第 46 卷 第 12 期 计 算 机 工 程 2020 年 12 月
Vol. 46 No. 12 Computer Engineering December 2020

·网络空间安全· 文章编号：1000-3428(2020)12-0120-07 文献标志码：A 中图分类号：TP309

高斯矢量多路输入信道下的消息认证方案

韩佳良，徐 明

（上海海事大学 信息工程学院，上海 201306）

摘 要： 消息认证可使消息接收者检测消息是否被合法发送者之外的其他人伪造或非法修改，而传统消息认证方案通常在网络层或更高层上执行，容易遭受重放攻击、拒绝服务攻击等安全威胁。在分析基于物理层的消息认证方案基础上，构建高斯矢量多路输入信道模型。通过最小均方误差法进行信道估计，提出消息认证方案并制定敌手的最优攻击策略，同时根据敌手攻击成功的概率确定可达的保密边界。在信道传输功率一定的情况下，通过信息论分析信道的最大安全认证速率，得到信道的保密容量区域。实验结果表明，随着接收消息数的增加，敌手攻击成功的概率均值呈指数级下降，且当所有发送者与窃听方的空间相关系数均低于 0.3 时，敌手攻击成功的概率均值小于1.87×10^{-7}，验证了该方案的安全性。

关键词： 高斯矢量多路输入信道；消息认证；假设检验；最优攻击策略；保密容量

开放科学(资源服务)标志码(OSID)：

中文引用格式： 韩佳良，徐明. 高斯矢量多路输入信道下的消息认证方案[J]. 计算机工程，2020，46(12)：120-126.

英文引用格式： HAN Jialiang，XU Ming. Message authentication scheme under Gaussian vector multiple-input channels[J]. Computer Engineering，2020，46(12)：120-126.

Message Authentication Scheme Under Gaussian Vector Multiple-Input Channels

HAN Jialiang，XU Ming

（College of Information Engineering，Shanghai Maritime University，Shanghai 201306，China）

【Abstract】 Message authentication allows the receiver of a message to detect whether the message is forged or illegally modified by someone other than the legitimate sender. Traditional message authentication schemes are typically implemented at the network layer or higher，which are vulnerable to security threats such as replay attacks，denial of service attacks and so forth. Based on the existing schemes based on the physical layer，this paper proposes a message authentication scheme using the Minimum Mean Square Error（MMSE）method for estimation of channels under the Gaussian vector multiple-input channel model. An optimal attack strategy for the eavesdropper is also formulated，and determines the reachable secrecy boundary according to the probabilities of successful attacks of the eavesdropper. By using the information theory to analyze the maximum security authentication rate of the channel，the secrecy capacity domain of the channel is obtained. Experimental results show that the average probability of successful attack of the eavesdropper decreases exponentially with the increased number of received messages. When the spatial correlation coefficients between all senders and the eavesdropper are lower than 0.3，the average probability of successful attack of the eavesdropper is less than 1.87×10^{-7}，which verifies the security of the proposed scheme.

【Key words】 Gaussian vector multiple-input channel；message authentication；hypothesis testing；optimal attack strategy；secrecy capacity

DOI： 10.19678/j.issn.1000-3428.0056745

0 概述

高斯矢量多路输入信道是多个发送者分别独立地将包括时间、频率和空间的三维矢量信息传输给一个接收者，且信道传输概率分布为高斯分布的信道，适用于蜂窝通信的上行链路、局域网的介质接入及水声传感器网络的多址接入[1]。传统消息认证方案通常在网络层或更高层上执行，依赖于散列函数，

基金项目： 国家自然科学基金(61202370)。

作者简介： 韩佳良(1994—)，男，硕士研究生，主研方向为密码学、网络与信息安全；徐 明，副教授、博士。

收稿日期： 2019-11-28 **修回日期：** 2020-01-22 **E-mail：** aptx1234@qq.com

使得窃听方伪造或修改的消息无法复制正确的散列标记[2]。然而，此类消息认证方案会产生较大的计算开销，难以适应终端资源受限的情况，同时认证机制的安全性来自认证算法的计算复杂度。随着计算机性能的不断提升，传统消息认证方案可能会面临新的安全威胁，而基于物理层的消息认证方案可以快速拒绝非法消息，降低更高层认证协议的负担，并对阻止拒绝服务攻击特别有效[3-5]。高斯矢量多路输入信道下的消息认证方案是一种基于物理层的认证技术。本文在消息认证前先对信道状态信息进行估计，在宽频带和多径环境中利用精确的信道估计验证物理层消息源并保护消息完整性，而无需预先共享密钥，从而有效降低更高层认证协议的负担[6]，并且通过使用最小均方误差（Minimum Mean Square Error，MMSE）法对高斯矢量多路输入信道进行信道估计以减少信息量损耗。

1　相关研究

文献[7]提出基于物理层的消息认证方案，将认证信息与数据并发发送，无需额外的带宽或传输功率，并给出了时变信道误码率的改进方法。文献[8]提出一种增强的物理层认证方案，通过 Neyman-Pearson 假设检验和最小二乘自适应信道估计对突发事件中的后续帧进行认证。文献[9]基于物理层安全提出解码转发、放大转发和协同干扰 3 种协同方案来分配发射功率，使发射功率约束下的可达保密率实现最大化。文献[10]针对有敌手的多路输入信道，提出一种基于遗传算法的联合信道方案，并使用 Wyner 窃听编码对信息进行保密。文献[11]研究强保密条件下多址窃听信道上的安全通信问题，通过信道输出统计逼近方法建立强安全性的多用户信道。文献[12]提出一种基于可靠度混合重传协议的物理层安全通信技术，与传统 HARQ 协议相比进一步提升了物理层通信安全。文献[13]对带有机密信息的离散无记忆多路输入信道模型进行推导，得到不确定容量区域和保密容量区域。文献[14]推导出多路输入衰退信道下的中断容量区域，获得每个衰落状态下的最优译码顺序和功率分配。文献[15]研究点到点的多天线安全通信方法，使用信号与干扰加噪声比（Signal to Interference plus Noise Ratio，SINR）作为性能度量，提出不完美信道状态下的安全通信方案。文献[16]基于高斯矢量广播信道将最优预编码结构与广义决策反馈均衡器相对应，在发送端对高斯信道采用预编码策略获得总容量。

以上工作主要研究点到点的物理层消息认证方案，提出多路输入信道上的安全联合信道编码和基于该信道的消息认证算法，并计算高斯矢量广播信道的总容量及推导不同条件下多路输入信道的保密容量区域，而高斯矢量多路输入信道下的消息认证以及该信道下的保密容量区域定界仍有待进一步研究。

2　消息认证方案

2.1　基本定义

定义 1　如果一个高斯矢量信道上有 $k(k\geqslant 2)$ 个发送节点将消息相互独立地传输给一个接收节点，则称其为高斯矢量多路输入信道[17]。

设高斯矢量多路输入信道模型为：

$$\boldsymbol{y}=\boldsymbol{G}_1\boldsymbol{x}_1+\boldsymbol{G}_2\boldsymbol{x}_2+\boldsymbol{w}_1 \tag{1}$$

其中，$\boldsymbol{y}$ 为 n 维输出矢量，$\boldsymbol{x}_1$、$\boldsymbol{x}_2$ 为 m 维输入矢量，$\boldsymbol{G}_1$、$\boldsymbol{G}_2$ 为 $n\times m$ 维信道增益矩阵，$\boldsymbol{w}_1\sim \mathrm{CN}(\boldsymbol{0}_{n\times 1},\boldsymbol{K}_{w_1})$ 为 n 维噪声矢量，$\boldsymbol{K}_{w_1}$ 为噪声矢量信号 $\boldsymbol{w}_1$ 的协方差矩阵。

