基于直觉模糊集理论的 IDS 方法研究

邢瑞康 李成海

(空军工程大学防空反导学院 西安 710051)

摘 要 入侵检测是网络系统安全维护过程中的有效方法之一,主要指通过对网络系统中的各种数据进行收集、分析,进而发现其中存在的可能对系统安全构成威胁的入侵攻击行为,并迅速作出响应的过程。但由于网络空间中的攻击形式多样,具有许多未知和不确定性,因此如何对其中的不确定性进行描述并采取相应的措施成为了构建入侵检测模型的重要一环。直觉模糊理论就是一种针对系统中存在的不确定性问题进行研究的理论。因此,通过对基于直觉模糊集理论的入侵检测方法进行深入研究发现,其对于处理入侵检测系统中大量不确定性问题具有重要的作用和意义。文中对现有文献中 3 种典型的基于直觉模糊集理论的入侵检测方法进行了相对全面的分析介绍,并进行了适当的对比总结,指出了目前各种方法仍存在的不足和未来的研究方向,这对其进一步的发展具有一定的参考价值。

关键词 入侵检测,直觉模糊,模糊推理,模糊聚类,综合评判

中图法分类号 TP301.6 **文献标识码** A

Research on Intrusion Detection System Method Based on Intuitionistic Fuzzy Sets

XING Rui-kang LI Cheng-hai

(Air and Missile Defense College, Air Force Engineering University, Xi'an 710051, China)

Abstract Intrusion detection refers to the technology that collects and analyzes various kinds of data through several key points in a computer network or a computer system, so as to find and respond to possible intrusion attacks. However, due to the variety of attacks in cyberspace and many uncertainties, how to describe and deal with its objective existence of uncertainty has become an important part of constructing an intrusion detection system model. Intuitionistic fuzzy set theory is a theory that studies the problem of uncertainty in the system. Therefore, studying intrusion detection methods based on intuitionistic fuzzy set theory plays an important role in dealing with a large number of uncertainties in intrusion detection systems. This paper summarized the typical intrusion detection methods based on intuitionistic fuzzy set theory in existing literatures and made a proper analysis and comparison, pointing out the shortcomings in the current related methods and the future development direction, which provide some reference value for further study.

Keywords Intrusion detection, Intuitionistic fuzzy, Fuzzy reasoning, Fuzzy clustering, Comprehensive evaluation

1 引言

当今世界正全面走向信息化高速发展的新时代,而信息化的核心即网络。它与国家安全、商业运营以及人们的日常生活息息相关。因此,网络安全问题受到了更多人的关注。了解计算机网络中所存在的各种威胁和攻击,有效地防护和抵抗影响系统安全的威胁,直至最终使网络系统安全有序地发展已经成为人们不懈追求的目标。作为网络安全系统的核心技术之一,入侵检测技术已经成为保障网络空间安全的重要构成要素,而且仍在不停的发展与创新。目前,入侵检测已成为各个相关专家学者以及科研院所研究的重点内容。直觉模糊集(Intuitionistic Fuzzy Sets, IFS)[1]最初是由保加利亚学者 Atanassov 于 1986 年提出的,有效地扩充了 Zadeh 模糊集理论,是对模糊集理论的发展和应用,具有十分重要的意义。本文通过将入侵检测技术与直觉模糊理论相结合,针对网络中的各种入侵行为特征,合理运用直觉模糊理论,深入研究入侵检测系统,为发展入侵检测提供了一种新的方法尝试。

2 入侵检测技术与直觉模糊理论

2.1 入侵检测概念

入侵检测是指通过收集计算机系统网络流量或审计记录中的信息,并对其作相应分析,从而发现计算机系统中存在的违背安全策略的入侵和攻击行为。它是对防火墙的有力补充,不仅防护计算机系统抵抗各种网络入侵,而且有效地提高了管理人员对计算机系统安全的管理能力。入侵检测通常被称为位于防火墙后又一扇网络安全的"防护门",能够在网络各项性能保持不变的情况下对其进行安全监测,针对内部恶意破坏、外部非法入侵和错误操作等提供实时保护措施。入侵检测系统(IDS)主要是由进行入侵检测所需的软、硬件组合而成,通过分析计算机网络流量或系统审计记录等信息,实时发现系统中是否有违反安全策略的异常入侵、攻击行为,对危害到系统机密性、完整性和可用性的潜在行为进行响应和拦截[2]。

