基于 Dempster-Shafer 证据理论的端口扫描检测方法

赖海光[1,2], 许 峰[3], 黄 皓[1], 谢俊元[1]
(1. 南京大学计算机软件新技术国家重点实验室, 江苏南京 210093;
2. 解放军理工大学指挥自动化学院, 江苏南京 210007;
3. 南京航空航天大学信息科学与技术学院, 江苏南京 210016)

摘 要: 端口扫描是通过对目标系统端口试探性的访问来判断端口是否开放的行为. 它往往是攻击者入侵行为的第一步. 端口扫描检测是入侵监测系统不可缺少的一部分, 而当前端口扫描的检测方法不多, 并且准确性不高. 为提高扫描检测的准确性, 本文使用 Dempster-Shafer 证据理论对两种扫描检测方法产生的数据进行融合: 一种是基于端口分布特征的扫描检测方法, 该方法简单且具有较高的检测率; 另一种是基于序列假设测试的扫描检测方法, 该方法充分利用了端口扫描的本质特征. 实验结果表明, 同单独使用基于端口分布特征或序列假设测试的方法相比, 这种基于 Dempster-Shafer 证据理论的扫描检测方法对端口扫描的检测准确得多.

关键词: 扫描检测; 入侵检测; Dempster-Shafer 证据理论; 数据融合
中图分类号: TP393.08 文献标识码: A 文章编号: 0372-2112 (2006) 11-1946-05

A Portscan Detection Method Based on Dempster-Shafer Theory of Evidence

LAI Hai-guang[1,2], XU Feng[3], HUANG Hao[1], XIE Jun-yuan[1]
(1. *State Key Laboratory for Novel Software, Nanjing University, Nanjing, Jiangsu 210093, China;*
2. *Institute of Command Automation, PLA University of Science and Technology, Nanjing, Jiangsu 210007, China;*
3. *College of Information Science & Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu 210016, China*)

Abstract: Portscan is used to figure out whether the target system's ports are open by trying to access these ports. It is usually the fist step of a sequence of intrusion actions. Portscan detection is an indispensable part of an intrusion detection system. However, there are only a few portscan detection methods nowadays. Moreover, they are not very accurate. In order to improve the accuracy of portscan detection, the data produced by two portscan detection methods is fused using Dempster-Shafer theory of evidence. One method is the ports distribution based portscan detection, which is very simple and has a pretty high detection ratio. The other is the sequential hypothesis testing based detection method, which sufficiently exploits the portscan's essential character. The experiment shows that the portscan detection method based on Dempster-Shafer theory of evidence is far more accurate than the one base on ports distribution or sequential hypothesis testing.

Key words: portscan detection; intrusion detection; Dempster-Shafer theory of evidence; data fusion

1 引言

端口扫描是网络入侵的前奏, 通过端口扫描可以发现目标系统提供的服务[1,2]. 进而, 攻击者才可能利用服务的漏洞入侵系统. 目前, 大部分入侵检测系统根据单位时间内从一个源地址发往不同目的地址或端口的数据包个数来判断是否存在端口扫描[3,4]. 这种方法简单易行, 但攻击者很容易通过降低数据包发送速率来躲避检测. S. Staniford 等人提出了一种称为 SPICE 的检测方法, 使用模拟退火对数据包进行归类, 检测其中的扫描[5]. 该方法的缺点是需要记录大量的数据包. Alfonso Valdes 使用竞争学习技术对 TCP 连接进行分类, 对出现概率最小的模式进行报警[6]. 该方法的特点是不需要"干净"的训练数据, 但其本质是基于异常的检测, 误报率较高. Raj Basu 等人应用神经网络和专家系统对扫描进行检测[7]. 该系统的特点是允许用户在误报率和检测率之间进行权衡, 但是需要训练数据. Guo Xiaobing 等人设计了一种通过发送虚假信息迷惑扫描者以保护目标主机的方法, 但他们并未提出任何新的扫描检测方法[8]. Jaeyeon Jung 等人根据扫描行为成功建立连接的比率远低于正常网络应用的特点, 使用序列假设测试判断发起连接的主机是否在进行扫描[9]. 该方法具有较好的及时性和准确性. 然而, 正常的应用有时也会因网络或主机的故障而产生很低的连接成功率.

