面向认知物联网的隐蔽通信智能功率控制

李赞[1]，廖晓闽[1,2]，石嘉[1]，肖培[3]

（1. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 国防科技大学信息通信学院，陕西 西安 710106；3. 萨里大学 5G 创新研发中心，萨里郡 吉尔福德 GU2 7XH）

摘　要：针对认知物联网的安全问题，提出了一种基于生成对抗网络的认知物联网隐蔽通信智能功率控制算法。首先将认知物联网隐蔽通信问题转化为认知物联网用户和窃听者之间的动态博弈问题，然后利用生成器模仿认知物联网用户，利用鉴别器模仿窃听者，两者分别采用 3 层神经网络构建，并通过二人零和博弈实现学习优化过程，最终达到纳什均衡，获得隐蔽功率控制方案。仿真结果表明，所提出的算法收敛速度快，不仅可以获得近似最优的隐蔽功率控制方案，而且在未来认知物联网中更具有实用性。

关键词：认知物联网；隐蔽通信；生成对抗网络；功率控制

中图分类号：TN929.5

文献标识码：A

doi: 10.11959/j.issn.2096−3750.2020.00148

Intelligent power control for covert communication in cognitive Internet of things

LI Zan[1], LIAO Xiaomin[1,2], SHI Jia[1], XIAO Pei[3]

1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
2. School of Information and Communications, National University of Defense Technology, Xi'an 710106, China
3. Home of 5G Innovation Centre, University of Surrey, Guildford GU2 7XH, U.K.

Abstract: In order to solve the security problem of cognitive Internet of things (IoT), an intelligent power control algorithm of covert communication in cognitive IoT based on generative adversarial network was proposed. Firstly, the covert communication optimization problem in the cognitive IoT was transformed into a dynamic game between the cognitive IoT user and the eavesdropper. Then, the generator imitated the cognitive IoT user, while the discriminator imitated the eavesdropper. The generator and the discriminator were constructed by the three-layer neural network respectively. Through the two-person zero-sum game, the learning optimization process was realized to achieve the Nash equilibrium, and finally the covert power control scheme was obtained. The simulation results show that the proposed algorithm can not only obtain near-optimal covert power control scheme with rapid convergence ability, but also be more practical in the future cognitive IoT.

Key words: cognitive IoT, covert communication, generative adversarial network, power control

收稿日期：2020–02–02；**修回日期：**2020–03–01

通信作者：廖晓闽，lxm8410@163.com

基金项目：国家自然科学基金重点项目（No.61631015）；国家杰出青年科学基金项目（No.61825104）；国家自然科学基金项目（No.61941105，No.61901327）

Foundation Items: The Key Project of National Natural Science Foundation of China (No.61631015), National Natural Science Foundation for Distinguished Young Scholar of China (No.61825104), National Natural Science Foundation of China (No.61941105, No.61901327)

1　引言

随着传感网、云计算、微型芯片等关键技术的日渐成熟，物联网（IoT, Internet of things）成为继计算机、互联网之后，信息技术的第 3 次革命浪潮，并与人工智能、边缘计算一起被确立为未来 6G 网络的基础[1]。然而在物联网中，无线通信设备数量急剧增加，业务需求日趋多样化，有限的频谱资源必将难以满足日益增长的物联网用户的需求。为了突破物联网中资源匮乏的瓶颈，认知物联网应运而生。通过融合认知无线电技术，物联网能够共享授权频谱资源，使频谱的利用率大幅度提升，同时充分发挥大数据优势，采用人工智能技术解决实际问题，广泛应用于智慧金融、智慧车联网等智慧网络中，因此，认知物联网深受人们的青睐和关注[2-3]。然而由于无线信道的广播特性，认知物联网的安全问题也存在着不容忽视的巨大隐患，因此，研究认知物联网的安全问题、挖掘数据隐藏信息、模拟人类的学习行为、实现认知物联网的安全、可靠传输，成为未来智慧物联网领域急需解决的重点问题。

针对认知物联网的安全隐患问题，学术界已经展开了研究工作。文献[4]采用随机几何方法来模拟窃听者位置，考虑信道信息的不确定性，通过设置安全通信范围，选择性地传输秘密信息。文献[5]采用波束成形方法来增强认知物联网的安全性能，利用融合了认知无线电技术的物联网控制器来辅助主用户传输秘密信息。文献[6]针对干扰攻击，提出了一种基于概率的信道分配机制，对次级用户的共享频谱进行管控。认知物联网现有的安全通信方法安全性能低，信道开销大，相关的技术尚未成熟，而且随着量子计算机和第三方攻击者计算能力的提升，现有的安全机制必将受到严重的冲击。此外，认知物联网设备普遍尺寸较小，成本较低，数量庞大，对安全通信提出了更高的要求，因此，迫切需要一种安全性能更高的通信方式。

