第41卷第10期 中国科学技术大学学报 Vol. 41, No. 10
2011年10月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Oct. 2011

文章编号:0253-2778(2011)10-0915-09

一种基于多元异常分析的网络自主防护机制

谢丽霞,代其魁,杨宏宇

(中国民航大学计算机科学与技术学院,天津 300300)

摘要:基于网络自保护理论和多元异常分析方法,提出一种网络攻击自主防护机制.根据PDRR理论模型,设计网络自保护系统主要功能模块.运用多元异常分析方法,提出基于网络流的多元异常分析网络攻击检测算法.该算法根据网络流测量指标的异常偏差值对其分类,并对分类网络流分配路由调度优先级,削弱网络攻击对正常网络通信流的影响.实验结果表明,提出的网络自主防护机制能显著提高网络系统应对攻击行为的防御能力.

关键词:自主防护;网络安全;异常分析;网络流

中图分类号:TP309,TP393.08 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.10.012

A network self-protection mechanism based on multivariate abnormality analysis

XIE Lixia, DAI Qikui, YANG Hongyu

(*School of Computer Science and Technology, Civil Aviation University of China, Tianjin* 300300, *China*)

Abstract: A network self-protection mechanism against network attacks was proposed based on the network self-protection theory and multivariate abnormality analysis. According to PDRR theory model, the main function modules of network self-protection system were designed. By applying multivariate abnormality analysis theory, a flow-based multivariate abnormality analysis network attack detection algorithm was proposed. The algorithm uses a metric of abnormal distance to classify network flow into different types and prioritize the routing of different network flow packets, thus reducing the impact of network attacks against the normal traffic flow. Experimental results demonstrate that the proposed mechanism can significantly protect the network against attacks.

Key words: self-protection; network security; abnormality analysis; network flow

0 引言

近年来,随着人们安全意识日益提高,入侵检测系统、防病毒软件、防火墙等开始大量部署在网络中,但网络安全问题依旧没有太大改观.网络安全研究还存在很多亟待解决的问题,如:目前尚无一个符合PDRR[1]理论的网络安全系统模型;由于缺少统一指挥,现有安全产品往往各自为政,无法形成一个

收稿日期:2011-05-01;**修回日期**:2011-06-22

基金项目:国家自然科学基金(60776807,61179045),中国高技术研究发展(863)计划(2006AA12A106),天津市科技支撑计划重点项目(09JCZDJC16800),中国民航科技基金(MHRD201009,MHRD201021),中央高校基本科研业务费专项(ZXH2009A006,ZXH2010D009)资助.

作者简介:谢丽霞,女,1974年生,硕士/副教授.研究方向:网络与信息安全.E-mail:lxxie@126.com

通讯作者:杨宏宇,博士/教授.E-mail:yhyxlx@hotmail.com

统一的有机整体.当网络受到攻击时,响应、恢复等工作主要依靠手工完成,缺乏自动响应机制;现有的网络安全技术依赖于防火墙、入侵检测和反病毒软件等,属于静态的被动安全防御,强调以攻击为中心,检测到攻击后才有所响应,此时可能已经造成严重的损失.

倘若计算机网络具备类似人体的自我免疫系统功能,即网络自保护功能,则会大大减少网络安全事件的发生.网络自保护系统能够充分利用现有网络技术(防火墙、认证系统和入侵检测技术等),采用相同安全策略、共享网络安全信息和服务、相互协作,形成一个整体防御和自动响应的安全防护体系.

IBM公司在2001年首次引入自保护[2]概念,提出了自主计算研究计划,目的是建立一个具有自主防护功能的计算系统,具有自我管理、自配置、自优化和自保护功能.2003年,IBM陆续发表了与自保护相关的研究报告.出于保密原因和商业利益考虑,IBM研究报告的重点在于自主计算环境的自保护配置描述,未涉及自保护理论研究内容.

文献[3]提出了一个测、控结合的三层结构容入侵系统模型,系统在结构上采用本地、子网和企业网3个层次,分别监测并控制简单、联合及复杂的网络攻击.该模型的目标是对网络入侵的容忍,还不能实现网络自主保护.

文献[4]在分析DDoS攻击的网络流量特性基础上,提出了一个基于非线性预处理网络流量预测方法(non-linear preprocessing network traffic prediction, NLPP)的分布式拒绝服务DDoS攻击检测算法.该算法由基本检测算法和非线性预处理网络流量预测方法组成,但该检测算法的关键参数选取方法还不成熟,漏报率较高.

文献[5]提出了一种分布式神经网络学习算法(large-seale network intrusion detection algorithm based on distributed learning, LNIDDL),并将其用于大规模网络入侵检测,但该算法还不能在无监督学习情况下对未知攻击进行检测.

文献[6]基于改进的置信度机器学习算法,提出了一种基于直推式方法的网络异常检测方法(network anomaly detection method based on transduction scheme, NADMTS).它能够在高置信度的情况下,使用训练的正常样本有效地对异常进行检测,但该方法还需根据实际应用情况作进一步改进,以提高其性能.

文献[7]提出了一个轻量级的在线自适应网络异常检测算法(online adaptive network anomaly detection algorithm, OANAD).该算法能够对实时网络数据流进行在线学习和检测,在少量指导下逐渐构建网络的正常模式库和入侵模式库,并根据网络使用特点动态进行更新,但该算法的检测率仍有待提高.

