安全语义通信：基础与挑战

Zhaohui Yang、Mingzhe Chen、Gaolei Li、Yang Yang 和 Zhaoyang Zhang

arXiv:2301.01421v1 [cs.IT] 4 Jan 2023

摘要——**语义通信使接收端能够了解意图，而非比特信息本身。这是一种新兴技术，可支持未来无线通信中的实时人机交互和机器间交互。在语义通信中，发送端和接收端共享一些共同知识，可用于在发送端提取小规模信息，并在接收端恢复原始信息。由于设计目的不同，与传统的逐比特通信相比，语义通信中的安全问题具有两个独特特征。首先，语义通信中的攻击者不仅关注被窃数据的数量，也关注被窃数据的含义。其次，语义通信系统中的攻击者不仅可以像在传统通信系统中那样攻击语义信息传输，还可以攻击用于语义信息提取的机器学习（ML）模型，因为大多数语义信息都是通过基于机器学习的方法生成的。鉴于这些独特特征，本文概述了安全语义通信设计的基础和主要挑战。我们首先介绍定义和提取语义信息的各种方法，然后重点探讨两个领域的安全语义通信技术：信息安全和语义机器学习模型安全。针对每个领域，我们指出主要问题和挑战，并对这些问题进行全面讨论。总而言之，本文为如何在真实世界的无线通信网络中设计安全语义通信系统提供了一套全面的指导原则。**

索引词—**安全语义通信、信息安全、semanticML 模型安全。**

I. 引言

智能手机处理器的发展使边缘设备（即移动电话）能够生成和处理大量图像、视频及沉浸式扩展现实数据，这将显著加剧网络拥塞 [1]。因此，有必要设计新型通信技术，以支持此类大容量数据的传输与处理。当前研究 [1] 探讨了机器学习（ML）工具、反射式智能超表面（RIS）、毫米波（mmWave）和边缘计算在提升网络性能方面的应用。然而，利用这些技术的网络性能将受香农容量限制，因为这些技术大多旨在提高边缘设备的数据速率，使其达到香农容量极限 [2]。因此，有必要设计新型通信技术，进一步提升网络性能，使其超越香农容量极限。

语义通信技术是一种有望突破香农容量限制的方法，它使边缘设备能够提取大规模数据的含义（以下简称语义信息），并仅将语义信息传输给接收端，而非传输全部数据 [3]。因此，与目前仅关注最大化设备数据速率的研究相比，语义通信的目标不仅是最大化每个设备的数据速率，还要最大化传输数据所能承载的含义。由于语义通信仍处于起步阶段，面临诸多挑战，例如语义信息定义、语义信息提取、语义通信测量、安全问题和韧性。

近年来，[3]–[6]中出现了许多与语义通信相关的综述和教程。特别是，[3]–[5] 中的作者提供了一份全面的教程，介绍如何利用信息论进行语义信息表示和语义通信度量设计。[6] 中的作者介绍了一种基于边缘智能的语义通信框架，并阐述了其实现面临的挑战。然而，现有的这些综述和教程中，没有一篇 [3]–[6]介绍语义通信中的安全问题。与在标准通信系统中只考虑被窃数据数量的攻击者相比，语义通信中的攻击者具有两个独特特征。首先，语义通信中的攻击者不仅会考虑被窃数据的数量，也会考虑被窃数据的含义。例如，如果攻击者从用户处窃取了大量数据，却未能从被窃数据中获取目标内容或含义，我们就认为该攻击者未能成功攻击用户。其次，语义通信系统中的攻击者不仅可以像在标准通信系统中那样攻击语义信息传输，还可以攻击用于语义信息提取的机器学习模型，因为大多数语义信息都是通过基于机器学习的方法生成的。鉴于语义通信中攻击者的这些独特特征，有必要介绍实现安全语义通信的基础知识和挑战。

Zhaohui Yang 和 Zhaoyang Zhang 任职于中国杭州 310027 的浙江大学信息科学与电子工程学院，以及中国杭州 310007 的浙江省信息处理、通信与网络重点实验室（IPCAN）。Zhaohui Yang 同时任职于中国杭州 31121 的之江实验室。（电子邮箱：yang zhaohui@zju.edu.cn 和 ning ming@zju.edu.cn）。Gaolei Li 任职于中国上海交通大学电子信息与电气工程学院。（电子邮箱：gaolei li@sjtu.edu.cn）Yang Yang 任职于北京邮电大学信息与通信工程学院。（电子邮箱：yangyang01@bupt.edu.cn）Mingzhe Chen 任职于美国佛罗里达州科勒尔盖布尔斯 33146 的迈阿密大学电气与计算机工程系及数据科学与计算研究所。（电子邮箱：mingzhe.chen@miami.edu）

