基于三方生成对抗网络的隐蔽通信方法

于季弘[1]，林子砚[1]，叶能[2]，杨凯[1]，安建平[2]

（1. 北京理工大学信息与电子学院，北京 100081；
2. 北京理工大学网络空间安全学院，北京 100081）

摘 要：针对隐蔽通信中隐蔽信息的传输隐蔽性与解调准确性联合优化问题，设计了一种新型三方生成对抗网络（TripartiteGAN），提出了基于该神经网络的隐蔽通信方法，并给出理论性能分析。TripartiteGAN 隐蔽通信方法从幅度和相位等维度对经传统数字调制后的隐蔽信号进行优化，使最终生成的隐蔽信号与公开的合法信号叠加发送后，其信号分布逼近仅存在合法信号时的分布。该方法可以应对利用神经网络进行信号监测的侦听方，此侦听方不需要发送方功率特征先验信息，不需要人为确定检测阈值。仿真实验结果表明，在加性白高斯噪声信道下，所提 TripartiteGAN 隐蔽通信方法在保证隐蔽信息接收方解调准确率的同时，可使侦听方判决当前信号是隐蔽信号或合法信号的概率均逼近 0.5。该方法的解调准确率和隐蔽性均优于现有基于生成对抗网络的隐蔽通信方法。

关键词：无线通信；生成对抗网络；隐蔽通信；机器学习

中图分类号：TN929.52

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023215

Covert communication method based on tripartite generative adversarial network

YU Jihong[1], LIN Ziyan[1], YE Neng[2], YANG Kai[1], AN Jianping[2]

1. School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China
2. School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China

Abstract: A novel tripartite generative adversarial network (TripartiteGAN) and a covert communication method based on TripartiteGAN were designed for jointly optimizing the transmission covertness and the demodulation accuracy of the covert message. The performance of the method was analyzed. Specifically, TripartiteGAN was used to manipulate the amplitude and phase of an input modulated covert data so that the distribution of the generated covert signal superposing the overt signal approximates to that of the overt signal for the public user. The proposed method could work with an optimum warden that needs neither to set the detection threshold manually nor to know the transmit power characteristics of the sender. Simulation results show that under the additive white Gaussian noise channel, the proposed TripartiteGAN improved the demodulation accuracy at the covert receiver end while keeping the probability of regarding the detected signal as the covert one or the overt one at the warden around 0.5. Moreover, the proposed method outperforms the existing covert communication scheme based on generative adversarial network (GAN).

Keywords: wireless communication, generative adversarial network, covert communication, machine learning

收稿日期：2023−05−26；**修回日期：**2023−08−15

通信作者：安建平，an@bit.edu.cn

基金项目：国家自然科学基金资助项目（No.62271055, No.U1836201）

Foundation Item: The National Natural Science Foundation of China (No.62271055, No.U1836201)

0 引言

无线通信具备部署灵活、通信速率高等优势，相关的蜂窝通信、室内通信和卫星通信技术已被广泛部署于多种场景。人们利用无线通信传输大量的信息，其中会涉及私密信息。无线信道的广播特性使这些私密信息及通信意图存在被泄露的风险[1]，因此，如何同时保证信息安全和通信意图安全成为当前无线通信中亟待解决的关键问题。

经典的信息安全技术主要分为应用层加密和物理层安全。前者利用密钥和加密算法来扰乱信息，从而使窃听者无法解码正确信息[2-3]；后者通过变化无线信号特征[4]或利用无线信道质量差异性[5]来实现安全通信。这两类方法的重心在于保护传输的信息不被窃听者解码，而无法隐藏通信双方的通信意图。

近年来，隐蔽通信成为可以同时提供信息安全和通信意图安全的解决方案[6]。隐蔽通信可以将敏感信息隐藏于噪声或承载合法信息的无线信号中进行隐蔽传输，从而使侦听方难以检测到隐蔽信号的存在。由于侦听方仅能概率性地检测隐蔽通信是否存在，因此隐蔽通信也称为低检测概率通信。Bash 等[7]、Che 等[8]、Wang 等[9]和 Abdelaziz 等[10]分别研究了加性白高斯噪声信道、二进制对称信道、离散无记忆信道和 MIMO（multiple input multiple output）信道下的隐蔽通信容量，奠定了平方根律的理论基石。研究人员在隐蔽通信理论指导下设计了干扰辅助的隐蔽通信方法，可以提升隐蔽通信速率，包括集接收和干扰于一体的全双工接收端[11]、增加额外的辅助干扰节点[12]、利用合法用户信号充当干扰源[13-14]等。此外，Yan 等[15]从理论上证明非高斯信号可以具有比高斯信号更佳的隐蔽性能。Liao 等[16]利用生成对抗网络（GAN, generative adversarial network）来配置隐蔽信号功率和合法信号功率，该方法不需要人为干预，但是与传统随机功率方法本质相同，仅涉及信号幅值参数的优化，缺少对信号完整特征的考虑，因此隐蔽性能仍有很大的提升空间。

现有研究具有如下局限。其一，假设侦听方仅根据信号功率特性进行判决，如果侦听方具备检测信号其他特征的能力，如信号相位等，那么隐蔽性能将会退化。其二，性能度量大多仅考虑隐蔽性能，忽略隐蔽信息接收方接收信息的可靠性，甚至造成接收时隐蔽信息误码率过高，不适于实际应用。其三，假设发送方在设计传输功率方案时知道侦听方功率计门限，或者假设侦听方具有发送方发送功率的先验信息。针对上述问题，本文面向将隐蔽信号隐藏于公开的合法信号下的隐蔽通信场景，提出了一种新型三方生成对抗学习网络，并基于此神经网络设计了隐蔽通信方法。该方法以通信信号的隐蔽为目标，利用发送方和隐蔽信息接收方的合作性以及侦听方和发送方的对抗性，训练生成对抗网络，同时从幅度和相位两方面对通信信号的波形进行优化。在方法层面，在经典生成对抗网络的基础上，加入了一个新的神经网络来增强隐蔽信息接收方的解调可靠性，并设计了针对三方对抗的神经网络损失函数，通过在损失函数中加入 2 个调控系数来调控三方神经网络间的对抗强度。所提方法可以有效提升隐蔽信息接收方的接收可靠性；可用于有限长度的发送信号序列和受限的功率，更贴近实际系统；不需要功率计门限或功率信息等功率方面的先验信息；针对最优侦听方，性能优于现有基于 GAN 的隐蔽通信方法。

1 基于 TripartiteGAN 的隐蔽波形设计

1.1 隐蔽通信系统模型

如图 1 所示，隐蔽通信系统模型主要由四部分构成，分别是发送方（如地面基站或卫星）、隐蔽信息接收方、侦听方和公开用户。侦听方尝试检测发送方和隐蔽信息接收方之间的信号传输，而发送方则尝试利用自己和公开用户间的通信信号（称为合法信息）作为掩体来掩护其与隐蔽信息接收方间的隐蔽通信。假设每个节点配备一根天线，且接收方和侦听方均已知其自身与发送方之间信道状态。假设通信的基本单位是时隙，发送方、侦听方和接收方时间同步齐次。在每个时隙，发送方要么仅发送合法信息，要么发送隐蔽信息和合法信息的叠加信号，侦听方监测无线信道来检测发送方是否发送了隐蔽信息。

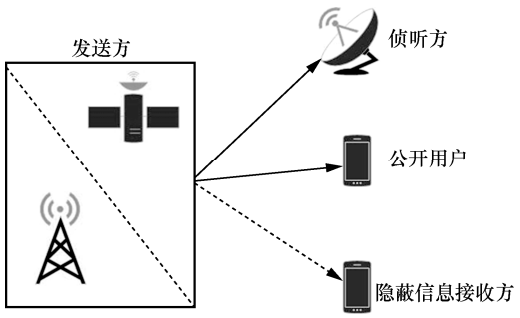


图 1 隐蔽通信系统模型

经典的生成对抗网络仅涉及生成器和鉴别器两方之间的博弈，而隐蔽通信不但需要关注发送方与侦听方间的对抗，还需要考虑发送方与隐蔽信息接收方间的协作。因此，经典的生成对抗网络难以直接用于隐蔽通信波形设计。针对这一问题，本文受三方生成对抗网络 TripleGAN[17]启发，设计了一种适用于隐蔽通信波形设计的神经网络 TripartiteGAN，其结构如图 2 所示。

