基于DSimC和EWDS的网络安全态势要素提取方法

赖积保[1,2] 王慧强[3] 郑逢斌[1] 冯光升[3]
(河南大学计算机与信息工程学院 开封 475004)[1] (中国科学院遥感应用研究所 北京 100101)[2]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[3]

摘 要 为了融合多源异构的网络安全信息,提取反映网络整体安全状况的要素信息,提出了一种基于相异度计算和指数加权DS证据理论的网络安全态势要素提取方法,该方法包括多源报警聚类和融合两个阶段。针对多源报警的不同阶段,首先研究一种基于DSimC的多源报警聚类方法,即通过计算报警之间的不同类型特征相异度来判断报警之间的相似程度;其次研究一种基于EWDS的多源报警融合方法,即通过融合不同数据源所提供的证据综合识别入侵攻击行为。实验结果表明,所提出的方法在TPR、FPR和DIR指标方面均取得了不错的效果,克服了单个安全设备误报率和漏报率高的问题,为进一步的网络安全态势评估和预测提供了有力的数据保障。

关键词 网络安全态势,要素提取,相异度计算,指数加权DS证据理论
中图法分类号 TP393 **文献标识码** A

Network Security Situation Element Extraction Method Based on DSimC and EWDS

LAI Ji-bao[1,2] WANG Hui-qiang[3] ZHENG Feng-bin[1] FENG Guang-sheng[3]
(School of Computer and Information Engineering, Henan University, Kaifeng 475004, China)[1]
(Institute of Remote Sensing Applications, Chinese Academy of Sciences, Beijing 100101, China)[2]
(College Computer Science & Technology, Harbin Engineering University, Harbin 150001, China)[3]

Abstract For the sake of fusing multi-source heterogeneous security information and extracting security element information about the whole network, a network security situation element extraction method based on Dissimilarity Computing (DSimC) and Exponentially Weighted DS Evidence Theory (EWDS) was proposed. The method was divided into two phases including multi-source alert clustering and alert fusing. First of all, multi-source alert clustering method was put forward through computing different characteristics dissimilarity of alert to judge the dissimilarity among alerts. Then multi-source alert fusion method based on EWDS was proposed through fusing different sources to indentify intrusion attack behaviors. Experimental results indicate that the proposed method does well in True Positive rate (TPR), False Positive rate (FPR) and Data to Information Rate (DIR), remarkably reduces the number of alerts and enhances detection performance, and supplies data sources for network security situation evaluation and situation prediction.

Keywords Network security situation, Element extraction, Dissimilarity computing, Exponentially weighted DS evidence theory

随着网络的不断推广使用,其规模日趋庞大,入侵攻击也正朝着规模化、复杂化和智能化的方向发展,给网络带来的各种威胁越来越多,造成的损失也越来越大。在这种形势下建立了以入侵检测、防火墙、防病毒系统等一系列安全设备为基础的纵深防御体系,但随之也出现了一些新的问题。首先,入侵检测系统本身存在较高的误报率、漏报率,同时随着安全系统的不断增加,各类报警信息及日志呈数量级增长,使安全管理员面对如此大量的信息很难了解系统的安全威胁状况,无法及时采取有效的响应措施;其次,同一个攻击往往会在多个安全设备上留下痕迹,如何有效地利用这些安全设备所提供的安全信息进行互补,从不同侧面反映攻击的影响,降低报警的冗余度,使入侵的检测和识别更加准确、有效等问题有待解决;再次,分布式攻击增长速度很快,缺乏时空域上的关联,难以发现完整的攻击场景。在这种情况下,迫切需要一种有效的多源异构安全信息分析处理技术。

本文提出一种基于DSimC和EWDS的网络安全态势要素提取方法,针对多源报警的不同阶段采用不同的方法予以处理。经仿真实验证实,所提出的方法在TPR、FPR和DIR指标方面均取得了不错的效果。第2节介绍相关工作;第3节构建网络安全态势要素提取模型;第4节研究基于DSimC

到稿日期:2009-12-28 返修日期:2010-03-09 本文受国家863计划(2007AA01Z401)和国家自然科学基金(90718003,60973126)资助。
赖积保(1982—),男,博士,主要研究方向为网络安全、空间数据处理等,E-mail:laijibao@163.com;**王慧强**(1960—),男,教授,博士生导师,主要研究方向为可信网络与信息安全、自律计算等;**郑逢斌**(1963—),男,教授,主要研究方向为自然语言理解、空间数据处理等;**冯光升**(1980—),男,博士,主要研究方向为信息安全、认知网络等。