目前，从信息论的角度出发，学术界提出了一种低检测/低截获的通信方式即隐蔽通信[7]，来有效提升网络安全性能。Bash 等[8]提出了在加性高斯白噪声（AWGN, additive white Gaussian noise）信道中，若窃听者能获得完整的信道信息，则隐蔽速率可达到 $o(n)$（n 为可用信道数），即当 n 趋于无穷时，隐蔽速率趋于 0。在此基础上，Wang 等[9]考虑中继和干扰场景，若存在信道不确定性，则隐蔽节点可以获得较好的隐蔽性能，即隐蔽速率为正值。文献[10]和文献[11]进一步研究了干扰不确定性对隐蔽通信的影响，通过对干扰源的发射功率、干扰源位置等进行管控，对窃听者实施干扰，虽然会增大隐蔽用户的噪声信号，但是可以改善隐蔽性能。目前，尚没有从信息论的角度出发对认知物联网隐蔽通信展开的研究，而且随着 6G 网络向智能化、大数据、动态化、高安全方向发展，传统隐蔽通信资源分配方法不再适用于未来的认知物联网，例如：窃听者检测阈值固定不变，则很难适应动态变化的环境；没有充分发挥大数据优势，则无法挖掘隐藏在数据中的信息等。

当前，以机器学习、深度学习为代表的人工智能技术已被广泛地应用于智能家居、安防、交通、医疗等领域，从最初的算法驱动逐渐向数据、算法和算力的复合驱动转变，这个转变取得了显著成效。目前，机器学习在物联网安全中的研究还处于早期探索阶段。如文献[12]针对物联网提出了一种基于生成对抗网络（GAN, generative adversarial network）的加密算法，该算法对原图像进行处理，利用 GAN 生成带有加密信息的新图像，并尽可能不被窃听者识别。文献[13]通过收集历史数据，采用数据驱动的机器学习方法训练神经网络，实时监测 IoT 设备的运行情况，检测网络攻击和恶意行为。文献[14]采用 4 种深度学习方法来识别分布式拒绝服务攻击，并分析比较了这 4 种深度学习方法的识别性能。目前，机器学习方法不仅可以充分利用大数据的优势，挖掘数据隐藏信息，而且可以模拟人类的学习行为，机器学习不需要人为干预的特点非常符合认知物联网的需求。此外，机器学习还可以实现动态实时交互，具有很强的泛化能力。因此，采用机器学习方法来解决认知物联网的隐蔽通信问题，具有广泛的应用前景。

本文考虑认知物联网隐蔽通信场景，基于 GAN 提出了一种全新的认知物联网隐蔽通信智能功率控制算法，通过联合优化主用户（干扰源）和认知物联网发送用户的发射功率，使认知物联网用户达到隐蔽通信的目的。该算法分为两部分，即采用生成器模拟认知物联网用户来生成隐蔽功率控制方案，采用鉴别器模拟窃听者来窃听认知物联网用户信号，生成器和鉴别器不断博弈，寻找纳什均衡解，最终得到最优的隐蔽功率控制方案。本文所提算法收敛速度快，不仅可以得到近似最优的隐蔽功率控

制方案，而且在未来认知物联网中更具有实用性。

2 系统模型

假设在认知物联网场景中，主用户网络存在一个主网络基站和若干主用户，采用正交频分复用（OFDM, orthogonal frequency division multiplexing）方案，每个频率只分配给一个主用户。认知物联网用户为次要用户，毗邻主用户网络，认知物联网中的发送用户和接收用户可以表示为用户之间的通信，也可以表示为基站到用户之间的通信。认知物联网用户通过侦测主用户的活动情况，采用 underlay 频谱共享方式共享最多一个主用户的上行频谱资源。由于无线信道的广播特性，存在一个恶意窃听者对认知物联网用户信号实施窃听。认知物联网用户融合了认知无线电技术，可以共享主用户的频谱，因此，为了确保认知物联网用户的安全通信，在通信过程中，共享频谱资源的主用户可充当干扰源，对窃听者实施干扰，在这种场景下，需要对认知物联网用户和主用户的发射功率进行智能管控，在不影响主用户通信和不被窃听者截获的情况下，使认知物联网用户的隐蔽速率最大化。认知物联网隐蔽通信的系统模型如图 1 所示。