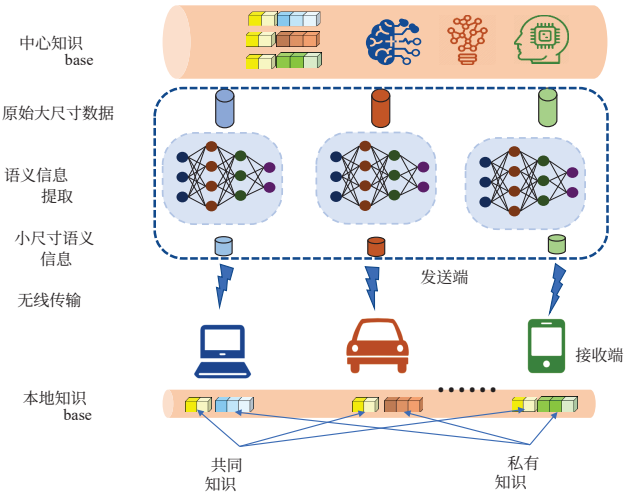

图1. 语义通信系统基本结构示意图。

本文介绍安全语义通信系统设计的基础知识、解决方案和挑战。在此背景下，我们首先介绍基本的语义通信流程。随后，我们概述定义语义信息的四种方法：a）自编码器，b）信息瓶颈（IB），c）知识图谱，以及 d）概率图，并总结它们的优点、缺点和应用。然后，我们介绍攻击者如何攻击语义信息传输和提取，并从信息安全和机器学习安全两个角度阐述防御这些攻击的方法。

II. 语义通信基础

本节首先介绍语义通信的过程。然后，我们介绍四种对从原始数据中提取的语义信息进行建模的方法，并解释它们之间的差异、优点、缺点和应用。

A. 语义通信过程

整体语义通信过程主要包括三个阶段。在第一阶段，发送端利用机器学习工具，基于中央知识库从原始大尺寸数据中提取小尺寸语义信息，如图1所示。随后，在第二阶段，语义信息通过无线链路传输。在第三阶段，接收端基于自身的本地知识库恢复语义信息背后的预期含义，其中本地知识库包含共同知识和私人知识。

B. 语义信息构建

1) 自编码器：语义通信传输语义消息，即从源背后的“含义”中学习到的、由一系列规范符号构成的序列。相应地，接收端旨在充分理解编码后的语义符号所承载的“含义”。因此，在忽略冗余信息的同时有效提取信源语义，对于语义通信至关重要。神经网络具有强大的表示与学习能力，因此通常用于提取信源语义。具体而言，自编码器是一种用于学习高维数据高效表示的神经网络，能够提取最重要的信息，因此特别适用于语义通信。自编码器由编码器和解码器组成。编码器输出的编码符号维度远低于源数据，因为它只保留关键信息，丢弃数据中不重要的部分。随后，解码器用于根据低维符号恢复原始数据。

使用自编码器提取语义信息具有以下优点。首先，自编码器可以基于多种类型的神经网络实现，例如卷积神经网络、变换器和全连接神经网络。因此，它适用于文本、图像、视频和多模态数据等不同源数据的语义通信。此外，由于编码器的输出维度大幅减少，语义通信的传输效率可以显著提高。而且，自编码器可以通过自监督方式进行训练。然而，自编码器也面临一些关键挑战。特别是，尽管机器能够高效地理解自编码器生成的编码，但人类却无法理解，这在某种程度上似乎与语义通信的原则相矛盾。表 I 总结了使用自编码器对语义信息进行建模的优点、缺点和应用。

2）信息瓶颈：由于语义通信旨在仅保留语义，因此语义通信的本质是一个有损压缩问题。为了解决这类问题，克劳德·香农提出了基础理论，即率失真理论，该理论解决了压缩与保真度之间的最优权衡问题 [7]。具体而言，率失真理论旨在给定失真的条件下，将所需码率降至最低，可用于指导语义通信系统的训练过程。然而，率失真理论的一个问题是，它需要预先选择特定的失真函数，而这将进一步决定所提取的语义。不过，失真函数的选择并不属于该理论的范畴。