假设在如式(1)所示的信道模型中存在一个敌手 Eve，则关于 Eve 的窃听信道模型为：

$$\boldsymbol{z}=\boldsymbol{G}_3\boldsymbol{x}_1+\boldsymbol{G}_4\boldsymbol{x}_2+\boldsymbol{w}_2 \tag{2}$$

其中，$\boldsymbol{G}_3$、$\boldsymbol{G}_4$ 为 $n\times m$ 维信道增益矩阵，$\boldsymbol{w}_2\sim \mathrm{CN}(\boldsymbol{0}_{n\times 1},\boldsymbol{K}_{w_2})$ 为 n 维噪声矢量，$\boldsymbol{K}_{w_2}$ 为噪声矢量信号 $\boldsymbol{w}_2$ 的协方差矩阵。

假设每个发送节点都可以访问多个平坦衰落信道，并在复高斯矢量 $\boldsymbol{g}$ 中收集每个信道的衰落系数，同时对有 M 根发射天线和 N 根接收天线的平坦衰落信道矩阵 $\boldsymbol{G}$，用矢量 $\boldsymbol{g}$ 表示为：

$$\boldsymbol{g}=[[\boldsymbol{G}]_{0,0},[\boldsymbol{G}]_{1,1},\cdots,[\boldsymbol{G}]_{N-1,M-1}]^{\mathrm{T}} \tag{3}$$

如图 1 所示，A_1、A_2 与 Bob 间的信道估计可以用 α 维的矢量分别表示为：

$$\boldsymbol{g}_{\mathrm{A_1B}}\sim \mathrm{CN}(\boldsymbol{0}_{\alpha\times 1},\boldsymbol{R}_{\mathrm{A_1B}}) \tag{4}$$

$$\boldsymbol{g}_{\mathrm{A_2B}}\sim \mathrm{CN}(\boldsymbol{0}_{\alpha\times 1},\boldsymbol{R}_{\mathrm{A_2B}}) \tag{5}$$

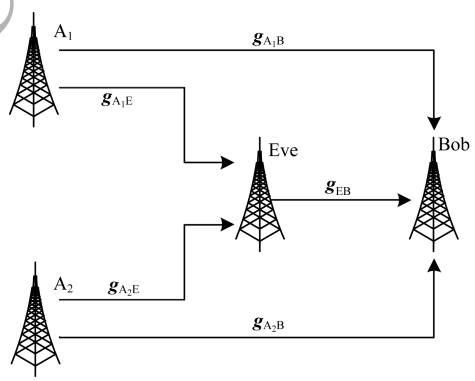

图 1　高斯矢量多路输入窃听信道模型

Fig. 1　Eavesdropping channel model of Gaussian vector multiple-input

同样地，A_1、A_2 与 Eve 间的信道用 β 维的矢量分别表示为：

$$\boldsymbol{g}_{\mathrm{A_1E}}\sim \mathrm{CN}(\boldsymbol{0}_{\beta\times 1},\boldsymbol{R}_{\mathrm{A_1E}}) \tag{6}$$

$$\boldsymbol{g}_{\mathrm{A_2E}}\sim \mathrm{CN}(\boldsymbol{0}_{\beta\times 1},\boldsymbol{R}_{\mathrm{A_2E}}) \tag{7}$$

Eve 与 Bob 间的信道用 γ 维的矢量表示为：

$$\boldsymbol{g}_{\mathrm{EB}}\sim \mathrm{CN}(\boldsymbol{0}_{\gamma\times 1},\boldsymbol{R}_{\mathrm{EB}}) \tag{8}$$

通过对高斯矢量多路输入信道进行最小均方误差估计,可以得到由 A_1、A_2、Bob 和 Eve 中任意两方构成的信道 X、Y 对应的协方差矩阵如式(9)所示,例如 $E[\boldsymbol{g}_{A_1B}\boldsymbol{g}_{A_1E}]=\boldsymbol{R}_{A_1B,A_1E}$。

$$E[\boldsymbol{g}_X\boldsymbol{g}_Y]=\boldsymbol{R}_{X,Y} \tag{9}$$

定义 2 信道容量 C 是在输入 $\boldsymbol{x}$ 和输出 $\boldsymbol{y}$ 的消息传输系统下,概率分布函数满足 $\sum p(\boldsymbol{y}|\boldsymbol{x})=1$ 时选择不同的概率分布 $p(\boldsymbol{y}|\boldsymbol{x})$ 求得 $I(\boldsymbol{x};\boldsymbol{y})$ 最大值,即[18]:

$$C=\max_{p(\boldsymbol{x})} \boldsymbol{I}(\boldsymbol{x};\boldsymbol{y}) \tag{10}$$

2.2 消息认证方案描述

本文提出一个高斯矢量多路输入信道下的消息认证方案,具体分为 3 个阶段:

1)A_1、A_2 分别发送给 Bob 一个训练序列,假设其能被完美验证,最初的传输可以使 Bob 获得关于 A_1、A_2 的参考估计信道 $\hat{\boldsymbol{g}}_{A_1B}$、$\hat{\boldsymbol{g}}_{A_2B}$,则根据上文假设得到:

$$\hat{\boldsymbol{g}}_{A_1B}=\boldsymbol{g}_{A_1B}e^{j\Phi_1}+\boldsymbol{w}_1 \tag{11}$$

$$\hat{\boldsymbol{g}}_{A_2B}=\boldsymbol{g}_{A_2B}e^{j\Phi_2}+\boldsymbol{w}_2 \tag{12}$$

其中,$\boldsymbol{w}_1\sim CN(\boldsymbol{0}_{\alpha\times1},\sigma_1^2\boldsymbol{I}_\alpha)$,$\boldsymbol{w}_2\sim CN(\boldsymbol{0}_{\alpha\times1},\sigma_2^2\boldsymbol{I}_\alpha)$。

2)A_1、A_2 将 (M_1,K_1)、(M_2,K_2) 编码为 $\boldsymbol{x}_1$、$\boldsymbol{x}_2$,在 t 时刻将相互独立的信道输入 $\boldsymbol{x}_1$、$\boldsymbol{x}_2$ 传输给 Bob,此时 A_1、A_2 与 Bob 的信道矢量分别为:

$$\hat{\boldsymbol{g}}_1(t)=\boldsymbol{g}_{A_1B}(t)e^{j\Phi_1}+\boldsymbol{w}_3(t) \tag{13}$$

$$\hat{\boldsymbol{g}}_2(t)=\boldsymbol{g}_{A_2B}(t)e^{j\Phi_2}+\boldsymbol{w}_4(t) \tag{14}$$

其中,$\boldsymbol{w}_3(t)\sim CN(\boldsymbol{0}_{\alpha\times1},\sigma_3^2\boldsymbol{I}_\alpha)$,$\boldsymbol{w}_4(t)\sim CN(\boldsymbol{0}_{\alpha\times1},\sigma_4^2\boldsymbol{I}_\alpha)$。

3)Bob 接收数据包 $\boldsymbol{y}$ 进行解码并对其来源进行认证,该阶段可能重复多次,通过比较当前消息执行的信道估计值 $\hat{\boldsymbol{g}}_1(t)$、$\hat{\boldsymbol{g}}_2(t)$ 与第 1 个阶段中获得的参考估计值 $\hat{\boldsymbol{g}}_{A_1B}$、$\hat{\boldsymbol{g}}_{A_2B}$ 来进行认证,其中每一次传输 $t\in[1,a]$ 对 $\boldsymbol{x}_1$、$\boldsymbol{x}_2$ 中每个码字 $\boldsymbol{x}_1(m,t)$、$\boldsymbol{x}_2(m,t)$ 存在的平均传输功率约束设为 P,则有:

$$\sum_{t=1}^{a}[\boldsymbol{x}_1^{\mathrm{T}}(m,t)\boldsymbol{x}_1(m,t)+\boldsymbol{x}_2^{\mathrm{T}}(m,t)\boldsymbol{x}_2(m,t)]\leqslant aP \tag{15}$$