收稿日期: 2005-07-12; 修回日期: 2006-04-02
基金项目: 国家高技术研究发展计划(No. 2003AA142010); 国家自然科学基金(No. 60303023, No. 60473091)

本文提出了一种基于 Dempster Shafer 证据理论的扫描检测方法,通过综合基于端口分布特征和基于序列假设测试的检测方法,大幅度地降低了扫描检测的误报率、改善了检测率.其中,基于端口分布特征的扫描检测方法是我们提出的一种新的检测方法,其具有很高的扫描检测率.本文只讨论对实际网络中占大多数的TCP扫描的检测[10],不讨论对 UDP 扫描的检测.

2　扫描端口分布

端口扫描可以分成三类:水平扫描、垂直扫描和块扫描[10].水平扫描是对多个主机的同一个端口进行扫描.垂直扫描是对同一个主机的多个端口进行扫描.将水平扫描和垂直扫描结合起来就是块扫描.攻击者进行端口扫描的目的是寻找可以利用的系统漏洞.因此,攻击者通常不会扫描任意的端口,而是选择可能存在漏洞的端口进行扫描.首先,考虑水平扫描和块扫描,假设攻击者感兴趣的端口集合为 A,对各个主机进行探测时访问的端口集合分别为 $A_1, A_2, \cdots, A_n$.对于水平扫描,根据定义,$A_1 = A_2 = \cdots = A_n = A$,因此,$A_1 \cap A_2 \cap \cdots \cap A_n = A$.对于块扫描,如果攻击者在扫描不同主机时除了访问 A 中的端口外还随机访问了其它一些端口,则 A_1 至 A_n 不会都相等,但是 $A_1 \cap A_2 \cap \cdots \cap A_n = A$ 依然成立.而对于正常的网络应用而言,目的主机提供服务的端口是已知的,而且通常不同的主机提供不同的服务.所以,正常应用在不同主机上访问的端口很可能不同,既在不同主机上访问端口的集合的交集很可能为空.对于垂直扫描,扫描行为也不同于正常网络应用.一般来说,单独一台主机所提供的服务是比较少的.对于某个主机而言,正常的网络应用只会访问其少数几个提供服务的端口,而且可能会反复的访问(交互大量的数据包).而攻击者为了确定该主机上存在的漏洞,很可能会访问许多可能提供服务的端口,并且为了提高扫描速度和避免被发现,访问每个端口的次数很少.

3　基于 Dempster-Shafer 证据理论的端口扫描检测

类似于传统的概率理论,Dempster Shafer 证据理论也是一种处理不确定性的理论,但它处理的是主观不确定性[11,12].Dempster Shafer 证据理论提供了一种对数据进行融合的方法,在很多方面都有所应用,例如:多探测器的数据融合[13]、结构化文档中的不确定性的描述[14]、图像纹理的分类[15]等.在入侵检测领域,Christos Siaterlis 等人也提出了一种利用 Dempster Shafer 证据理论对 DoS(拒绝服务)攻击进行检测的方法[16].

由于现有的各种扫描检测方法都只根据端口扫描某一方面的特征进行检测,所以很难做到非常准确.基于 Dempster Shafer 证据理论的端口扫描检测利用 Dempster Shafer 证据理论对不同检测方法获得的数据进行融合,从而获得比单独使用某一种方法更高的准确性.这里使用两种端口扫描检测方法,一种是我们提出的利用端口分布特征的检测方法,另一种是基于序列假设测试的扫描检测方法.

3.1　基于端口分布特征的扫描检测

如前所述,对于水平和块扫描,攻击者在不同主机上访问的端口有共同之处,而正常网络应用在不同主机上访问的端口很可能不同.由于攻击者除端口扫描外还可能进行一些正常的网络活动,所以攻击者在每个主机上访问的端口集合不一定都存在相同之处.但是,相同端口集合的数目在攻击者访问的主机数目中所占的比例会比较高.据此,我们记录某一主机在各个目的主机上所访问端口的集合,统计这些端口集合中相同集合个数的最大值,如果该值同其所访问的主机个数的比率大于设定的阈值,则认为其在进行扫描.具体的扫描检测算法如下:

1. 假设主机 x 所访问的主机为 $a_1, a_2, \cdots, a_n$,记录 x 在 $a_1, a_2, \cdots, a_n$ 上访问不超过两次的端口的集合:$A_1, A_2, \cdots, A_n$.

