[1]网络入侵意图识别方法综述

宁卓　龚俭

（东南大学计算机科学与工程系 江苏南京 210096）

（江苏省计算机网络技术重点实验室）

摘要　复合攻击的检测是近年来 IDS 致力解决的一个重要问题。研究表明解决这个问题的根本途径在于建立有效的模型积累、识别多报文间的上下文关系，从而进一步对入侵的意图进行精确判断。本文跟踪了近年来意图识别领域的技术发展，详细介绍了几种有代表性方法的核心思想，分析它们适用的范围和存在的问题，比较了各自的优劣所在，最后总结了这个领域的难点问题和发展趋势。

关键词　复合入侵　IDS　意图识别　警报关联

A Survey on Network Intrusion Plan Recognition

Ning Zhuo　Gong Jian

(Department of Computer Science and Technology, Southeast University, Nanjing 210096)

Abstract　The detection of composed intrusion is an active topic for IDS now. The past research have shown that intrusion plan recognition technology is critical to reduce false or missed alert rate,which try to construct an effective model to accumulate the relationship among alerts in different context and promote recognition accuracy. This paper summarizes the advantage and the shortcoming of the known intrusion plan recognition methods. The special requirements are discussed and the most promising development is proposed.

Keywords　Composed intrusion; IDS;　plan recognition;　event correlation

1 引言

随着 Internet 技术的飞速发展，安全问题日益突出，入侵检测系统(IDS)也越来越成为关注的焦点。不可回避的是目前 IDS 无论是检测准确性还是可用性、灵活性上仍然存在着很大的问题。据[1]统计 IDS 面临的五大主要问题分别是误报漏报严重、海量数据处理、无法联动、难以部署、存在安全隐患。其中前两个问题显得尤为突出，这使得 IDS 处于一种“鸡肋”的尴尬境地。究其本质原因在于 IDS 还缺乏对攻击事件背后的逻辑关系的正确理解。

目前主流的滥用 IDS 采取的特征分析技术均基于检测规则集，而这些规则往往是各自独立地描述某个攻击特征，这实质上采用了一种割裂的眼光看待问题，没有有效利用攻击步骤间的上下文联系，因此导致对复合攻击的误报漏报严重。而要理解多事件攻击之间的逻辑关系并非易事，这涉及到对攻击语义的理解，目前的检测冗余消除只是试图发现与单个攻击动作相关的安全事件，并不能关联一个攻击序列中各个攻击动作之间的安全事件。这些问题表明滥用 IDS 的规则描述和检测方法都需要进行相应的改进。入侵意图识别技术的任务正是希望能够有效地识别隐藏在单独的攻击事件背后的逻辑关系，将组成一次复合攻击的所有步

本文得到国家973计划课题（2003CB314804）；教育部科学技术重点研究项目（105084）；江苏省网络与信息安全重点实验室（BM2003201）资助。

作者简介：**宁卓**（1975－），女，博士生，主要研究方向为网络安全检测，Email：zhning@njnet.edu.cn。**龚俭**（1957－），男，教授，博士生导师，主要研究方向为网络安全，网络管理和网络体系结构等。

骤关联起来，从而获得比单事件语义之和更多的攻击语义信息，提高检测的准确性。另外通过重现该攻击步骤的序列，使 IDS 有可能在攻击完成之前就识别出该攻击，从而可增强入侵响应的效果，使 IDS 从被动检测向主动防御转化。因此意图识别技术在入侵检测领域有很好的应用前景。

在人工智能领域传统的意图识别按照被推断意图的 agent 在系统中扮演的角色不同分为 keyhole recognition 和 intended recognition 两种。前者中 agent 感知不到自己的动作被观测，后者进一步要求 agent 协助意图识别的工作。网络入侵意图识别技术由于其领域特殊应用背景较之传统技术更为复杂。文献[2]提出了理想的入侵意图识别算法应该满足的几点要求，可以看作一个定性衡量算法好坏的基准。它们是：（1）识别偏序攻击计划的意图；（2）识别并发意图；（3）能够处理多目的的动作，不会导致意图的漏报；（4）具有缺省推理能力；（5）考虑外部环境对攻击意图的影响；（6）在不能识别唯一意图的情况下，能够报送多个可能意图及其概率。