2.3 安全性检验

在第 2 个阶段,Eve 可以估计信道并向 Bob 发送伪造的消息进行攻击。假设 Eve 已知以下信息:1)调制方案;2)Bob 采用的信道估计技术;3)所有信道统计量,尤其是相关矩阵;4)$\boldsymbol{g}_{A_1B}$、$\boldsymbol{g}_{A_2B}$ 和 $\boldsymbol{g}_{EB}$ 的可靠估计。

Eve 处理信号的目的是修改 Bob 执行的信道估计。令 $\boldsymbol{h}$ 表示 Eve 预处理信道 $\boldsymbol{g}_{EB}$ 后得到的等效信道,如果在 t 时刻 Bob 接收到 Eve 伪造 A_1 或 A_2 的身份发送的消息,则有:

$$\hat{\boldsymbol{g}}_1(t)=\boldsymbol{h}_1(t)+\boldsymbol{w}_3(t) \tag{16}$$

$$\hat{\boldsymbol{g}}_2(t)=\boldsymbol{h}_2(t)+\boldsymbol{w}_4(t) \tag{17}$$

一个安全的消息认证方案需要满足以下条件:

1)Bob 经过认证拒绝接收从 A_1 或 A_2 发送来消息的概率为 $P_R\leqslant e^{-\varepsilon i}$,其中,$\varepsilon>0$,$i$ 是窃听信道 $(\boldsymbol{g}_{A_1E}\boldsymbol{g}_{A_2E})$ 的使用次数。

2)Bob 经过认证接收从 EVE 发送来消息的概率 P_A,其对于 i 可以忽略不计。

为验证消息的安全性,Bob 使用假设检验[19]方式验证消息来源,其中,H_0 表示消息来自 A_1 和 A_2,H_1 表示消息不来自 A_1 或 A_2。

本文将检验统计量设为:

$$J=\min_{\Phi_1,\Phi_2}\frac{1}{\sigma^2}\left(\sum_{n=0}^{\alpha-1}|\boldsymbol{h}_1-\hat{\boldsymbol{g}}_{A_1B}e^{j\Phi_1}|^2+\sum_{n=0}^{\alpha-1}|\boldsymbol{h}_2-\hat{\boldsymbol{g}}_{A_2B}e^{j\Phi_2}|^2\right) \tag{18}$$

令 Φ_1、Φ_2 最小化可以减小 P_R 的发生概率,因此 Φ_1、Φ_2 可以取到的最小值分别为:

$$\Phi_1^*=\arg\left(\sum_{n=0}^{\alpha-1}\boldsymbol{h}_1\hat{\boldsymbol{g}}_{A_1B}^*\right) \tag{19}$$

$$\Phi_2^*=\arg\left(\sum_{n=0}^{\alpha-1}\boldsymbol{h}_2\hat{\boldsymbol{g}}_{A_2B}^*\right) \tag{20}$$

当消息来自 A_1、A_2 时,J 是自由度 χ 为 2α 的中心卡方随机变量:

$$J=\frac{1}{\sigma^2}\left(\sum_{n=0}^{\alpha-1}n_1^2+\sum_{n=0}^{\alpha-1}n_2^2\right)\sim\chi_{2\alpha,0}^2 \tag{21}$$

当消息来自 Eve 时,J 是自由度 χ 为 2α 的非中心卡方随机变量:

$$J=\frac{1}{\sigma^2}\left(\sum_{n=0}^{\alpha-1}(\Delta\boldsymbol{g}_1^*+n_1)^2+\sum_{n=0}^{\alpha-1}(\Delta\boldsymbol{g}_2^*+n_2)^2\right)\sim\chi_{2\alpha,\mu}^2 \tag{22}$$

其中,$\Delta\boldsymbol{g}_1^*$、$\Delta\boldsymbol{g}_2^*$ 分别为 $(\boldsymbol{h}_1-\hat{\boldsymbol{g}}_{A_1B}e^{j\Phi_1^*})$、$(\boldsymbol{h}_2-\hat{\boldsymbol{g}}_{A_2B}e^{j\Phi_2^*})$ 的实部,关于 J 的部分非中心系数为:

$$\mu=\frac{1}{\sigma^2}\left(\sum_{n=0}^{\alpha-1}|\boldsymbol{h}_1-\hat{\boldsymbol{g}}_{A_1B}e^{j\Phi_1^*}|^2+\sum_{n=0}^{\alpha-1}|\boldsymbol{h}_2-\hat{\boldsymbol{g}}_{A_2B}e^{j\Phi_2^*}|^2\right) \tag{23}$$

在拒绝域 H_0 条件下,令 $J<k$,k 是临界值,那么可得:

$$P_R=P_{H_0}(J>k)=1-F_{\chi_{2\alpha,0}^2}(k) \tag{24}$$

$$P_A=P_{H_0}(J\leqslant k)=F_{\chi_{2\alpha,\mu}^2}(k) \tag{25}$$

其中,F_X 是关于 X 的概率密度函数,进一步可得:

$$P_A=F_{\chi_{2\alpha,\mu_L}^2}\left(F_{\chi_{2\alpha,0}^2}^{-1}(1-P_R)\right) \tag{26}$$

3　敌手攻击策略与可达的保密边界

本节制定敌手对本文消息认证方案的最优攻击策略。假设 Eve 观察到 Bob 与 A_1、A_2 进行消息传输的信道估计分别为:

$$\hat{\boldsymbol{g}}_{A_1E}=\boldsymbol{g}_{A_1E}+\boldsymbol{w}_{A_1E} \tag{27}$$

$$\hat{\boldsymbol{g}}_{A_2E}=\boldsymbol{g}_{A_2E}+\boldsymbol{w}_{A_2E} \tag{28}$$

其中,$\boldsymbol{w}_{A_1E}\sim CN(\boldsymbol{0}_{\beta\times1},\sigma^2_{A_1E}\boldsymbol{I}_\beta)$,$\boldsymbol{w}_{A_2E}\sim CN(\boldsymbol{0}_{\beta\times1},\sigma^2_{A_2E}\boldsymbol{I}_\beta)$。

另外,假设 Eve 关于 Bob 的信道估计为:

$$\hat{\boldsymbol{g}}_{EB}=\boldsymbol{g}_{EB}+\boldsymbol{w}_{EB} \tag{29}$$

其中,$\boldsymbol{w}_{BE}\sim CN(\boldsymbol{0}_{\gamma\times1},\sigma^2_{EB}\boldsymbol{I}_\gamma)$。

通过讨论 $\boldsymbol{h}$ 的推导过程得出 Eve 的最优攻击策略,即 Eve 对认证方案攻击成功概率的最大值,并对敌手攻击成功的概率确定可达的保密边界。

$$\boldsymbol{R}_1=\begin{pmatrix}\boldsymbol{R}_{A_1B}+\sigma_1^2\boldsymbol{I}_\alpha & \boldsymbol{R}_{A_1B,A_2B} & \boldsymbol{R}_{A_1E,A_1B} & \boldsymbol{R}_{A_1E,A_2B} & \boldsymbol{R}_{A_1B,EB}\\ \boldsymbol{R}^*_{A_1B,A_2B} & \boldsymbol{R}_{A_2B}+\sigma_2^2\boldsymbol{I}_\alpha & \boldsymbol{R}_{A_2E,A_1B} & \boldsymbol{R}_{A_2E,A_2B} & \boldsymbol{R}_{A_2B,EB}\\ \boldsymbol{R}^*_{A_1E,A_1B} & \boldsymbol{R}^*_{A_2E,A_1B} & \boldsymbol{R}_{A_1E}+\sigma^2_{A_1E}\boldsymbol{I}_\beta & \boldsymbol{R}_{A_1E,A_2E} & \boldsymbol{R}_{A_1E,EB}\\ \boldsymbol{R}^*_{A_1E,A_2B} & \boldsymbol{R}^*_{A_2E,A_2B} & \boldsymbol{R}^*_{A_1E,A_2E} & \boldsymbol{R}_{A_2E}+\sigma^2_{A_2E}\boldsymbol{I}_\beta & \boldsymbol{R}_{A_2E,EB}\\ \boldsymbol{R}^*_{A_1B,EB} & \boldsymbol{R}^*_{A_2B,EB} & \boldsymbol{R}^*_{A_1E,EB} & \boldsymbol{R}^*_{A_2E,EB} & \boldsymbol{R}_{EB}+\sigma^2_{EB}\boldsymbol{I}_\gamma\end{pmatrix} \tag{31}$$