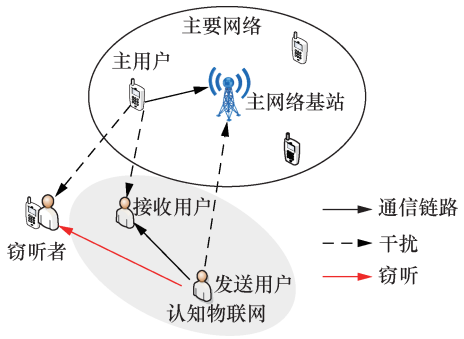


图 1 认知物联网隐蔽通信的系统模型

系统中所有通信链路经历的都是独立同分布的平坦瑞利衰落。$h_{\mathrm{pu,pbs}}$，$h_{\mathrm{pu,e}}$，$h_{\mathrm{pu,cr}}$，$h_{\mathrm{ct,pbs}}$，$h_{\mathrm{ct,cr}}$，$h_{\mathrm{ct,e}}$ 分别表示链路主用户—主网络基站、主用户—窃听者、主用户—认知物联网接收用户、认知物联网发送用户—主网络基站、认知物联网发送用户—认知物联网接收用户、认知物联网发送用户—窃听者的信道增益。T_1 表示认知物联网采用共享频谱传输信息，T_0 表示认知物联网没有采用共享频谱传输信息。主网络基站在第 k 个可用信道上的接收信号表示为

$$S_{\mathrm{pbs}}[k]=\begin{cases}\sqrt{p'_{\mathrm{pu}}}h_{\mathrm{pu,pbs}}S_{\mathrm{pu}}[k]+N_{\mathrm{pbs}}[k], T_0\\ \sqrt{p_{\mathrm{pu}}}h_{\mathrm{pu,pbs}}S_{\mathrm{pu}}[k]+\sqrt{p_{\mathrm{ct}}}h_{\mathrm{ct,pbs}}S_{\mathrm{ct}}[k]+N_{\mathrm{pbs}}[k], T_1\end{cases} \tag{1}$$

其中，p'_{pu} 表示认知物联网用户没有采用共享频谱传输信息时，主用户的发射功率；p_{pu} 和 p_{ct} 分别表示认知物联网用户采用共享频谱传输信息时，主用户和认知物联网发送用户的发射功率；$S_{\mathrm{pu}}[k]$ 和 $S_{\mathrm{ct}}[k]$ 分别表示主用户和认知物联网发送用户在第 k 个可用信道上的发射信号，满足 $E[S_{\mathrm{pu}}[k]S^*_{\mathrm{pu}}[k]]=E[S_{\mathrm{ct}}[k]S^*_{\mathrm{ct}}[k]]=1$；$N_{\mathrm{pbs}}[k]$ 表示主网络基站 PBS 在第 k 个可用信道上的 AWGN，方差为 σ^2_{pbs}。

认知物联网接收用户在第 k 个可用信道上的接收信号可以表示为

$$S_{\mathrm{cr}}[k]=\begin{cases}\sqrt{p'_{\mathrm{pu}}}h_{\mathrm{pu,cr}}S_{\mathrm{pu}}[k]+N_{\mathrm{cr}}[k], T_0\\ \sqrt{p_{\mathrm{ct}}}h_{\mathrm{ct,cr}}S_{\mathrm{ct}}[k]+\sqrt{p_{\mathrm{pu}}}h_{\mathrm{pu,cr}}S_{\mathrm{pu}}[k]+N_{\mathrm{cr}}[k], T_1\end{cases} \tag{2}$$

其中，$N_{\mathrm{cr}}[k]$ 表示认知物联网接收用户在第 k 个可用信道上的 AWGN，方差为 σ^2_{cr}。

当窃听者窃听认知物联网用户信号时，主用户信号会对窃听者实施干扰，因此，窃听者在第 k 个可用信道上的接收信号可以表示为

$$y_{\mathrm{e}}[k]=\begin{cases}\sqrt{p'_{\mathrm{pu}}}h_{\mathrm{pu,e}}S_{\mathrm{pu}}[k]+N_{\mathrm{e}}[k], T_0\\ \sqrt{p_{\mathrm{ct}}}h_{\mathrm{ct,e}}S_{\mathrm{ct}}[k]+\sqrt{p_{\mathrm{pu}}}h_{\mathrm{pu,e}}S_{\mathrm{pu}}[k]+N_{\mathrm{e}}[k], T_1\end{cases} \tag{3}$$

