第12讲

第12讲：量子计算在自动驾驶中的应用

牛温佳 教授

北京交通大学 · 网络空间安全学院

本讲内容

1. 12.1 量子计算赋能自动驾驶
2. 12.2 3D深度欺骗攻击——针对单目深度估计的新型威胁
3. 12.3 量子增强的防御：QSNN防御框架
4. 思考题与小结

学习目标

了解量子计算在自动驾驶中的潜在应用场景

理解3D深度欺骗攻击的原理

认识量子技术提升自动驾驶安全性的多种路径

12.1 量子计算赋能自动驾驶

Section 12.1 量子计算赋能自动驾驶

12.1 量子计算赋能自动驾驶

量子计算在自动驾驶中的潜在应用涵盖多个方面：

12.1.1 路径规划优化

自动驾驶的路径规划本质上是一个组合优化问题——如何从A点到B点，在避开障碍物的同时，优化路径长度、时间和能耗。量子近似优化算法（QAOA）理论上可以在解决此类NP-hard问题时提供加速。

12.1.2 量子传感与定位

量子传感器利用量子效应（如量子纠缠）可以实现远超经典传感器的灵敏度。量子加速度计和量子陀螺仪可以在GPS信号失效时提供高精度的惯性导航。

12.1.3 量子增强感知

12.1 量子计算赋能自动驾驶（续）

量子成像技术可以在极端弱光条件下获取图像（如夜间驾驶、隧道场景），量子雷达（量子照明）在噪声环境中具有比传统雷达更好的目标检测性能。

12.2 3D深度欺骗攻击——针对单目深度估计的新型威胁

Section 12.2 3D深度欺骗攻击——针对单目深度估计的新型威胁

12.2 3D深度欺骗攻击——针对单目深度估计的新型威胁

12.2.1 背景：单目深度估计的脆弱性

自动驾驶的单目深度估计（MDE）系统虽然成本低、部署灵活，但近年来研究发现，这类模型在面对对抗攻击时表现出显著的脆弱性。攻击者可以通过在目标车辆表面施加特定的噪声或纹理，让MDE系统对目标车辆的深度感知产生巨大偏差——甚至让车辆在深度图中"消失"。

12.2.2 从2D补丁到3D全纹理攻击

早期的物理攻击采用**2D对抗补丁**——将设计好的对抗图案打印出来，贴在目标物体的局部表面。这种方法的局限性很明显：

- 只覆盖物体表面的一小部分

- 在视角变化时容易失效

- 对物理变形（如曲面、褶皱）敏感

新一代的攻击方法（如3D2Fool）将对抗纹理从"局部平面扰动"升级为"全表面三维伪装"，通过可微渲染技术建立从二维纹理到三维物理场景的梯度传播路径，生成可以覆盖整个车辆表面的对抗伪装纹理。

12.2.3 3D2Fool攻击的核心机制

3D2Fool包含两个关键的创新模块：

1. **纹理转换模块**：以一个二维对抗纹理种子为起点，通过旋转、平铺、随机裁剪等操作，生成不依赖于特定车型的通用对抗纹理，可以"包裹"在任意物体的表面。

12.2 3D深度欺骗攻击——针对单目深度估计的新型威胁（续）

2. **物理增广模块**：模拟现实世界中的光照变化、阴影、雨雾等环境干扰，确保生成的对抗纹理在各种天气和光照条件下都能保持攻击效果。

实验表明，这种全纹理攻击在多种MDE模型上均取得显著效果，平均深度估计误差超过10米，受影响区域超过40%。即使在雨雾天气下，攻击效果依然稳定。

12.3 量子增强的防御：QSNN防御框架

Section 12.3 量子增强的防御：QSNN防御框架

12.3 量子增强的防御：QSNN防御框架

12.3.1 为什么QSNN能防御3D攻击?

针对3D2Fool这类强物理攻击，传统防御手段普遍失效。而量子-脉冲混合神经网络（QSNN）的防御机制源自其底层的计算范式变革：

1. **脉冲阻断梯度**：SNN中LIF神经元的脉冲发放本质上是不可微的，切断了攻击者依赖的精确梯度回传路径。攻击者无法准确计算出如何调整对抗纹理来最大化模型误差。

2. **量子特征解耦**：参数化量子电路（PQC）将特征映射到高维希尔伯特空间，将"真实物体特征"与"对抗噪声特征"在空间中拉开距离。

3. **时序扰动衰减**：SNN膜电位的泄漏机制使对抗扰动在时间维度上自然衰减，无法像在ANN中那样无损传播。

12.3.2 防御效果的实验验证

12.3 量子增强的防御：QSNN防御框架（续）

消融实验（逐步移除QSNN的组件）清晰地揭示了各组件的贡献：

- **脉冲编码（SNN）** 是防御的主导组件，贡献了约90%的防御增益，从根本上重塑了模型的损失地貌，将攻击优化困在高损失平台上。

- **量子电路（PQC）** 提供了稳定的协同增益，进一步将目标区域的深度受损程度降低约16%。

两者分别作用于攻击优化流程的不同环节，构成"底层梯度阻断+高层特征空间扰乱"的双层防御体系。

延伸阅读

📖单目深度估计与对抗攻击相关论文（Monodepth2, RobustDepth等）

📖PennyLane量子机器学习: https://pennylane.ai/

思考题

1. 1. 为什么3D全纹理攻击比2D补丁攻击更难防御?

2. 2. QSNN在干净数据上的表现和受攻击时的表现之间存在权衡吗?

3. 3. 你认为量子计算在自动驾驶安全中还能发挥什么作用?

📌本讲小结

- ✓ 12.1 量子计算赋能自动驾驶
- ✓ 12.2 3D深度欺骗攻击——针对单目深度估计的新型威胁
- ✓ 12.3 量子增强的防御：QSNN防御框架
- ✓ 思考与讨论

感谢聆听

第12讲 · 量子计算在自动驾驶中的应用