的报警聚类方法；第 5 节研究基于 EWDS 的报警融合方法；第 6 节是实验与结果分析；最后是本文结论。

1 相关工作

多源安全信息融合和关联处理最初主要是针对 IDS 重复报警、误报率和漏报率过高等问题提出的，用于弥补单一 IDS 检测能力有限的缺陷。所采用的方法主要分为两类：一类是概率关联，另一类是因果关联[1]。Dain 等人[2]使用数据挖掘的方法获得攻击过程，依据人类专家知识或数据挖掘方法获得合适的聚合与关联模板，该模板既可以实现聚合也可以实现关联，实时性好，有利于在此基础上进行深入的报警处理。但由于各方面的不确定性很难获得合适的训练集，同时存在过学习问题，不能处理在训练集中未出现的攻击过程模式，并且这种模板匹配方法抗噪能力较差，Anderson 等人[3]提出一种基于 Snort 和 Emerald 的报警信息关联方法，充分利用了二者的互补性，进一步降低了误报率。Valdes 等人[4]提出了一种基于概率相似度的报警关联算法，将相似度接近的报警聚集在一起，但概率相似度的定义方法过多依赖于先验知识且只能兼容 SRI 的 Emerald 系统。Peng Ning 等人[5]提出了一种基于逻辑谓词的方法，将因果关系的入侵报警进行关联，这种方法需要对每类攻击分别定义其前因后果，可扩展性不强。Yu Jinqiao 等人[6]提出一种基于 NIDS 和 HIDS 的综合报警处理方法。黄厚宽等人[7]提出了一种基于模糊综合评判的方法来处理入侵检测系统的报警信息、关联报警事件，并引入有监督的确信度学习方法，通过确信度来对报警信息进行进一步的过滤。田俊峰等人[8]提出了一种基于多 IDS 的入侵检测融合模型，然而这种安全信息融合关联方法仍局限于 IDS 本身，属于同种类型的报警处理，从根本上无法克服 IDS 固有的误报、漏报过高等缺陷。

而随着信息安全保障所呈现出来的实时化、一体化等特点，多源安全信息处理也正由同类型安全信息之间的融合处理逐渐转向多源异构安全信息的融合处理。Wenke Lee 等人[9]提出了一种基于统计因果分析的异构安全事件关联方法，但在处理时不同报警的威胁度优先级多依赖于经验知识。B. X. Fang 等人[10]提出了一种结合 Nessus 和 Snort 的报警关联方法，该方法针对非常依赖具体漏洞的攻击行为（如 U2R 和 R2L）具有较好的检测效果，但对于不是非常依赖漏洞的攻击行为（如 DDOS 和 Probe）和复杂度较高的缓冲区溢出攻击则无法检测。诸葛建伟等人[11]提出了一种基于 DS 证据理论的网络流异常检测方法，通过融合多个特征对网络流量进行综合评判，该方法仅采用网络流作为数据源，而未考虑主机安全日志信息。

目前针对多源信息融合关联的研究主要集中在 IDS 报警信息的“二次处理”上，而对于不同种类安全设备所提供的安全信息处理研究较少，所提出的方法大都未能充分考虑各安全设备之间的互补性，存在诸如语义理解差异、简单关联等问题。在这种情况下，本文尝试研究一种基于相异度计算（DSimC）和指数加权 DS 证据理论（EWDS）的网络安全态势要素提取方法，该方法既充分考虑各安全设备之间的互补性，又能有效提取反映网络安全态势的要素，为下一步的网络安全态势评估和预测提供了数据支持。

2 网络安全态势要素提取建模

针对各个安全传感器所提供的数据，如果没有一个合适的模型对其进行综合处理，很多有用的安全信息将被淹没在大量的噪声中，并且会极大地降低时效性，无法为上层的网络安全态势评估和预测提供必要的数据支持，因此开展网络安全态势要素提取的研究是至关重要的。所提取的要素主要包括攻击要素、漏洞要素、资产要素等，而其中攻击要素对于网络安全态势研究来说是最为重要的，并且该要素也能在一定程度上反映出漏洞要素和资产要素，因此本文提取的对象主要是攻击行为。图 1 给出了网络安全态势要素提取模型，它主要包括报警聚类和报警融合两大部分，逐步实现报警信息的时间和空间融合，达到要素提取的目的。各传感器采集和初步分析来自多源异构环境的数据，这些数据主要包括有诸如入侵检测系统（IDS）、防火墙（Firewall）、病毒检测系统（VDS）等安全设备的报警信息、系统日志信息等；随后采用报警验证算法对报警信息进行检测和验证，并使用 IDMEF XML 对验证后的信息进行格式统一；经初步处理之后的报警提交到报警聚类模块，依据格式化后的安全信息相似度进行聚类，分类结果包括有类别 1、类别 2 等。报警融合是在报警聚类的基础上，通过各传感器之间安全信息的互补性，更加准确地定位入侵攻击行为，精简报警数量，有效地降低误报率和漏报率。输出结果有 DDOS，PROBE，U2R，R2L 以及其他信息。

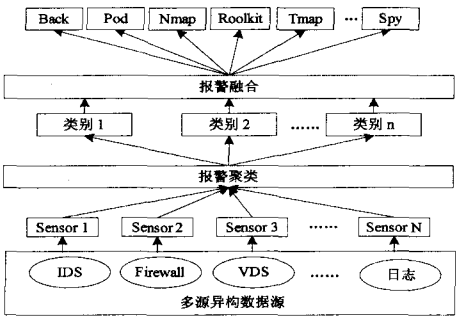

图 1 多源异构网络安全态势要素提取模型

3 基于相异度计算（DSimC）的报警聚类

报警聚类的目的是依据来自不同 IDS 或其它安全部件产生的报警，将属同类的报警划分到同一个报警集合中。由于发生报警的时间、源/目的地址等不同，同属一个报警类别集合的信息需要根据特征进行相关度计算，并依据计算结果进行聚类，聚类后的报警集合可视为一个独立的报警体。由此可见，聚类的关键问题是定义两个报警之间的相似性，只有相似程度比较高的报警才能进行聚类。本文采取相关属性距离计算方法对报警进行聚类，通过计算每一个报警的特征之间距离，并依据事先设定的相应阈值，进行报警类别判断。假设有报警 $Alert_i=\{$ Src_IP, Src_Port, Dst_IP, Dst_Port, Time, Attack_Type, Other $\}$ 和报警 $Alert_j=\{$ Src_IP, Src_Port, Dst_IP, Dst_Port, Time, Attack_Type, Other $\}$，不同类型属性相异度的计算方法不同，通过计算 IP、端口、时间等属性之间的相异度来表示属性的相似度。报警属性的类型主要包括有数值型、布尔型和枚举型，采用数据挖掘[12]方法分别对其进行计算。图 2 给出基于相异度计算的报警聚类算法（Dissimila-

