文章编号:1671-6833(2024)01-0064-06

基于 QAM 的协作通信系统物理层认证技术

韩刚涛, 刘瑞雪, 闫 利, 王俊杰, 马雪粉

(郑州大学 电气与信息工程学院,河南 郑州 450001)

摘 要: 针对两用户协作通信系统的身份认证问题,提出了一种基于正交幅度调制(QAM)的协作物理层认证机制。在该机制中,两个单天线用户分别使用同相与正交分量传输自己及伙伴的消息和标签,从而实现两用户消息和标签的唯一分解。基站采用最大比合并检测用户消息和标签,并通过标签对比完成物理层身份认证。在等功率分配且用户上行信道对称的典型场景下,给出了消息和标签的误码率闭合表达式。结果表明:在信噪比(*SNR*)为 6~15 dB 时,所提机制的认证概率与非协作物理层认证相比提高了 12%~20%,非法攻击认证概率仅保持在 10^{-3} 量级,所提认证机制具有更好的身份认证性能。

关键词:物理层认证; 协作通信; 标签叠加; 最大比合并; QAM

中图分类号:TN918.91;TN92 **文献标志码**:A **doi**:10.13705/j.issn.1671-6833.2023.04.011

用户协作分集技术可以有效对抗衰落。在用户协作通信系统中,单天线用户共享彼此的天线资源,由此形成虚拟的多天线发射机,不仅可以获得多天线分集增益,而且可以在不扩展频带或不改变发射功率的前提下增加用户的系统容量,改善系统的鲁棒性[1]。

在资源共享的协作通信系统中,由于无线信道具有开放性和广播性,非法攻击者易于冒充合法用户给接收端发送虚假信息,系统可能会受到严重的安全威胁[2]。因此,协作通信系统的身份认证问题不容小觑。目前,无线通信系统主要通过上层认证机制进行身份认证,但该机制存在一定的局限性[3]:一是算法容易受到重放攻击;二是上层操作复杂,算法通信开销大、复杂度高;三是算法安全性是在假设破译工具计算能力有限的基础上实现的。而物理层认证(physical layer authentication,PLA)主要利用物理层信道、信号或设备等不可伪造特征进行认证。PLA 具有复杂度低、处理延迟低及兼容性高等显著优势,结合上层加密认证机制可以有效提升系统安全[4-5]。

PLA 主要分为被动认证和主动认证。被动认证机制是将通信系统的固有特征作为认证信息对发送端进行身份认证,如射频信号特征、信道特征等[6]。然而,这些特征对温度、潜在的恶意攻击和信道变化等外部因素很敏感,对动态环境适应能力弱,因此应用比较受限。主动认证机制则是在发送端根据密钥生成标签并将其隐藏到消息中[7-8],接收端检测接收信号中是否存在标签以进行认证。与被动认证机制相比,主动认证利用标签修改了源消息,提供了额外的物理层特性,因而更具灵活性。

针对两用户协作通信系统的身份认证问题,本文提出一种了基于正交幅度调制(quadrature amplitude modulation,QAM)的 PLA 技术。在该系统中,用户使用相互正交的调制符号传输自己的消息和标签,同时在消息和标签的正交分量上传输协作用户的消息和标签,从而实现两用户消息和标签在接收端的唯一分解。在接收端,基站首先通过最大比合并(maximum ratio combining,MRC)检测消息和标签。接着,基站利用检测所得消息及共享密钥重新生成标签并与检测所得标签进行比较,根据假设检验完成认证决策。在两用户上行信道对称且采用等功率分配的场景下,推导了消息和标签的误码率

收稿日期:2023-03-14;**修订日期**:2023-04-03

基金项目:国家自然科学基金资助项目(62101504);嵩山实验室项目(纳入河南省重大科技专项管理体系)(221100211300-01);嵩山实验室预研项目(YYJC022022002)

作者简介:韩刚涛(1986—),男,河南开封人,郑州大学副教授,博士,主要从事无线通信技术研究,E-mail:iegthan@zzu.edu.cn。

引用本文:韩刚涛,刘瑞雪,闫利,等. 基于 QAM 的协作通信系统物理层认证技术[J]. 郑州大学学报(工学版),2024,45(1):64-69. (HAN G T, LIU R X, YAN L, et al. QAM based physical layer authentication technology for cooperative communication systems[J]. Journal of Zhengzhou University (Engineering Science),2024,45(1):64-69.)

