基于机器学习的智能路由解释方法

Interpreting Machine Learning-Based Intelligent Routing Algorithms

孟子立/MENG Zili，徐明伟/XU Mingwei
（清华大学，中国 北京 100084）
（Tsinghua University，Beijing 100084，China）

DOI：10.12142/ZTETJ.202305009
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20231017.0948.002.html
网络出版日期：2023-10-17
收稿日期：2023-08-02

摘要：综述了基于机器学习的智能路由方法的进展，并提出了一种针对基于机器学习的智能路由技术的解释方法。该方法可以对神经网络等黑盒子技术的输出决策结果进行解释，支持几乎所有类型的智能路由算法。网络管理员可以利用该方法理解智能路由算法为何做出某些决策，并在此技术上进一步优化算法，排除故障，增强部署信心。

关键词：智能路由；图神经网络；超图；可解释性

Abstract: The recent advances in machine-learning-based intelligent routing algorithms are reviewed and a new interpretation method for machine-learning-based intelligent routing algorithms is proposed. This method can explain output decision results of black-box technologies such as neural networks. Network operators can therefore utilize such an interpretation method to understand the logic behind it. Further optimizations of the algorithm, debugging, and enhancing the confidence of deployment can be explored.

Keywords: intelligent routing; graph neural network; hypergraph; interpretability

引用格式：孟子立, 徐明伟. 基于机器学习的智能路由解释方法 [J]. 中兴通讯技术, 2023, 29(5): 56-60. DOI: 10.12142/ZTETJ.202305009
Citation：MENG Z L, XU M W. Interpreting machine learning-based intelligent routing algorithms [J]. ZTE technology journal, 2023, 29(5): 56-60. DOI: 10.12142/ZTETJ.202305009

路由是网络中的重要科学问题，是数据包从一端到另一端寻路所必需的组成部分。近年来，智能路由技术也得到业界越来越多的关注。智能路由技术智能的智能性主要体现在路由算法开始采用机器学习、深度学习等技术，并使用了图神经网络、强化学习等建模、训练方法来对路由算法进行优化。

然而，随着机器学习等复杂算法的引入，路由的决策过程逐渐变得黑盒化、不透明。因此，尽管网络管理员知道某神经网络的路由算法较优，但可能较难理解其背后的逻辑，从而不敢轻易相信。因此，基于机器学习的智能路由技术面临部署困难等问题。

1 基于机器学习的智能路由主要技术

一方面，人工智能技术在近年来发展十分迅猛；另一方面，软件定义网络与可编程路由设备的研究甚至规模部署也为基于机器学习的复杂路由算法提供了部署的可能。本节将按照机器学习技术的分类，从监督学习和强化学习两种常用的机器学习方法对智能路由的主要技术进行介绍。

1.1 基于监督学习的技术

监督学习是一种预先将网络状态和与其对应的较优的路由策略标记出来的技术。该技术使得模型能够准确地完成输入到输出映射。目前监督学习的趋势是所采用的模型基本上是深度神经网络。近年来，业界提出了一些基于监督学习的路由方法，这些方法要么直接采用深度神经网络进行决策优化，要么引入一些深度学习的模块辅助现有算法进行决策。

在直接使用深度神经网络进行决策的解决方案中，常见的做法是将网络拓扑（网络信息）与数据包序列号、流量需求矩阵、链路利用率、延迟、吞吐量、流量特征等信息通过滤波器进行特征提取后，放到深度学习模型中，然后让深度

基金项目：国家自然科学基金项目（62221003）

学习模型决定这一数据包（或者这一条流）应该遵循什么样的路由路径。在这一模型中，有的解决方案会选用卷积神经网络[1]或循环神经网络[2]，有的则会选择图神经网络[3]。

在使用智能模块辅助路由计算的解决方案中，传统方法或启发式算法依然会被启用。例如，在一个典型的路由优化问题中，神经网络可能只是替代网络环境建模、拥塞检测或者流量预测中的一个模块，其他模块依然采用启发式算法来进行计算优化。例如：有的工作仅仅是利用神经网络对链路的拥塞情况进行预测，然后采用启发式算法决策[1]；有的工作则对路径时延进行实时预测，然后基于预测的时延进行路由决策[2]。