文献[8]提出了一种多层次入侵检测系统(multi level intrusion detection system, ML-IDS).ML-IDS从3个层次(网络数据流、数据报头信息和有效载荷)对网络通信流进行检查和分析,并采用高效融合决策算法提高整体检测率和最大限度地减少误报率.因为ML-IDS系统只对网络报文头部信息和网络通信流进行监控,因此尚无法检测对有效载荷和主机的攻击行为.

文献[9]提出一种前摄监管保护(proactive surge protection, PSP)机制,旨在建立应对DDoS攻击的第一道防线.该机制通过在各网络流间提供带宽隔离以最大限度地减少附带损害,并很容易通过现有的路由器机制进行部署.但该机制无法有效抵御针对网络协议或终端主机资源的非带宽攻击行为,无法准确识别并过滤具体网络攻击流.

针对当前网络安全的现状,为了提高网络防御体系的整体检测和防御能力,本文提出一种基于异常分析算法的网络自主防护方法,实现对网络系统的有效防护.

1 多元异常分析方法

由于单个网络属性参数无法准确捕捉网络中的异常行为,为提高网络攻击检测效率和准确性,本文采用多变元分析方法,通过研究各网络参数指标的观测值及其相关性,确定网络系统运行状况.

在二维变量空间中,如图1所示,椭圆封闭区域表示正常取值区域,点C为正常取值区域中心,UCL_i和LCL_i($i=1,2$)分别为变元X_1和X_2合法取值控制上限和下限.$V(x_1,x_2)$表示某一评估点,其每个变元x_1和x_2均为合法取值,当把这两个变元关联起来,$V(x_1,x_2)$则在正常取值区域之外.

由于单变元只反映某一评估点的局部特征,而多变元能从多个角度描述该评估点的状态,因此,在异常行为检测中,多变元异常分析方法比单变元分

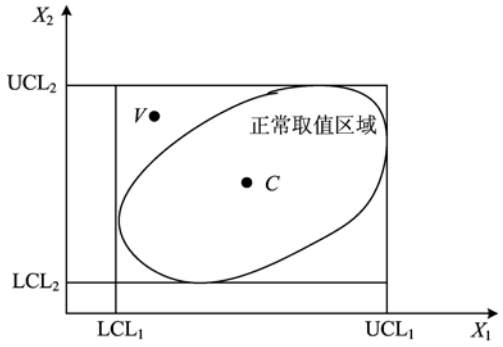

图 1　多元分析模型

Fig. 1　The multivariate analysis model

析方法的检测准确性更高.

基于 Hotelling's T^2 控制图[10]思想,本文提出的多元异常分析方法如下.

首先,在观察窗口大小为时间段 T 内对某网络实体或组件的 k 个属性指标 $M_j(j=1,2,\cdots,k)$进行 $n(n>20)$次采样记录,采样结果序列以矩阵形式表示如下:

$$\mathbf{MA}=\left\{\begin{bmatrix}MA_1(t)\\MA_2(t)\\\vdots\\MA_k(t)\end{bmatrix}\begin{bmatrix}MA_1(t+t_1)\\MA_2(t+t_1)\\\vdots\\MA_k(t+t_1)\end{bmatrix}\cdots\begin{bmatrix}MA_1(t+t_n)\\MA_2(t+t_n)\\\vdots\\MA_k(t+t_n)\end{bmatrix}\right\} \tag{1}$$

由式(1),可求得样本均值$\overline{MA}$和协方差矩阵 $\mathbf{S}$,控制上限(upper control limit, UCL)和控制下限(lower control limit, LCL),确定出 p 个属性指标正常取值区域的基本范围. 其中协方差矩阵 $\mathbf{S}$ 确定正常取值区域边界,样本均值$\overline{MA}$为正常取值区域中心.

当网络实体或组件遭受异常攻击时,其各测量指标(measurement attributes, MAS)将会受攻击的影响而发生变化,并运行于不正常状态. 异常偏差(abnormal distance, AD)[11]是一个用来表征某网络实体或组件当前运行状况与正常状态偏差的物理量,它通过一个或多个测量指标观测值的变化情况,描绘出某网络实体或组件当前运行状况,如图 2 所示.

对于测量指标 MA_j 在 t 时刻的异常偏差,其正规化表达式为

$$\mathrm{AD}_j(t)=\frac{(MA_j(t)-\mu_{MA_j})^2}{\sigma^2_{MA_j}} \tag{2}$$

式中,μ_{MA_j} 和 $\sigma^2_{MA_j}$ 表示在正常工作状态下,测量指标

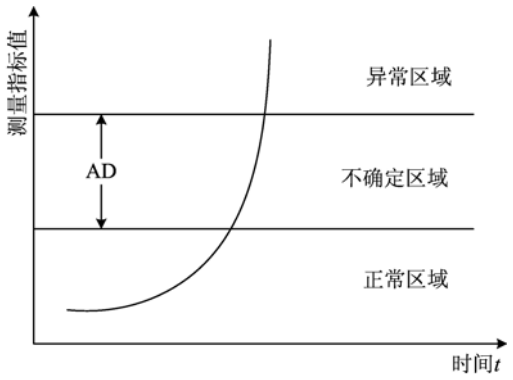

图 2　测量指标状态曲线

Fig. 2　The measurement index state curve

MA_j 的均值和方差;$MA_j(t)$为测量指标 MA_j 在 t 时刻的观测值.