从逻辑上讲意图识别问题要识别多事件攻击间的逻辑关系可以划分为两个子任务。1）寻求有效的数学模型刻画攻击；2）在模型上寻求有效的识别方法以识别攻击。按照不同的攻击表示方法和识别方法可以将目前 IDS 意图识别方法分为三种：

表 1　入侵意图识别方法分类图

项目 / 名称	攻击表示方法	意图识别方法
基于文法的意图识别	上下文无关文法	下推自动机
基于警报关联的意图识别	有向无环图/树	属性相似+概率统计
		图的匹配、覆盖问题
		因果关联技术
		混合数据
基于贝叶斯推理的意图识别	贝叶斯网络	贝叶斯推理

（1）采用上下文无关文法表示意图，从而将意图识别转化为下推自动机判定语言问题。

（2）采用警报关联的方法。警报关联是指通过对 IDS 报送的警报进行处理，发现警报之间的逻辑关系的过程。目前这个方向的研究成果最为丰富，按对关联方法的不同又可以进一步分为基于概率统计/属性值相似方法的警报关联、基于已知攻击图方法的警报关联、基于因果关联方法的警报关联、基于综合数据分析的警报关联四个子类。

（3）基于 Bayes 网络的意图识别技术。

本文将详细介绍这三大类方法的核心思想，分析它们适用的范围和存在的问题，对照上述考核基准比较各种方法的优劣，并从中归纳出这个领域的难点问题和发展趋势建议。

2 基于文法的意图识别

文献[3]提出用上下文无关文法来表示 Agent 意图，从而可用下推自动机实现对 Agent 行为的意图识别。但是这种经典的模式识别技术有很多假设在入侵检测领域不适用。 [4]进一步证明了任何一种复合攻击的标准攻击序列集合是正则文法，从理论的角度保证了有穷自动机识别标准攻击序列能力的有效性和完备性。提出了基于有穷自动机模型的意图识别算法 **CFGPRA**，算法复杂度为 $O(m*n)$，其中 m 是知识库中复合攻击类型的数量，n 是标准攻击状态数量。当 n 值较小时 **CFGPRA** 表现相当优秀，不仅填充的环境参数相当丰富，而且能识别并发意图、能够处理多目的动作、推断未观察到的攻击。但是由于攻击者在探索某种攻击序列失败时，会退回尝试另一种攻击序列，实际上的攻击序列大都是非标准攻击序列。这导致 **CFGPRA** 中 n 值指数级增加，大大削弱其实际运行效果。

3 警报关联方法

警报关联是指从 IDS 报送的警报中发现警报之间的逻辑关系的过程。通常由于底层 IDS 报送的攻击警报数量非常多，不同的冗余消除技术的效果也不尽相同，而且存在漏报和误报等情况，当前的警报关联技术趋向于先将 IDS 报送的底层警报聚类，然后对经过聚类的高层警报进行关联。关联通常都具有以下四个步骤：1）警报聚类；2）赋予警报不同的优先权；3）关联警报；4）构建攻击场景。按照不同的关联方法，警报关联技术大致可分为以下四类。

3.1 基于概率统计/属性相似的警报关联方法

这类方法通常基于警报的各个属性（比如地址、端口、时间、事件类型）的相似度来关联警报，经过聚类后的警报数量大幅减少，所以优点是大幅度降低了后继的分析难度。但是尽管这种方法在某些情况下非常有效,比如关联相同源宿 IP 地址/端口的警报，它仍然缺乏认识攻击警报间更本质的因果关系的能力，实际效果值得怀疑。[5]试图通过统计攻击事件同时发生的频率来发现它们之间的因果关系，但是如果两个没有因果关系的攻击事件恰好具有统计规律时会导致错误。而知识库作为滥用检测的基石其准确性必须可靠保证，所以[5]得到的结果必须提交给安全专家审核之后才能加入知识库中。实际上这种方法只能算一种专家辅助技术。另外存在的一个难点是如何合理的衡量警报间相似度。数据挖掘中传统的相似度衡量方法在警报关联中不是很实用。[7][8]采用概念聚类和分层抽象的办法进行分类，在实践中取得了较好的效果。