为了解决这一问题，信息瓶颈（IB）原理从信息论的角度被提出，可视为率失真理论的一种推广 [8]。一方面，信息瓶颈（IB）原理中的失真通过编码后的语义符号与目标变量之间的互信息来衡量。在语义通信中，目标变量因应用而异。例如，对于图像分类任务，目标变量是源图像的标签，因为我们的目标是正确地对源图像进行分类。另一方面，信息瓶颈（IB）原理中的码率由信源与编码符号之间的互信息表征，这表明编码符号用于表示信源所需的比特数。

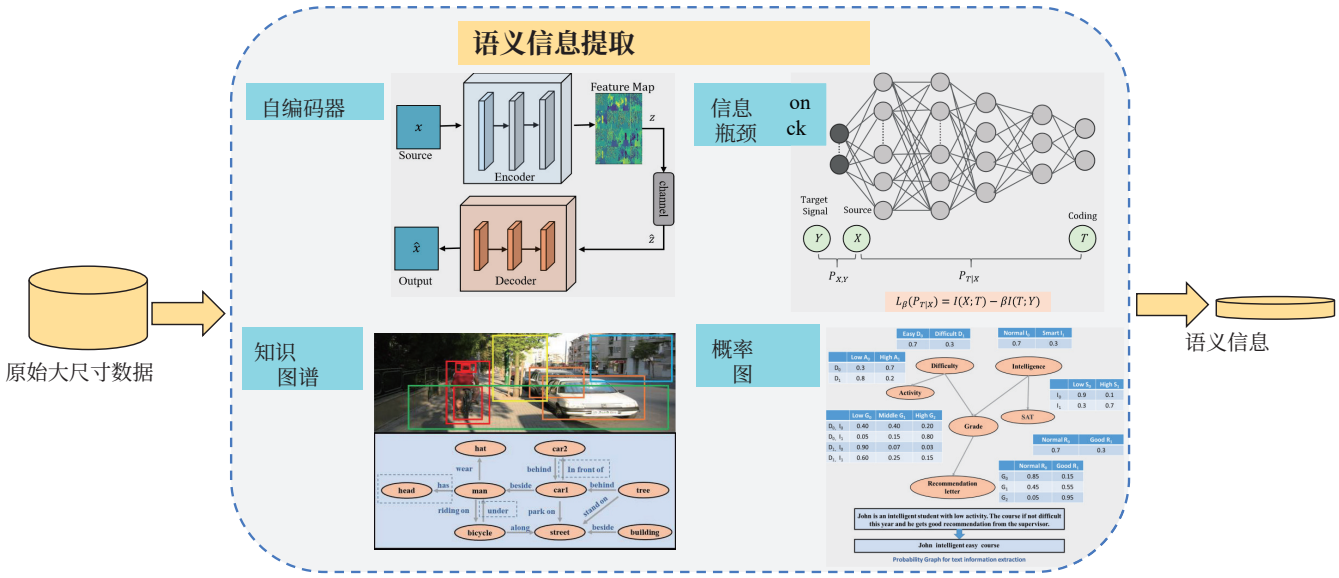

图2. 四种语义信息提取类型示意图。

信息瓶颈（IB）的优点在于，它为在给定失真条件下最小化码率提供了明确的理论界限。然而，在实践中，信息比特的联合分布和边缘分布难以获得，因此，原始的信息瓶颈（IB）无法直接用于指导语义通信的训练过程。表 I 总结了使用信息瓶颈对语义信息建模的优点、缺点和应用。

3）知识图谱：由于自编码器输出所表示的语义信息难以被人类理解，也不具有任何物理意义，接下来我们将介绍如何使用知识图谱来表示语义信息。知识图谱由节点和边组成，因此我们用节点表示原始数据中的对象或概念，并用边表示每对节点之间的关系。每对节点及其关系由一个三元组定义。因此，以知识图谱建模的语义信息由多个三元组组成。与其他图模型不同，知识图谱中的三元组由用户想要传输的原始数据以及该用户理解原始数据所具备的知识共同决定。因此，不同用户凭借不同知识从同一原始数据中提取的语义信息可能不同。