(symbol error rate, SER)闭合表达式,并仿真分析了所提机制的身份认证性能。

1　系统模型

图 1 所示为一个两用户协作通信系统模型,其中单天线用户 A 和 B 通过彼此协作将他们的消息和标签发送给共同的单天线基站 D,基站利用最大比合并的方法完成用户自身发送的消息、标签及合作用户转发的消息、标签的合并检测。在该系统中,用户采用半双工模式交替向基站发送消息和标签,即 k 时隙用户 A 向基站 D 发送消息和标签,$k+1$ 时隙用户 B 向基站 D 发送消息和标签。发送端未知信道状态信息(channel state information,CSI),接收端已知 CSI。不失一般性,考虑系统节点之间的信道均为瑞利衰落信道,衰落系数 $h_{n,k}(n=1,2)$ 相互独立,且服从零均值循环对称复高斯(circularly symmetric complex Gaussian,CSCG)分布,方差为 1。用户间的协作转发采用译码转发(decode-and-forward,DF)方式,可以有效避免噪声的放大。基站端的噪声服从均值为 0、方差为 σ_n^2 的循环对称复高斯分布。此外,假设用户间的协作信道是可靠的、译码转发的过程是理想的,不会产生错误。用户附近有潜在的攻击者,试图模仿合法用户向基站发送虚假信息[9]。

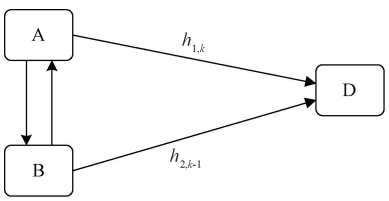

图 1　两用户协作通信系统模型

Figure 1　Two-user cooperative communication system model

用户协作传输消息和标签的过程如图 2 所示。图 2 给出了用户 A 协助转发用户 B 消息和标签的过程,反之,用户 B 转发用户 A 消息和标签的过程类似。具体地,用户 A、B 发送的消息符号 $s_{1,k}$、$s_{2,k-1}$ 分别采用正交二进制调制,即调制消息符号 $x_{1,k}\in\{1,-1\}$、$x_{2,k-1}\in\{\mathrm{j},-\mathrm{j}\}$。同时,将用户消息序列 $\{s_{1,k}\}$、$\{s_{2,k-1}\}$ 和共享密钥 $\boldsymbol{e}_1$、$\boldsymbol{e}_2$ 分别代入哈希(Hash)函数生成标签序列,即 $\{m_{1,k}\}=\mathrm{Hash}(\{s_{1,k}\},\boldsymbol{e}_1)$、$\{m_{2,k-1}\}=\mathrm{Hash}(\{s_{2,k-1}\},\boldsymbol{e}_2)$。同一用户的标签与消息采用相同的调制方式,即调制标签符号 $t_{1,k}\in\{1,-1\}$、$t_{2,k-1}\in\{\mathrm{j},-\mathrm{j}\}$。用户以功率 α^2 传输自身消息及标签的同时,以功率 β^2 协助转发伙伴上一时隙发送的消息及标签。两用户的归一化总发射功率均为 1,即满足 $\alpha^2+\beta^2=1$,基站端在第 k 时隙接收到的用户 A 发送的信号为

$$y_k=h_k(\alpha(\rho_s x_{1,k}+\rho_t t_{1,k})+\beta(\rho_s x_{2,k-1}+\rho_t t_{2,k-1}))+n_k。\tag{1}$$