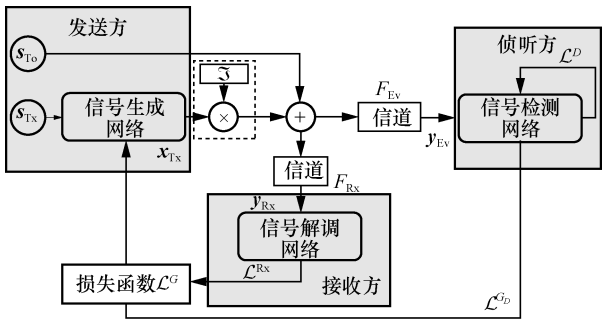


图 2　TripartiteGAN 结构

TripleGAN 包含 3 个神经网络，第 1 个网络根据真实标签生成假样本，第 2 个网络根据真实样本生成假标签，将这 2 种生成的数据和真实样本真实标签的数据共同输入第 3 个网络中从而完成对抗过程。TripleGAN 的 3 个网络的输入和输出一致（均为标签和数据），其对抗关系只有两方。

与 TripleGAN 不同，TripartiteGAN 由信号生成网络、信号检测网络和信号解调网络三部分组成，分别负责发送方的信号生成、侦听方的信号检测和隐蔽信息接收方的信号解调。TripartiteGAN 涉及发送方、侦听方和隐蔽信息接收方三方对抗，且 3 个网络的输入输出不一致。TripartiteGAN 中三方神经网络的连接结构如图 3 所示，信号生成网络只输入隐蔽信息，而信号检测网络输入隐蔽信息和合法用户信息。此外，这 3 个网络拥有和 TripleGAN 完全不同的损失函数。TripartiteGAN 的对抗性从损失函数的极大极小值这一神经网络的本质问题来看，三方存在相互制约的参量；从通信系统来看，信号生成网络和信号检测网络之间的对抗与经典生成对抗网络[18]的思想相同，但是信号解调网络是对生成器 G 的一个约束，其不会对信号检测网络的训练产生直接影响。但是隐蔽信息接收方希望自身的解码准确率更高，而提高解码准确率的方法除了提高信号解调网络的性能之外，还可以利用信号生成网络使发送的隐蔽信号更容易解调；而侦听方的信号检测网络为了获得更好的检测准确率，希望信号生成网络输出的信号幅度更高。由此可见，信号检测网络和信号解调网络均与信号生成网络有对抗过程，因此本文提出的 TripartiteGAN 更加适用于解决以合法信号作为掩体的隐蔽通信问题。

1.2　基于 TripartiteGAN 的隐蔽通信方法

1) 发送方

发送方发送的信号包含 $\boldsymbol{s}_{\mathrm{To}}$ 和 $\boldsymbol{s}_{\mathrm{Tx}}$ 两部分，其中，$\boldsymbol{s}_{\mathrm{To}}=\left\{s_{\mathrm{To},1}, s_{\mathrm{To},2},\cdots,\mathrm{s}_{\mathrm{To},N}\right\}$ 是公开用户发送的合法信息，$\boldsymbol{s}_{\mathrm{Tx}}=\left\{s_{\mathrm{Tx},1},s_{\mathrm{Tx},2},\cdots,s_{\mathrm{Tx},N_{\mathrm{Tx}}}\right\}$ 是需要隐蔽传输的敏感信息，N 是发送方在一个时隙内所传送的符号数。在信号发送前，发送方首先通过信号生成网络对需要隐蔽传输的信号 $\boldsymbol{s}_{\mathrm{Tx}}$ 进行幅值和相位处理。处理后的信号可以表示为

$$\boldsymbol{x}_{\mathrm{Tx}}=G(\boldsymbol{s}_{\mathrm{Tx}})=\left\{x_{\mathrm{Tx},1},x_{\mathrm{Tx},2},\cdots,x_{\mathrm{Tx},N_{\mathrm{Tx}}}\right\} \tag{1}$$

由于 $\boldsymbol{x}_{\mathrm{Tx}}$ 的长度可能小于 $\boldsymbol{s}_{\mathrm{To}}$，因此对 $\boldsymbol{x}_{\mathrm{Tx}}$ 执行式(2)所示操作，使 $\boldsymbol{x}_{\mathrm{Tx}}$ 的长度等于 N。

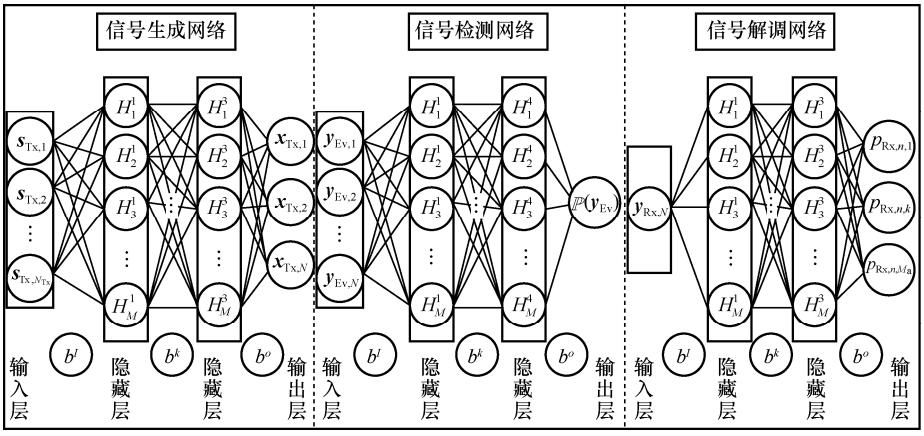


图 3　TripartiteGAN 中三方神经网络的连接结构

$$\boldsymbol{x}_{\mathrm{Tx}}=\begin{cases}\boldsymbol{x}_{\mathrm{Tx}} & , \quad N=N_{\mathrm{Tx}} \\ \{\boldsymbol{x}_{\mathrm{Tx}},\underbrace{0,\cdots,0}_{N-N_{\mathrm{Tx}}}\} & , N_{\mathrm{Tx}}<N\leqslant 2N_{\mathrm{Tx}} \\ \{\underbrace{\boldsymbol{x}_{\mathrm{Tx}},\cdots,\boldsymbol{x}_{\mathrm{Tx}}}_{\frac{N}{N_{\mathrm{Tx}}}},\underbrace{0,\cdots,0}_{N \bmod N_{\mathrm{Tx}}}\}, & N>2N_{\mathrm{Tx}}\end{cases} \tag{2}$$

随后，发送方将经过处理的隐蔽信号 $\boldsymbol{x}_{\mathrm{Tx}}$ 和公开用户的信号 $\boldsymbol{s}_{\mathrm{To}}$ 进行叠加并发送，叠加后的信号可以表示为

$$\boldsymbol{x}_{\mathrm{T}}=\Im\boldsymbol{x}_{\mathrm{Tx}}+\boldsymbol{s}_{\mathrm{To}} \tag{3}$$

其中，$\Im$ 是预设的系统参数，用来控制信号生成网络输出信号幅值的大小（如节点功率受限）。具体来说，信号生成网络在最后的全连接网络加入一个激活函数 Tanh，通过这个激活函数将输出信号的幅值限制在一定范围，这可以保证所设计方法适用于受不同功率限制的发送方。

