

张玲<sup>1,2</sup>, 白中英<sup>1</sup>, 罗守山<sup>1,2</sup>, 谢康<sup>2,3</sup>, 崔冠宁<sup>1,2</sup>, 孙茂华<sup>1,2</sup>. 基于粗糙集和人工免疫的集成入侵检测模型[J]. 通信学报, 2013, (9): 166~176

## 基于粗糙集和人工免疫的集成入侵检测模型

### Integrated intrusion detection model based on rough set and artificial immune

投稿时间: 2013-04-20

DOI: 10.3969/j.issn.1000-436x.2013.09.020

中文关键词: [粗糙集](#) [人工免疫](#) [误用检测](#) [异常检测](#) [RSAI-IID模型](#)

英文关键词: [rough set](#) [artificial immune system](#) [misuse detection](#) [anomaly detection](#) [integrated intrusion detection model based on rough set and artificial immune](#)

基金项目: 国家自然科学基金资助项目 (61121061, 61161140320)

作者

单位

[张玲<sup>1,2</sup>](#), [白中英<sup>1</sup>](#), [罗守山<sup>1,2</sup>](#), [谢康<sup>2,3</sup>](#), [崔冠宁<sup>1,2</sup>](#), [孙茂华<sup>1,2</sup>](#)

[1. 北京邮电大学 信息安全中心, 北京 100876;](#) [2. 云安全北京工程实验室, 北京 100876;](#) [3. 山东大学 信息科学与工程学院, 山东 济南 250100](#)

摘要点击次数: 270

全文下载次数: 86

中文摘要:

针对当前入侵检测存在的问题, 通过引入粗糙集方法, 综合误用检测和异常检测设计了一种基于粗糙集和人工免疫的集成入侵检测 (RSAI-IID) 模型, 提出了一种在入侵检测中实现疫苗注入的方法。采用粗糙集方法获取疫苗, 并保证了疫苗的优良性, 优化检测性能; 误用检测筛掉已知的入侵行为, 提高检测的速度; 异常检测针对未知攻击进行实时检测。最后在KDD99数据集上进行实验仿真, 验证了模型的可行性和有效性。

英文摘要:

According to the problems of intrusion detection, an integrated intrusion detection model based on rough set and artificial immune (RSAI-IID) was proposed by using rough set and integrating misuse detection and anomaly detection. The rough set method was used to achieve the vaccine which was injected in the model, to get better vaccine, and to optimum the performances of detection; misuse detection was used to get off the known intrusions; anomaly detection was used to detect the novel intrusions. RSAI-IID model was validated on KDD 99 dataset. The experimental results show its feasibility and effectiveness.

[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: 北京市丰台区成寿寺路11号邮电出版大厦8层 电话: 010-81055478, 81055479

81055480, 81055482 电子邮件: [xuebao@ptpress.com.cn](mailto:xuebao@ptpress.com.cn)

技术支持: 北京勤云科技发展有限公司