

引文格式:欧力源,高德民,王浩宇,等. 基于元强化学习的跨技术欺骗攻击研究[J]. 太原理工大学学报, 2026, 57(2): 397-406.

OU Liyuan, GAO Demin, WANG Haoyu, et al. Cross-technology-deception attacks based on meta reinforcement learning[J]. Journal of Taiyuan University of Technology, 2026, 57(2): 397-406.

基于元强化学习的跨技术欺骗攻击研究

欧力源, 高德民, 王浩宇, 刘 同

(南京林业大学 a. 信息科学技术学院, b. 人工智能学院, 江苏 南京)

摘 要:【目的】物联网设备已被广泛部署和应用,但其传输的开放性使得链路极易遭受攻击,欺骗攻击是目前主要攻击类型之一,传统欺骗攻击通常发生在同一类型设备中,即同构设备,如 ZigBee 对 ZigBee 设备的攻击。当前跨技术通信(Cross-technology Communication, CTC)使得不同类型设备即异构设备可以在不修改物理层下直接相互通信,如 WiFi 到 ZigBee 直接传输。跨技术通信为异构物联网带来新的安全问题,使得欺骗攻击更普遍也更容易。【方法】提出了一种基于元强化学习的跨技术欺骗攻击方法, WiFi 设备利用其传输功率较大和通信距离较远的优势对 ZigBee 无线网络进行欺骗攻击。WiFi 设备通过侦听 ZigBee 网络数据流传输特点,利用元强化学习模型,预测欺骗攻击最佳时刻。【结果】实验结果表明,本文方法相较于传统同构无线网络有效提升了对 ZigBee 网络欺骗攻击成功概率。

关键词:物联网;跨技术通信;欺骗攻击;生成对抗网络;强化学习

中图分类号:TP391 **文献标识码:**A

DOI: 10.16355/j.tyut.1007-9432.20240800

文章编号:1007-9432(2026)02-0397-10

Cross-Technology-Deception Attacks Based on Meta Reinforcement Learning

OU Liyuan, GAO Demin, WANG Haoyu, LIU Tong

(a. College of Information Science and Technology, b. College of Artificial Intelligence, Nanjing Forestry University, Nanjing, Jiangsu, China)

Abstract: 【Purposes】 Internet of things (IoT) devices have been widely deployed and applied, but the openness of their transmission makes the links extremely vulnerable to attacks. Spoofing attacks are one of the main types of attack. Traditional spoofing attacks usually occur in the same type of device, that is, homogeneous devices, such as ZigBee attack on ZigBee device. The current cross-technology communication (CTC) allows different types of device, that is, heterogeneous devices, to communicate directly with each other without modifying the physical layer, such as direct transmission from WiFi to ZigBee. CTC brings new security issues to heterogeneous IoT, making spoofing attacks more common and easier. 【Methods】 In this paper, a cross-technology spoofing attack method based on meta-reinforcement learning was proposed. WiFi devices, with their advantages of large transmission power and long communication distance were adopted to carry out spoofing attacks on ZigBee wireless networks. WiFi devices with the meta-reinforcement learning model were used to predict the best time for spoofing attacks by listening to the transmission characteristics of ZigBee network data

收稿日期:2024-11-04;修回日期:2025-01-20

通信作者:欧力源,硕士研究生,主要从事物联网安全研究, (E-mail)liyuanyou@njfu.edu.cn

streams. **【Results】** Experimental results show that compared with traditional homogeneous wireless networks, the proposed method effectively improves the success rate of spoofing attacks on ZigBee networks.

Keywords: internet of things; cross-technology communication; spoofing attack; generative adversarial network; reinforcement learning

目前,物联网技术被广泛应用于智能家居^[1]、智慧城市^[2]、工业物联网^[3]和现代农业^[4]等领域。物联网技术的快速发展,安全性直接影响其大规模应用,如医疗急救^[5]、公共安全^[6]以及工业安全^[7]。在物联网中,对于使用ISM频段的设备,其通信介质的开放性和共享性使得它们比有线网络更容易受到恶意攻击^[8]。ISM频段无需许可便可使用,大量设备在该频段上进行通信,这不仅增加了干扰的可能性,也使物联网设备更容易遭受欺骗攻击、拥塞攻击等安全威胁。

关于物联网设备攻击的研究主要分为欺骗攻击^[9]和拥塞攻击^[10]。欺骗攻击通过伪装成合法发送方利用伪造数据欺骗接收设备,实现网络访问或数据传输^[11]。拥塞攻击则通过发射无线射频干扰信号保持通信介质繁忙来阻碍无线通信,从而导致其他设备停止通信,造成数据发送延迟^[12]。传统物联网设备通信中存在信息屏障,如WiFi只能与其他WiFi设备通信,而ZigBee只能与其他ZigBee设备通信,WiFi虽然可以实现对ZigBee等无线设备的拥塞攻击,但难以实现对其他无线设备的欺骗攻击^[13]。当前,跨技术通信技术可以实现WiFi、ZigBee和蓝牙等异构设备之间的数据直传。

在传统的无线网络中,欺骗攻击通常发生在同构网络中,如利用ZigBee设备攻击ZigBee网络或利用WiFi设备攻击其他WiFi网络^[14]。跨技术通信是指异构设备之间能够实现直接的数据传输和信息交换,不需要中间的网关。跨技术通信技术能让两个异构设备之间可以相互模仿,无法区分出谁是同质设备还是异构设备,从而实现攻击。针对跨技术欺骗攻击,WiFi设备可以直接与ZigBee设备进行通信,相较于通信距离近、资源有限的ZigBee设备,WiFi设备拥有更远的传输距离,更强的发射功率,并且不受能量供应的限制^[15]。

该研究结合了强化学习和CTC技术,针对ZigBee无线传感器网络提出了一种针对物理层欺骗攻击策略。WiFi设备侦听ZigBee信道状态,获取ZigBee设备的发送帧,然后将身份信息伪装成ZigBee设备,WiFi设备将WiFi数据包伪装成普通的Zig-

