ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.3, March 2006, pp.463−471
DOI: 10.1360/jos170463

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于 D-S 证据理论的网络异常检测方法*

诸葛建伟+, 王大为, 陈 昱, 叶志远, 邹 维

(北京大学 计算机科学技术研究所,北京 100871)

A Network Anomaly Detector Based on the D-S Evidence Theory

ZHUGE Jian-Wei+, WANG Da-Wei, CHEN Yu, YE Zhi-Yuan, ZOU Wei

(Institute of Computer Science and Technology, Peking University, Beijing 100871, China)

+ Corresponding author: Phn: +86-10-82529607, E-mail: zhugejianwei@icst.pku.edu.cn, http://www.icst.pku.edu.cn

ZhuGe JW, Wang DW, Chen Y, Ye ZY, Zou W. A network anomaly detector based on the D-S evidence theory. *Journal of Software*, 2006,17(3):463−471. http://www.jos.org.cn/1000-9825/17/463.htm

Abstract: Network anomaly detection has been an active research topic in the field of Intrusion Detection for many years, however, it hasn't been widely applied in practice due to some issues. The issues include high false alarm rate, limited types of attacks the approach can detect, and that such approach can't perform real-time intrusion detection in high speed networks. This paper presents a network anomaly detector based on Dempster-Shafer (D-S) evidence theory. The detector fuses multiple features of network traffic to decide whether the network flow is normal, and by such fusion it achieves low false alarm rate and missing rate. It also incorporates some self-adaptation mechanisms to yield high accuracy of detection in dynamic networks. Furthermore, light-computation features are used to develop an efficient fusion mechanism to guarantee high performance of the algorithm. On the 1999 DARPA/Lincoln Laboratory intrusion detection evaluation data set, this detector detects 69% attacks at low false alarm rate. Such result is better than the 50% detection rate of EMERALD—the winner of 1999 DARPA/Lincoln Laboratory intrusion detection evaluation, and results from other research projects.

Key words: intrusion detection; anomaly detection; D-S theory; evidence theory; data fusion

摘 要: 网络异常检测技术是入侵检测领域研究的热点内容,但由于存在着误报率较高、检测攻击范围不够全面、检测效率不能满足高速网络实时检测需求等问题,并未在实际环境中得以大规模应用.基于 D-S 证据理论,提出了一种网络异常检测方法,能够融合多个特征对网络流量进行综合评判,有效地降低了误报率和漏报率,并引入自适应机制,以保证在实时动态变化的网络中的检测准确度.另外,选取计算代价小的特征以及高效的融合规则,保证了算法的性能满足高速检测的要求.该方法已实现为网络入侵检测原型系统中的异常检测模块.通过 DARPA 1999 年 IDS 基准评测数据的实验评测表明,该方法在低误报率的前提下,达到了 69%的良好检测率,这一结果优于 DARPA 1999 年入侵检测系统评测优胜者 EMERALD 的 50%检测率和同期的一些相关研究成果.

关键词: 入侵检测;异常检测;D-S 理论;证据理论;数据融合
中图法分类号: TP309 文献标识码: A

* Supported by the Science-Technology Project of the National "Tenth Five-Year-Plan" of China under Grant No.2001BA802B07 (国家"十五"科技攻关计划); the "Microsoft Fellow" Plan (微软学者计划); the "IBM Ph.D. Fellowship" Plan (IBM 博士生英才计划)
Received 2004-11-04; Accepted 2005-07-11

入侵检测系统是网络安全防御体系的一个重要组成部分,它的基本原理是:通过对网络和主机上某些关键信息进行收集分析,检测其中是否有违反安全策略的事件或攻击事件发生,并对检测到的事件发出警报.基于机器学习的异常检测是一类重要的入侵检测技术,它是通过各种机器学习方法,建立起正常情况下某些特征的数据轮廓,检测期间则将当前收集到的数据与正常数据轮廓相比较,当两者达到一定的偏移时视为有异常发生,并进行报警.而在网络应用越来越广泛的今天,网络数据流是探测网络攻击行为的最佳数据源.所以,基于网络的入侵检测系统目前是研究最为集中、也是应用最为广泛的检测技术.本文关注于针对网络数据流的异常检测方法.