其中，$N_{\mathrm{e}}[k]$ 表示窃听者在第 k 个可用信道上的 AWGN，方差为 σ^2_{e}。

当认知物联网发送用户采用共享信道与接收用户进行通信时，主用户会对认知物联网用户产生干扰。综合考虑所有可用信道，认知物联网用户的隐蔽速率为

$$\mathrm{CR}=\mathrm{lb}\left(1+\frac{p_{\mathrm{ct}}\left|h_{\mathrm{ct,cr}}\right|^2}{\sigma^2_{\mathrm{cr}}+p_{\mathrm{pu}}\left|h_{\mathrm{pu,cr}}\right|^2}\right) \tag{4}$$

此外，当认知物联网采用 underlay 频谱共享方式共享主用户信道时，必须保证主用户的通信服务质量（QoS, quality of service）。假设主用户最低频谱效率为 $\mathrm{SE}^{\min}_{\mathrm{pbs}}$，则主用户通信必须满足

$$\mathrm{SE}_{\mathrm{pbs}}=\mathrm{lb}\left(1+\frac{p_{\mathrm{pu}}\left|h_{\mathrm{pu,pbs}}\right|^2}{\sigma^2_{\mathrm{pbs}}+p_{\mathrm{ct}}\left|h_{\mathrm{ct,pbs}}\right|^2}\right)\geqslant \mathrm{SE}^{\min}_{\mathrm{pbs}} \tag{5}$$

窃听者根据预先设置的阈值ε来判断认知物联网用户是否进行通信，判别方法为

$$E \underset{t_0}{\overset{t_1}{\gtrless}} \varepsilon \tag{6}$$

其中，E表示窃听者接收到的信号功率，可以表示为

$$E=\begin{cases} p'_{\mathrm{pu}}\left|h_{\mathrm{pu,e}}\right|^2+\sigma_{\mathrm{e}}^2, T_0 \\ p_{\mathrm{ct}}\left|h_{\mathrm{ct,e}}\right|^2+p_{\mathrm{pu}}\left|h_{\mathrm{pu,e}}\right|^2+\sigma_{\mathrm{e}}^2, T_1 \end{cases} \tag{7}$$

若$E>\varepsilon$，则窃听者判断认知物联网用户传输信息，记为t_1；若$E<\varepsilon$，则窃听者判断认知物联网用户没有传输信息，记为t_0。因此，$\Pr(t_1|T_0)$可以表示为窃听者的误检概率，即认知物联网用户没有传输信息，可窃听者判断其传输信息；$\Pr(t_0|T_1)$可以表示为窃听者的漏检概率，即认知物联网用户传输信息，可窃听者判断其没有传输信息。窃听者的检测错误概率可以表示为

$$\eta=\Pr(T_0)\Pr(t_1|T_0)+\Pr(T_1)\Pr(t_0|T_1) \tag{8}$$

其中，$\Pr(T_0)$表示认知物联网用户没有采用共享频谱传输信息的概率，$\Pr(T_1)$表示认知物联网用户采用共享频谱传输信息的概率。

在图 1 所示的隐蔽认知物联网通信模型中，系统通过联合优化认知物联网发送用户和主用户的发射功率，在保证主用户通信质量和不被窃听者截获的情况下，最大化隐蔽速率。根据系统优化目标，要解决的多目标优化问题描述如式(9)～式(12)所示。

$$\max_{\{p_{\mathrm{ct}},p_{\mathrm{pu}}\}} \quad \mathrm{CR} \tag{9}$$

$$\max_{\{p_{\mathrm{ct}},p_{\mathrm{pu}}\}} \quad \eta \tag{10}$$

约束条件为

$$\mathrm{SE}_{\mathrm{pbs}} \geqslant \mathrm{SE}_{\mathrm{pbs}}^{\min} \tag{11}$$

$$p_{\mathrm{ct}} \leqslant P_{\mathrm{ct}}^{\max} \tag{12}$$

$$p_{\mathrm{pu}} \leqslant P_{\mathrm{pu}}^{\max} \tag{13}$$

其中，$P_{\mathrm{ct}}^{\max}$和$P_{\mathrm{pu}}^{\max}$分别表示认知物联网发送用户和主用户的最大发射功率。

3　基于 GAN 的功率控制算法

本文综合考虑优化隐蔽速率和检测错误概率，这两者是相互冲突的，难以求得最优解。目前的研究方法将检测错误概率转化为约束条件，仅考虑理想情况，即认知物联网用户预知窃听者的预设门限[15-16]，这种假设与实际情况不符，很难实现。因此，本文采用 GAN 来求解该问题，将优化问题转化为认知物联网用户和窃听者之间的博弈问题，通过不断训练，获得纳什均衡解。

