系统工程与电子技术 2012, 34(3) 625-630 DOI: 10.3969/j.issn.1001-506X.2012.03.36 ISSN: 1001-506X CN: 11-2422/TN

软件、算法与仿真

基于SSC-tree流聚类的入侵检测算法

程春玲[1,2,3]，余志虎[1]，张登银[1,3]，徐小龙[1,2]

1. 南京邮电大学计算机学院， 江苏 南京 210003；
2. 江苏省无线传感网高技术研究重点实验室， 江苏 南京 210003;
3. 宽带无线通信与传感网技术教育部重点实验室， 江苏 南京 210003

摘要：

由于数据流具有快速、无限、突发等特性，实现高速网络下的实时入侵检测已成为一个难题。设计一种维持数据流概要特征的相似搜索聚类树(similarity search cluster-tree, SSC-tree)结构，在此基础上提出一种基于SSC-tree的流聚类算法用于高速网络的入侵检测。为适应高速、突发到达的数据流，算法采用了链式缓存、捎带处理和局部聚类策略。SSC-tree中的链式缓存区用于临时存放数据流突发时算法不能及时处理的数据对象，缓冲区中的内容随后被捎带处理。在高速数据流未插入SSC-tree参与全局聚类之前，利用局部聚类产生微簇来适应高速流的到达。实验结果表明，该算法具有良好的适用性，能够在高速网络环境下产生较好的聚类精度，有效实现高速网络环境下的入侵检测。

关键词： 入侵检测；聚类；数据流；高速网络

Intrusion detection algorithm based on SSC-tree stream clustering

CHENG Chun-ling[1,2,3], YU Zhi-hu[1], ZHANG Deng-yin[1,3], XU Xiao-long[1,2]

1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3. Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education Jiangsu Province, Nanjing 210003, China

Abstract:

As data streams show the fast, unlimited and bursting characteristics, real-time intrusion detection in high-speed networks becomes a problem. A similarity search cluster-tree (SSC-tree) is designed to maintain the summary feature of data streams and a clustering algorithm based on the SSC-tree is proposed to detect intrusion in high speed networks. In order to process high speed and bursting streams in time, chaining buffer, piggyback and local cluster mechanisms are used. The chaining buffer in SSC-tree is used to store temporary data stream objects which are piggybacked later to solve the problem that high-speed streams cannot be clustered in time when the bursting data streams arrive. Besides, in order to meet the arrival of high-speed stream, the algorithm introduces a local cluster mechanism, which is the process of pre clustering to produce local micro-clusters before data stream objects are inserted in the SSC-tree. The experiment results show that the proposed algorithm has good applicability and high clustering accuracy in high-speed networks. It can detect the intrusion in high-speed networks effectively.

Keywords: intrusion detection; cluster; data streams; high speed network

收稿日期 修回日期 网络版发布日期

DOI: 10.3969/j.issn.1001-506X.2012.03.36

基金项目:

通讯作者:

作者简介:

作者Email:

参考文献：

本刊中的类似文章