单位1。用PH表示处于“PT”状态的用户数，用F表示用户2的有效用户数，通过计算编译码方法每个步骤的复杂度得到总复杂度。

联合有效用户识别与信道安全编码方法：

步 骤 1　用户1生成有效用户识别码，复杂度为N；

步 骤 2　用户1生成正交随机安全序列，复杂度为$64\times N$。

联合有效用户识别与信道安全译码方法：

步 骤 1　计算接收向量$\boldsymbol{r}$的协方差矩阵$\mathbf{CovR}$，复杂度为$2N^2\times H-N^2+N$；

步 骤 2　对$\mathbf{CovR}$进行特征值分解，复杂度为N^3；

步 骤 3　生成正交随机安全序列集合B_2，复杂度为$65\times N\times \mathrm{PH}$；

步 骤 4　生成置信度集合D_2，复杂度为$64\times \mathrm{PH}\times(2N\times H+H-1)$；

步 骤 5　将置信度与判决门限d_{th}进行比较，复杂度为$64\times \mathrm{PH}$；

步 骤 6　解扩得到6 bit符号，复杂度为$65\times N\times F$。令F取最大值H，复杂度为$65\times N\times H$。

为分析方便假设$\mathrm{PH}=H=Q/2$，根据表5所示的参数值总复杂度为$2064Q^2+8256Q+262272$，近似表示为$O(Q^2)$。

表6列出了本文方法、文献[6]和文献[7]方法的复杂度。可以看出本文方法的复杂度高于SIS-LF的

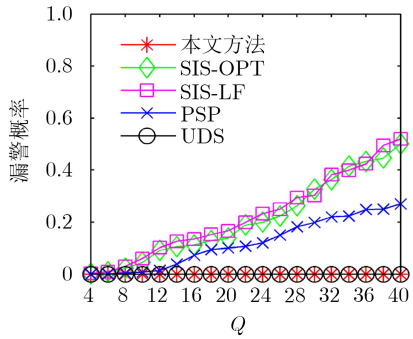

图 10 $E_b/N_0=-5$ dB时不同Q下5种方法的虚警概率

表 6　5种方法的复杂度

有效用户识别方法	复杂度
联合有效用户识别与信道安全编译码方法	$O(Q^2)$
文献[6]SIS-OPT	$O(3^Q)$
文献[6]SIS-LF	$O(Q)$
文献[6]PSP	$O(3^{2Q})$
文献[7]UDS	$O(Q^2)$

复杂度，与UDS的复杂度在一个数量级，低于SIS-OPT和PSP的复杂度。

5　结束语

Ad hoc网络中用户能量受限导致有效用户识别的可靠性和信道安全性面临威胁。针对已有的有效用户识别方法在低信噪比情况下误判概率较大且没有考虑信道安全，本文提出一种联合有效用户识别与信道安全编译码方法。实验结果表明通过建立判决模型并选择合适的判决门限识别有效用户，当漏警概率为10^{-3}时本文方法与SIS-OPT, SIS-LF, PSP和UDS相比信噪比增益改善1.6 dB，同时具有较低的复杂度。随着5G时代的到来，Ad hoc网络在智能交通、空天地一体化、卫星组网等领域有着广泛的应用前景。其中车联网是Ad hoc网络在智能交通领域的一个热点应用，解决车联网中的有效用户识别问题有助于缓解交通拥堵，减少交通事故。因此在未来工作中我们将对车联网中的有效用户识别问题开展进一步研究。

参 考 文 献

[1] WU W C and CHEN K C. Identification of active users in synchronous CDMA multiuser detection[J]. *IEEE Journal on Selected Areas in Communications*, 1998, 16(9): 1723–1735. doi: 10.1109/49.737641.

[2] LIN D D and LIM T J. Subspace-based active user identification for a collision-free slotted ad hoc network[J]. *IEEE Transactions on Communications*, 2004, 52(4): 612–621. doi: 10.1109/TCOMM.2004.826415.

[3] PAD P, SOLTANOLKOTABI M, HADIKHANLOU S, *et al*. Errorless codes for over-loaded CDMA with active user detection[C]. 2009 IEEE International Conference on Communications, Dresden, Germany, 2009: 1–6. doi: 10.1109/ICC.2009.5199003.

