[文章编号] 1007－7405(2024)02－0188－05 DOI:10.19715/j.jmuzr.2024.02.11

MEC-NOMA 系统的物理层安全性能评估

张 敏

（集美大学计算机工程学院，福建 厦门 361021）

[摘要] 面向移动边缘计算（mobile edge computing，MEC）场景，建立了一个存在主动攻击者的非正交多址协议（nonorthogonal multile access，NOMA）网络传输模型，并设计一种卷积神经网络（convolutional neural network，CNN）模型来评估该传输模型的安全中断概率（security outage probability，SOP）。研究结果表明：所提出的MEC-NOMA系统不仅提高了SOP，而且能够对抗主动窃听者的攻击；此外，通过CNN模型评估的SOP与其他方法（蒙特卡洛方法和数学解析表达式）非常接近，且执行时间更短。

[关键词] 移动边缘计算；非正交多址协议；物理层安全；安全中断概率；卷积神经网络

[中图分类号] TP 391

Performance Evaluation on PHY-Security of MEC-NOMA System

ZHANG Min

(College of Computer Engineering, Jimei University, Xiamen 361021, China)

Abstract: In this paper, a NOMA model with active eavesdropper is established for mobile edge computing (MEC) scenarios, and evaluated the security outage probability (SOP) of the transport model by convolutional neural network (CNN) model. The results show that the proposed MEC-NOMA system not only improves the SOP, but also overcomes the active eavesdropper attacks. In addition, the SOP estimated by CNN model is very close to other methods (Monte Carlo method and analytical expression), but the execution time is shorter.

Keywords: mobile edge computing; nonorthogonal multile access; PHY-security; security outage probability; convolutional neural network

0 引言

由于移动终端计算处理能力有限，对于一些高强度计算、低时延的业务（比如虚拟现实、增强现实等）无法进行高效处理[1]。文献[2]给出了一种移动边缘计算（mobile edge computing，MEC）的解决方案，将更多的计算和存储资源部署在移动网络边缘端，移动边缘计算节点可以承担用户更多的计算任务。功率域的非正交多址（nonorthogonal multile access，NOMA）是最新的多址技术之一，能有效解决网络频谱资源缺乏的问题，实现多用户之间的资源共享[3]。在移动边缘计算场景中，边缘服务器与终端设备之间会有大量的连接，为此，文献[4]提出了NOMA-MEC系统的方案。

随着移动用户和物联网设备的增加，终端设备与边缘服务器之间可能传输一些敏感信息，例如银行信息、个人信息等。由于无线空间的开放性，在无线信道中传输的信息容易被恶意窃听[5]。因此，如何提高移动边缘计算网络中安全通信性能，引起了人们的广泛关注。利用无线介质的特性屏蔽信号

[收稿日期] 2022－06－25
[基金项目] 福建省自然科学基金项目（2021J01857）；福建省中青年教师教育科研项目（JAT210251）
[作者简介] 张敏，主要从事智能信息处理、人工智能方向研究。

信息，被认为是保护消息免受窃听攻击的有效解决方案之一[6]。在物理层安全通信中，安全传输意味着主信道（两个合法用户之间）的信道容量高于窃听信道的信道容量[7]。刘元伟等[8]研究了下行大规模 NOMA 网络的安全性能，提出用户安全中断概率（security outage probability，SOP）的计算表达式。此外，从信息理论安全角度看，当主信道和窃听信道的信道容量之差增大时，系统变得更加健壮。由于多个用户同时使用单个资源块，可能会损害合法用户的服务质量，因此主动窃听在 NOMA 环境中更具挑战性。Allipuram 等[9]研究了主动窃听对安全通信的影响。在安全通信中，发送端根据接收端的反馈决定是否发送数据，以防止消息被主动窃听。文献［10］提出了一种新型的合作 NOMA 方案，主要采用蒙特卡洛算法进行仿真验证，但是并未对执行时间作出分析。近年来，基于深度学习模型的系统性能评估的研究开始取代基于模型的数学方法。文献［11－13］的研究表明，基于深度学习模型的方法成为研究性能分析的一种有效工具，能够提供准确的结果且执行时间更短。