式中:ρ_s、ρ_t 为消息和标签的功率分配系数,满足 $\rho_s^2+\rho_t^2=1$ 且 $\rho_t\ll\rho_s$;h_k 为 k 时隙接收端接收信号经历的传输信道,此处为表述方便省去了图 1 中 $h_{n,k}(n=1,2)$ 的 n;$x_{i,k}$、$t_{i,k}(i=1,2)$ 分别表示用户 A 或 B 在第 k 时隙生成的调制消息符号和调制标签符号;y_k 和 n_k 分别表示基站在第 k 时隙接收的信号和加性噪声。为简化分析,考虑采用等功率分配(即 $\alpha^2=\beta^2=0.5$)且两协作用户上行信道对称的场景。则式(1)可转化为

$$y_k=h_k(\mu(x_{1,k}+x_{2,k-1})+\theta(t_{1,k}+t_{2,k-1}))+n_k。\tag{2}$$

式中:$\mu=\sqrt{\rho_s^2/2}$,$\theta=\sqrt{\rho_t^2/2}$。

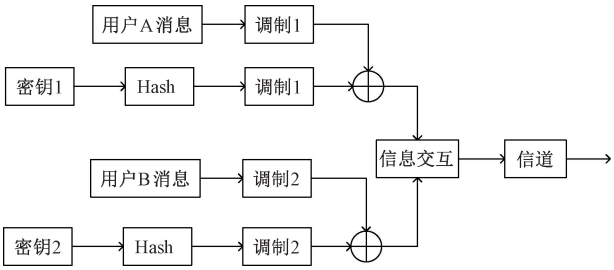

图 2　k 时隙用户 A 和用户 B 协作传输消息和标签的过程

Figure 2　Cooperative transmission process of messages and tags of user A and user B at the k-th slot

同理可得基站端在第 $k+1$ 和 $k+2$ 时隙接收到的用户 B 和 A 发送的信号分别为

$$y_{k+1}=h_{k+1}(\mu(x_{2,k+1}+x_{1,k})+\theta(t_{2,k+1}+t_{1,k}))+n_{k+1};\tag{3}$$

$$y_{k+2}=h_{k+2}(\mu(x_{1,k+2}+x_{2,k+1})+\theta(t_{1,k+2}+t_{2,k+1}))+n_{k+2}。\tag{4}$$

2　协作信号检测及认证机制

2.1　信号检测

信号检测主要分为消息检测和标签检测,这是实现 PLA 的前提。由于标签符号的传输功率远小于消息符号,在进行消息符号检测时,首先将标签符号作为噪声来处理。在完成消息符号检测之后,从接收信号中减去检测的消息符号并利用残差信号来完成标签符号的检测。

首先,对式(2)、(3)进行最大比合并,则 k 时隙用户 A 的消息符号的检测值[10]为

$$\hat{x}_{1,k}=\mathrm{sign}[\mu\mathrm{Re}(h_k^* y_k)+\mu\mathrm{Re}(h_{k+1}^* y_{k+1})]。\tag{5}$$

同理,根据式(3)、(4)可得 $k+1$ 时隙用户 B 发送的消息符号的检测值为

$$\hat{x}_{2,k+1} = \mathrm{sign}[\mu \mathrm{Im}(h_{k+1}^{*} y_{k+1}) + \mu \mathrm{Im}(h_{k+2}^{*} y_{k+2})] \cdot \mathrm{j}。 \quad (6)$$

式中：Re(·) 和 Im(·) 分别表示取实部和取虚部；上标 * 表示取共轭。

其次，式(3)、(4)中去掉检测的用户消息符号可得残差信号为

$$r_{k+1} = h_{k+1}(\theta(t_{2,k+1} + t_{1,k})) + n_{k+1}; \quad (7)$$

$$r_{k+2} = h_{k+2}(\theta(t_{1,k+2} + t_{2,k+1})) + n_{k+2}。 \quad (8)$$

同理，根据式(7)、(8)，利用最大比合并检测用户 B 的标签符号的检测值为

$$\hat{t}_{2,k+1} = \mathrm{sign}[\theta \mathrm{Im}(h_{k+1}^{*} r_{k+1}) + \theta \mathrm{Im}(h_{k+2}^{*} r_{k+2})] \cdot \mathrm{j}。 \quad (9)$$

2.2 误码率性能分析

以用户 A 的消息符号的检测值 $\hat{x}_{1,k}$ 为例，将式(2)和式(3)代入式(5)可得

$$\hat{x}_{1,k} = \mathrm{sign}[\mu^2(|h_k|^2 + |h_{k+1}|^2)x_{1,k} + \mu\theta(|h_k|^2 + |h_{k+1}|^2)t_{1,k} + \tilde{n}_k + \tilde{n}_{k+1}]。 \quad (10)$$