3.2 基于已知攻击图的警报关联方法

基于事先定义好的攻击场景来进行关联，这类方法把攻击场景（通常用图来刻画）作为模式，采用各种基于图论的方法或和滥用检测相似的方法进行匹配。这方面的工作包括[9][10][11]，这类方法可以识别偏序攻击，识别并发意图，具有缺省推理能力，能够报送多个可能意图及其概率。但也存在共同的致命缺陷——它们无法发现未知的攻击类型。另一个难点在于攻击图的构造。这项充满挑战性的工作很费时费力，而且由于涉及到定义什么是攻击这个更高抽象层次的固有难题研究（如何保障知识的正确性是知识工程的固有难题），不同的安全专家定义的攻击图也不尽相同，因此基于其上的 IDS，其各项指标也无法做出有意义的横向比较。文献[11]提出一个通用意图识别框架，将意图识别问题转化为在对已观察到的 Agent 行为的基础上，判断其代表 Agent 目标的终极行为。 [11]中将 Agent 意图以图的形式表示，其中结束节点表示对象的终极行为，其他节点表示蕴含终极行为的行为，从而将意图识别问题转化为图的覆盖问题；即若当前对象的行为序列图是某个对象意图的子图，则其目标为该意图的终极行为。这种方法的缺点是不能支持并发目标的识别，另外当用于入侵意图识别时，图的规模以及数量可能会非常大，会导致状态爆炸问题。而且由于环境参数无法计算，限制了方法的实用性能。考虑到简化复杂度[10]构造了深度为一的攻击关联树来计算两个警报 A_i, A_j 之间的关联度。根节点代表关联结果，只有高关联和低关联两个取值。根节点有七个子节点，分别表示违反访问政策、丢失敏感信息等七种攻击结果。每个子节点对应一个 evaluator，负责分析 A_i, A_j 对应不同结果的因果关系，然后依据近似 Bayes 的诊断概率公式计算最终结果填入根节点。但是由于七个子节点高度抽象，evaluator 的复杂性相应增加。只通过有限数据集的检验，[10]在多大程度上简化了复杂度尚缺乏理论依据。

3.3 基于因果关联的警报关联方法

因果关联方法也是意图识别方法中研究得最为广泛的分支。这种方法的思想建立在下述观察上：即大多数的攻击都不是孤立的，它们通常是整个攻击过程中的某一步，而且通常上一步攻击是为下一步攻击做准备。这个符合人类思维直觉的观察说明了攻击之间最重要的逻

辑联系是因果关系。因此关联的核心思想是：当前一个攻击事件的后果匹配后一个攻击警报的前提时，说明前一个攻击实际上为后一个攻击做好了准备，此时就可以将两个攻击关联起来。

JIGSAW[12] 是早期采用因果关联方法的系统。但是由于 JIGSAW 要求只有攻击的前提完全匹配时才能进行关联使得它在实践中的效果不佳。这在理论上是合理的，但是在实践中负面影响太大；为了解决上述问题[13]对攻击结果集合进行了扩展，提出了扩展结果集的概念，扩展结果集包含了所有由攻击结果集蕴涵为真的结果。显然攻击结果集合包含于攻击扩展结果集合。关联方法也由完全匹配修改为部分匹配，即在 ExpConseq（h1）中只要有至少一个的谓词 p 使得 Prereq（h2）部分为真，就可以进行关联。[13]中使用了 2000 年 DARPA 的攻击检测场景数据集 LLDOS1.0 和 LLDOS2.02 对上述方法的有效性进行验证，结果表明因果关联方法具有以下优点：(a)这种对超警报关联的方法揭示了警报之间的因果关系，清晰地反映出攻击策略的核心所在；(b)这种方法减少了误报对警报关联算法的影响。因为按照关联图一个真实的警报很容易与其他警报相关联，而错误的警报较之正确的警报而言不太可能符合关联条件，会被忽略，因而大大降低了误报的影响；(c)这种方法不依靠事前定义好的攻击场景来发现相关攻击的序列，而是动态地依据因果关系关联警报，生成关联图。克服了以前只能识别已知攻击类型的缺点。