目前，对深度学习模型的 NOMA 系统性能分析的研究相对较少。文献［14］研究基于深度学习的物理层无线通信技术，通过对卷积神经网络（convolutional neural network，CNN）、循环神经网络和深度神经网络的比较与分析，发现 CNN 模型的性能最优。传统的深度学习模型为获得更高的准确率，采用多层次叠加的方式，使模型复杂度更高。由于 CNN 模型能够实现权值共享，使模型更简单，具有更强的泛化能力，而且模型对样本的畸变不敏感，要比传统的深度学习模型性能更优越。本文拟建立主动窃听场景下的 MEC-NOMA 系统，并设计 CNN 模型对该系统的物理层安全性能进行评估。

1　系统模型与 NOMA 网络

不失一般性，本文考虑 1 个边缘服务器、2 个合法用户设备和 1 个主动窃听者组成的 MEC-NOMA 模型。

如图 1 所示，首先将 MEC-NOMA 系统中的边缘服务器标记为 S，包含一组 K 个单天线发射机，即 $S=\{S_i \mid i=1,2,\cdots,K\}$。合法用户 1 距离边缘服务器较近即处于信号源 S 覆盖范围的中心位置，为中心用户，标记为 U_1；合法用户 2 距离边缘服务器较远，即处于 S 覆盖范围的边缘位置，为边缘用户，标记为 U_2。S 基于 NOMA 协议对 U_1 和 U_2 发送计算结果的信号。同时，主动窃听者标记为 E，能够窃听 U_1 和 U_2 的合法传输信息，主要目的为降低系统的传输速率，减少用户解码的正确率。

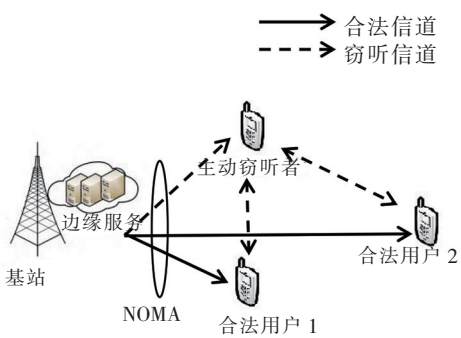


图 1　MEC-NOMA 系统模型

Fig.1　MEC-NOMA system model

在物理层安全分析中，SOP 是评估安全性能的重要指标之一。SOP 定义为主信道和窃听信道容量之间的差值低于预定义阈值的概率[15]。该阈值称为安全目标数据速率，单位为(bit/s)/Hz[15]。根据文献［15］中的定义，在用户 U_1 处消息的 SOP 可简化定义为：$P_{\text{out},1}=P_r[C_{S,1}<R_{\text{th},x_1},C_{1,x_2}\geqslant R_{d,x_2}]+P_r[C_{1,x_2}<R_{d,x_2}]$；在用户 U_2 处消息的 SOP 定义为：$P_{\text{out},2}=P_r[C_{S,x_2}<R_{\text{th},x_2}]$。其中：$R_{\text{th},x_1}$ 为用户 U_1 报文的安全目标数据率；R_{d,x_2} 为在用户 U_1 处解码边缘用户 U_2 消息的码字速率；$C_{S,1}$ 为用户 U_1 消息的主信道容量；C_{1,x_2} 为用户 U_1 处的边缘用户信息 x_2 的主信道容量；C_{S,x_2} 为边缘用户 U_2 消息的主信道容量。

2　仿真结果与分析

由于在复杂的系统模型中数学推导方法计算量大，执行时间长，较难应用。CNN 模型主要通过训练端到端的映射发现网络参数与安全性能之间的关系。本研究设计了一个 CNN 模型来评估 SOP。