式中：$\tilde{n}_k$ 表示均值为 0、方差为 $\mu^2|h_k|^2\sigma_n^2/2$ 的加性噪声；$\tilde{n}_{k+1}$ 表示均值为 0、方差为 $\mu^2|h_{k+1}|^2\sigma_n^2/2$ 的加性噪声。由于 $\rho_t \ll \rho_s$，故将式(10)中 $\mu\theta(|h_k|^2 + |h_{k+1}|^2)t_{1,k}$ 对消息符号检测的影响视为噪声。假设输入比特为等概率分布，那么接收端检测的消息符号的瞬时误码率可以表示[10]为

$$P_{e,M}^{I} = P(\hat{x}_{1,k} = 1 \mid x_{1,k} = -1) = P(\tilde{n}_k + \tilde{n}_{k+1} > \mu^2(|h_k|^2 + |h_{k+1}|^2)) = Q((2(\mu^2(\gamma_{AD} + \gamma_{BD})))^{1/2})。 \quad (11)$$

式中：γ_{AD} 和 γ_{BD} 表示用户和接收端的信噪比(*SNR*)；Q 函数定义为 $Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t$。

由于用户上行通道对称且为瑞利衰落信道，接收端信噪比的概率密度函数可以表示为

$$p(\gamma_{AD}) = p(\gamma_{BD}) = \frac{1}{\bar{\gamma}_{BD}} \exp\left(-\frac{\gamma_{BD}}{\bar{\gamma}_{BD}}\right)。 \quad (12)$$

式中：$\bar{\gamma}_{BD}$ 为信噪比的平均值。

根据相应的信噪比概率密度函数对消息符号的瞬时误码率求期望可得用户消息平均误码率为

$$P_{e,M} = \int_0^{\infty} P_{e,M}^{I} p(\gamma_{BD}) \mathrm{d}\gamma_{BD} = \left(2 + \left(\frac{\mu^2\bar{\gamma}_{BD}}{1+\mu^2\bar{\gamma}_{BD}}\right)^{\frac{1}{2}}\right)\left(\frac{1}{2}\left(1 - \left(\frac{\mu^2\bar{\gamma}_{BD}}{1+\mu^2\bar{\gamma}_{BD}}\right)^{\frac{1}{2}}\right)\right)^2。 \quad (13)$$

与消息符号的检测类似，通过最大比合并从残差信号中检测标签符号。以用户 A 的标签符号的检测值 $\hat{t}_{1,k}$ 为例，其瞬时误码率为

$$P_{e,T}^{I} = P(\hat{t}_{1,k} = 1 \mid t_{1,k} = -1) = P(\tilde{n}_k + \tilde{n}_{k+1} > \theta^2(|h_k|^2 + |h_{k+1}|^2)) = Q((2[\theta^2(\gamma_{AD} + \gamma_{BD})])^{1/2})。 \quad (14)$$

于是，可得用户标签平均误码率为

$$P_{e,T} = \int_0^{\infty} P_{e,T}^{I} p(\gamma_{BD}) \mathrm{d}\gamma_{BD} = \left(2 + \left(\frac{\theta^2\bar{\gamma}_{BD}}{1+\theta^2\bar{\gamma}_{BD}}\right)^{\frac{1}{2}}\right)\left(\frac{1}{2}\left(1 - \left(\frac{\theta^2\bar{\gamma}_{BD}}{1+\theta^2\bar{\gamma}_{BD}}\right)^{\frac{1}{2}}\right)\right)^2。 \quad (15)$$

2.3 物理层认证机制

在接收端，将检测出的消息序列和共享密钥代入 Hash 函数，重新生成标签序列并与检测所得标签序列进行逐位比较，通过二元假设检验完成身份认证，即

H_1：存在标签，发送方合法；

H_0：不存在标签，发送方非法。

以用户 A 发送的调制标签序列 $\{t_{1,k}\}$ 的检测为例进行详细介绍。接收端对检测的消息序列 $\{\hat{x}_{1,k}\}$ 和检测的标签序列 $\{\hat{t}_{1,k}\}$ 进行解调分别得 $\{\hat{s}_{1,k}\}$、$\{\hat{m}_{1,k}\}$。通过 $\{\hat{s}_{1,k}\}$ 和密钥 $\boldsymbol{e}_1$ 以及 Hash 函数重新生成期望标签序列 $\{m'_{1,k}\}$，然后对 $\{\hat{m}_{1,k}\}$ 和 $\{m'_{1,k}\}$ 进行逐位比较，统计相同位数并记为 l。令标签长度为 L，定义标签精度 $\tau = l/L$，则通过对比标签精度 τ 与阈值 τ_0 可得认证结果，即