本文受国家自然科学基金(61703426)资助。

邢瑞康(1994—),男,硕士生,主要研究方向为网络信息安全,E-mail:18149236069@163.com(通信作者);**李成海**(1966—),男,教授,硕士生导师,主要研究方向为网络信息安全等。

2.2　入侵检测的发展

入侵检测的概念最初是由 Anderson 提出的，他把那些对系统信息以非授权方式进行的访问、操作，以及致使系统稳定性和可靠性降低甚至破坏的行为定义为入侵行为[2]。Denning[3]于 1985 年最先提出了一种入侵检测的基本通用模型。1988 年，Smaha[4]设计开发了用以辅助系统安全管理员对网络入侵行为进行安全监查的 Haystack 入侵检测系统。Lunt 等[5]进一步深入研究了入侵检测模型，并于 1989 年提出了新的入侵检测专家系统 IDES(Intrusion Detection Expert System)模型，这种模型通常采用统计和基于规则的方法来对系统进行异常检测，并有效地提高了入侵检测系统的检测效率，使系统更加完善。1990 年，Heberlein 等[6]提出了基于网络的入侵检测概念。1996 年，Chen 等[7]提出了一种基于图形的入侵检测系统，为解决多数入侵检测系统中存在的可伸缩性不足的问题做出了巨大的贡献。

2.3　入侵检测概念

入侵检测系统(IDS)通常使用两种基本的方法来对事件进行分析并对入侵行为进行检测，一种是误用检测(Misuse Detection)，另一种即为异常检测(Anomaly Detection)。通常，将两种检测方法加以结合就构成了混合型入侵检测的方法。

误用检测又称为特征检测，其基本假设为：所有的入侵行为都可以被表示出来，系统负责检查主体的行为是否与这些入侵行为相符。因此，对于已知入侵行为检测，误用检测的效率较高，但入侵行为特征数据库需要实时更新，才能满足系统将新的入侵行为检测出来，因此，其灵活性和自适应性相对较差，漏警率也比较高。目前，通常将专家系统、模式匹配、着色 Petri 网、神经网络、人工免疫学等技术应用于误用入侵检测系统中。

异常检测的基本假设是：入侵者的攻击行为与主体的行为活动不同。通过将正常行为活动构建为授权的用户活动轮廓，把现有行为活动中的违背授权用户活动轮廓的情况判定为入侵行为。在此机制下，它的检测方式不依赖于攻击模式库的完备性，而且能够发现新的攻击类型。但通常来讲，它对攻击的检测精度低，存在相对较高的误报、漏报率。通常应用于异常检测方法有：基于统计分析方法的异常检测方法、基于模式预测方法的异常检测方法、基于相似度实例学习的方法、基于神经网络的方法等。

混合型检测的主要过程是通过对入侵者的攻击行为和系统授权的正常行为活动进行学习，进而将系统的数据特征模式加以描述，最后形成一种既适应于异常检测，又适应于误用检测的入侵检测模型。

通过获取数据来源不同的方式对入侵检测技术进行划分，其通常可以分为两种，即基于主机的入侵检测系统和基于网络的入侵检测系统。基于主机的入侵检测系统是在单个主机上获取数据，包括其中的审计记录和日志文件中的数据等，通常也对主机上的其他重要信息也进行监测，如文件属性、进程状态等，通过有效地分析这些提取的数据来达到对入侵行为检测的目的。基于网络的入侵检测系统的核心是将通过对网络数据包进行捕获过滤得到的数据作为数据源，并通过协议分析、特征识别、统计分析等方法对系统中的入侵行为进行识别检测。

1985 年，Dennning[3]研发并提出了通用的入侵检测系统模型，该模型收集主机系统审计记录等相关数据源，分析并生成了网络系统中正常行为模式的轮廓，通过对轮廓的变化差异进行检测对比，进而检测出网络系统中的异常行为模式。