因为接收方和侦听方均已知其自身与发送方之间信道状态，所以发送方与接收方之间的通信信道和发送方与侦听方之间的侦听信道可以被视为加性白高斯噪声信道。

信号生成网络的输入和输出神经元个数与一个时隙内发送方发送的隐蔽信息所需的比特数成正比。隐蔽信息总长度的增加只影响时隙个数，对输入输出神经元个数没有影响。载体长度会增加隐蔽信息对应的数字信号长度，具体关系为

$$N=N_{\mathrm{s}}L_{\mathrm{c}} \tag{4}$$

其中，N_{s} 是一个时隙内发送的未经调制的隐蔽信息比特数，L_{c} 是载体长度。

2) 侦听方

侦听方收到的信号为

$$\boldsymbol{y}_{\mathrm{Ev}}=\boldsymbol{F}_{\mathrm{Ev}}\boldsymbol{x}_{\mathrm{T}}+\boldsymbol{n}_{\mathrm{Ev}}=\left\{y_{\mathrm{Ev},1},y_{\mathrm{Ev},2},\cdots,y_{\mathrm{Ev},N}\right\} \tag{5}$$

其中，$\boldsymbol{F}_{\mathrm{Ev}}$ 表示信号从发送方到侦听方所经历的衰减，$\boldsymbol{n}_{\mathrm{Ev}}$ 为侦听方处的加性白高斯噪声。

侦听方利用信号检测网络对接收的信号 $\boldsymbol{y}_{\mathrm{Ev}}$ 进行处理。经过各层神经元后，信号检测网络的输出为一个常量 $\Lambda_{\mathrm{D}}\in[0,1]$。该值越大，表明当前检测到的信号越可能是隐蔽信号。随后，将 Λ_{D} 与神经网络中提前设置好的阈值 V 进行比较。假设发送方发送 0 和 1 是等概率的，通常设置 V=0.5。当 $\Lambda_{\mathrm{D}}>V$ 时，信号检测网络判定环境中存在隐蔽通信；反之，则判定环境中没有隐蔽通信。经过隐蔽通信生成→阈值判决检测→隐蔽通信生成的不断循环迭代训练后，信号生成网络所生成的波形的隐蔽通信性能不断提升，同时侦听方的检测能力也不断提升。Goodfellow 等[18]证明了通过不断对抗最终获得的鉴别器是最优的，因此本文提出的 TripartiteGAN 获得的鉴别器是针对当前隐蔽信号的所有侦听策略当中最优的。理想情况下，希望 Λ_{D}=0.5，表示当前检测到的信号是隐蔽信号的概率为 0.5，是合法信号的概率也为 0.5。

信号检测网络的输入神经元个数与信号 $\boldsymbol{x}_{\mathrm{T}}$ 的长度有关。根据式(3)，$\boldsymbol{x}_{\mathrm{T}}$ 和公开用户发送的信息长度和信号生成网络的输出信息长度有关。由于公开用户一直发送信息，公开用户的信息长度一定大于或等于隐蔽用户的信息长度，因此信号检测网络的输入神经元个数由公开用户发送的信息长度决定。信号检测网络的输出是一个常量，因此输出神经元个数不发生变化，始终为 1。

3) 接收方

接收方收到的信号为

$$\boldsymbol{y}_{\mathrm{Rx}}=\boldsymbol{F}_{\mathrm{Rx}}\boldsymbol{x}_{\mathrm{T}}+\boldsymbol{n}_{\mathrm{Rx}}=\left\{y_{\mathrm{Rx},1},y_{\mathrm{Rx},2}\cdots,y_{\mathrm{Rx},N}\right\} \tag{6}$$

其中，$\boldsymbol{F}_{\mathrm{Rx}}$ 表示信号从发送方到接收方所经历的衰减，$\boldsymbol{n}_{\mathrm{Rx}}$ 为接收方处的加性白高斯噪声。

为保证解调可靠性，将信号解调网络隐藏层的神经元个数设置为

$$M_i=2M_{i-1}+1 \tag{7}$$

其中，M_i 是当前层神经元个数，M_{i-1} 是上一层神经元个数。信号生成网络和信号检测网络中的神经元个数可以采用相同的方式进行设置。在实际部署神经网络时，可以根据神经网络的拟合情况适当地改变神经网络的规模，使在保持网络规模较小的情况下尽可能匹配不同长度的输入信号，从而减小网络的训练时间。信号解调网络有 M_{a} ($M_{\mathrm{a}}>2$)个输出神经元，对应相关调制星座图上的点数。例如，QPSK 调制下 $M_{\mathrm{a}}=4$，BPSK 调制下 $M_{\mathrm{a}}=2$，即解调过程是二分类问题，所以信号解调网络的输出神经元个数为 1。

信号解调网络的输入粒度是符号级，即在一段时间窗内发送方传输给隐蔽信息接收方的一串数字信号序列中的一个信号，输入神经元个数为 1。每个输出神经元会输出一个数值 $p_{\mathrm{Rx},n,k}$，代表神经网络判决第 n 个信号出现在第 k 个星座点的概率。在所有输出中，最大的 $p_{\mathrm{Rx},n,k}$ 所对应的信息会被认

为是接收到的信号所携带的隐蔽信息。也就是说，接收方通过信号解调网络对每一个信号单独进行处理，根据信号解调网络输出值的大小，将最大的数值所对应的信息作为最终的解调信息。

2　TripartiteGAN 设计

本节介绍 TripartiteGAN 的神经网络设计、隐蔽传输算法和性能分析。TripartiteGAN 中三方神经网络的网络单元如图 4 所示。将采用经典调制方式调制后的隐蔽信息输入信号生成网络，会输出一个变换后的隐蔽信号。这个信号与合法信号叠加后进行传输。叠加后的信号将被隐蔽信息接收方和侦听方检测到，分别是信号解调网络和信号检测网络的输入，这 2 个网络分别对此输入信号进行判决。下面将展开详细介绍。

2.1　神经网络设计

1) 信号生成网络

位于发送方处的信号生成网络在生成隐蔽通信时，需要在保证信息传输质量的同时，尽可能地减少通信信号被侦听方发现的概率。图 4(a)展示了信号生成网络的结构。信号生成网络以经过 BPSK 或 QPSK 调制的信号为输入，经过复实信号转换层，将复信号转换成实信号，便于神经网络的输入。再经过三层全连接层和 ReLU 激活函数，其作用是提取信号的特征结构。再经过一个输出神经元个数与输入隐蔽信号个数相同的全连接层，对提取的特征进行重构。将重构后的信号通过功率限制层，从而加入功率上的限制。如前文所述，功率限制层采用激活函数 Tanh，并搭配超参数 $\Im$ 实现有效的功率控制。最后，通过实复信号转换层，形成信号生成网络的最终输出信号。

定义信号生成网络的损失函数为

$$\mathfrak{L}^{G}=\phi\mathfrak{L}^{G_D}+\psi\mathfrak{L}^{\mathrm{Rx}} \tag{8}$$

