窃听信道下基于双分簇技术的信源安全有损传输

徐 明,胡沐宇
(上海海事大学信息工程学院,上海 201306)

摘 要: 针对图像、视频等文件在压缩传输时的可靠性和安全性问题,提出一种具有边信息和状态信息的窃听信道模型以及该模型下基于双分簇技术的信源安全有损传输方案,并利用信息理论对速率-失真-信息泄露率三元组进行可达性和逆命题证明. 考虑到现实环境中的噪声因素,以高斯噪声信道为例进行具体分析,通过误差估计和微分熵定理推导出速率和失真的下界. 此外,引入模糊率,将信息泄漏率转化为估计信源的最小均方误差,得出此误差的上界. 仿真实验表明,所提方案在最优条件下比现有方案速率高,失真和信息泄露率小,在非最优条件下比现有方案模糊率高.

关键词: 窃听信道; 双分簇技术; 安全有损传输; 边信息; 状态信息; 信息泄漏
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2022)09-2196-09
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20200932

Secure Lossy Source Transmission over Wiretap Channel Based on Double Binning Technique

XU Ming, HU Mu-yu
(*College of Information Engineering*, *Shanghai Maritime University*, *Shanghai* 201306, *China*)

Abstract: Aiming at the reliability and security problem of transmitting compressed images, videos and other files, a wiretap channel model with side information and state information and a secure lossy source transmission scheme based on double binning technique under this model are proposed. Moreover, the achievability and the converse of the triple rate-distortion-leakage are proved by the information theory. Considering the noise factors in the real environment, the Gaussian noise channel under this model is analyzed concretely as an example and the lower bounds of the rate and the distortion are derived based on the error estimation and the differential entropy theorem. In addition, the equivocation rate is introduced to transform the information leakage rate into the minimum mean square error of the estimated source and its upper bound is obtained. The simulation results show that the proposed scheme has higher rate and lower distortion and information leakage rate than the existing schemes under the optimal conditions, and has higher equivocation rate than the existing schemes under the non-optimal conditions.

Key words: wiretap channel; double binning technique; secure lossy transmission; side information; state information; information leakage

1 引言

随着网络信息技术的发展,各个领域产生的信息量呈现出爆炸性增长,其中敏感和隐私信息如生物识别中的特征数据、植入式医疗电子设备中的无线可靠传输、视频流媒体传输以及电子商务交易数据集之类的传输处理方式就显得尤为重要[1~4]. 未经处理的原始信息量巨大,为了有效传输,需要进行压缩即编码. 在该背景下,信息的压缩和安全传输技术面临挑战. 信息论通过研究网络传输中信息流的极限以及达到这些极限的最优编码方案来提高系统的安全性.

基于信息论实现信源的安全传输最早由 Shannon 提出[5]. 在此基础上,Wyner提出假设窃听信道与合法信道相比是退化的,那么消息在有噪信道中可以安全传输[6]. Csiszár 和 Körner将此结论拓展到一般的广播信道,并根据窃听者对传输信息的不确定程度来衡量信道的保密级别,建立存在公共消息和保密消息的速

收稿日期:2020-08-24;修回日期:2021-12-29;责任编辑:梅志强
基金项目:国家自然科学基金(No.62172269)

率-泄露率区域(rate-leakage region)[7]. 上述工作都基于信源的安全无损传输,即合法接收者在信源压缩传输时不产生失真的情况下重建信源. 如果信源在压缩传输时产生失真,那么就要考虑失真对信源安全传输的影响. Wyner和Ziv定义了信源安全有损传输下的速率-失真函数(rate-distortion function),并在传输的约束条件中增加了速率、失真和泄露率等有限码率约束,目的是让窃听者对传输的消息尽可能保持未知[8]. Chia和Chong刻画了具有边信息的Wyner-Ziv信源编码的速率-失真区域,指出解码器到编码器的反馈不会减少总速率[9]. Villard和Piantanida构建了边信息对窃听者非因果性可知的信道模型,考虑了未编码边信息对合法用户非因果性可知时,合法用户接收到的信源能无损重建的情况,得出更紧的速率-失真-模糊率区域[10]. 考虑到无线衰落信道的统计特性不断变化,Koyluoglu等人引入状态信息,对具有状态的广播信道建立索引,得出退化高斯信道模型的最优角点以及上界与可达区域的距离[11]. Han等人提出状态信息对编码器非因果性可知的窃听信道模型,并得出该信道模型的保密容量下界以及密钥容量[12].

通过上述分析可知,边信息有助于解码器减小信源与信源估计之间的失真,状态信息可以用来表征统计特征不确定的无线衰落信道以及提高消息传输速率. 然而,由于无线信道的复杂性,特别是在无线衰落窃听信道下,往往既包含边信息又包含状态信息,并且窃听者可能窃听到边信息. 如何设计安全可靠的编解码机制并对相关有限码率约束进行定界需要进一步研究. 本文提出一种边信息对解码器非因果性可知和状态信息对编码器非因果性可知的安全有损传输方案,基于双分簇技术设计出信源编解码机制,并以该模型下的高斯噪声窃听信道为例进行具体分析,推导出速率-失真-信息泄露率的下界,然后引入模糊率,将信息泄漏率转化为估计信源的最小均方误差,得出信源估计最小均方误差的上界. 考虑噪声功率不同的情况下的速率和失真的下界以及信源估计最小均方误差的上界进行仿真,得到三者之间最优权衡并对实验结果进行比较分析.

2　预备知识

2.1　基本符号

熵$H(\cdot)$表示随机变量不确定性的度量;互信息$I(\cdot)$表示一个随机变量中包含的关于另一个随机变量的信息量;X、Y、Z表示有限集合$\mathcal{X}$、$\mathcal{Y}$、$\mathcal{Z}$上的离散型随机变量,x、y、z表示X、Y、Z的取值,概率分布分别为$P(x)$、$P(y)$和$P(z)$;x_k^n表示由$(x_i)_{i\in\mathbb{N}^*}$构成的序列$(x_k,x_{k+1},\cdots,x_n)$,其中$\mathbb{N}^*$表示正自然数集,x_1^n简化为x^n;若P和Q是联合高斯随机变量,Γ_{PQ}表示P和Q的协方差矩阵;$\mathbb{R}$表示实数集,$\mathbb{R}^d$表示d维欧几里得空间.

