一种入侵检测系统中告警信息量化评估方法[[1]](#footnote-1)\*

◆马苗苗

（四川大学计算机学院 四川 610065）

摘要：入侵检测系统作为一种比较重要的安全防护技术被广泛部署于实际环境中，如Snort、Suricata、Snorby等各类IDS。但是，当前的IDS仍存在一些问题。在前入侵检测阶段，检测技术不够完善，致使存在漏报、误报等现象；在后入侵检测阶段，产生大量冗余的告警信息，一方面，有价值的警报被湮没在海量冗余的告警信息里；另一方面，很难快速区分判断出这些告警信息的重要程度。使得安全管理员无法充分的了解当前网络环境的安全状况以致于不能及时作出相应的安全响应策略。针对上述存在的问题，本文提出了一种告警信息量化评估方法，综合考虑目标主机或设备的重要性，攻击源的危害性以及攻击危害性三个方面，对这些告警信息进行量化评估以区分紧急的、危害性高的告警信息，使得安全管理员能够清晰直观的了解当前网络的安全状况。

关键词：入侵检测系统；告警信息；量化评估；优先级



0 引言

入侵检测系统IDS作为一种软件系统或硬件设备，用于监视网络和主机活动，包括数据流和信息访问，以识别未经授权的条目和恶意活动[1]。IDS被置于企业组织机构中监视网络中发生的事情，一旦检测到违反安全策略的活动或者攻击迹象等相应行为就产生安全警报，来提醒管理员网络中发生的活动和受保护主机所处的状态以采取相应的措施。然而，IDS每天产生数以万计的告警信息，这些告警信息来自于不同系统的各类事件并充斥着大量无关紧要的警报和误报以及重复告警等。导致真正重要的告警信息被湮没，依靠安全管理员去一条条地识别和判断处理是困难费时和易错的，这是急需解决的问题[2]。针对以上涉及的几个问题，本文提出一种告警信息量化评估方法。根据攻击源的危害性、攻击的危害程度（可能的攻击类型和攻击的置信度）以及所受保护主机的重要性三方面对告警信息进行量化评估。使得安全管理员能够快速直观的判断告警信息的重要性，优先处理紧急的重要报警和清晰的了解当前主机或设备所处的网络安全环境。本文提出的方法在告警信息方面取得不错的效果。

1 信息量化方法

## 1.1 专家赋值法

专家赋值法是一种主观的权重确定方法，又称德尔菲法(Delphi),这种方法是通过邀请该领域内多个专家对考核指标体系进行深入研究。专家根据自身的专业经验知识对指标进行打分，主观判断各指标的重要性，指标权重的结果由统计均值得出，具体流程如图1所示：

1. 确定专家；
2. 专家初评；
3. 统计专家意见；
4. 计算各指标的权重平均数确定权重。

## 1.2 层次分析法

其基本思想是依据相互间的从属关系把复杂问题的各指标分解成递阶层次结构的整体，每层内部指标请该领域内的专家在各个待评价项目之间进行两两比较打分量化，根据两两比较的结果量化形成对应的判断矩阵，通过一定的数学方法计算各个评价项目的相对重要性权值。。具体流程如图2所示:

1. 明确问题，建立层次结构（复杂问题层次结构化，一般分为目标层-要评估的对象、准则层-衡量目标的准则、方案层-具体到因素或手段）
2. 专家量化，形成判断矩阵
3. 进行归一化处理，权重系数求解
4. 检验判断矩阵的一致性（确认计算出的各指标权重是否合理），定义一致性比例指标为,其中定义一致性指标,平均随机性一致指标可通过查询表2-6取得,若CR=0，说明判断矩阵具有完全一致性；<0.1,说明判断矩阵具有满意一致性，即专家量化的判断矩阵是合理的；否则需要调整判断矩阵，重新计算
5. 层次单排序
6. 层次总排序

## 图2 信息熵属性权重计算

## 1.3 变异系数法

变异系数法又称离散系数法[39] ，是一种客观权重确定方法。其基本思想是直接利用各项指标所包含的信息，通过计算数据的差异程度得到变异系数，即可确定指标的权重,指标内部数据差异性越大，权重取值越大。具体流程如图3所示：

