多 IDS 环境中基于可信度的警报关联方法研究

梅海彬，龚俭

（东南大学 计算机科学与工程学院 江苏省计算机网络技术重点实验室，江苏 南京 210096）

摘 要：针对现有警报关联方法在关联来自多个 IDS 的警报时未考虑各 IDS 报告警报可信度的不足，利用证据理论提出了一种基于可信度对多个 IDS 的警报进行关联分析的方法。方法将各 IDS 报告警报的情况作为推测网络攻击是否发生的证据，并采用 Dempster 组合规则来融合这些证据，最后决策判断警报所对应的攻击是否发生，从而消除各 IDS 报告警报的模糊性和冲突性，达到提高警报质量的目的。在 DARPA 2000 测试数据集上的实验结果表明，该方法能有效降低误报率，减少警报数目 60%以上。

关键词：网络安全；入侵检测系统；警报关联；证据理论；可信度

中图分类号：TP393.08 **文献标识码**：B **文章编号**：1000-436X(2011)04-0138-09

Research on alert correlation method based on alert confidence in multi-IDS environment

MEI Hai-bin, GONG Jian

(Computer Network Technology Key Laboratory of Jiangsu Province, School of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: To overcome the shortcoming of current alert correlation methods which didn't consider the confidence of IDS, an alert correlation method based on alerts confidence using the evidence theory was presented. Each alert was regarded as a piece of evidence of a network attack. Then multiple pieces of evidence were combined by the Dempster's combination rule, and used to infer whether the attack corresponding to the alerts took place. As a result, the ambiguity and confliction in alerts were eliminated, achieving the goal of improving alerts quality. Experimental results on the DARPA 2000 IDS test dataset show that the proposed method can efficiently decrease the false alert rate and reduce more than 60% of the alerts.

Key words: network security; intrusion detection system; alert correlation; evidence theory; confidence

1 引言

入侵检测系统（IDS, intrusion detection system）作为保障网络安全的有效工具，得到了越来越多的重视与应用，它能够检测网络上的攻击行为，并提示系统管理员进行及时响应，以避免入侵带来的损失[1,2]。但单一的 IDS 由于自身技术的局限和观察视点的孤立，还存在误报率高以及无法检测到所有攻击的不足。一种较好的解决途径是使用分布式的多个 IDS，即在网络中的不同位置部署相同或不同种类的 IDS 来监视网络环境中的不同实体[3]。通过多个 IDS 间的相互协作和相互补充，来丰富入侵检测数据的来源，提高检测的覆盖范围和准确度，以弥补单一 IDS 检测技术的缺陷与盲点，从而提高对整

收稿日期：2010-07-05；修回日期：2011-02-10

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2009CB320505）

Foundation Item: The National Basic Research Program of China (973 Program) (2009CB320505)

个网络安全的保护力度。

然而，由于 IDS 本身检测技术还不够成熟，以及各 IDS 的异构性和自治性使得产生的警报在内容、详略程度、不确定性等方面存在很大的差异，从而导致系统中出现了大量冗余的、不完整、可信度不同并含有误报的警报数据，这些数据已远超出了管理员的手工分析处理能力[4~6]，管理员很难从这些警报数据中找到真正有用的安全信息，也限制了 IDS 的自动响应。因此，如何综合分析和处理这些来自不同 IDS 的警报，对其进行精简、合并和消除不确定性，从而提高警报信息的可信度，减少误报具有重要的实际意义。

目前虽然已经提出了多种警报关联方法，但它们都存在各自的缺点，并且在关联来自多个 IDS 的警报时，仅考虑了警报之间的内在联系，没有考虑各 IDS 报告警报的可信度差异，而将各 IDS 报告警报的可信度同等对待。实际上，由于每种 IDS 所采用的入侵检测技术不同，其侧重点也会不同[4,7]，有的 IDS 对某些攻击的检测效果很好，但对另外一些攻击的检测效果却一般。另外，由于 IDS 部署的位置不同，导致 IDS 收集到的攻击证据也会存在较大的差异[8]，因此不同 IDS 报告警报的可信度会存在一定差异。在进行警报关联时，如果充分考虑这种可信度的差异将有利于进一步降低警报的不可靠性、含糊性，从而降低误报率，提高警报的可信性。

基于上述分析，本文利用 D-S 证据理论[9]具有擅长处理不确定性、不精确以及不准确信息的特点，提出了一种综合多 IDS 报告警报的可信度对警报进行关联分析的新方法，以消除警报数据中的不可靠性和含糊性，从而降低误报率，提高警报质量。本文将来自各个 IDS 报告的警报作为推断网络攻击是否发生的证据，通过信度分配函数的度量方式，区分和描述每个 IDS 报告警报的可信度，借助于时间复杂度为 $O(n)$的证据组合规则来融合这些证据，并选取相应的决策方法来推断警报对应的网络攻击是否真的发生。通过在标准测试数据集 DARPA 2000[10]上所做的实验表明，本文提出的 D-S 证据理论方法能有效减少警报数目，降低误报率，提高报告警报的准确度。