对网络异常检测方法的研究从 1990 年的第 1 个网络入侵检测系统 NSM[1]问世开始,迄今为止,提出的方法有概率统计分析方法[2−6]、数据挖掘方法[7]、神经网络方法[8]、模糊数学理论[9]、人工免疫方法[10]、支持向量机方法[11−13]等.其中,基于概率统计分析方法实现了大量能够应用于实时网络流量异常检测的原型系统,包括 DARPA 1999 年 IDS 评测[14]优胜者 EMERALD 项目[15]中的 eBayes 组件[2],以 Snort 的第三方异常检测插件发布的 Spade[3]等.但这些方法还存在着不足之处,首先,漏报率和误报率都还较高:EMERALD 结合了特征检测和异常检测两种方法,虽然是 DARPA 1999 年评测的优胜者,但检测率仅达到了 50%;而 Spade 仅针对导致网络流量显著异常的扫描和洪水攻击,其误报率也较高;其次,虽然大部分方法使用多种特征来加大检测范围,但没有融合多个特征进行综合评判,或仅根据专家经验给出简单的特征组合公式[6],而没有任何理论根据;另外,大部分的方法[2−6]需要干净的训练数据集,而这一前提在真实的网络环境中并不能够确保;最后,有些方法[4−6]使用了数据包应用负载中的特征进行检测,虽然利用这些特征有助于提高检测率,但由于应用负载的数据量过大,使用这些特征往往导致检测算法不能够满足高速网络的检测需求.

为了克服上述方法的缺点,本文提出了一种基于 D-S 证据理论[16]的网络异常检测方法,并通过原型实现和实验评测分析、验证了其有效性.D-S 证据理论可以看作是有限域上对经典概率推理理论的一般化扩展,其主要特性是支持描述不同等级的精确度和直接引入了对未知不确定性的描述,这些特性在处理某些特征的差异不足以区分正常或攻击的情况时有着较大优势.Dempster 证据组合规则也为融合多个网络流特征提供了理论依据.在一些研究工作中,D-S 证据理论也已被引入到网络异常检测领域,如融合多个传感器数据进行异常检测[17],但其检测范围仅限于拒绝服务攻击.

本文针对包括探测、拒绝服务攻击及远程到本地攻击等绝大部分网络攻击方法,采用多个计算量小且区分度高的网络流特征,通过概率统计原理建立每个特征的正常数据轮廓,并基于 D-S 理论融合这多种特征对网络流量进行综合评判,从而确定当前网络流是否异常.同时还引入了自适应机制,以保证本文提出的网络异常检测方法的通用性及检测的准确性.通过 DARPA 1999 评测数据[14]进行测试获得的实验结果表明,本文提出的网络异常检测方法在保证较低误报率的前提下,达到了 69%的较高检测率.

本文第 1 节介绍 D-S 证据理论背景.第 2 节全面阐述基于 D-S 证据理论的网络异常检测引擎.第 3 节给出算法原型实现及实验结果,并对实验结果进行分析和对比.第 4 节给出本文的结论.

1 D-S 证据理论背景

D-S 证据理论由 Dempster 于 1967 年提出[16],其学生 Shafer 将其发展并整理成一套完整的数学推理理论.D-S 证据理论可以看作是有限域上对经典概率推理理论的一般化扩展,其主要特性是支持描述不同等级的精确度和直接引入了对未知不确定性的描述.D-S 证据理论可以支持概率推理、诊断、风险分析以及决策支持等,并在多传感器网络、医疗诊断等应用领域内得到了具体应用.

D-S 证据理论是建立在非空有限域Θ上的理论,Θ称为辨识框架(frame of discernment,简称 FOD),表示有限个系统状态$\{\theta_1,\theta_2,\ldots,\theta_n\}$,而系统状态假设 H_i 为Θ的一个子集,即Θ的幂集 P(Θ)的一个元素.D-S 证据理论的目标是仅根据一些对系统状态的观察 $E_1,E_2,\ldots,E_m$ 推测出当前系统所处的状态,这些观察并不能够唯一确定某些系统状态,而仅仅是系统状态的不确定性表现.作为 D-S 证据理论最底层的概念,首先需要定义对某个证据支持一个系统状态的概率函数,称为信度分配函数(basic probability assignment,简称 BPA).

定义 **1**. 信度分配函数定义为从Θ的幂集到[0,1]区间的映射: $m: P(\Theta) \to [0,1], m(\Phi) = 0, \sum_{A \in P(\theta)} m(A) = 1$.

D-S 证据理论中还提出了对多个证据的组合规则,即 Dempster 规则.

定义 **2**. Dempster 规则形式化定义如下:

设 m_1 和 m_2 为两个证据的信度分配函数,则对这两个证据的组合得出组合证据的信度分配函数为

$$m_1(A) \oplus m_2(A) = K^{-1} \sum_{B \cap C = A} m_1(B) m_2(C) \text{ when } A \neq \varnothing \tag{1}$$

其中 K 为归一化因子, $K = \sum_{B \cap C \neq A} m_1(B) m_2(C)$.