1. 进行差异性度量
2. 计算各指标所对应元素的变异系数
3. 综合计算得到各指标的权重

## 1.4 模糊规则

模糊规则（fuzzy rule）本质上来说是一种定义关于x和y的二元模糊关系R，模糊规则表现形式为if x is A then y is B,可简写为A—>B[41] 。其中A、B是由x、y论域上的模糊集定义的，即x、y是条件，A、B是结论。模糊规则决定了输入隶属值对输出集的影响，即if(条件)—>then(结果)，其建立应保证规则库的相关特性，模糊规则的流程表示如图2-5所示

## 图3 改进k-means聚类流程图

2 入侵检测系统中的告警信息量化方法

## 2.1 目标主机或设备的重要性度量方法

当前，主机或设备重要性度量方法一般采用专家赋值法定性直接给出，即专家根据经验知识直接对设备进行打分，或者简单加和得出，即各组成要素的值直接相加，没有考虑主机或设备在不同特性上的要求即不同数据、软件或服务在三元素上的不同侧重点。本文提出的主机或设备整体重要性度量方法既综合考虑了三元素对主机或设备整体重要性，又兼顾了不同类型的主机或设备在三元素方面的不同要求，通过加权赋值定性定量分析能够得到一个相对客观的度量值。本文参照评估标准在C、I、A上采用加权对数平均法来度量。根据不同主机或设备的特点，采用层次分析法对三方面进行赋权，既综合考虑了主机或设备在三属性方面的重要性，又能根据具体种类的不同突出某一属性对主机或设备重要性的影响。量化时使用一个映射函数来度量。

图4 Fisher分特征排序

输入： 样本数据集,属性值构成的决策矩阵A=(Xij)nm,Xij表示第i个数据对象的第j维属性值

步骤：1）正则化决策矩阵A=(Xij)nm为R=(rij)nm

2）第j个属性的信息熵为： 其中

3）数据集第j个属性的权重为：

4）重复2）-3）依次计算各属性权重

输出：数据集属性权重W1 W2 Wr



图3-1 层次结构图

本文提出分类加权和的方法进行重要性度量，其本质和公式3.1一样。由于主机或设备是由软件、数据、硬件组成的，根据主机或设备上安装的软件、包含的数据和承载的硬件本文给出一种细化的方法进行主机或设备重要性度量。具体计算见式3.2。其中α、β、γ为具体主机或设备在软件、数据、硬件上的对应指标权重，由层次分析法所得；V\_soft 、〖V\_data 、V〗\_(hardware )由主机或设备具体包含的软件、数据、硬件度量所得

（3.2）

的具体计算见式3.3，首先罗列出待度量对象包含的软件，并按5分赋值法评估每类软件在功能性(Functionality，F)、可靠性(Dependability，D)、稳定性(Stability，S)上的取值，为每个软件在F、D、S上的权重。

（3.3）

的具体计算见式3.4，首先罗列出待度量对象包含的数据，并按5分赋值法评估每种数据在保密性(Confidentiality，C)、完整性(Integrity，I)、可用性(Availability，A)上的取值，为每个软件在C、I、A上的权重。

（3.4）

的具体计算见式3.5，首先罗列出待度量对象包含的硬件，并按5分赋值法评估每种硬件在可维护性(Mantainability，M)、可控性(Controllability，C)、可扩展性(Extensibility，E)上的取值，为每个软件在M、C、E上的权重。

（3.5）

本文将目标主机或设备的重要性映射到0-1之间，值越高表示该主机越重要，受到安全威胁时造成的损失越严重。

## 2.2 基于攻击源的危害性度量方法

本文采用模糊逻辑的方法从以下三方面判定攻击源的危害性。第一，根据攻击范围进行度量，第二，发动入侵的次数，即频率，频率越高的攻击源认为其下一次是入侵行为的概率更大。第三，发动入侵的危害程度，根据历史记录里发动入侵造成危害性的严重程度来辅助度量其危害性大小，找出过去一段时间内其发动入侵造成的危害性大小，这里，取危害度最高的入侵行为作为度量其危害性大小的值max⁡(H)。综合度量攻击源危害性的模糊规则(fuzzy rules)及度量值如下表3-6所示。