当 $\tau \geqslant \tau_0$ 时，认为发送端是合法用户，记为事件 H_1 发生；反之，认为发送端是非法攻击者，记为事件 H_0 发生。

设非法攻击者随机生成 L 位二进制序列伪造标签，则伪造标签与正确标签在对应位相同的概率为 1/2[11]，那么虚警概率可以表示为

$$P_f = P(H_1 \mid H_0) = \sum_{i=\lceil L\tau_0 \rceil}^{L} \binom{L}{i} \left(\frac{1}{2}\right)^i \left(\frac{1}{2}\right)^{L-i}。 \quad (16)$$

式中：$\lceil \cdot \rceil$ 表示向上取整。

根据奈曼-皮尔逊准则(Neyman-Pearson criterion, N-P)，即在虚警概率 P_f 尽可能小时使检测概率 P_d 尽可能大，由式(16)可得，在给定 $P_f \leqslant \varepsilon$ 的要求下容易求得 τ_0。同时，检测概率可以表示为

$$P_d = P(H_1 \mid H_1) = \sum_{i=\lceil L\tau_0 \rceil}^{L} \binom{L}{i} (1-p_t)^i (p_t)^{L-i}。 \quad (17)$$

式中：p_t 表示标签误码率。

具体的协作物理层认证步骤如下。

步骤 1　标签生成。在发送端，用户消息和共享密钥根据 Hash 函数生成标签。

步骤 2　消息和标签的协作传输。用户消息和标签采用正交二进制调制，将已调标签叠加在已调消息上同时传输。用户在同相分量上传输本地信号的同时，也在正交分量上转发上一时隙收到的信号。

步骤 3　消息和标签的检测。在接收端，基站利用 MRC，根据相邻两个时隙的接收信号检测用户

消息。同理,利用 MRC,根据相邻两个时隙的残差信号检测标签。

步骤 4　重构期望标签。在接收端,解调步骤 3 中检测到的消息,利用其与共享密钥以及 Hash 函数(发送端和接收端采用相同的 Hash 函数)重新生成期望的标签。

步骤 5　认证决策。解调步骤 3 中检测到的标签,并与步骤 4 中重构的期望标签逐位比较,记录对应位相同的位数,它与标签长度的比值作为认证的精度。根据 N-P 准则确定认证阈值,当认证精度大于等于认证阈值时,认证成功,认为发送方合法;否则,认证失败,认为发送方非法。

3　仿真结果与分析

本节采用蒙特卡洛法对所提两用户协作认证技术进行了详细的 MATLAB 仿真。在仿真中,两用户采用等功率分配策略发送符号,同时假定其上行通道对称,且服从瑞利衰落,即信道状态信息服从均值为 0、方差为 1 的循环对称复高斯分布,即 $h_k \sim CN(0,1)$。此外,用户对的消息及标签信号采用 QAM 调制,消息和标签序列长度 $L = 160$。发送端和接收端生成标签时所采用的 Hash 函数是单向散列函数 SHA-1。仿真实验中设置标签分配功率为 $\rho_t^2 = 0.01$ 或 $\rho_t^2 = 0.10$,给定虚警概率的门限值 ε 为 0.01。

首先,图 3 给出了标签分配功率为 0.01 时,所提协作认证机制的消息和标签平均误码率随信噪比变化的情况。从图 3 中可以看出,消息和标签平均误码率均随 *SNR* 的增加而降低,并且所提认证机制的消息和标签平均误码率的理论结果与仿真结果相吻合,验证了理论分析的准确性。