Bee数据包对ZigBee网络进行欺骗攻击。使用跨技术方法,WiFi设备利用自身强大传输功率和远距离通信的优势对ZigBee无线网络进行攻击。在该研究中,强化学习被应用于WiFi设备,使其能够在适当的时机发起欺骗攻击。使用元强化学习,通过与ZigBee网络环境交互,WiFi设备可以学习何时发起攻击,以达到最佳的攻击效果。在元任务的选择标准中,选择不同网络通信节点数量和设备状态,这种选择标准确保训练模型能够在多样化的网络环境中进行有效学习。采用模型无关的元迁移机制,模型经过训练后,具有较好的初始化参数,当无线网络环境发生变化时,可以通过少量的梯度更新迅速调整策略,以适应新的环境,与现有研究方法相比,该研究方法发起的欺骗攻击成功率更高。

1 相关工作

目前针对物联网已经提出较多欺骗攻击模型,在[16,17]文献中,作者全面地阐述了针对无线传感器网络的欺骗攻击以及检测技术。文献[18]提出了一种新颖的对抗性攻击框架,用于生成欺骗流量分类系统的恶意流量。在研究[19]中,对抗性发射-接收器对在生成对抗网络中扮演生成器和鉴别器的角色,在最小最大游戏中制造最佳的欺骗信号。此外,针对CTC的特殊性,WEI等^[20]提出了一种密钥建立协议(KEP),该协议探索并利用CTC独特的PN序列接收,不仅可以实现不同物理层之间的异构物联网设备的密钥建立,同时还可以提高通信的可靠性。

基于机器学习和深度神经网络技术引发的无线网络流量安全威胁对防御方案要求日益增强。例如,YANG等^[21]提出了一种基于神经网络的有效流量混淆方法,该方法使用神经网络混淆网络流量,有效抵御窃听或流量分析攻击。HAN等^[22]开发了一种基于深度强化学习神经网络DQN的跨技术干扰攻击防御算法,该算法利用LSTM学习CSI的长期依赖关系,预测干扰攻击可能的类型和强度。

CHEN等^[23]对异构物联网中使用的CTC技术进行了全面调查。现在普遍的是基于物理层级别

跨技术通信方法,即通过精心设计数据包,让发送方能够模拟出接收方所能解调的信号。如 WE-Bee^[24]在 WiFi 的物理层限制之下,利用精心构造的数据包,让该数据单元在经过物理层之后,产生的 WiFi 信号中的一部分与 ZigBee 信号近似,从而可以被 ZigBee 设备直接解调;WiBeacon^[25]采用了不同的设计方法,采用基于互补码键控的 CTC 技术,它观察到互补码键控的每个正交相移键控码片在特定样本处产生一个正交相位,因此,通过随时间操纵正交相移键控码片(即相位)可以创建完全模拟 BLE 芯片的相位变化。NNCTC^[26]通过可解释神经网络实现物理层跨技术通信的框架,将无线通信物理层的相关知识融入神经网络中。XiTuX^[27]利用神经网络填补了跨技术通信的空白,实现了 WiFi 到任意设备的通信。

JamCloak^[28]实现了一种反应式干扰系统,它可以攻击大多数现有的 CTC 协议,显著降低数据传输效率。Wi-attack^[29]使用 WiFi 设备对蓝牙定位服务进行冒充攻击,Wi-attack 不受蓝牙广播间隔的限制,能够同时冒充多个蓝牙数据帧,实现对蓝牙定位服务的高效攻击。在先前的工作中^[30],使用 WiFi 设备有效地攻击 ZigBee 设备,显著降低了网络性能,在此工作基础之上,使用元强化学习发起欺骗攻击,旨在实现更高的攻击成功概率。

2 时隙模型

2.1 WiFi 和 ZigBee 设备的时隙模型

在无线传感器网络中,为降低能耗和减少信号干扰,通常采用较低占空比并将工作时间按照时隙划分(Time slots)。时隙模型将节点的周期性工作时间长度定义为 t 。其次,对于每一个工作时间表,将其分割成一系列长度为 τ 的时间片段, τ 是一个活动所需的工作时间单位。时隙持续时间 τ 等于传输最大 MAC 帧长度所需时间的一半,图 1 展示了 WiFi 和 ZigBee 设备的时隙情况。

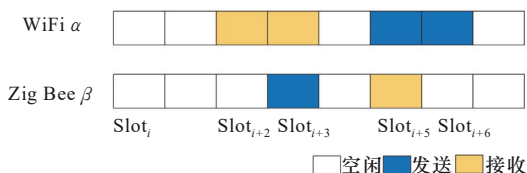


图 1 WiFi 和 ZigBee 设备的时隙

Fig.1 Time slots for WiFi and ZigBee devices

在无线传感器网络中,采用调节能耗的占空比设备只能处于两种状态:活跃状态和休眠状态。在

活跃状态下,设备能够进行数据包的发送或接收,而在休眠状态下,设备关闭了除唤醒定时器外的所有模块,所有设备都需要根据任务需求或预先安排的情况定期在活跃状态和休眠状态之间切换。在同步 MAC 协议中,每个传感器都存储其他传感器的工作时间表,并在建立通信路径之前加入邻居节点的工作时间表。因此,对于传感器设备而言,其工作时间表状态相对稳定,与欺骗攻击的基础思想一致,即基于过去时隙观察预测未来时隙中的最佳操作。

WiFi 和 ZigBee 使用相同的时隙模型,并且具有相同的时隙持续时间。这个具有相同时隙持续时间的时隙模型,简单且有效,可以将可用通信时间分割成不同的时间间隔或时隙。WiFi 和 ZigBee 都采用了这种模型进行数据传输,使得多个设备能够共享同一通信频道而不产生任何干扰。WiFi 和 ZigBee 的不同数据传输速率和占空比并不妨碍它们利用相同的时隙模型。时隙模型使得具有不同数据传输速率和占空比的设备能够在同一通道上共存而不会产生任何干扰。