定义矢量 $\Delta=[\boldsymbol{a}_1^{\mathrm{T}},\boldsymbol{a}_2^{\mathrm{T}},\hat{\boldsymbol{g}}^{\mathrm{T}}_{A_1E},\hat{\boldsymbol{g}}^{\mathrm{T}}_{A_2E},\hat{\boldsymbol{g}}^{\mathrm{T}}_{EB}]^{\mathrm{T}}$,则:

$$\bar{\boldsymbol{h}}=\underset{a_1,a_2\in\mathbb{C}^\alpha}{\operatorname{argmax}}[P(\Delta|\hat{\boldsymbol{g}}_{A_1E},\hat{\boldsymbol{g}}_{EB})+P(\Delta|\hat{\boldsymbol{g}}_{A_2E},\hat{\boldsymbol{g}}_{EB})]=\underset{a_1,a_2\in\mathbb{C}^\alpha}{\operatorname{argmin}}\Delta^*\boldsymbol{R}^{-1}\Delta \tag{32}$$

再令 $\boldsymbol{S}=\boldsymbol{R}_1^{-1}$ 且用 $\boldsymbol{S}_{ij}$ 表示 $\boldsymbol{S}$ 中第 i 行、第 j 列的元素,则 $\bar{\boldsymbol{h}}$ 可改写为:

$$\bar{\boldsymbol{h}}=-\boldsymbol{S}_{11}(\boldsymbol{S}_{13}\hat{\boldsymbol{g}}_{A_1E}+\boldsymbol{S}_{15}\hat{\boldsymbol{g}}_{EB})-\boldsymbol{S}_{22}(\boldsymbol{S}_{24}\hat{\boldsymbol{g}}_{A_1E}+\boldsymbol{S}_{25}\hat{\boldsymbol{g}}_{EB}) \tag{33}$$

在 P_R 取最优解的情况下分析概率 P_A,令 $\alpha=\beta=\gamma=N$,那么得到:

$$\boldsymbol{R}'=\begin{pmatrix}\boldsymbol{\Lambda}+\sigma_1^2\boldsymbol{I}_\alpha & \boldsymbol{0} & \rho_{EB}\boldsymbol{\Lambda} & \boldsymbol{0} & \rho_{A_1E}\boldsymbol{\Lambda}\\ \boldsymbol{0} & \boldsymbol{\Lambda}+\sigma_2^2\boldsymbol{I}_\alpha & \boldsymbol{0} & \rho_{EB}\boldsymbol{\Lambda} & \rho_{A_2E}\boldsymbol{\Lambda}\\ \rho_{EB}\boldsymbol{\Lambda}^* & \boldsymbol{0} & \boldsymbol{\Lambda}+\sigma^2_{A_1E}\boldsymbol{I}_\beta & \boldsymbol{0} & \rho_{A_1B}\boldsymbol{\Lambda}\\ \boldsymbol{0} & \rho_{EB}\boldsymbol{\Lambda}^* & \boldsymbol{0} & \boldsymbol{\Lambda}+\sigma^2_{A_2E}\boldsymbol{I}_\beta & \rho_{A_2B}\boldsymbol{\Lambda}\\ \rho_{A_1E}\boldsymbol{\Lambda}^* & \rho_{A_2E}\boldsymbol{\Lambda}^* & \rho_{A_1B}\boldsymbol{\Lambda}^* & \rho_{A_2B}\boldsymbol{\Lambda}^* & \boldsymbol{\Lambda}+\sigma^2_{EB}\boldsymbol{I}_\gamma\end{pmatrix} \tag{34}$$

其中,$\boldsymbol{\Lambda}=\operatorname{diag}\{\lambda_0,\lambda_1,\cdots,\lambda_{N-1}\}$,$\rho_{XY}$为与 Z 相连节点 X、Y 的空间相关系数。

此时,对于第 n 个接收节点有:

$$\boldsymbol{w}_{A_1E}(n)=1+\frac{\sigma^2_{A_1E}}{\lambda_n} \tag{35}$$

3.1　敌手攻击策略

设 $\boldsymbol{S}$ 是 α 复数域的子集,并且 Bob 在信道估计 $\hat{\boldsymbol{g}}$ 处于 $\boldsymbol{S}$ 内时会接收该消息,那么可以通过选择 $\boldsymbol{h}$ 获得 Bob 估计的信道位于 $\boldsymbol{S}$ 中的最大概率,从而使 Eve 攻击成功概率最大化,即:

$$\bar{\boldsymbol{h}}=\underset{a_1,a_2\in\mathbb{C}^\alpha}{\operatorname{argmax}}[P(\hat{\boldsymbol{g}}_1\in\boldsymbol{S}|\boldsymbol{h}_1=\boldsymbol{a}_1)+P(\hat{\boldsymbol{g}}_2\in\boldsymbol{S}|\boldsymbol{h}_2=\boldsymbol{a}_2)] \tag{30}$$

因为 Eve 对 $\boldsymbol{g}_{A_1B}$、$\boldsymbol{g}_{A_2B}$ 未知,所以可以根据 Eve 可用的估计观测值 $\hat{\boldsymbol{g}}_{A_1B}$、$\hat{\boldsymbol{g}}_{A_2E}$ 和 $\hat{\boldsymbol{g}}_{EB}$,通过对 $\boldsymbol{g}_{A_1B}$、$\boldsymbol{g}_{A_1B}$ 进行信道估计,获得 Eve 攻击成功概率的最大值。均值为 0 的随机高斯矢量 $[\hat{\boldsymbol{g}}^{\mathrm{T}}_{A_1B},\hat{\boldsymbol{g}}^{\mathrm{T}}_{A_2B},\hat{\boldsymbol{g}}^{\mathrm{T}}_{A_1E},\hat{\boldsymbol{g}}^{\mathrm{T}}_{A_2E},\hat{\boldsymbol{g}}^{\mathrm{T}}_{EB}]^{\mathrm{T}}$ 对应的相关矩阵可以表示为:

$$\boldsymbol{w}_{A_2E}(n)=1+\frac{\sigma^2_{A_2E}}{\lambda_n} \tag{36}$$

$$\boldsymbol{w}_{EB}(n)=1+\frac{\sigma^2_{EB}}{\lambda_n} \tag{37}$$

进一步代入式(30)可以得出:

$$\begin{aligned}\bar{\boldsymbol{h}}(n)=&\boldsymbol{g}_{A_1E}\left(\frac{\rho_{EB}+\boldsymbol{w}_{EB}(n)-\rho_{A_1B}\rho_{A_1E}}{\boldsymbol{w}_{A_1E}(n)\boldsymbol{w}_{EB}(n)-\rho^2_{A_1B}}\right)+\\&\boldsymbol{g}_{A_2E}\left(\frac{\rho_{EB}+\boldsymbol{w}_{EB}(n)-\rho_{A_2B}\rho_{A_2E}}{\boldsymbol{w}_{A_2E}(n)\boldsymbol{w}_{EB}(n)-\rho^2_{A_2B}}\right)+\\&\boldsymbol{g}_{EB}\left(\frac{\rho_{A_1E}+\boldsymbol{w}_{A_1E}(n)-\rho_{A_1B}\rho_{EB}}{\boldsymbol{w}_{A_1E}(n)\boldsymbol{w}_{EB}(n)-\rho^2_{A_1B}}+\right.\\&\left.\frac{\rho_{A_2E}+\boldsymbol{w}_{A_2E}(n)-\rho_{A_2B}\rho_{EB}}{\boldsymbol{w}_{A_2E}(n)\boldsymbol{w}_{EB}(n)-\rho^2_{A_2B}}\right)\end{aligned} \tag{38}$$