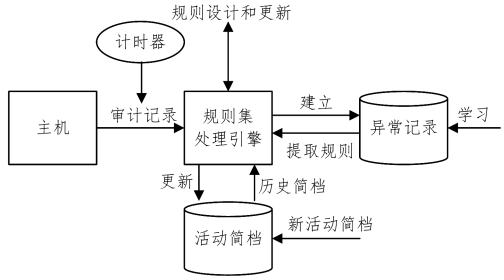

图 1　通用入侵检测系统模型

2.4　直觉模糊集理论及发展

由于直觉模糊集增加了一个新的属性参数——非隶属度函数，因此极大地发展和完善了 Zadeh 模糊集理论。1986 年，保证利亚学者 Atanassov 完整地定义了直觉模糊集以及直觉模糊集理论中基础运算法则和定理的相关内容。1993 年，Gun 等[8]首次提出并命名了 Vague 集，并且 Bustince 等[9]证明了 Vague 集也是直觉模糊集的一种，同时对直觉模糊关系的运算性质[10]、直觉模糊集的构造和熵等进行了深入的研究[11]。Eulalia 等[12]对直觉模糊集之间的距离进行了研究并作出了相关定义，同时研究并发展了在距离基础上的相似度的概念[13]；Xu 等[16]对直觉模糊相似度进行了研究并将其应用于多属性决策。Zhao 等[17]对基于 Vague 关系的模糊聚类进行了研究发展。雷英杰及其科研团队研究了包括直觉模糊关系及其合成运算、直觉模糊推理及其在威胁估计和态势评估中的应用、直觉模糊逻辑语义算子、直觉模糊聚类及其在数据关联和目标识别中的应用等一些列问题[18]。

直觉模糊理论已经成功应用于人工智能领域、决策分析领域、模式识别领域及智能信息处理等许多方面。

3　基于 IFS 的 IDS 技术

对于网络的各种攻击入侵，如果系统能够将它们迅速高效地检测出来，就可以使得系统免于遭受各种不必要的资源以及网络空间的浪费，让系统更好地运行，进而使其更为安全可靠地为用户和网络提供帮助服务。因此，大量专家学者从不同方面提出了许多机制下的入侵检测方法，如混沌理论[19]、多元相关分析[20]、行为分析、模式匹配、生物免疫系统、神经网络、专家系统、数据挖掘、遗传算法、统计方法[21]和时间序列分析[22]等。这些方法优劣不同，所应用的情形亦不同。它们不同程度地提高了检测的效率和效能，能够满足不同条件下的需求。而本文所做的工作是归纳总结直觉模糊集理论是如何有效地应用于入侵检测系统并使之完善。正如前所述，由于网络中各种攻击存在许多的未知和不确定性，因此在建立入侵检测系统的模型时必须对其客观存在的不确定性进行描述并作处理，因此关于入侵检测的研究也是基于不确定性理论开展的，而直觉模糊理论就是利用直觉模糊知识进行的一种不确定性理论研究，它对处理不确定信息系统建模具有更大的灵活性和更好的说服力。

3.1 基于直觉模糊推理的入侵检测方法

文献[23]提出了一种基于直觉模糊推理的入侵检测模型,其主要思想是:首先对入侵的特征属性进行处理,对其构建直觉模糊集合、隶属函数以及非隶属函数;然后,在直觉模糊空间中构建推理规则,进而设计推理算法和解模糊算法;最后通过入侵检测的实例仿真,验证入侵检测的结果。

基于直觉模糊推理算法的入侵检测方法的基本过程描述如下。

(1)对攻击行为的特征属性及检测的模糊性进行描述,同时对初始数据进行预处理,其步骤为:采用十进制方式对每一个字符进行编号,然后将字符型的数据转换成数值型数据,并把每一类特征数据的值域限定在区间[0,1]中,最后再将这些数值(包括连续性数值)都线性映射到[0,1]之间。对于入侵检测所得到结果的预处理主要是将入侵检测的结果分成 5 类,即正常、DoS 攻击、Probing 攻击、R2L 攻击和 U2R 攻击,并分别与 0,1,2,3,4 相对应,最后再将这些数值线性映射到[0,1]之间。

(2)对入侵的特征属性进行处理,对其构建直觉模糊集合、隶属函数以及非隶属函数的过程就是将数据集的属性看作直觉模糊变量,使得每一个直觉模糊变量都有不同的直觉模糊值,进而通过相应的直觉模糊集以及其隶属函数和非隶属函数来描述直觉模糊值。在合理的情况下令 $\pi_A(x)=0$。

类别属性就是含有 M 个类别值的属性。为每个类别分别建立直觉模糊集合,即其隶属函数为:

$$\mu_A(x)=\begin{cases}0, & x\leqslant a\\ \dfrac{x-a}{b-a}, & a\leqslant x\leqslant b\\ \dfrac{c-x}{c-b}, & b\leqslant x\leqslant c\\ 0, & c\leqslant x\end{cases} \tag{1}$$