2.1　训练数据准备

网络参数包括发送用户数 M，发射机的发送功率 P_S，U_1、U_2 和 E 的功率 P_1、P_2 和 P_E，发射机

和 U_1、U_2、E 之间的距离 d_{S1}、d_{SE}、d_{E1}、d_{E2}，U_1 的功率分配系数 θ_1，以及 U_1 和 U_2 的安全目标数据速率 $R_{\mathrm{th},x1}$、$R_{\mathrm{th},x2}$。因此，输入数据向量（$\boldsymbol{v} \triangleq \mathrm{CNN}_{\mathrm{in},U_i}, i = 1,2$）包含以下参数：$\boldsymbol{v} \triangleq [M, P_S, P_1, P_2, P_E, d_{S1}, d_{SE}, d_{E1}, d_{E2}, \theta_1, R_{\mathrm{th},x_1}, R_{\mathrm{th},x_2}]$。

用于训练 CNN 模型的输入数据设置如表 1 所示。

表 1 CNN 模型训练和测试的输入参数

Tab. 1 Imput parameters for CNN training and testing

输入	值	输入	值	输入	值
M	4	P_S/dB	[−20:5:60]	d_{S1}/m	[0.2,0.4]
P_1/dB	[5,10]	θ_1/(°)	[0.2,0.4]	d_{E1}/m	[0.5,1.0]
P_2/dB	[5,10]	d_{E2}/m	[0.5,1.0]	$R_{\mathrm{th},x1}$/(bit · s^{-1})	[0.1,0.2]
P_E/dB	[5,10]	d_{SE}/m	[0.5,1.0]	$R_{\mathrm{th},x2}$/(bit · s^{-1})	[0.1,0.2]

2.2 CNN 模型架构

CNN 模型的架构参数如表 2 所示，包括 1 个输入层、2 个卷积与池化层、1 个全连接层和 1 个输出层。输入层接收输入数据，以便 CNN 模型找到系统参数与对应 SOP 之间的关系。由于输入数据为二维数据，所以 2 个卷积层采用 1 维 CNN，激活函数采用 RELU 函数，这样激活特性更优。池化层采用最大池化方式，大小为 2。卷积层和池化层提取的特征可作为全连接层的输入，用于预测 SOP。输出层由单个神经元组成。与输入层类似，输出层的神经元不包含激活函数。CNN 模型通过迭代更新找到最佳权重和偏置。

表 2 CNN 模型架构参数

Tab.2 CNN architecture parameters

输入	输出	参数
input_1 (InputLayer)	(None, 12, 1)	0
conv1d (Conv1D)	(None, 12, 32)	96
max_pooling1d (MaxPooling1D)	(None, 6, 32)	0
conv1d_1 (Conv1D)	(None, 5, 64)	4160
max_pooling1d_1 (MaxPooling1	(None, 2, 64)	0
flatten (Flatten)	(None, 128)	0
dense (Dense)	(None, 128)	16512
dense_1 (Dense)	(None, 1)	129

2.3 CNN 模型训练与实时预测

当训练完成后，生成的 CNN 模型可用于预测 SOP。值得注意的是，该模型的训练为离线型。这意味着 CNN 模型是在数据传输之前即在网络规划步骤中完成训练的。CNN 模型离线训练完成后，只需保存该模型，并在较短的执行时间内供 MEC-NOMA 系统实时调用即可预测 SOP，用于安全性能的分析。因此，可将 CNN 模型用于实时预测。

2.4 CNN 模型在 SOP 预测中的性能

本研究样本数据生成量为 10 000，其中 80% 用于训练，10% 用于验证，10% 用于测试。损失函数考虑采用均方误差（MSE）表示。采用自适应学习率设置，初始学习率为 10^{-2}，最低学习率为 10^{-10}，因子为 0.8，patience 为 1，batch 大小为 200，epoch 为 30。