对 n 个证据进行组合的 Dempster 一般化规则为

$$m_{1..n}(A) = K_n^{-1} \sum_{\cap_i A_i = A} m_1(A_1) m_2(A_2) ... m_n(A_n) \quad \text{when } A \neq \varnothing, K_n = \sum_{\cap_i A_i \neq A} m_1(A_1) m_2(A_2) ... m_n(A_n) \tag{2}$$

2 基于 D-S 证据理论的网络异常检测引擎

在网络异常检测领域中,将网络流量的状态定义为正常和攻击两类,而异常检测算法的目标就是根据对网络流量各种特征的观察去评价其是否包含攻击行为.由于网络攻击一般会在多个不同的特征上表现异常,因此,依据 D-S 证据理论,融合多个特征上得到的观察作出综合评判,将能够有效地提高异常检测的准确度.

2.1 系统架构

基于 D-S 证据理论的思想,本文提出了一种融合多种特征的网络异常检测方法.系统架构如图 1 所示,选取多个区分度较高且容易计算的网络流量特征,通过概率统计方法对这些特征的正常轮廓进行学习和维护.在检测阶段,首先根据当前流量的特征值与正常轮廓的偏差给出此特征值的信度,然后通过基于 D-S 证据理论的多特征融合算法对多个特征值的信度进行组合,给出这多个网路流特征对网络流量是否异常的综合信度,并最终作出当前网络流量是否异常的评判.本文还引入了一些老化和实时更新机制来保证网络异常检测方法对网络流量变化的自适应性.

下面将分别从网络流特征选取与量化、基于 D-S 证据推理的检测引擎以及网络流自适应机制 3 个方面对本文提出的网络异常检测方法进行详细论述.

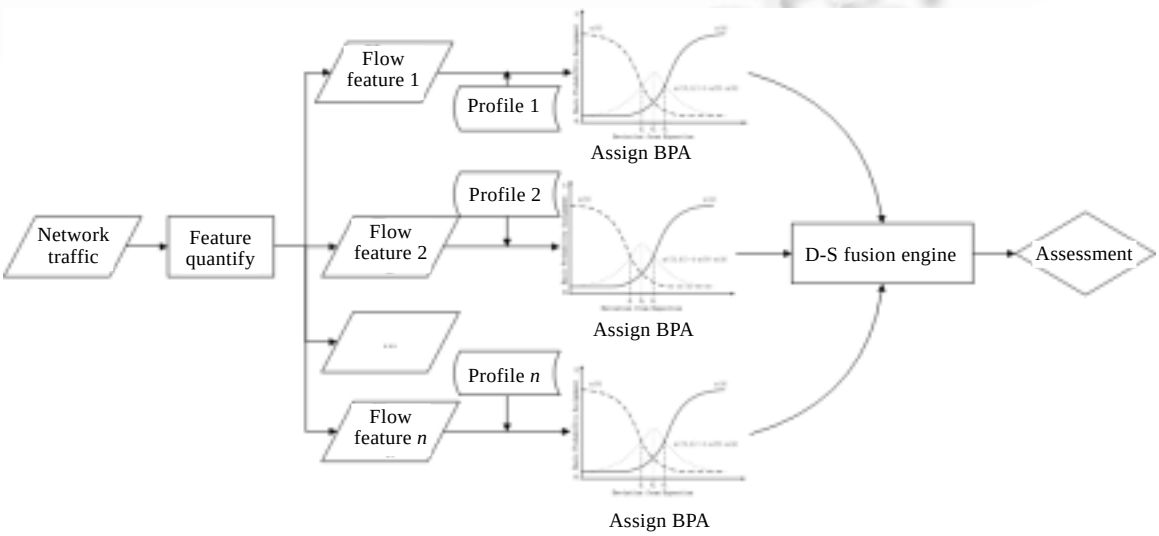

Fig.1 Architecture of network anomaly detector based on the D-S evidence theory

图 1 基于 D-S 证据理论的网络异常检测引擎系统架构

2.2 网络流特征选择与量化

目前,异常检测中的特征选取一般都依赖于专家经验,选取的标准在于:选择的特征对正常及异常的区分度较高,且从网络流量中量化该特征值的计算量较小.本文提出的基于 D-S 证据理论的网络异常检测方法对选取特征无任何限制.但出于对检测性能的考虑,在本文所提出方法的实现中,只选取了从应用层以下各层协议头部中的域值通过简单计算即可获得的特征.

我们根据网络流的源、目标 IP 地址和 IP 协议类型、服务端口对网络流进行分类,以获取网络流统计特征.首先,对网络流量根据源-目标 IP 地址对进行分类,形成多个源-目标 IP 对节点;然后,再利用服务协议(即 IP 协议类型和服务端口号)进行二级分类,对不同的服务协议分别建立对应的服务协议节点;第 3 层则根据不同的源端口号将源-目标对之间属于同一服务协议的不同网络流区分开;而每个网络流包括一个服务流和一个客户流,构成第 4 层.每个层次上的节点都维护了不同层次关注的网络流特征.另外,我们维护了两张向量表——源层特征和目标层特征,分别用来记录属于同一源 IP 地址和发往同一目标的所有网络流的统计特征.

