

李志东, 杨武, 王巍, 尚大鹏. 多源入侵检测警报的决策级融合模型[J]. 通信学报, 2011, (5): 121~128

## 多源入侵检测警报的决策级融合模型

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[李志东](#)

[杨武](#)

[王巍](#)

[尚大鹏](#)

摘要点击次数: 249

全文下载次数: 188

中文摘要:

为了大幅降低对训练样本的要求, 摒弃苛刻的约束条件, 提出了一种支持在线增量训练的警报融合模型。将初级警报向量映射为表决模式, 以缩小统计空间。通过训练统计出各种表决模式在正常或攻击流量下的条件概率分布, 依据统计特征的变化即时推断待检测流量的构成情况, 使用阈值约束法和贝叶斯推断做出融合决策。从而拓展了适用范围, 并且能较好地跟踪适应待检测流量, 仅需少量训练样本便可显著提升检测性能。

英文摘要:

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

[关闭](#)

版权所有: 通信学报

地址: 北京东城区广渠门内大街80号通正国际大厦6层602室 电话: 010-67110006-869/878/881 电子邮件: xuebao@ptpress.com.cn

技术支持: 北京勤云科技发展有限公司