为了评估所提出的 CNN 模型的性能，使用 MSE 测量预测 SOP 和测试集输出数据之间的准确性。MSE 越小，预测的 SOP 和观察结果越相似。从图 2 可以看出，当迭代 25 次后，CNN 模型收敛，且训练集和测试集的拟合程度较好，说明该模型具有较好的泛化能力。

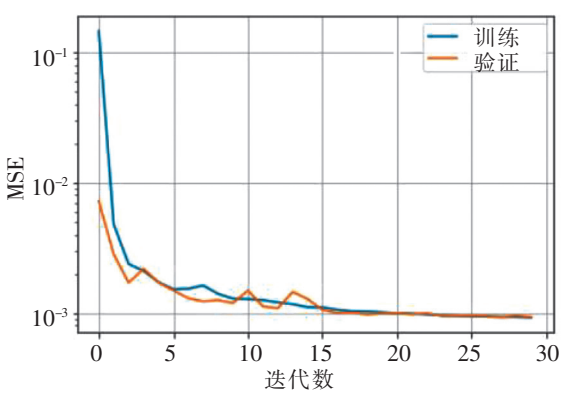


图 2 CNN 模型迭代收敛图

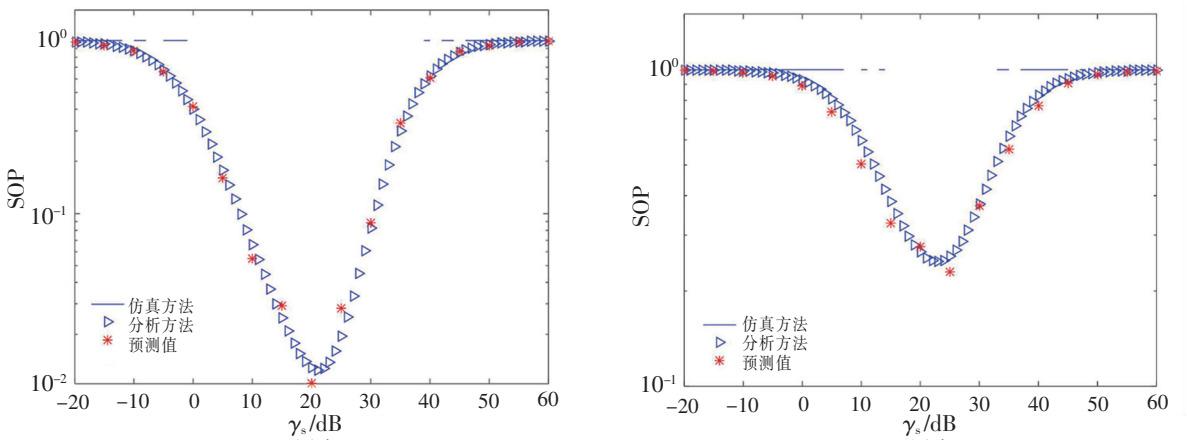
Fig.2 Iterative convergence craph of CNN

2.5 仿真结果评估与分析

对仿真结果进行评估与分析，模型的仿真参数取值如下：$d_{S1} = 0.2$ m，$d_{S2} = 1$ m，$d_{SE} = 1$ m，$d_{E1} = 0.5$ m，$d_{E2} = 0.5$ m，路径损耗指数 $\varepsilon = 2.7$，位于 $d_0 = 1$ m 处的参考路径损耗 $L = -30$ dB，不完全串

行干扰消除（successive interference cancelation，SIC）系数 $\beta = 0.1$，U_1 和 U_2 的目标安全数据速率 $R_{\mathrm{th},x_2} = 0.2$（bit/s）/Hz。执行时间定义为评估安全中断性能所花费的时间。采用蒙特卡洛方法、数学方法和 CNN 模型需要的执行时间分别为 310.3、1.2 和 0.22 s，可以看出，CNN 模型在三种方法中执行时间最短。蒙特卡洛方法只需要通过网络参数来估计安全性能，但其执行时间非常长。数学方法尽管可以很容易地研究哪些网络参数会影响安全性能，但是计算更为复杂。而 CNN 模型通过离线训练保存再实时加载，可以简化计算过程，显著减少执行时间。