1.2 基于强化学习的技术

强化学习是一种并不需要标记网络状态及其对应策略，而是提供一个路由环境供强化学习智能体进行学习的技术。在每个时间点t，强化学习的智能体都能观察到当前的状态s_t，并相应做出行动a_t，且收到反馈奖励r_t的过程。强化学习智能体的任务是，不断地尝试最大化学到的奖励r_t的累积求和。在采用强化学习进行路由优化的工作中，通过采取的算法，我们也可以对现有工作进行简单区分。现有强化学习算法要么采取简单传统的Q-learning进行优化，要么采用深度神经网络来学习更加复杂的策略。这其中，Q-learning以及深度神经网络便是强化学习智能体的两种表示形式。

采用Q-learning优化的智能路由算法最早可以追溯到1994年。BOYAN J. A.等提出将路由转发过程建模为马尔可夫决策的过程[4]，以路由下一跳即将选择的节点作为动作，路由每一跳所花费的时延作为奖励值。通过对每一条延迟进行优化的方式，可以有效避免路由造成的网络拥塞的发生。

采用深度神经网络的强化学习方法在输入、输出以及奖励函数上可能和上述的Q-learning对应的表示方法一致。其主要差别在于，上述Q-learning可能基于表等简单的数据结构对状态-动作的映射进行记录，但深度神经网络会采用复杂的神经网络对这一映射进行表示。XU Z.等的工作便采用多层的神经网络对智能体的策略进行表示[5]。

2 基于机器学习的智能路由主要场景

除了上述按照算法来分类外，我们还可以按照场景来对智能路由进行分类。近年来，在数据中心网络、无线网络中，智能路由的解决方案都广泛地被研究者们提出。这主要是因为，数据中心网络和无线网络有一个突出的特性，即网络内的设备大多由同一组织、实体等控制，更新换代比较容易，同时也便于部署集中式算法。对于广域网传输等领域，由于涉及的参与者众多（无线路由器、骨干网路由器、接入网路由器很可能各自归属不同的厂商），很难在短期内迅速部署一些新的路由算法。因此，本节中，我们主要围绕数据中心网络和无线网络，特别是无线传感器网络，介绍智能路由近年来的一些代表性进展。

2.1 数据中心中的智能路由

数据中心是智能路由较容易应用的一类场景。在数据中心中，发送端、接收端、网内路由器交换机等均由同一实体控制，便于运营者集中化、中心式管理。同时，由于网络规模小、设备易于控制，设备可以轻易更新为面向集中控制的路由器，例如支持软件定义网络的路由器等。在部署上，各方面都为智能路由的部署创造了条件。

例如，文献[6]提出通过深度强化学习来对全局路由表进行优化，然后再通过软件定义网络将每个路由器的路由表部署到相应路由器上，可以带来智能路由性能提升。文献[7]进一步将智能路由技术与多路径等技术进行结合，提出了基于强化学习的数据中心多路径路由技术。这些技术都在数据中心场景下，采用强化学习等智能路由技术对路由算法进行了优化，并在实际部署中取得了一定的效果。

2.2 无线网络中的智能路由

无线网络一方面作为接入网，为用户提供接入互联网的服务，似乎不需要路由；另一方面，在传感器网络等场景中，也有许多路由操作需要完成。相比于有线网络，无线网络更为复杂的是：没有固定的有线链路——理论上只要在覆盖范围内的两个节点都可以建立链接通信。这为路由算法的优化引入了新的复杂度：路由算法需要与网络拓扑进行协同优化。基于深度学习等智能路由技术恰好能够解决这一复杂的问题，其在无线场景的应用也因此应运而生。

无线网络路由问题的优化目标可能更为复杂：除去基本的延迟、吞吐等性能优化外，很多场景的应用都需要注重路由算法的能耗、健壮性等。目前已经有了一些初步的尝试，如文献[8]就介绍了一种可以让无线传感器网络中的路由结果变得更加节能、健壮的机器学习算法。基于不同应用场景，运营者可以很轻易地对优化目标做修改，重新训练机器学习模型便可获得一个目标不同的智能路由模型，因此这一场景下的智能路由模型具有很强的迁移性。TANG F.等[9]提出，基于深度学习的算法可以整合路由与拓扑优化，直接进行全局优化。通过构建实时的深度学习流量控制机制，该工作可以直接对各个节点发送流量以及目的节点进行优化控制，达到整体上降低节点间发送延迟、提高吞吐量的目的。