rity Computing-based Alert Clustering,DCAC)。以新来的报警作为输入,并与当前的报警逐一进行相异度计算,因此该算法的时间复杂度为 $O(i \cdot m)$。不难看出,本算法判断新来报警是否属于同一个报警类别,取决于设定的阈值。如果相异度不大于这个设定的阈值,那么新来的报警可以划分到同一个报警类别中去。所以说阈值的设定对于聚类结果的影响是很大的,合理的阈值可以通过在具体的实验环境下对聚类算法进行训练得到。

输入:经过格式化和验证的报警 $Alert_j$

输出:最终分类结果

```
Begin
    Threshold /* 初始化,依据经验设定相异度阈值 */
    D=+∞ /* 设定初始相异度为最大值 */
    Alert_database={Alert1,Alert2,……,Alerti}
     /* 初始化报警数据库 */
    k=1 /* 计数器 */
    While (k<=i) do
      begin
        Get(Alert_database(k)) /* 从报警数据库中取第 k 个报警
*/
        Compute(d(Alertj,Alertk)) /* 计算 Alertj 和 Alertk 相异
度 d */
        If (d<D) then
          D=d /* 更新为当前相异度 */
        else
          k=k+1 /* 更新计数器 */
        end
    if (D>Threshold) then
        Add(new_alert_class) /* 添加一个新报警类别 */
        else
            Add(new_alert) /* 添加一个新的报警到已有类别中
*/
End
```

图 2 DCAC 算法

4 基于指数加权 DS 证据理论(EWDS)的报警融合

4.1 DS 证据理论

DS 证据理论[13]是建立在非空有限域 Θ 上的理论,Θ 称为识别框架,表示有限个系统状态$\{\theta_1,\theta_2,\cdots,\theta_n\}$。而假设系统状态 H_i 为 Θ 的一个子集,即 Θ 的幂集 $P(\Theta)=2^{\Theta}$ 的一个元素。其目标是仅根据系统状态的观察 $E_1,E_2,\cdots,E_m$ 推测出的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 DS 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,称为基本概率赋值。

定义 1 基本概率赋值可描述为从 Θ 的幂集到$[0,1]$区间的映射:

$$m:2^{\Theta}\to[0,1],m(\phi)=0,\sum_{A\subset\Theta}m(A)=1 \tag{1}$$

4.2 Dempster 组合规则

假定 $A\subset\Theta$,$m_1(A_1)$和 $m_2(A_2)$是 2^{Θ} 上互相独立的基本概率赋值,则组合这两个证据的基本概率赋值可定义为

$$m(A)=m_1\oplus m_2(A)=\frac{\sum_{A_1\cap A_2=A}m_1(A_1)m_2(A_2)}{1-K},\text{当 } K\neq 1,K=\sum_{A_1\cap A_2=\phi}m_1(A_1)m_2(A_2) \tag{2}$$

$$m_1\oplus m_2(\phi)=0 \tag{3}$$

对于 n 个证据进行组合的 Dempster 一般化规则可定义为

$$m_1\oplus m_2\oplus\cdots\oplus m_n(A)=\frac{\sum_{\bigcap_{i=1}^{n}A_i=A}m_1(A_1)m_2(A_2)\cdots m_n(A_n)}{1-K},$$

$$\text{当 } K\neq 1,K=\sum_{\bigcap_{i=1}^{n}A_i=\phi}m_1(A_1)m_2(A_2)\cdots m_n(A_n) \tag{4}$$

$$m_{1\cdots n}(\phi)=0 \tag{5}$$

4.3 指数加权 DS 证据理论

DS 证据理论对于解决非冲突的评价合成问题是非常有效的,但对于来自于不同传感器的证据在同一识别框架 Θ 下的作用如果不是完全一致的(即证据间存在冲突),用传统 DS 证据理论无法直接予以解决。用式(5)中的 k 来表示证据间的冲突程度,k 值越大,说明证据间的冲突越大,反之,说明证据间的冲突越小。究其原因主要有两方面:一是与传感器本身有关,由于传感器设计缺陷或外界干扰而导致出现误报的情况;二是来自 mass 函数本身,即组合规则对于不同传感器所提供的证据是同等对待的,而实际情况并非如此。就同一类传感器来说,本地传感器应该比远程传感器所提供的证据更加可信,并且更加及时[14];即使完全相同的传感器部署在不同的位置亦会有不同的检测能力;另外,不同的传感器对于同一攻击的检测能力和精度也是不一样的,例如某一传感器检测 DDOS 攻击时的检测率高达 90%,而检测 Local to Root (L2R)时的检测率仅仅为 50%;另外,某一基于主机的传感器根本就不能检测到 DDOS 攻击,但是在检测 L2R 时有非常高的精确度。在这种情况下,应该给予第一类传感器在检测 DDOS 时更高的可信度,而第二类传感器在检测 L2R 时给予了更高的可信度,最终目的是为融合提供的证据能确实反映其重要性和可信性。为了解决上述情况,提出了一种指数加权的 DS 证据理论,通过赋予不同的权重值来区分各个传感器所提供证据的重要性和可信性,并把每个传感器对攻击的识别率作为相应报警的基本置信度,表示如下:

$$m(A)=m_1\oplus m_2(A)=\frac{\sum_{A_1\cap A_2=A}[m_1(A_1)]^{w_1}[m_2(A_2)]^{w_2}}{1-k},\text{当 } K\neq 1,K=\sum_{A_1\cap A_2=\phi}[m_1(A_1)]^{w_1}[m_2(A_2)]^{w_2} \tag{6}$$

$$m_1\oplus m_2(\phi)=0 \tag{7}$$

式中,w_1 和 w_2 分别表示传感器对应元素的权重。当 $w_1=w_2$ 时,式(7)和传统 DS 组合规则是一样的。对于 n 个证据进行组合的 Dempster 一般化规则可定义为

$$m_1\oplus m_2\oplus\cdots\oplus m_n(A)=\frac{\sum_{\bigcap_{i=1}^{n}A_i=A}[m_1(A_1)]^{w_1}[m_2(A_2)]^{w_2}\cdots[m_n(A_n)]^{w_n}}{1-K} \tag{8}$$

$$m_{1\cdots n}(\phi)=0 \tag{9}$$

式中,$K\neq 1,K=\sum_{\bigcap_{i=1}^{n}A_i=\phi}[m_1(A_1)]^{w_1}[m_2(A_2)]^{w_2}\cdots[m_n(A_n)]^{w_n}$。$w_i(i=1,2,\cdots,n)$表示 n 个传感器所对应元素的权重。当 $w_1=w_2=\cdots=w_n$ 时,式(8)与传统 DS 组合规则是一致的。权值的确定依据传感器对于不同攻击的检测能力历史

统计数据，采用最大熵准则和最小均方差来分析实验样本，给出传感器所对应攻击的权重区间，如表 1 所列。指数加权 DS 证据理论也能在一定程度上解决证据之间的冲突，这种解决冲突的思想与文献[15]中的思想相似。

表 1　传感器的权值

检测能力	权值
强	[0.7,1]
中	[0.4,0.7]
弱	[0,0.4]

4.4　融合决策方法

在采用 DS 证据理论得到组合后的基本概率分配值之后，需要对其进行决策判断。采用基本概率函数 m 的融合决策，其基本思路是假设 $\exists A_1, A_2 \subset \Theta$ 且满足如下条件。

$$m(A_1)=\max\{m(A_i), A_i \subset \Theta\} \tag{10}$$

$$m(A_2)=\max\{m(A_i), A_i \subset \Theta, \text{且 } A_1 \neq A_2\} \tag{11}$$

$$\text{若有} \begin{cases} m(A_1)-m(A_2)>\varepsilon_1 \\ m(\Theta)<\varepsilon_2 \\ m(A_1)>m(\Theta) \end{cases} \tag{12}$$

式中，A_1 即为判决结果，ε_1 和 ε_2 为预先设定的门限值。

4.5　基于 EWDS 的报警融合算法

对于聚类后的报警分类结果进行融合有很多方法。采用基于 EWDS 的报警融合，主要是因为 EWDS 证据理论具有以下几方面的优势：其一，证据组合规则能够有效地融合多源异构安全传感器的信息，同时随着证据的积累，判断将会更加清晰、准确；其二，证据理论不需要先验概率和条件概率，而网络环境中的入侵攻击行为具有很大的随机性和不确定性，其先验知识很难获取；其三，证据理论具有很好的可扩展性，随着各种网络安全技术的发展，会不断涌现一些新的安全传感器，DS 证据理论可以很方便地将这些新安全传感器的证据加进去，而无需改变原有的要素体系框架结构；其四，依据攻击在不同传感器中的重要性和可信性差异，可以动态调整组合策略，确保获得较高的识别精确度。

图 3 是基于 EWDS 的报警融合算法。主要分为两个阶段：一个是算法训练阶段，一个是算法测试阶段。训练阶段的主要任务是尽可能地获得每种传感器对于攻击的识别率和权重分配；测试阶段的主要任务是通过融合多源证据进一步识别攻击。通过对报警的聚类和融合分析，不仅精简了攻击报警数量，而且完成了对入侵攻击的识别，达到了态势要素提取的目的。

```
输入：报警分类结果
输出：攻击识别结果
Begin
/* Training Phase */
Begin
  Get(DPR_i^sk) /* 依据训练样本，获取每种传感器对攻击的识别率 DPR */
  Initial(w_i^sk)/* 依据训练样本，初始化各传感器对攻击的权重分配 w_i=1,2,…,n,sk=1,2,…m */
  Initial(ε1,ε2) /* ε1 和 ε2 用于融合判决 */
End
/* Testing Phase */
/* 假设有 t 个攻击类型报警 */
Begin
  for sk:= 1 to m do
    for j:= 1 to t do
    Begin
      m_sk(A_j)=DPR_j^sk
/* 第 sk 个传感器对 A_j 的基本置信度赋予其相应识别率 */
      W_j^sk=w_j^sk/* 获得第 sk 个传感器对 A_j 的权重 */
    End
    Compute(m(A_j)) /* 计算综合置信度 */
    /* 依据式(8)和式(9)，融合判断 */
    Compute(m(A1))
    Compute(m(A2))
    if ((m(A1)-m(A2)>ε1) and (m(Θ)<ε2) and (m(A1)>m(Θ)) then
      Identify(A1)
End
```

