第13讲

第13讲：类脑计算在智能汽车安全中的应用

牛温佳 教授

北京交通大学 · 网络空间安全学院

本讲内容

学习目标

理解类脑计算在车载环境中的独特优势

了解脉冲神经网络在深度感知防御中的作用

认识多模态融合感知的发展方向

13.1 为什么汽车需要"大脑"一样高效的计算?

Section 13.1 为什么汽车需要"大脑"一样高效的计算?

13.1 为什么汽车需要"大脑"一样高效的计算?

13.1.1 车载计算的严苛要求

智能汽车的"大脑"需要在极其苛刻的条件下运行:

- **实时性**: 毫秒级的决策延迟可能决定生死
- **低功耗**: 算力系统不能显著消耗电动汽车的续航
- **可靠性**: 在任何天气、光照条件下都必须稳定工作
- **低成本**: 量产车需要控制硬件成本

13.1 为什么汽车需要"大脑"一样高效的计算？（续）

13.1.2 类脑计算的优势

类脑芯片相比传统GPU/CPU在车载场景中具有显著优势：

指标	传统GPU	类脑芯片
功耗	数百瓦	毫瓦级

13.1 为什么汽车需要"大脑"一样高效的计算？（续）

| 计算模式 | 连续密集计算 | 事件驱动稀疏计算 |

| 实时响应 | 受限于帧率 | 微秒级脉冲响应 |

| 物理体积 | 大 | 小 |

能效比提升2-3个数量级——这是类脑芯片最令人振奋的优势。

13.2 脉冲神经网络在防御中的独特作用

Section 13.2 脉冲神经网络在防御中的独特作用

13.2 脉冲神经网络在防御中的独特作用

13.2.1 脉冲编码如何对抗攻击?

SNN在防御对抗攻击方面具有三个天然优势:

1. 物理级去噪滤波器

LIF神经元具有严格的膜电位触发阈值。攻击产生的微小、精细的对抗扰动，在输入SNN后很难累积足够的电位来触发放电。这意味着SNN能够像天然的非线性滤波器一样，在编码早期直接"阻断"异常的高频噪声。

2. 梯度掩码效应

SNN的脉冲发放函数本质上不可微。这种离散特性从根本上切断了攻击者依赖的精确梯度回传路径，使得攻击者无法有效优化对抗纹理。

3. 时序冗余编码

SNN将空间信息展开到多个时间步中处理。对抗纹理所引入的扰动虽然能影响个别时间步的脉冲发放，但难以系统性地操控整个时序窗口内的脉冲统计分布——就像一颗石子扔进河里虽然激起水花，但无法改变河流的整体流向。

13.2.2 混合架构的协同效应

将SNN的脉冲编码与参数化量子电路结合，构建QSNN防御框架，两者产生协同防御效应：

- SNN在梯度传播层面设置离散化屏障（底层阻断）

13.2 脉冲神经网络在防御中的独特作用（续）

- PQC在特征空间层面引入高维非局域扰动（高层扰乱）
- 两者协同将攻击能量从目标区域"驱散"至背景区域

13.3 未来发展：多模态融合感知

Section 13.3 未来发展：多模态融合感知

13.3 未来发展：多模态融合感知

13.3.1 为什么需要多模态融合?

单一传感器都有其局限性:

- 摄像头在强光、夜间、雨雾中性能下降
- 激光雷达在雾霾、雪天中受限
- 雷达分辨率不足以区分物体类别

多传感器融合通过综合摄像头、激光雷达、毫米波雷达的数据，可以弥补各自的不足，提供更可靠的环境感知。

13.3.2 类脑多模态融合的潜力

类脑计算在融合多模态传感器数据方面具有独特优势：

- **时空同步**：脉冲编码天然可以对齐不同传感器的时间戳
- **事件驱动**：只在关键事件发生时进行计算，大幅降低功耗
- **稀疏表示**：脉冲的稀疏性有利于多模态数据的高效融合

13.3.3 挑战与展望

将量子类脑计算从单目深度估计推广到多模态融合感知系统、抵御跨模态或协同式物理对抗攻击，是一个极具工程价值的研究方向。

延伸阅读

📖SpikingJelly官方文档和教程: https://spikingjelly.readthedocs.io/

📖灵汐科技类脑计算平台相关资料

思考题

1. 1. 为什么说SNN的"不可微性"是防御的优势而非劣势?

2. 2. 如果一个攻击者同时欺骗了摄像头和激光雷达，防御系统应该怎么做?

3. 3. 类脑计算的低功耗特性在自动驾驶中除了感知还能在哪些方面发挥作用?

📌本讲小结

- ✓ 13.1 为什么汽车需要"大脑"一样高效的计算?
- ✓ 13.2 脉冲神经网络在防御中的独特作用
- ✓ 13.3 未来发展：多模态融合感知
- ✓ 思考与讨论

感谢聆听

第13讲 · 类脑计算在智能汽车安全中的应用