当入侵检测系统监听到一个数据包时,首先通过此分类模型逐层寻找对应的节点:若不存在,则新建节点并统计网络流特征;若存在,则只需维护更新相关的特征.基于此网络流分类模型,就可以获得在各个层次上的网络流内部特征及统计特征的取值.

2.3 基于D-S证据理论的检测引擎

由于网络异常检测只需要根据观察到的网络流量特征来判断网络流的状态是否异常,根据 D-S 证据理论,取辨识框架 Θ为 $\{N,A\}$,N 为正常,A 为异常,有 $N\cap A=\varnothing$.定义信度分配函数 $m:P(\{N,A\})\to[0,1],m(\varnothing)=0$,$m(\{N,A\})+m(N)+m(A))=1$.其中 $m(N)$表示当前特征支持正常行为的信度,$m(A)$则表示支持异常的信度,而 $m(\{N,A\})=1-m(N)-m(A)$表示根据该证据不能确定属于正常行为或攻击事件的信度,即支持未知的信度.

定义 **3**. 期望偏差函数:设 X为一个随机变量,若数学期望 $E(X)$与标准差 σ_X 存在,则称 $\xi(x)=\dfrac{|x-E(X)|}{\sigma_X}$ 为 X 上的期望偏差函数,即偏离数学期望多少个标准差.

我们基于期望偏差函数来定义信度分配函数,这是因为期望偏差函数比概率分布更能够反映特征异常程度,期望偏差描述了一个特征值与数学期望的距离,根据切比雪夫不等式 $P(x\,|\,\xi(x)\ge\delta)\le\dfrac{1}{\delta^2}$,概率分布随着期望偏差的增大呈平方量级递减,因此使用期望偏差与概率分布也保持了一致性.

图 2 描述了信度分配函数的基本设计原则,即当特征值的期望偏差较小($\xi<\xi_1$)时,表明该期望值处于一个较正常的范围内,因此支持正常流量的信度应较大,同时支持异常及未知的信度较小;随着期望偏差的增大,该特征值支持正常流量的信度将快速降低,而支持异常和未知的信度将逐渐升高,在一个临界点($\xi=\xi_2$),支持未知的信度将达到极值,同时支持异常的信度将超过支持正常的信度;在越过此临界点后,支持未知的信度将下降,而支持异常的信度将快速提升,并在$\xi>\xi_3$这段区间内超越支持未知的信度.

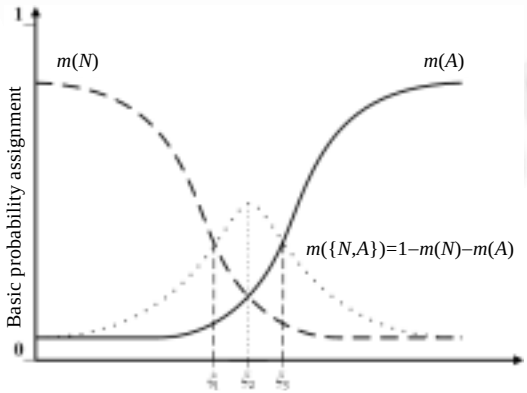

Fig.2 Basic probability assignment defined by deviation from expectation

图 2 根据期望偏差定义的信度分配函数

在如图 2 所示的信度分配函数的基本设计原则下,我们通过从训练数据中计算得出对正常和异常特征值区分最为适当的ξ_1,ξ_2,ξ_3这 3 个坐标点,并调整 $m(N),m(A),m(\Theta)$3 条信度分配函数曲线,从而适应正常轮廓曲线.

使用单个特征,我们很难将攻击事件(特别是隐蔽攻击)和正常行为完全区分开.因此,如果使用单一特征进行异常检测,则我们很难保证漏报率和误报率同时很低.而事实上,正常行为很难在几个特征同时呈现较异常的取值.与之相反,攻击动作通常会同时造成多个特征出现异常.因

此,我们考虑通过对多个观察事件进行融合分析来提高检测的准确性,以期望在降低误报率的前提下尽量检测出全部攻击事件.

Dempster 一般化组合规则已被证明为 P 完全难解问题[18],但在本文的应用场景中,即识别框架为只有两个互斥元素时,Dempster 规则的计算代价是 $O(n)$,从而可以证明本文提出的对多个网络流特征信度的融合算法的时间代价为 $O(n)$,其中 n 为网络流特征个数.