2.2　相关定义

定义1　若$\hat{\mathcal{X}}$为重建字母,失真度量是映射$d:\mathcal{X}\times\hat{\mathcal{X}}\to[0,\infty)$,表示符号$x$被恢复为符号$\hat{x}$的代价,则$x^n$和$\hat{x}^n$之间的平均失真可定义为

$$d(X^n,\hat{X}^n)=\frac{1}{n}\sum_{i=1}^{n}d(x_i,\hat{x}_i) \tag{1}$$

定义2　若随机变量X在集合$\mathcal{X}$上均匀分布,则保密编码$(2^{nR},n)$对应的信息泄露率I_e为

$$I_e=\frac{1}{n}I(X^n;\ Z^n,E^n) \tag{2}$$

定义3　如果一个以速率R,失真D,信息泄露率I_e构成的三元组(R,D,I_e)存在并进行信息的安全有损传输,对于任意$\delta>0$和$n\geq1$,一个$(n,R+\delta)$码序列满足以下2个条件,则$(R,D,I_e)\in\mathbb{R}_+^3$是可达的.

$$\mathrm{E}[d^n(X^n,\hat{X}^n)]\leq D+\delta \tag{3}$$

$$\frac{1}{n}I(X^n;\ Z^n,E^n)\leq I_e+\delta \tag{4}$$

3　系统模型与编解码机制

3.1　系统模型

本文所构建的具有边信息和状态信息的窃听信道模型由合法发送者Alice,合法接收者Bob以及窃听者Eve组成. Alice想发送信源信息给Bob,Bob根据接收到的消息重构信源,并确保泄露给Eve的信息尽可能少. 编码器和解码器由编码函数$f^{(n)}:X^n\times S^n\to F^n$和解码函数$g^{(n)}:Y^n\times B^n\to X^n$构成. 编码器产生的序列$F^n$通过信道传输给Bob,Eve通过窃听信道进行窃听,状态信息S^n对编码器非因果性可知,并且与信道噪声相互独立. 假设存在平均传输功率约束

$$\sum_{i=1}^{n}\mathrm{E}(x_i{}^2(j,S^n))\leq nP,j\in[1,2^{nR}] \tag{5}$$

则Bob可以通过接收到的序列Y^n和边信息B^n重构信源,而Eve根据窃听到的序列Z^n和边信息E^n不能重构信源.

3.2　编解码机制

根据上节提出的系统模型,设计了信源安全有损传输方案. 该方案中的编码机制通过双分簇技术构造二维码本,目标是在有限码率约束下,使压缩失真和信息泄漏率尽可能小.

3.2.1　码本生成

(1) 固定概率$P_{F|X}P_{V|XF}P_{U|V}$使其达到信道容量,随机生成$2^{nI(X;\ F)}$个序列$f^n(w_f),w_f\in\{1,\cdots,2^{nF}\}$. 对于每个$w_f$,独立并随机生成$2^{nI(U;\ X|F)}$个独立同分布的码字序列$u^n(w_f,w_u),w_u\in\{1,\cdots,2^{nI(U;\ X|F)}\}$,并将$u^n(w_f,w_u)$随机分到

大小相同的 2^{nR_x} 个簇 $\mathcal{C}_1(r_u)$ 中，簇的索引 $r_u\in\{1,2,\cdots,2^{nR_x}\}$，该层分簇构成了码本的第1维.

（2）对于每个 (w_f,w_u) 索引对，随机生成 $2^{nI(V;\,X|U,F)}$ 个独立同分布的码字序列 $v^n(w_f,w_u,w_v)$，$w_v\in\{1,\cdots,2^{nI(V;\,X|U,F)}\}$，然后将码字序列 $v^n(w_f,w_u,w_v)$ 随机分配到 2^{nR_c} 个大小相同的簇 $\mathcal{C}_2(r_v)$ 中，簇的索引 $r_v\in\{1,2,\cdots,2^{nR_c}\}$，该层分簇构成了码本的第2维.

3.2.2 编码

（1）查找一个与信源序列 x^n 联合典型的序列 $f^n(w_f)$. 根据覆盖引理[13]，存在这样的 $f^n(w_f)$，随机选择一个与 (x^n,f^n) 高概率同分布的序列索引 w_f，将其发送给解码器.

（2）查找一个与 (x^n,f^n) 联合典型的序列 $u^n(w_f,w_u)$. 根据覆盖引理，随机选择一个相应簇的索引 w_u，将其发送给解码器.

（3）查找一个与 (x^n,f^n,u^n) 联合典型的序列 $v^n(w_f,w_u,w_v)$. 根据覆盖引理，随机选择一个相应簇的索引 w_v，将其发送给解码器.

3.2.3 传输

Alice 发送索引 w_f,w_u,w_v，Bob 得到 $Y^n(\bar{w}_f,\bar{w}_u,\bar{w}_v)$，其中 $\bar{w}_f,\bar{w}_u,\bar{w}_v$ 是 w_f,w_u,w_v 经过合法信道传输后得到的索引估计值；Eve 得到 $Z^n(\tilde{w}_f,\tilde{w}_u,\tilde{w}_v)$，其中 $\tilde{w}_f,\tilde{w}_u,\tilde{w}_v$ 是 w_f,w_u,w_v 经过窃听信道传输后得到的索引估计值.

3.2.4 解码

Bob 以速率 R 和失真 D 接收到 Y^n 并获得关于信源的边信息 B^n，通过解码器在簇 $\mathcal{C}_1(r_u)$ 中查找与 (b^n,f^n) 联合典型的序列 u^n，在簇 $\mathcal{C}_2(r_v)$ 中查找与 (b^n,f^n,u^n) 联合典型的序列 v^n，由此得到状态序列 s^n，继续解码可得估计信源 $\hat{x}^n$.

3.2.5 错误概率分析

将编码和解码过程中出现错误的事件记为 ξ，考虑存在以下情形：

（1）典型性错误

将边信息的典型性错误记为事件 ξ_1，根据典型序列性质，存在 $\varepsilon\to0$ 使得不等式 $P(\xi_1)=P\{(X^n,F^n,B^n,E^n)\notin T_\varepsilon^{\,n}(X,F,B,E)\}\le\varepsilon$ 成立. 将信道的典型性错误记为事件 ξ_2，其错误概率 $P(\xi_2)=P\{(F^n,Y^n,Z^n)\notin T_\varepsilon^{\,n}(F,Y,Z)\}\le\varepsilon$.