对于一组多个相关的测量指标 $\mathbf{J}$ 在 t 时刻的总体异常偏差,定义为

$$\mathrm{AD}_{\mathbf{J}}(t)=(MA_{\mathbf{J}}(t)-\mu_{MA_{\mathbf{J}}})^{\mathrm{T}}\mathbf{S}^{-1}(MA_{\mathbf{J}}(t)-\boldsymbol{\mu}_{MA_{\mathbf{J}}}) \tag{3}$$

式中,$\mathbf{J}=(MA_1, MA_2,\cdots,MA_k)^{\mathrm{T}}$;$MA_{\mathbf{J}}(t)$为相关测量指标 $\mathbf{J}$ 在 t 时刻的一组测量值,$MA_{\mathbf{J}}(t)=(MA_1(t), MA_2(t)\cdots,MA_k(t))^{\mathrm{T}}$;$\boldsymbol{\mu}_{MA_{\mathbf{J}}}$为相关测量指标 $\mathbf{J}$ 观测值的均值向量.

2　网络自保护系统的功能模块设计

根据 PDRR 理论模型,本文设计的网络自保护系统主要包括 4 个模块(如图 3 所示):监测模块、样本采集模块、异常分析模块、响应模块.

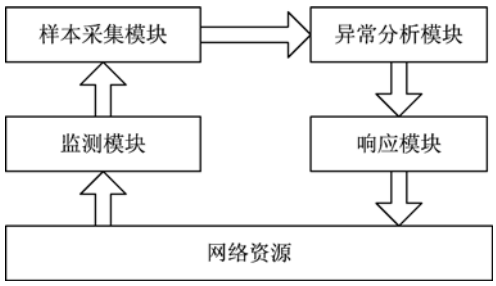

图 3　自保护系统的功能模块

Fig. 3　Function modules of self-protection system

(Ⅰ)监测和样本采集模块

通过数据分析和异常特征提取,确定描述网络系统及其组件工作状态的最相关测量指标,获得用于监测网络异常的最佳测量指标集[12],提高检测网络攻击的准确性. 部分测量指标如表 1 所示.

表 1 网络属性测量指标

Tab. 1 Network attributes measurement index

网络协议层	测量指标(MAS)
应用层 HTTP,DNS, SMTP	IF：调用频率
传输层 TCP/UDP	Src/Dest Port：源/目的端口号 SID：序列号 Sequence_num：帧序号 Time：日期和时间 Packect Size：字节数 Frame Type/Subtype：帧类型
网络层 ICMP/ARP	AR：ARP 请求速率 Src/Dest IP：源/目的 IP 地址
数据链路层 MAC	Src/Dest MAC：源/目的 MAC 地址

(Ⅱ) 异常分析模块

为了描述网络系统当前运行状态与其正常运行状态的偏离情况,根据 Hotelling's T^2 方法建立 AD 值计算公式.该模块基于监测和样本采集模块提供的网络组件各种测量指标样本数据有效信息,实时计算出其总体异常偏差值 $AD_J(t)$,当 $AD_J(t)$ 偏离正常取值范围后,及时发送该异常报告至响应模块.

(Ⅲ) 响应模块

当检测到网络攻击后,该模块立即做出响应,如关闭网络接口、关闭一个网络节点、临时切断网络连接、终止系统调用、终止进程、注销用户等,并及时将此网络异常消息通知给其相邻 Agent.

3 网络攻击检测算法

为了对网络攻击进行实时监测和分析,基于网络流 (network flow)[13] 概念,本文提出基于多元异常分析的网络攻击检测算法.算法流程如图 4 所示.

本文对网络流的定义并不局限于 TCP/IP 协议,而是指网络系统内部网络节点间在一次通信过程中所产生的网络数据流.只要属于该网络流的数据包在小于设定的超时器内到达目的地址,就认定其仍然处于活动状态.

以该算法为基础,本文设计了一个网络流分类模型(如图 5 所示),根据网络流相关测量指标的总体异常偏差值 $AD_J(t)$ 分为以下 4 类:

①正常网络流(normal traffic)——此类网络流的 $AD_J(t)$ 值低于阈值 α.

②类正常网络流——此类网络流的 $AD_J(t)$ 值介于阈值 α 与 β 之间.

③类异常网络流(probable abnormal traffic)——此类网络流的 $AD_J(t)$ 值介于阈值 β 与 γ 之间.

④异常网络流(attacking traffic)——此类网络流的 $AD_J(t)$ 值高于阈值 γ.

其中,

α=probable_normal_threshold,

β=probable_abnormal_threshold,

γ=abnormal_threshold.

算法为不同种类网络流分配不同路由调度优先级,对于正常网络流数据包赋予较高路由调度优先级,而对于攻击性网络流赋予较低路由调度优先级.