2.2 WiFi 对 ZigBee 设备的欺骗攻击

ZigBee 网络由于功耗限制,节点通常传输距离较短并以低占空比工作形成自组网。网络中节点以多跳形式进行数据中继并传输到远程基站,网络拓扑图如图 2 所示。根据跨技术通信特点,当 WiFi 设备距离 ZigBee 网络较近时,既然 WiFi 可以直接与 ZigBee 节点通信,WiFi 设备能够有效地仅捕获在 ZigBee 频段内运行的 ZigBee 的信号,这使得 WiFi 可以侦听 ZigBee 节点数据,以及 ZigBee 网络节点数据传输规律。

WiFi 设备分析接收到的 ZigBee 节点数据以及 ZigBee 网络节点数据传输规律,使得 WiFi 设备可以伪装成 ZigBee 节点参与 ZigBee 网络的通信中,从而对其他 ZigBee 设备进行欺骗攻击。WiFi 对攻击的 ZigBee 节点信息掌握得越多,欺骗攻击的成功率越高。

从图 2 中可以看出,WiFi 对 ZigBee 欺骗攻击流程为:WiFi α 设备作为攻击者,在每个时间段内能够执行三种不同的操作:休眠、接收、欺骗(发送)。当 WiFi α 设备接收到模仿 ZigBee 设备进行欺骗攻击指令时,它首先转移到接收模式,并立即尝试捕获 ZigBee 信号。随后,WiFi 设备利用捕获到的数据来预测在随后时间段中采取最佳行动的时刻。最后,WiFi α 转换到发送状态并广播欺骗攻击信号,如果

WiFi设备预计即将到来的 ZigBee 设备时间段将是接收时间段,则在该时间段内采取伪造行动,发送伪造信号。否则, WiFi 设备转换接收状态,尽可能捕获 ZigBee 信号,或保持休眠状态以节省能量。此外,处理捕获的信号并进行预测需要时间,攻击者无法立即获取实际状态并在下一个时隙的开始时进行正确的预测,因此需要在信道检测时隙和预测之间添加一个时隙的间隔。

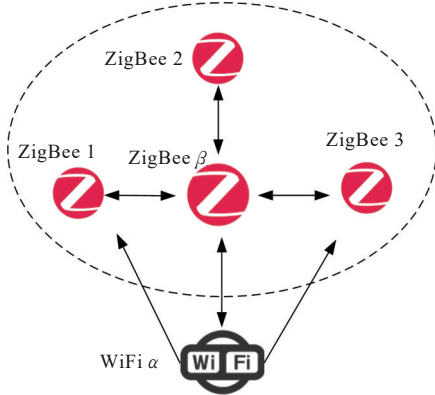


图2 WiFi对ZigBee设备的欺骗攻击示意图

Fig.2 Schematic diagram of WiFi spoofing attack on ZigBee devices

预测过程如图3所示,在第 Slot_{i+4} 个时隙中, WiFi α 首先处理 Slot_{i+2} 和 Slot_{i+3} 个时隙中捕获的信息。然后利用第 Slot_{i+4} 之前监视到的信道状态来预测在第 Slot_{i+5} 和 Slot_{i+6} 个时隙中应该采取的最佳行动。

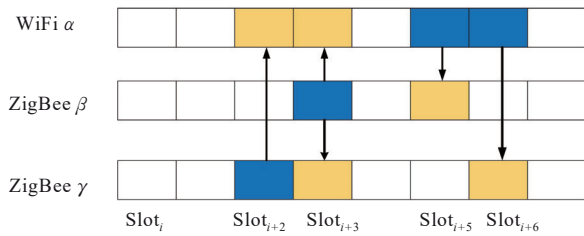


图3 WiFi α 尝试捕获 ZigBee 信号并发起欺骗攻击

Fig.3 WiFi α attempts to capture ZigBee signals and launches spoofing attacks

3 AMRL 模型

3.1 AMRL 网络架构

生成性对抗样本元强化学习 AMRL (Adversarial Generative Sample Meta-Reinforcement Learning, AMRL) 欺骗攻击模型,采用模型不可知元学习 (Model-Agnostic Meta-Learning, MAML), 利用生成对抗网络 (Generative Adversarial Network, GAN) 产生对抗样本进行训练。同时利用 GAN 来

生成样本噪声,模拟无线网络传输中的数据流,提升模型的鲁棒性。AMRL 的网络架构如图4所示。

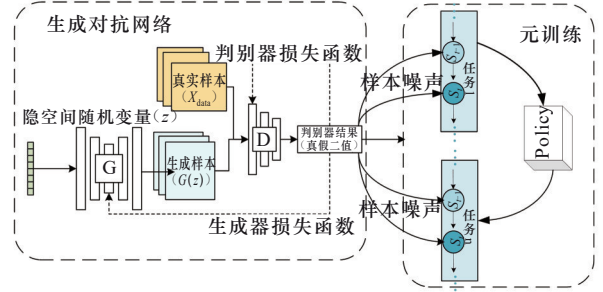


图4 AMRL 网络框架

Fig.4 AMRL network framework

图4中, AMRL 由两个主要部分组成。(i) 对抗性训练, 包含生成器、判别器和强化学习模型。生成器用于生成判别器无法准确区分的对抗样本, 判别器用于判别样本的真实性。(ii) 协同损失函数, 让判别器与元强化学习中智能体 (Agent) 相互协作, 分配合适的权重, 使模型更好地进行无线网络流量分析。

在训练过程中, MAML 利用前期获取的 ZigBee 网络数据流作为任务 T_{Pre} 的样本进行模型训练, 生成攻击模型, 该模型可以用于新的网络数据流预测任务。该方法假设先前任务 T_{Pre} 和新任务都按照同一任务分布 $p(T)$ 进行采样, 在元强化学习的场景中, MAML 通过建立函数 f_{θ} , 其中元强化学习参数为 θ , 将损失函数 L_T 最小化。MAML 的学习过程表示为 $\theta' = u_{\varphi}(D_T^{\text{tr}})$, 因此, MAML 整体损失函数为:

$$\begin{aligned} \min_{\theta, \varphi} E_{T \sim p(T)} [L(D_T^{\text{test}}, \theta')] \\ \text{s.t. } \theta' = u_{\varphi}(D_T^{\text{tr}}, \theta) \end{aligned} \quad (1)$$

