# 新研究提出针对虚假数据注入攻击的防御机制

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/18888.html



**新研究提出针对虚假数据注入攻击的防御机制**。近日，华东理工大学信息科学与工程学院教授杨文课题组提出一种针对虚假数据注入攻击的安全防御机制，相关成果以《一种抵御多传感器远程状态估计中欺骗攻击的安全编码机制》为题，发表于《IEEE信息取证与安全汇刊》。

随着数字化和信息化建设的推进，通讯网络开放导致信息安全问题日益突出。无线传感器网络的开放性给系统中各个节点带来通信效率提升的同时，也面临不法分子篡改数据和破坏系统的严峻挑战。


编码机制示意图 受访者供图

杨文课题组用伪随机数和线性变换的方式，对无线传感器采集的数据进行预先编码，能够有效阻止隐秘网络攻击者在不触发安全警报的前提下降低系统性能。引入伪随机数的目的是增加虚假数据和真实数据之间的差异性，而线性变换可防止攻击者根据截获的数据推断出编码参数。相比于传统的加密算法，该方法在算法复杂度和数据准确性等方面取得了显著改善。

该研究发现，利用多传感器对系统进行远程状态估计时，所提出的方案能够有效解决现有检测方法无法准确识别线性最优攻击的难题。此外，作者着重分析了编码机制在多个不同情况下的有效性。

研究表明，攻击者无论是在已经掌握伪随机数的统计特性的情况下，还是利用历史数据实施重放攻击的情况下，都无法在实施虚假数据注入攻击的过程中不被检测器发现。

研究人员还从攻击者的角度调查了编码参数能被推演的条件，揭示了伪随机数和攻击者推演的准确性之间的关系，为编码参数的设计和防御机制的完善提供了重要保障。（来源：中国科学报 张双虎 黄辛）

相关论文信息：https://doi.org/10.1109/TIFS.2022.3175617


作者：杨文等 来源：《IEEE信息取证与安全汇刊》