（2）编解码错误

将编解码错误记为事件 ξ_3，存在错误概率上界使得 $P(\xi_3)\le\varepsilon$. 因此

$$P(\xi)\le P(\xi_1)+P(\xi_2)+P(\xi_3)\to0.$$

4 速率-失真率-信息泄露率

本节利用信息论推导速率-失真-信息泄露率的下界并给出可达性证明和逆命题证明.

定理 1 若三元组速率-失真-信息泄露率 $(R,D,I_e)\in\mathbb{R}_+^3$，$U,V$ 分别属于有限集合 $\mathcal{U},\mathcal{V}$ 中的辅助随机变量，并存在马尔科夫链 U-V-(X,F)-(B,E) 和 U-V-(F,S)-(Y,Z)，$\hat{X}(V,B,Y)$ 表示解码信源序列函数，则需要满足

$$R\ge I(V;\,F|B) \tag{6}$$

$$D\ge\mathrm{E}[d(X,\hat{X}(\bar{V},B,Y))] \tag{7}$$

$$I_e\ge I(X;\,\tilde{V},\tilde{F},B)-I(X;\,B|\tilde{U},\tilde{F})+I(X;\,E|\tilde{U},\tilde{F}) \tag{8}$$

其中 $\bar{F}$、$\bar{U}$、$\bar{V}$ 为合法接收者接收到的序列，$\tilde{F}$、$\tilde{U}$、$\tilde{V}$ 为窃听者接收到的序列.

证明

（1）可达性证明

① 速率

定义信源的传输速率为 $R+\delta(\delta\to0)$，δ 表示传输中的误差值，则

$$\begin{aligned}R+\delta&>I(U;\,F)-I(U;\,B)+I(V;\,F|U)-I(V;\,B|U)\\&=I(V;\,F|B)\end{aligned}$$

② 失真

将 ϑ 记为在编码步骤或者解码步骤出现错误的事件，令 $\varepsilon\to0$，则

$$\begin{aligned}&\mathrm{E}(d(X^n,g^{(n)}(Y^n,B^n)))\\&\le P\{\bar{\vartheta}\}\mathrm{E}[d(X^n,g^{(n)}(r_u,Y^n,B^n))|\bar{\vartheta}]+P\{\vartheta\}\mathrm{E}(d_{\max})\\&=\mathrm{E}[d(X,\hat{X}(\bar{V},Y,B))]+\varepsilon\le D+\varepsilon\end{aligned}$$

③信息泄露率

$$\begin{aligned}&I(X^n;\,Z^n,E^n)=I(X^n;\,\tilde{w}_f,\tilde{w}_u,\tilde{w}_v,E^n|C_n)\\&\overset{(a)}{\le}n[-H(E|X,\tilde{F})+I(X;\,\tilde{F})+I(\tilde{U};\,X|\tilde{F})+\delta\\&+I(\tilde{V};\,X|\tilde{U},\tilde{F})-I(\tilde{V};\,B|\tilde{U},\tilde{F})]\\&\le n[R_i+\delta]\end{aligned}$$

式中（a）是因为在所有序列都高概率联合典型的条件下，根据信源的无记忆特性得到 $H(E^n|X^n,\tilde{F}^n)$ 和 $H(E^n|F^n,U^n,C^n)$[14].

（2）逆命题证明

① 速率

$$\begin{aligned}&n(R+\varepsilon)\ge H(Y^n)=I(Y^n;\,F^n|B^n)\\&\overset{(a)}{=}\sum_{i=1}^{n}I(Y^nF^{i-1}B^{i-1}B_{i+1}^n;\,F_i|B_i)\\&\ge\sum_{i=1}^{n}I(V_i;\,F_i|B_i)\end{aligned}$$

式中（a）是根据随机变量 F 和 B 在时间上的独立性得到.

② 失真

Bob 利用解码函数进行解码，失真可表示为 $\mathrm{E}[d(X^n,g^n(\bar{w}_v,B^n,Y^n))]=\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}[d(X_i,\hat{X}_i(\bar{V}_i,\bar{B}_i,Y_i))]$，所以 $\mathrm{E}[d(X,\hat{X}(\bar{V}_i,B_i,Y_i))]\le D$.

③ 信息泄露率

$$
\begin{aligned}
&n(R_i+\delta)\geq I(X^n;\ Z^n,E^n)\\
&\overset{(a)}{\geq}\sum_{i=1}^{n}\{H(X_i)-H(X_i|Z^n,\tilde{F}^n,B^n,X^{i-1})\\
&\quad-[H(B_i|Z^n,\tilde{F}^n,B_{i+1}^n)-H(B_i|X_i,\tilde{F}_i)]\\
&\quad+H(E_i|Z^n,\tilde{F}^n,E^{i-1})-H(E_i|X_i,\tilde{F}_i)\}\\
&\overset{(b)}{=}\sum_{i=1}^{n}[\underbrace{I(X_i;\ \tilde{V}_i,\tilde{F}_i,B_i}_{\overset{\text{def}}{=}P_i}-I(X_i;\ B_i|\tilde{F}^n)+I(X_i;\ E_i|\tilde{F}_i))\\
&\quad+I(Z^n,B_{i+1}^n,\tilde{F}^{n\setminus i};\ B_i|\tilde{F}_i)-I(Z^n,E^{i-1},\tilde{F}^{n\setminus i};\ E_i|\tilde{F}_i)]
\end{aligned}
$$

式中(a)是根据Fano不等式和马尔科夫链$(F^n,S^n,X^{n\setminus i},B_{i+1}^n,E^{i-1})$-$(F_i,X_i)$-$(B_i,E_i)$得到. 式中$(b)$根据解码器的解码机制,利用Csiszár求和式得到$\sum_{i=1}^{n}I(B_i;E^{i-1}|F^n,Z^n,B_{i+1}^n)-I(E_i;\ B_{i+1}^n|F^n,Z^n,E^{i-1})=0$,因此$n(R_i+\delta)\geq\sum_{i=1}^{n}[P_i+I(Z^n,B_{i+1}^n,E^{i-1},\tilde{F}^{n\setminus i};\ B_i|\tilde{F}_i)-I(Z^n,B_{i+1}^n,E^{i-1},\tilde{F}^{n\setminus i};\ E_i|\tilde{F}_i)]=\sum_{i=1}^{n}[I(X_i;\ \tilde{F}_i,\tilde{V}_i,B_i)-I(X_i;\ B_i|\tilde{U}_i,\tilde{F}_i)+I(X_i;\ E_i|\tilde{U}_i,\tilde{F}_i)]$.