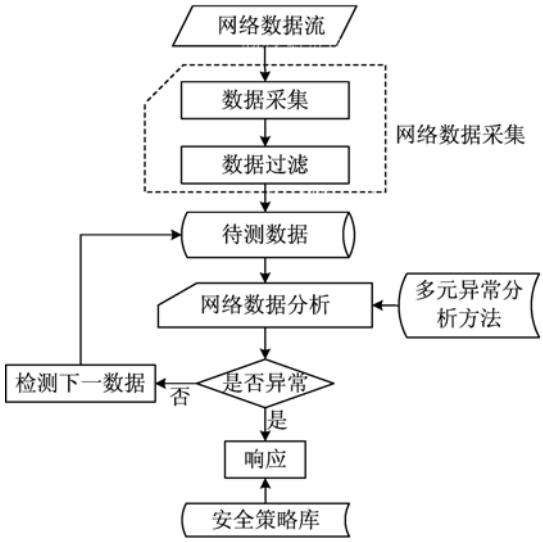

图 4 网络攻击检测流程

Fig. 4 Network attack detection procedure

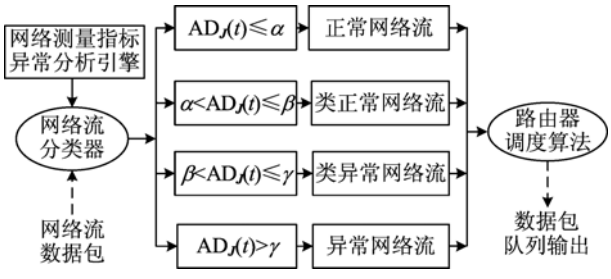

图 5 网络流分类模型

Fig. 5 The network traffic classification model

为降低网络攻击等非正常网络流对网络通信的影响,本文提出一种基于网络流总体异常偏差值的路由调度优先级分配算法:

$$f_{\text{prioriy}}(t)=\begin{cases}2, & \text{AD}_J(t)\leqslant\alpha\\ \dfrac{1}{\text{AD}_J(t)}, & \text{AD}_J(t)>\alpha\end{cases}\tag{4}$$

式中，$f_{\text{priority}}(t)$表示网络流在 t 时刻的路由调度优先级. 对于正常网络流，$f_{\text{priority}}(t)$最高值默认为 2；对于非正常网络流，$f_{\text{priority}}(t)$等于 $\text{AD}_J(t)$的倒数. 由于异常网络流的各测量指标观测值大大偏离正常阈值，$\text{AD}_J(t)>\gamma>\alpha$，$\text{AD}_J(t)\geqslant 1$，由式(4)，$f_{\text{priority}}(t)\approx 0$. 对于异常网络流，其测量指标总体异常偏差值越大，则路由调度优先级别越低. 在默认情况下，路由器自动丢弃 $f_{\text{priority}}(t)$小于 0.5 的网络流数据包.

面对复杂网络系统，为统一管理和控制，算法给每个网络流定义一个全局标识 id 和一个全局网络流异常偏差值 GFAD(global flow abnormality distance). GFAD 是通过网络系统内部各观测点间(如 Agent)互相交流它们对异常网络流计算出的 $\text{AD}_J(t)$值，建立起的一个基于整个网络的全局变量. 在网络系统中，对于一个攻击性网络流所导致的网络异常现象，会被某些 Agent 提前检测到，它们会把此异常消息及时通知给其他邻近 Agent，该异常流的 GFAD 值将会增加，同时其相应的路由调度优先级将会降低，最终导致其不能被路由器转发而丢弃. 通过引入 GFAD，可以提升对异常流检测响应效率，即从网络攻击发动的上游网络节点起，就削弱了它们对正常网络通信的影响.

基于多元异常分析的网络攻击检测算法实现描述如下. Agent 作为网络运行状况实时检测引擎，被部署在各路由器上. 当 Agent 进入启动状态时，首先创建一个消息接受线程 ReceiveEventThread，以实时接受邻近 Agent 发来的异常消息. 当 ReceiveEventThread 接受到从其他 Agent 发送来的异常事件 ADEvent，它会将该事件中网络流 $\text{AD}_J(t)$值与本地该网络流 GFAD 值相比较，并做必要更新. 当 Agent 监测到新网络流时，自动为其创建一个网络流监测线程 FlowDetectionThread，以实时监测该网络流运行状态. 其中 FlowDetectionThread 伪代码如下：

```
FlowDetectionThread(){
  while(true){
    MAJ(t)=Monitor_Collect(MA1(t), MA2(t), …MAk(t));
    ADJ(t)=Calculate_AD(MAJ(t));
    if(ADJ(t)>this.GFAD)
      GFAD = ADJ(t);
    if(ADJ(t)>probable_abnormal_threshold)
      Multicast_Event(ADEvent);
    if(ADJ(t)>abnormal_threshold)
      Self_Protection();
  }
}
```

4　实验与结果

通过在真实网络环境下设计对比实验，验证本文提出的多元异常分析网络攻击自主防护机制应对网络异常攻击的防御能力. 其中实验组各路由器和主机未部署本文提出的网络自主防护机制，而对照组中各路由器和主机均部署本文提出的网络自主防护机制，实现对网络系统进行实时监测和防护.

4.1　测试环境

真实网络环境为某单位 100M 局域网，该局域网共包括 5 个子网，它们分别为 Network 1，Network 2，Network 3，Network 4 和 Network 5，该网络的拓扑结构如图 6 所示. 在实验方案中，通过 Code Red Ⅱ[14]蠕虫攻击测试验证本文所提出的网络自主防护机制抵御 Code Red Ⅱ蠕虫攻击的有效性.

