

# 基于扩展目标规划图的网络攻击规划识别算法

诸葛建伟 韩心慧 叶志远 邹 维

(北京大学计算机科学技术研究所 北京 100871)

**摘 要** 在人工智能领域经典规划识别方法的基础上,针对网络攻防领域攻击规划识别问题的特性,对目标规划图进行进一步扩充,引入观察节点以区分规划者动作以及识别者对动作的观察,将动作节点分化为由具体动作层和抽象动作层组成的层次结构,并根据抽象攻击模式在抽象攻击层面上维护与安全状态节点的前提和后果条件,形成扩展目标规划图(Extended Goal Graph, EGG)模型;并进一步提出基于扩展目标规划图的攻击规划识别算法,该算法能够有效地从大量底层入侵报警信息中正确识别背后蕴藏的攻击者意图及规划.通过 DARPA 2000 入侵场景关联评测数据集和在蜜网环境中捕获的实际僵尸网络攻击场景数据的实验测试以及与 TIAA 入侵报警关联分析系统<sup>[5]</sup>的实验结果对比,验证了该文提出算法的完备性与有效性.

**关键词** 规划识别;知识表示;报警关联;目标规划图

中图法分类号 TP309

## A Network Attack Plan Recognition Algorithm Based on the Extended Goal Graph

ZHUGE Jian-Wei HAN Xin-Hui YE Zhi-Yuan ZOU Wei

(Institute of Computer Science and Technology, Peking University, Beijing 100871)

**Abstract** Based on the classical plan recognition methods in the domain of artificial intelligence, and considering the characteristics of attack plan recognition problem in the domain of network security operation, this paper extends the goal graph model, introducing the observation node to distinguish the planner's actions and the recognizer's observations against the actions, replacing the unitary action nodes using the hierarchy composed with detail actions and abstract actions, maintaining the precondition and effect conditions between the actions and security states in the abstract action level according to the abstract attack patterns, therefore, proposes the Extended Goal Graph (EGG) model. Furthermore, this paper proposes an attack plan recognition algorithm based on the Extended Goal Graph, the algorithm can recognize the hidden attack intention and plan from the large volume of low level intrusion detection system alerts correctly and effectively. Through the experiments using DARPA 2000 intrusion scenario correlation benchmark dataset and in-the-wild botnet scenarios data captured in the honeynet, the results show the completeness and soundness of the algorithm, as well as its advantage beyond the alert correlation systems such as TIAA<sup>[5]</sup>.

**Keywords** plan recognition; knowledge representation; alert correlation; goal graph

收稿日期:2006-04-03;修改稿收到日期:2006-06-07. 本课题得到国家信息安全计划项目基金(2005C32)、微软学者计划和 IBM 博士生英才计划项目基金资助. 诸葛建伟,男,1980 年生,博士,助理研究员,主要研究方向为入侵检测与关联分析、蜜罐与蜜网技术、恶意软件分析与防范技术. E-mail: zhugejianwei@icst.pku.edu.cn. 韩心慧,男,1969 年生,博士研究生,助理研究员,主要研究方向为蜜罐与蜜网技术、恶意软件分析与防范技术. 叶志远,男,1963 年生,高级工程师,主要研究领域为网络与信息安全. 邹 维,男,1964 年生,研究员,主要研究领域为网络与信息安全.

## 1 引言

随着全球信息化时代的到来, Internet 已经成为人类生活中不可或缺的组成部分. Internet 天生具有的开放性、自由性和国际性在造就了一个无处不在的 Internet 同时, 也使得 Internet 的安全问题日益凸显. 从 1988 年 Internet 前身 ARPANET 遭受的 Morris 蠕虫攻击开始, Internet 始终面临大量而且严重的安全威胁. 对网络攻击的检测及行为关联分析是达到发现和理解安全威胁的关键技术, 是 P<sup>2</sup>DR 动态网络安全模型中的重要环节, 因此也成为网络安全领域的热点研究问题之一.