3.1　算法原理

GAN 由生成器和鉴别器组成，其中，生成器的主要作用是对采集的环境状态进行加工处理，不断重构直到生成的隐蔽功率控制方案无法被窃听者检测，从而窃听者判断认知物联网用户没有进行通信；而鉴别器的主要任务是分别对认知物联网没有进行隐蔽通信的功率控制方案和生成器生成的隐蔽功率控制方案进行鉴别，尽量正确地判别认知物联网用户是否进行通信，并辅助训练生成器生成隐蔽功率控制方案的能力，由此两者通过二人零和博弈实现学习优化过程，最终达到纳什均衡。

GAN 是一个博弈过程，可以描述为

$$\min_G \max_D Q(G,D)=E_{d\sim p_d}[\lg(\Pr{}^D(d))]+E_{g\sim p_g}[\lg(1-\Pr{}^D(G(g)))] \tag{14}$$

其中，d表示认知物联网用户没有采用共享频谱传输信息时的采样数据，g表示当前环境状态，D表示鉴别器，G表示生成器。鉴别器的输出$\Pr^D \in [0,1]$，表示判定认知物联网用户采用共享频谱传输信息的概率，若大于阈值τ，则判断认知物联网用户没有传输信息；若小于阈值τ，则判断认知物联网用户传输信息。因此对于鉴别器来说，当输入为样本数据d时，鉴别器使输出结果$\Pr^D(d)$尽可能大；当输入为生成器生成的隐蔽功率控制方案$G(g)$时，鉴别器使输出结果$\Pr^D(G(g))$尽可能小。对于生成器来说，生成器通过对当前环境状态g进行处理，生成隐蔽功率控制方案$G(g)$，然后将$G(g)$输入鉴别器，其目标是使鉴别器的输出结果$\Pr^D(G(g))$尽可能大，即$1-\Pr^D(G(g))$尽可能小，从而使鉴别器判断错误，做到“以假乱真”。

生成器模仿认知物联网用户，以最大化隐蔽速率为目标，生成隐蔽功率控制方案，因此，生成器与优化问题式(9)、式(11)、式(12)和式(13)相关。在计算优化问题式(9)、式(11)、式(12)和式(13)时，需

要 10 个环境状态，即 $g=\{h_{\mathrm{ct,cr}},h_{\mathrm{pu,cr}},h_{\mathrm{pu,pbs}},h_{\mathrm{ct,pbs}},\sigma_{\mathrm{cr}}^2,\sigma_{\mathrm{pbs}}^2,\mathrm{SE}_{\mathrm{pbs}}^{\min},p'_{\mathrm{pu}},P_{\mathrm{ct}}^{\max},P_{\mathrm{pu}}^{\max}\}$，通过计算得到输出结果 $G(g)=\{p_{\mathrm{ct}},p_{\mathrm{pu}}\}$。本文将生成器设计成 3 层神经网络，输入神经元为 10 个环境状态，输出神经元为隐蔽功率控制方案。此外，根据 Kolmogorov 定理，第 2 层神经元数目可设为 $2m+1$，其中 m 为输入神经元数目，因此，生成器的第 2 层神经元数目可设为 21。每层的激活函数都采用线性整流函数（ReLU, rectified linear unit）[17]。

鉴别器模仿窃听者，以最小化检测错误概率为目标，对样本数据 d 和生成器产生的隐蔽功率控制方案 $G(g)$ 进行判别，因此，鉴别器与优化问题式(10)相关。通过分析式(6)～式(8)，鉴别器主要与 p_{ct}、p_{pu} 和 p'_{pu} 相关，经过计算后，得到判别概率。因此本文将鉴别器设计成 3 层神经网络，输入神经元数目为 3，输出神经元数目为 1。同样地，根据 Kolmogorov 定理，鉴别器的第 2 层神经元数目可设为 7。第 2 层激活函数采用 ReLU 函数，第 3 层激活函数采用 Sigmoid 函数[17]。