其中 D_T^{tr} 和 D_T^{test} 表示分别表示任务 T 对应的训练集和测试集。 $E_{T \sim p(T)}$ 表示任务 T 的期望值, $\theta' = u_{\varphi}(D_T^{\text{tr}})$ 表示更新后的参数, 该函数依赖于训练数据 D_T^{tr} 和参数 φ 。MAML 采用梯度下降法, 能够在一次或多次梯度下降后获得一个能适应新任务的有效初始参数:

$$u_{\varphi}(D_T^{\text{tr}}, \theta) = \theta - \alpha \nabla_{\theta} L(D_T^{\text{tr}}, \theta). \quad (2)$$

$\nabla_{\theta} L$ 表示函数 L 对参数 θ 的梯度, α 表示学习率, 是控制参数更新步长的超参数, D_T^{tr} 表示训练数据。

3.2 对抗性训练

在一般的强化学习中, 任务 T_i 被描述为马尔可夫决策过程, 其中决策的步数为 H , 包含一个初始概率分布 $q_i(x_1)$ 和转移概率分布 $q_i(x_{i+1}|x_i, a_i)$, 损失函数 L_{T_i} 对应于奖励函数 R 。而在 AMRL 设计 (见算法 1)

算法 1:生成对抗样本元强化学习(AMRL)

```

1. 随机初始化网络参数  $\theta$  和生成对抗网络参数  $\varphi$ 
2. while 执行 do
3. 任务  $T_i \sim p(T)$ 
4. for 所有  $T_i$  do
5. 根据当前任务,使用生成对抗网络生成对抗样本
6. 更新数据集  $D = \{(\widetilde{x}_1, a_1, \dots, \widetilde{x}_H)\}$ , 其中  $\widetilde{x}_i$  由生成器生成
7. 使用公式(3)计算  $\nabla_{\theta} L_{T_i}(f_{\theta})$  数值
8. 使用式(1)计算梯度下降的自适应参数
9. 更新数据集  $D' = \{(\widetilde{x}'_1, a'_1, \dots, \widetilde{x}'_H)\}$ , 其中  $\widetilde{x}'_1$  为判别器无法辨别的对抗样本
10. end for
11. 更新参数  $\theta$ 
12. 自适应更新对抗网络参数  $\varphi$ 
13. end while

```

中,元强化学习从任务 $p(T)$ 中采样多个任务样本,并针对每个任务执行以下步骤:1)状态到动作的映射 f_{θ} :元强化学习在每个时间步 $t \in \{1, 2, \dots, H\}$ 中,将状态 x_t 映射到动作 a_t ;2)计算损失函数 L_{T_i} :任务 T_i 的损失函数与奖励函数 R 相关,损失函数被定义为负的累计奖励。任务 T_i 的损失函数表示为:

$$L_{T_i}(f_{\theta}) = -E_{x_t, a_t \sim f_{\theta}, q_{T_i}} \left[\sum_{t=1}^H R_t(x_t, a_t) \right]. \quad (3)$$

通过 GAN 网络生成任务 T_i 的对抗样本,该网络由三个部分组成:生成器 G 、判别器 D 和强化学习模型 RL。GAN 中生成器 G 将噪声 z'_i 和类别标签 y'_i 作为输入,以 $G(z'_i, y'_i)$ 为输出,在此过程中,生成器 G 会逐渐生成并拟合出类别标签为 y'_i 的潜在虚假数据。然后,将这些生成的对抗数据与原始数据混合,通过判别器进行判断。GAN 中判别器 D 主要为对抗判别器,用于判别真实数据和生成的虚假数据,真实数据通过数据集来选择,而虚假数据是由 G 生成的。在对抗性训练性场景中,GAN 生成对抗性样本并扰动正常状态 X_t 到 $\widetilde{X}_t$ 。在 AMRL 模型中使用 GAN 的目的是生成对抗攻击,从而显著提高元强化学习(MRL)模型的鲁棒性。GAN 的关键是破坏强化学习中的每个当前状态,诱使 Agent 相信它处于正确的状态,但实际上会导致 Agent 在每一步中做出次优选择,并进一步降低奖励。在训练的交互过程中,GAN 会生成对抗性样本并误导 Agent 降低总奖励。

3.3 协同损失函数

为了解决训练过程中的样本不均衡问题,创建协同损失函数 L ,函数 L 表示为:

$$L = L_{adv'} + \alpha L_{GAN} + \beta L_{hinge}. \quad (4)$$

其中, $L_{adv'}$ 表示误导智能体(Agent)损失函数, $L_{adv'}$ =

$-L_{T_i}(f_{\theta'})(T_i \in D_i')$, L_{GAN} 表示对抗损失函数, $L_{GAN} = E_x \log D(x) + E_x \log(1 - D(x + G(x)))$, L_{hinge} 为约束函数, $L_{hinge} = E_x \max(0, \|G(x)_2 - c\|)$ 。

AMRL 使用一般强化学习的损失函数的负数, $L_{adv'}$ 鼓励生成器生成降低智能体性能的样本,欺骗智能体在当前状态下采取不正确的行动,最终减少总奖励。 L_{GAN} 中鉴别器 $D(x)$ 旨在区分真实样本 x 和由生成器 $G(x)$ 生成的“假”样本,最终生成与原始样本分布相同的样本。函数 L_{GAN} 经过生成器和判别器的制衡过程,整个网络最终达到纳什均衡。函数 L_{hinge} 主要作用为约束和限制扰动的变化范围,避免样本与原始样本差距太大。通过优化 L_{GAN} 函数,可以获得与真实样本具有相同分布的对抗样本。通过优化 $L_{adv'}$ 函数避免系统性能下降。模型扰动的尺度受到 L_{hinge} 函数约束。动态调制因子 α 和 β , 可以控制每个子目标函数的相对重要性。