以下为全文的组织结构：第 2 节简要介绍相关的研究工作；第 3 节是 D-S 证据理论的相关概念与理论；第 4 节详细阐述了基于证据理论进行警报关联的具体实现步骤以及相应算法；第 5 节是本文的实验和结果分析；最后是结束语。

2　相关工作

对警报关联技术的研究是近几年来 IDS 领域的一个研究热点[11]，目前研究者们已提出了多种警报关联分析方法，其中比较具有代表性的有基于警报属性相似性的警报关联[6, 12, 13]，基于已知攻击场景的警报关联[14~16]，基于前因后果的警报关联[5, 17, 18]和基于统计因果分析的警报关联[19, 20]等。但这些方法在关联来自多个 IDS 的警报时，都没有考虑各 IDS 报告警报的可信度的差异，无法有效处理警报中存在的不确定性。

与本文的思路类似，文献[8]采用了一种加权证据理论的方法来处理不同 IDS 间可信度的差异，但该方法的信度分配函数依赖于基于隐着色 Petri 网的关联组件的输出，而此关联组件的实现需要知道每种多步攻击的先验知识，并需要获得合理的训练数据来估计模型的参数，从而限制了方法的使用。此外，基于隐着色 Petri 网的警报关联与基于前因后果的警报关联一样，在时间和空间上的计算复杂度都很大，不适合对多 IDS 环境下的大量警报进行实时关联。最后，该方法在信度分配函数定义上未考虑未知的情况，直接对未知的支持度设置为零，没有充分利用证据理论在支持不确定性描述方面的特性。

此外，证据理论在网络安全研究的其他领域也得到了应用。文献[21]将证据理论用于进行网络的异常检测，其基本思想是将网络流的一些特征作为衡量网络流是否异常的证据，并使用证据理论将这些证据进行融合从而最终判定该网络流是否异常。该方法属于异常入侵检测本身的研究，是对底层网络流的异常检测。而本文方法是对 IDS 警报的后处理，即在多 IDS 的环境中，将每个 IDS 报告警报的情况作为推测警报所对应的攻击是否发生的证据，从而判定警报的真假。两者不论是在应用场景、目标，还是证据理论的使用方面，如证据的选择，信任度函数的分配等，都存在较大的差别。

3　证据理论

本文方法的理论基础是证据理论，证据理论又称 D-S 理论或 Dempster-Shafer 证据理论，是一种不确定推理理论，首先由 Dempster 于 1967 年提出[22]，

并由 Shafer 将其发展并整理成一套完整的数学推理理论。它可以看为是在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[9]。由于具有这种优点，近年来，D-S 理论已被应用到多传感器网络、医疗诊断、目标识别和网络异常检测等多种领域[21]。本文选用该理论的主要原因是：1) 证据理论上述的主要特性在处理多个 IDS 所报的警报存在差异，以及难以评判是否确实发生网络攻击时有着较大的优势；2) 证据理论中的证据组合规则为有效融合多个 IDS 报告的警报提供了较好的理论依据；3) 证据理论具有较好的可扩展性。在不改变算法框架的条件下，可以方便地融合新的 IDS 警报证据。以下是证据理论的相关定义与理论的描述。

在 D-S 理论中，设有一判决问题 X，并设其所有可能取值所构成的集合为$\{\theta_1, \theta_2, \cdots, \theta_n\}$。如果集合内的元素是有限的，且元素间互斥，则称该集合为 X 的识别框架，通常用符号Θ表示。Θ的一个子集，即Θ幂集 2^{Θ} 的一个元素，表示为一个命题假设 H。

定义 1 设Θ为识别框架，函数 $m: 2^{\Theta} \to [0,1]$ 是一基本信度分配（BPA, basic probability assignment）函数，当且仅当：

1) $M(\varnothing) = 0$；

2) $\sum_{A \subseteq \Theta} m(A) = 1$。

若 $m(A)>0$，则称 A 为该函数的一个焦元。

定义 2 设Θ为识别框架，函数 $Bel: 2^{\Theta} \to [0,1]$ 称为信任函数，如果对于 $A \subseteq \Theta$，满足：

$$Bel(A) = \sum_{B \subseteq A} m(B) \tag{1}$$

$Bel(A)$ 称为 A 的信任度。

定义 3 设Θ为识别框架，函数 $Pl: 2^{\Theta} \to [0,1]$ 称为似真函数，如果对于 $A \subseteq \Theta$，满足：

$$Pl(A) = 1 - Bel(\bar{A}) = \sum_{B \cap A \neq \varnothing} m(B) \tag{2}$$

$Pl(A)$ 称为 A 的似真度，表示不怀疑 A 的程度，或者说发现 A 可靠的程度。

定义 4 D-S 理论中多个证据的组合规则，即 Dempster 规则。令 m_1 和 m_2 为 Θ 上的 2 个证据的基本信度分配函数，它们的焦元分别为 A_1，A_2，…，A_m 和 B_1，B_2，…，B_n。则这 2 个证据组合得出的组合证据的信度分配函数定义为

$$m_{12}(A) \equiv m_1(A) \oplus m_2(A) = \begin{cases} 0, & A = \varnothing \\ K^{-1} \sum_{A_i \cap B_j = A} m_1(A_i) m_2(B_j), & A \neq \varnothing \end{cases} \tag{3}$$