但是因果关联方法也有难于克服的缺点：(a)这种方法无法对那些没有明显因果联系的攻击步骤进行关联。(b)对底层 IDS 的漏报很敏感。如果恰好漏报了一个连接攻击不同步骤的关键警报，那么警报关联图将被分裂为两个不相干的部分。(c)这种方法的性能如何很大程度上取决于对攻击形式化抽象的合理程度，即对攻击的前提和结果的形式化刻画很关键，直接影响因果关联方法的效果，很难想象如果攻击的前提和结果不明确，有矛盾的话，因果关联方法会得到什么好结果。(d)尽管上述因果关联模型[12] [13] [14]可以从攻击序列中抽取出攻击策略，却很难抓住攻击策略的本质。实际上即使采用相同的攻击策略，如果攻击者替换其中某个步骤的具体攻击方法，本模型得到的攻击关联图会大不相同。比如攻击者可能将某个攻击步骤无意义地重复若干遍，这将导致生成的关联图过于复杂，导致可读性差，开销过高等等问题。同理如果攻击者将攻击的某一步用等效攻击替换也会生成不同的关联图，而实际上这两种攻击序列的本质策略是相同的。

[10] [15]等工作试图通过结合多种关联方法克服缺点（a）。其中 [10]结合了基于概率的统计方法和因果关联方法，[15]采用因果关联方法+基于属性值相似度判断的聚类方法。

[16][20]提出了一系列假设和推理的方法试图弱化漏报对正确构造高层攻击策略图的影响。不失一般性，[16]提出要关联由于漏报被分割成两部分的攻击策略图实际上要解决两个问题：A 识别哪两个是应该关联的攻击图；B 识别出这两个攻击图间的因果关系。[16]找到了解决问题 A 的简单方法：将源宿地址相同的攻击警报聚为一类，赋予相同的 ID 号。则当不同的关联图含有相同 ID 号的攻击警报时可以确定它们是需要再次关联的关联图。解决问题 B 要困难的多。[16]提出的方法分为三步：（1）改造专家知识库，库中以攻击类型图的形式事先定义好了所有已知攻击，并计算出了所有的攻击类型间的属性值相等性约束。依据这个约束特性推理出所有符合条件的攻击类型作为备选攻击；（2）过滤（1）中不合理攻击，比如（1）中假设的攻击类型在原始攻击数据中根本没有出现过，则可以排除这种备选攻击；（3）巩固（2）中假设推理的结果。这是因为上述假设推理过程没有考虑到在不同上下文中同一个攻击类型被多次假设的情形，这会给攻击策略图增加不必要的复杂度，使实用性变差。因此步骤（3）的主要任务就是去掉简单重复的攻击类型，整合同类攻击类型。

要解决缺点（d）就不可避免地涉及到如何自动地进一步抽象出更高层次的超警报类型，使之既提取出攻击的本质特征，又可以隐藏不同攻击变形的细节。目前尚未有突破性的技术，实际上都是靠人工提取来完成的，甚至对于那些安全专家来说这也是件费时费力的问题。[14]

在此方面做了一些有益的尝试，致力于自动化简已经识别出的攻击策略图的复杂性问题。首先结合攻击信息和图论知识形式化定义了可聚合子图的概念，指导化简关联图为不可约的。试验显示此方法将攻击关联图从几十个结点化简到了一般不超过十个结点，大大提高了实用性。还提出了容错的图同构算法，通过计算图的编辑距离来衡量攻击策略图之间的相似性。同理采用容错的子图同构算法来判断一个攻击关联图是否是另一个的一部分。众所周知寻找子图同构的问题是一个 NP 难题，但是在实践中 Peng Ning 发现通过[14]化简过的攻击策略图很少有超过 10 个节点的，所以对于如此小的图[14]采用子图同构是可行的。另外[14]提出的衡量两个超警报之间的相似度的方法也能帮助安全专家半自动地完成人工提取工作。