4 实验结果与分析

4.1 实验设置

本文构建 Matlab 模拟器来模拟真实的无线网络, WiFi 网络和 ZigBee 网络共存于一个 8 m × 10 m 的房间中,随机选择 AP、协调器、WiFi 和 ZigBee 设备位置。WiFi 使用 802.11b/g 协议,设置 MAC 帧平均长度为 1 190 字节, WiFi 的传输速率为 54 Mb/s, 一个 MAC 帧的平均传输时间为 388 μ s。使用 MATLAB 模拟 ZigBee 设备的物理层。ZigBee 网络中所有 MAC 帧设置最大长度为 127 字节。模拟的 ZigBee 网络设置信标启用,并且采用分时 CS-MA/CA 访问信道。

实验场景如图 5 所示, USRP B210 平台来充当攻击方,使用 ZigBee 设备(CC 2650)作为被攻击方。USRP B210 设备产生 WiFi 信号,通过采用跨技术通信, WiFi 信号被用来模拟 ZigBee 信号,发射向 ZigBee 设备传输数据。因此, USRP B210 被伪装成 ZigBee 设备,对 ZigBee 网络中的设备进行信号欺骗。

AMRL 通过 Python 编程语言进行实验仿真,模型运行在 Intel Core i7-10875H 2.3 GHz CPU,内存 8 GB 的商用个人计算机上,虚拟环境采用框架 Tensorflow 2.4。提出的对抗性元强化学习超参数设置如下: $\alpha=0.8$, $\beta=0.2$ 。

本研究中的数据包使用 CTC 技术进行编码。表 1 展示了实验中使用的模拟参数,包括传感器设

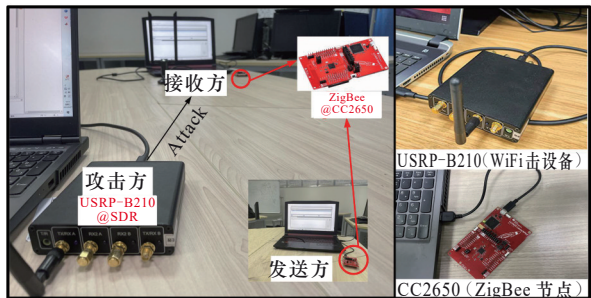


图 5 欺骗攻击实验场景
Fig.5 Spoofing attack experimental scenario

备工作能耗和单位数据传输能耗。其中 E_{elec} 表示传感器设备在发送或接收数据消耗的能量, ϵ_s 表示在自由传播模型中,传感器在发送每比特数据时,信号在每平方米上所消耗的能量, ϵ_{amp} 则表示传感器发送每比特数据时,信号每平方米的距离能耗。

4.2 性能分析

在初始配置下,AMRL 大约 3 100 个时隙(约 6.3 s)收敛,实现了 69.1% 的欺骗成功概率。跨技术通信技术存在一些固有的缺陷,所以仍然存在一些欺骗攻击失败的情况。

表 1 仿真参数

Table 1 Simulation parameters

参数名称	值
网络面积/ m^2	8×10
传感器节点数/个	10
信标大小/字节	25
$E_{elec}/(nJ \cdot bit^{-1})$	50
$\epsilon_s/(pJ \cdot bit^{-1} \cdot m^{-3})$	10
$\epsilon_{amp}/(pJ \cdot bit^{-1} \cdot m^{-3})$	0.001 3
ZigBee 传输距离/m	50
WiFi 传输距离/m	300
MAC 协议	BoX-MAC ^[31]

在 WiFi 到 ZigBee 的跨技术通信的实现中存在信号仿真误差^[32],一方面,误差来自 WiFi 循环前缀(CP),这是一种消除符号间干扰(ISI)的技术,即每个 WiFi symbol 中会有持续 0.8 μs 的保护间隔从 WiFi 的右侧复制并覆盖到 symbol 的左侧,这样一来, WiFi 信号的前端和后端是相同的,然而 ZigBee 的 I/Q 信号没有这样的重复。另一方面, ZigBee symbol 持续时间为 16 μs ,而 WiFi Symbol 持续时间为 4 μs ,因此需要将一个 ZigBee symbol 分割成 4 份分别进行仿真,这种分割将进一步加大仿真误差。这些都是信号仿真中无法控制的,这就使得 WiFi 设备发射的前导码不能完全被 ZigBee 设备识别,进一步导致欺骗攻击成功率降低。

具体实验分析如下。

4.2.1 不同欺骗攻击方法对比实验分析

为了更好地测试 AMRL 的性能,与传统的随机欺骗攻击、反应式欺骗攻击和使用一般强化学习(RL)欺骗攻击进行对比,基线超参数都选择最优。结果如图 6 所示,可以看到,一般强化学习算法欺骗成功的概率为 49.8%,反应式欺骗攻击的概率低于 30%,随机欺骗攻击的概率最低,成功概率不到 10%。此外,一般的强化学习算法需要更多的步数来收敛,这说明 AMRL 能够更快更高效地适应任务场景。

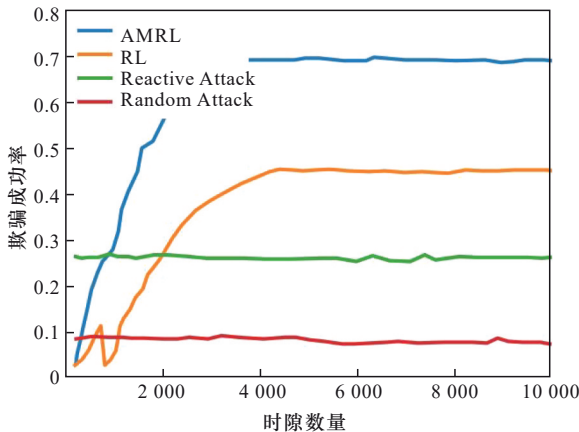


图 6 不同方法欺骗攻击成功率
Fig.6 Success rates of deception attacks by different methods

一般强化学习算法(RL)需要通过大量的探索来找到最佳的攻击策略,尤其是在复杂的网络环境中,RL 依赖于环境的反复交互来获取奖励反馈并调整策略,这意味着模型需要在大量的失败尝试中积累经验,从而导致其收敛速度较慢和成功率较低。随机欺骗攻击不依赖任何学习过程,它仅仅是通过随机生成攻击行为来试探,这意味着随机攻击无法根据环境反馈进行调整和优化,也无法在多次攻击中逐步提升攻击成功率。