2. 令 c_i 为同集合 A_i 相同的其它集合的个数$(1 \leqslant i \leqslant n)$,取 $h = \dfrac{\max(c_1, c_2, \cdots, c_n)}{n}$.

3. 如果 h 大于设定的阈值 T_1,则主机 x 在进行扫描,$h\_score = 1$,否则 $h\_score = 0$.

对于垂直扫描,我们认为攻击者在目标主机上访问的端口数目会多于正常的网络应用.因此,我们根据主机在目标主机上访问的端口数来计算扫描攻击的可能性:

1. 记录主机对某个目标主机上端口的访问,统计那些访问不超过两次的端口的数目 v.

2. 如果 v 大于设定的阈值 T_2,则该主机在进行扫描,$v\_score = 1$,否则 $v\_score = 0$.

令 $score = h\_score \cup v\_score$,如果 $score = 0$,则未发现端口扫描;如果 $score = 1$,则检测到端口扫描.

在上述端口扫描的检测算法中,我们只统计被访问不超过两次的端口,这是因为攻击者为了提高扫描速度以及避免暴露自己通常只对特定端口的状态进行很少次数的测试.例如:著名的扫描软件 Nmap 进行 SYN 扫描时只向目标端口发送一个 SYN 数据包.而对于正常的网络应用,其同服务器之间的通信过程包括建立 TCP 连接、数据传输和释放 TCP 连接的完整过程,需要交互大量的数据包,因而对服务器端口的访问次数远不止两次.可以看到,基于端口分布特征的扫描检测方法非常简单,但是实验结果表明,该方法具有相当高的扫描检测率.

3.2　基于序列假设测试的扫描检测

基于序列假设测试的扫描检测将从某个主机发起的第 i 次连接请求的结果表示为随机变量 Y_i.如果连接成功的话,$Y_i = 0$,否则,$Y_i = 1$.观察 Yi 的序列,使用序列假设测试可以判断发起连接的主机是否在进行扫描.考虑两个假设:H_0 和 H_1,H_0 代表发起连接的主机正常,而 H_1 表示发起连接的主机在进行端口扫描.每次请求结果在两个假设下的条件概率可以表示为:

$$\begin{aligned} &\Pr[Y_i = 0 \mid H_0] = \theta_0, \Pr[Y_i = 1 \mid H_0] = 1 - \theta_0 \\ &\Pr[Y_i = 0 \mid H_1] = \theta_1, \Pr[Y_i = 1 \mid H_1] = 1 - \theta_1 \end{aligned} \quad (1)$$

由于扫描者事先不知道端口是否开放,所以正常主机建立连接的成功率要大于扫描者建立连接的成功率,既 $\theta_0 > \theta_1$.定义 Y_i 的序列为:$Z_n = (Y_1, Y_2, \cdots, Y_n)$,序列假设测试通过计

算序列 Z_n 在两种假设条件下出现概率的比值来决定接受哪一个假设, 如式(2)所示:

$$\Lambda(Z_n)\equiv\frac{\Pr[Z_n|H_1]}{\Pr[Z_n|H_0]} \tag{2}$$

将 $\Lambda(Z_n)$ 同两个阈值 η_0 和 η_1 相比较, 如果 $\Lambda(Z_n)\geqslant\eta_1$, 则接受假设 H_1; 如果 $\Lambda(Z_n)\leqslant\eta_0$, 则接受假设 H_0; 如果 $\eta_0<\Lambda(Z_n)<\eta_1$, 则不能决定该接受何种假设, 需要观察更多的连接请求. 其中 η_0 和 η_1 由检测率和误报率决定, 按照 Jaeyeon Jung 等人的分析, 如果用户要求误报率小于 α, 检测率大于 β, 可以设置 $\eta_1=\frac{\beta}{\alpha}$, $\eta_0=\frac{1-\beta}{1-\alpha}$. 假设在每种假设条件下随机变量 Y_i 都是独立同分布的, 则:

$$\Lambda(Z_n)=\prod_{i=1}^{n}\frac{\Pr[Y_i|H_1]}{\Pr[Y_i|H_0]} \tag{3}$$

令 $\phi(Y_i)\equiv\frac{\Pr[Y_i|H_1]}{\Pr[Y_i|H_0]}=\begin{cases}\frac{\theta_1}{\theta_0}, & \text{如果 } Y_i=0\\ \frac{1-\theta_1}{1-\theta_0}, & \text{如果 } Y_i=1\end{cases}$, 则:

$$\Lambda(Z_n)=\prod_{i=1}^{n}\phi(Y_i)=\Lambda(Z_{n-1})\phi(Y_n) \tag{4}$$

由式(4)可见, 我们可以根据当前连接请求的结果很方便的更新 $\Lambda(Z_n)$.

在实际网络中, 有时某个正常的网络应用会反复向一个已经关闭的端口发起连接请求, 这种情况经常在服务器发生故障而客户软件被配置为自动保持同服务器的连接时出现. 此时, 连接请求总是失败, 从而导致很低的连接成功率而被误判为端口扫描. 所以我们对 Jaeyeon Jung 等人提出的方法作了部分改进, 只有当主机访问一个访问次数小于三的端口时才计算 $\Lambda(Z_n)$.

3.3 利用 Dempster Shafer 证据理论进行数据融合

现实世界中的不确定性可以分为两类[11]: 一类是偶然不确定性, 也被称为客观不确定性. 这类不确定性的产生是由于被观察的系统会按照随机的方式运行. 另一类是认识不确定性, 也叫主观不确定性. 产生这类不确定性的原因是缺乏关于被观察系统的知识. 相对于经典的概率理论, Dempster-Shafer 证据理论更适合于刻划由于认识的不足而产生的认识不确定性. 在数据融合方面, 和传统的贝叶斯理论相比, Dempster Shafer 证据理论处理"信任", 而不是概率, 而且"信任"可以和事件的集合相关, 不一定是单个事件.

Dempster Shafer 证据理论中有一个非常重要的函数, 称为基本可能性指派函数 m:

令所有事件的集合为 U, 基本可能性指派函数 m 表示对 U 的某一子集的信任度, 定义为:

$$m:2^U\rightarrow[0,1] \tag{5}$$

同时 m 必须满足:

$$m(\Phi)=0,\ \sum_{A\in 2^U}m(A)=1 \tag{6}$$

基于基本可能性指派函数, Dempster Shafer 证据理论提供了合并多个证据的方法. 该证据合并规则称为 Dempster 合并规则:

$$m_{12}(A)=\frac{\sum_{B\cap C=A}m_1(B)m_2(C)}{1-\sum_{B\cap C=\phi}m_1(B)m_2(C)},\quad \text{当 } A\neq\Phi \tag{7}$$

$$m_{12}(\Phi)=0$$

虽然该合并规则在冲突证据合并时存在一些不足, 因而也发展了一些改进的合并规则[17, 18], 但由于其简单、易用, 我们仍然采用该规则. 应用该合并规则的前提是被合并的证据必须彼此独立. 将基于端口分布特征的扫描检测和基于序列假设测试的扫描检测作为两个基本可能性指派, 由于这两种检测方法分别从扫描的不同侧面对其进行检测, 我们认为它们之间是彼此独立的, 因而能够应用 Dempster 合并规则对它们进行合并. 对于扫描检测问题, 事件集合 $U=\{$扫描, 正常$\}$, 它的幂集为$\{\{$扫描$\},\{$正常$\},\{$扫描, 正常$\},\Phi\}$.