图 3　基于 EWDS 的报警融合算法

5　实验与结果分析

为了验证所提出的安全态势要素提取方法的可行性和有效性，搭建了如图 4 所示的实验环境。该实验环境是封闭的，主要分为 DMZ(Demilitarized Zone)和内部网络两部分。该环境中包括 Windows 2000 主机、Windows XP 主机、Red hat 9.0主机、运行了 IIS 服务的 Windows XP 主机、运行了 Apache 服务的 Linux 主机等，开启的服务包括 WWW，FTP，DNS，HTTP，MAIL，TELNET 等，并且安装了 IDS，Firewall，VDS 等安全设备，通过 Router，Switch 等将所有的设备进行互联，并部署所实现的 Netfow 传感器、SNMP 传感器、日志传感器以及服务传感器进行信息获取。

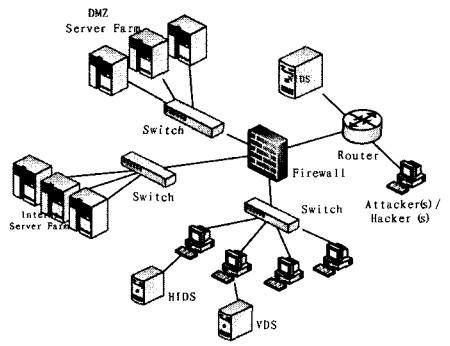

图 4　网络安全态势要素提取实验环境

采用 Netpoke 工具在所搭建的实验环境中重放 KDD CPU 1999[16]。该数据集包含 5 周的网络数据，包括 Probe，U2R，DOS 和 R2L 等类型的攻击。在本实验中将原始数据分为训练样本和测试样本。其中训练样本主要由前 3 周的原始数据组成，共包含有 494020 条连接记录；测试样本主要由第 4 周和第 5 周的原始数据组成，共包含有 311029 条连接记录。通过所部署的传感器获取 IDS，Firewall，VDS 等设备的报警信息，并进行报警验证和格式化，然后在此基础上，进行报警聚类和融合。此外，在进行报警聚类和融合时需要注意：①采用训练样本对聚类阈值、攻击识别率和攻击权重进行训练；②报警聚类和融合方法性能指标不仅反映在检测率、误报率上，而且应该反映在报警的精简程度以及攻击的识别率上。

5.1　评价指标

为了评价算法性能，采用检测率、误报率和精简率 3 个指

标来刻画。其中漏报率和误报率体现算法的检测能力，精简率则体现算法的冗余处理能力。

定义 2(检测率 TPR，True Positive Rate) 系统检测出的入侵攻击行为记录在总入侵攻击行为记录数中所占的比例。

定义 3(误警率 FPR，False Positive Rate) 被系统错误地检测为入侵攻击行为记录的正常行为记录数在总的正常行为记录数中所占的比例。

定义 4(精简率 DIR，Data to Information Rate)[17] 系统所发现的全体报警与所发现攻击之间的比例。

DIR 越小，说明方法的精简能力越强。反之，则说明方法的精简能力越弱。DIR=1 时，是一种非常理想的状态，说明一种攻击对应于一条报警；DIR<1 时，说明存在对攻击的漏报；DIR>1 时，说明存在对攻击的重复报警。这 3 个指标能很好地度量一个态势要素提取算法的性能，因为一个好的要素提取算法是要尽量多地检测出入侵攻击行为记录(TPR)，同时使得被误检测为入侵攻击行为记录的正常行为的记录尽量地少(FPR)，并能取得较为满意的攻击精简率(DIR)。

5.2 报警聚类实验

为了进一步精简经过验证和格式化的报警，便于报警的后续高效处理(主要包括攻击的精确定位和综合态势处理)，采用本文所提出的方法对所获取的报警进行聚类。

5.2.1 聚类阈值的确定

聚类阈值的确立对于报警聚类的成败至关重要。在所提供的 3 周训练样本上进行训练，使之在正确识别警报类型的同时，能够合理地对警报进行聚类。表 2 显示经过该数据集实验所获得的部分较为理想的聚类阈值。可以看出，端口扫描、R2L、U2R 和拒绝服务攻击的警报聚类的条件是源地址和目的地址分别完全匹配。另外，从分布式拒绝服务攻击警报聚类满足的条件可以看出，该类攻击是在一时间段内，由大量的不同主机向同一台主机发起攻击，属于未知类别的警报聚类须满足完全匹配。

表 2 聚类阈值

AlertClass	SourceIP	TargetIP	SourcePort	TargetPort	Time(s)
PortScan	0	0	+∞	+∞	360
R2L	0	0	0	+∞	120
U2R	0	0	+∞	0	120
DoS	0	0	+∞	+∞	240
DDoS	+∞	0	+∞	+∞	240
Other	15	0	+∞	+∞	480

5.2.2 聚类结果及对比分析

为了便于与同类方法比较，在如图 4 所示的环境中，按照最大覆盖原则配置 RealSecure Network Sensor 6.0来监控网络中的数据包。测试结果如表 3 所列。本文所提出的警报聚类方法在检测率上几乎达到了 RealSecure Network Sensor 6.0的水平，而误报率大幅度降低。产生这种效果的主要原因是报警通过多源异构信息的相互验证和聚类，去除了与系统无关的攻击所产生的误报警。从实验结果可以清晰地发现，这部分误报警占总误报警的绝大部分，而报警数量的精简主要依赖于报警验证和聚类。