3.4 基于综合数据源分析的警报关联方法

[17][18]试图将从多个不同信息源收集到的信息关联起来，以获得更全面的攻击全貌。比如说从 IDS、防火墙、漏洞扫描程序、反病毒工具，甚至是被检测系统的特性等等信息。较之其它方法这种方法最突出的优点就是充分考虑外部环境对攻击意图的影响，因为对同一攻击任务不同源的信息反映了从不同的视角看到的轨迹，因此汇总信息有利于对攻击有更全面的认识。M2D2[17]建立了一个形式化模型，该模型定义了不同信息源的概念和它们之间的联系，以方便安全管理员将不同源的信息关联起来，尽快查明并阻止攻击。但是这些方法也面临挑战：不同源的信息语法或语义上有很大差别，有的甚至是相互矛盾。

4 基于贝叶斯网络的意图识别

贝叶斯网络是由 Pearl 于 1986 年提出的一种采用概率推理的办法来解决不确定性问题的方法，被认为是人工智能领域近二十年来最重要的研究成果之一。在入侵检测中贝叶斯网络的核心思想体现在贝叶斯规则的变化形式上：$P(H \mid e) = \frac{p(e \mid H) * P(H)}{P(e)}$。我们要从观测到的攻击警报 e 推测发生了攻击 H 的可能性 P（H|e）是相当困难的，但是依据贝叶斯规则，这件困难的事情可以划分为完成另外两件容易得多的事情，即估计发生攻击 H 后会出现警报 e 的概率 P（e|H）和攻击 H 发生的概率 P（H），其中 P（e）为常量。Cooper 指出即使在条件无关的假定下，Bayes 网络的概率推理仍是一个 NP 难题。所以这方面的很多研究都集中在如何更合理地构造 Bayes 网络，简化网络结构以获得可行性算法。

[19]中采用单一连接的因果树来刻画攻击策略图，这样就可以在线性时间里完成概率推理。因果树的根节点代表了最终的攻击目标，各个非叶节点代表了其父亲节点的各个子目标，叶子节点表示了最低级的攻击步骤。每个节点有两个状态：1 状态表示为真，0 状态表示为假。叶节点为真表示检测到了响应的攻击警报，非叶节点为真表示攻击目标/子目标达到。各个兄弟之间只有“与”和“或”的关系。攻击知识库由攻击树组成的森林描述。边表示节点代表的攻击事件之间存在的直接因果关系。假设 X 是因果树中的任一个节点，我们用下列符号表示：$PI(x)$——结点 x 的先前概率；$LMD(x)$——从结点 x 的祖先所得到的诊断支持；$BEF(x)$——结点 x 的确信度；$PI_x(y)$——PI 的信息从 y 到 x 遍历传递（自顶向下）；$LMD_x(y)$——从 x 到 y 传递的 l 信息（自底向上遍历）；a ——改变单位向量的标准化常量。如果提供了下列三个参数变量，x 的确信可以计算出来。1）$PI_x(u_i)$——从每个父亲 u_i 到 x 的输入 PI；2）$LMD_{y_i}(x)$——从每个孩子 y_i 到 x 的输入 l ；3） c_i——每个 u_i 到 x 的

信任度；在运行时当 X 节点被激活时其信念更新过程分为三步：

（1）x 的确信修改为 $BEF(x) = a * LMD(x) * PI(x);$

（2）从 x 到父结点 u_i 所传递的输出 l 信息（从底向上的信念传递）：

$$LMD_x(u_i) = [LMD_0 * Q_i * PROD(i) + LMD_1 * (1 - Q_i * PROD(i)),$$
$$LMD_0 * PROD(i) + LMD_1 * (1 - PROD(i))];$$