对于基于序列假设测试的扫描检测, 当 $\Lambda(Z_n)$ 小于 η_0 时, 判定当前的端口访问不是扫描; 当 $\Lambda(Z_n)$ 大于 η_1 时, 判定其为扫描; 而当 $\Lambda(Z_n)$ 位于 η_0 与 η_1 之间时, 不能够决定当前的端口访问行为是否为扫描, 但 $\Lambda(Z_n)$ 的数值越接近 η_1 就越有可能是扫描. 因此定义基本可能性指派 m_1 如下:

$$m_1(\{\text{扫描}\})=\begin{cases}0, & \Lambda(Z_n)\leqslant\eta_0\\ \frac{\Lambda(Z_n)-\eta_0}{\eta_1-\eta_0}, & \eta_0<\Lambda(Z_n)<\eta_1\\ 1, & \Lambda(Z_n)\geqslant\eta_1\end{cases} \tag{8}$$

$$m_1\{(\text{正常})\}=1-m_1(\{\text{扫描}\})$$

$$m_1(\{\text{扫描, 正常}\})=0$$

$$m_1(\Phi)=0$$

对于基于端口分布特征的扫描检测, 其输出 $score$ 要么是 1 要么是 0, 表示当前的端口访问要么是扫描要么不是扫描. 我们直接将其作为扫描可能性的度量, 定义基本可能性指派 m_2 如下:

$$\begin{aligned}&m_2(\{\text{扫描}\})=score\\ &m_2(\{\text{正常}\})=1-m_2(\{\text{扫描}\})\\ &m_2(\{\text{扫描, 正常}\})=0\\ &m_2(\Phi)=0\end{aligned} \tag{9}$$

使用 Dempster 合并规则对 m_1, m_2 进行合并, 合并后对集合$\{$扫描$\}$的基本可能性指派为:

$$m_{12}(\{\text{扫描}\})=\frac{\sum_{B\cap C=\{\text{扫描}\}}m_1(B)m_2(C)}{1-\sum_{B\cap C=\phi}m_1(B)m_2(C)} \tag{10}$$

根据 m_1、m_2 的定义可知:

$$m_{12}(\{\text{扫描}\})=\frac{m_1(\{\text{扫描}\})m_2(\{\text{扫描}\})}{1-[m_1(\{\text{扫描}\})m_2(\{\text{正常}\})+m_1(\{\text{正常}\})m_2(\{\text{扫描}\})]} \tag{11}$$

$m_{12}(\{$扫描$\})$反映了融合两种扫描检测方法所产生的数据后对扫描可能性的度量, 该值越大就越有可能是扫描. 设定阈值 T, 当其超过 T 时判定当前的端口访问行为为扫描.

4 实验

实验使用的是 1999 年 DARPA(国防高级研究计划局)的入侵检测测试数据集,我们选取了 TCP 扫描较多的第四周星期一的测试数据[19]. 该测试数据分为内网和外网两个部分,分别使用基于端口分布特征、序列假设测试和 Dempster Shafer 证据理论的扫描检测方法对其进行检测. 其中基于端口分布特征检测方法的阈值 T_1 定为 0.9 是因为根据我们的观察,正常连接的成功率一般都会高于 90%,设置 T_1= 0.9 可以保证较高的检测率. 而将 T_2 设为 3 的依据是正常应用在某一主机上访问的端口通常小于 3 个. 基于序列假设测试检测方法的参数是按照 Jaeyeon Jung 等人的研究结果确定的,他们的实验表明取 θ_0= 0.8、θ_1= 0.2、α= 0.01、β= 0.99 能够很好的对扫描进行检测. 表 1、表 2、表 3 分别是上述三种检测方法对测试数据进行检测后的结果如表 1~3。

从实验结果可以看出,基于端口分布特征的扫描检测方法具有非常高的检测率,但同时,它的误报率也相当高. 基于序列假设测试的扫描检测方法只是在对内网数据检测的误报率上比基于端口分布特征的方法好,其它都更差. 而基于 Dempster Shafer 证据理论检测方法的测试结果比前两种方法好得多. 该方法无论是检测率还是误报率都比基于序列假设测试的扫描检测方法好. 虽然其检测率同基于端口分布特征的检测方法相同,但是它没有误报. 以上三种方法都没有能够检测出 172.16.118.20 这个攻击者,通过分析 172.16.118.20 发送和接收的数据包,我们发现其只有一次连接请求,并且是一次成功的连接请求,所以无法同正常应用进行区分.