定理 **1**. Dempster 组合规则在$\Theta=\{N,A\}$, $N\cap A=\varnothing$ 的情况下的计算时间是 $O(n)$.

首先我们可以证明:在识别框架为两个互斥元素的情况下,Dempster 规则满足结合律,即证明

$$m_{1...n}(A)=m_{1...n-1}(A)\oplus m_n(A) \tag{3}$$

证明过程如下:

$$\begin{aligned}
m_{1...n}(A)&=\frac{\sum_{\cap_i A_i=A} m_1(A_1)m_2(A_2)...m_n(A_n)}{\sum_{\cap_i A_i\neq\varnothing} m_1(A_1)m_2(A_2)...m_n(A_n)}\\
&=\frac{\left(\sum_{\cap_i A_i=A} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(A)+\left(\sum_{\cap_i A_i=A} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(\Theta)+\left(\sum_{\cap_i A_i=\Theta} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(A)}{\left(\sum_{\cap_i A_i=A} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(A)+\left(\sum_{\cap_i A_i=A} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(\Theta)+\left(\sum_{\cap_i A_i=N} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(N)+\left(\sum_{\cap_i A_i=N} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(\Theta)+\left(\sum_{\cap_i A_i=\Theta} m_1(A_1)m_2(A_2)...m_{n-1}(A_{n-1})\right)m_n(\Theta)}\\
&=\frac{m_{1...n-1}(A)K_{n-1}m_n(A)+m_{1...n-1}(A)K_{n-1}m_n(\Theta)+m_{1...n-1}(\Theta)K_{n-1}m_n(A)}{m_{1...n-1}(A)K_{n-1}m_n(A)+m_{1...n-1}(A)K_{n-1}m_n(\Theta)+m_{1...n-1}(N)K_{n-1}m_n(N)+m_{1...n-1}(N)K_{n-1}m_n(\Theta)+m_{1...n-1}(\Theta)K_{n-1}m_n(\Theta)}\\
&=\frac{m_{1..n-1}(A)m_n(A)+m_{1...n-1}(A)m_n(\Theta)+m_{1...n-1}(\Theta)m_n(A)}{m_{1...n-1}(A)m_n(A)+m_{1...n-1}(A)m_n(\Theta)+m_{1...n-1}(N)m_n(N)+m_{1...n-1}(N)m_n(\Theta)+m_{1...n-1}(\Theta)m_n(\Theta)}\\
&=m_{1...n-1}(A)\oplus m_n(A).
\end{aligned}$$

在上述结合律的基础上,由数学归纳法容易证得:

$$m_{1..n}(A)=m_1(A)\oplus m_2(A)\oplus...\oplus m_n(A) \tag{4}$$

而两个证据的组合公式可以在常数时间内运算获得.因此,n 个观察证据的组合信度 $m_{1...n}(A)$的计算可以通过式(4)在 $n-1$ 个步骤内完成,代价为 $O(n)$.因此,本文提出的网络异常检测方法符合检测的高性能需求.

根据上述过程对 n 个网络流特征值的信度分配进行融合,得到综合信度评价,即 $m_{1...n}(A)$,$m_{1...n}(N)$与$m_{1...n}(\Theta)$,分别表示 n 个网络流特征对攻击事件、正常情况与未知的支持信度.然后,根据这 3 个值的最大者给出当前网络流异常、正常或者不能确定是否异常的综合评判.

2.4 网络流自适应机制

网络流量具有实时变化性,即使是同一网络,在不同的时间段也会存在差异.因此,不能总是使用静态不变的系统正常轮廓去检测,而要引入正常轮廓对网络流量变化的自适应机制.

我们实现的自适应机制如图 3 所示.在初期学习阶段,由于还未从足够多的网络流量学习获得可用的轮廓,将不对特征取值进行异常评定,而仅仅将这些特征取值通过学习机制获得网络流量特征轮廓.由于我们并不依赖于完全干净的训练数据,因此需要根据特征取值的概率分布剔除异常取值点,保证轮廓反映了正常的流量特征取值分布.然后进入在线检测阶段,在线检测阶段进行检测的同时,对当前正常的网络流量也进行学习,将原有的轮廓进行老化,并结合新的特征取值分布,获得新的轮廓,提供给下一时刻异常检测使用.

引入网络自适应机制,使得本文的网络异常检测方法能够方便地部署在实际网络上,无须完全干净的训练数据,经过短时间适应训练能够马上发挥效果,并通过对网络流量变化的实时适应能力保证了检测准确性.