非隶属函数为:

$$\gamma_A(x)=1-\mu_A(x)$$

关于量化属性,其隶属函数为:

$$\mu_{A\text{-high}}(x)=\begin{cases}0, & x\leqslant a\\ \dfrac{x-a}{b-a}, & a\leqslant x\leqslant b\\ 1, & x>b\end{cases} \tag{2}$$

$$\mu_{A\text{-medium}}(x)=\begin{cases}0, & x<a\\ \dfrac{x-a}{b-a}, & a\leqslant x<b\\ 1, & x=b\\ \dfrac{c-x}{c-b}, & b\leqslant x<c\\ 0, & x\geqslant c\end{cases} \tag{3}$$

$$\mu_{A\text{-low}}(x)=\begin{cases}1, & x<a\\ \dfrac{b-x}{b-a}, & a\leqslant x\leqslant b\\ 0, & x>b\end{cases} \tag{4}$$

非隶属函数为:

$$\gamma_{A\text{-high}}(x)=1-\mu_{A\text{-high}}(x) \tag{5}$$

$$\gamma_{A\text{-medium}}(x)=1-\mu_{A\text{-medium}}(x) \tag{6}$$

$$\gamma_{A\text{-low}}(x)=1-\mu_{A\text{-low}}(x) \tag{7}$$

量化属性的直觉模糊集合及其隶属函数如图 2 所示。

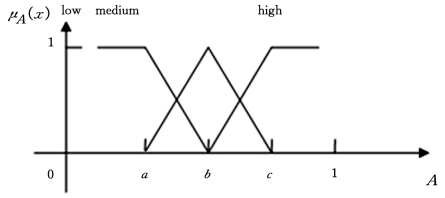

图 2 量化属性的直觉模糊集合及其隶属函数

在输出论域 U,入侵检测结果化分为 5 类,即输出在[0,0.2]之间为正常,在[0.2,0.4]之间为 DoS 攻击,在[0.4,0.6]之间为 Probe 攻击,在[0.6,0.8]之间为 R2L 攻击,在[0.8,1]之间为 U2R 攻击。

(3)建立系统推理规则,其形式为:

L^l:IF x_1 is A_{ix1} and x_2 is A_{ix2} and … and x_6 is A_{ix6}

THEN z_l is C_j

$i_{x1}=1,2,\cdots,N_{\text{duration}}$, $i_{x2}=1,2,\cdots,N_{\text{protocol}}$, …, $i_x=1,2,\cdots,N_{\text{dst}}$

$j=1,2,\cdots,N_u$

其中,x_1, x_2, …, x_6 是输入变量,A_{ix1}, A_{ix2}, …, A_{ix6} 是前提部分语言项。z_l 为系统根据第 l 条规则所得到的输出。C_j 为输出论域中的一个模糊子集 U_k,$k=1,2,\cdots,N_u$。

(4)设计推理算法和清晰化算法。算法的具体过程如算法 1 所示。

算法 1

输入:规则库 R(设含有 n 条规则),事实即某条数据 A′

输出:检测结果

Step1 计算某条数据与各规则的相似度 $S(A',A_i)$,i=1,2,…,n。

Step2 计算某条数据与各规则的方向函数 $D(A',A_i)$,i=1,2,…,n。

Step3 计算某条数据与第 i 条规则的推理结果。

Step3.1 当 $s=S(A',A_i)\geqslant 0.5$ 时,若 $D(A',A_i)\geqslant 0$,则 $z_i'=z_i^s$,否则 $z_i'=z_i^{-s}$。

Step3.2 当 $s=S(A',A_i)<0.5$ 时,$z_i'=sz_i$。

Step4 计算最后推理结果:$z'=z_1'\cup z_2'\cup\cdots\cup z_n'$。

该算法的时间复杂度为 $O(qn)$。

(5)采用重心法解模糊算法。

这个方法将 IFS 理论引入信息安全领域,用来进行入侵检测研究,但它也存在一个重要问题,即随着考虑因素的增加存在“组合爆炸”的问题。

文献[24]提出了一种基于自适应直觉模糊推理的入侵检测算法,通过分析入侵检测的特点与存在的局限性,建立基于自适应神经网络直觉模糊推理系统(ANIFIS)的入侵检测模型。其对解决“组合爆炸”的问题提供了方法思路。