3.2 算法流程

基于 GAN 的认知物联网隐蔽通信智能功率控制算法主要对生成器和鉴别器进行训练，在训练过程中，需要保持生成器和鉴别器的训练一致性。算法流程如图 2 所示。

步骤 1 采用随机初始化方法初始化生成器和鉴别器。

步骤 2 采集数据，对生成器和鉴别器进行预训练。

步骤 3 将探测的网络环境状态 g 输入生成器，生成隐蔽功率控制方案 $G(g)$。

步骤 4 将生成的隐蔽功率控制方案 $G(g)$ 和认知物联网用户没有采用共享频谱传输信息时的采样数据 d 输入鉴别器。

步骤 5 构建鉴别器的 Loss 函数，计算梯度，采用梯度上升法更新鉴别器的权值 ω_d，其中，鉴别器的 Loss 函数为

$$F_d=\nabla_{\omega_d}(\lg(\Pr^D(d))+\lg(1-\Pr^D(G(g)))) \quad (15)$$

步骤 6 构建生成器的 Loss 函数，计算梯度，采用梯度下降法更新生成器的权值 ω_g，其中，生成器的 Loss 函数为

$$F_g=\nabla_{\omega_g}\lg(1-\Pr^D(G(g))) \quad (16)$$

步骤 7 若鉴别器和生成器的 Loss 函数都小于训练阈值 λ，则输出隐蔽功率控制方案 $G(g)$；否则，重复步骤 3～步骤 6。

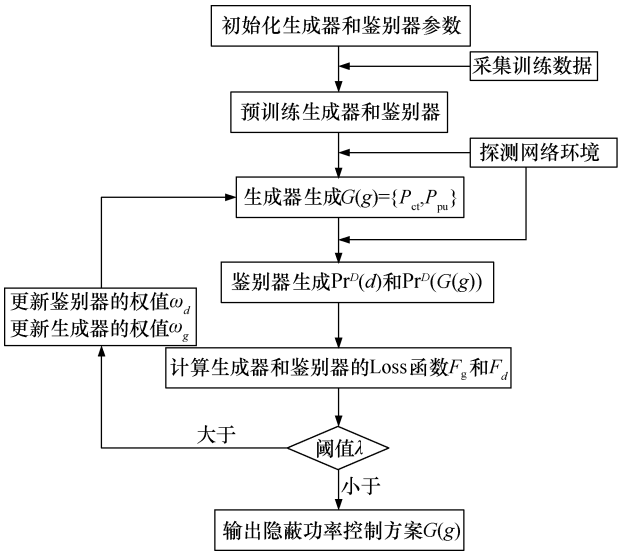


图 2 算法流程

4 仿真与分析

为了验证基于 GAN 的认知物联网隐蔽通信智能功率控制算法的有效性，首先理论分析了算法复杂度，接着仿真分析了算法收敛性，并比较了算法性能。收集整理了 3 000 组训练数据和 300 组测试数据对生成器和鉴别器分别进行预训练，训练速率设置为 0.001，鉴别器的判别阈值 τ 设置为 0.5，Loss 函数训练阈值 λ 设置为 0.001，仿真参数设置为 $|h_{\mathrm{pu,pbs}}|^2=|h_{\mathrm{ct,cr}}|^2=|h_{\mathrm{pu,cr}}|^2=|h_{\mathrm{ct,pbs}}|^2=2$，$p'_{\mathrm{pu}}=34.8\ \mathrm{dBm}$，$\sigma_{\mathrm{pbs}}^2=\sigma_{\mathrm{cr}}^2=-174\ \mathrm{dBm}$，$\mathrm{SE}_{\mathrm{pbs}}^{\min}=1\ \mathrm{bit/(s\cdot Hz)}$。

首先，分析算法复杂度。假设生成器中每层神经元数量分别为 m_1、m_2 和 m_3，则在前向训练权值时，需要进行 $m_1\times m_2$ 和 $m_2\times m_3$ 次计算。同理，假设鉴别器中每层神经元数量分别为 n_1、n_2 和 n_3，则在前向训练权值时，需要进行 $n_1\times n_2$ 和 $n_2\times n_3$ 次计算。由于算法流程包括对生成器和鉴别器进行前向训练权值和反向更新权值两个过程，而且反向更新权值的时间复杂度和前向训练权值相同，因此，假设总共有 L 个训练样本，每个样本训练 Q 次，那么算法的时间复杂度为 $o(L\times Q\times(m_1\times m_2+m_2\times m_3+n_1\times n_2+n_2\times n_3))$。算法模型训练完成后，如果对当前数据进行预测，那么时间复杂度为 $o(Q\times(m_1\times m_2+m_2\times m_3+n_1\times n_2+n_2\times n_3))$。