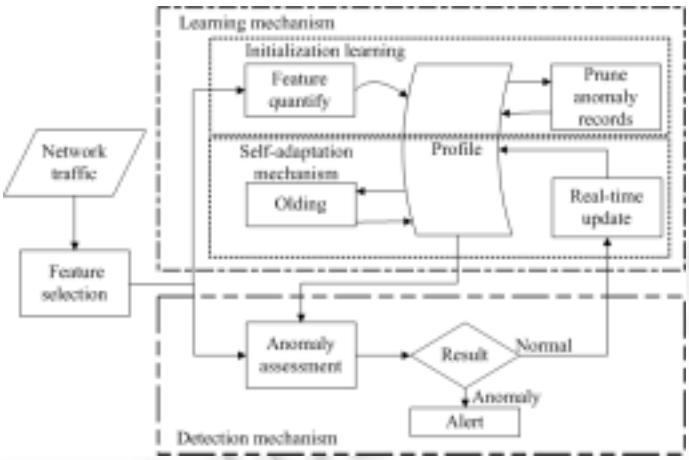

Fig.3 Self-Adaptation mechanism

图 3 网络流量自适应机制

3 原型实现及实验分析

本文提出的基于 D-S 证据理论网络异常检测方法在网络入侵检测原型系统 Morpheus 上进行了实现,作为它的一个检测模块,称为流异常检测器(flow anomaly detector,简称 FAD),并通过基准评测数据集对其进行实验测试.

3.1 测评数据背景

FAD 使用 MIT 林肯实验室开发的 DARPA 1999 年 IDS 评测数据集进行了实验测试.DARPA 1999 年评测数据包括覆盖了 Probe,DoS,R2L,U2R 和 Data 等 5 大类 58 种典型攻击方式,是目前最为全面的攻击测试数据集.同时,作为研究领域共同认可及广泛使用的基准评测数据集,DARPA 1999 年评测数据为新提出的入侵检测算法和技术与其他算法之间的比较提供了可能.DARPA 1999 评测数据给出了 5 周的模拟数据,其中前两周是提供给参于评测者的训练数据:第 1 周为不包含任何攻击的正常数据;第 2 周中插入了属于 18 种类型的 43 次攻击实例.后 3 周的数据则用于评测:第 3 周为正常数据;第 4 周、第 5 周中包含了属于 58 种类型的 201 次攻击实例,其中 40 种攻击类型并没有在前两周的训练数据中出现,属于新的攻击类型.

18 个研究中的 IDS 系统参与了 1999 年的评测,优胜者为 SRI International 提交的 EMERALD 系统,在其检测范围内的 169 个攻击实例中检测出 85 个,检测率为 50%.此外,58 种攻击类型中有 21 种类型共计 77 个攻击实例被划分为 Poor Detected,参与测评的系统最多也仅能检测其中的 15 个攻击实例.

3.2 实验结果

在我们对 FAD 的评测实验中,使用了 Mahoney 实现的报警结果评测工具[4],其所采用的评测标准完全按照 DARPA 在 1999 年对各个参与系统进行评测的方案.我们在 FAD 的实现中采取了如下 8 个网络流特征:

- TGT_SVCNT:一台主机同时被访问的服务类型数量;
- TGT_CLTRSTCNT:一台主机同时被客户端 Reset 的网络流数量;
- PEER_TCPANCNT:一对主机间同时违反 TCP 协议规范的次数;
- SV_SVTYPE:内部网的服务器 IP 及其服务类型;
- SV_FLOWCNT:对一个服务同时发起的网络流数目;
- SV_REQCNT:一个服务中客户端发出的请求包数量;

• TCPFLAG:TCP 的标志位;

• IPFRAG:IP 协议分片长度和分片位.

在 FAD 的一次运行中,我们首先使用第 1 周和第 3 周共 10 天的内部网监听数据文件作为训练数据,之后对第 4 周和第 5 周的内部网监听数据和外部网监听数据都进行检测,得到的检测结果见表 1.

Table 1 Results of FAD evaluation (Based on 1999 DARPA IDS evaluation dataset)

表 **1** FAD 实验结果(DARPA 1999 IDS 评测数据集)

Attack type	Detection rate (false alarm below 10 per day)
Probe	34/37(92%)
DoS	44/65(68%)
R2L	31/56(55%)
U2R/Data	11/43(26%)
New	26/62(42%)
Stealthy	21/36(58%)
All	119/201(59%)
In scope (Probe+DoS+R2L)	109/158(69%)
Poor detected	40/77(52%)