其中，$A \subseteq \Theta$，$K = 1 - \sum_{A_i \cap B_j = \varnothing} m_1(A_i) m_2(B_j) = \sum_{A_i \cap B_j \neq \varnothing} m_1(A_i) \cdot m_2(B_j)$。设 $m_1, m_2, \cdots, m_n$ 是 Θ 上的 n 个证据的基本信度分配函数，则一般化 Dempster 组合规则定义为

$$m_{1\cdots n}(A) = \begin{cases} 0, & A = \varnothing \\ K^{-1} \sum_{A_1 \cap \cdots \cap A_n = A} m_1(A_1) m_2(A_2) \cdots m_n(A_n), & A \neq \varnothing \end{cases} \tag{4}$$

其中 $A \subseteq \Theta$，$K = 1 - \sum_{A_1 \cap \cdots \cap A_n = \varnothing} m_1(A_1) m_2(A_2) \cdots m_n(A_n) = \sum_{A_1 \cap \cdots \cap A_n \neq \varnothing} m_1(A_1) m_2(A_2) \cdots m_n(A_n)$。

4 基于可信度的警报关联方法

4.1 系统架构

本文提出的基于可信度的多 IDS 警报分析方法的系统框架如图 1 所示，主要由警报接收模块 ARM、冗余消除模块 REM 和警报关联引擎 ACE 3 部分组成。

ARM 负责接收各 IDS 产生的原始警报数据，然后对警报数据进行相应的格式转换。REM 的功能是依据冗余消除规则对一次持续性攻击产生的冗余警报进行消除[23]。ACE 是系统的核心功能部件，其主要功能是利用证据理论对 IDS 报告的警报赋予可信度并作为推测网络攻击发生的证据，然后对这些证据进行组合，求出总的可信度，最后根据可信度来判断警报对应的攻击是否真的发生，过滤掉攻击发生可信度较低的警报，并将经过关联后的警报结果呈现给控制终端和存放在警报数据库中。控制终端接收经过处理后的警报结果，并将结果展示给安全管理者。

4.2 警报格式

由于本文需要将多个 IDS 报告的警报进行关联处理，而各 IDS 所使用的原始警报格式可能各不相同，并非所有的 IDS 都支持 IDMEF[24]格式，因此必须先将各 IDS 产生的原始警报转化为统一格式的警报。为了处理的方便，本文没有采用 IDMEF 作为不同 IDS 警报的通用格式，而是通过简化处理采

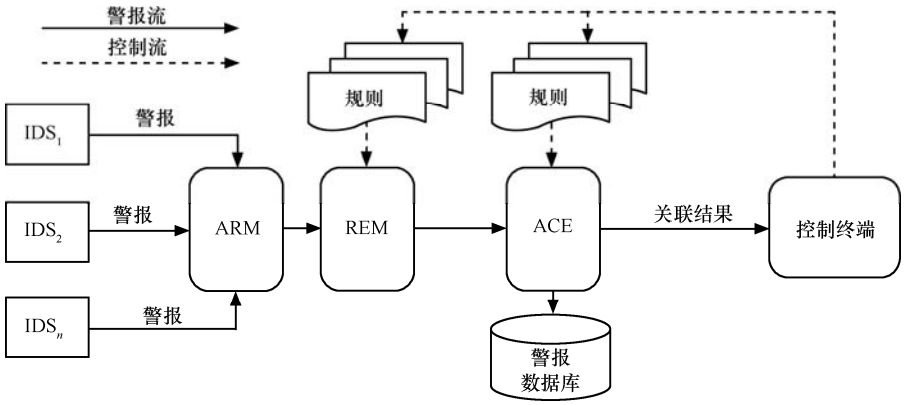


图 1　基于可信度的多 IDS 警报关联系统架构

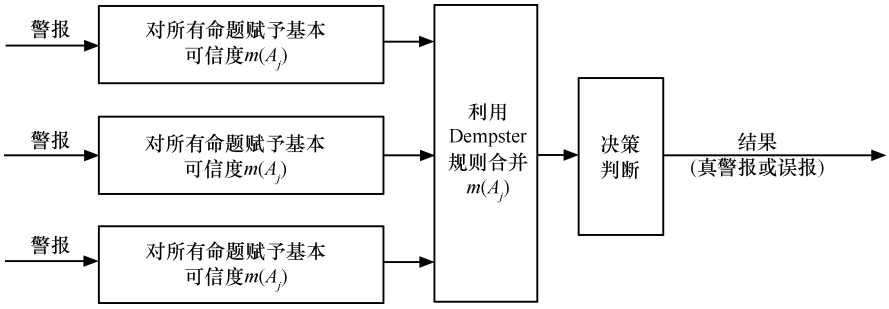


图 2　基于证据理论的警报关联引擎的工作原理

用自定义的警报格式。表 1 为统一警报格式的通用字段定义以及每个字段的简要说明。

表 1　　警报通用字段格式定义

字段名	描述说明
idsID	入侵检测系统的 ID 号
alertID	警报 ID 号 (主要参考 Bugtraq ID, CERT ID 和 MITRE CVE)
alertType	警报类型
srcIP	警报源 IP 地址
dstIP	警报宿 IP 地址
srcPort	警报源端口
dstPort	警报宿端口
alertTime	警报时间戳
alertInfo	警报信息和附加说明