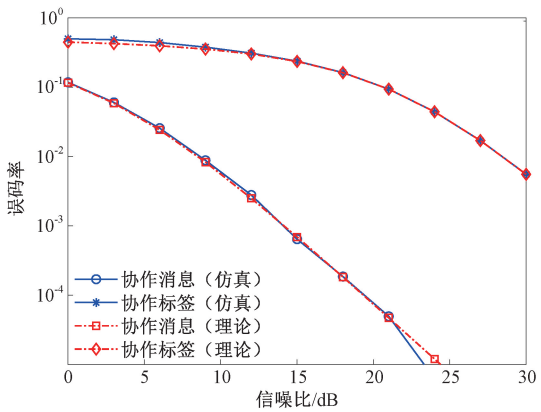

图 3　协作物理层认证机制的消息和标签平均误码率($\rho_t^2 = 0.01$)

Figure 3　Average SERs of messages and tags of the cooperative PLA mechanism ($\rho_t^2 = 0.01$)

标签分配功率为 0.01 时,所提认证机制和文献[8]中非协作物理层认证的消息和标签平均误码率对比如图 4 所示。通过对比可以发现,所提认证机制的消息和标签平均误码率要明显低于非协作认证的情况,这是因为用户协作传输带来了虚拟的多天线分集增益,改善了信号的传输性能。此外,从图 4 中还可以看出,所提认证机制的消息平均误码率略高于文献[10]中协作通信(无叠加标签)的消息平均误码率。换言之,叠加小功率标签对消息传输的影响极小。这是因为用户消息和叠加标签的分配功率之比为 99:1,低功率标签的叠加相当于附加了小的加性噪声,致使消息的平均误码率有限增加,故低功率标签叠加的影响可以忽略。

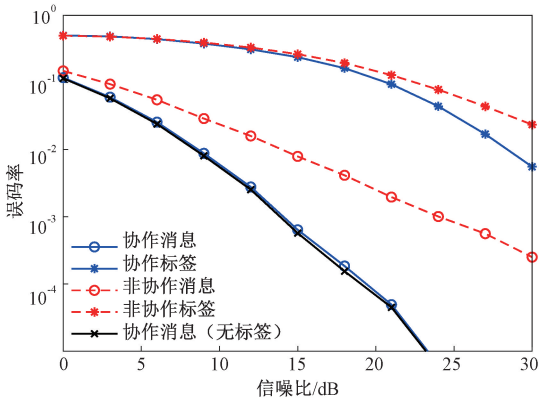

图 4　不同认证机制的消息和标签平均误码率($\rho_t^2 = 0.01$)

Figure 4　Average SERs of messages and tags of different authentication mechanisms ($\rho_t^2 = 0.01$)

在标签分配功率为 0.10 时,所提认证机制和文献[8]中非协作物理层认证的消息和标签平均误码率对比如图 5 所示。可以观察到,此时所提机制的误码性能仍优于非协作认证。对比图 4 和图 5 发现,对于所提机制和非协作认证机制而言,标签分配功率越大,标签的平均误码率越低,如标签分配功率分别为 0.01 和 0.10 时,所提机制在 *SNR* = 15 dB 时对应的标签平均误码率分别是 0.238 和 0.051。

其次,所提协作认证机制在标签分配功率为 0.01 且信噪比为 9 dB 时的 ROC 曲线如图 6 所示。从图 6 中可以看出,当给定虚警概率大于 0.4 时,所提认证机制的检测概率略高于文献[8]中非协作认证机制。而在给定虚警概率为 0~0.4 时,协作认证机制的检测概率显然更大。不同虚警概率下,两种认证机制检测概率的具体数值如表 1 所示,可以看出,虚警概率门限值越小,所提两用户协作认证机制的认证性能优势越显著。这是因为协作传输提升了消息和标签的检测性能,而随着虚警概率门限值条件的放宽,两种认证机制的检测概率均趋于 1,差别

不明显。

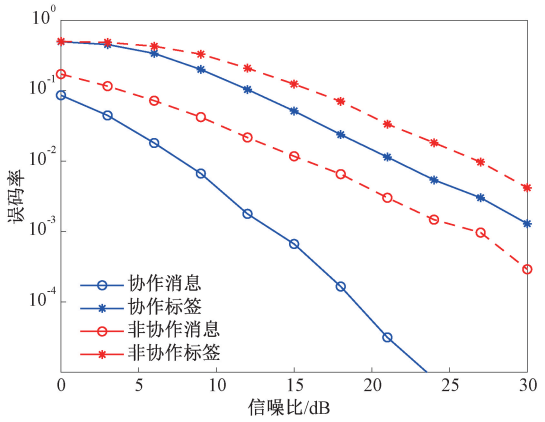

图 5 不同认证机制的消息和标签平均误码率($\rho_t^2 = 0.10$)