[4] ANGELOSANTE D, BIGLIERI E, and LOPS M. Multiuser detection in a dynamic environment—part II: Joint user identification and parameter estimation[J]. *IEEE Transactions on Information Theory*, 2009, 55(5): 2365–2374. doi: 10.1109/TIT.2009.2016008.

[5] ANGELOSANTE D, BIGLIERI E, and LOPS M. Low-complexity receivers for multiuser detection with an unknown number of active users[J]. *Signal Processing*, 2010, 90(5): 1486–1495. doi: 10.1016/j.sigpro.2009.10.019.

[6] VÁZQUEZ M A and MÍGUEZ J. User activity tracking in DS-CDMA systems[J]. *IEEE Transactions on Vehicular Technology*, 2013, 62(7): 3188–3203. doi: 10.1109/TVT.2013.2251024.

[7] ZHANG Yijin, SHUM K W, WONG W S, *et al*. Binary sequences for multiple access collision channel: Identification and synchronization[J]. *IEEE Transactions on Communications*, 2014, 62(2): 667–675. doi: 10.1109/TCOMM.2013.121313.130331.

[8] 田珊, 张灿. 无线ad hoc网络中基于跨层设计的有效用户识别方法[J]. 中国科学院研究生院学报, 2009, 26(5): 681–687.
TIAN Shan and ZHANG Can. Virtual user identification based on cross-layer design in wireless ad hoc networks[J]. *Journal of the Graduate School of the Chinese Academy of Sciences*, 2009, 26(5): 681–687.

[9] ROZOVSKY R and KUMAR P R. Seedex: A MAC protocol for ad hoc networks[C]. The 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, USA, 2001: 67–75. doi: 10.1145/501426.501427.

[10] JEONG B K, SHIM B, and LEE K B. MAP-based active user and data detection for massive machine-type communi cations[J]. *IEEE Transactions on Vehicular Technology*, 2018, 67(9): 8481–8494. doi: 10.1109/TVT.2018.2849621.

[11] AHN J, SHIM B, and LEE K B. EP-based joint active user detection and channel estimation for massive machine-type communications[J]. *IEEE Transactions on Communications*, 2019, 67(7): 5178–5189. doi: 10.1109/TCOMM.2019.2907853.

[12] KIM W, LIM G, AHN Y, *et al*. Active user detection of machine-type communications via dimension spreading neural network[C]. 2019 IEEE International Conference on Communications, Shanghai, China, 2019: 1–6. doi: 10.1109/ICC.2019.8761407.

[13] 葛文萍, 张雪婉, 吴雄, 等. 基于部分码字消息传递的SCMA多用户检测算法[J]. 电子与信息学报, 2018, 40(10): 2309–2315. doi: 10.11999/JEIT171073.
GE Wenping, ZHANG Xuewan, WU Xiong, *et al*. Message passing multiuser detection algorithm for SCMA based on partial codewords searching[J]. *Journal of Electronics & Information Technology*, 2018, 40(10): 2309–2315. doi: 10.11999/JEIT171073.

[14] 杨维, 赵懿伟, 侯健琦. 一种改进基于门限的稀疏码多址接入低复杂度多用户检测算法[J]. 电子与信息学报, 2018, 40(5): 1044–1049. doi: 10.11999/JEIT170647.
YANG Wei, ZHAO Yiwei, and HOU Jianqi. An improved threshold-based low complexity multiuser detection scheme for sparse code multiple access system[J]. *Journal of Electronics & Information Technology*, 2018, 40(5): 1044–1049. doi: 10.11999/JEIT170647.

[15] Rand Corporation. A Million Random Digits with 100, 000 Normal Deviates[M]. New York, USA: Free Press, 1955: 5–404.

张克楠：男，1990年生，博士生，研究方向为信号与信息处理.

涂国防：男，1954年生，教授，研究方向为深空通信.

张　灿：女，1954年生，教授，研究方向为Ad hoc网络、信息安全.

陈德元：男，1968年生，副教授，研究方向为信道编码.

责任编辑：陈　倩