4.3　警报关联引擎的实现

在面向多 IDS 的警报关联中，警报关联引擎的目标是根据各 IDS 所报告警报情况来推测网络攻击是否发生，从而判断警报的真假。当使用证据理论来实施警报关联分析时，命题应该为网络攻击是否发生，而各 IDS 报告警报的情况就是命题的证据。警报关联时，首先利用这些证据，构造相应的基本信度分配函数，并对识别框架内的所有命题假设赋予相应的可信度；然后用 Dempster 证据组合规则将这些证据的基本信度分配进行合并，产生一个总体基本信度分配；最后根据决策规则进行决策判断。警报关联引擎的工作原理如图 2 所示。

具体地，分为以下几个步骤。

1) 构建警报关联的识别框架。

由于需要根据多个 IDS 报告的警报来判断对应的网络攻击是否发生，从而确定警报是否为误报，故本文取识别框架 Θ 为$\{A,\neg A\}$，其中 A 表示网络攻击 a 确实发生，$\neg A$ 表示攻击没有发生，且有 $A\cap\neg A=\varnothing$，满足 D-S 理论的条件。依据此识别框架 Θ，则所有可能的命题有：$2^{\Theta}=\{\varnothing,\{A\},\{\neg A\},\{A,\neg A\}\}$，其中命题$\{A\}$，$\{\neg A\}$分别对应于攻击发生和未发生，命题$\{A,\neg A\}$表示根据目前的收到的证据无法推断攻击是否发生。

2) 选择证据体。

在确定 Θ 后，本文使用 IDS 报告警报的情况作为该识别框架 Θ 的证据。对于一个网络攻击 a，设理论上能检测到该攻击的 IDS 集合为 $IDS_{\text{set}}=\{d_i|i=1,2,\cdots,n\}$，则对于任意 $d_i\in IDS_{\text{set}}$，其有产生警报和没有产生警报 2 种情况。

3) 为每个证据定义 BPA 函数。

BPA 函数在 D-S 理论中没有给出通用的求解方法，在实际应用环境中通常需要根据相应的需求来设定。从 IDS 的主要组成部分来看，误报的产生主要与 IDS 的数据收集与分析检测这 2 部分相关[25]，因此，本文在给定具体的信度分配函数值时，采用这 2 个因素作为衡量警报可信度的依据。对于前一个因素，考虑到 IDS 数据的采集直接与 IDS 所处的位置相关，不同的位置 IDS 收集到的数据也会存在差异。因此，本文采用 IDS 所处的位置与被监测系统的位置关系作为衡量 IDS 报告警报可信性度的要素之一。此外，不同的 IDS 由于所采用的检测算法、技术存在差异，对于不同形态的攻击行为，不同的 IDS 将有着不一样的检测精度，所以本文将不同种类的 IDS 检测每种攻击的确信度作为衡量警报可信度的另一要素。

由于 IDS 对网络攻击有产生警报和没有产生警报 2 种情况，所以信度分配函数应分别定义。定义 5 给出了当 IDS 产生警报时，对攻击发生的信度分配函数。当 IDS 不产生警报时，对攻击发生的的信度分配函数和定义 5 类似，只是将等式(5)中当 $X=\{A\}$ 的函数值和当 $X=\{\neg A\}$ 的函数值互换。

定义 5 攻击信度分配函数。设识别框架为 $\Theta=\{A, \neg A\}$，则攻击信度分配函数定义为 $m: 2^{\Theta} \to [0,1]$：

$$m(X)=\begin{cases}0, & X=\varnothing\\ \alpha_{i|a}(1-\beta_i), & X=\{A\}\\ (1-\alpha_{i|a})(1-\beta_i), & X=\{\neg A\}\\ \beta_i, & X=\{A,\neg A\}\end{cases} \tag{5}$$

从式(5)可以看出满足攻击信度分配函数的基本要求 $m_i(\{A\})+m_i(\{\neg A\})+m_i(\{A,\neg A\})=1$。其中，$m(\{A\})$表示当前收到的证据支持网络攻击 a 发生的可信度，$m(\{\neg A\})$表示支持网络攻击 a 没有发生的可信度，$m(\{A,\neg A\})$则表示根据目前收到的证据，还不能确定网络攻击 a 是已发生或未发生的可信度，即支持未知的可信度。式(5)中的参数 $\alpha_{i|a}$ 表示入侵检测系统 d_i 检测网络攻击 a 的确信度，β_i 参数与被攻击系统与该入侵检测系统间的位置关系信息相关，β_i 值越大说明入侵检测系统与被攻击系统之间的距离越远，其警报可信度就会越不确定。