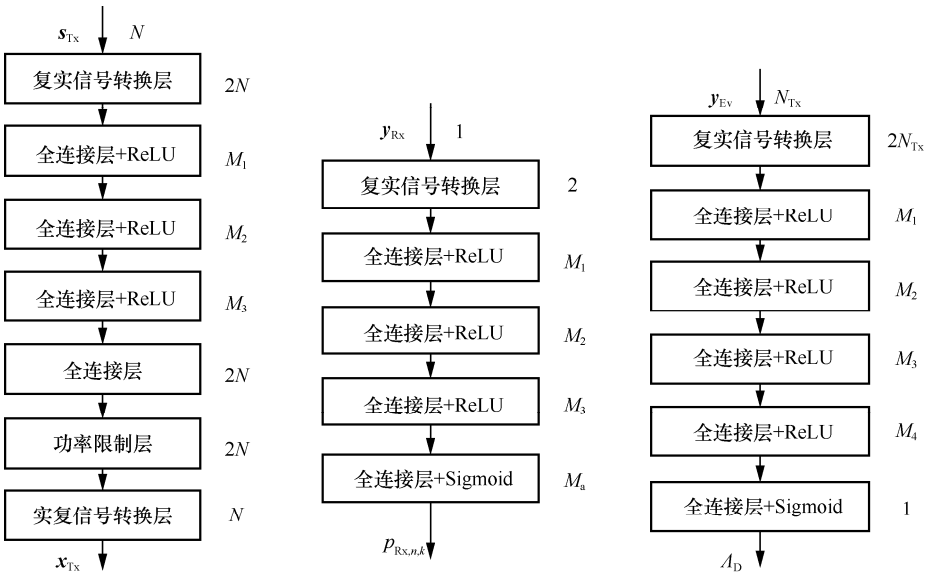
其中，ϕ 和 ψ 是 2 个常数，依据神经网络训练结果确定，ϕ 值通常随着发送方信号幅值的增大而逐渐减小，否则信号生成网络由于过度重视隐蔽性能导致隐蔽信息接收方的解调准确率急剧下降，甚至会得到随机等概率进行判决的信号解调网络；$\mathfrak{L}^{\mathrm{Rx}}$ 是信号解调网络的损失函数，$\mathfrak{L}^{G_D}$ 是侦听方的判别结果反馈到信号生成网络后所得到的损失函数，计算式为

$$\mathfrak{L}^{G_D}=-\log\left(1-\mathbb{P}(\boldsymbol{y}_{\mathrm{Ev}}|\delta_1)\right) \tag{9}$$

其中，δ_1 表示环境中存在隐蔽通信；$\mathbb{P}\left(\boldsymbol{y}_{\mathrm{Ev}}|\delta_1\right)$ 表示在有隐蔽信息传输的情况下，鉴别器（即侦听方）成功检测出隐蔽通信的概率。

2) 信号解调网络

发送方信号在经过神经网络处理后，会失去原有的信号特征（BPSK 或 QPSK 等信号调制的特征），需要重新探索对应的解调方法。因此，本文加入信号解调网络。信号解调网络的主要作用是在有噪声和合法信号的干扰下，通过神经网络直接拟



(a) 信号生成网络　　(b) 信号解调网络（接收）　　(c) 信号检测网络（侦听）

图 4　TripartiteGAN 中三方神经网络的网络单元

合出高效的信号解调方法以便接收方将发送方所传输的隐蔽信息正确解调，从而保证隐蔽信号的可靠接收。

信号解调网络的结构如图 4(b)所示，将隐蔽信息接收方接收到的信号直接输入信号解调网络。接收信号经复实信号转换层和 ReLU 激活函数，由复信号转换成实信号。再经过三层全连接层，对信号中的合法用户信号和噪声信号进行分析，进而在接收信号中提取隐蔽信息的特征。再利用全连接层和 Sigmoid 激活函数或 Softmax 激活函数将提取到的隐蔽信息的特征转化为特定隐蔽信息的概率值，即 $p_{\mathrm{Rx},n,k}$。

信号解调网络的损失函数是通过交叉熵损失函数变形得到的。对于不同的 M_{a}，信号解调网络损失函数有不同的变形结果。当 $M_{\mathrm{a}}>2$ 时，信号解调网络的损失函数定义为

$$\mathfrak{L}^{\mathrm{Rx}}=-\sum_{n=1}^{N}\sum_{k=1}^{M_a}\left(\tilde{p}_{\mathrm{Rx},n,k}\log(p_{\mathrm{Rx},n,k})\right) \tag{10}$$

$\mathfrak{L}^{\mathrm{Rx}}$ 是隐蔽信息接收方的判别结果反馈到发送方生成器后得到的损失函数。其中，$p_{\mathrm{Rx},n,k}$ 是信号解调网络的输出值，$\tilde{p}_{\mathrm{Rx},n,k}$ 是发送方当前发送的符号是第 k 个星座点的概率，起到标签的作用。令 x_k 表示隐蔽信号星座点对应的码字，则有

$$\tilde{p}_{\mathrm{Rx},n,k}=\begin{cases}1, x_k=\mathrm{s}_{\mathrm{Tx},n}\\ 0, x_k\neq s_{\mathrm{Tx},n}\end{cases} \tag{11}$$

当 $M_a=2$ 时，信号解调网络的损失函数定义为

$$\mathfrak{L}^{\mathrm{Rx}}=-\sum_{n=1}^{N}\sum_{k=1}^{M_a}\left(\tilde{p}_{\mathrm{Rx},n,k}\log(p'_{\mathrm{Rx},n,k})\right) \tag{12}$$

其中，$p'_{\mathrm{Rx},n,k}$ 是信号解调网络判断第 n 个信号是第 k 个星座点的概率，表达式为

$$p'_{\mathrm{Rx},n,k}=\begin{cases}p_{\mathrm{Rx},n,k}, & x_k=1\\ 1-p_{\mathrm{Rx},n,k}, & x_k=0\end{cases} \tag{13}$$

3) 信号检测网络

信号检测网络主要用于判断环境中是否存在隐蔽通信行为。图 4(c)是信号检测网络的网络结构，侦听方将接收到的信号以序列的形式输入信号检测网络中，通过全连接层和 ReLU 激活函数组成的连续结构，分析信号中合法用户信息和噪声的成分，最后利用全连接层和 Sigmoid 激活函数将分析结果转化成有无隐蔽信息的概率。

定义信号检测网络的损失函数为

$$\mathfrak{L}^{D}=-\log\left(\mathbb{P}(\boldsymbol{y}_{\mathrm{Ev}}|\delta_1)\right)-\log\left(1-\mathbb{P}(\boldsymbol{y}_{\mathrm{Ev}}|\delta_0)\right) \tag{14}$$

其中，δ_0 表示环境中不存在隐蔽通信；$\mathbb{P}(\boldsymbol{y}_{\mathrm{Ev}}|\delta_0)$ 表示在无隐蔽通信行为的情况下，鉴别器检测出隐蔽通信（即误判）的虚警概率。

通过式(9)和式(14)可知，信号生成网络和信号检测网络虽然具有不对称的输入信号形式，但是两者优化的损失函数都与 $\mathbb{P}(\boldsymbol{y}_{\mathrm{Ev}}|\delta_1)$ 和 $\mathbb{P}(\boldsymbol{y}_{\mathrm{Ev}}|\delta_0)$ 有关，所以不对称的输入不会导致网络无法收敛。

根据图 3 中信号检测网络结构可知，信号检测网络是一个深度神经网络（DNN, deep neural network）。Wang 等[19]研究表明，能量检测方法需要在具备一定先验信息的条件下通过计算才能得到最优的检测门限，而使用 DNN 的侦听方不需要通过计算获得检测门限，只需在信号检测网络训练过程中设置常量门限为 V=0.5[16]。

2.2 隐蔽传输算法

首先，将调制（如 BPSK 或 QPSK 或其他通信调制方式）后的隐蔽信息输入信号生成网络。此处需要设置好 TripartiteGAN 独有的网络超参数(包括 $\Im,\phi,\psi$)、优化器参数（包括学习率）、betas 以及全连接层初始化方法所需的参数（包括高斯分布的均值、方差）。然后，将信号生成网络输出的隐蔽信号与合法用户信号叠加，分别通过侦听方信道和隐蔽信息接收方信道传到信号检测网络和信号解调网络中。在训练信号生成网络时，固定信号检测网络和信号解调网络的参数不变，最小化损失函数式(8)。在训练信号解调网络和信号检测网络时，固定信号生成网络的参数不变，分别最小化损失函数式(10)或式(12)和式(14)。不断重复以上过程，直到网络达到收敛。

2.3 TripartiteGAN 性能分析

本文中，隐蔽信息发送方利用神经网络生成隐蔽信号，侦听方并非采用经典隐蔽通信理论中功率计，而是利用神经网络来监测信道并对信道中的信号进行判别。由于无法对神经网络的输出信号进行式化表征，因此本文没有采用经典隐蔽通信理论的分析框架，而是扩展了 Goodfellow 等[18]提出的经典 GAN 最优性证明方法，从 KL（Kullback-Leibler）散度和 JS（Jensen-Shannon）散度 2 个角度，证明