3.2 基于直觉模糊综合评判的入侵检测方法

文献[18]将入侵检测问题归结为综合评价问题,建立 5 种基于三角模的直觉模糊综合评判模型。

模型 1 $B_1=T_1(X,R)=X\cdot R$,即定义:

$$(\mu_{bj},\gamma_{Rij})=\left(\bigvee_{i=1}^{n}(\mu_{xi}\cdot\mu_{Rij}),1-\bigvee_{i=1}^{n}(\mu_{xi}\cdot(1-\gamma_{Rij}))\right),\quad j=1,2,\cdots,m \tag{8}$$

这种评判模型突出了主要元素,定义为主因素突出型。

模型 2 $B_2=T_2(X,R)=X*R$,即定义:

$$(\mu_{bj},\gamma_{Rij})=\left(\sum_{i=1}^{n}(\mu_{xi}\cdot\mu_{Rij}),\sum_{i=1}^{n}(\mu_{xi}\cdot\gamma_{Rij})\right),j=1,2,\cdots,m \tag{9}$$

这种评判模型将各种因素按加权比分别计入决策结果之中,使得决策过程更为均衡。

模型 3　$B_3=T_3(X,R)=X\otimes R$,即定义:

$$(\mu_{bj},\gamma_{Rij})=((\mu_{x1}\wedge\mu_{R1j})\exp(\mu_{x2}\wedge\mu_{R2j})\cdots\exp(\mu_{xn}\wedge\mu_{Rnj}),1-((\mu_{x1}\wedge(1-\gamma_{R1j}))\exp(\mu_{x2}\wedge(1-\gamma_{R2j}))\cdots\exp(\mu_{xn}\wedge(1-\gamma_{Rnj})))),\ j=1,2,\cdots,m \tag{10}$$

这种评判模型则主要突出次要因素的作用,定义为次因素突出型。

模型 4　$B_4=T_4(X,R)=X\vec{\otimes}R$,即定义:

$$(\mu_{bj},\gamma_{Rij})=(\sum_{i=1}^{n}(\mu_{xi}\wedge\frac{\mu_{Rij}}{\sum_{k=1}^{n}\mu_{Rkj}}),1-\sum_{i=1}^{n}(\mu_{xi}\wedge\frac{1-\gamma_{Rij}}{\sum_{k=1}^{n}(1-\gamma_{Rkj})})),j=1,2,\cdots,m \tag{11}$$

这种评判模型经各种因素的影响程度平均化。

模型 5　$B_5=T_5(X,R)=X\vec{\otimes}R$,即定义:

$$(\mu_{bj},\gamma_{Rij})=(\sum_{i=1}^{n}(\mu_{xi}\wedge\mu_{Rij}),1-\sum_{i=1}^{n}(\mu_{xi}\wedge1-\gamma_{Rij})),j=1,2,\cdots,m \tag{12}$$

这种评判模型的特点是重点突出主要因素的作用。

用直觉模糊综合评判方法来求解入侵检测问题的基本步骤如下。

步骤 1　建立归一化的直觉模糊综合评判模型;

步骤 2　建立入侵检测指标体系;

步骤 3　确定入侵特征的权重向量;

步骤 4　确定入侵特征的效用值,进行归一化处理及直觉模糊度量,形成检测矩阵;

步骤 5　进行检测计算,得到检测结果。

模糊综合评判方法是一种得到广泛使用的成熟而通用的评价方法。本方法在本质上把基于模糊集理论的综合评判法推广成为基于三角模的直觉模糊综合评判方法,使得评判结果的客观性和可靠性得到提高。但由于评判模型的特点各异,给使用者带来了一定的麻烦,对于同一事物采用不同的两种模型有可能会得到两种截然相反的结果;另外,评判模型权重确定的过程中主观因素影响也相对较大,在最后的评估过程中,用"最大真值原则"来对评判结果进行处理,使得对于评判结果的感知过于灵敏。

3.3　基于直觉模糊聚类的入侵检测方法

模糊聚类分析[26]是入侵检测领域中常见的方法之一,也是目前许多专家学者研究的热点之一。直觉模糊 C 均值(Intuitionistic Fuzzy C-Means,IFCM)聚类算法[27]也是一种基于目标函数的聚类算法。

文献[36]详细描述了直觉模糊 C-均值聚类算法,主要过程如下。

设被分类对象的集合为:

$A=\{A_1,A_2,\cdots,A_n\}$

假定每一个对象的特征指标是 m 维的直觉模糊集,可以表示为:

$$A_j=(\langle\mu_{A_j}(x_1),\gamma_{A_j}(x_1)\rangle,\langle\mu_{A_j}(x_2),\gamma_{A_j}(x_2)\rangle,\cdots,\langle\mu_{A_j}(x_m),\gamma_{A_j}(x_m)\rangle)$$

如果将对象构成的集合 A 最终分为 c 类($2\leqslant c\leqslant n$),且由 c 个聚类中心向量所构成的矩阵表示为 $V=(V_1,V_2,\cdots,V_c)^{\mathrm{T}}$,其中:

$$V_i=(\langle\mu_{V_i}(x_1),\gamma_{V_i}(x_1)\rangle,\langle\mu_{V_i}(x_2),\gamma_{V_i}(x_2)\rangle,\cdots,\langle\mu_{V_i}(x_m),\gamma_{V_i}(x_m)\rangle)$$

分类对象 A_j 与聚类中心 V_i 之间的关系为模糊关系,对 A 的每一种分类结果仍然是一个模糊矩阵 $U=(\mu_{ij})_{c\times n}$,且满足条件:

$$\mu_{ij}\in[0,1];\sum_{i=1}^{c}\mu_{ij}=1,\forall j;\sum_{j=1}^{n}\mu_{ij}>0,\forall i$$

求出合适的模糊分类的矩阵 U 和中心矩阵 V,使得如下的目标函数:

$$J(U,V)=\sum_{j=1}^{n}\sum_{i=1}^{c}(\mu_{ij})^qD(A_j,V_i)^2 \tag{13}$$

达到极小,以此得到最佳的模糊分类。其中 $D(A_j,V_i)$ 为直觉模糊集 A_j 与 V_i 之间的直觉模糊距离。根据需要,选择通过式(14)来计算距离:

$$D(A_j,V_i)=\{\sum_{k=1}^{m}w_k[\alpha(\mu_{A_j}(x_k)-\mu_{V_i}(x_k))^2+\beta(\gamma_{A_j}(x_k)-\gamma_{V_i}(x_k))^2+\lambda(\pi_{A_j}(x_k)-\pi_{V_i}(x_k))^2]\}^{\frac{1}{2}} \tag{14}$$

其中,$w_k\in[0,1]$,$k=1,2,\cdots,m$ 表示特征比例权重,一般取 $w_k=\frac{1}{2m}$;$\alpha,\beta,\lambda\in[0,1]$,用来表示隶属度、非隶属度以及直觉指数差异分别所占的比例权重,通常取 $\alpha=\beta=\lambda=1$。

用迭代法求式(13)近似解的步骤如下:

第 1 步　选定分类数 c,$2\leqslant c\leqslant n$,取一初始模糊分类矩阵 $U^{(0)}$,逐步迭代,$l=0,1,2,\cdots$。

第 2 步　对于 $U^{(l)}$,计算聚类中心:

$V^{(l)}=(V_1^{(l)},V_2^{(l)},\cdots V_c^{(l)})^{\mathrm{T}}$

其中,

$$V_{\mu_i}^{(l)}=\sum_{j=1}^{n}(\mu_{ij}^{(l)}/2+\gamma_{ij}^{(l)}/2)^qA_{\mu_j}/\sum_{j=1}^{n}(\mu_{ij}^{(l)}/2+\gamma_{ij}^{(l)}/2)^q \tag{15}$$

$$V_{\gamma_i}^{(l)}=\sum_{j=1}^{n}(\mu_{ij}^{(l)}/2+\gamma_{ij}^{(l)}/2)^qA_{\gamma_j}/\sum_{j=1}^{n}(\mu_{ij}^{(l)}/2+\gamma_{ij}^{(l)}/2)^q \tag{16}$$

第 3 步　修正模糊分类矩阵 $U^{(l)}$:

(1)对于 $\forall i$,$i=1,2,\cdots c$,都有 $D(A_j,V_i)>0$,则:

$$\mu_{ij}^{(l+1)}[\sum_{k=1}^{c}(\frac{D(A_j,V_i^{(l)})}{D(A_j,V_k^{(l)})})^{\frac{2}{q-1}}]^{-1} \tag{17}$$