使用知识图谱对语义信息进行建模具有几个主要优点。首先，提取出的语义信息易于人类理解。因此，接收端收到语义信息后可能无需恢复原始数据，因为语义信息表达了与原始数据相似的含义。其次，可以根据网络条件和资源管理由若干三元组组成的语义信息的数据量。具体而言，当网络资源（即带宽）有限时，可以限制语义信息中的三元组数量，以满足通信服务要求（即时延）。然而，利用知识图谱进行语义信息建模也面临若干挑战。首先，语义信息中的所有三元组均由基于神经网络的方法提取。因此，在面向能源受限设备（即物联网设备）使用知识图谱时，必须考虑并降低这些神经网络的训练复杂度和耗时。其次，目前大多数研究都假设所有用户在提取三元组时拥有相同的知识，这可能不切实际。因此，有必要设计新方法，为每位用户建模并生成独有的知识库。表 I 总结了使用知识图谱对语义信息进行建模的优点、缺点和应用。

4）概率图：有向概率图也可用于表征传输信息 [9] 的内在信息。在有向概率图中，每个顶点代表一个语义实体，边则表示这两个顶点之间的连接概率。由于多个彼此之间连接概率较高的顶点可以融合为一个顶点，因此新生成的顶点能够包含比原始顶点更高层次的语义信息。概率图展示了不同实体之间的概率，可用于提取概率图中整体概率较高的核心语义信息。

使用概率图提取语义信息具有一些优点。首先，可以利用概率将高度相关的低层语义实体组合成高层语义实体，从而生成不同层次的语义信息。其次，概率图可用于预测接收端即将接收到的信息。通过预测和推理，接收端可以提前调整其行动。然而，使用概率图仍面临一些挑战。由于概率图可以通过神经网络学习，而且提取多层语义信息需要额外的计算，因此构建多层语义信息的复杂度

表 I 各种语义信息构建方法

分类	优点	缺点	应用
自编码器	• 自编码器适用于不同模态的数据 • 自编码器可以通过自监督方式进行训练	•提取出的语义信息人类无法理解	• Deep 联合信源-信道编码 • 多模态语义传输
信息瓶颈	• 信息瓶颈为在给定失真条件下最小化码率扭曲	• 互信息难以获得 •提取出的语义信息人类无法理解	• 面向任务的语义传输传输
知识图谱	• 建模后的语义信息具有物理含义 • 接收端无需恢复原始 data	• 发送方需要生成用于机器学习模型训练的知识库库，用于机器学习模型训练 • 词元选择由复杂的神经网络实现	• 机器到机器通信 • 人类 to 机器通信
概率图	• 概率图可用于进行推理 • 不同层次的语义信息可以被提取	• 计算复杂度高 • 发送端和接收端都需要共享一些共同知识	• 多层语义信息 •信息预测与推理

很高。此外，为确保接收端能够准确预测发送端未来的信息，发送端和接收端都需要共享一些高度相关的共同知识。表 I 总结了使用概率图对语义信息建模的优点、缺点和应用。因此，图 2 展示了上述四种方法的语义提取过程。

III. 信息安全

接下来，我们介绍语义信息传输中的安全问题。具体而言，我们将讨论信息瓶颈、转换通信和物理层中的安全问题，并总结在这些场景中实现安全语义通信所面临的挑战。

A. 信息瓶颈安全

本小节介绍信息瓶颈在安全语义通信中的应用。如前所述，信息瓶颈利用信源与编码符号之间的互信息，以及编码符号与目标变量之间的互信息，分别表示语义通信系统的码率和失真。遵循这一原则，可以进一步将信息瓶颈扩展到安全语义通信中。具体而言，当存在攻击者试图在语义通信过程中检测合法用户的敏感语义信息时，可以通过最小化敏感信息与编码后的语义符号之间的互信息，降低敏感语义信息泄漏概率。这样，信息瓶颈便能同时考虑语义通信的码率、失真和安全性，因此其目标是在给定失真和信息泄漏风险的条件下，将码率降至最低。