证毕.

5　高斯噪声窃听信道的安全有损传输

在本节中,我们以具有边信息和状态信息的高斯窃听信道为例分析本文所提出的安全有损传输方案,推导出高斯噪声窃听信道中有限码率约束的界并给出证明,然后考虑不同传输条件下的情况并利用具体数据进行实验和分析.

5.1　高斯噪声窃听信道模型

图1描绘了高斯噪声窃听信道下具有边信息和状态信息的安全有损传输模型. 其中Bob和Eve观测到的边信息噪声分别服从$N_b\sim\mathcal{N}(0,P_b)$和$N_e\sim\mathcal{N}(0,P_e)$分布. 信道状态服从$S\sim\mathcal{N}(0,P_s)$分布,合法信道噪声服从$N_1\sim\mathcal{N}(0,P_y)$分布,窃听信道噪声服从$N_2\sim\mathcal{N}(0,P_z)$分布. 合法信道的信道增益为$g_1$,窃听信道的信道增益为$g_2$,信道平均输入功率约束为$P$.

由于状态信息对编码器非因果性可知,所以可以将S^n看作有限遍历的马尔科夫链,通过最优功率分配函数$\Upsilon(\cdot)$对信道状态进行优化,求解出最优信道状态功率P_s^*.

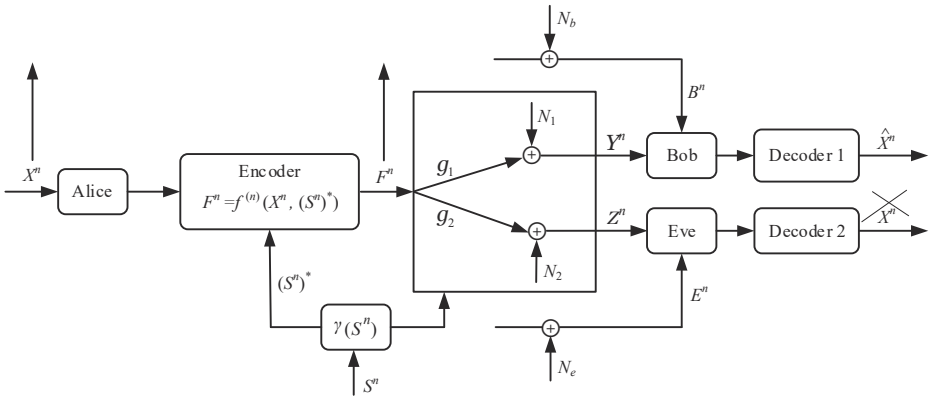

图1　高斯噪声窃听信道的安全有损传输

根据拉格朗日乘子和Kuhn-Tucker条件,最优功率分配函数需要满足

$$\int_0^{\infty}\frac{X}{1+X\Upsilon(S)}p(X|S)\mathrm{d}X\leq\lambda \tag{9}$$

其中拉格朗日乘子$\lambda>0$,其实际值可以通过求解

$$\sum_S p(S)\Upsilon(S)=nP \tag{10}$$

得出,确保满足信道平均输入功率约束. 最后得出

$$P_s^*=\left[\frac{1}{\lambda}-\frac{1}{X}\right]^+ \tag{11}$$

根据本文编码机制,Bob接收到的序列为

$$Y^n(\bar{w}_f,\bar{w}_u,\bar{w}_v)=g_1F^n(w_f,w_u,w_v)+N_1 \tag{12}$$

Eve窃听到的序列为

$$Z^n(\tilde{w}_f,\tilde{w}_u,\tilde{w}_v)=g_2F^n(w_f,w_u,w_v)+N_2 \tag{13}$$

高斯窃听信道下的失真用定义在$\mathbb{R}$上的欧氏距离$d(x,\hat{x})=(x-\hat{x})^2$来衡量. 此外,引入模糊率[15](equivocation rate)$\Delta\in\mathbb{R}$作为Eve对传输信息不确定性的度量,可表示为$\frac{1}{n}H(X^n|Z^n,E^n)=\Delta+\delta$. 定量$I_{\mathcal{DE}}$表示Eve对信源估计的最小均方误差,可以得出$\Delta$关于$I_{\mathcal{DE}}$的表达式. 通过把求$I_e$的下界转化为求$I_{\mathcal{DE}}$的上界,则信息泄露率$I_e$可表示为

$$I_e\triangleq\frac{1}{n}I(X^n;\ Z^n,E^n)\leq H(X)-\Delta=\frac{1}{2}\log_2\frac{1}{I_{\mathcal{DE}}}.$$

5.2　速率-失真率-信源估计的最小均方误差

定理2　若三元组$(R,D,I_{\mathcal{DE}})\in\mathbb{R}_+^3$,$U=\varnothing$,$V$属于有

限集合 $\mathcal{V}$ 中的辅助随机变量且存在马尔科夫链 V-(X,F)-(B,E) 和 V-(F,S)-(Y,Z) 则需要满足

$$R\geq\frac{1}{2}\log_2\frac{\det\boldsymbol{\Gamma}_{FB}\cdot\mathrm{var}[V]}{\det\boldsymbol{\Gamma}_{FV}\cdot\mathrm{var}[B]} \tag{14}$$

$$D\geq\frac{\det\boldsymbol{\Gamma}_{XBY}\cdot\det\boldsymbol{\Gamma}_{\bar{V}XY}}{2\pi\mathrm{e}\cdot\det\boldsymbol{\Gamma}_{\bar{V}BY}\cdot\mathrm{var}[XY]} \tag{15}$$

$$I_{\mathcal{DE}}\leq\frac{\det\boldsymbol{\Gamma}_{\bar{F}X}\cdot\det\boldsymbol{\Gamma}_{\bar{V}X}\cdot\det\boldsymbol{\Gamma}_{B\tilde{F}}\cdot\det\boldsymbol{\Gamma}_{EX}}{\det\boldsymbol{\Gamma}_{\tilde{V}\tilde{F}}\cdot\det\Gamma_{BX}\cdot\det\Gamma_{E\tilde{F}}} \tag{16}$$

证明

（1）速率 R

由式（7）可得 $R\geq I(V;F|B)$，其中 $I(V;F|B)=\frac{1}{2}\log_2\frac{\mathrm{var}[F|B]}{\mathrm{var}[F|V]}=\frac{1}{2}\log_2\frac{\mathrm{var}[F|B]}{\mathrm{var}[F|V]}$. 因 $\mathrm{var}[F|B]=\frac{\det\boldsymbol{\Gamma}_{FB}}{\mathrm{var}[B]}$，$\mathrm{var}[F|V]=\frac{\det\boldsymbol{\Gamma}_{FV}}{\mathrm{var}[V]}$，所以 $R\geq\frac{1}{2}\log_2\frac{\det\boldsymbol{\Gamma}_{FB}\cdot\mathrm{var}[V]}{\det\boldsymbol{\Gamma}_{FV}\cdot\mathrm{var}[B]}$.