TripartiteGAN 存在最优解且在网络收敛时取得最优解，此时 KL 散度和 JS 散度均逼近 0，表明 TripartiteGAN 实现了最佳的隐蔽性和可靠性。

信号解调网络处的 KL 散度可表示为

$$\begin{aligned}&\mathrm{KL}(p_{\mathrm{Tx},i}\|q_{\mathrm{Rx},i})=\int p_{\mathrm{Tx},i}\log\left(\frac{p_{\mathrm{Tx},i}}{q_{\mathrm{Rx},i}}\right)\mathrm{d}x=\\&\int p_{\mathrm{Tx},i}\log\left(\frac{1}{q_{\mathrm{Rx},i}}\right)\mathrm{d}x-\int p_{\mathrm{Tx},i}\log\left(\frac{1}{p_{\mathrm{Tx},i}}\right)\mathrm{d}x=\\&H(p_{\mathrm{Tx},i}\|q_{\mathrm{Rx},i})-H(p_{\mathrm{Tx},i})\end{aligned}\tag{15}$$

其中，$p_{\mathrm{Tx},i}$ 是发送方发送的隐蔽信息 $s_{\mathrm{Tx},i}$ 的分布，$q_{\mathrm{R}x,i}$ 是信号解调网络输出的信号分布；当发送方发送的隐蔽信息调制方式确定后，$H(p_{\mathrm{Tx},i})$ 是常数。因此，优化 KL 散度相当于优化交叉熵 $H(p_{\mathrm{Tx},i}\|q_{\mathrm{Rx},i})$。交叉熵的计算式为

$$H\left(p_{\mathrm{Tx},i}\|q_{\mathrm{Rx},i}\right)=-\int p_{\mathrm{Tx},i}\log(q_{\mathrm{Rx},i})\mathrm{d}x\tag{16}$$

比较式(10)或式(12)和式(16)可知，最小化信号解调网络的损失函数等价于最小化交叉熵，即

$$\begin{aligned}&\min\mathfrak{L}^{\mathrm{Rx}}\equiv\min H(p_{\mathrm{Tx},i}\|q_{\mathrm{Rx},i})=\\&\min\left(-E_{x\sim p_{Tx,i}}(\log(U(\boldsymbol{F}_{\mathrm{Rx}}(\Im G(\boldsymbol{x})+\boldsymbol{s}_{\mathrm{To}})+\boldsymbol{n}_{\mathrm{Rx}})))\right)=\\&\min\left(\mathrm{KL}(p_{\mathrm{Tx},i}\|q_{\mathrm{Rx},i})+H(p_{\mathrm{Tx},i})\right)\end{aligned}\tag{17}$$

在训练 TripartiteGAN 时，本文采用了 2 种常见的标签反转技巧以提高网络的训练效率。经典的 GAN 生成器生成的数据标签为 0，而非生成器生成的数据标签为 1。不同于此，本文在训练 TripartiteGAN 的信号检测网络时，将 2 个标签调换，即含有信号生成网络生成的隐蔽信息的信号标签为 1，不含隐蔽信息的信号标签为 0。因此，信号检测网络的损失函数表示为

$$\begin{aligned}&\mathfrak{L}^{D}=-\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Tx}}}(\log(D(F_{\boldsymbol{Ev}}(\Im G(\boldsymbol{x})+\boldsymbol{s}_{\mathrm{To}})+\boldsymbol{n}_{\mathrm{Ev}})))-\\&\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Ev}}^{0}}(\log(1-D(\boldsymbol{x})))=-\\&\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Ev}}^{1}}(\log(D(\boldsymbol{x})))-\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Ev}}^{0}}(\log(1-D(\boldsymbol{x})))\end{aligned}\tag{18}$$

其中，p_{Tx} 是发送方发送的隐蔽信息 $\boldsymbol{s}_{\mathrm{Tx}}$ 的分布，p_{Ev}^{1} 是侦听方接收的含有隐蔽信息的信号分布，p_{Ev}^{0} 是侦听方接收的不含隐蔽信息的信号分布，$D(x)$是检测网络输出值。

对于经典 GAN，生成器生成的数据标签和鉴别器处的标签相同，但在训练 TripartiteGAN 时，信号生成网络处的数据标签和信号检测网络处的数据标签相反。因此，信号生成网络的损失函数表示为

$$\mathfrak{L}^{G_D}=-\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Ev}}^{1}}(\log(1-D(\boldsymbol{x})))\tag{19}$$

根据复合函数的单调性，最小化式(19)等价于

$$\min\mathfrak{L}^{G_D}\equiv\max\left(-\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Ev}}^{1}}(\log(D(\boldsymbol{x})))\right)\tag{20}$$

结合式(17)、式(18)和式(20)，最优化三方神经网络的损失函数等效于求解 TripartiteGAN 的极大极小值问题，表示为

$$\begin{aligned}&\max_{G}\max_{U}\min_{D}V(G,D,U)=\\&\max_{G}\max_{U}\min_{D}-\phi\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Tx}}}(\log(D(\boldsymbol{F}_{\mathrm{Ev}}(\Im G(\boldsymbol{x})+\boldsymbol{s}_{\mathrm{To}})+\boldsymbol{n}_{\mathrm{Ev}})))-\\&\phi\mathrm{E}_{\boldsymbol{x}\sim p_{\mathrm{Ev}}^{0}}(\log(1-D(\boldsymbol{x})))+\\&\psi NE_{x\sim p_{\mathrm{Tx},i}}(\log(U(x|\mathrm{x}\in\boldsymbol{F}_{\mathrm{Rx}}(\Im G(\boldsymbol{x})+\boldsymbol{s}_{\mathrm{To}})+\boldsymbol{n}_{\mathrm{Rx}})))\end{aligned}\tag{21}$$

当固定信号生成网络时，TripartiteGAN 信号检测网络极值求解和 GAN 相同，最优信号检测网络为

$$D_{G}^{*}(\boldsymbol{x})=\frac{p_{\mathrm{Ev}}^{1}}{p_{\mathrm{Ev}}^{0}+p_{\mathrm{Ev}}^{1}}\tag{22}$$

将式(22)代入式(21)，可以得到

$$\begin{aligned}&C(G,U)=\min_{D}V(G,D,U)=\\&\phi\log4-2\phi\mathrm{JS}(p_{\mathrm{Ev}}^{1}\|p_{\mathrm{Ev}}^{0})-\\&\psi N(\mathrm{KL}(p_{\mathrm{Tx},i}\|q_{\mathrm{R}_{x},i})+H(p_{\mathrm{Tx},i}))\end{aligned}\tag{23}$$

式(23)右边第一项和 $H(p_{\mathrm{Tx},i})$ 是常数，JS 散度和 KL 散度都大于或等于 0，因此最小化 JS 散度和 KL 散度可以得到 $C(G,U)$的最大值。当且仅当 $p_{\mathrm{Ev}}^{1}=p_{\mathrm{Ev}}^{0},p_{\mathrm{Tx},i}=q_{\mathrm{Rx},i}$ 时，JS 散度和 KL 散度等于 0。其中，$p_{\mathrm{Ev}}^{1}=p_{\mathrm{Ev}}^{0}$ 约束信号生成网络生成的信号分布，$p_{\mathrm{Tx},i}=q_{\mathrm{Rx},i}$ 约束经过信号解调网络解调后的信号分布。信号解调网络解调后的信号是由信号生成网络生成的信号经过信号解调网络得到的。根据 Zhu 等[20]的研究，当神经网络容量足够大时，可以将相同的数据映射到任意数据集。因此，2 个约束条件可以同时成立，此时 TripartiteGAN 达到了当前环境约束下的最优解。这也说明 TripartiteGAN 可最大化隐蔽性和隐蔽信息传输的可靠性，在达到稳态时系统取得最佳性能。