目前，很多 IDS 并没有提供检测某种网络攻击的确信度这样的参数 $\alpha_{i|a}$，对参数 $\alpha_{i|a}$ 值的设定最直接的方法是利用专家的先验知识，但对专家知识依赖太多，工作量较大。本文提出如下统计方法来估计参数 $\alpha_{i|a}$，以便进行报警信息的处理。设 IDS 的历史警报数据集合为 D_L，每条历史警报记录 x_i 对应的攻击种类为 x_{ai}，对应的类标 x_{ci} 取{t，f} 2 种值，t 表示为真警报，f 为误报，则其 $\alpha_{i|a}$ 的估计值可由式(6)估计出。

$$\hat{\alpha}_{i|a} \equiv P(x_{ci}=t \mid x_{ai}=a)=\frac{\sum_{i=1}^{|D_L|} S_i N(a,x_i)}{\sum_{i=1}^{|D_L|} N(a,x_i)} \tag{6}$$

其中，函数 S_i 的值由第 i 个警报记录的真假来决定，函数 $N(a, x_i)$的值由警报记录的对应的网络攻击种类决定，两函数具体定义如下：

$$\begin{cases} S_i=\begin{cases}1, x_{ci}=t\\ 0, x_{ci}=f\end{cases}\\ N(a,x_i)=\begin{cases}1, x_{ai}=a\\ 0, x_{ai}\neq a\end{cases}\end{cases} \tag{7}$$

对于参数 β_i，主要利用具体的网络环境以及被攻击的目标地址来确定。本文认为当 IDS 离被攻击系统越近则报告的关于该系统被攻击的警报的可信度就会越高，本文使用网络中的跳数来衡量网络距离。β_i 的具体计算公式如下：

$$\beta_i=\frac{h_i}{h_{\max}} \tag{8}$$

其中，h_i 表示警报报告的被攻击系统与该入侵检测系统 d_i 间的距离，取值范围为[0,15]，$h_{\max}$ 为最大可能的距离值，本文使用网络中的跳（hop）数来度量，缺省值为 15，当 IDS 与被保护系统同在一个网段上时则 h_i=0，β_i=0。

4) 证据的合成。

根据信度分配函数，可利用 D-S 理论的 Dempster 组合规则式(4)，求得多个证据联合作用下的信度函数值。虽然一般化的 Dempster 组合规则已被证明为 P 完全难解问题[26]，但如果在识别框架只有 2 个互斥元素的具体应用环境时，则由如下的定理 1 可知计算时间复杂度变为 $O(n)$。定理的具体证明可参见文献[21]。

定理 1 Dempster 组合规则在识别框架Θ只有 2 个互斥元素时（即$\Theta=\{B,\neg B\}$时），满足结合律且计算时间复杂度是 $O(n)$，n 为需要合成的证据数目。

式(9)是根据定理 1 得到的对 n 个证据进行组合的计算公式，其中 $C \subset \Theta$。

$$\begin{aligned} m_{1\cdots n}(C) &= m_{1\cdots n-1}(C) \oplus m_n(C) \\ &= (m_{1\cdots n-2}(C) \oplus m_{n-1}(C)) \oplus m_n(C) \\ &\vdots \\ &= m_1(C) \oplus m_2(C) \oplus \cdots \oplus m_n(C) \end{aligned} \tag{9}$$

具体地，2 个警报证据对于不同命题的组合计算公式如式(10)所示：

$$\begin{cases} m_{i,j}(\{A\}) \\ = \dfrac{m_i(\{A\})m_j(\Theta) + m_j(\{A\})m_i(\Theta) + m_i(\{A\})m_j(\{A\})}{1 - m_i(\{A\})m_j(\{\neg A\}) - m_i(\{\neg A\})m_j(\{A\})} \\ m_{i,j}(\{\neg A\}) \\ = \dfrac{m_i(\{\neg A\})m_j(\Theta) + m_j(\{\neg A\})m_i(\Theta) + m_i(\{\neg A\})m_j(\{\neg A\})}{1 - m_i(\{A\})m_j(\{\neg A\}) - m_i(\{\neg A\})m_j(\{A\})} \\ m_{i..j}(\{\Theta\}) \\ = \dfrac{m_i(\Theta)m_j(\Theta)}{1 - m_i(\{A\})m_j(\{\neg A\}) - m_i(\{\neg A\})m_j(\{A\})} \end{cases} \tag{10}$$

5) 综合判断。

根据上述过程对 n 个 IDS 报告警报情况的信度分配进行合成，得到综合信度评价，即 $m_{1\cdots n}(\{A\})$、$m_{1\cdots n}(\{\neg A\})$ 与 $m_{1\cdots n}(\{\Theta\})$，它们分别表示 n 个 IDS 的报警情况对网络攻击 a 发生、未发生以及未知的支持信任度。本文的综合判断原则是取这 3 个信任度中的最大值为最终判定结果，为了安全起见，当输出结果是未知时，本文也认为攻击发生。图 3 给出了描述警报关联算法的伪代码。

input: alerts reported from multiple IDSs that correlate with a network attack *a* which should be decided;
output: alerts are true positive or not;