Figure 5 Average SERs of messages and tags of different authentication mechanisms ($\rho_t^2 = 0.10$)

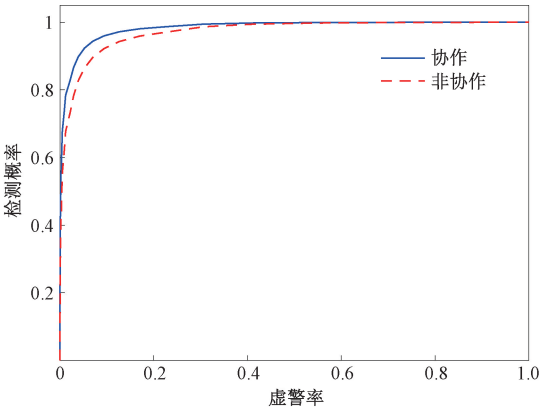

图 6 不同认证机制的 ROC 曲线($\rho_t^2 = 0.01$, $SNR = 9$ dB)

Figure 6 ROC curves of different authentication mechanisms ($\rho_t^2 = 0.01$, $SNR = 9$ dB)

表 1 不同认证机制的检测概率

Table 1 Detection probabilities of different authentication mechanisms %

机制	检测概率			
	$P_f = 10^{-3}$	$P_f = 10^{-2}$	$P_f = 10^{-1}$	$P_f = 0.5$
协作	49.04	92.36	97.19	99.93
非协作	36.35	86.47	94.31	99.78

最后,设两个合法协作用户附近各有一个非法攻击者,两个攻击者模仿合法用户对的协作传输模式并伪造了标签,试图让接收端认证其身份并接受虚假信息,给定虚警概率为 0.01 时,其认证概率如图 7 所示。从图 7 中可以观察到,所提机制和文献[8]中非协作认证的合法用户认证概率均随着信噪比的增加而逐渐增大到 1,且当信噪比大于 4 dB 时,与文献[8]相比,所提机制的合法用户认证概率更大,在 $SNR = 6 \sim 15$ dB 时,所提机制的认证概率相比非协作认证提高了 12%~20%。而非法攻击者的认证概率在信噪比 0~30 dB 时很小(10^{-3} 量级),且几乎不随信噪比发生变化,这是因为 Hash 函数 SHA-1 具有不可逆性,非法攻击者不知道密钥的相关信息,因此即使窃听到完整的消息信号,也难以破解标签信号。这说明所提协作认证机制具有很好的安全性,不容易受到欺骗攻击的影响。

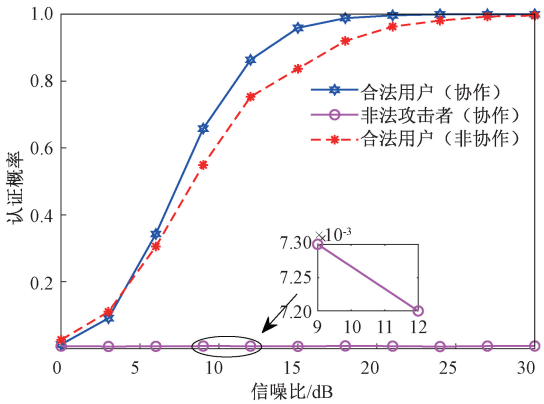

图 7 合法用户和非法攻击者的认证概率($\varepsilon = 0.01$)

Figure 7 Probabilities of authentication of legal user and illegal attacker ($\varepsilon = 0.01$)

4 结论

针对两个单天线用户的协作通信系统的身份认证问题,提出一种基于 QAM 的叠加标签物理层认证机制。将低功耗的标签叠加在消息上,用户在同相分量上传输自身消息和标签的同时,在正交分量上协作转发伙伴用户的消息和标签,从而实现了用户消息和标签的唯一分解。在等功率分配且用户上行信道对称的场景下,给出了所提认证机制的消息和标签误码率、虚警概率、检测概率及认证概率。仿真结果表明,与现有的非协作认证机制相比,所提的基于 QAM 的协作 PLA 机制具备更好的认证性能。

参考文献:

[1] LI G X, MISHRA D, HU Y L, et al. Adaptive relay selection strategies for cooperative NOMA networks with user and relay cooperation[J]. IEEE Transactions on Vehicular Technology, 2020, 69(10): 11728-11742.