在本实验中，通过网络流量模拟产生器 GenSyn 软件[15]在真实网络环境中生成通信流量，利用网络攻击发生器 Attack Launcher 产生各种网络攻击行为，并使用 Cisco NetFlow[16]对网络通信性能进行实时监测.

4.2　实验过程与结果

在本实验网络环境中，子网 Network 1，Network 2 与 Network 3 中各主机设置为服务器端，子网 Network 4 和 Network 5 中各主机设置为客户端. 其中，在服务器各主机上配置 HTTP Server Tomcat 服务器软件，在客户端各主机上安装网络流量模拟产生器 GenSyn 工具软件，各客户端和服务器间通过简单数据文件的持续传输来模拟真实网络环境中网络通信状况.

在 $t=150$ s 时，由子网 Network 5 中客户端主机 5-1 发起 Code Red Ⅱ蠕虫攻击，将其所在子网 Network5 内所有客户端主机感染，并在较短时间内感染子网 Network 1 与 Network 3 中部分服务器. $t=350$ s 时，被感染主机数目达到 53 台(包括 39 台服务器和 Network 5 中的 14 台客户端主机)，此

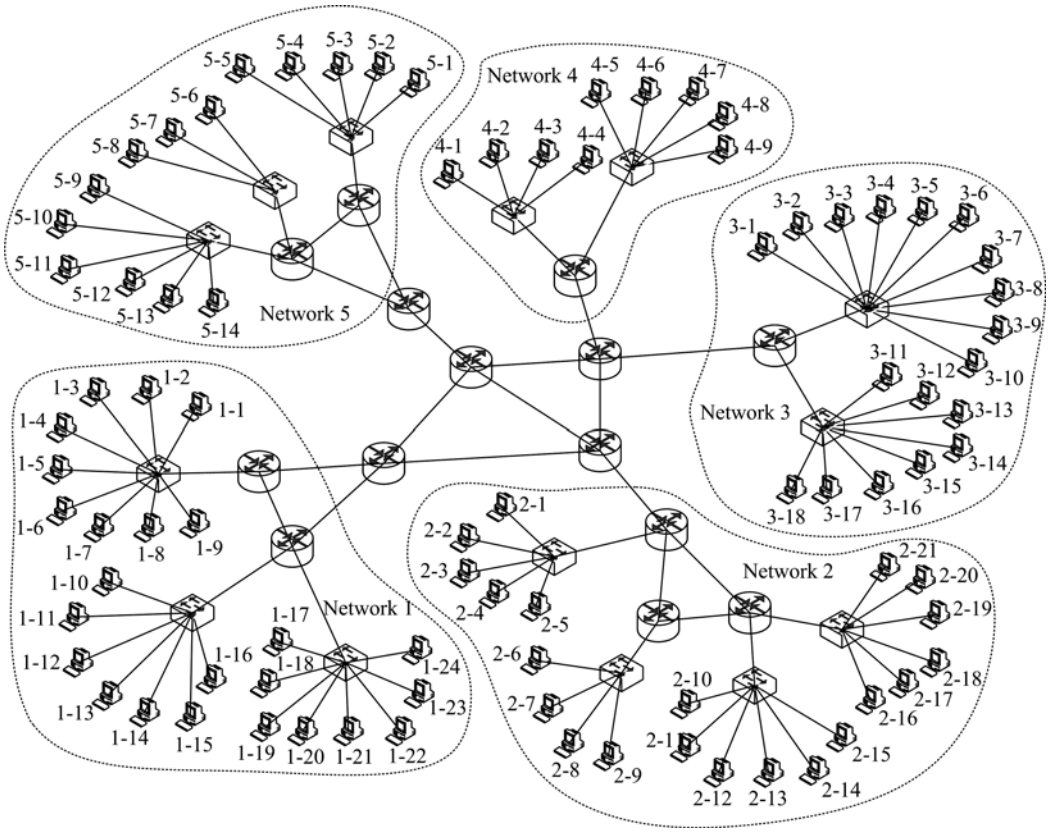

图 6 实验网络拓扑结构

Fig. 6 The network topology of experiment

时撤销 Code Red Ⅱ蠕虫攻击，所有被感染主机自动恢复至正常状态. 图 7 显示服务器端子网中同时被蠕虫病毒所感染的各组主机，各组主机被感染时刻如表 2 所示.

表 2 子网中各组服务器被感染时刻

Tab. 2 Infection time of severs in subnetworks

组号	被感染时刻/s	服务器端子网主机编号	
		Network 1	Network 3
Group 1	180	1-13, 1-14, 1-15	
Group 2	220		3-1, 3-2, 3-3, 3-4
Group 3	250	1-7,1-8, 1-9, 1-10,1-11,1-12	
Group 4	270		3-5, 3-6, 3-7
Group 5	300	1-4, 1-5, 1-6	
Group 6	350		3-8, 3-9

在实验中，根据网络流源子网地址和目的子网地址将正常网络流分为 4 类，并重点监测 Code Red Ⅱ蠕虫攻击对其的影响：

（Ⅰ）源头网络被蠕虫感染，但目的网络未被感染的正常网络流

实验中，选择客户端主机 5-2 与服务器端主机 2-1 之间的网络流作为监测对象，记作 flow1.