3.3 与相关工作的比较

与本文同样关注于网络异常检测的研究工作较多,本节仅列出使用 DARPA 1999 基准 IDS 评测数据进行测评并公布结果的相关检测系统,并将 FAD 获得的实验结果与它们进行比较.DARPA 1999 评测中获得优胜的 EMERALD[15]系统采用了 eBayes 异常检测部件[2],eBayes 的基本思想是:基于贝叶斯网络模型,通过学习获得各种特征对所属攻击类的条件概率,然后据此对网络流进行分类,判断其是否属于某种攻击.PHAD,ALAD 和 NETAD 是 Mahoney[4]的博士论文中提出的异常检测方法:PHAD 仅关注包头字段特征;ALAD 则使用了应用协议负载中的命令及参数信息进行异常检测;而 NETAD 则结合了包头字段特征和有效负载特征.PAYL 方法[5]则仅对各种应用协议负载中的字符分布进行建模,根据字符的异常分布情况对攻击进行检测.以上 3 种方法虽然都使用了多种特征,但未能将其进行融合评判.同时,使用应用协议负载中的特征,将使得异常检测过程需要处理数据量庞大的负载,其计算代价往往不能适应高速网络流量检测的性能需求.

表 2 给出了 FAD 的实验结果以及与一些同类研究工作的评测结果之间的比较.

Table 2 The comparison of FAD and related work

表 **2** FAD 与相关工作实验结果的对比

System	Detection method	Detection rate	Detection rate in the scope	Detection rate of poor detected attacks
EMERALD	Expert system & anomaly detection	85/201(42%)	85/169(50%)	15/77(19%)
PHAD	Anomaly detection using packet header fields	54/201(27%)	46/102(45%) (Probe+DoS)	17/77(22%)
ALAD	Anomaly detection using application payload	60/201(30%)	35/99(35%) (R2L+U2R+Data)	14/77(18%)
NETAD	Combine PHAD with ALAD	132/201(66%)	132/201(66%)	44/77(57%)
PAYL	Anomaly detection based on application payload distribution	No data	57/97(59%)	No Data
FAD	Anomaly detection based on D-S fusion of multiple flow features	119/201(59%)	109/158(69%) (Probe+DoS+R2L)	40/77(52%)

可以看到,FAD 在只使用传输层以下特征.不涉及应用层有效负载的情况下,达到了较高的检测率,总共检测率超过了 DARPA 1999 年的优胜者 EMERALD,而检测范围内的检测率也略优于结合了包头字段特征和有效负载特征的 NETAD[4].此外,PHAD 和 NETAD 检测攻击中的一大部分依赖于源 IP 地址特征(PHAD:11/54, NETAD:72/132),而 Adamic 等人通过对网站访问源 IP 地址的实验统计数据研究[19]发现,无论训练周期有多长,观察到的新客户源 IP 地址总是会以常数速度增长.因此,源 IP 地址属于异常非一致性特征,不宜用其进行异常评估.PHAD 和 NETAD 对用源 IP 地址特征检测到的大部分攻击无法进行解释,与测评数据中仅包含少量源 IP 地址有关.而在用插入真实背景流量的 DARPA 1999 测评数据进行评测的结果中,也发现了此特征的检测攻击

数量大为减少[4].另外,FAD 对 DARPA 1999 年测评中检测最不理想的几类攻击(隐蔽的 portsweep,ipsweep,queso 等)的检测率也达到了 52%,比测评中最好的 19%的结果有较大提高,仅略低于总共检测率.这也说明 FAD 对大部分隐蔽攻击的检测是理想的.

4 结 论

D-S 证据理论作为一种新兴的不确定性推理理论,已经被用于多传感器网络、医学诊断等领域.本文探讨了其在网络异常检测领域中的应用,提出了一种基于 D-S 证据理论的网络异常检测方法,并使用 DARPA 1999 年 IDS 基准评测数据进行了实验,得出的实验结果表明,该算法在较低误报率的基础上达到了理想的检测率,与相关研究工作的实验结果的对比分析也说明该算法具有相当的优势.随着多源异构分布式入侵检测系统的发展,可以预见 D-S 证据理论在入侵检测领域内的应用将越来越广泛.

本文提出的网络异常检测方法还需要在某些方面做进一步的研究,包括:扩展数据源,使其能够融合主机上获取的一些特征;在能够获取部分攻击数据的前提下,研究如何学习获得每个特征的区分度和覆盖率,并据此确定在多特征融合时其所占的权重大小等.

References:

[1] Heberlein L, Dias GV, Levitt KN, Mukherjee B, Wood J, Wolber D. A network security monitor. In: Proc. of the IEEE Computer Society Symp. Research in Security and Privacy. 1990. 296−304. http://seclab.cs.ucdavis.edu/papers/pdfs/th-gd-90.pdf

[2] Valdes A, Skinner K. Adaptive, model-based monitoring for cyber attack detection. In: Debar H, Mé L, Wu SF, eds. Proc. of the 3rd Int'l Workshop on the Recent Advances in Intrusion Detection (RAID 2000). LNCS 1907, Heidelberg: Springer-Verlag, 2000. 80−92.

