通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

杨宏宇,常 媛.基于K均值多重主成分分析的App-DDoS检测方法[J].通信学报,2014,(5):16~24

基于K均值多重主成分分析的App-DDoS检测方法

App-DDoS detection method based on K-meansmultiple principal component analysis

投稿时间： 2013-08-24

DOI：10.3969/j.issn.1000-436x.2014.5.003

中文关键词：应用层 网络攻击 主成分分析 均值聚类 日志

英文关键词:application layer network attack principal component analysis means clustering log

基金项目:国家科技重大专项基金资助项目(2012ZX03002002)；国家自然科学基金资助项目(60776807, 61179045)；国家高技术研究发展计划（“863”计划）重点基金资助项目(2006AA12A106)；天津市科技计划重点基金资助项目(09JCZDJC16800)；中国民航科技基金资助项目(MHRD201009, MHRD201205)

作者	单位
杨宏宇，常 媛	中国民航大学 计算机科学与技术学院，天津 300300

中文摘要:

针对应用层分布式拒绝服务攻击，利用Web日志的数据挖掘方法提出一种K均值多重主成分分析算法和基于该算法的App-DDoS检测方法。首先，通过分析正常用户和攻击者的访问行为区别，给出提取统计属性特征的方法；其次，根据主成分分析法的数据降维特性并利用最大距离划分法，提出一种K均值多重主成分分析算法，构建基于该算法的检测模型。最后，采用CTI-DATA数据集及模拟攻击获取的数据集，进行与模糊综合评判、隐半马尔科夫模型、D-S证据理论3种检测方法的App-DDoS攻击检测对比实验，实验结果证明 KMPCAA检测算法具有较好的检测性能。

英文摘要:

Aiming at the application layer distributed deny of service(App-DDoS) attacks, a K-means multiple principal component analysis algorithm(KMPCAA) utilizing the Web log mining was proposed, then an App-DDoS detection method based on KMPCAA was presented. Firstly, a statistical properties feature extracting method was designed by analyzing the difference between normal users’ and attackers’ access behavior. Secondly, a k-means multiple principal component analysis algorithm was proposed by using the maximum distance classification method according to the data dimension reduction property of the principal component analysis, and then the testing model based on the algorithm was established. Finally, an App-DDoS attack detection experiment on the CTI-DATA dataset and the simulated attack dataset was conducted. In this experiment, the proposed method was compared with the fuzzy synthetical evaluation (FSE) algorithm, the hidden semi-Markov model (HsMM) detection algorithm and the dempster-shafer evidence theory (D-S) algorithm. Experimental results demonstrate that the KMPCAA detection algorithm has better detection performance.

查看全文 查看/发表评论 下载PDF阅读器

关闭