3 基于超图的智能路由解释技术

本节中，我们介绍一种使用超图来对基于机器学习的智能路由算法进行解释的技术。我们首先简要介绍超图，以及如何使用超图来表示网络系统。然后，介绍如何使用超图来解释网络系统中的关键组件。

3.1 超图形式化

超图由点和超边组成。一个普通图中的边与超图中超边的主要区别在于：超边可以覆盖多个顶点，如图1所示。我们将所有顶点和超边的集合分别表示为V和E，每个顶点v和超边e的特征分别表示为f_v和f_e，所有顶点和超边的特征矩阵分别表示为F_V和F_E。

使用超图，我们还可以表示SDN路由优化的建模。SDN控制器收集所有数据平面交换机的信息。在这种情况下，SDN路由优化器分析每个源–目的地对的流量需求，并基于拓扑结构和链路容量为所有源–目的地流量需求生成路由路径。

然而，由于路径中交换机的数量是不确定的，因此路由路径是很难表示的高阶信息。以前研究者尝试使用整数规划来表示路径，但是这种方法很难在有限的时间内进行有效优化。RouteNet[3]设计了一种基于深度神经网络的优化算法，以连续地为每个源–目的地流量需求对选择最佳路由路径。

为了使用超图来形式化系统，我们将路径视为超边，物理链路视为顶点。覆盖顶点的超边表示该对需求的路径包含一条链路。图1展示了超图映射结果的一个例子。链路（1，2，…，8）被建模为顶点。两对传输需求（$a \to e$和$a \to g$）被建模为超边（表示为e_1和e_2）。顶点特征F_V是链路容量。超边特征F_E是每对交换机之间的流量需求量。如果超边e覆盖顶点v，则e的对应的网络流量需求应通过v的对应的链路。

RouteNet生成整体路由结果，即所有流量需求的路径。例如，假设RouteNet决定从a到e的需求通过链路2、5、6（蓝色路径），从a到g的需求通过链路1、3、6、8，相应的超图应该是图1（c）。超边e_1覆盖顶点2、5、6，超边e_2覆盖1、3、6、8。所有顶点–超边连接$\{v,e\}$是：

$$\{(2,e_1),(5,e_1),(6,e_1),(1,e_2),(3,e_2),(6,e_2),(8,e_2)\}, \quad (1)$$

其中，解释工作的关键是我们需要知道哪些是对整体路由决策至关重要的连接。如果网络管理员知道这个机器学习的智能体中决定性的决策，那么他们或许就可以从关键决策的对比中理解智能路由决策的原因。在这里，我们总结了我们能用超图对路由结果表示的两个原因：

1）图结构化输入或输出。由于图是超图的一种简单形式，如果全局系统的输入或输出是图结构化的，则该系统可以自然地用超图表示。

2）二元变量映射。如果全局系统构建两个变量之间的映射，这两个变量可以用顶点和超边表示。映射可以用超图中的连接关系表示。这不仅仅包括路由，有时候也可以拓展至许多资源分配系统中资源（如物理服务器）和请求（如网络功能）之间的映射构建。