[2] 黄万伟, 袁博, 王苏南, 等. 基于非零和信号博弈的主动防御模型[J]. 郑州大学学报(工学版), 2022, 43(1): 90-96.
HUANG W W, YUAN B, WANG S N, et al. Proactive defense model based on non-zero-sum signal game[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(1): 90-96.

[3] XIE N, LI Z Y, TAN H J. A survey of physical-layer au-

thentication in wireless communications[J]. IEEE Communications Surveys & Tutorials, 2021, 23(1): 282-310.

[4] FANG H, WANG X B, HANZO L. Learning-aided physical layer authentication as an intelligent process[J]. IEEE Transactions on Communications, 2018, 67(3): 2260-2273.

[5] ZHANG N, FANG X J, WANG Y, et al. Physical-layer authentication for Internet of Things via WFRFT-based Gaussian tag embedding[J]. IEEE Internet of Things Journal, 2020, 7(9): 9001-9010.

[6] 李兆斌, 崔钊, 魏占祯, 等. 基于物理层信道特征的无线网络认证机制[J]. 计算机科学, 2020, 47(12): 267-272.
LI Z B, CUI Z, WEI Z Z, et al. Wireless network authentication method based on physical layer channel characteristics[J]. Computer Science, 2020, 47(12): 267-272.

[7] XIE N, CHEN C S, MING Z. Security model of authentication at the physical layer and performance analysis over fading channels[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(1): 253-268.

[8] 吴聪, 杨炜伟. 基于嵌入水印的物理层认证及优化[J]. 通信技术, 2020, 53(9): 2233-2240.
WU C, YANG W W. Physical layer authentication and optimization based on embedded watermark[J]. Communications Technology, 2020, 53(9): 2233-2240.

[9] 吴小燕, 刘强, 朱成璋. 社交网络中协同舆论欺诈检测方法应用研究[J]. 郑州大学学报(工学版), 2022, 43(2): 7-14.
WU X Y, LIU Q, ZHU C Z. Research on application of collaborative public opinion fraud detection method in social network[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(2): 7-14.

[10] 李靖, 葛建华, 王勇, 等. 一种资源利用率高的协作无线系统[J]. 西安电子科技大学学报, 2009, 36(1): 28-32, 51.
LI J, GE J H, WANG Y, et al. Resource efficient cooperative wireless system[J]. Journal of Xidian University, 2009, 36(1): 28-32, 51.

[11] GU Z F, CHEN H, XU P P, et al. Physical layer authentication for non-coherent massive SIMO-enabled industrial IoT communications[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3722-3733.

QAM Based Physical Layer Authentication Technology for Cooperative Communication Systems

HAN Gangtao, LIU Ruixue, YAN Li, WANG Junjie, MA Xuefen

(School of Electrical and Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: A quadrature amplitude modulation (QAM) based cooperative physical layer authentication mechanism was proposed for the identity authentication in two-user cooperative communication systems. In the proposed mechanism, two single-antenna users transmitted their own messages and tags as well as those of the partner with the in-phase component and orthogonal component, respectively. Thus, the messages and tags of two users could be uniquely decomposed. Maximal ratio combining was employed at the base station to detect the messages and tags, and physical layer identity authentication was performed through tag comparison. In a typical scenario with equal power distribution and symmetric user uplink channels, the closed expressions of symbol error rates of message and tag were derived. The simulation results showed that the authentication probability of the proposed mechanism was improved by 12%-20% compared with the non-cooperative physical layer authentication when the signal-to-noise ratio (*SNR*) was 6-15 dB. Meanwhile, the authentication probability of illegal attack remained only around 10^{-3}. Consequently, the proposed mechanism had better authentication performance.

Keywords: physical layer authentication; cooperative communication; tag superposition; maximal ratio combining; QAM