网络安全数据可视化融合的分析方法

张　杰，傅文博

（山西大同大学 计算机与网络工程学院，山西 大同 037009）

摘　要：文章提出一种基于时间序列的网络安全数据可视化融合分析方法，利用网络数据之间的关联性进行特征选择和一致性过滤，保留原始特征的同时消除冗余特征；通过网络数据特征之间的信息熵计算，利用 INTERACT 方法实现归一化处理；通过时间序列分析法对处理后的网络数据进行可视化融合分析，利用切比雪夫法对网络数据包进行验证，判断是否存在入侵行为，实现网络安全数据的可视化融合.实验结果表明，通过对检测阈值的调控能够提高检测率，随着数据规模的不断扩大，所提方法的检测率较为平稳，且误报率相比其他方法更低.

关键词：网络；安全数据；可视化融合；分析

Analysis method of visual fusion of network security data

ZHANG Jie,FU Wen-bo

(School of Computer and Network Engineering,Shanxi Datong University,Datong 037009,China)

Abstract：In this paper a visual fusion analysis method for network security data based on time series is proposed. The correlation between network data is used for feature selection and consistency filtering. The original features are preserved while the redundant features are eliminated. The information entropy between network data features is proposed. Calculation, using the INTERACT method to achieve normalization processing; through the time series analysis method for visual fusion analysis of the processed network data, using the Chebyshev method to verify the network packets to determine whether there is intrusion behavior, to achieve network security data Visual fusion. The experimental results show that the detection rate can be improved by regulating the detection threshold. With the continuous expansion of data size, the detection rate of the proposed method is relatively stable, and the false alarm rate is lower than other methods.

Key words：The internet；safety data；visual fusion；analysis

作者简介：

张　杰　男，（1979-），硕士研究生，讲师.研究方向为网络安全、物联网.

E-mail:ss356398632@163.com

傅文博　男，（1976-），硕士，副教授.研究方向为网络安全，物联网.