3.2　可达的保密边界

一个可达区域的边界函数对可以表示为:

$$d(P_R,P_A)=P_R\operatorname{lb}\frac{P_R}{1-P_A}+(1-P_R)\operatorname{lb}\frac{1-P_R}{P_A} \tag{39}$$

$$d(\bar{P}_R,\bar{P}_A)\leqslant D \tag{40}$$

其中,D 是 Bob 的观测分布在任何一个假设条件下的散度。当 $\bar{P}_R\to0$ 时,得到:

$$\bar{P}_A\geqslant e^{-D} \tag{41}$$

根据消息认证方案的第 2 个阶段,可以对应 $\boldsymbol{R}_1$ 生成一个新的矩阵 $\boldsymbol{R}_2$:

$$\boldsymbol{R}_2=\begin{pmatrix}\boldsymbol{R}_{A_1B}+\sigma_3^2\boldsymbol{I}_\alpha & \boldsymbol{R}_{A_1B,A_2B} & \boldsymbol{R}_{A_1E,A_1B} & \boldsymbol{R}_{A_1E,A_2B} & \boldsymbol{R}_{A_1B,EB}\\ \boldsymbol{R}^*_{A_1B,A_2B} & \boldsymbol{R}_{A_2B}+\sigma_4^2\boldsymbol{I}_\alpha & \boldsymbol{R}_{A_2E,A_1B} & \boldsymbol{R}_{A_2E,A_2B} & \boldsymbol{R}_{A_2B,EB}\\ \boldsymbol{R}^*_{A_1E,A_1B} & \boldsymbol{R}^*_{A_2E,A_1B} & \boldsymbol{R}_{A_1E}+\sigma^2_{A_1E}\boldsymbol{I}_\beta & \boldsymbol{R}_{A_1E,A_2E} & \boldsymbol{R}_{A_1E,EB}\\ \boldsymbol{R}^*_{A_1E,A_2B} & \boldsymbol{R}^*_{A_2E,A_2B} & \boldsymbol{R}^*_{A_1E,A_2E} & \boldsymbol{R}_{A_2E}+\sigma^2_{A_2E}\boldsymbol{I}_\beta & \boldsymbol{R}_{A_2E,EB}\\ \boldsymbol{R}^*_{A_1B,EB} & \boldsymbol{R}^*_{A_2B,EB} & \boldsymbol{R}^*_{A_1E,EB} & \boldsymbol{R}^*_{A_2E,EB} & \boldsymbol{R}_{EB}+\sigma^2_{EB}\boldsymbol{I}_\gamma\end{pmatrix} \tag{42}$$

根据式(31)、式(42)得到一个均值为 0 的协方差矩阵:

$$\boldsymbol{R}=\begin{pmatrix}\boldsymbol{R}_{A_1B,A_2B} & \boldsymbol{R}_{A_2B}+\sigma_4^2\boldsymbol{I}_\alpha & \boldsymbol{R}_{A_2B}\\ \boldsymbol{R}_{A_1B}+\sigma_3^2\boldsymbol{I}_\alpha & \boldsymbol{I}_\alpha & \boldsymbol{R}_{A_2B}+\sigma_2^2\boldsymbol{I}_\alpha\\ \boldsymbol{R}_{A_1B} & \boldsymbol{R}_{A_1B}+\sigma_1^2\boldsymbol{I}_\alpha & \boldsymbol{R}_{A_1B,A_2B}\end{pmatrix} \tag{43}$$

令 $\boldsymbol{T}=\boldsymbol{R}_2^{-1}$,用 $\boldsymbol{I}_{ij}$ 表示 $\boldsymbol{I}$ 中第 i 行、第 j 列的元素,由 $\boldsymbol{S}$ 和 $\boldsymbol{T}$ 可以分别得到:

$$\boldsymbol{S}_{\mathrm{I}}=\begin{pmatrix}\boldsymbol{S}_{13}\\ \boldsymbol{S}_{14}\\ \boldsymbol{S}_{15}\end{pmatrix}^{\mathrm{T}},\boldsymbol{S}_{\mathrm{II}}=\begin{pmatrix}\boldsymbol{S}_{23}\\ \boldsymbol{S}_{24}\\ \boldsymbol{S}_{25}\end{pmatrix}^{\mathrm{T}},\boldsymbol{F}_1=\begin{pmatrix}\boldsymbol{S}_{33} & \boldsymbol{S}_{34} & \boldsymbol{S}_{35}\\ \boldsymbol{S}^*_{34} & \boldsymbol{S}_{44} & \boldsymbol{S}_{45}\\ \boldsymbol{S}^*_{35} & \boldsymbol{S}^*_{45} & \boldsymbol{S}_{55}\end{pmatrix} \tag{44}$$

$$\boldsymbol{T}_{\mathrm{I}}=\begin{pmatrix}\boldsymbol{T}_{13}\\ \boldsymbol{T}_{14}\\ \boldsymbol{T}_{15}\end{pmatrix}^{\mathrm{T}},\boldsymbol{T}_{\mathrm{II}}=\begin{pmatrix}\boldsymbol{T}_{23}\\ \boldsymbol{T}_{24}\\ \boldsymbol{T}_{25}\end{pmatrix}^{\mathrm{T}},\boldsymbol{F}_2=\begin{pmatrix}\boldsymbol{T}_{33} & \boldsymbol{T}_{34} & \boldsymbol{T}_{53}\\ \boldsymbol{T}^*_{34} & \boldsymbol{T}_{44} & \boldsymbol{T}_{54}\\ \boldsymbol{T}^*_{35} & \boldsymbol{T}^*_{45} & \boldsymbol{T}_{55}\end{pmatrix} \tag{45}$$

至此,可以生成一个矩阵 $\boldsymbol{V}$:

$$\boldsymbol{V}=\begin{pmatrix}-\boldsymbol{S}_{\mathrm{I}}\boldsymbol{F}_1\boldsymbol{S}_{\mathrm{II}}^{\mathrm{T}} & \boldsymbol{S}_{22}-\boldsymbol{S}_{\mathrm{II}}\boldsymbol{F}_2\boldsymbol{S}_{\mathrm{II}}^{\mathrm{T}} & -\boldsymbol{T}_{\mathrm{II}}\boldsymbol{F}_2\boldsymbol{S}_{\mathrm{II}}^{\mathrm{T}}\\ \boldsymbol{S}_{\mathrm{II}}-\boldsymbol{S}_{\mathrm{I}}\boldsymbol{F}_1\boldsymbol{S}_{\mathrm{I}}^{\mathrm{T}} & \boldsymbol{I}_\alpha & \boldsymbol{T}_{22}-\boldsymbol{T}_{\mathrm{II}}\boldsymbol{F}_2\boldsymbol{T}_{\mathrm{II}}^{\mathrm{T}}\\ -\boldsymbol{S}_{\mathrm{I}}\boldsymbol{F}_1\boldsymbol{T}_{\mathrm{I}}^{\mathrm{T}} & \boldsymbol{T}_{\mathrm{II}}-\boldsymbol{T}_{\mathrm{I}}\boldsymbol{F}_1\boldsymbol{T}_{\mathrm{I}}^{\mathrm{T}} & -\boldsymbol{T}_{\mathrm{II}}\boldsymbol{F}_1\boldsymbol{T}_{\mathrm{I}}^{\mathrm{T}}\end{pmatrix} \tag{46}$$