（2）失真 D

根据文献[16]可得 $\mathrm{E}(X-\hat{X}^2)\geq\frac{1}{2\pi\mathrm{e}}\cdot2^{2h(X)}$，因此 $\mathrm{E}[d(X,\hat{X}(\bar{V},B,Y))]\geq\frac{2^{2h(X|\bar{V}BY)}}{2\pi\mathrm{e}}$，$D\geq\frac{2^{2h(X|\bar{V}BY)}}{2\pi\mathrm{e}}$，其中 $h(X|\bar{V}BY)=\frac{1}{2}\log_2\frac{\det\boldsymbol{\Gamma}_{XBY}\det\boldsymbol{\Gamma}_{\bar{V}XY}}{\det\boldsymbol{\Gamma}_{\bar{V}BY}\mathrm{var}[XY]}$，因此可得 $D\geq\frac{\det\boldsymbol{\Gamma}_{XBY}\cdot\det\boldsymbol{\Gamma}_{\bar{V}XY}}{2\pi\mathrm{e}\cdot\det\boldsymbol{\Gamma}_{\bar{V}BY}\cdot\mathrm{var}[XY]}$.

（3）信源估计的最小均方误差 $I_{\mathcal{DE}}$

由式(8)可得

$$\begin{aligned}I_{\mathrm{e}}&\geq I(X;\tilde{V},\tilde{F},B)-I(X;B|\tilde{U},\tilde{F})+I(X;E|\tilde{U},\tilde{F})\\&=[h(X)-h(\tilde{F}|X)]+[h(\tilde{F})-h(X)]\\&\quad+[h(\tilde{V}|\tilde{F})-h(\tilde{V}|X)]-[h(B|\tilde{F})-h(B|X)]\\&\quad+[h(E|\tilde{F})-h(E|X)]\end{aligned}$$

因此

$$I_{\mathcal{DE}}\leq\frac{\det\boldsymbol{\Gamma}_{\bar{F}X}\cdot\det\boldsymbol{\Gamma}_{\bar{V}X}\cdot\det\boldsymbol{\Gamma}_{B\tilde{F}}\cdot\det\boldsymbol{\Gamma}_{EX}}{\det\boldsymbol{\Gamma}_{\tilde{V}\tilde{F}}\cdot\det\boldsymbol{\Gamma}_{BX}\cdot\det\boldsymbol{\Gamma}_{E\tilde{F}}}.$$

证毕.

5.3 实验和分析

本节对本文提出的系统模型及其编解码机制的安全性和可靠性进行仿真. 仿真中所有信道为独立同分布的衰落信道且服从均值为0和方差为1的高斯分布. 合法接收者和窃听者分别观测到的噪声功率是 P_b 和 P_e，合法信道的加性高斯信道噪声功率为 P_y，窃听信道噪声功率为 P_z，信道平均输入功率约束为 P，最优信道状态功率 P_s^* 根据式(11)计算得出.

根据构造的高斯噪声窃听信道模型和编码机制，选取以下随机变量

$$U=\varnothing \tag{17}$$

$$V=X+\alpha S^*-\gamma N \tag{18}$$

$$F=(\alpha X+\beta S^*-\gamma N)\sqrt{P} \tag{19}$$

其中，$\alpha\in(0,1]$，$\beta\in(0,1]$，$\gamma=\sqrt{1-\alpha^2-\beta^2}$，$\mathrm{var}[X]\leq P$，随机变量之间的相互关系如图2所示.

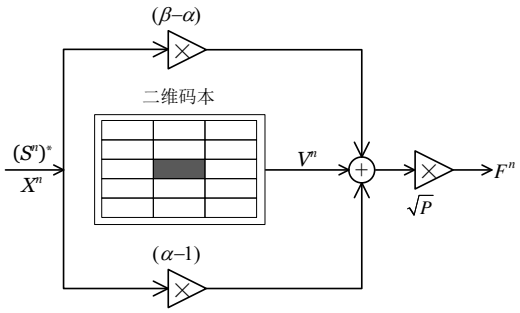

图2 随机变量之间的相互关系

函数关系可表示为

$$F=[(\alpha-1)X+(\beta-\alpha)S^*+V]\sqrt{P} \tag{20}$$

$$\bar{V}=g_1(X+\alpha S^*-\gamma N)+N_1 \tag{21}$$

$$\bar{F}=g_1[(\alpha-1)X+(\beta-\alpha)S^*+V]\sqrt{P}+N_1 \tag{22}$$

$$\tilde{V}=g_2(X+\alpha S^*-\gamma N)+N_2 \tag{23}$$

$$\tilde{F}=g_2[(\alpha-1)X+(\beta-\alpha)S^*+V]\sqrt{P}+N_2 \tag{24}$$

令信道增益 $g_1=g_2=1$，根据等式 $\gamma=\sqrt{1-\alpha^2-\beta^2}$ 得到 R、D 和 $I_{\mathcal{DE}}$ 的上下界关于 α 和 β 的表达式，然后对 R、D 和 $I_{\mathcal{DE}}$ 定界后分情况进行实验和分析.

（1）R 的下界

$R\geq\frac{1}{2}\log_2\frac{\mathrm{var}[F|B]}{\mathrm{var}[F|V]}$，其中 $\mathrm{var}[F|B]=\frac{\det\boldsymbol{\Gamma}_{FB}}{\mathrm{var}[B]}$，

$\boldsymbol{\Gamma}_{FB}=\begin{pmatrix}P(\beta^2P_s^*-\beta^2+1) & \alpha\sqrt{P}\\ \alpha\sqrt{P} & 1+P+P_b\end{pmatrix}$，可得

$\mathrm{var}[F|B]=\frac{P[\alpha^2(P+P_b)+(\beta^2P_s^*+1)(1+P+P_b)]}{1+P+P_b}$.