let ES= {E_i| E_i correlated with a, i=1,2,⋯,m，$m \leqslant n$};
let $m_s(\{A\})$=0; $m_s(\{\neg A\})$=0; $m_s(\{\Theta\})$=1;
for (each $E_i \in ES$) {
let $m_i(\{A\})$, $m_i(\{\neg A\})$, $m_i(\{\Theta\})$ are the basic probability assignment of E_i;
let $m_s(\{A\}) = m_s(\{A\}) \oplus m_i(\{A\})$;
let $m_s(\{\neg A\}) = m_s(\{\neg A\}) \oplus m_i(\{\neg A\})$;
let $m_s(\{\Theta\}) = m_s(\{\Theta\}) \oplus m_i(\{\Theta\})$;
}
if ($m_s(\{\neg A\}) \geqslant m_s(\{A\})$ and $m_s(\{\neg A\}) \geqslant m_s(\{\Theta\})$) {
network attack *a* is not happened;
combine all alerts into one alert and report it as false alert;
}
else {
network attack *a* is real happened;
combine all alerts into one alert and report it as true alert;
}

图 3　基于可信度的警报关联算法描述

5　实验结果与分析

5.1　实验数据

为了验证方法的有效性，本文采用 DARPA 2000 测试数据集[10]进行实验。DARPA 2000 数据集是由 MIT 林肯实验室创建的入侵检测评估数据集，数据由包括 14 台主机的外部 Internet 环境，以及由 39 台主机组成的内部（inside）网络和 6 台主机组成的 DMZ 区域产生。该数据集内容全面，有较为详细的攻击说明文档，同时也是到目前为止得到大家普遍公认，在警报关联分析技术研究中常使用的数据集。数据集包含 2 个多步攻击的场景，分别为 LLDOS1.0 和 LLDOS2.0.2。每个场景的测试数据又由 2 部分组成：一部分数据来源于 DMZ 区域；另一部分来源于内部网络。

考虑到 DARPA 2000 数据集的 2 个场景基本相似，本文仅在第一个场景 LLDOS1.0 的测试数据上进行了实验。实验中，对 DMZ 区域的数据进行入侵检测的 IDS 是 RealSecure Network Sensor 6.0[27]，配置规则为最大覆盖原则；对内部网络数据采用的 IDS 是著名的开源网络入侵检测系统 Snort 2.4[28]，采用与之相对应的 2.4 版本的缺省规则集。图 4 给出了这 2 种 IDS 产生的原始警报的种类和数目的统计情况。

5.2　结果分析

表 2 为 RealSecure Network Sensor 和 Snort 分别在 LLDOS1.0 的 DMZ 区域和内部网络数据上进行检测后，报告的总警报数和误报率情况。

表 2　报告的警报数以及误报率

数据集		IDS	警报数	真警报数	*FPR*
LLDOS 1.0	DMZ	RealSecure Network Sensor 6.0	891	57	93.60%
	Inside	Snort 2.4	840	44	94.76%
	小计		1 731	101	94.17%

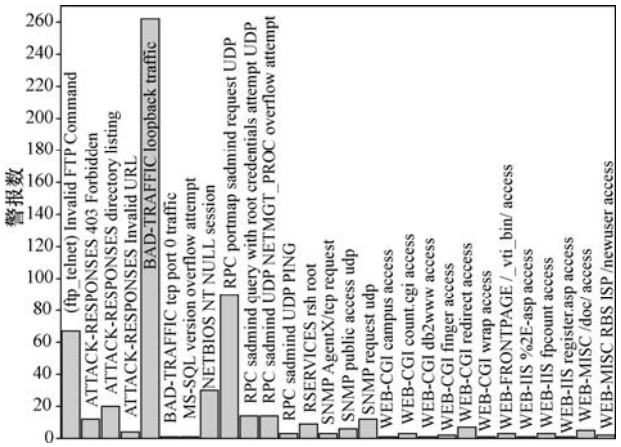
其中，误报率的定义为

$$FPR = \frac{NOFA}{NOA} \times 100\% = \frac{NOA - NOTA}{NOA} \times 100\% \tag{11}$$

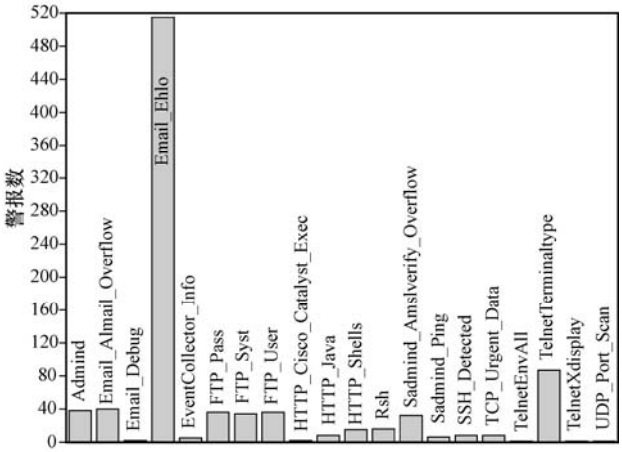
其中，*FPR* 为误报率，*NOFA* 为误报数，*NOA* 为总警报数，*NOTA* 为真警报数。