只要全局系统具有上述特征之一，我们就可以用超图进行表示并解释。

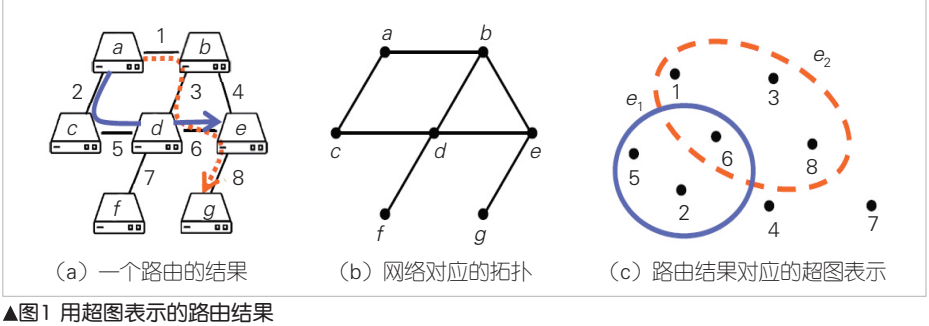
3.2 关键连接搜索

下一步，我们要找到对原始系统优化结果至关重要的顶点–超边连接。首先，我们介绍超图的关联矩阵表示。关联矩阵I（大小为$|E|\times|V|$）是一个0–1矩阵，用于表示顶点和超边之间的连接关系。$I_{ev}=1$表示超边e包含顶点v。例如，图1中超图的关联矩阵为：

$$I=\begin{pmatrix}0&1&0&0&1&1&0&0\\1&0&1&0&0&1&0&1\end{pmatrix}。 \quad (2)$$

我们的设计目标是评估原始系统的每个连接对优化结果的影响。以SDN路由为例，我们将评估式（2）中每个（链接、路径）连接对原始系统优化结果的影响。我们通过分数的关联矩阵$W\in[0,1]^{|E|\times|V|}$来表示每个超边–顶点连接的重要性。如果v和e之间没有连接，则$W_{ev}=0$。关键连接搜索算法的概述为：

$$\min D(Y_W,Y_I)+\lambda_1||W||+\lambda_2 H(W) \quad \text{s.t.}\ 0\leqslant W_{ev}\leqslant I_{ev},\ \forall v\in V,\ e\in E, \quad (3)$$



（a）一个路由的结果　（b）网络对应的拓扑　（c）路由结果对应的超图表示

▲图1 用超图表示的路由结果

其中，$D(Y_W,Y_I)$、$||W||$、$H(W)$分别展开为：

$$D(Y_W, Y_I) = \begin{cases} \sum Y_W \log \frac{Y_W}{Y_I}, & \text{离散} \\ \sum ||Y_W - Y_I||^2, & \text{连续} \end{cases}, \quad (4)$$

$$||W|| = \sum_{v,e} |W_{ev}|, \quad (5)$$

$$H(W) = -\sum_{v,e} \left(W_{ev} \log W_{ev} + (1 - W_{ev}) \log (1 - W_{ev}) \right), \quad (6)$$

其中，优化目标包含3个部分：

1）性能退化$D(Y_W,Y_I)$。关键的连接应是那些对网络系统输出有很大影响的连接，这是与任务无关的。因此，我们需要测量机器学习智能路由系统原始输入特征和掩码W加权的输入特征的差别。掩码特征（需求、容量）生成的路由决策应该与原始决策类似。我们将原始输入和输入掩码W生成的决策分别记为Y_I和Y_W。因此，我们最大化Y_W和Y_I之间的相似性，记为$D(Y_W, Y_I)$。路由系统的输入/输出有时是连续的，有时也可能会是离散的。例如，当预测一条流的转发路径时，路由系统的输出就是一个离散的节点序列；当预测一条链路上的拥塞程度时，路由系统的输出就是一个连续的值。针对不同的变量类型，我们分别采用不同的距离估计方法。我们采用KL散度来测量离散输出（如路由决策序列）和均方误差。这两者都是机器学习社区中常见的相似性度量。

2）解释简洁性$||W||$。通常，人们可以理解的解释数量是有限的。因此，关键连接的数量也应尽可能少，以便网络操作员理解。如果算法提供了太多的“关键”连接，网络操作员则会感到困惑，无法轻松解释网络系统。我们将W的简洁性定义为所有元素的和（矩阵的规模）。另外，我们还需要在优化目标中惩罚掩码W的大小。

3）确定性$H(W)$。此外，我们还期望W的结果是确定的，即对于每个连接(v,e)，要么和结果毫无关系（W_{ev}接近0），要么对结果影响很大（W_{ev}接近1）。否则，智能体可能将学会掩盖所有具有相同权重的连接并生成无意义的解释。在本文优化掩码W的熵，以鼓励W中的连接接近1或0，其中熵是信息论中的不确定性度量。