其次，分析算法收敛性。Loss 函数值是神经网络收敛的重要指标，当 Loss 函数值小于预定的训练阈值，神经网络训练结束，输出最终结果[17]。图 3 给出了鉴别器和生成器的 Loss 函数值训练情况。鉴别器的 Loss 函数值随着训练逐渐增大，生成器的 Loss 函数值随着训练逐渐减小，这与算法中对鉴别器和生成器中权值的训练规则相符。当训练次数达到 26 时，鉴别器和生成器的 Loss 函数值都小于阈值λ，算法收敛，输出生成器生成的隐蔽功率控制方案 $G(g)=\{p_{\mathrm{ct}},p_{\mathrm{pu}}\}$。

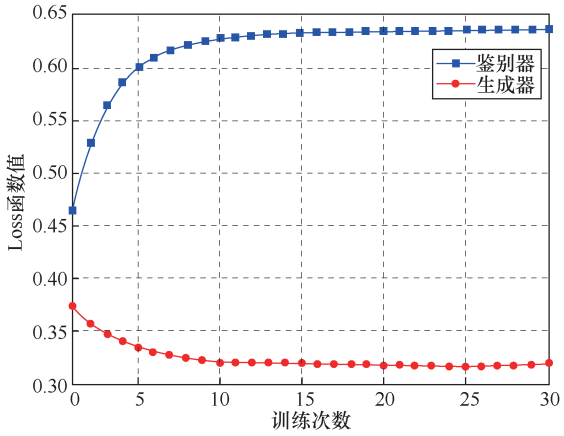


图 3　鉴别器和生成器的 Loss 函数值训练情况

最后，分析比较算法性能。隐蔽速率和检测错误概率是评估隐蔽通信性能的两个重要指标[7-11]，本文的目标是通过联合优化认知物联网发送用户和主用户的发射功率，最大化隐蔽速率和检测错误概率，使认知物联网用户传输的信息不被窃听者截获。因此，通过改变窃听者预设阈值ε，分别从隐蔽速率和检测错误概率两方面，将本文提出的基于 GAN 的智能功率控制算法与文献[16]提出的算法进行比较，分析隐蔽通信中功率控制的性能。文献[16]提出的算法仅考虑理想情况，即认知物联网用户预知窃听者的预设阈值ε，而本文所提算法假设窃听者预设阈值ε未知。图 4 和图 5 分别给出了隐蔽速率和检测错误概率随窃听者预设阈值ε的变化情况。可以看出，随着窃听者预设阈值ε的增加，认知物联网用户隐蔽发射功率增大，因此隐蔽速率增大，同时也增加了认知物联网用户被窃听者截获的风险，最小检测错误概率减小。同时，当认知物联网增大隐蔽通信概率，可获得的隐蔽速率增大，最小检测错误概率减小。此外，本文所提算法性能接近于文献[16]提出的算法性能，但是文献[16]所提算法隐蔽速率的增加，是以牺牲检测风险为代价的，而本文所提算法是从隐蔽通信实际场景出发，在未来认知物联网中更具有实用性。

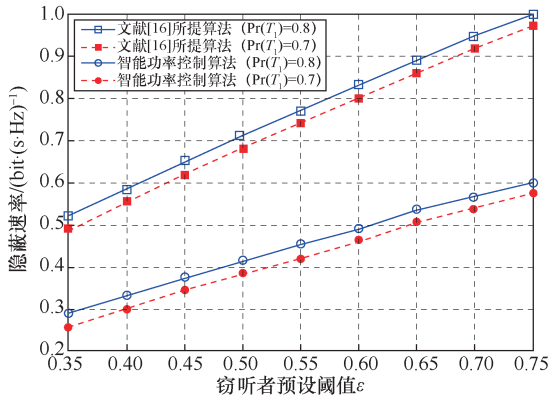


图 4　隐蔽速率随窃听者预设阈值ε的变化情况

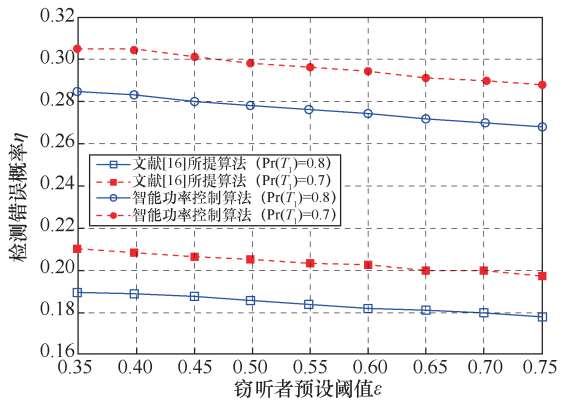


图 5　检测错误概率随窃听者预设阈值ε的变化情况

5　结束语

为了提高认知物联网通信的安全性，本文讨论了认知物联网中隐蔽通信的功率控制问题，提出了一种基于 GAN 的认知物联网隐蔽通信智能功率控制算法。该算法包含生成器和鉴别器两个模块，分别用 3 层神经网络来表示，生成器模拟认知物联网用户，鉴别器模拟窃听者，两者通过不断博弈，最终达到纳什均衡，获得隐蔽功率控制方案。仿真结果显示，本文提出的算法收敛速度快，不仅可以获得近似最优的隐蔽功率控制方案，而且在未来认知物联网中更具实用性。