定义：表示针对单个主机发起入侵、表示大范围进行，表示入侵频率很低，表示入侵频率频繁，表示危害性低，表示危害性中等，表示危害性高

，方法流程如图5所示

|  |  |  |  |
| --- | --- | --- | --- |
| **范围（单/多）** | **频率（低/高）** | **严重程度** | **整体危害性** |
| ~ | ～ | Blacklist\_IP | 1 |
|  |  |  | 0.9 |
|  |  |  | 0.8 |
|  |  |  | 0.7 |
|  |  |  | 0.6 |
|  |  |  | 0.5 |
|  |  |  | 0.4 |
|  |  |  | 0.3 |
|  |  |  | 0.2 |
|  |  |  | 0.1 |

|  |
| --- |
| 输入：确定待评估对象-攻击源SIP  步骤：   1. 判断SIP是否在黑名单backlist\_ip里，如果在直接赋值1，否则转3）； 2. 不在黑名单的SIP从三个方面考虑，得到所需的三个参数A 、B、 C;   2.1）通过时间邻域判断源主机是针对单个目的主机还是大范围的目的主机入侵，得到参数A  2.2）查看历史记录t时间内SIP发动入侵的次数，即频率  2.3）查看历史告警信息，获取t时间内发动入侵造成的攻击危害度大小的列表，取造成最大值为其发动入侵的危害程度，得到参数C  3）通过粗糙模糊规则匹配，得到攻击源危害性大小具体度量值  输出：攻击源危害性具体度量值 |

2.3 攻击危害性度量方法

攻击的危害性F(P,V)与攻击种类的优先级P和攻击的置信度V有关。其中攻击种类的优先级P即priority，snort中的priority取值为1-4，值越小表示该类攻击造成的危害性越高，置信度V是指攻击种类与目标节点的相关性，即攻击对象上是否存在这个攻击事件所需的漏洞信息。如果完全匹配即节点上存在被攻击利用的漏洞信息，则置信度为1；否则，置信度为0.1（这里不设置为0和1的原因分别是大量无效攻击也会对主机的正常服务造成影响）

攻击的置信度V取值如式3.10所示：

（3.10）

攻击种类所需的环境可以通过sid查找snort os xml配置文件获取攻击所需的条件

|  |
| --- |
| 1. 通过Classfication字段得知具体攻击类型ClassType，从而得知量化攻击危害性H(t)所需的一个因子H(t)的值-priority 2. 通过sid查找snort os xml和host os xml或目的主机配置，查看该攻击类型所需的条件或环境是否与目的主机的配置满足，若满足条件V(e)为1，否则V(e)为0.1，从而得到量化攻击危害性的因子V(e)的值 3. 从攻击种类的危害性和攻击的置信度来量化攻击危害程度，H(t)=F(P,V)=H(T).V(e),得到攻击危害度值-H(t) |

## 3 实验测试与分析

## 3.1 实验数据

实验将选取IDS数据集DARPA2000作为实验数据集输入；这个数据集是通过模拟LL-DOS1.0和LL-DOS2.0这俩个网络攻击场景，捕获并存储相关的网络流量和数据。在进行实验之前，对样本做过滤、聚合关联信息，