表 3 报警聚类实验结果及比较

检测区域	实际攻击数目	检测工具	全体警报	发现攻击	TPR(%)	真实警报	FPR(%)
DMZ	628	Real-Secure	6268	392	62.42	547	91.27
		Our method	669	374	59.53	532	20.49
Inside	227	Real-Secure	2728	140	61.67	194	92.89
		Our method	242	135	59.47	191	21.07

5.3 报警融合实验

在报警聚类的基础上，选取同一个时间窗口内分别来自 IDS，Firewall，VDS 的报警共 147 条。其中 IDS 产生了 61 条报警，Firewall 产生了 50 条报警，VDS 产生了 36 条报警。表 4 给出了在这个时间段内 IDS、Firewall 和 VDS 对应 Port_Scan 攻击、DNS_Attack 攻击、ICMP_Attack 攻击、Web_Attack 攻击、Http_Attack 攻击、TCP_Attack 攻击、FTP_Overflow 攻击所产生报警的分布情况。

表 4 IDS，Firewall 和 VDS 对应的报警情况

描述 \ 来源	IDS	Firewall	VDS	报警总数
Port_Scan	17	13	5	35
DNS_Attack	3	2	1	6
ICMP_Attack	18	4	11	33
Web_Attack	5	2	2	9
Http_Attack	6	11	5	22
TCP_Attack	3	16	7	26
FTP_Overflow	9	2	5	16

将 IDS、Firewall 以及 VDS 针对 Port_Scan 攻击、DNS_Attack 攻击、ICMP_Attack 攻击、Web_Attack 攻击、Http_Attack 攻击、TCP_Attack 攻击、FTP_Overflow 攻击的检测率作为它们相应的置信度，表 5 给出了 3 种安全设备分别对应同一攻击的不同检测率。依据 DS 证据理论要求，对表 5 中的检测率进行归一化后将其作为每一种攻击的置信度(m)，表 6 给出了对应每一种攻击对应的置信度。

表 5 IDS，Firewall 和 VDS 对应攻击的检测率

描述 \ 来源	IDS	Firewall	VDS
Port_Scan	0.9	0.8	0.6
DNS_Attack	0.6	0.8	0.1
ICMP_Attack	0.4	0.2	0.3
Web_Attack	0.3	0.3	0.2
Http_Attack	0.7	0.6	0.8
TCP_Attack	0.2	0.7	0.5
FTP_Overflow	0.8	0.4	0.7

表 6 IDS，Firewall 和 VDS 对应攻击的归一化检测率

描述 \ 来源	IDS	Firewall	VDS
Port_Scan	0.2308	0.2105	0.1875
DNS_Attack	0.1538	0.2105	0.0313
ICMP_Attack	0.1026	0.0526	0.0937
Web_Attack	0.0769	0.0789	0.0625
Http_Attack	0.1795	0.1579	0.2500
TCP_Attack	0.0513	0.1842	0.1563
FTP_Overflow	0.2051	0.1053	0.2187

运用式(4)，充分融合 3 种安全设备所提供的攻击基本置信度，得到每一种攻击的总置信度，表 7 给出了采用传统 DS 证据理论融合后的结果。从融合结果我们可以清晰地看出，Port_Scan 攻击、Http_Attack 攻击和 FTP_Overflow 攻击置信度明显大于 DNS_Attack 攻击、ICMP_Attack 攻击、Web_Attack 攻击和 TCP_Attack 攻击，由此可以基本判断网络中

正在进行 Port_Scan 攻击、Http_Attack 攻击和 FTP_Overflow 攻击，提醒安全管理人员重点关注，予以确认并调整相应的 IDS，Firewall 以及 VDS 等安全设备的策略，及时遏制攻击的进一步蔓延，以免带来不必要的损失，并有效地降低各种安全设备的误报率和漏报率。与此同时，我们也可以发现，3种置信度大的攻击所产生的报警数不一定是最多的，所以不能简单地依赖报警数量来判断是否发生攻击。在实验中虽然 ICMP_Attack 和 TCP_Attack 所产生的报警数很多，但是经管理员确认发现均为误报。究其原因是链路不可达，产生了大量得不到响应的 ICMP_Packet 和 TCP_Packet，而非认为的恶意攻击。但超过了系统的处理能力，所以 IDS 或 Firewall 或 VDS 将其当成了 ICMP_Attack 或 TCP_Attack。由此可以看出，融合算法确实能达到报警之间的互补和精简报警的目的，并能对部分攻击进行较为精确的定位。

表 7　DS 融合后 7 种攻击的总置信度

描述 \ 融合	总置信度
Port_Scan	0.3750
DNS_Attack	0.0417
ICMP_Attack	0.0208
Web_Attack	0.0156
Http_Attack	0.2917
TCP_Attack	0.0608
FTP_Overflow	0.1944

通过进一步分析，发现表 7 中 DNS_Attack 攻击确实发生，但是经过融合后置信度却变为 0.0417。究其原因是 VDS 本身针对该攻击的检测能力就非常差，而传统 DS 证据理论却将各传感器所提供的证据同等对待，才导致这种结果的出现。在这种情况下，及时、动态地调整权重，对于 DNS_Attack 重新分配 IDS，Firewall，VDS 的权重(1，1，0.4)，其他不变。表 8 给出了采用动态调整策略的指数加权 DS 证据理论组合结果。从中我们也能发现，经过及时调整后的结果不仅能反映原来的攻击结果，而且更加符合实际真实情况。图 5 给出了分别采用传统 DS 证据理论和 EWDS 融合后的结果，从中可以直观地发现权值调整前后的融合结果。