同样由 $\mathrm{var}[F|V]=\frac{\det\boldsymbol{\Gamma}_{FV}}{\mathrm{var}[V]}$，其中，

$\boldsymbol{\Gamma}_{FV}=\begin{pmatrix}P(\beta^2P_s^*-\beta^2+1) & \sqrt{P}(\alpha+\beta+1)\\ \sqrt{P}(\alpha+\beta P_s^*+1) & 1+\alpha P_s^*\end{pmatrix}$，可得

$\mathrm{var}[F|V]=P[(\beta^2P_s^*-\beta^2+1)-(\alpha+\beta P_s^*+1)^2]$.

最后得出 R 的下界关于 α 和 β 的表达式.

（2）D 的下界

$$D\geq\frac{\det\boldsymbol{\Gamma}_{XBY}\cdot\det\boldsymbol{\Gamma}_{\bar{V}XY}}{2\pi\mathrm{e}\cdot\det\boldsymbol{\Gamma}_{\bar{V}BY}\cdot\mathrm{var}[XY]},$$

其中，根据式(17)~(19)可得

$$\boldsymbol{\Gamma}_{XBY}=\begin{pmatrix}1 & 1 & (\alpha-1)\sqrt{P}\\ 1 & 1+P+P_b & \alpha\sqrt{P}\\ (\alpha-1)\sqrt{P} & \alpha\sqrt{P} & P+P_y\end{pmatrix}.$$

根据式(19)和(20)可得

$$\boldsymbol{\Gamma}_{\bar{V}XY}=\begin{pmatrix}1+\alpha P_s^*+P_y & 1 & (\alpha+\beta P_s^*+1)\sqrt{P}\\ 1 & 1 & \alpha\sqrt{P}\\ (\alpha+\beta P_s^*+1)\sqrt{P} & \alpha\sqrt{P} & P+P_y\end{pmatrix}$$

其中,根据式(19)可得

$$\begin{aligned}&\mathrm{E}[(\bar{V}-\mathrm{E}(\bar{V}))(Y-\mathrm{E}(Y))]=\mathrm{E}(\bar{V}Y)=\mathrm{E}(\bar{V}F)\\&=[\alpha\mathrm{E}(\bar{V}X)+\beta\mathrm{E}(\bar{V}S)-\mathrm{var}(\bar{V})]\sqrt{P}\\&=(\alpha+\beta P_s^*+1)\sqrt{P}.\end{aligned}$$

根据式(17)和(20)可得

$$\boldsymbol{\Gamma}_{\bar{V}BY}=\begin{pmatrix}1+\alpha P_s^*+P_y & 1 & (\alpha+\beta P_s^*+1)\sqrt{P}\\ 1 & 1+P+P_b & \alpha\sqrt{P}\\ (\alpha+\beta P_s^*+1)\sqrt{P} & \alpha\sqrt{P} & P+P_y\end{pmatrix}.$$

最后得出D的下界关于α和β的表达式.

(3) $I_{\mathcal{DE}}$的上界

$$I_{\mathcal{DE}}\le\frac{\det\boldsymbol{\Gamma}_{\bar{F}X}\cdot\det\boldsymbol{\Gamma}_{\bar{V}X}\cdot\det\boldsymbol{\Gamma}_{B\tilde{F}}\cdot\det\boldsymbol{\Gamma}_{EX}}{\det\boldsymbol{\Gamma}_{\tilde{V}\tilde{F}}\cdot\det\boldsymbol{\Gamma}_{BX}\cdot\det\boldsymbol{\Gamma}_{E\tilde{F}}},$$

其中$\boldsymbol{\Gamma}_{\tilde{V}\tilde{F}}=\begin{pmatrix}1+\alpha P_s^* & \sqrt{P}\,(\alpha+\beta P_s^*+1)\\ \sqrt{P}\,(\alpha+\beta P_s^*+1) & P(\beta^2P_s^*-\beta^2+1)+P_z\end{pmatrix}$,同理可得不等式中其余矩阵的行列式,最后得出$I_{\mathcal{DE}}$的上界关于$\alpha$和$\beta$的表达式.

本节将根据合法信道与窃听信道噪声功率的不同以及合法接收者与窃听者边信息传输时噪声功率不同划分为表1所示的4种情况,然后分析本文方案在不同情况下的速率、失真、泄露率和模糊率. 其中,情况1表示Bob比Eve的信道噪声小且Bob边信息的噪声比Eve小,信道状态功率取最优值P_s^*,是合法接收者相对于窃听者的最优条件. 其余3种情况为非最优条件,信道状态功率也取相应的最优值P_s^*.

表1　不同噪声功率条件下划分的4种情况

	$P_b<P_e$	$P_b>P_e$
$P_y<P_z$	情况1	情况2
$P_y>P_z$	情况3	情况4

根据表1考虑噪声功率不同的4种情况,将各种情况下的数据代入化简得到的表达式中,速率R,失真D,信源估计的最小均方误差$I_{\mathcal{DE}}$和模糊率Δ的单位是bit/source-bit. 本节将寻找速率-失真-信源估计的最小均方误差三者之间的最优权衡点转化为目标值W最大化的优化问题,优化问题表述如下:

$$\begin{aligned}&\max_{\alpha,\beta}\ W=[\mathrm{atan}(R)+1/\mathrm{atan}(D)+\mathrm{atan}(I_{\mathcal{DE}})]^+\\&\text{s.t.}\qquad\alpha\in(0,1],\quad\beta\in(0,1].\end{aligned}\tag{25}$$

其中,atan()为反正切函数,$[x]^+$表示$\max\{0,x\}$.

情况1:Bob比Eve的信道噪声小且Bob边信息的噪声比Eve小. 令P_y=0.5,P_z=1,P_b=0.5,P_e=1,P=1.

情况2:Bob比Eve的信道噪声小但Bob边信息的噪声比Eve大. 令P_y=0.5,P_z=1,P_b=1,P_e=0.5,P=1.

情况3:Bob比Eve的信道噪声大但Bob边信息的噪声比Eve小. 令P_y=1,P_z=0.5,P_b=0.5,P_e=1,P=1.

情况4:Bob比Eve的信道噪声大且Bob边信息的噪声比Eve大. 令P_y=1,P_z=0.5,P_b=1,P_e=0.5,P=1.

图3描绘了情况1下目标值W与α和β的函数关系,最优权衡在α=0.1,β=0.9,γ=0.43时取得,此时最大目标值为196.9906,速率为0.7601 bit/source-bit,失真为0.0051 bit/source-bit,信源估计的最小均方误差为0.8427 bit/source-bit.