基于安全性检验结果,由式(43)、式(46)最终得到散度 D:

$$D=\mathrm{tr}(\boldsymbol{VR})-\mathrm{lb}|\boldsymbol{RV}|-2\alpha \tag{47}$$

4 保密通信容量

本节将推导高斯多路输入信道在消息传输时的安全认证速率,该速率可通过信道在功率约束 P 下能够达到的保密通信容量进行衡量[20]。根据消息认证方案下的信道模型,给出有敌手的高斯矢量多路输入信道的保密容量区域。

定理 1 高斯矢量多路输入信道的保密容量区域需满足以下码率对(L_1,L_2)组成的集合:

$$\begin{cases}L_1\leqslant C(\boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}})-C(\boldsymbol{G}_3\boldsymbol{K}_{x_1}\boldsymbol{G}_3^{\mathrm{T}})\\ L_2\leqslant C(\boldsymbol{G}_2\boldsymbol{K}_{x_2}\boldsymbol{G}_2^{\mathrm{T}})-C(\boldsymbol{G}_4\boldsymbol{K}_{x_2}\boldsymbol{G}_4^{\mathrm{T}})\\ L_1+L_2\leqslant C(\boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}}+\boldsymbol{G}_2\boldsymbol{K}_{x_2}\boldsymbol{G}_2^{\mathrm{T}})-\\ C(\boldsymbol{G}_3\boldsymbol{K}_{x_1}\boldsymbol{G}_3^{\mathrm{T}}+\boldsymbol{G}_4\boldsymbol{K}_{x_2}\boldsymbol{G}_4^{\mathrm{T}})\end{cases} \tag{48}$$

其中,$C(\boldsymbol{X}_n)=\frac{1}{2}\mathrm{lb}|\boldsymbol{X}_n+\boldsymbol{I}_n|$为高斯容量函数,$\boldsymbol{K}_{x_i}$为输入矢量信号的协方差矩阵。

证明

1)逆命题证明。高斯矢量多路输入信道的安全容量可以通过具有输入代价的多路输入信道容量区域进行刻画,对于安全信道容量 L_1,有:

$$\begin{aligned}&L_1\leqslant\boldsymbol{I}(\boldsymbol{x}_1;\boldsymbol{y}|\boldsymbol{x}_2,\boldsymbol{Q})-\boldsymbol{I}(\boldsymbol{x}_1;\boldsymbol{z}|\boldsymbol{x}_2,\boldsymbol{Q})\overset{(a)}{=}\\ &H(\boldsymbol{y}|\boldsymbol{x}_2,\boldsymbol{Q})-H(\boldsymbol{y}|\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{Q})-H(\boldsymbol{z}|\boldsymbol{x}_2,\boldsymbol{Q})+\\ &H(\boldsymbol{z}|\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{Q})=H(\boldsymbol{G}_1\boldsymbol{x}_1+\boldsymbol{G}_2\boldsymbol{x}_2+\boldsymbol{w}_1|\boldsymbol{x}_2,\boldsymbol{Q})-\\ &H(\boldsymbol{G}_1\boldsymbol{x}_1+\boldsymbol{G}_2\boldsymbol{x}_2+\boldsymbol{w}_1|\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{Q})-\\ &H(\boldsymbol{G}_3\boldsymbol{x}_1+\boldsymbol{G}_4\boldsymbol{x}_2+\boldsymbol{G}_2|\boldsymbol{x}_2,\boldsymbol{Q})+\\ &H(\boldsymbol{G}_3\boldsymbol{x}_1+\boldsymbol{G}_4\boldsymbol{x}_2+\boldsymbol{G}_2|\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{Q})=\\ &H(\boldsymbol{G}_1\boldsymbol{x}_1+\boldsymbol{w}_1|\boldsymbol{Q})-H(\boldsymbol{w}_1|\boldsymbol{Q})-\\ &H(\boldsymbol{G}_3\boldsymbol{x}_1+\boldsymbol{w}_2|\boldsymbol{Q})+H(\boldsymbol{w}_2|\boldsymbol{Q})\overset{(b)}{\leqslant}\\ &\frac{1}{2}\mathrm{lb}|2\pi\mathrm{e}(\boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}}+\boldsymbol{I}_n)|-\\ &\frac{1}{2}\mathrm{lb}|2\pi\mathrm{e}\boldsymbol{I}_n|-\frac{1}{2}\mathrm{lb}|2\pi\mathrm{e}(\boldsymbol{G}_3\boldsymbol{K}_{x_1}\boldsymbol{G}_3^{\mathrm{T}})+\boldsymbol{I}_n|+\\ &\frac{1}{2}\mathrm{lb}|2\pi\mathrm{e}\boldsymbol{I}_n|=\frac{1}{2}\mathrm{lb}|\boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}}+\boldsymbol{I}_n|-\\ &\frac{1}{2}\mathrm{lb}|\boldsymbol{G}_3\boldsymbol{K}_{x_1}\boldsymbol{G}_3^{\mathrm{T}}+\boldsymbol{I}_n|=\\ &C(\boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}})-C(\boldsymbol{G}_3\boldsymbol{G}\boldsymbol{K}_{x_1}\boldsymbol{G}_3^{\mathrm{T}})\end{aligned} \tag{49}$$

其中,H 为信息熵,$\boldsymbol{Q}$ 是一个与信道参数无关的分时随机变量,$\boldsymbol{Q}\rightarrow(\boldsymbol{x}_1,\boldsymbol{x}_2)\rightarrow\boldsymbol{y}$ 构成一个马尔科夫链,(a)表示根据互信息量 $\boldsymbol{I}$ 的定义,(b)表示由最大微分熵引理[17]得出。对于 L_2 和 (L_1+L_2) 的证明同理。

2)可达性证明。令$\boldsymbol{x}_1+\boldsymbol{x}_2\sim N(0,P)$,得到:

$$\begin{cases}\boldsymbol{I}(\boldsymbol{x}_1;\boldsymbol{y}|\boldsymbol{x}_2)=C(\boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}})\\ \boldsymbol{I}(\boldsymbol{x}_2;\boldsymbol{y}|\boldsymbol{x}_1)=C(\boldsymbol{G}_2\boldsymbol{K}_{x_2}\boldsymbol{G}_2^{\mathrm{T}})\\ \boldsymbol{I}(\boldsymbol{x}_1,\boldsymbol{x}_2;\boldsymbol{y})=C(\boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}}+\boldsymbol{G}_2\boldsymbol{K}_{x_2}\boldsymbol{G}_2^{\mathrm{T}})\end{cases} \tag{50}$$

对 $j\in N^*$,令$[\boldsymbol{x}_1]_j,[\boldsymbol{x}_2]_j\in\{-j\varphi,-(j-1)\varphi,\cdots,-\varphi,0,\varphi,\cdots,j\varphi\}$为$\boldsymbol{x}_1$、$\boldsymbol{x}_2$ 的离散采样,其中 $\varphi=1/\sqrt{j}$。采样过程中将$\boldsymbol{x}_1$、$\boldsymbol{x}_2$ 映射到最近的采样点并使$|[\boldsymbol{x}_1]_j|\leqslant|\boldsymbol{x}_1|$、$|[\boldsymbol{x}_2]_j|\leqslant|\boldsymbol{x}_2|$。显然,$E([\boldsymbol{x}_1]_j^2)+E([\boldsymbol{x}_2]_j^2)\leqslant E(\boldsymbol{x}_1^2)+E(\boldsymbol{x}_2^2)=P$。令 $\boldsymbol{y}_j=\boldsymbol{G}_{1j}[\boldsymbol{y}_1]_j+\boldsymbol{G}_{2j}[\boldsymbol{y}_2]_j+\boldsymbol{w}_1$ 为对应输出,同样有 $\boldsymbol{z}_j=\boldsymbol{G}_{3j}[\boldsymbol{x}_1]_j+$