3 实验结果及分析

本节通过实验评估 TripartiteGAN 的性能，并比较该方法与已有基于 GAN[16]的隐蔽通信方法的性能。为了公平比较，实验中赋予基于 GAN 的隐蔽通信方法中的侦听方利用 DNN 进行侦听的能力。实验结果表明，TripartiteGAN 的隐蔽性和解调准确率均优于基于 GAN 的隐蔽通信方法。

3.1 实验参数设置

本文实验设置发送方发送给公开用户的合法信号采用 16QAM，功率为 10 W；发送给隐蔽信息接收方的信号为 QPSK 调制信号或 BPSK 调制信号。生成器和信号解调网络的隐藏层数目设置为 3，鉴别器隐藏层的数目设置为 4，序列长度 N 设置为 12。N 的长度不应过大，否则会导致网络的训练时间过长，且由于 TripartiteGAN 的输入层数是确定的，因此序列长度在系统中是不变量。由于信道为加性白高斯噪声信道，不失一般性地，设置信道衰减 $\boldsymbol{F}_{\mathrm{Rx}}=\boldsymbol{F}_{\mathrm{Ev}}=1$，高斯白噪声功率 $\sigma^2_{\mathrm{Ev}}=\sigma^2_{\mathrm{Rx}}=0.01\,\mathrm{W}$，生成器损失函数的系数 $\frac{\phi}{\psi}=500$。正式训练 TripartiteGAN 之前需要加入 2 个预训练：一是信号解调网络在去除信号生成网络的情况下单独训练，二是信号检测网络在去除信号生成网络的情况下单独训练。这样可以降低网络整体的训练时间，并且防止信号检测网络陷入局部最优解。实验参数如表 1 所示。

表 1 实验参数

网络	超参数	数值
信号生成网络	全连接隐藏层数	3
	全连接隐藏层神经元个数	100，200，300
	训练批数量	256
信号解调网络	全连接隐藏层数	3
	全连接隐藏层神经元个数	5，11，23
	训练批数量	256×12
信号检测网络	全连接隐藏层数	4
	全连接隐藏层神经元个数	25，51，103，207
	训练批数量	256
DNN（基于 GAN 的隐蔽通信方法中的侦听网络）	全连接隐藏层数	3
	全连接隐藏层神经元个数	100，200，300
	训练批数量	256
所有网络	隐藏层激活函数	ReLU
	优化器	Adam
	学习率	0.000 05

3.2 TripartiteGAN 性能评估

本文根据神经网络的判决特点来评估隐蔽信号的传输隐蔽性，即侦听方利用 DNN 对无线信道中传输信号进行检测和判决，其输出是该信号含隐蔽信号的概率（称为检测准确率）。对于理想的隐蔽系统，该检测准确率保持在 0.5，即侦听方认定当前传输信号含隐蔽信号的概率是 0.5，不含隐蔽信号的概率也是 0.5。因此根据实验结果中检测准确率是否逼近 0.5 来衡量隐蔽性。

设置 $\Im$=0.3 和 QPSK 信号调制方式，检测准确率随生成器系数变化情况如表 2 所示。表 2 显示，随着 $\frac{\phi}{\psi}$ 的增大，检测准确率的最大值和平均值均逐渐减小。这是因为 $\frac{\phi}{\psi}$ 会影响发送方生成器的损失函数中对信号解调网络和信号检测网络的权重。增大此比值会使生成器 G 更优先考虑信号检测网络的性能。检测准确率最大值反映整个系统隐蔽性最差的情况，侦听方鉴别器恰好预测到和生成器相似的规律，因而获得更好的检测结果。检测准确率的平均值代表着系统在一段时间内（即鉴别器未进行新一轮更新）的结果，可以反映生成器的性能。解调准确率开始没有变化，但如果去掉生成器损失函数中对信号解调网络的考虑，系统的解调准确率最低；反之，解调准确率显著上升，而且隐蔽性无明显退化。

表 2 检测准确率随生成器系数变化情况

生成器系数	检测准确率最大值	检测准确率平均值	解调准确率
$\frac{\phi}{\psi}$=10	0.932	0.611	0.998
$\frac{\phi}{\psi}$=20	0.843	0.602	0.997
$\frac{\phi}{\psi}$=100	0.801	0.542	0.995
$\frac{\phi}{\psi}$=500	0.691	0.502	0.993
$\psi=0$	0.531	0.503	0.270

神经网络达到平衡后，一轮训练下 QPSK 信号经过生成器后的信号星座图如图 5 所示。图 5(a)中，信号集中在中间区域，且呈高斯分布，和系统的噪声相似，因此信号能融入系统噪声中，使鉴别器无法发现隐蔽信号。图 5(b)中，部分信号集中在原始 QPSK 信号星座图附近，而有向 y 轴靠近的趋势，部分信号分布在靠近 $x=0$ 的区域，但在 y 轴可以区分 4 种 QPSK

信号。观察输出信号可以发现，为了保证隐蔽信息接收方的解调准确率，神经网络保留了一部分原始信号的特征，而为了抑制鉴别器的性能，又降低了隐蔽信号功率。与此同时，由于输出信号保留了纵坐标的可分辨性（可以区分 4 种 QPSK 信号），因此获得较高的解调准确率。信号分布在 $x=0$ 附近，而没有分布在 $y=0$ 附近，是预训练导致的结果。图 5(b)体现了神经网络自身动态平衡的特点，靠近 $x=0$ 的星座点会在一定区域内呈现分散和聚合的状态。四周的信号会聚合或向中间靠拢。这符合表 2 所示结果，因为信号的检测准确率会在一定范围内波动，说明鉴别器 D 和生成器 G 保持动态平衡。

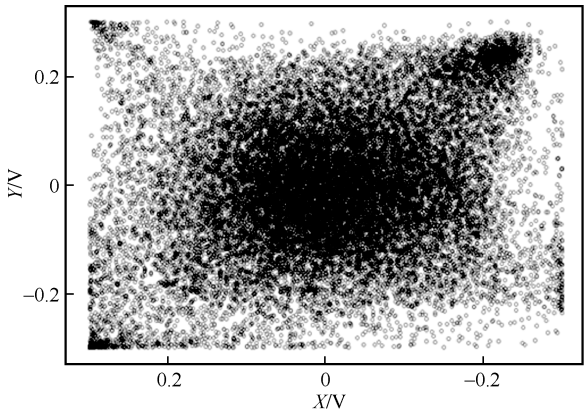


图 5　QPSK 信号经过生成器后的信号星座图

当 $\Im$=0.3，$n=0.01$ W，$\dfrac{\phi}{\psi}=500$ 时，BPSK 调制后的隐蔽信号通过生成器后星座点分布如图 6 所示。实验选择较大的 $\Im$。若 $\Im$ 过小，则会导致信号大部分处在边界处，无法较好地呈现信号生成的结果。图 6(a)中信号类似于 2 个高斯分布叠加的结果，图 6(b)中信号的分布类似于高斯分布，神经网络平衡后生成的隐蔽信号分布会在图 6(a)与图 6(b)之间变换。结果表明，神经网络会自动对输出信号进行幅度调制，并将信号幅值控制在 0.16 V 左右，此时接收方的解调准确率为 0.993，且满足设定的隐蔽性要求。

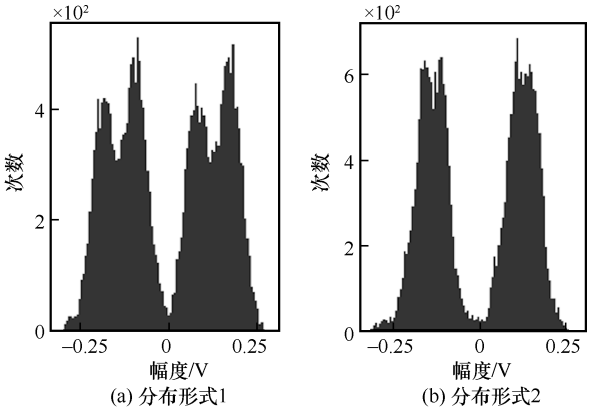


图 6　BPSK 调制后的隐蔽信号通过生成器后星座点分布

根据 Yan 等[15]的研究结果，在高斯白噪声信道下，不考虑信号解调准确率且在不同条件概率下得到的 2 种最优信号分布形式，即高斯分布和类似偏态高斯分布（具体信号形式未知）。由图 5 和图 6 可知，当 TripartiteGAN 侧重于增强隐蔽性时，即增大 $\dfrac{\phi}{\psi}$，信号的分布情况更接近于高斯分布或类似于 2 个高斯分布叠加的分布，符合理论分析结果。