为了平衡上述的优化目标，我们为网络操作员提供了两个可定制的超参数（λ_1和λ_2）。例如，路由结果的在线监视器可能只需要最关键的信息来帮助它快速做决策，而如果管理员想要离线分析解释结果，则解释结果必须要很详细才能进一步改进智能路由模型。在这种情况下，网络操作员可以增加（或减少）λ_2来减少（或增加）具有中位掩码值的未确定连接的数量。然后，我们将向网络操作员公开更少（或更多）的关键连接。网络操作员可以在其应用程序中调整优化目标不同部分的权重。

在这种情况下，连接对输出的贡献可以被定量表示。我们可以通过连接所涉及的链路流量来定量地了解连接对输出的贡献。同时，还可以通过掩码值来进一步判断哪个连接上的哪个流量在整体结果中起主导作用。这样，我们就可以提供更细粒度的解释。

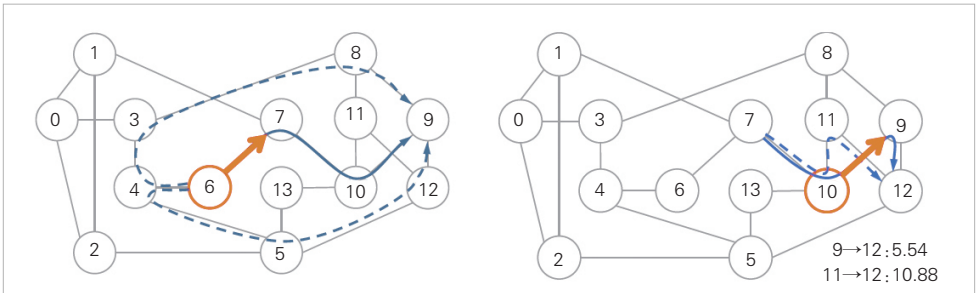
4 一个解释的例子

我们首先复现了RouteNet[3]的代码原型，并基于真实流量数据在RouteNet上测试了所提出的解释方法。同时，我们测试了RouteNet中的NSFNet拓扑以及流量数据，具体如图2所示。如第3节中所描述的解释方法，每个连接的掩码值W代表了该连接对于最终智能路由方法的决策影响程度。掩码值前5名的连接组合列见表1。

在表1中，可以看出，掩码值越接近于1，该链路的选择对整体路由路径的选择就越关键。例如，路由路径6→7→10→9和链路6→7之间的掩码值为0.886，这说明在节点6

▼表1 RouteNet在NSFNet上的解释结果的前5名掩码值

	路由路径	关键链路	掩码值M_{ve}	决策原因
#1	6→7→10→9	6→7	0.886	路径更短
#2	1→7→10→9	1→7	0.880	路径更短
#3	7→10→9→12	10→9	0.878	负载更低
#4	8→3→0→2	8→3	0.875	路径更短
#5	6→4→3→0	6→4	0.874	负载更低



(a)表1中连接#1的选择　(b)表1中连接#4的选择

▲图2 两个RouteNet路由结果解释方法的示意

上做出选择链路6→7这一个决策十分关键。与之相反，在节点7上选择链路7→10、在节点10上选择链路10→9，可能因为这些结果的选择都比较显然，或者它们对性能影响不大，因此就不是那么关键。例如，在节点7上如果不选择7→10而选择7→1，那么便和目的节点南辕北辙了，选择7→1的路径性能会显著劣于7→10，因此做出这一判断并非难事。

我们选取了表1中路径更短、负载更低这两个原因中掩码值最高的两条路由路径分别做进一步的解释。

对于#1，如图2（a）所示，如果流量想从节点6（源）到节点9（目的），路由算法选取的路径就有很多，常见的有3条（如图2（a）中蓝色的3条）。这3条路径长度差不多，均不超过4跳；而其他路径则都要在5跳以上才能到达节点9。在3条候选路径（蓝色）中，最短路径（实线路径）的第1跳是6→7，而其他路径（虚线路径）的第1跳是6→4。因此，我们发现，第1跳的选择对于从6到9的路径来说是是重要的，因此选择6→7。一旦路由算法能够正确地将第1跳的路由决策选择为6→7而不是6→4，那么后面的路由决策就变得很简单了。因此，第1跳的决策在路由路径中至关重要。

