计算机工程与应用 2010 46 (3): 20-22 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

有监督S-kv-Isomap在入侵检测中的应用

郑凯梅[1，2]，钱 旭[1]

1.中国矿业大学 机电与信息工程学院，北京 100083
2.中国防卫科技学院 信息工程系，北京 101601

收稿日期 2009-10-14 修回日期 2009-12-13 网络版发布日期 2010-1-28 接受日期

摘要 入侵检测是计算机安全研究方面的热点领域，在入侵检测数据可视化和分类方面面临的问题是其高维特性。流形学习算法Isomap是有效的非线性降维工具。但是Isomap算法在实际应用中存在不能保证构造连通的邻接图和没有利用样本已知类别标记的缺点，针对上述缺陷提出了健壮的有监督S-kv-Isomap算法。该算法利用类别标记来指导降维，并且利用k-variable算法构造联通的邻接图。实验选用KDDCUP1999数据集，对四类入侵数据即Dos、R2L、Probe、U2R进行了可视化和分类研究。可视化中比较了S-kv-Isomap算法与kv-Isomap算法，前者具有更好的可视化效果。在分类研究中比较了S-kv-Isomap、kv-Isomap、SVM和k-NN算法，实验结果表明，S-kv-Isomap方法在入侵检测中不仅保持较高的入侵检测率，而且误警率很低。

关键词 有监督学习 维数约简 流形学习 Isomap 可视化 分类 入侵检测

分类号 TP393

Intrusion detection based on supervised S-kv-Isomap algorithm

ZHENG Kai-mei[1，2]，QIAN Xu[1]

1.School of Mechanical Electronic & Information Engineering，China University of Mining & Technology Beijing，Beijing 100083，China
2.Information Engineering Department，China Institute of Defense Science and Technology，Beijing 101601，China

Abstract

Intrusion detection is still a hot area in computer security.When performing visualization and classification，the problem should be confronted is the high dimensionality.As one of the manifold learning algorithms Isomap is an effective nonlinear dimension reduction tool.However，when Isomap is applied to the real-world data，it shows some limitations，such as failing to guarantee connectedness of the constructed neighborhood graphs and not using the class labels of the data.An improved version of Isomap，namely S-kv-Isomap，is proposed.S-kv-Isomap utilizes class information to guide the dimension reduction procedure and k-variable method to build connected neighborhood graphs so as to enhance the robustness.The new scheme is evaluated with KDD CUP 1999 datasets in visualization and classification on four kinds of intrusion types： Dos，R2L，Probe，and U2R.Experiment results show that S-kv-Isomap performs best compared with kv-Isomap in visualization.In the classification test，S-kv-Isomap is compared with kv-Isomap，SVM，and k-NN.The results show that S-kv-Isomap performs higher detection rate and very low false positive rate.

Key words supervised learning dimension reduction manifold learning Isomap visualization classification intrusion detection

DOI: 10.3778/j.issn.1002-8331.2010.03.006

通讯作者 郑凯梅 zhengkaimei@126.com