考虑到一次持续性攻击会在一段时间内产生大量的重复警报，为了便于后续的处理和提高

关联效率，本文使用冗余消除模块 REM 对每个 IDS 产生的原始警报进行了冗余消除，冗余消除时主要使用了警报的类型、空间和时间等多个特征来判断警报是否为冗余警报，限于篇幅，具体的冗余消除方法可参见文献[23]。表 3 为表 2 中 2 个 IDS 报告的原始警报分别经过冗余消除后的结果。



(a) Snort 报告结果



(b) RealSecure Network Sensor 报告结果

图 4　Snort 和 RealSecure Network Sensor 报告的警报种类和数目

表 3　　冗余消除后警报数以及误报率

数据集		IDS	警报数	真警报数	*FPR*
LLDOS1.0	DMZ	RealSecure Network Sensor 6.0	235	51	78.30%
	Inside	Snort 2.4	197	37	81.22%
	小计		432	88	79.62%

表 4 为表 3 中 2 个 IDS 的警报数据经过基于可信度的警报关联引擎 ACE 进行关联处理后的结果。

表 4　　警报关联后的警报数以及误报率

数据集	警报数	真警报数	*FPR*
LLDOS1.0	138	72	47.83%

从实验结果可以看出，由于在关联警报时综合考虑了各 IDS 报告警报的可信度，最终报告的警报数目从原来的 432 条减少为 138 条，减少数目大约为原警报总数的三分之二，同时误报率也由原来的 2 个 IDS 的平均误报率 79.76%下降到 47.83%，可见，本文方法能够有效地减少警报数目和降低误报率。在算法的时间效率上，由本文提出的关联方法花费的时间主要是在多个证据的融合计算上，而根据 4.3 节的定理 1 可知这个计算的时间复杂度为 $O(n)$，因此本文方法还具有较好的实时性。表 5 列出了本文方法与目前具有代表性的几种警报关联方法在多个方面的比较情况。

表 5　　本文方法与其他相关方法的比较

方法	主要目的	实时性能	参数选择难度	需要先验知识	实现难度
基于前因后果	构建攻击场景	差	中	多	高
基于特征相似度	减少警报数	好	高	中	低
基于已知攻击场景	构建攻击场景	差	中	多	中
基于统计分析	构建攻击场景	差	高	少	中
基于数据挖掘	构建攻击场景	中	高	少	中
本文方法	减少警报数和误报	好	低	少	低

由表 5 可知，与目前具有代表性的方法不同，本文方法是从警报可信度的角度来对警报进行精炼，达到减少警报数目和误报的目的。而其他方法的主要目是将隶属于同一攻击步或复合攻击的多个攻击步产生的警报串联起来，以减少警报数目和实现攻击场景重构。这些方法可以很大程度上减少数目和误报，但方法是基于“成功攻击一般是多步攻击场景中的一个步骤，而误报通常都是孤立和随机的”这一假设，认为与攻击场景无关的独立报警为误报。但这一结果缺乏理论上的证明，并且在实际情况中，攻击者有时仅需一个攻击步就可以对系统进行入侵，因此有学者提出识别与过滤误报应当是获得准确的多步攻击场景的前提，而不应当通过关联过程本身来减少误报[29]。而本文方法可以作为这些方法的补充，对警报进行预处理来减少后续处理的警报数目和误报。此外，本文方法还具有对先验知识要求较少且易于实时地对多个 IDS 报告的警报数据进行关联处理等优点。

6　结束语

在多IDS环境中，对大量的警报数据进行精简、合并和消除不确定性，以减少警报数目和降低误报率具有重要的现实意义。为了弥补当前警报关联方法在对来自多个 IDS 警报进行关联时没有考虑各 IDS 可信度差异的不足，本文提出了一种基于各 IDS 报告警报的可信度对警报进行关联的方法。方法以一种实用的不确定性推理理论——证据理论为理论基础，通过构建基本信度分配函数量化各 IDS 报告警报的可信度，并使用 Dempster 证据组合规则融合来自多个 IDS 报告的警报信息，从而推断出所报警报的真实性。通过在 MIT 林肯实验室提供的 DARPA 2000 测试数据集上的实验结果表明，本文方法能够很大程度地消除各 IDS 报告警报的含糊性与冲突性，达到减少警报数目 60%以上，降低误报率到 40%左右。此外，与其他相关的警报关联方法相比较，方法需要的先验知识少，在实时性和实用性方面也具有一定的优势。

参考文献：

[1] 龚俭，吴桦，杨望．计算机网络安全导论[M]．南京：东南大学，2007.
GONG J, WU H, YANG W. The Principles of Computer Network Security[M]. Nanjing: Southeast University Press, 2007.

[2] DOROTHY E, DENNING. An intrusion detection model[J]. IEEE Transactions on Software Engineering, 1987, 13(2):222-232.

[3] SIRAJ A, VAUGHN R B. Alert correlation with abstract incident modeling in a multi-sensor environment[J]. International Journal of Computer Science and Network Security, 2007, 7(8):8-19.

[4] 李家春，李之棠．分布式入侵告警关联分析[J]．计算机研究与发展，2004, 41(11):1919-1923.
LI J C, LI Z T. Correlation analysis for distributed intrusion alert[J]. Journal of Computer Research and Development, 2004, 41(11): 1919-1923.