对于#2，如图2（b）所示，如果流量想要从节点7（源）到节点12（目的），长度相等的最短路径有2条（图2（b）中蓝色的两条），网络管理员需要理解为什么RouteNet选择了7→10→9→2。我们的解释方法显示，在节点10上时，选择10→9这个链路而非10→11非常重要。有了这个线索，我们在进一步分析两条路径的负载情况后发现，11→12链路的负载大约是9→12的2倍（如图2（b）所示）。如果要避开11→12的链路，到了节点11再避开就太晚了，因为次优的路径将不得不选择7→10→11→8→9→12，远远长于7→10→9→2。因此，在节点10上选择链路10→9这一决策对性能影响非常大。我们的解释算法能够准确揭示出来这两个决定，显示了解释方法的有效性。

5 结束语

随着基于机器学习的智能路由技术的广泛应用，对这些机器学习技术进行解释的需求也会应运而生。这可以让更多的智能路由技术得到应用，推动智能路由的部署。随着机器学习技术的发展以及可解释性的提高，性能更强的智能路由方法将会出现，路由算法的提升前景将会非常乐观。未来，智能路由技术及其解释技术将会成为网络路由的主流技术之一。

参考文献

[1] BARABAS M, BOANEA G, DOBROTA V. Multipath routing management using neural networks-based traffic prediction [EB/OL]. [2023-08-12]. http://personales.upv.es/thinkmind/EMERGING/EMERGING_2011/emerging_2011_6_30_40129.html

[2] VALADARSKY A, SCHAPIRA M, SHAHAF D, et al. Learning to route [C]// Proceedings of the 16th ACM Workshop on Hot Topics in Networks. ACM, 2017: 185-191. DOI: 10.1145/3152434.3152441

[3] RUSEK K, SUAREZ V J, MESTRES A, et al. Unveiling the potential of Graph Neural Networks for network modeling and optimization in SDN [C]//In proceedings of the ACM symposium on SDN research, ACM, 2019: 140-151

[4] BOYAN J A, LITTMAN M L. Packet routing in dynamically changing networks: a reinforcement learning approach [C]//Proceedings of the 6th International Conference on Neural Information Processing Systems. ACM, 1993: 671-678. DOI: 10.5555/2987189.2987274

[5] XU Z Y, TANG J, MENG J S, et al. Experience-driven networking: a deep reinforcement learning based approach [C]//Proceedings of IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. IEEE, 2018: 1871-1879. DOI: 10.1109/INFOCOM.2018.8485853

[6] LIU W X, CAN J, CHEN Q C, et al. DRL-R: deep reinforcement learning approach for intelligent routing in software-defined data-center networks [EB/OL]. [2023-08-10]. https://www.sciencedirect.com/science/article/abs/pii/S1084804520303313

[7] JUA A, SINGH K K , VIMALA D K, et al. Reinforcement learning based weighted multipath routing for datacenter networks [EB/OL]. [2023-08-10]. https://www.sciencedirect.com/science/article/pii/S2214785321003412

[8] NAYAK P, SWETHA G K, GUPTA S, et al. Routing in wireless sensor networks using machine learning techniques: challenges and opportunities [J]. Measurement, 2021, 178: 108974. DOI: 10.1016/j.measurement.2021.108974

[9] TANG F X, MAO B M, FADLULLAH Z M, et al. On removing routing protocol from future wireless networks: a real-time deep learning approach for intelligent traffic control [J]. IEEE wireless communications, 2018, 25(1): 154-160. DOI: 10.1109/MWC.2017.1700244

作 者 简 介

孟子立，清华大学在读博士研究生；主要研究领域为实时多媒体传输与基于人工智能的网络系统；曾获微软学者奖学金、字节跳动奖学金等；发表论文30余篇。

徐明伟，清华大学教授、网络科学与网络空间研究院执行院长、国家杰出青年基金获得者、国家自然科学基金委创新群体负责人、国家“万人”计划领军人才、国家重点研发计划“宽带通信与新型网络”和“多模态网络与通信”重点专项专家、中国通信学会常务理事、中国计算机学会互联网专委会副主任委员；主要研究领域为互联网体系结构、大规模路由和网络空间安全。