(2)若 $\exists k$,$k=1,2,\cdots,c$,使得 $D(A_j,V_k)=0$,则:

$$\begin{cases}\mu_{ij}^{(l+1)}=1, & i=k\\ \mu_{ij}^{(l+1)}=0, & i\neq k\end{cases} \tag{18}$$

第 4 步　比较 $U^{(l)}$ 与 $U^{(l+1)}$,若对于取定的精度 $\varepsilon>0$,有

$\max\{|\mu_{ij}^{(l+1)}-\mu_{ij}^{(l)}|\}\leqslant\varepsilon$

则 $U^{(l+1)}$ 和 $V^{(l)}$ 即为所求,停止迭代;否则,$l=l+1$,回到第 2 步,重复进行。

算法中,在需分类的对象的数目较多、分类数十分有限而且聚类中心点相对特殊的情况下,通常也选用初始化的聚类中心 $V^{(0)}$ 来作为初始起点,可以大大缩减计算量。然而,传统的基于直觉模糊聚类的算法也存在易陷入局部最优的问题等。

文献[25]提出了一种基于 GA 与 IFCM 的入侵检测算法,用于解决直觉模糊 C-均值(IFCM)聚类算法易陷入局部最优的问题,其主要过程是:首先,通过标定适应度值和群体多样化使遗传算法(GA)得到改进,并把 IFCM 算法和改进后的 GA 算法相联系,形成一种改进的 IFCM 算法并将之应用于入侵检测技术中。基于 GA 与 IFCM 的入侵检测算法通过对传统遗传算法的改进,使其克服了"早熟"现象,算法收敛的

速度得以提高，全局寻优的效果也更加突出。但该算法在入侵检测过程中的时间效度指标有待提高，因此，下一步的改进的方向是减少算法的工作量以提高时间效度。

4 发展方向

本文研究了现阶段直觉模糊理论在入侵检测方法中的应用，而直觉模糊集理论还需要不断的完善与发展，入侵检测技术本身也处于不断变化的网络空间中，亟需广大专家学者进行更加深化的研究与创新，譬如以下几个方面。

关于 IFS 理论研究：目前为止，世界上关于直觉模糊理论的研究文献在逐渐增加，推动了 IFS 的发展，IFS 理论研究成果也越来越多。直觉模糊理论虽然受到了较高的关注度，但作为 Zadeh 模糊集理论发展的主要方向之一，仍有许多工作有待完善。譬如，非隶属度函数加入后，基于 Zadeh 模糊集的结论定理运算性质是否同样适用，应如何改进与完善等都需要进一步研究。

关于 IFS 应用研究：目前，多数关于 IFS 的研究仍处于理论研究阶段，而其应用成果相对较少，只有在少数几个领域的应用，比如医学、多属性决策等领域。从现有的研究成果来看，相对于 Zadeh 模糊集理论，直觉模糊理论有更强的适用性和更高的效用度，因此，对基于直觉模糊理论的应用研究仍需不断深入。

关于 IDS 研究：利用直觉模糊相关理论解决入侵检测技术中的相关应用问题，是对网络信息安全技术方面的一次新思路的拓展探索。虽然目前关于入侵检测技术的研究是网络安全研究的热点之一，而且方法繁多，成果显著，但网络安全形势日渐险峻，目前的技术方法与实际的应用需求仍有较大距离，还需相关研究专家学者不断地进行方法创新，为营造良好的网络安全环境不懈努力。

结束语 本文针对入侵检测，首先研究了基于直觉模糊推理的入侵检测方法，给出了一种新的直觉模糊相似度的度量方法，并依此建立了基于强相似度的推理方法；其次将入侵检测归结为一个综合评判问题，给出了基于直觉模糊综合评判的入侵检测方法；进而对基于直觉模糊聚类的入侵检测方法进行了研究；最后对各种基于直觉模糊与入侵检测方法的不足之处与发展方向进行总结。本研究对今后入侵检测的发展研究具有一定的借鉴意义。

参 考 文 献

[1] ATANASSOV K. Intuitionistic fuzzy sets [J]. Fuzzy Sets and Systems, 1986, 20(1): 87-96.

[2] ANDERSON J P. Computer security threat monitoring and surveillance[R]. PA 19034, USA, 1980, 4.

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

[4] SMAHA S E. Haystack: an intrusion detectionsystem[C]// Aerospace Computer Security Applications Conference. Piscataway: IEEE Conference Publications, 1988: 37.