本文进一步讨论不同加性白高斯噪声对隐蔽通信的隐蔽性和稳定性的影响。TripartiteGAN 在噪声功率 $n=0.01$W 时，进行训练并达到收敛。固定网络不变，保持实验其他参数不变，仅变化噪声功率 $n\in[0.001\text{W},0.1\text{W}]$，使信噪比 SNR$\in[20,40]$，可以得到隐蔽通信的检测准确率和解调准确率，如图 7 和图 8 所示。

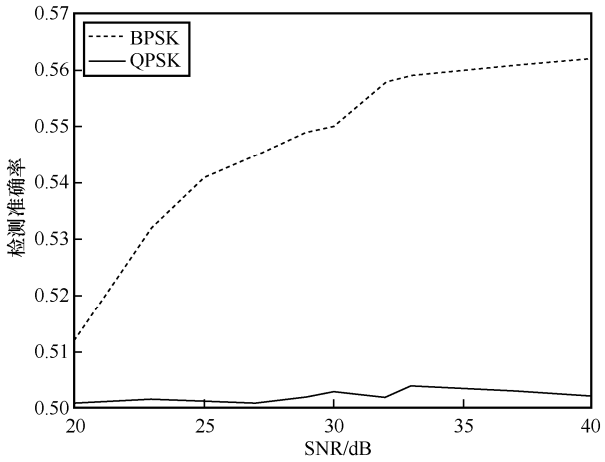


图 7　在不同 SNR 下 TripartiteGAN 的检测准确率

从图 7 可知，在 QPSK 调制下，当噪声功率较小时，侦听方已经达到最优的检测结果，此时的检测准确率接近理想值 0.5。此时，增加噪声功率不会明显提升隐蔽性。在 BPSK 调制下，噪声功率的增加可以明显提升隐蔽性。这说明 TripartiteGAN 生成的隐蔽信号具有一定的泛化能力，在侦听方固定的非训练环境下，也可以实现一定的隐蔽性。从图 8 可知，针对 BPSK 和 QPSK 调制，当 n>0.01 W，即 SNR<30 dB 时，解调准确率均开始降低。实验结果表明，在对解调准确率要求不高的场景下，TripartiteGAN 具有很好的泛化能力；但相反地，TripartiteGAN 需要针对不同噪声进行训练，以保证通信的质量。

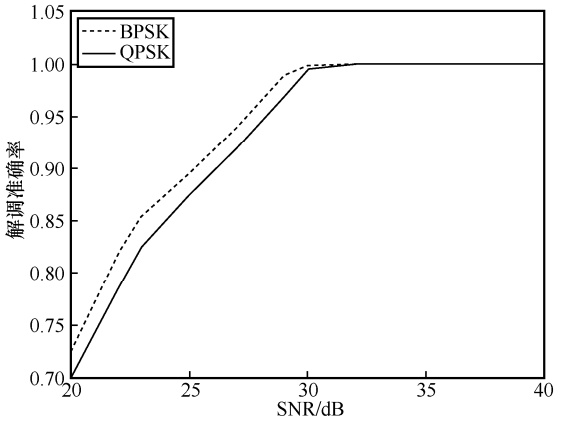


图 8 在不同噪声功率下 TripartiteGAN 的解调准确率

合法用户信息长度保持 256 bit 不变，信号生成网络系数比 $\frac{\phi}{\psi}=500$，$\Im$=0.3，$n=0.01$W，隐蔽信息长度对 TripartiteGAN 隐蔽性的影响如表 3 所示。从表 3 可知，随着隐蔽信息长度的增加，TripartiteGAN 出现无法收敛的情况。相较于 QPSK，TripartiteGAN 可以支持更长的 BPSK 调制的隐蔽信息实现隐蔽传输。

表 3 隐蔽信息长度对 TripartiteGAN 隐蔽性的影响

隐蔽信息长度/bit	BPSK 调制		QPSK 调制	
	检测准确率	解调准确率	检测准确率	解调准确率
32	0.503	0.997 7	0.506	0.991 3
64	0.502	0.996 2	0.501	0.991 0
128	0.506	0.994 2	不收敛	
256	不收敛		不收敛	

3.3 性能对比分析

为了保证结果图的简洁，使用 TGAN 代表 TripartiteGAN。由于发送方发送的信号序列长度有限且存在随机性，信号检测网络输出的结果会在一定范围内波动。因此，本节采用 3 000 次仿真实验所得检测准确率的平均值作为实验结果。

QPSK 调制下 TripartiteGAN 和基于 GAN 的隐蔽通信方法[16]的检测准确率如图 9 所示。从图 9 可知，GAN 方法下的检测准确率随着噪声的减少以及隐蔽信号功率的增加显著增加，这是由于隐蔽信号的信噪比越大，就越难隐藏在噪声中。TripartiteGAN 随着信噪比的增加，只有在 $n=0.001$W 且隐蔽通信功率很大时，侦听方检测准确率有一定上升；而其他情况下，其性能较稳定且明显优于 GAN 方法。TripartiteGAN 检测准确率在隐蔽通信功率较大时，隐蔽性明显优于 GAN 方法。在隐蔽信号功率较小时，由于已经接近理论极限 0.5，因此隐蔽性无法提升。

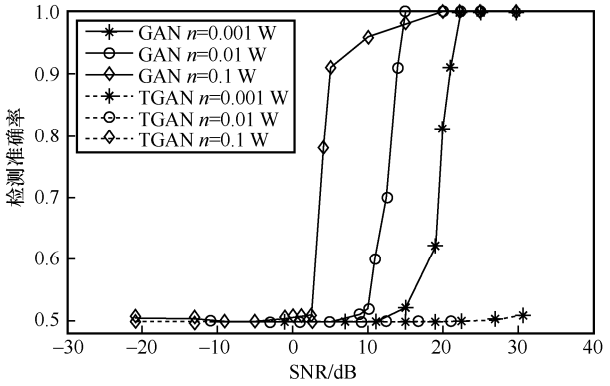


图 9 QPSK 调制下不同隐蔽通信方法的检测准确率

QPSK 调制下基于 TripartiteGAN 和基于 GAN 的隐蔽通信方法[16]的解调准确率如图 10 所示。TripartiteGAN 的解调准确率明显优于基于 GAN 的方法。联合图 9 和图 10 可以发现，相比基于 GAN 的隐蔽传输方法，TripartiteGAN 实现了更好的解调准确率和更高的检测准确率。

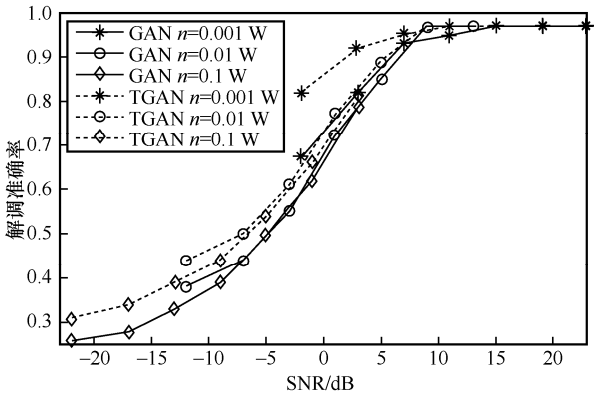


图 10 QPSK 调制下不同隐蔽通信方法的解调准确率

QPSK 调制下 TripartiteGAN 和基于 GAN 的隐蔽通信方法[16]的检测准确率如图 11 所示。这里的合法信号功率设置为 1 W。从图 11 可知，TripartiteGAN 随着噪声功率的增加，侦听方的检测准确率逐渐下降。由式(5)可知，噪声增大导致侦听方接收到的信号不确定性增加，有利于隐蔽信息传输。对比 2 种方法可知，TripartiteGAN 的隐蔽性始终高于 GAN，且随着噪声的增大，两者隐蔽性差距更加明显。当 $n=0.1$ W 时，TripartiteGAN 的隐蔽性能接近理论极限 0.5。由此可见，TripartiteGAN 的隐蔽性更优。