图 7 显示的是 AMRL 和一般强化学习在不同发射功率下欺骗成功的概率,在低功率下,AMRL 欺骗攻击成功率要高于一般强化学习,这表明 AMRL 在低功率条件下已经能够利用其训练中积累的元任务经验,有更强的适应性和初始性能。此外 AMRL 在中高功率区间(-51 至 -30 dBm),表现出显著的快速提升。在所有功率区间内,AMRL 的欺骗成功概率显著高于一般强化学习。

4.2.2 节点数量影响分析

图 8 展示 ZigBee 网络中节点数量从 1 个增加至 10 个时, WiFi 欺骗 ZigBee 设备的成功概率。节点数量从 1 到 10 的平均欺骗成功率为: 51.1%、

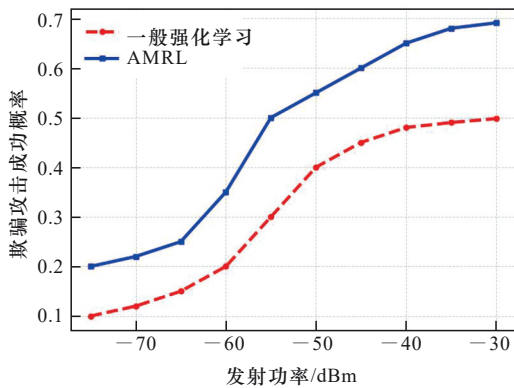


图7 不同发射功率下欺骗攻击成功率

Fig.7 Success rates of deception attack under different TX powers

55.2%、61.8%、58.6%、62.1%、59.1%、69.1%、65.2%、58.6%、52.1%。从图8中可以看出,WiFi攻击成功率均高于50%。当网络中节点数量较少时,ZigBee设备之间的通信频率较低,WiFi设备能够侦听到ZigBee设备通信的机会较少,从而降低了攻击的成功率,当网络中节点数量较多时,网络拥塞的可能性增大,这会导致执行欺骗攻击时,难以准确捕捉到目标设备的通信信号,降低了欺骗攻击成功率。当节点数为7时,攻击成功率最高,成功率将近70%。虽然存在一些欺骗失败的情况,但WiFi设备依靠稳定电源供应可以持续攻击,对ZigBee安全通信带来了极大的威胁。

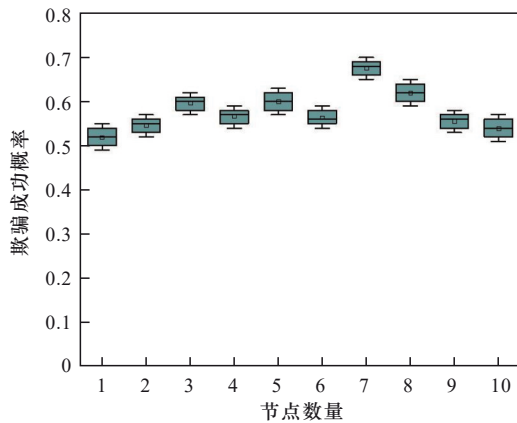


图8 不同节点数量欺骗攻击成功率

Fig.8 Success rates of deception attacks with different numbers of nodes

4.2.3 加噪对比实验分析

为了验证GAN生成的对抗样本对元智能体训练效果,使用随机噪声、DeepFool进行对比实验。首先,使用MAML训练一个元智能体,使用GAN生成对抗样本对元智能体进行攻击。在没有对抗样本攻击的情况下,AMRL的平均奖励为-12.41,接近MAML的平均奖励-12.24。同时,通过随机

噪声训练和DeepFool训练的能较差,分别为-13.34和-21.20。在有对抗样本攻击中,AMRL始终优于所有其他具有对抗性攻击的元学习方法,在元测试阶段注入对抗样本时,AMRL获得-45.72的总奖励,而MAML仅获得了-63.21的总奖励,随机噪声训练获得了-50.23的总奖励,DeepFool训练仅获得-80.21的总奖励。这表明了AMRL在对抗元训练过程中具有优越性。

4.2.4 不同任务场景性能分析

为了验证不同场景下AMRL的性能,图9给出了3个不同任务场景下的比较结果,分别使用HalfCheetah-Vel、Reacher和Ant数据集。HalfCheetah-