表 8　EWDS 融合后 7 种攻击的总置信度

描述 \ 融合	总置信度
Port_Scan	0.2898
DNS_Attack	0.2580
ICMP_Attack	0.0159
Web_Attack	0.0127
Http_Attack	0.2261
TCP_Attack	0.0478
FTP_Overflow	0.1497

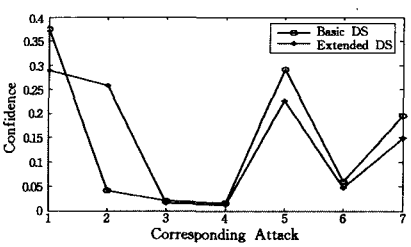

图 5　传统 DS 和 EWDS 融合结果

5.4　安全态势要素提取实验结果

表 9 给出了基于 EWDS 的网络安全态势要素提取综合实验结果。从表中可以发现，本文提出的安全态势要素提取方法无论是在报警检测率和误报率方面，还是在报警精简率方面都取得了不错的效果，能大大降低系统的误报率，获得较高可信度的检测结果，并能通过充分融合多源信息进一步对部分攻击进行精确定位。此外，EWDS 方法在 TPR、FPR 和 DIR 上明显优于传统 DS 证据理论，报警的精简程度令人满意，极大地精简了报警数量，明显优于文献[18]中 D-Force 所采用的方法。

表 9　网络安全态势要素提取综合实验结果

对比 \ 指标	报警数量	真实报警	实际攻击	发现攻击	TPR (%)	FPR (%)	DIR (%)
原始报警	9821	741	855	532	62.22	92.45	18.46
聚合报警	911	723	855	509	59.53	20.63	1.79
Basic-DS	896	809	855	645	75.44	9.71	1.39
EWDS	876	827	855	743	86.90	5.59	1.18

结束语　本文提出了基于 DSimC 和 EWDS 的多源异构网络安全态势要素提取方法，研究了各个传感器提供的多源异构报警之间的相异程度，并在此基础之上充分考虑了不同传感器针对不同攻击的检测能力和效率，采用指数加权机制解决了传感器之间提供证据的冲突问题，有效地实现了多源异构安全信息的动态融合。实验结果表明，提出的方法不仅有较高的检测率(TPR)和较低的误报率(FPR)，而且取得了较为理想的精简率(DIR)。

参 考 文 献

[1] 穆成坡，黄厚宽，田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述[J]. 计算机研究与发展，2006，43(1)：1-8

[2] Dain O，Cunningham R K. Fusing a heterogeneous alert stream into scenarios[C]//Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications. Philadelphia，PA，2001

[3] Anderson D，Fong M，Valdes A. Heterogeneous sensor correlation：a case study of live traffic analysis[C]//Proceedings of the 2002 IEEE Information Assurance Workshop. NUS，USA，2002

[4] Valldes A，Skinner K. Probabilistic alert correlation[C]//Proceedings of the 4th Int'l Symp on Recent Advances in Intrusion Detection. Davis，CA，2001

[5] Ning P，Cui Y，Reeves D S. Techniques and tools for analyzing intrusion alerts[J]. ACM Transactions on Information and System Security，2004(7)：274-234

[6] Yu J Q，Reddy Y V R，Selliah S，et al. TRINETR：an intrusion detection alert management system[C]//Proceedings of the 13th IEEE International Workshops on Enabling Technologies：Infrastructure for Collaborative Enterprise. Mondena，Italy，2004：235-240

[7] 穆成坡，黄厚宽，田盛丰，等. 基于模糊综合评判的入侵检测报警信息处理[J]. 计算机研究与发展，2005，42(10)：1679-1685

[8] 田俊峰，赵卫东，杜瑞忠，等. 新的入侵检测数据融合模型——IDSFP[J]. 通信学报，2006，27(6)：115-120

[9] Qin X Z，Lee W K. Statistical causality of infosec alert data[C]//Proceedings of Recent Advances in Intrusion Detection 2003. LNCS 2820. Berlin，Springer Verlag，2003：73-94

[10] Tian Z H，Fang B X，et al. A vulnerability-driven approach to active alert verification for accurate and efficient intrusion detection[J]. WSEAS Transactions on Communications，2005，4(10)：1002-1009

(下转第 77 页)

好	0.9	0.05	2	0.99
较好	0.8	0.35	1.75	0.95
一般	0.7	0.55	1.6	0.92
较差	0.6	0.7	1.45	0.89
差	0.5	1	1.2	0.85

根据本文 2.2 节多维云模型的生成算法，生成通信网可靠性四维综合云模型。由于二维云的概念可以表示为三维图形，为说明问题且便于表示，这里给出“节点设备可靠性、端到端平均时延”两个属性对应于评语“较好”的二维云模型，如图 2 所示。

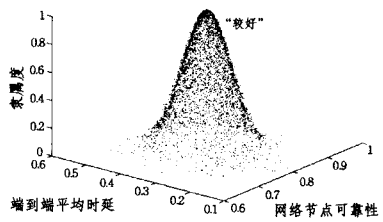

图 2 “较好”二维评判云

以某通信网某个时段性能数据作为样本进行实验。样本集为(0.85,0.04,1.68,0.9)，将其分别输入各属性对应的概化云模型，计算结果如表 2 所列。

表 2 隶属度计算结果

属性	隶属度	激活云
0.85	0.5904	(0.9,0.05,0.003)(好)
0.04	0.9960	(0.05,0.1,0.003)(好)
1.68	0.3230	(1.75,0.05,0.003)(较好)
0.9	0.5449	(0.89,0.0089,0.001)(较差)