（Ⅱ）源头网络未被蠕虫感染，但目的网络被感染的正常网络流

实验中，选择客户端主机 4-2 与服务器主机 3-5 间的网络流作为监测对象，记作 flow2.

（Ⅲ）源头网络和目的网络均被蠕虫感染的正常网络流

实验中，选择客户端主机 5-3 与服务器主机 1-15 间的网络流作为监测对象，记作 flow3.

（Ⅳ）源头网络和目的网络均未被蠕虫感染的正常网络流

实验中，选择客户端主机 4-1 与服务器主机 2-3 间的网络流作为监测对象，记作 flow4.

实验中对上述 4 种网络流通信状况进行详细监测记录，观测窗口为 600 s，时间粒度为 1 s，每组数据进行 600 次数据采样.

图 8 和图 9 分别显示在本实验中，未使用和使用异常分析自主防护机制情况下的 Code Red Ⅱ蠕虫攻击对各网络流丢包率的影响状况. 通过对比发

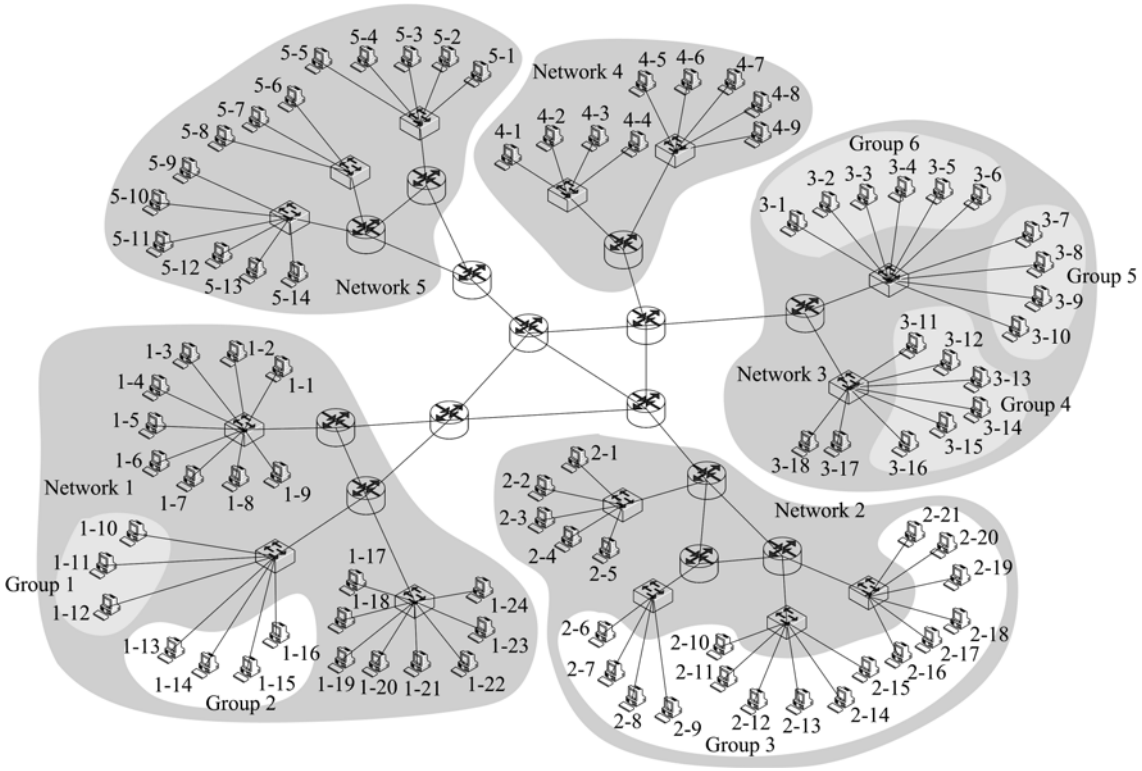

图 7　被蠕虫病毒感染服务器组

Fig. 7　Server groups infected by worm

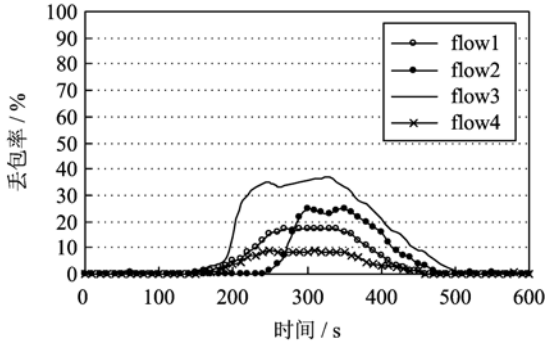

图 8　未使用异常分析自主防护机制的各网络流丢包率

Fig. 8　Network packet loss rates without the anomaly analysis self-protection mechanism

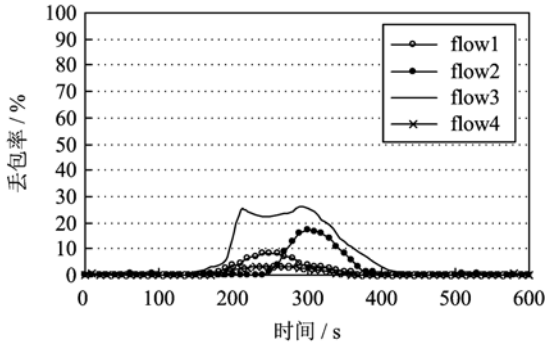

图 9　使用异常分析自主防护机制的各网络流丢包率

Fig. 9　Network packet loss rates with the anomaly analysis self-protection mechanism

现，当在网络中各路由器上部署本文提出的异常分析自主防护机制时，可明显削弱 Code Red Ⅱ蠕虫攻击对正常网络流通信影响.