[5] LUNTTF, JAGANNATHANR, LEER, et al. Knowledge-based intrusion detection[C] // AI Systems in Government Conference. Piscataway: IEEE Conference Publications, 1989: 102-103.

[6] HEBERLEIN L T, DIAS G V, LEVITT K N, et al. Anetwork security monitor [C]// IEEE Computer Society Symposium on Research in Security and Privacy. 1990: 296-207.

[7] CHEN S S, CHEUNG S, CRAWFORD R H, et al. GrIDS-A Graph Based Intrusion Detection System for Large Networks[C]// Proceedings of the 19th National Information System Security Conference. 1996: 56-57.

[8] GUN, BUEHRER. Vague sets are intuitionistic fuzzy sets[J]. Fuzzy Sets and Systems, 1996, 79(3): 403-405.

[9] BURILLO P, BUSTINCE H. Intuitionistic fuzzy relations (Part I) [J]. Mathware Soft Computing, 1995, 2: 5-38.

[10] BUSTINCE H, BURILLO P. Vague sets are intuitionistic fuzzy sets[J]. Fuzzy Sets and Systems, 1996, 79(3): 403-405.

[11] BUSTINCE H, BURILLO P. Correlation of interval-valued intuitionistic fuzzy sets[J]. Fuzzy Sets and Systems, 1995, 74(2): 237-244.

[12] EULALIA S, JANUSZ K. A concept of similarity for intuitionistic fuzzy sets and its use in group decision making [C]// IEEE International Conference on Fuzzy Systems. 2004: 1129-1134.

[13] EULALIA S, JANUSZ K. Entropy for intuitionistic fuzzy sets [J]. Fuzzy Sets and Systems, 2001, 118(3): 467-477.

[14] 林琳. 直觉模糊集在近似推理与决策中的应用[D]. 大连：大连理工大学，2006.

[15] 雷英杰，王宝树，苗启广. 直觉模糊关系及其合成运算[J]. 系统工程理论与实践，2005，25(2)：113-118，133.

[16] XU Z S, CHEN J, WU J J. Clustering algorithm for intuitionistic fuzzy sets [J]. Information Sciences, 2008(178): 3775-3790.

[17] ZHAO F X, MA Z M, YAN L. Fuzzy Clustering Based on Vague Relations[C]// FSKD 2006. 2006: 79-88.

[18] 雷英杰，王宝树. 直觉模糊集时态逻辑算子及扩展运算性质[J]. 计算机科学，2005，11(32)：52-55.

[19] CHEN Y H, MA X L, WU X Y. DDoS Detection Algorithm Based onPreprocessing Network Traffic Predicted Method and Chaos Theory[J]. IEEE Communications letters, 2013, 17(5): 1052-1054.

[20] TAN Z Y, JAMDAGNI A, He X J, et al. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(2): 447-456.

[21] FEINSTEIN L, SCHNACKENBERG D, BALUPARI R, et al. Statistical Approaches to DDoS Attack Detection and Response [C] // Proceedings of the DARPA Information Servivability Conference and Exposition (DISCEX'03). Washington DC: IEEE Computer Society, 2003: 303-314.

[22] THANASIS V, ALEXANDROS P, CHRISTOS I, et al. Real-time Network Data Analysis Using Time Series Models[J]. Simulation Modelling Practice and Theory, 2012, 29(C): 173-180.

[23] 张弛，雷英杰，黄孝文. 基于直觉模糊推理的入侵检测方法[J]. 微电子学与计算机，2009，11(26)：185-188.

[24] 黄孝文，张弛. 基于自适应自觉模糊推理的入侵检测方法[J]. 计算机应用，2010，5(30)：1198-1207.

[25] 王亚男，叶蓓，雷英杰. 基于 GA 与 IFCM 聚类算法的入侵检测[J]. 计算机工程，2013，9(39)：170-173.

[26] 张国锁，周创明，雷英杰. 改进 FCM 聚类算法及其在入侵检测中的应用[J]. 计算机应用，2009，29(5)：1336-1338.

[27] 贺正洪，雷英杰. 直觉模糊 c-均值聚类算法研究[J]. 控制与决策，2011，26(6)：847-850，856.

[28] 贺正洪，雷英杰，王刚. 基于直觉模糊聚类的目标识别[J]. 系统工程与电子技术，2011，33(6)：1283-1286.

[29] 张弛. 基于直觉模糊推理的入侵检测方法研究[D]. 西安：空军工程大学，2008.