此外，信息瓶颈（IB）也可用于分析安全语义通信系统的训练过程。具体而言，我们可以将信息瓶颈（IB）用作损失函数来训练语义通信系统。在训练过程中，我们可以估算三个互信息项的值，从而分析训练各阶段码率、失真和安全性之间的性能权衡过程。这样，我们就能更好地理解安全语义通信系统的训练过程，并进一步据此选择合适的超参数，以优化系统性能。

然而，将信息瓶颈用于指导安全语义通信仍面临一些关键挑战。具体而言，与信息瓶颈的原始形式类似，由于编码符号和敏感信息的联合分布及边缘分布通常未知，因此互信息难以计算。因此，需要互信息项的紧致可训练界，以便有效训练语义通信。

B. 隐蔽语义通信

本小节介绍隐蔽通信在语义信息传输中的应用。在语义通信中，我们不仅关注攻击者检测到的数据量，也关注其检测到的原始数据含义。因此，我们可以采用两种方法保护发送方的数据隐私。首先，可以使用传统的隐蔽通信技术来保护发送方的数据隐私。具体而言，可以向攻击者试图攻击的用户发送干扰信号，从而保护该用户的数据隐私。其次，可以修改语义信息中的三元组，避免携带攻击者试图检测的三元组。我们还可以结合使用传统隐蔽通信方法和三元组选择方法，以保护用户的数据安全。

然而，采用转换通信实现安全语义通信也面临着若干挑战。首先，发送方需要估计攻击者想要检测的三元组

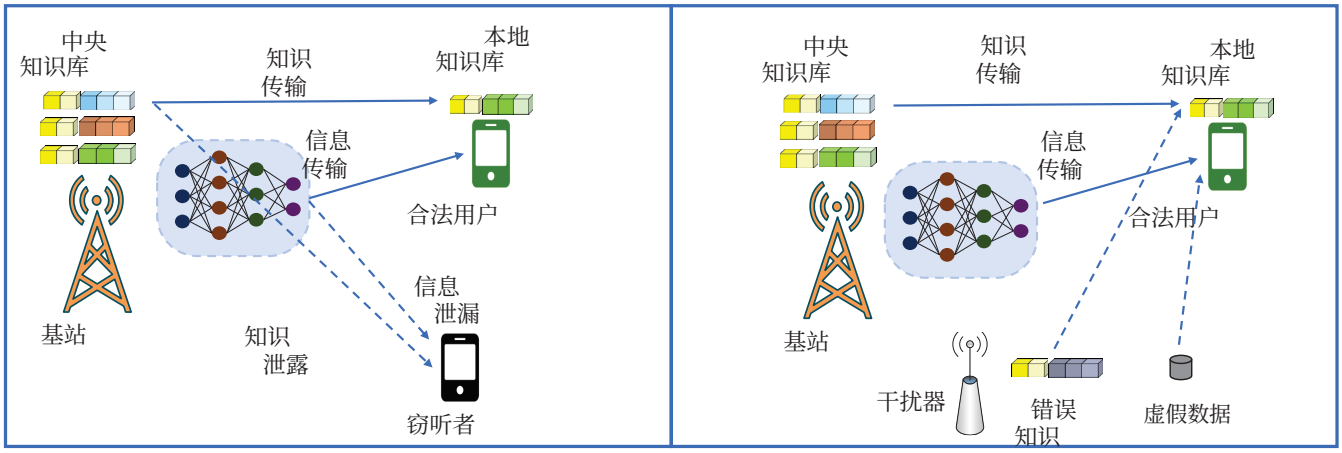

图3. 窃听者和干扰器参与的语义通信系统物理层安全示意图。

以及接收端希望接收的三元组，因为在语义信息传输之前，发送方不会与攻击者和接收端进行通信。其次，有必要分析实施这两种数据保护方法所产生的能耗、数据传输时延及其他成本。为此，可以根据不同的网络条件，决定采用传统的转换通信方法还是三元组选择方法。例如，当发送方的发射功率有限，无法满足语义信息传输需求时，我们可能无法采用传统的转换通信方法来保护用户数据安全，因为接收端可能无法检测到发送方的原始信号。最后，研究发送方与接收端之间的协作，以进一步提升数据安全，也是一个有趣的研究方向。