[3] Staniford S, Hoagland JA, McAlerney JM. Practical automated detection of stealthy portscans. Journal of Computer Security, 2002,10(1/2):105−136.

[4] Mahoney VM. A machine learning approach to detecting attacks by identifying anomalies in network traffic [Ph.D. Thesis]. Melbourne: Florida Institute of Technology, 2003.

[5] Wang K, Stolfo SJ. Anomalous payload-based network intrusion detection. In: Jonsson E, Valdes A, Almgren M, eds. Proc. of the 7th Int'l Symp. on Recent Advances in Intrusion Detection (RAID 2004). LNCS 3224, Heidelberg: Springer-Verlag, 2004. 203−222.

[6] Krugel C, Toth T, Kirda E. Service specific anomaly detection for network intrusion detection. In: Lamont GB, Haddad H, Papadopoulos G, Panda B, eds. Proc. of the 2002 ACM Symp. on Applied Computing. New York: ACM Press, 2002. 201−208.

[7] Lee W, Stolfo SJ. A framework for constructing features and models for intrusion detection systems. ACM Trans. on Information and System Security, 2000,3(4):227−261.

[8] Manikopoulos C, Papavassiliou S. Network intrusion and fault detection: A statistical anomaly approach. IEEE Communications Magazine, 2002,40(10):76−82.

[9] Zhang J, Gong J. An anomaly detection method based on fuzzy judgment. Journal of Computer Research and Development, 2003,40(6):776−783 (in Chinese with English abstract).

[10] Aickelin U, Greensmith J, Twycross J. Immune system approaches to intrusion detection—A review. In: Nicosia G, *et al*., eds. Proc. of the 3rd Int'l Conf. on Artificial Immune Systems. LNCS 3239, Heidelberg: Springer-Verlag, 2004. 316−329.

[11] Rao X, Dong CX, Yang SQ. An intrusion detection system based on support vector machine. Journal of Software, 2003,14(4): 798−803 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/798.htm

[12] Li KL, Huang HK, Tian SF, Liu ZP, Liu ZQ. Fuzzy multi-class support vector machine and application in intrusion detection. Chinese Journal of Computers, 2005,28(2):274−280 (in Chinese with English abstract).

[13] Xiao Y, Han CH, Zheng QH, Wang Q. Network intrusion detection method based on multi-class support vector machine. Journal of Xi'an Jiaotong University, 2005,39(6):562−565 (in Chinese with English abstract).

[14] McHugh J. Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA offline intrusion detection system evaluation as performed by lincoln laboratory. ACM Trans. on Information and System Security, 2000,3(4):262−294.

[15] Porras PA, Neumann PG. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In: Proc. of the 20th National Information Systems Security Conf. Baltimore. 1997. 353−365. http://www.csl.sri.com/papers/emerald-niss97/

[16] Dempster A. Upper and lower probabilities induced by multivalued mapping. Annals of Mathematical Statistics, 1967,38(2): 325−339.

[17] Siaterlis C, Maglaris B. Towards multisensor data fusion for DoS detection. In: Haddad HM, Omicini A, Wainwright RL, Liebrock LM, eds. Proc. of the 2004 ACM Symp. on Applied Computing. New York: ACM Press, 2004. 439−446.

[18] Orponen P. Dempster's rule of combination is #P-complete. Artificial Intelligence, 1990,44(1-2):245−253.

[19] Adamic LA, Huberman BA. Zipf's law and the Internet. Glottometrics 3, 2002. 143−150.

附中文参考文献:

[9] 张剑,龚俭.一种基于模糊综合评判的入侵异常检测方法.计算机研究与发展,2003,40(6):776−783.

[11] 饶鲜,董春曦,杨绍全.基于支持向量机的入侵检测系统.软件学报,2003,14(4):798−803. http://www.jos.org.cn/1000-9825/14/798.htm

[12] 李昆仑,黄厚宽,田盛丰,刘振鹏,刘志强.模糊多类支持向量机及其在入侵检测中的应用.计算机学报,2005,28(2):274−280.

[13] 肖云,韩崇昭,郑庆华,王清.一种基于多分类支持向量机的网络入侵检测方法.西安交通大学学报,2005,39(6):562−565.

诸葛建伟(1980－),男,浙江瑞安人,博士生,主要研究领域为入侵检测与关联分析,蜜罐与蜜网技术,网络攻防技术.

叶志远(1963－),男,高级工程师,主要研究领域为网络与信息安全.

王大为(1977－),女,硕士生,主要研究领域为入侵检测.

邹维(1964－),男,研究员,主要研究领域为网络与信息安全.

陈昱(1966－),男,副研究员,主要研究领域为入侵检测与关联分析,模式识别.