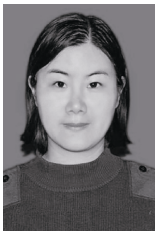
参考文献：

[1]　JUNTTI M, KANTOLA R, KYÖSTI P, et al. Key drivers and research challenges for 6G ubiquitous wireless intelligence[R]. Finland: Uni-

versity of Oulu, 2019.
[2] WU Q H, QING G R, XU Y H, et al. Cognitive Internet of things: a new paradigm beyond connection[J]. IEEE Internet of Things Journal, 2014, 1(2): 129-143.
[3] ZHU J, SONG Y H, JIANG D D, et al. A new deep-Q-learning-based transmission scheduling mechanism for the cognitive Internet of things[J]. IEEE Internet of Things Journal, 2018, 5(4): 2375-2385.
[4] ZHU Z, YU B, CHU X, et al. Design and optimization of physical layer security transmission scheme in random cognitive Internet of things[C]//2019 11th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2019: 2325-3746.
[5] DENG Z, LI Q, ZHANG Q, et al. Beamforming design for physical layer security in a two-way cognitive radio IoT network with SWIPT[J]. IEEE Internet of Things Journal, 2019, 6(6): 10786-10798.
[6] BANY H A, ALMAJALI S, AYYASH M, et al. Spectrum assignment in cognitive radio networks for Internet of things delay-sensitive applications under jamming attacks[J]. IEEE Internet of Things Journal, 2018, 5(3): 1904-1913.
[7] SOLTANI R, GOECKEL D, TOWSLEY D, et al. Covert wireless communication with artificial noise generation[J]. IEEE Transactions on Wireless Communications, 2018, 17(11): 7252-7267.
[8] 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.
[9] WANG J Q, TANG W B, ZHU Q Q, et al. Covert communication with the help of relay and channel uncertainty[J]. IEEE Wireless Communications Letters, 2019, 8(1): 317-320.
[10] LIU Z, LIU J, ZENG Y, et al. On covert communication with interference uncertainty[C]//2018 IEEE International Conference on Communications (ICC). IEEE, 2018: 1-6.
[11] HE B, YAN S H, ZHOU X Y, et al. Covert wireless communication with a Poisson field of interferers[J]. IEEE Transactions on Wireless Communications, 2018, 17(9): 6005-6017.
[12] MENG R H, CUI Q, ZHOU Z L, et al. A steganography algorithm based on CycleGAN for covert communication in the Internet of things[J]. IEEE Access, 2019, 7: 90574-90584.
[13] LI F Y, SHINDE A, SHI Y, et al. System statistics learning-based IoT security: feasibility and suitability[J]. IEEE Internet of Things Journal, 2019, 6(4): 6396-6403.
[14] ROOPAK M, TIAN G Y, CHAMBERS J. Deep learning models for cyber security in IoT networks[C]//2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2019: 452-457.
[15] HU J S, YAN S H, SHU F, et al. Covert transmission with a self-sustained relay[J]. IEEE Transactions on Wireless Communications, 2019, 18(8): 4089-4102.
[16] SHI X, WU D, YUE C, et al. Resource allocation for covert communication in D2D content sharing: a matching game approach[J]. IEEE Access, 2019, 7: 72835-72849.
[17] HAGAN M T, DEMUTH H B, BEALE M H, et al. Neural network design (2nd Edition)[M]. USA: Martin Hagan, 2014.

[作者简介]

李赞（1975− ），女，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为隐蔽通信、频谱管控。



廖晓闽（1984− ），女，江西德兴人，西安电子科技大学博士生，国防科技大学信息通信学院副教授，主要研究方向为频谱管控、隐蔽通信。

石嘉（1987− ），男，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为无线系统资源分配、毫米波通信、隐蔽通信等。

肖培（1968− ），男，湖北武汉人，英国萨里大学教授、博士生导师，主要研究方向为无线通信理论与信号处理、5G 通信关键技术等。