C. 物理层安全

语义通信的物理层安全 [10], [11] 包括两个方面：共享知识库安全和语义信息安全。

1) 知识库安全： 发送端和接收端共享共同知识库，这有助于发送端提取语义信息，并使接收端能够恢复接收比特背后的信息。因此，保护共同知识库至关重要。如图3所示，语义通信的物理层安全包括两种情况。在窃听情况下，发送端的知识可能会泄露。在干扰情况下，干扰器可能发送错误知识，导致合法用户从接收到的语义信息中恢复出错误消息。为保护知识安全，可采用波束成形设计和安全密钥分发方法。

2）语义信息安全：语义信息基于发送端与接收端共享的知识，这表明语义信息与条件信息相关。根据语义信息的构建过程，除了传统的干扰和噪声之外，还存在语义干扰和噪声。语义干扰包括信息的歧义。例如，同一个词或短语在不同场景中可能有不同的含义。背景信息有限时，很难辨别特定语义信息的真实含义，从而造成语义干扰。原始信息映射到语义空间后会引入语义噪声，因为多个信息可能映射到相同或相似的语义信息，从而引入额外噪声。因此，计算安全语义信息速率时应考虑语义干扰和噪声，这要求采用新的设计来保护语义信息安全。一种可行的方法是联合学习与通信设计[12]，以确保语义通信的安全性。

IV. 语义机器学习安全

如第二节所述，知识图谱、编码器/解码器和深度神经网络等许多机器学习技术，被认为是构建语义通信系统基本组件的重要助力。本节将这些助力统称为“语义机器学习”。为推动未来语义通信系统的发展和普及，提前预测、建模和分析语义机器学习新兴的安全风险具有重要意义。例如，上传至知识库的所有语义特征都应设置完善的审查机制，以防止其被恶意用户篡改。本节首先分析语义机器学习的漏洞和已知威胁，随后讨论应对这些威胁的潜在对策。最后，我们展望可信和可解释技术在构建面向语义通信系统的安全语义机器学习模型方面的潜力。

A. 安全风险

semanticML 的主要安全风险可概括为内生风险和衍生风险，如图4所示。

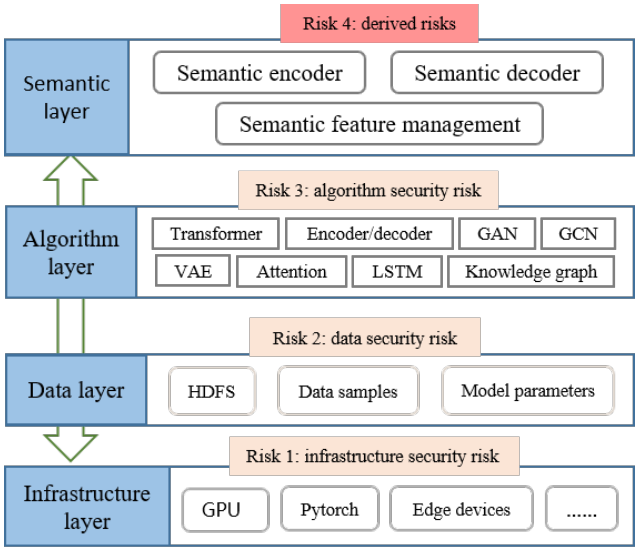

图4. 语义机器学习的层次化组成及其安全风险。

1）内生风险：对于语义机器学习而言，数据是重要的驱动因素，算法是核心技术，基础设施则提供底层支撑。内生风险可能导致数据安全威胁、算法安全威胁和基础设施安全威胁。

风险1：数据安全风险。已知的数据安全风险 [13]包括隐私泄露、数据投毒、数据污染、数据伪造等。在语义通信系统中，我们可以使用机器学习提取语义特征、生成知识库，并将传输的语义特征解析为原始数据。在每个语义通信节点的模型训练过程中，如果对手通过投毒、污染等方式篡改部分原始数据样本，数据传输的准确率就会显著下降。此外，如果在语义通信的机器学习模型中植入特定后门，即迫使机器学习模型对特定触发器（具有特定语义的内容）极为敏感，那么整个语义通信系统就容易受到恶意操纵。此外，随着模型反演、梯度泄露和成员推理等问题的出现，黑盒和白盒数据重建都可能威胁机器学习在语义通信系统中的实用性，而且这类问题很难防范。