为进一步验证本文提出的异常分析自主防护机制可以更有效抵御较严重 Code Red Ⅱ蠕虫攻击对正常网络流通信影响，进行了 Code Red Ⅱ严重攻击对比实验. 在实验中，选择客户端主机 5-3 与 Group 3 中服务器主机 1-15 之间的正常网络流作为监测对象，记作 flow 3′. 图 10 和图 11 分别显示了网络中未使用和使用异常分析自主防护机制情况下的网络流 flow 3′丢包率状况.

由表 2 可知，在 $t=180$ s 时，Group 1 中有 3 台服务器被蠕虫病毒感染；在 $t=270$ s 时，Group 3 中有 6 台服务器被蠕虫病毒感染. 对比图 8 和图 10，发现未部署异常分析自主防护机制情况下，网络流 flow3′较 flow3 的通信状况受 Code Red Ⅱ蠕虫攻击的影响更大. 在 $t=330$ s 时，由于蠕虫攻击影响，网络流 flow3 丢包率达到最大值 38%，而网络流

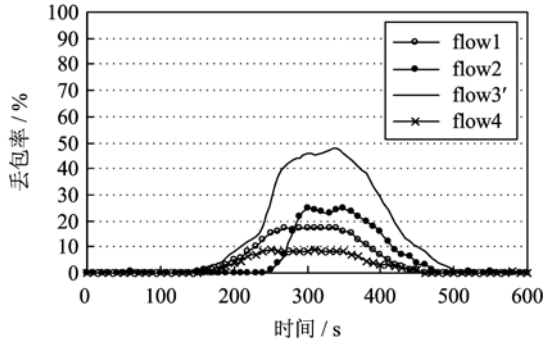

图 10 未使用异常分析自主防护机制的各网络流丢包率

Fig. 10 Network packet loss rates without the anomaly analysis self-protection mechanism

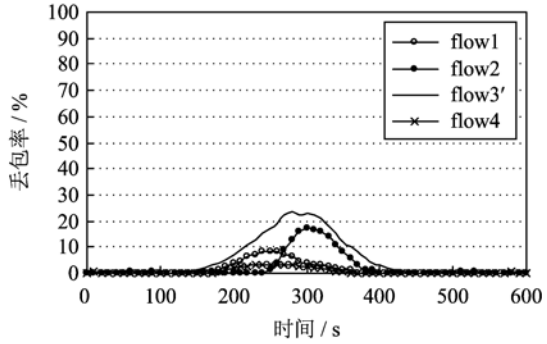

图 11 使用异常分析自主防护机制的各网络流丢包率

Fig. 11 Network packet loss rates with the anomaly analysis self-protection mechanism

flow3′丢包率达到最大值 43.5%. 由图 9 和图 11 可知,当网络中部署异常分析自主防护机制后,在 $t=300$ s 时,网络流 flow3 丢包率最大值降低至 26.5%,而网络流 flow3 丢包率最大值降低至 23%. 相对于未部署异常分析自主防护机制的情况,网络流 flow3 丢包率最大值降低 30.3%,网络流 flow3′丢包率最大值降低 47.13%.

由以上实验数据可得出结论,正常通信网络流受到 Code Red Ⅱ蠕虫攻击的影响越严重,采用异常分析自主防护机制时对其恢复效果越明显. 其原因是:Code Red Ⅱ蠕虫攻击造成的影响越严重,它所产生的攻击性网络流异常偏差值就越大,相对于异常偏差值较小的攻击性网络流数据包,异常偏差值较大的网络流数据包在转发过程的丢弃率更高.

在相同网络环境下,对本文提出的异常分析算法与 NLPP[4], LNIDDL[5], NADMTS[6], OANAD[7], ML-IDS[8] 和 PSP[9] 算法进行了 Code Red Ⅱ蠕虫、Email 蠕虫和 DDoS 网络攻击检测对比实验,上述算法的检测性能结果如表 3 所示.

表 3 检测性能比较

Tab. 3 Detection performance comparison

攻击方案	Code Red Ⅱ		Email 蠕虫		DDoS	
检测性能	检测率 /%	误报率 /%	检测率 /%	误报率 /%	检测率 /%	误报率 /%
本文算法	92.78	2.15	94.52	1.73	97.5	0.21
NLPP	87.6	4.3	89.3	2.95	91.7	3.2
LNIDDL	85.3	3.7	87.57	2.06	91.9	0.51
NADMTS	82.12	4.79	80.23	3.23	93.3	1.29
OANAD	92.15	3.05	92.16	2.3	97.18	0.46
ML-IDS	90.25	2.83	91.7	1.95	96.1	0.92
PSP	87.6	5.1	58.6	3.77	92.8	2.1

从表 3 中可见,本文算法对 Code Red Ⅱ蠕虫攻击的检测率为 92.78%,误报率为 2.15%;对 Email worm 攻击的检测率为 94.52%,误报率为 1.73%;对 DDoS 攻击的检测率为 97.5%,误报率为 0.21%. 通过表 3 的检测结果可见,本文提出的异常分析算法对 Code Red Ⅱ蠕虫、Email 蠕虫和 DDoS 网络攻击的检测效率明显优于其他算法.