图 3 分别给出了用户 U_1、U_2 关于边缘服务器传输信噪比 SNR（γ_s）与 SOP 的关系。该数据传输方案利用窃听信道容量来选择最佳发射机。结果表明，当 γ_s 增加时，SOP 减少；当 γ_s 继续增加至 22 dB时，SOP 达到最低点；而当 γ_s 再持续增加时，SOP 的值反而增加。这是由于当 γ_s 增大时，存在不完全 SIC 系数 β，使中心用户和边缘用户的干扰分别增大。通过 CNN 模型预测的 SOP 与数学分析方法的计算结果非常接近，这表明 CNN 模型是一种可用于评估复杂系统性能的有效模型。



a) 用户 U_1　　b) 用户 U_2

图 3　边缘服务器传输信噪比对 SOP 的影响

Fig.3　Effect of transmit SNR on the SOP

为了研究 MEC-NOMA 系统安全性能，需考虑系统的 SOP（P_{sys}），可将其数学式[7]定义为：

$$P_{\mathrm{sys}} = 1 - (1 - P_{\mathrm{out},1})(1 - P_{\mathrm{out},2})。$$

图 4 给出了系统 SOP 和发射信噪比 SNR（γ_s）与功率分配系数（θ_1）之间的关系。随着 γ_s 和 θ_1 的增加，系统 SOP 呈现凹型结构。当 γ_s 增大时，主信道的干扰增大，接收信号的强度也增大。当 θ_1 增大时，由于不完全 SIC 系数的影响，使用户 U_1 的干扰增大，而用户 U_2 基于 NOMA 原理，其干扰也增大。

为了评估本研究提出的 MEC-NOMA 系统的安全性能，将本系统与传统的 NOMA 系统进行比较。图 5 为系统 SOP 与窃听者 E 处发射的信噪比 γ_E 的关系图。

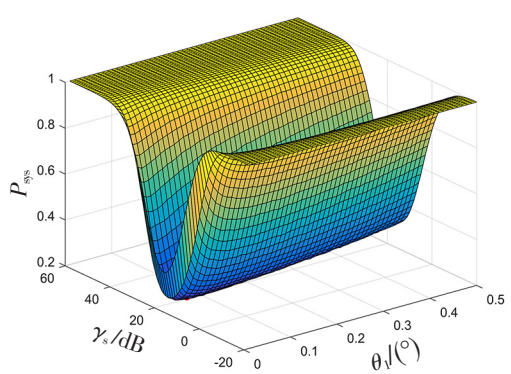


图 4　γ_s 和 θ_1 对系统 SOP 的影响

Fig.4　Effect of γ_s and θ_1 on system SOP

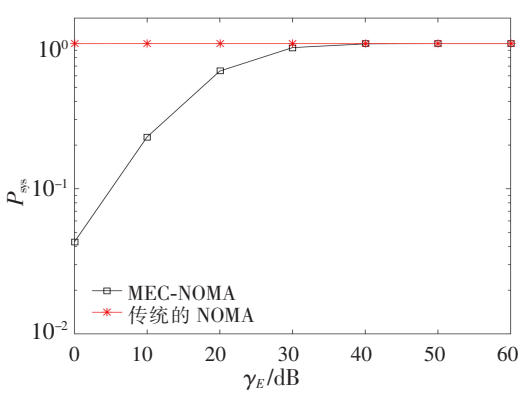


图 5　窃听者 E 处发射信噪比对系统 SOP 的影响

Fig.5　Effect of transmit SNR at E (γ_E) on system SOP

从图 5 可以看出，与传统的 NOMA 系统相比，本系统的安全性能有了显著提高。这是因为本系统的 U_1 和 U_2 可作为干扰器，对主动窃听者和接收者都进行了干扰。而传统的 NOMA 系统不会在 U_1 和 U_2 处产生信号来迷惑主动窃听者。因此，与传统的 NOMA 系统不同，本系统可以对抗主动窃听者的攻击。