$\boldsymbol{G}_{4j}[\boldsymbol{x}_2]_j+\boldsymbol{w}_2$,令$[\boldsymbol{y}_j]_k$为遵循同样定义的$\boldsymbol{y}_j$的采样,$[\boldsymbol{z}_j]_k$同理,由此可得对每一个$j$和$k$,任意码率对存在式(51)成立,且在信道输入为$[\boldsymbol{x}_1]_j$和$[\boldsymbol{x}_2]_j$、输出为$[\boldsymbol{y}_j]_k$及功率约束为$P$时可达安全信道容量区域的上界。

$$\begin{cases}L_1\leqslant \boldsymbol{I}([\boldsymbol{x}_1]_j;[\boldsymbol{y}_j]_k\mid[\boldsymbol{x}_2]_j)-\boldsymbol{I}([\boldsymbol{x}_1]_j;[\boldsymbol{z}_j]_k\mid[\boldsymbol{x}_2]_j)\\ L_2\leqslant \boldsymbol{I}([\boldsymbol{x}_2]_j;[\boldsymbol{y}_j]_k\mid[\boldsymbol{x}_1]_j)-\boldsymbol{I}([\boldsymbol{x}_2]_j;[\boldsymbol{z}_j]_k\mid[\boldsymbol{x}_1]_j)\\ L_1+L_2\leqslant \boldsymbol{I}([\boldsymbol{x}_1]_j,[\boldsymbol{x}_2]_j;[\boldsymbol{y}_j]_k)-\boldsymbol{I}([\boldsymbol{x}_1]_j,[\boldsymbol{x}_2]_j;[\boldsymbol{z}_j]_k)\end{cases} \tag{51}$$

由数据处理不等式可得:

$$\boldsymbol{I}([\boldsymbol{x}_1]_j;[\boldsymbol{y}_j]_k\mid[\boldsymbol{x}_2]_j)\leqslant \boldsymbol{I}([\boldsymbol{x}_1]_j;\boldsymbol{y}_j\mid[\boldsymbol{x}_2]_j)=H(\boldsymbol{y}_j\mid[\boldsymbol{x}_2]_j)-H(\boldsymbol{w}_1) \tag{52}$$

因为对所有j有$\mathrm{Var}(\boldsymbol{y}_j\mid[\boldsymbol{x}_2]_j)\leqslant \boldsymbol{G}_1\boldsymbol{K}_{x_1}\boldsymbol{G}_1^{\mathrm{T}}+1$,即$H(\boldsymbol{y}_j\mid[\boldsymbol{x}_2]_j)\leqslant H(\boldsymbol{y}\mid\boldsymbol{x}_2)$,所以:

$$\boldsymbol{I}([\boldsymbol{x}_1]_j;[\boldsymbol{y}_j]_k\mid[\boldsymbol{x}_2]_j)\leqslant \boldsymbol{I}(\boldsymbol{x}_1;\boldsymbol{y}\mid\boldsymbol{x}_2) \tag{53}$$

最终将结果代入式(50)和式(51),证毕。

5　实验结果与分析

实验环境配置为 Intel® Core™ i5-4210U CPU@ 1.70 GHz、双核、4 GB RAM、Windows 10 操作系统。编程环境为 Matlab R2014a。通过设置不同的信道条件来观察 Eve 攻击成功的概率均值$\bar{P}_A$的变化情况,分析并研究消息认证方案的安全性能。

5.1　度量标准

根据消息认证方案可以得出第 1 个阶段信道的信噪比S_1和S_2为:

$$S_1=\frac{1}{\alpha\sigma_1^2}\mathrm{tr}(\boldsymbol{R}_{\mathrm{A_1B}}),S_2=\frac{1}{\alpha\sigma_2^2}\mathrm{tr}(\boldsymbol{R}_{\mathrm{A_2B}}) \tag{54}$$

同理,第 2 个阶段信道的信噪比S_3和S_4为:

$$S_3=\frac{1}{\alpha\sigma_3^2}\mathrm{tr}(\boldsymbol{R}_{\mathrm{A_1B}}),S_4=\frac{1}{\alpha\sigma_4^2}\mathrm{tr}(\boldsymbol{R}_{\mathrm{A_2B}}) \tag{55}$$

令$\eta=(1+S_1^{-1})(1+S_3^{-1})+(1+S_2^{-1})(1+S_4^{-1})$,那么式(47)可以改写为:

$$D=2N(\rho_{\mathrm{A_1E}}\rho_{\mathrm{A_2E}}-\rho_{\mathrm{A_1E}}^2\rho_{\mathrm{A_2E}}^2)/[\eta-\rho_{\mathrm{A_1E}}^2\rho_{\mathrm{A_2E}}^2]-N\mathrm{lb}[(\eta-1)/(\eta-\rho_{\mathrm{A_1E}}^2\rho_{\mathrm{A_2E}}^2)] \tag{56}$$

5.2　结果分析

本节通过实验观察高斯矢量多路输入信道模型在不同条件下的安全性能。表 1 刻画了 Eve 攻击成功的概率均值$\bar{P}_{\mathrm{A}}$在不同信道条件下的变化关系。假设$S_1=S_2=15$ dB、$S_3=S_4=20$ dB,并令$\rho_{\mathrm{A_1E}}=\rho_{\mathrm{A_2E}}=\rho$,其中显示了$\rho$分别为 0.3、0.4 和 0.5 时$\bar{P}_A$随$N$的变化情况。由实验结果可知,随着节点数$N$的增大,Eve 攻击成功的概率均值$\bar{P}_{\mathrm{A}}$呈指数级降低,这是由于节点间存在波束成形使得 Eve 收到的信号减弱。当$N=20$且$\mathrm{A_1}$、$\mathrm{A_2}$与 Eve 的相关系数都小于 0.3 时,敌手攻击成功的概率均值小于1.87×10^{-7}。

表 1　信道变量N、ρ与 Eve 攻击成功概率均值$\bar{P}_{\mathrm{A}}$的关系

Table 1　Relationship between channel variables N,ρ and the average probability of successful Eve attack $\bar{P}_{\mathrm{A}}$

N	$\bar{P}_{\mathrm{A}}$		
	$\rho=0.3$	$\rho=0.4$	$\rho=0.5$
8	2.03×10^{-3}	3.27×10^{-3}	6.02×10^{-3}
10	4.33×10^{-4}	7.83×10^{-4}	1.68×10^{-3}
12	9.19×10^{-5}	1.87×10^{-4}	4.61×10^{-4}
14	1.95×10^{-5}	4.48×10^{-5}	1.28×10^{-4}
16	4.15×10^{-6}	1.72×10^{-5}	3.56×10^{-5}
18	8.81×10^{-7}	2.57×10^{-6}	9.91×10^{-6}
20	1.87×10^{-7}	6.14×10^{-7}	2.75×10^{-6}