其中，$Q_i = 1 - C_i;\ PROD(i) = \prod_{k \neq i} (1 - c_k * PI_x(u_k))$；

（3）从 x 到每个子结点 y_i 的输出 PI 信息（自顶向下的信念传递）：

$$PI_{y_i}(x) = a * BEL(x) / LMD_{y_i}(x)$$；

依照上述信念更新过程，在接收到任何一个有效的诊断信息，即一个有用的攻击警报后都会引起因果树的信念更新。每次更新后信念可信度最大的那个节点即被视为预测的可能攻击。

贝叶斯网络可以识别偏序攻击，识别并发意图，处理多目的动作，具有缺省推理能力，能够报送多个可能意图及其概率。但也存在下述不足：1）无环假定。现有的研究中建模的一个基本假定就是网中不存在环，从图论的角度来说，即贝叶斯网络模型只能是有向无环图。直观上讲贝叶斯网络不考虑结果作为原因的原因。但是在入侵检测中经常有因果互相影响的反馈效应，即原因影响结果后，结果又作为原因影响原来的原因。所以突破无环假定的限制是一个值得深究的问题；2）静态假设。现有的研究目前都没有考虑原因节点影响结果节点的滞后时间。而时间因素对贝叶斯推理结论是有很大影响，所以有必要考虑动态贝叶斯网络。实际上对有环贝叶斯网络的研究也会导致对动态推理的研究。在有环贝叶斯网络中只有引入时间概念才能解释因果环上的信息不一致现象。

5 总结

入侵意图识别技术试图从入侵者的行为中推断其后续动作和最终目的，其本源思想来自于传统模式识别技术，但是由于入侵领域自身的特点导致入侵意图识别技术比传统模式识别技术更加复杂。它的难点问题在于：首先，传统的模式识别技术都是在一种没有干扰和对抗的环境中进行的，有时甚至可以得到被观测对象的帮助。但是在入侵领域攻击者会千方百计地躲避甚至干扰识别过程；其次，传统的模式识别技术都隐含下述假设，即一个 agent 活动只有一个意图，但是入侵者通常可视被攻击目标的反应不同，采取动态的多目标攻击，有时甚至是多个攻击者协作攻击。最后，由于 IDS 性能和准确性因素，总是存在误报和漏报。不可能达到传统模式识别要求可靠地观测到被观察者所有动作的假设。

上述的意图识别方法从各个不同的角度出发解决这些难点。除了基于概率/属性的方法相对来说显得较为粗燥，识别攻击的能力有限，不具备缺省推理的能力外，其他方法理论上都能识别偏序攻击，识别并发意图，具有缺省推理能力。能够处理多目的动作，报送多个可能意图及其概率。实际应用中由于各种方法抽象的层次、方法不同，形式化的具体方法不同，实际的性能效率也各不相同。遗憾的是由于它们采用不同的数据集进行验证，很难做出定量的横向比较。在考虑外部环境的影响这一点上基于综合数据源的方法远胜过其他方法，它利用视野宽，信息量大的特点降低数据的不确定性。其他方法也提出了一些相应措施，如：**CFGPRA** 可以增加宏观攻击行为分析发掘复合攻击规律，在入侵意图识别时考虑入侵者的

攻击习惯；因果关联技术应用了上述一系列的假设推理技术，有助于消除外部环境影响，获取事件间本质的因果关系；贝叶斯网络也可以通过增加语义刻画，修改先验知识概率来达到一定效果。

就各个方向的发展趋势而言，基于 Bayes 网络的意图识别应是最有潜力的发展方向。其一，入侵检测领域特殊的检测需求天生和概率表示分不开，比如多攻击意图识别，在攻击的某一步要衡量攻击者向不同意图的发展可能性必须用到概率；其二，众多研究表明多事件攻击中事件间最本质的逻辑联系是因果关系，意图识别本质上属于不确定性推理。Bayes 网络正是人工智能不确定推理领域中为此提出的很有影响的模型。因此无论是在知识的不确定性表示、领域知识的表示（先验概率）、信念的更新，还是在多目标的攻击推理的能力和效率上较之其他方法都更有优势；其三，除了因果关系，还要考虑两个攻击事件间的时间和空间关系。如果考虑加入时间因素的动态 Bayes 网，模型完全满足推理的所有逻辑要求。时间因素的引入也有利于解决因果循环的推理问题，将极大扩展 Bayes 网络在入侵检测领域能解决的问题范围；其四，尽管 Bayes 网络发现新的攻击类型的能力有限，但是加入上述其他意图识别方法的技术特点还是有可能提高它识别新攻击的能力的。