5 结论

为提高网络系统整体防御能力,本文结合自保护理论,应用多元分析方法,提出了基于异常分析的网络攻击检测算法. 此算法根据网络流 AD 指标值,将其分为正常、类正常、类异常和异常 4 类网络流. 通过对不同网络流分配不同路由调度优先级,明显削弱网络攻击对正常网络通信的影响,实现应对网络攻击的自主防护机制. 在真实网络环境中,通过 Code Red Ⅱ蠕虫攻击实验证明了该机制可有效抵御网络异常攻击. 在相同网络环境下,对本文算法与其他算法进行了 Code Red Ⅱ蠕虫、Email 蠕虫和 DDoS 网络攻击检测对比实验,实验结果表明本文算法对 Code Red Ⅱ蠕虫攻击、Email 蠕虫和 DDoS 网络攻击的检测效率明显优于其他算法.

参考文献(References)

[1] IBM. An architectural blueprint for autonomic computing[R]. Armonk, NY: IBM, 2006.

[2] Ganek A G, Corbi T A. The dawning of the autonomic computing era [J]. IBM Systems Journal, 2003, 42(11): 5-18.

[3] Wang Xianpei, Xu Liang, Li Feng, et al. A tri-level self-protected intrusion tolerant system for electric power information network system[J]. Automation of Electric Power Systems, 2005, 29(10): 69-72.

王先培，许靓，李峰，等. 一种 3 层结构带自保护的电力信息网络容入侵系统[J]. 电力系统自动化，2005，29(10)：69-72.

[4] Yang Xinyu，Yang Shusen，Li Juan. A flooding-based DDoS detection algorithm based on non-linear preprocessing network traffic predicted method[J]. Chinese Journal of Computers，2011，34(2)：395-405.
杨新宇，杨树森，李娟. 基于非线性预处理网络流量预测方法的泛洪型 DDoS 攻击检测算法[J]. 计算机学报，2011，34(2)：395-405.

[5] Liu Yanheng，Tian Daxin，Yu Xuegang，et al. Large-scale network intrusion deteetion algorithm based on distributed learning[J]. Journal of Software，2008，19(4)：993-1 003.
刘衍珩，田大新，余雪岗，等. 基于分布式学习的大规模网络入侵检测算法[J]. 软件学报，2008，19(4)：993-1 003.

[6] Wei Xiaotao，Huang Houkuan，Tian Shengfeng. An online adaptive network anomaly detection system-model and algorithm[J]. Journal of Computer Research and Development，2010，47(3)：485-492.
魏小涛，黄厚宽，田盛丰. 在线自适应网络异常检测系统模型与算法[J]. 计算机研究与发展，2010，47(3)：485-492.

[7] Li Yang，Fang Binxing，Guo Li，et al. A network anomaly detection method based on transduction scheme[J]. Journal of Software，2007，18(10)：2 595-2 604.
李洋，方滨兴，郭莉，等. 基于直推式方法的网络异常检测方法[J]. 软件学报，2007，18(10)：2 595-2 604.

[8] Hariri S，Nashif Y，Kumar A，et al. Multi-level intrusion detection system (ML-IDS)[C]//Proceedings of International Conference on Automonic Computing. Piscataway，NJ：IEEE Computer Society，2008：131-140.

[9] Lin B，Sen S，Spatscheck S，et al. Proactive surge protection：A defense mechanism for bandwidth-based attacks[J]. IEEE/ACM Transactions on networking，2009，17(6)：1 711- 1 723.

[10] Montgomery D C. Design and Analysis of Experiments[M]. 5th ed. New York：Wiley，2000.

[11] Qu G Z，Hariri S，Jangiti S，et al. Online monitoring and analysis for self-protection against network attacks[C]//Proceedings of the International Conference on Autonomic Computing. Piscataway，NJ：IEEE Computer Society，2004：324-325.

[12] Hariri S，Yousif M，Qu G. A new dependency and correlation analysis for features[J]. IEEE Transactions on Knowledge and Data Engineering，2005，17(9)：1 199- 1 207.

[13] Hariri S，Qu G，Modukuri R，et al. Quality- of-protection (QoP)-an online monitoring and self-protection mechanism[J]. IEEE Journal on Selected Areas in Communications，2005，10(23)：1 983- 1 993.

[14] Wikipedia. Code Red Ⅱ (computer worm)[EB/OL]. [2011-05-01]. http://en. wikipedia. org/wiki/Code_Red_Ⅱ_(computer_ worm).

[15] NTNU. GenSyn-generator of Synthetic Internet traffic[EB/OL]. [2011-05-01]. http://www. item. ntnu. no/ people/personalpagesfac/poulh/gensyn.

[16] Network Uptime. Free NetFlow Tools[EB/OL]. [2011-05-01]. http://www. networkuptime. com/tools/netflow.