表 1　基于端口分布特征检测方法的结果

参数	数据集	实际的扫描者 IP	检测方法输出的扫描者 IP	检测率	误报率
T_1= 0.9 T_2= 3	内网	202.77.162.213, 172.16.118.50, 153.107.252.61, 172.16.118.20	172.16.112.100, 194.27.251.21, 194.7.248.153, 172.16.112.50, 135.13.216.191, 135.8.60.182, 172.16.114.148, 197.218.177.69, 195.115.218.108, 172.16.113.50, 196.37.75.158, 172.16.114.50, 196.227.33.189, 202.77.162.213, 172.16.118.50, 153.107.252.61	75%	81.25%
	外网	202.77.162.213, 153.107.252.61	194.27.251.21, 194.7.248.153, 135.13.216.191, 135.8.60.182, 172.16.114.148, 197.218.177.69, 195.115.218.108, 196.37.75.158, 196.227.33.189, 172.16.112.100, 202.77.162.213, 153.107.252.61	100%	83.33%

表 2　基于序列假设测试检测方法的结果

参数	数据集	实际的扫描者 IP	检测方法输出的扫描者 IP	检测率	误报率
θ_0= 0.8 θ_1= 0.2 α= 0.01 β= 0.99	内网	202.77.162.213, 172.16.118.50, 153.107.252.61, 172.16.118.20	172.16.114.169, 172.16.112.207, 172.16.115.87, 172.16.115.5, 202.77.162.213, 172.16.117.132, 172.16.118.50, 172.16.116.201, 172.16.117.103	50%	77.78%
	外网	202.77.162.213, 153.107.252.61	172.16.114.169, 172.16.112.207, 172.16.113.204, 172.16.114.168, 172.16.113.84, 172.16.115.87, 172.16.115.5, 202.77.162.213, 172.16.117.132, 172.16.116.201, 172.16.117.103	50%	90.91%

表 3　基于 Dempster Shafer 证据理论检测方法的结果

参数	数据集	实际的扫描者 IP	检测方法输出的扫描者 IP	检测率	误报率
T_1= 0.9 T_2= 3 θ_1= 0.8 θ_2= 0.2 α_1= 0.01 α_2= 0.99	内网	202.77.162.213, 172.16.118.50, 153.107.252.61, 172.16.118.20	202.77.162.213, 172.16.118.50, 153.107.252.61	75%	0%
	外网	202.77.162.213, 153.107.252.61	202.77.162.213, 153.107.252.61	100%	0%

5 结论

本文提出了一种基于 Dempster Shafer 证据理论的端口扫描检测方法,利用 Dempster Shafer 证据理论对两种扫描检测方法进行综合,一种是我们提出的基于端口分布特征的检测方法,另一种是基于序列假设测试的检测方法. 这两种扫描检测方法分别从不同的侧面对端口扫描进行检测,单独使用某一种方法的检测效果都不够理想,但是,通过定义各自的基本可能性指派函数和应用 Dempster 合并规则对两种检测方法产生的数据进行融合,基于 Dempster Shafer 证据理论的检测方法大大降低了误报率,同时依然保持了高的检测率.

参考文献:

[1] Fyodor. The Art of Port Scanning[DB/OL]. http://www.phrack.org, 1997.

[2] dethy. Examining Port Scan Methods-Analysing Audible Techniques [DB/OL]. http://synnergy.net/downloads/papers/portscan.txt, 2001.

[3] V Paxson. Bro: A system for detecting network intruders in real-time[J]. Computer Networks, 1999, 31(23-24): 2435-2463.

[4] M Roesch. Snort: Lightweight intrusion detection for networks [A]. Proceedings of the 13th USENIX Conference on System Administration[C]. Seattle, USA: USENIX, 1999. 229-238.

[5] S Staniford, J A Hoagland, J M McAlerney. Practical automated detection of stealthy portscans[J]. Journal of Computer Security, 2002, 10(1/2): 105- 136.