3 结论

本文主要研究边缘计算场景下存在主动窃听者时下行链路 NOMA 系统的安全性能。为了实时评估安全性能并克服蒙特卡洛和数学方法的局限性，本研究设计了用于评估 SOP 的 CNN 模型。从分析结果来看，与传统 NOMA 系统相比，本文提出的 MEC-NOMA 系统和数据传输方案提高了对主动窃听攻击的安全中断性能。由于数学推导的复杂性使基于模型的数学方法难以应用时，本文提出的 CNN 模型是一个有效的解决方案和工具，能够很好地预测系统的安全性能。

[参 考 文 献]

[1] BARBERA M V, KOSTA S, MEI A, et al. To offload or not to offload? The bandwidth and energy costs of mobile cloud computing[C]//Proceedings-IEEE INFOCOM. Turin, Italy: IEEE, 2013: 1285-1293. DOI: 10.1109/INFCOM.2013.6566921.

[2] TAN L T, HU R Q, HAN Z L. Twin-timescale artificial intelligence aided mobility-aware edge caching and computing in vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(4): 3086-3099. DOI: 10.1109/TVT.2019.2893898.

[3] DAI L, WANG B, YUAN Y, et al. Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends[J]. IEEE Commun Mag, 2015, 53(9): 74-81.

[4] DING Z, NG D W K, SCHOBER R, et al. Delay minimization for NOMA-MEC offloading[J]. IEEE Signal Processing Letters, 2018, 25(12): 1875-1879.

[5] 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.

[6] SHU F, SHEN T, XU L. et al. Directional modulation: a physical-layer security solution to B5G and future wireless networks [J]. IEEE Netw, 2019, 34(2): 210-216.

[7] SHIM K, NGUYEN T V, AN B. Exploiting opportunistic scheduling schemes to improve physical-layer security in MU-MISO NOMA systems[J]. IEEE Access, 2019, 7: 180867-180886.

[8] LEI H, ZHANG J, PAPK K H. et al. On secure NOMA systems with transmit antenna selection schemes[J]. IEEE Access, 2017, 5: 17450-17464.

[9] ALLIPURAM S, MOHAPATRA P, CHAKRABARTI S. Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper[J]. IEEE Commun Lett, 2020, 24(5): 971-975.

[10] HAMMOUTI H E, GHONGHO M, RAZA Z S A. A machine learning approach to predicting coverage in random wireless networks[C]//IEEE Globecom Workshops (GC Wkshps). Abu Dhabi, UAE: IEEE, 2018: 1-6.

[11] BAO T, ZHU J, YANG H C, et al. Secrecy outage performance of ground-to-air communications with multiple aerial eavesdroppers and its deep learning evaluation[J]. IEEE Wireless Commun Lett, 2020, 9(9): 1351-1355.

[12] NGUYEN T V, TRAN T N, SHIM K, et al. A deep neural network-based relay selection scheme in wireless powered cognitive IoT networks[J]. IEEE Internet Things J, 2021, 8(9): 7423-7436.

[13] 路晓华，贺玉成，周林. 自适应窃听下 NOMA 用户协作干扰的物理层安全研究[J]. 无线电通信技术，2020，46(2)：192-198.

[14] 桂冠，王禹，黄浩. 基于深度学习的物理层无线通信技术：机遇与挑战[J]. 通信学报，2019，40(2)：19-23.

[15] SHIM K, NGUYEN T V, AN B. Exploiting opportunistic scheduling schemes and WPT-based multi-hop transmissions to improve physical layer security in wireless sensor networks[J]. Sensors, 2019, 19(24): 5456.

（责任编辑 朱雪莲 英文审校 黄振坤）