## 3.2 实验设计与结果分析

本文设计实验如下：

第一步：收集原告警信息

实验的目的是生成告警信息。实验使用snort检测引擎对数据集进行检测，触发并执行相应规则动作产生报警。最后，收集告警信息存入数据库。

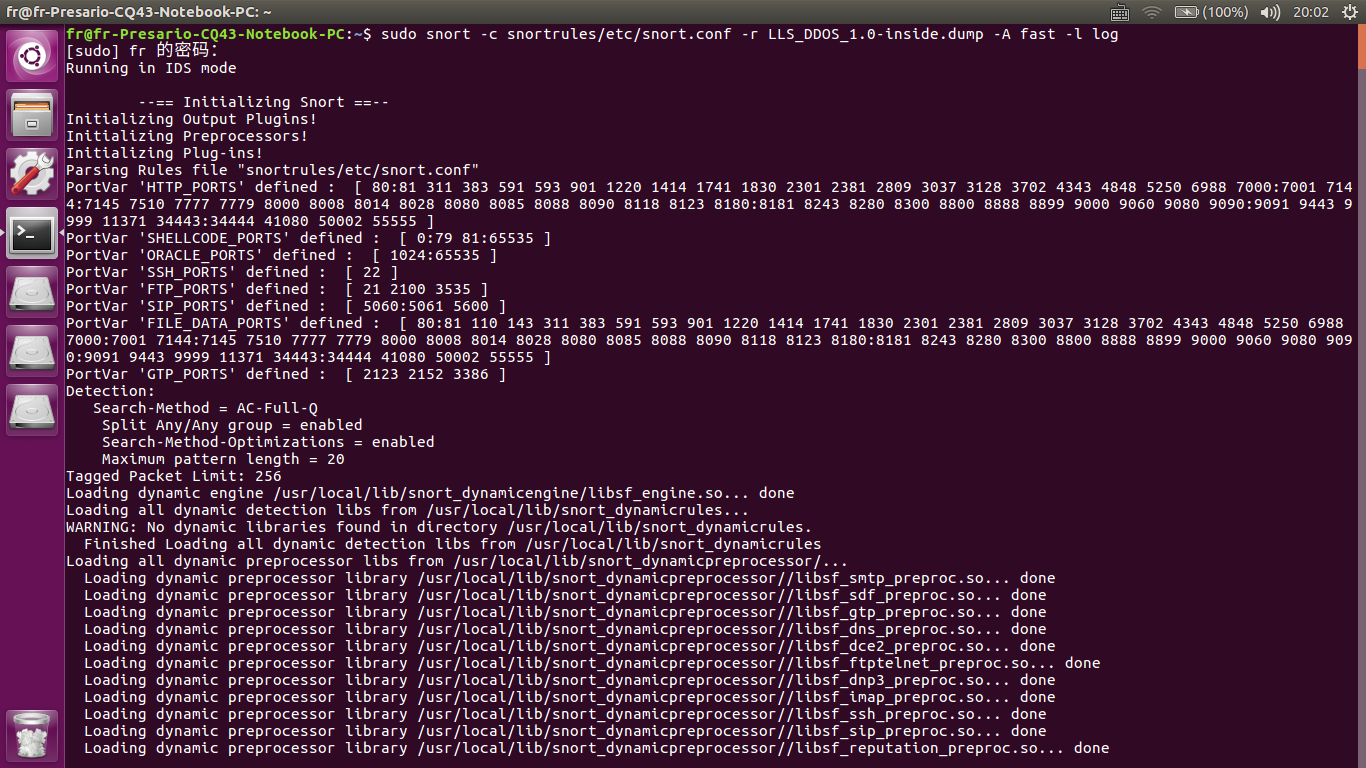


表1 Fisher分对数据特征排序

第二步：过滤告警信息

实验对收集到的告警信息进行预处理，通过分析警报的特征和内容来过滤无效的、不相关、重复等各类无用告警信息，得到有用的告警信息。

表5-1 过滤步骤的实验结果

|  |  |  |  |
| --- | --- | --- | --- |
| 原始告警信息数量 | 无效告警数量 | 重复告警数量 | 不相关告警数量 |
| 27399 | 0 | 10872 | 330 |