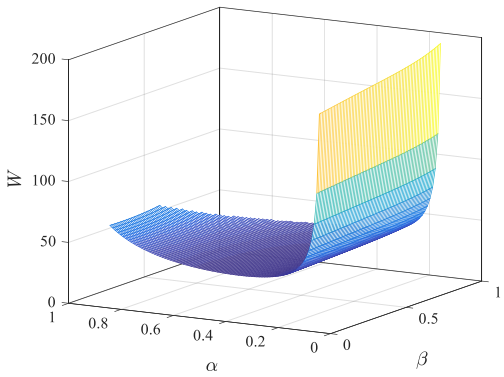

图3　情况1:传输信道噪声小且边信息噪声小

图4描绘了情况2下目标值W与α和β的函数关系,最优权衡点在α=0.9,β=0.1,γ=0.43时取得,此时最大目标值为51.1407,速率为0.6305 bit/source-bit,失真为0.0198 bit/source-bit,信源估计的最小均方误差为0.7202 bit/source-bit.

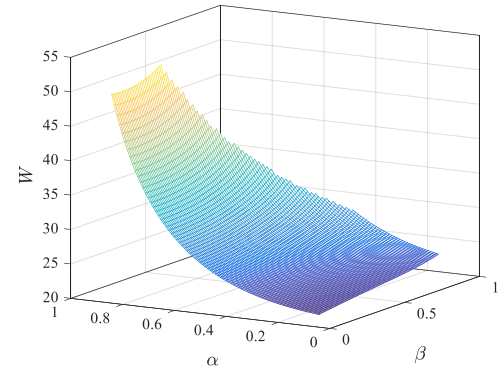

图4　情况2:传输信道噪声小但边信息噪声大

图5描绘了情况3下目标值W与α和β的函数关系，最优权衡点在α=0.9，β=0.1，γ=0.43时取得，此时最大目标值为34.6518，速率为0.3285 bit/source-bit，失真为0.0306 bit/source-bit，信源估计的最小均方误差为1.2815 bit/source-bit.

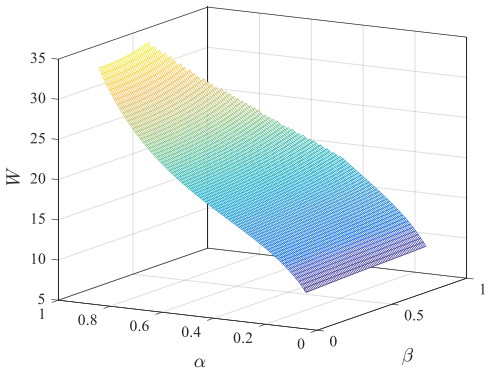

图5 情况3:传输信道噪声大但边信息噪声小

图6描绘了情况4的目标值W与α和β的函数关系，最优权衡点在α=0.9，β=0.1，γ=0.43时取得，此时最大目标值为29.2453，速率为0.3998 bit/source-bit，失真为0.0367 bit/source-bit，信源估计的最小均方误差为1.2079 bit/source-bit.

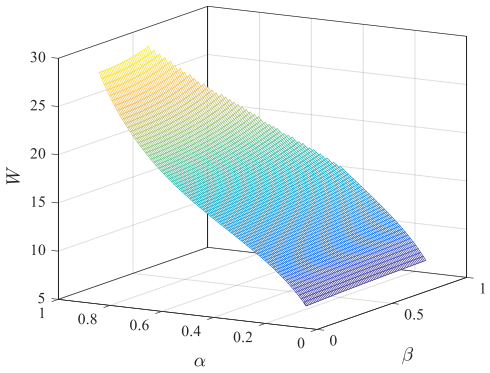

图6 情况4:传输信道噪声大且边信息噪声大

进一步，分析本文方案在以上4种情况下模糊率的变化情况. 图7描绘的是在情况1下模糊率关于α和β的变化情况. 当α=0.15，β=0.42，γ=0.8950时，窃听者对信源的模糊率最高，达到0.1410 bit/source-bit.

图8描绘了情况2下模糊率关于α和β的变化情况. 当α=0.15，β=0.42，γ=0.8950时，窃听者对信源的模糊率最高，达到0.1357 bit/source-bit.

图9描绘了情况3下模糊率关于α和β的变化情况. 当α=0.32，β=0.61，γ=0.7249时，窃听者对信源的模糊率最高，达到0.1996 bit/source-bit.

图10描绘了情况4下模糊率关于α和β的变化情况. 当α=0.32，β=0.61，γ=0.7249时，窃听者对信源的模糊率最高，达到0.1945 bit/source-bit.

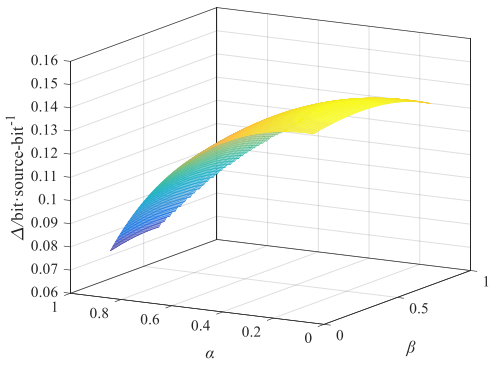

图7 情况1下的模糊率

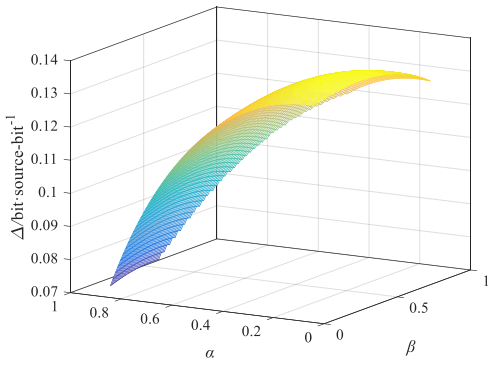

图8 情况2下的模糊率

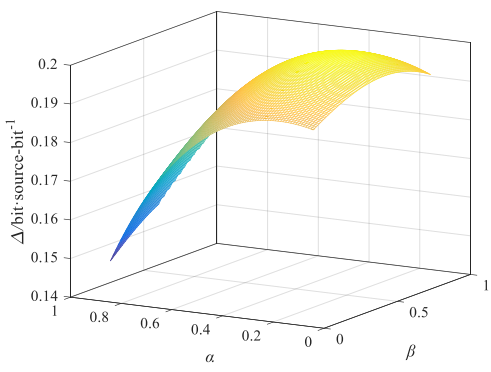

图9 情况3下的模糊率

综合以上实验结果可以得出：在最优条件下，即Bob比Eve的信道噪声小且Bob边信息的噪声比Eve小，所得目标值达到4种情况下的最大值，速率最大且失真最小，根据信源估计的最小均方误差推算出信息泄漏率为0.1277 bit/source-bit，所得结果比文献[10]中所提出的安全有损信源传输方案中的速率高，比其所得的失真低；信源估计的最小均方误差比文献[11]所提出的最优方案得出的值高. 利用速率和失真来衡量其可靠性，信源估计的最小均方误差来衡量其安全性，