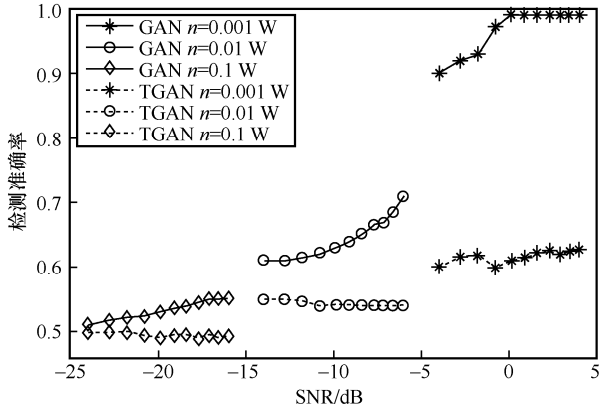


图 11　BPSK 调制下不同隐蔽通信方法的检测准确率

QPSK 调制下 TripartiteGAN 和基于 GAN 的隐蔽通信方法[16]的解调准确率如图 12 所示。从图 12 可知，不同噪声功率下，TripartiteGAN 的解调准确率相比于 GAN 方法的解调准确率均有提升。结合图 9～图 12 可知，对于经过不同调制方式调制后的隐蔽信息，TripartiteGAN 的隐蔽性和解调准确率均优于 GAN 方法。

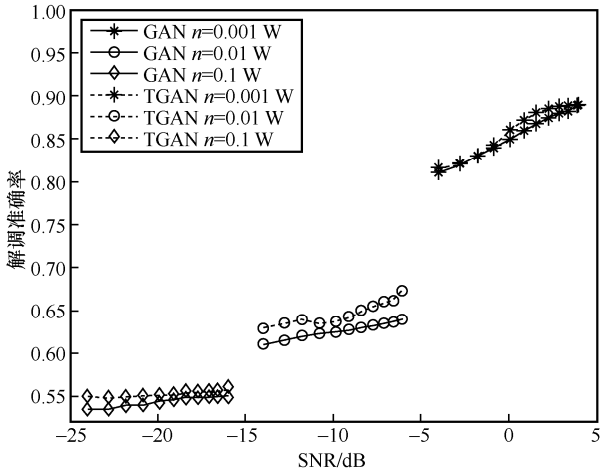


图 12　BPSK 调制下不同隐蔽通信方法的解调准确率

4　结束语

根据隐蔽通信中发送方和侦听方固有的对抗特性，本文提出了一种新型的三方生成对抗网络 TripartiteGAN，并基于此对抗网络设计了隐蔽信号波形。理论分析证明 TripartiteGAN 存在最优解且在网络收敛时达到最优解。仿真结果显示基于 TripartiteGAN 的隐蔽传输方法在隐蔽信号的隐蔽性和解调准确率方面均优于现有基于 GAN 的隐蔽通信方法。

参考文献：

[1] QI Y, VAEZI M, VINCENT POOR H. K-receiver wiretap channel: optimal encoding order and signaling design[J]. IEEE Transactions on Wireless Communications, 2023: doi.org/10.1109/TWC.2023.3264491.

[2] HUI H W, ZHOU C C, XU S G, et al. A novel secure data transmission scheme in industrial Internet of things[J]. China Communications, 2020, 17(1): 73-88.

[3] 侯剑, 鲁辉, 刘方爱, 等. 加密恶意流量检测及对抗综述[J]. 软件学报, 2023, 34(5): 1-24.
HOU J, LU H, LIU F A, et al. Overview of encrypted malicious traffic detection and countermeasures[J] Journal of Software, 2023, 34(5): 1-24.

[4] HAMAMREH J M, FURQAN H M, ARSLAN H. Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1773-1828.

[5] LI X W, JIANG J J, WANG H, et al. Physical layer security for wireless-powered ambient backscatter cooperative communication networks[J]. IEEE Transactions on Cognitive Communications and Networking, 2023, 9(4): 927-939.

[6] CHEN X Y, AN J P, XIONG Z H, et al. Covert communications: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 1173-1198.

[7] BASH B A, GOECKEL D, TOWSLEY D. Limits of reliable communication with low probability of detection on AWGN channels[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1921-1930.

[8] CHE P H, BAKSHI M, JAGGI S. Reliable deniable communication: hiding messages in noise[C]//Proceedings of 2013 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2013: 2945-2949.

[9] WANG L G, WORNELL G W, ZHENG L Z. Fundamental limits of communication with low probability of detection[J]. IEEE Transactions on Information Theory, 2016, 62(6): 3493-3503.

[10] ABDELAZIZ A, KOKSAL C E. Fundamental limits of covert communication over MIMO AWGN channel[C]//Proceedings of IEEE Conference on Communications and Network Security (CNS). Piscataway: IEEE Press, 2017: 1-9.

[11] LIU J H, YU J H, CHEN X M, et al. Covert communication in ambient backscatter systems with uncontrollable RF source[J]. IEEE Transactions on Communications, 2022, 70(3): 1971-1983.

[12] DU H Y, NIYATO D, XIE Y A, et al. Performance analysis and optimization for jammer-aided multiantenna UAV covert communication[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(10): 2962-2979.

[13] LIU J H, YU J H, NIYATO D, et al. Covert ambient backscatter communications with multi-antenna tag[J]. IEEE Transactions on Wireless Communications, 2023, 22(9): 6199-6212.
[14] KIM S W, TA H Q. Covert communications over multiple overt channels[J]. IEEE Transactions on Communications, 2022, 70(2): 1112-1124.
[15] YAN S H, CONG Y R, HANLY S V, et al. Gaussian signaling for covert communications[J]. IEEE Transactions on Wireless Communications, 2019, 18(7): 3542-3553.
[16] LIAO X M, SI J B, SHI J, et al. Generative adversarial network assisted power allocation for cooperative cognitive covert communication system[J]. IEEE Communications Letters, 2020, 24(7): 1463-1467.
[17] LI C X, XU K, ZHU J, et al. Triple generative adversarial networks[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 44(12): 9629-9640.
[18] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial networks[J]. Communications of the ACM, 2020, 63(11): 139-144.
[19] WANG Y D, YAN S H, ZHONG C J, et al. Probabilistic accumulate-then-transmit in covert communications with energy harvesting[C]//Proceedings of IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 685-691.
[20] ZHU J Y, PARK T, ISOLA P, et al. Unpaired image-to-image translation using cycle-consistent adversarial networks[C]//Proceedings of IEEE International Conference on Computer Vision (ICCV). Piscataway: IEEE Press, 2017: 2242-2251.

[作者简介]

于季弘（1987− ），男，满族，河北秦皇岛人，博士，北京理工大学教授，主要研究方向为空天物联网高效安全多址接入。

林子砚（1998− ），男，吉林呼兰人，北京理工大学硕士生，主要研究方向为隐蔽通信。

叶能（1993− ），男，浙江绍兴人，博士，北京理工大学助理教授，主要研究方向为空天通信、智能信号处理等。

杨凯（1983− ），男，河南济源人，博士，北京理工大学教授，主要研究方向为卫星移动通信、激光通信等。

安建平（1965− ），男，山西原平人，博士，北京理工大学教授，主要研究方向为空间信号处理、空天信息网络与安全等。