风险 2：算法安全。黑箱问题和公平性是算法安全风险的两个主要来源。一方面，基于神经网络的机器学习算法通过复杂的计算过程提取输入数据的特征，然后将其分类到标定类别中，但现有的科学知识和原理无法对分类结果给出合理解释，这是攻击难以得到有效防御的根本原因。例如，在基于神经网络的语义通信系统中，接收端输出错误结果时，很难定位故障所在。另一方面，在从海量数据中提取知识的过程中，通常会使用排序、分类、关联、过滤和注意力机制等算法来处理数据项。如果算法在不同性别或族裔设置下表现出不公平的输出，使用语义通信系统进行信息传输就会面临复杂的社会问题。

风险 3：基础设施安全。为训练语义机器学习模型并提供智能通信服务，需要构建各种开发库、连接异构计算设备并搭建云平台。一旦攻击者利用这些语义机器学习基础设施中的漏洞，通过这些基础设施生成的语义机器学习模型就可能出现异常行为。例如，Tensorflow 和 PyTorch 上的恶意软件可能会修改模型结构，而一些黑客则会试图非法占用深度学习节点的计算资源（例如图形处理器、中央处理器和虚拟机）进行挖矿。

2）衍生风险：除了现有的内生风险外，由于真实应用场景具有开放性，在语义通信中部署机器学习模型还面临许多衍生风险。衍生风险主要包括语义对抗样本和语义后门。例如，可用于构建实时语义通信的视觉变换器容易受到对抗样本攻击 [14]。此外，衍生风险还包括中间人攻击、分布式拒绝服务攻击和信号干扰攻击，因为语义通信发送端和接收端上的机器学习模型需要进行跨域训练。

B. 对策

为说明如何针对语义通信系统中存在上述安全风险的机器学习模型发起攻击，图5展示了大多数已知攻击。根据已知攻击的特征，相应的对策主要分为三个方面：1）抗投毒；2）提高对对抗样本的鲁棒性；3）防止隐私泄露。抗投毒方法有三种不同的设计范式，包括：a）移除投毒数据；b）平滑异常激活值；c）清除隐藏后门。a）和b）都需要访问模型训练过程，这对于服务提供商而言通常并不实际。触发器反演和无数据知识蒸馏作为黑盒防御技术，正日益受到关注。

在模型鲁棒性方面，最常见的对策是对抗训练和差分隐私。然而，对抗训练通常需要更多数据样本，而差分隐私可能会降低模型准确率，因此，结合模型可解释性来探究对抗样本成因已成为当前研究热点。为防止攻击者从机器学习模型中恢复原始数据和语义，人们正在研究机密计算、差分隐私 [15],和联邦学习等隐私保护框架，以满足不同场景下的个体需求。在不同应用场景中，用户需要根据自身需求选择合适的隐私保护方法。此外，许多人工智能服务提供商高度重视模型水印和认证技术，以保护其知识产权。

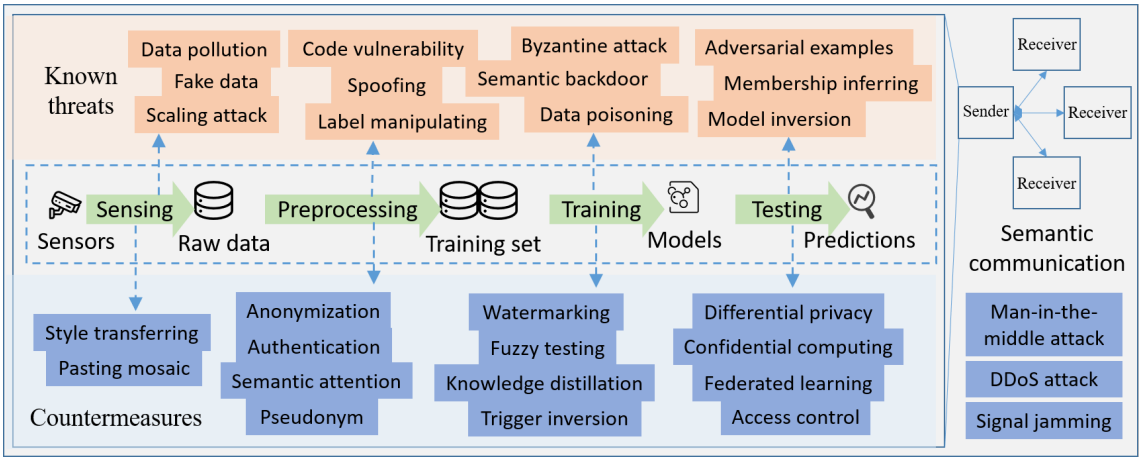

图5. 机器学习生命周期中已知威胁与对策的示意图。语义通信网络中配置了至少一个机器学习模型的每个智能体都可能遭受各种攻击。当发送端和接收端需要联合训练编码器/解码器网络时，语义通信还可能面临来自传输信道的安全威胁。