图 2 给出 Eve 与$\mathrm{A_1}$、$\mathrm{A_2}$关联信道的空间相关系数$\rho_{\mathrm{A_1E}}$、$\rho_{\mathrm{A_2E}}$与 Eve 攻击成功的概率均值$\bar{P}_A$之间的关系。初始假设条件与表 1 相同,并将节点数N固定为 20。由实验结果可知,随着发送者与敌手关联空间相关系数的减小,Eve 攻击成功的概率均值$\bar{P}_{\mathrm{A}}$呈指数级下降,即使当 Eve 估计出一侧的信道信息而对另一侧了解较少时,$\bar{P}_{\mathrm{A}}$仍处于一个较低的范围区间。

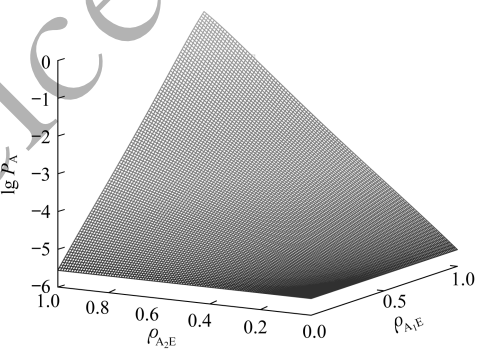

图 2　空间相关系数$\rho_{\mathrm{A_1E}}$、$\rho_{\mathrm{A_2E}}$与 Eve 攻击成功概率均值$\bar{P}_{\mathrm{A}}$的关系模型

Fig. 2　The relational model among the spatial correlation coefficients $\rho_{\mathrm{A_1E}}$,$\rho_{\mathrm{A_2E}}$ and the average probability of successful Eve attack $\bar{P}_{\mathrm{A}}$

图 3 给出了第 1 个阶段信道的信噪比S_1、S_2与 Eve 攻击成功的概率均值$\bar{P}_{\mathrm{A}}$的关系,假设$S_1=S_2=15$ dB,$\rho_{\mathrm{A_1E}}=\rho_{\mathrm{A_2E}}=0.5$。实验结果表明,在第 1 个阶段发送训练序列时的信噪比越大,安全性越强。当S_1和S_2为(0 dB,5 dB)时,则安全性迅速提升;当S_1和S_2大于 15 dB 时,则安全性提升效果趋于减缓。

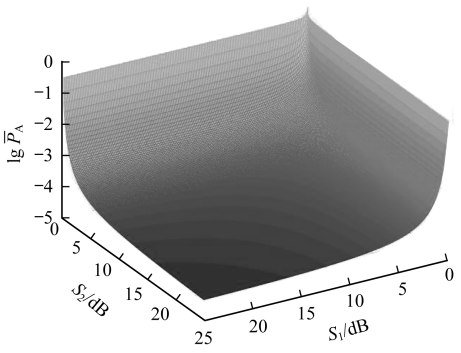

图 3 信噪比 S_1、S_2 与 Eve 攻击成功概率均值 $\bar{P}_A$ 的关系模型

Fig.3 The relational model among the signal to noise ratio S_1, S_2 and the average probability of successful Eve attack $\bar{P}_A$

6 结束语

本文利用最小均方误差法进行信道估计，提出一种高斯矢量多路输入信道下的消息认证方案，运用假设检验方法对消息认证方案进行安全性检验，制定敌手的最优攻击策略，并对敌手攻击成功的概率进行定界，同时在发送功率受约束的情况下，推导出消息认证方案的保密容量区域。通过实验测试与分析该方案在不同信道条件下敌手攻击成功的概率，从而验证其安全性和可行性，为多路输入信道下物理层消息认证的安全性分析提供了参考。后续将针对高斯矢量广播信道等其他信道模型下的物理层消息认证方案做进一步研究。

参考文献

[1] JEREMY P V, PHILIP S. Expectation-maximization Gaussian-mixture approximate message passing[J]. IEEE Transactions on Signal Processing, 2013, 61(19): 4658-4672.

[2] XIAO L, GREENSTEIN L, MANDAYAM N, et al. MIMO-assisted channel-based authentication in wireless networks [C]//Proceedings of the 42nd Annual Conference on Information Sciences and Systems. Washington D. C., USA: IEEE Press, 2008: 642-646.

[3] VISURI S, BOLCSKEI H. MIMO-OFDM multiple access with variable amount of collision[C]//Proceedings of 2004 IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2004: 286-291.

[4] YANG Xiaodong, LI Yanan, ZHOU Qixu, et al. ID-based sever-aided verification proxy re-signature scheme [J]. Computer Engineering, 2017, 43(4): 166-170, 176. (in Chinese)
杨小东，李亚楠，周其旭，等. 基于身份的服务器辅助验证代理重签名方案[J]. 计算机工程，2017，43(4)：166-170，176.

[5] YU Binbin, HU Liang, CHI Ling. Digital signature scheme against internal and external attack for wireless sensor networks [J]. Journal of Jilin University (Engineering and Technology Edition), 2019, 49(5): 1676-1681. (in Chinese)
于斌斌，胡亮，迟令. 可抵抗内外部攻击的无线传感器网络数字签名方案[J]. 吉林大学学报(工学版)，2019，49(5)：1676-1681.

[6] PAOLO B, NICOLA L, STEFANO T. Physical layer authentication over MIMO fading wiretap channels[J]. IEEE Transactions on Wireless Communications, 2012, 11(7): 2564-2573.

[7] YU P L, BARAS J S, SADLER B M. Physical-layer authentication [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(1): 38-51.

[8] XIAO L, GREENSTEIN L, MANDAYAM N, et al. A physical-layer technique to enhance authentication for mobile terminals [C]//Proceedings of 2008 IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2008: 1520-1524.

[9] LUN D, ZHU H, PETROPULU A P, et al. Improving wireless physical layer security via cooperating relays[J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1875-1888.

[10] SADAF S, MOHAMMAD R A. Joint source-channel coding for multiple-access wiretap channels [C]// Proceedings of IEEE International Symposium on Information Theory. Washington D. C., USA: IEEE Press, 2013: 369-373.

[11] YASSAEE M H, AREF M R. Multiple access wiretap channels with strong secrecy[C]//Proceedings of 2010 IEEE Information Theory Workshop. Washington D. C., USA: IEEE Press, 2010: 1-5.

[12] ZOU Qinyu, ZHANG Bangning, GUO Daoxing, et al. Physical layer safety communication technology based on reliability mixed restansmission protocol [J]. Computer Engineering, 2018, 44(1): 182-186, 192. (in Chinese)
邹芹宇，张邦宁，郭道省，等. 基于可靠度混合重传协议的物理层安全通信技术[J]. 计算机工程，2018，44(1)：182-186，192.

[13] LIANG Y B, POOR H V. Multiple-access channels with confidential messages [J]. IEEE Transactions on Information Theory, 2008, 54(3): 976-1002.

[14] LI L, JINDAL N, GOLDSMITH A. Outage capacities and optimal power allocation for fading multiple-access channels[J]. IEEE Transactions onInformation Theory, 2005, 51(4): 1326-1347.

[15] MUKHERJEE A, SWINDLEHURST A L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI [J]. IEEE Transactions on Signal Processing, 2011, 59(1): 351-361.

[16] YU W, CIOFFI J M. Sum capacity of Gaussian vector broadcast channels[J]. IEEE Transactions on Information Theory, 2004, 50(9): 1875-1892.

[17] ABBAS E G, YOUNG-HAN K. Network information theory[M]. London, UK: Cambridge University Press, 2011: 230-234.

[18] MARTINIAN E, WORNELL G W, CHEN B. Authentication with distortion criteria[J]. IEEE Transactions on Information Theory, 2005, 51(7): 2523-2542.

[19] MAURER U M. Authentication theory and hypothesis testing[J]. IEEE Transactions on Information Theory, 2000, 46(4): 1350-1356.

[20] COVER T, MCELIECE R, POSNER E. Asynchronous multiple-access channel capacity[J]. IEEE Transactions on Information Theory, 1981, 27(4): 409-413.

编辑 陆燕菲