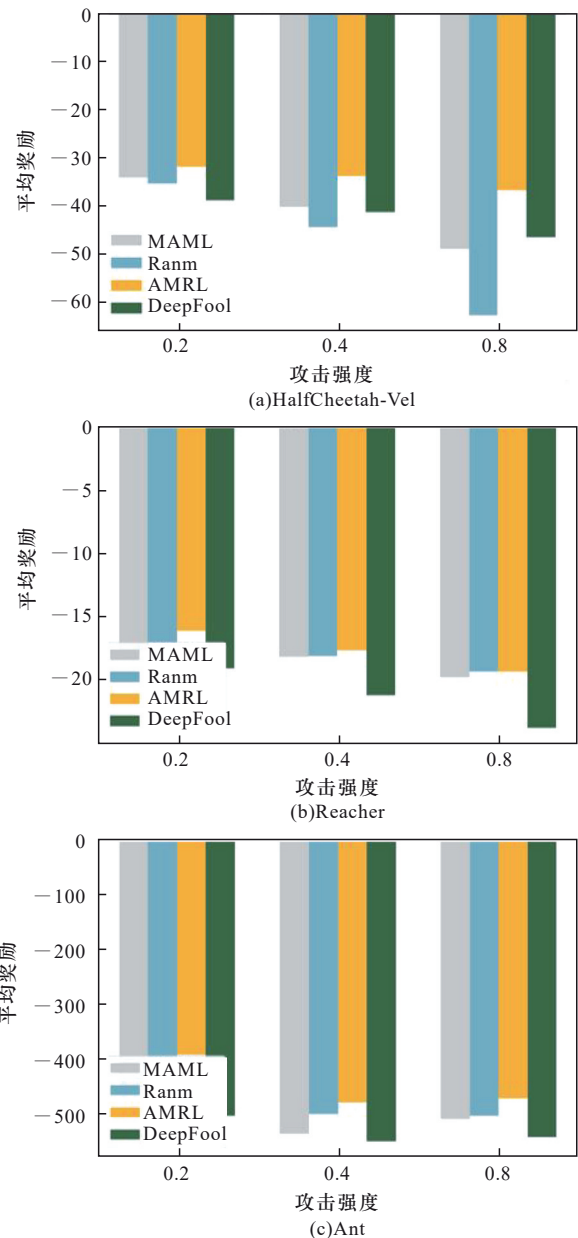


图9 三种环境下对抗性训练方法的比较

Fig.9 Comparison of adversarial training methods in three environments

Vel对应复杂物理环境中无线设备通信任务场景, Reacher和Ant对应多任务、多节点的任务场景。横坐标表示攻击强度(分别设置0.2、0.5和0.8三个等级的噪声级别),纵坐标显示元测试任务的平均奖励。结果显示,AMRL在各个场景中都优于其他方法,所有情况下都具有稳定且令人满意的性能,始终优于基线MAML。随机噪声和DeepFool方法的结果在不同的环境下差异很大,在不同的攻击下有相当大的变化范围,可能原因是这两种方法具有较大随机性。提出来的GAN训练具有自适应特性,总能够获得令人满意的结果。

AMRL在所有环境中具有快速的收敛性能。图10显示了平均奖励随epoch的增加而变化,其中总共设置了500个epoch,每50个epoch记录一次当前奖励。可以注意到,AMRL方法在HalfCheetah-Vel和Reacher场景中具有最佳的收敛性能。然而DeepFool方法在3个不同场景都表现出严重的低效率问题。由此,提出的方法在不同场景下具有良好的收敛性。

5 结束语

本文研究异构物联网中的安全问题,提出了一种欺骗攻击策略,将元强化学习和CTC技术相结合,利用WiFi传输功率较大和通信距离较远的优势,有效地欺骗ZigBee网络。首先,本文概述跨技术通信欺骗攻击的背景和理论,随后提出了针对WiFi和ZigBee设备共存网络设计的时隙模型,实现了以MAML为基础,使用生成对抗网络来生成强化学习的对抗样本的新方法AMRL。实验证明该方法相较于传统同构无线网络有效提升了ZigBee网络欺骗攻击的概率。

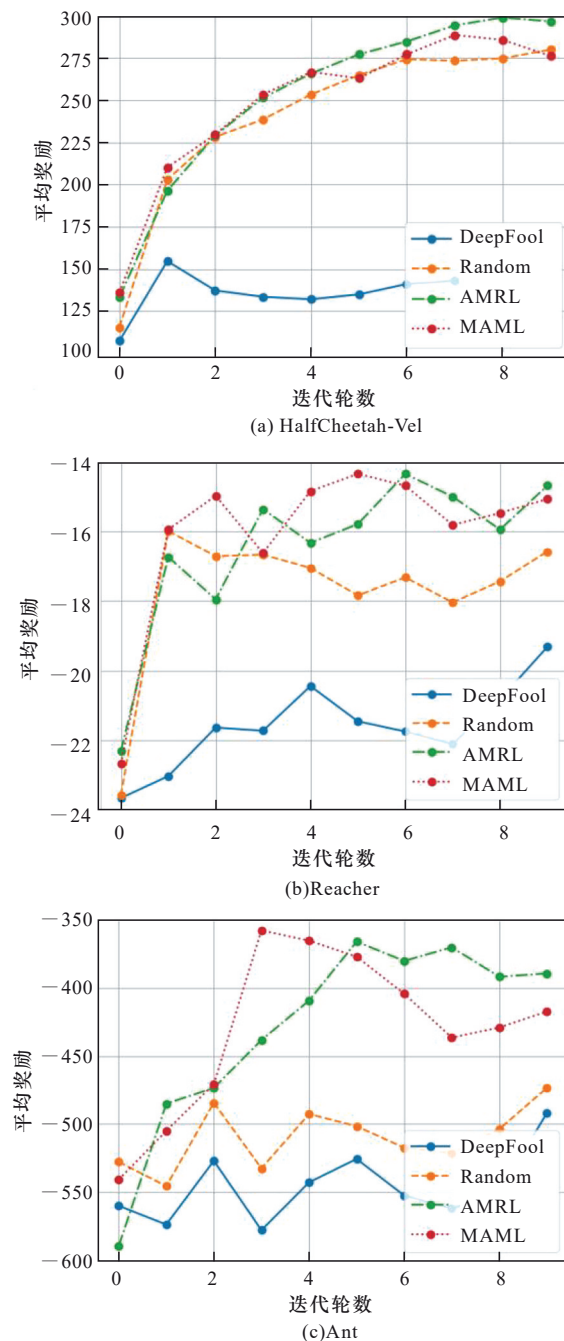


图10 三种场景下收敛性比较

Fig.10 Convergence comparison for three scenarios

参考文献:

- [1] ROCK L Y, TAJUDEEN F P, CHUNG Y W. Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective[J]. Universal Access in the Information Society, 2024, 23(1): 345-364.
- [2] ULLAH A, ANWAR S M, LI J, et al. Smart cities: the role of internet of things and machine learning in realizing a data-centric smart environment[J]. Complex & Intelligent Systems, 2024, 10(1): 1607-1637.
- [3] SERPANOS D. Industrial internet of things: trends and challenges[J]. Computer, 2024, 57(1): 124-128.
- [4] RIKEETH A. IoT in Agriculture 4.0: Farmer Adoption, Barriers, and the Path to Sustainable Farming[C]//2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE). Vellore, India: IEEE, 2024: 1-7.
- [5] AZMIN A, ABDULLAH S, FAIZA Z, et al. Fingerprint sensor integration in smart healthcare emergency app: Enhancing ambulance navigation through emergency route highlighting[C]//2024 20th IEEE International Colloquium on Signal Processing