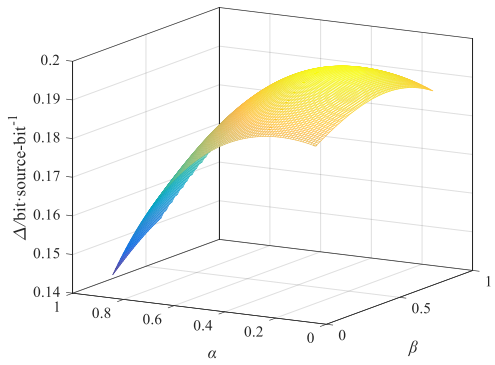

图 10　情况 4 下的模糊率

对比可得本文所提出的传输模型及其编解码方案具有更好的安全性和可靠性.

在非最优条件下,例如第 2 种情况,Bob 比 Eve 的信道噪声小,但 Bob 边信息的噪声比 Eve 大时,速率和信源估计的最小均方误差都减小且失真增大;情况 3 和情况 4 下,目标值都相对减小,但情况 4 的目标值最小,因此本文方案在情况 4 下性能最差. 进一步分析可得边信息的噪声功率对有限码率约束域的影响比信道噪声的影响小. 此外,在情况 3 下,即传输信道噪声大但边信息噪声小时,模糊率最高可达 0.1996 bit/source-bit. 其它 3 种情况下的模糊率也比文献[10]所提方案的模糊率 0.1330 bit/source-bit 要高,原因是利用双分簇技术构造的二维码本进行编解码时码字具有更高的隐蔽性.

6　结论

本文构建了窃听信道下具有边信息和状态信息的信源安全有损传输模型,根据该模型设计了基于双分簇技术的编解码机制,并推导出传输速率-失真-信息泄露率这三个有限码率约束的下界. 随后考虑现实噪声问题,分析了该模型下的高斯噪声窃听信道. 仿真实验结果表明当合法信道比窃听信道噪声功率小且合法接收者比窃听者的边信息噪声小时,传输速率-失真-信息泄露率之间的权衡最优,此时速率为 0.7601 bit/source-bit,失真为 0.0051 bit/source-bit,信息泄露率为 0.1277 bit/source-bit. 在非最优条件下,当传输信道噪声大但边信息噪声小时所提方案可以达到更高的模糊率.

参考文献

[1] BIGGIO B, FUMERA G, RUSSU P, et al. Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective[J]. IEEE Signal Processing Magazine, 2015, 32(5): 31-41.

[2] 张明, 王景璟, 马骏, 等. 从智能支架看植入式医疗电子的发展[J]. 电子学报, 2021, 49(7): 1406-1416.
ZHANG M, WANG J J, MA J, et al. Discussion on the new generation of vascular stent from the development of implantable medical devices[J]. Acta Electronica Sinica, 2021, 49(7): 1406-1416. (in Chinese)

[3] 梁永生, 柳伟, 周莺, 等. 基于视觉显著计算的视频流媒体渐进式表达方法[J]. 电子学报, 2017, 45(7): 1567-1575.
LIANG Y S, LIU W, ZHOU Y, et al. An approach to progressive description of video streaming based on visual saliency computation[J]. Acta Electronica Sinica, 2017, 45(7): 1567-1575. (in Chinese)

[4] AL-JALJOULI R, ABAWAJY J, HASSAN M M, et al. Secure multi-attribute one-to-many bilateral negotiation framework for E-commerce[J]. IEEE Transactions on Services Computing, 2018, 11(2): 415-429.

[5] SHANNON C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[6] WYNER A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[7] CSISZAR I, KORNER J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory, 1978, 24(3): 339-348.

[8] WYNER A, ZIV J. The rate-distortion function for source coding with side information at the decoder[J]. IEEE Transactions on Information Theory, 1976, 22(1): 1-10.

[9] CHIA Y K, CHONG H F. On lossy source coding with side information under the erasure distortion measure[J]. IEEE Transactions on Information Theory, 2015, 61(12): 6475-6484.

[10] VILLARD J, PIANTANIDA P. Secure lossy source coding with side information at the decoders[C]//2010 48th Annual Allerton Conference on Communication, Control, and Computing(Allerton). Piscataway: IEEE, 2010: 733-739.

[11] KOYLUOGLU O O, SOUNDARARAJAN R, VISHWANATH S. State amplification subject to masking constraints[J]. IEEE Transactions on Information Theory, 2016, 62(11): 6233-6250.

[12] HAN T S, SASAKI M. Wiretap channels with causal state information: Strong secrecy[J]. IEEE Transactions on Information Theory, 2019, 65(10): 6750-6765.

[13] GAMAL A A EL, KIM Y H. Network Information Theory[M]. Cambridge, UK: Cambridge University Press, 2011.

[14] GÜNLÜ O, KITTICHOKECHAI K, SCHAEFER R F, et al. Controllable identifier measurements for private authentication with secret keys[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 1945-1959.
[15] VILLARD J, PIANTANIDA P, SHAMAI S. Secure transmission of sources over noisy channels with side information at the receivers[J]. IEEE Transactions on Information Theory, 2014, 60(1): 713-739.
[16] COVER T M, THOMAS J A. Elements of Information Theory[M]. 2nd ed. Hoboken, NJ: Wiley-Interscience, 2006.

作者简介

徐 明 男,1977年出生,安徽省马鞍山人. 现为上海海事大学信息工程学院副教授,主要研究方向为网络与信息安全.
E-mail: mingxu@shmtu.edu.cn

胡沐宇 女,1995年出生,江苏南通人. 现为上海海事大学信息工程学院硕士研究生,主要研究方向为网络与信息安全.
E-mail: muyu.hu@foxmail.com