[6] Alfonso Valdes. Detecting novel scans through pattern anomaly detection[A]. Proceedings of the DARPA Information Survivability Conference and Exposition[C]. Washington, USA: IEEE Computer Society, 2003, 1: 140- 151.

[7] Raj Basu, Robert K Cunningham, Seth E. Webster, Richard P Lippmann. Detecting low-profile probes and novel denial-of-service attacks [A]. Proceedings of the 2001 IEEE Workshop on Information Assurance[C]. New York, USA: IEEE, 2001.

[8] Guo Xiaobing, Qian Depei, Liu Min, Zhang Ran, Xu Bin. Detection and protection against network scanning: IEDP[A]. Proceedings of the 2001 International Conference on Computer Networks and Mobile Computing [C]. Beijing, China: IEEE Computer Society, 2001. 487- 494.

[9] Jaeyeon Jung, Vern Paxson, Arthur W. Berger, Hari Balakrishnan. Fast portscan detection using sequential hypothesis testing [A]. Proceedings of the IEEE Symposium on Security and Privacy[C]. California, USA: IEEE CS Press, 2004. 211- 225.

[10] Cynthia Bailey Lee, Chris Roedel, Elena Silenok. Detection and characterization of port scan attacks[DB/OL]. http://www.cs.ucsd.edu/users/clbailey/PortScans.pdf, 2003.

[11] Kari Sentz, Scott Ferson. Combination of evidence in dempster shafer theory [DB/OL]. www.osti.gov/gpo/servlets/purl/800792-s9WKeP/native/, 2004.

[12] Challa S, Koks D. Bayesian and dempster shafer fusion[J]. Sadhana, 2004, 29(2): 145- 174.

[13] Huadong Wu, Mel Siegel, Rainer Stiefelhagen, JieYang. Sensor fusion using dempster shafer theory[A]. IEEE Instrumentation and Measurement Technology Conference [C]. Anchorage, USA: IEEE, 2002. 7- 12.

[14] Mounia Lalmas. Dempster shafer's theory of evidence applied to structured documents: modelling uncertainty [A]. Proceedings of the 20th annual international ACM SIGIR conference on Research and development in information[C]. Philadelphia, USA: ACM Press, 1997. 110- 118.

[15] Jia Yonghong, Li Deren, Feature fusion based on dempster shafer's evidential reasoning for image texture classification [J]. International Archives of Photogrammetry Remote Sensing and Spactial Information Science, 2004, 35(3): 662- 665.

[16] Christos Siaterlis, Basil Maglaris. Towards multisensor data fusion for DoS detection [A]. Proceedings of the 2004 ACM Symposium on Applied Computing[C]. Nicosia, Cyprus: Association for Computing Machinery, 2004. 439- 446.

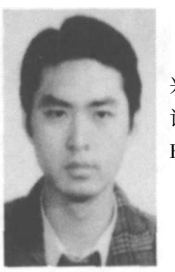
[17] Yager R. Using approximate reasoning to represent default knowledge[J]. Artificial Intelligence, 1987, 31(1): 99- 112.

[18] 徐凌宇, 张博锋, 徐炜民, 徐怀宇, 郭非凡. D-S 理论中证据损耗分析及改进方法[J]. 软件学报, 2004, 15(1): 69- 75.
Xu LY, Zhang BF, Xu WM, Xu HY, Guo FF. Evidence ullage analysis in D-S theory and development[J]. Journal of Software, 2004, 15(1): 69- 75. (in Chinese)

[19] MIT Lincoln Laboratory. DARPA Intrusion Detection Evaluation[DB/OL]. http://www.ll.mit.edu/IST/ideval/, 1999.

作者简介:

赖海光 男, 1975 年 6 月出生于贵州省平坝县, 现为解放军理工大学指挥自动化学院讲师, 主要研究方向为信息安全、计算机网络等.
E-mail: lite@263.net



许 峰 男, 1970 年 3 月出生于江苏省泰兴, 现为南京航空航天大学信息科学与技术学院讲师, 主要研究方向为信息安全和分布式计算.
E-mail: njxuf@163.com