由表 1 和表 2 结果建立样本属性云和各级评语对应的综合云，按式(3)计算相似度，计算结果如表 3 所列。

表 3 相似度计算结果

评语	好	较好	一般	较差	差
相似度	0.7591	0.8341	0.8090	0.7826	0.8153

上述计算结果表明，样本的属性云与“较好”对应的评判云相似度最高，所以评价结果为“较好”。同时，从计算过程不难得出，虽然该通信网在某时段的节点设备可靠性和端到端平均时延趋于“好”，但由于业务可用性“较差”，使得系统整体可靠性只能用“较好”来评判。

为验证算法且便于表示，这里给出“节点设备可靠性、端到端平均时延”分别为 0.85 和 0.04 时，其二维属性云与二维评判云的相似度比较情况，如图 3 所示。

从云滴分布的情况可以看出，样本(0.85,0.04)与“好”所对应的评判云相似度更高，所以评价结果趋向于“好”。且表 2 中计算结果表明，两个属性激活的相应概化云模型均为“好”，表明评价结果符合实际。

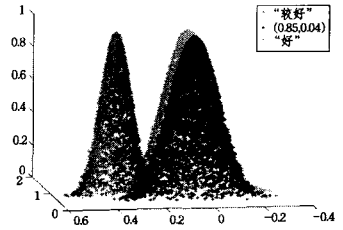

图 3 相似度比较

结束语 云模型作为知识表示和定性定量转换的有力工具，在诸多领域得到了广泛应用，然而关于多维云模型的应用研究尚不多见。本文提出了一种新的基于多维云模型的多属性综合评价方法，给出了“属性概化”的概念，首先用一维逆向云发生器给出各属性对应于各级评语的概念云模型，再用多维正向云发生器分别生成用于定量描述评语的“多维评判云”和定量刻画系统属性的“多维属性云”，最后通过比较两种云模型的相似程度得出综合评价结果，从而在单一价值分类的基础上实现多重价值分类和排序，以便更加直观地反映事物属性和评价结果。

出于简化计算过程的考虑，算法中存在一定假设，如假设所有属性的概化云模型均为正态云。而实际上，当某事物的属性值不是单一数值而是一个区间时，此时用梯形云描述更为合适。由于正态云是梯形云的一个特例，因此如何将算法进行扩展以适应更为一般的情况，从而更准确地反映事物属性并合理评价，是下一步的研究方向和重点。

参 考 文 献

[1] 苏为华. 多指标综合评价理论与方法问题研究[D]. 厦门：厦门大学，2000

[2] Li S H, Liu H, Wang J L. Research on evaluation method of graduates' comprehensive quality based on cloud model[C]// Proc. of the 2009 ICIA. 2009:815-820

[3] Yan W Z, Niu J, Su H Y. A Study on program evaluation and review technology based on cloud model[C]// Proc. of the 2007 IEEE IEEM. 2007:1047-1051

[4] 胡石元，李德仁，刘耀林. 基于云模型和关联度分析法的土地评价因素权重挖掘[J]. 武汉大学学报，2006,31(5):423-427

[5] Shi Y B, Zhang A, Gao X J. Cloud model and its application in effectiveness evaluation[C]// Proc. of the 15th ICMSE. Long Beach, 2008:250-255

[6] 柳炳祥，李海林，杨丽彬. 云决策分析方法[J]. 控制与决策，2009,24(6):957-960

[7] 吕辉军，王晔，李德毅. 逆向云在定性评价中的应用[J]. 计算机学报，2003,26(8):1009-1014

[8] 张国英，沙云，刘旭红. 高维云模型及其在多属性评价中的应用[J]. 北京理工大学学报，2004,24(12):1065-1069

[9] Li Deyi, Liu Changyu. Study on the universality of the normal cloud model[J]. Engineering Science, 2004,6(8):28-34

(上接第 69 页)

[11] 诸葛建伟，王大为，陈昱，等. 基于 DS 理论的网络异常检测方法[J]. 软件学报，2006,17(3):463-471

[12] 朱明. 数据挖掘[M]. 合肥：中国科技大学出版社，2002:132-136

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

[14] Frincke D. Balancing cooperation and risk in intrusion detection[J]. ACM Transactions on Information and System Security (TISSEC), 2000,3(1):1-29

[15] 林作铨，牟克典，韩庆. 基于未知扰动的冲突证据合成方法[J]. 软件学报，2004,15(8):1150-1156

[16] Stolfo S J, Fan W, Wenke L, et al. KDD Cup 1999 Intrusion Detection[EB/OL]. http://www.ics.uci.edu/~kdd/databases/kddcup99, 2008

[17] Salerno J, Blasch E, Hinman M, et al. Evaluating algorithmic techniques in supporting situation awareness[C]// Proceedings of SPIE-Multisensor, Multisource, Information Fusion: Architectures, Algorithms, and Applications. Orlando, FL, USA, 2005

[18] Sabata B, Ornes C. Multisource evidence fusion for cyber-situation assessment[C]// Proceedings of SPIE. the International Society for Optical Engineering. Kissimee, Florida, USA, 2006 (6242):1-9