[5] NING P, CUI Y, REEVES D S, *et al*. Techniques and tools for analyzing intrusion alerts[J]. ACM Transactions on Information and System Security, 2004, 7(2):274-318.

[6] DEBAR H, WESPI A. Aggregation and correlation of intrusion detection alerts[A]. Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection[C]. Davis, CA, USA, 2001. 85-103.

[7] CUPPENS F, MIEGE A. Alert correlation in a cooperative intrusion detection framework[A]. Proceedings of the 2002 IEEE Symposium on Security and Privacy[C]. Berkeley, California, USA, 2002, 202-215.

[8] YU D, FRINCKE D. Alert confidence fusion in intrusion detection systems with extended dempster-shafer theory[A]. Proceedings of the 43rd annual Southeast Regional Conference[C]. Kennesaw, Georgia, 2005, 142-147.

[9] KANG Y H. Theory and Application of Data Fusion[M]. Xian: Press of Electronic Technology University, 1997.

[10] MIT Lincoln Lab, DARPA 2000 intrusion detection scenario specific dataset[EB/OL]. http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index. html, 2000.

[11] 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.
MU C P, HUANG H K, TIAN S F. A survey of intrusion detection alert aggregation and correlation techniques[J]. Journal of Computer Research and Development. 2006, 43(1): 1-8.

[12] VALDES A, SKINNER K. Probabilistic alert correlation[A]. Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection[C]. Davis, CA, USA, 2001. 54-68.

[13] JULISCH K. Clustering intrusion detection alarms to support root cause analysis[J]. ACM Transactions on Information and System Security, 2003, 4(6): 443-471.

[14] MORIN B, DEBAR H. Correlation of intrusion symptoms: an application of chronicles[A]. Proceedings of the 6th International Conference on Recent Advances in Intrusion Detection[C]. Pittsburgh, USA, 2003. 202-215.

[15] PERDISCI R, GIACINTO G, ROLI F. Alarm clustering for intrusion detection systems in computer networks[J]. Engineering Applications of Artificial Intelligence, 2006, 19(4): 429-438.

[16] DAIN O, CUNNINGHAM R K. Fusing a heterogeneous alert stream into scenarios[A]. Proceedings of the 8th ACM Workshop on Computer and Communications Security[C]. Philadelphia, PA, 2001. 1-13.

[17] TEMPLETON S, LEVITT K. A requires/provides model for computer attacks[A]. Proceedings of the 2000 workshop on New security paradigms[C]. Cork Ireland, 2000. 31-38.

[18] ZHOU J, HECKMAN M, REYNOLDS B, *et al*. Modeling network intrusion detection alerts for correlation[J]. ACM Transactions on Information and System Security, 2007, 10(1):1-13.

[19] QIN X, LEE W. Statistical causality analysis of INFOSEC alert data[A]. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection[C]. Pittsburgh, USA, 2003. 73-94.

[20] MAGGI F, ZANERO S. On the use of different statistical tests for alert correlation: short paper[A]. Proceedings of the 10th international

Conference on Recent Advances in Intrusion Detection[C]. Gold Goast, Australia, 2007. 167-177.

[21] 诸葛建伟, 王大为, 陈昱等. 基于 D-S 证据理论的网络异常检测方法[J]. 软件学报, 2006, 17(3): 463-471.
ZHUGE J W, WANG D W, CHEN Y, *et al*. A network anomaly detector based on the D-S evidence theory[J]. Journal of Software. 2006, 17(3): 463-471.

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

[23] 龚俭, 梅海彬, 丁勇等. 多特征关联的入侵事件冗余消除[J]. 东南大学学报, 2005, 35(3): 366-371.
GONG J, MEI H B, DING Y, *et al*. A multi-feature correlation redundance elimination of intrusion event[J]. Journal of Southeast University, 2005, 35(3): 366-371.

[24] DEBAR H, CURRY D, FEINSTEIN B. The intrusion detection message exchange format (IDMEF)[EB/OL]. http://tools.ietf.org/html/rfc4765, 2007.

[25] PIETRASZEK T. Alert Classification to Reduce False Positives in Intrusion Detection[D]. Freiburg, Germany: Univeristy of Freiburg, 2006.

[26] 康耀红. 数据融合理论与应用[M]. 西安: 电子科技大学出版社, 1997.
KANG Y H. Theory and Application of Data Fusion[M]. Xian: Press of Electronic Technology University, 1997.

[27] REALSECURE. ISS RealSecure[EB/OL]. http://www.iss.net, 2007.

[28] ROESCH M. Snort-lightweight intrusion detection for networks[A]. Proceedings of the 13th USENIX Conference on System Administration[C]. Seattle, Washington, 1999. 229-238.

[29] KRUEGEL C, VALEUR F, VIGNA G. Intrusion Detection and Correlation: Challenges and Solutions[M]. Berlin: Springer, 2005.

作者简介：

梅海彬（1973-），男，湖南常德人，东南大学博士生，主要研究方向为网络安全。

龚俭（1957-），男，上海人，博士，东南大学教授、博士生导师，主要研究方向为网络安全、网络行为学。