参考文献

[1] 濮青，入侵检测系统面临问题与发展趋势研究，计算机工程与设计，2004.1

[2] Christopher W. Geib and Robert P. Goldman, Plan Recognition in Intrusion Detection Systems. IEEE 2001

[3] M.Vilain,Getting serious about parsing plans: a grammatical analysis of plan recognition. In Proceedings of the Eighth National Conference on Artificial Intelligence, pp. 190-197, Cambridge, MA, 1990, MIT Press

[4] 张剑，可回卷的动态反馈自动入侵响应系统，东南大学 博士论文，2004

[5] Xinzhou Qin and Wenke Lee. Statistical Causality Analysis of INFOSEC Alert Data. In *Proceedings of The 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003),* Pittsburgh, PA, September 2003

[6] Nong Ye.Multivariate statistical analysis of audit trails for host_based Intrusion Detection., IEEE Transactions on Computers,October 2001

[7] Julisch, K. & Dacier, M. Mining intrusion detection alarms for actionable knowledge. Proc. of ACM Conf. on Knowledge Discov. and Data Mining, (2002), 366-375

[8] Julisch, K. Mining alarm clusters to improve alarm handling efficiency. Proc. of the 17th Annual Computer Security Applications Conference (ACSAC).12-21

[9] Yian Huang and Wenke Lee. Attack Analysis and Detection for Ad Hoc Routing Protocols. In *Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004),* Sophia Antipolis, France, September 2004

[10] Xinzhou Qin and Wenke Lee.Discovering Novel Attack Strategies from INFOSEC Alert. In *Proceedings of The 9th European Symposium on Research in Computer Security (ESORICS 2004)* , Sophia Antipolis, France, September 2004

[11] H. Kautz and J. F. Allen, *Generalized plan recognition*. In Proceedings of the Fifth National Conference on Artificial Intelligence, pp. 34-44, dec 1992

[12] S.Templeton and K.Levit. A requires/provides model for computer attacks/InProc.of New Security Paradigms Workshop,pages 31-38.September 2000.

[13] Peng Ning, Yun Cui, Douglas S. Reeves, "Constructing Attack Scenarios through Correlation of Intrusion Alerts," in *Proceedings of the 9th ACM Conference on Computer & Communications Security*, pages 245--254, Washington D.C., November 2002.

[14] Peng Ning, Dingbang Xu, "Learning Attack Strategies from Intrusion Alerts," *in* Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), pages 200--209, Washington D.C., October, 2003. (Acceptance ratio: 35/253)

[15] Peng Ning, Dingbang Xu, Christopher G. Healey, and Robert A. St. Amant, "Building Attack Scenarios through Integration of Complementary Alert Correlation Methods," in *Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS '04)*, pages 97--111, February, 2004

[16] Peng Ning, Dingbang Xu, "Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems," *ACM Transactions on Information and System Security (TISSEC)*, Vol. 7, No. 4, pages 591--627, November 2004

[17] B.Morin,L.Me.M2D2: A formal data model for IDS alert correlation. In Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID 2002),PAGES 115-137,2002

[18] C.Michel and L.Me. Adele: an Attack Description Language for knowledge-based Intrusion Detection. In: Proc. Of the 16th International Conference on Information Security,2001

[19] Xinzhou Qin and Wenke Lee.Attack Plan Recognition and Prediction Using Causal Networks. In *Proceedings of The 20th Annual Computer Security Applications Conference (ACSAC 2004),* Tucson, Arizona, December 2004

[20] Yan Zhai, Peng Ning, Purush Iyer, Douglas S. Reeves, "Reasoning about Complementary Intrusion Evidence," in *Proceedings of 20th Annual Computer Security Applications Conference* , December 2004

[21] Joao B.D. Cabrera, Jaykumar Gosar, Wenke Lee, and Raman K. Mehra. On the Statistical Distribution of Processing Times in Network Intrusion Detection. In *Proceedings of The 43rd IEEE Conference on Decision and Control (CDC 2004),* Bahamas, December 2004

[22] Valdes,A.and Skinner,K. Probabilistic alert correlation. In proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection.PAGES 54-68