第三步：量化评估

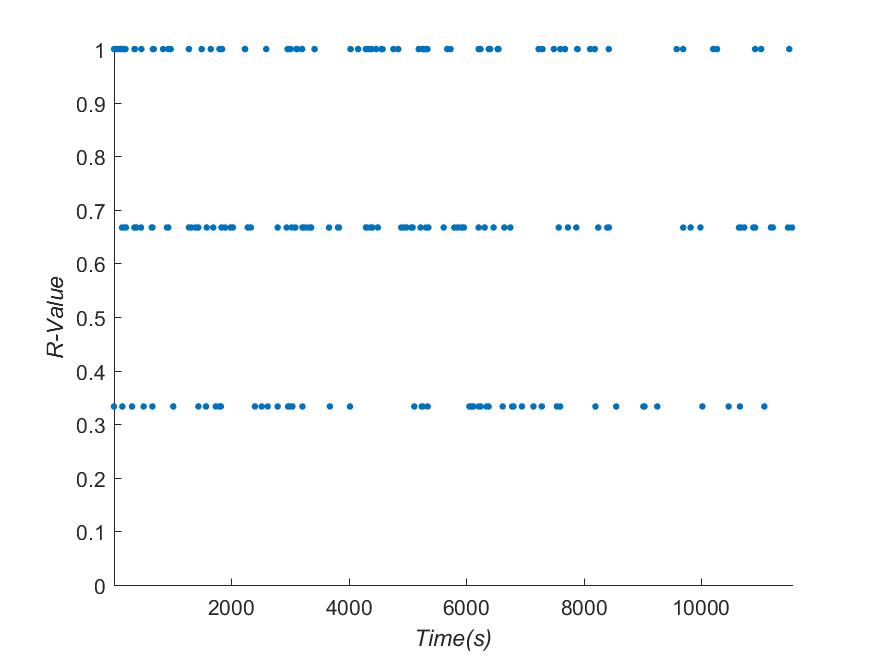


图7 Snort量化结果

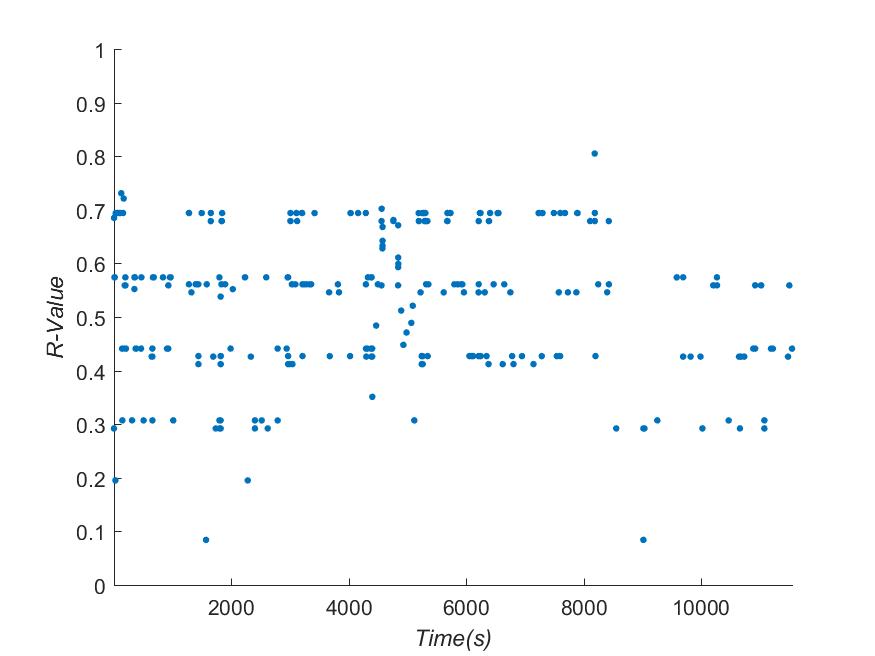


图5-9 本文方法量化结果

通过实验可以看到本文量化方法得到的值之间是波动的，因为考虑到了攻击源的危害性和目标主机的重要性以及攻击置信度，更全面综合的度量了告警信息的重要性，安全管理员可以根据具体值的大小，快速的识别出重要的告警信息，解决了在面对大量相似级别告警信息时难以定位的问题。

4 结束语

本文通过考虑到目标主机或设备的重要性，攻击源的危害性以及攻击危害性三个方面综合量化入侵检测系统中的告警信息，使得安全管理员能根据具体的风险值大小来快速识别出重要的告警信息以便及时作出相应的安全策略。

参考文献：

[1] 卿斯汉,蒋建春,马恒太,等.入侵检测技术研究 综述 [J]. 通信学报 ,2004,25(7):19-29.

[2] Lee W, Stolfo S J.A framework for constructing features and models for intrusion detection systems[J].ACM Transactions on Information and System Security(TISSEC),2000,3(4):227-261.

[3] 江颉,王卓方,陈铁明,等.自适应AP聚类算法及其在入侵检测中的应用[J]. 通信学报 ,2015,36(11):118-126.

[4] Aljarah I，Ludwig S A．Parallel particle swarm optimization clustering algorithm based on MapＲeduce methodology［C］/ /Proc of the 4th World Congress on Nature and Biologically Inspired Computing. [S.l.]: IEEE Press，2012: 104-111.

[5] 周涓,熊忠阳,张玉芳,等.基于最大最小距离法的多中心聚类算法[J]. 计算机应用,2006,26(6):1425-1427.

[6] Peter HARRINGTON.机器学习实战[M].李锐，李鹏，曲亚东，王斌译.北京:人民邮电出版社,2013.

[7] 程正东，章毓晋，樊祥，等.常用Fisher判别函数的判别矩阵研究 [J].自动化学报，2010，36(10):1361-1370. (CHENG Zhengdong，ZHANG Yujin，FAN Xiang，et al.Study on Discriminant Matrices of Commonly-Used Fisher Discriminant Functions [J].Scta Automatica Sinica，2010，36(10):1361-1370.

1. \* 基金项目:国家重点研发计划(2016yfb0800604，2016yfb0800605)，国家自然科学基金项目(61572334)。 [↑](#footnote-ref-1)