- & amp. Langkawi, Malaysia; IEEE, 2024; 85–89.
- [6] BANSAL N, BHARDWAJ E. Internet of things for public safety[C]//2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). Bengaluru, India; IEEE, 2024; 150–156.
 - [7] WANG J, ZHU M, LI M, et al. An access control method against unauthorized and noncompliant behaviors of real-time data in industrial IoT[J]. IEEE Internet of Things Journal, 2024, 11(1): 708–727.
 - [8] KAIL E, BANATI A, LASZLO E, et al. Security survey of dedicated IoT networks in the unlicensed ISM bands[C]//2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara; IEEE, 2018; 000449–000454.
 - [9] MERWEJ R V D, ZUBIZARRETA X, LUKČINI, et al. Classification of spoofing attack types[C]//2018 European Navigation Conference (ENC). Gothenburg, Sweden; MDPI, 2018; 91–99.
 - [10] MAHAJAN M, BATRA S, MALHIS S, et al. A Flooding attack detection and mitigation technique in wireless sensor networks[C]//2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS). Madurai, India; IEEE, 2023; 1473–1478.
 - [11] SIVASAKTHI D A, SATHIYARAJ A, DEVENDIRAN R. HybridRobustNet: enhancing detection of hybrid attacks in IoT networks through advanced learning approach[J]. Cluster Computing, 2024; 1–15.
 - [12] ADIL M, MIDHA S, SRIVASTAV V K, et al. Detection and prevention of DoS Attack in VANET using artificial neural network[C]//2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC). Tandojam, Pakistan; IEEE, 2024; 1–7.
 - [13] REWIENSKI J, GROTH M, KULAS L, et al. Investigation of continuous wave jamming in an IEEE 802.15.4 network[C]//In Proceedings of International Microwave and Radar Conference (MIKON). Poznań, Poland; IEEE, 2018; 242–246.
 - [14] PRASAD S, THUENTE D J. Jamming attacks in 802.11g—a cognitive radio based approach[C]//In Proceedings of IEEE Military Communications Conference (MILCOM). Baltimore, Maryland, USA; IEEE, 2011; 1219–1224.
 - [15] KALGHATGI H, DHAWLE M, RAUT U. Defense techniques against spoofing attacks in wireless sensor networks[J]. Materials Today: Proceedings, 2023, 58; 123–131.
 - [16] YILMAZ M H, ARSLAN H. A survey: Spoofing attacks in physical layer security[C]//2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops). Clearwater Beach, FL; IEEE, 2015; 812–817.
 - [17] SHAHRIAR C, LA PAN M, LICHTMAN M, et al. PHY-layer resiliency in OFDM communications: A tutorial[J]. IEEE Communications Surveys & Tutorials, 2014, 17(1): 292–314.
 - [18] SUN P, LI S, XIE J, et al. GPMT: Generating practical malicious traffic based on adversarial attacks with little prior knowledge[J]. Computers & Security, 2023, 130; 103257.
 - [19] KOTAK J, ELOVICI Y. Adversarial attacks against IoT identification systems[J]. IEEE Internet of Things Journal, 2023, 10(9): 7868–7883.
 - [20] WEI W, LIU X, CHI Z C, et al. Key establishment for secure asymmetric cross-technology communication[C]//In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security. Singapore; Press ACM, 2024; 412–422.
 - [21] YANG F, WEN B, COMANICIU C, et al. TONet: A fast and efficient method for traffic obfuscation using adversarial machine learning[J]. IEEE Communications Letters, 2022, 26(11): 2537–2541.
 - [22] HAN D, LI A. Deep learning-guided jamming for cross-technology wireless networks: Attack and defense[J]. ACM Transactions on Networking, 2021, 29(5): 1922–1932.
 - [23] CHEN Y, LI M, CHEN P, et al. Survey of cross-technology communication for IoT heterogeneous devices[J]. IET Communications, 2019, 13(12): 1709–1720.
 - [24] LI Z, HE T. WEBee: Physical-layer cross-technology communication via emulation[C]//Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking. New York, USA; Association for Computing Machinery, 2017; 2–14.
 - [25] LIU R, YIN Z, JIANG W, et al. WiBeacon: Expanding BLE location-based services via wifi[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. New Orleans Louisiana; ACM, 2021; 83–96.
 - [26] WANG H, WANG J, JIANG W, et al. Physical layer cross-technology communication via explainable neural networks[J]. IEEE Transactions on Mobile Computing, 2025, 24(3): 1550–1566.
 - [27] LIAO S, PAN Q, LEI Y, et al. XiTuXi: Sealing the gaps in cross-technology communication by neural machine translation[C]//In Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems. New York, USA; SenSys ACM, 2023; 70–82.
 - [28] CHEN G, DONG W. JamCloak: Reactive jamming attack over cross-technology communication links[C]//2018 IEEE 26th International Conference on Network Protocols (ICNP). Cambridge; IEEE, 2018; 34–43.

-
- [29] NA X, GUO X, HE Y, et al. Wi-attack: Cross-technology impersonation attack against iBeacon services[C]//2021 18th Annual IEEE international conference on sensing, communication, and networking (SECON). Rome, Italy: IEEE, 2021: 1-9.
- [30] GAO D, WANG S, LIU Y, et al. Spoofing-jamming attack based on cross-technology communication for wireless networks[J]. Computer Communications, 2021, 177: 86-95.
- [31] CHENG T, LI S, JIAO F, et al. WibZig: Reliable and commodity-device compatible phy-etc via chip emulation in phase[C]//The 22nd International Conference on Information Processing in Sensor Networks. San Antonio TX USA: ACM, 2023: 191-204.

(编辑: 杨 鹏)