量子类脑网络与智能汽车安全

第14讲

第14讲：案例分析——前沿技术落地

牛温佳 教授

北京交通大学 · 网络空间安全学院

本讲内容

学习目标

了解量子类脑计算在工业界的实际应用案例

通过案例分析加深对课程核心概念的理解

培养将理论知识与实际应用相结合的能力

14.1 案例分析一：宝马×英伟达的量子机器学习实践

Section 14.1 案例分析一：宝马×英伟达的量子机器学习实践

14.1 案例分析一：宝马×英伟达的量子机器学习实践

案例背景

2024年，宝马集团联合英伟达探索将量子机器学习用于汽车制造优化。他们利用英伟达的cuQuantum SDK，将量子线路模拟速度提升了300倍，将原本需要数小时的优化迭代缩短至分钟级。

关键启示

- 量子计算在工业优化问题上的潜力已经显现
- 经典-量子混合方案是目前最务实的路线
- 汽车行业正在积极探索量子技术

14.1 案例分析一：宝马×英伟达的量子机器学习实践（续）

讨论问题

量子计算在汽车行业还能在哪些环节发挥作用？生产制造？供应链优化？还是自动驾驶？

14.2 案例分析二：类脑芯片在自动驾驶中的探索

Section 14.2 案例分析二：类脑芯片在自动驾驶中的探索

14.2 案例分析二：类脑芯片在自动驾驶中的探索

案例背景

2024年，研究者开始将类脑芯片部署到自动驾驶的边缘计算平台上进行测试。相比传统GPU方案，类脑芯片在完成相同感知任务时功耗降低数十倍，响应延迟从数十毫秒降至微秒级别。

挑战

- 类脑芯片的通用性和灵活性不如GPU
- 现有的自动驾驶算法大多针对传统硬件优化
- 需要开发面向类脑芯片的新型算法

14.2 案例分析二：类脑芯片在自动驾驶中的探索（续）

讨论问题

对于L4/L5级自动驾驶，你认为类脑芯片是"替代方案"还是"补充方案"？

14.3 案例分析三：路牌对抗攻击事件

Section 14.3 案例分析三：路牌对抗攻击事件

14.3 案例分析三：路牌对抗攻击事件

案例背景

研究者展示了通过在停止路牌上粘贴特定图案的黑白贴纸，可以让特斯拉的自动驾驶系统将"STOP"标志识别为"限速45"标志。这一实验虽然仅在受控条件下进行，但引发了公众对自动驾驶安全性的广泛关注。

关键启示

- 对抗攻击不是理论威胁，而是有实际实施可能
- 物理世界攻击的关键挑战在于保持不同视角和环境下的稳定性
- 单一传感器的方案更容易受到攻击

14.3 案例分析三：路牌对抗攻击事件（续）

讨论问题

如果你是自动驾驶公司的安全主管，你会如何应对这类威胁？在技术之外，还需要什么样的保障措施？

14.4 案例分析四：QSNN防御框架

Section 14.4 案例分析四：QSNN防御框架

14.4 案例分析四：QSNN防御框架

研究背景

针对3D2Fool等强物理攻击，研究者提出了基于量子-脉冲混合神经网络（QSNN）的新型防御框架。该框架在干净数据上的性能与纯CNN相当，但在受到攻击时目标区域的深度信息保持度显著优于传统架构。

关键发现

1. 脉冲编码贡献了约90%的防御增益

2. 量子电路提供了额外的协同增益

3. 两者构成"底层梯度阻断+高层特征空间扰乱"的双层防御

14.4 案例分析四：QSNN防御框架（续）

4. 攻击能量从目标区域被驱散至背景区域

讨论问题

这一防御框架在未来实际部署中还面临哪些挑战？计算复杂度如何？能否实时运行在车载平台上？

14.5 案例分析五：中国量子计算与类脑计算产业布局

Section 14.5 案例分析五：中国量子计算与类脑计算产业布局

14.5 案例分析五：中国量子计算与类脑计算产业布局

国家战略

- "九章"系列光量子计算机：2023年发布"九章三号"，255光子
- 中国"脑科学与类脑研究"计划（2016年启动）
- 灵汐科技等类脑芯片企业快速成长
- 2025年神经形态芯片全球市场规模预计达70亿美元

产学研联动

14.5 案例分析五：中国量子计算与类脑计算产业布局（续）

- 清华大学"天机芯"（Nature封面论文）
- 浙江大学亿级神经元类脑计算机
- 多所高校开设类脑计算相关课程

讨论问题

在量子类脑计算这个赛道上，中国面临的机遇和挑战分别是什么？

延伸阅读

- 九章三号相关报道: 中国科学技术大学, 2023
- 宝马×英伟达量子计算合作: BMW Group Press, 2024

思考题

1. 1. 从以上案例中，你认为量子类脑计算在智能汽车安全领域最大的价值是什么？

2. 2. 技术从实验室走向产业化通常需要什么条件？量子类脑计算目前处于哪个阶段？

3. 3. 选择一个你感兴趣的案例，设想3-5年后的可能发展。

本讲小结

- ✓ 14.1 案例分析一：宝马×英伟达的量子机器学习实践
- ✓ 14.2 案例分析二：类脑芯片在自动驾驶中的探索
- ✓ 14.3 案例分析三：路牌对抗攻击事件
- ✓ 14.4 案例分析四：QSNN防御框架
- ✓ 14.5 案例分析五：中国量子计算与类脑计算产业布局
- ✓ 思考与讨论

感谢聆听

第14讲 · 案例分析——前沿技术落地