V. 结论

本文介绍了四种表示语义信息的方法。基于语义信息的构建，我们指出，语义信息安全主要包含两个方面：信息安全和机器学习安全。对于每个方面，我们都指出了主要问题及相应的解决措施。未来的研究方向包括联合设计通信与计算，以对安全语义通信进行性能分析和优化。

参考文献

[1] W. Saad、M. Bennis 和 M. Chen，“6G无线系统的愿景：应用、趋势、技术与开放研究问题”，*IEEE Network*，第34卷，第3期，第134–142页，2020年5/6月。[2] C. E. Shannon 和 W. Weaver，通信的数学理论。伊利诺伊大学出版社，1949年。[3] Z. Qin、X. Tao、J. Lu 和 G. Y. Li，“语义通信：原理与挑战”，*arXiv*预印本 *arXiv:2201.01389*，2021年。[4] Q. Lan、D. Wen、Z. Zhang、Q. Zeng、X. Chen、P. Popovski 和 K. Huang，“什么是语义通信？机器智能时代传递意义的观点”，《通信与信息网络杂志》，第6卷，第4期，第336–371页，2021年。[5] W. Yang、H. Du、Z. Liew、W. Y. B. Lim、Z. Xiong、D. Niyato、X. Chi、X. S. Shen 和 C. Miao，“面向6G未来互联网的语义通信：基础、应用与挑战”，*arXiv*预印本 *arXiv:2207.00427*，2022年。[6] G. Shi、Y. Xiao、Y. Li 和 X. Xie，“从语义通信到语义感知网络：模型、架构与开放问题”，*IEEE Communications Magazine*，第59卷，第8期，第44–50页，2021年8月。[7] C. E. Shannon，“满足保真度准则的离散信源编码定理”，*IRE*会议记录，第7卷，第9期，第56–83页，1959年。[8] Z. Goldfeld 和 Y. Polyanskiy，“信息瓶颈问题及其在机器学习中的应用”，*IEEE*通信领域精选期刊，第1卷，第1期，第19–38页，2020年。[9] T. L. Griffiths 和 M. Steyvers，“语义表示的概率方法”，载于第二十四届认知科学学会年会论文集。劳特里奇，2019年，第381–386页。[10] Y.-S. Shiu、S. Y. Chang、H.-C. Wu、S. C.-H. Huang 和 H.-H. Chen，“无线网络中的物理层安全：教程”，*IEEE* 无线通信，第18卷，第2期，第66–74页，2011年。[11] A. Mukherjee、S. A. A. Fakoorian、J. Huang 和 A. L. Swindlehurst，“多用户无线网络中的物理层安全原理：综述”，*IEEE*通信调查与教程，第16卷，1573，2014年第3期，第1550页。

[12] M. Chen、Z. Yang、W. Saad、C. Yin、H. V. Poor 和 S. Cui，“面向无线网络联邦学习的联合学习与通信框架”，*IEEE* 无线通信汇刊，第20卷，第1期，第269–283页，2021年1月。[13] M. Goldblum、D. Tsipras、C. Xie、X. Chen、A. Schwarzschild、D. Song、A. Madry、B. Li 和 T. Goldstein，“机器学习的数据集安全：数据投毒、后门攻击与防御”，*IEEE* 模式分析与机器智能汇刊，第1–1页，2022年。[14] K. Mahmood、R. Mahmood 和 M. van Dijk，“视觉变换器对对抗样本的鲁棒性”，载于*IEEE/CVF* 国际计算机视觉会议（*ICCV*）论文集，2021年，第7818–7827页。[15] T. Zhu、D. Ye、W. Wang、W. Zhou 和 P. S. Yu，“不止于隐私：在人工智能关键领域应用差分隐私”，*IEEE* 知识与数据工程汇刊，第34卷，第6期，第2824–2843页，2022年。