入侵检测是对计算机和网络资源的入侵行为进行识别和响应的处理过程<sup>[1]</sup>, 但由于存在“基调悖论 (base-rate fallacy)”现象<sup>[2]</sup>, 即提高检测率和降低误报率是互为矛盾的, 从而导致目前入侵检测系统存在误报率较高、报警数量过大以及报警语义弱等不足, 为了解决入侵检测技术存在的困难, 研究人员提出了入侵报警关联分析技术, 期望从简单高效的入侵检测系统所报告的底层报警信息中识别出攻击规划并重构攻击场景, 以帮助安全管理员快速对安全态势进行理解, 并及时做出正确的响应.

入侵报警关联分析技术对以入侵报警信息为主的安全报警进行组合、解释和分析, 目标是对报警信息的求精, 以对攻击规划进行识别和场景重构. 从实质上看, 入侵报警关联分析技术需要解决的是在网络攻防这一领域中对攻击方的规划识别问题, 即防御方根据对攻击行为的观察数据去推测攻击方的目标及其正在实施的动作规划. 规划识别技术是人工智能领域中的一个重要研究课题, 但目前仅关注于合作式 (Intended) 规划识别和锁孔式 (Keyhole) 规划识别两类问题, 而在网络攻防领域的规划识别则属于敌对式 (Adversarial) 规划识别问题. 由于规划者和识别者之间存在竞争关系, 识别者一般无法获取规划者的完整规划库, 此外规划者也将引入一些隐蔽和欺骗技术使得识别者更难识别和推测其真正在执行的动作及目标, 因此不能像一般的规划识别问题一样将识别者对动作的观察与规划者动作直接等同.

本文在规划识别问题中经典规划图<sup>[3]</sup>以及目标规划图<sup>[4]</sup>的基础上, 针对网络攻防领域规划识别问题的复杂性, 对目标规划图进行进一步扩充, 引入观察节点以区分规划者动作以及识别者对动作的观察, 将动作节点分化为由具体动作层和抽象动作层

组成的层次结构, 并根据抽象攻击模式在抽象攻击层面上维护与安全状态节点的前提和后果条件, 形成扩展目标规划图 (Extended Goal Graph, EGG) 模型; 进一步提出基于扩展目标规划图的攻击规划识别算法, 该算法能够有效地从大量底层入侵报警信息中正确识别背后蕴藏的攻击者意图及规划. 通过 DARPA 2000 入侵场景关联评测数据集<sup>①</sup>和在蜜网环境中捕获的实际僵尸网络攻击场景数据的实验测试以及与 TIAA 入侵报警关联分析系统<sup>[5]</sup>的实验结果对比, 验证了本文提出算法的完备性与有效性.

本文第 2 节讨论目前入侵报警关联分析方面的相关研究工作和研究进展; 第 3 节介绍本文提出的网络攻防知识模型; 第 4 节对扩展目标图模型以及规划识别问题进行形式化定义; 第 5 节则描述基于扩展目标图模型的攻击规划识别算法; 第 6 节是实验分析过程及结果; 最后, 第 7 节对全文进行总结并讨论未来进一步的工作方向.

## 2 相关工作

入侵报警关联分析从 2000 年左右开始在入侵检测技术领域受到关注, 目前已经提出了大量的分析方法, 主要可以分为报警聚类方法、基于攻击规划库的报警关联方法和基于攻击行为建模的报警关联方法三大类.

报警聚类 (clustering) 方法<sup>[6~9]</sup>属于最初步的关联分析, 通过报警属性值之间的相似性对报警进行聚类, 使得同个聚类的报警集合具有某些相同的特性, 然后选择一个抽象的“元报警”事件作为该聚类的代表元. 此类方法不能够完全揭示出相关报警之间的因果联系, 无法对报警反映的攻击场景给出清晰的解释, 也无法预测攻击者的目标和进一步的攻击规划.

基于攻击规划库的报警关联方法在拥有一个完整的已知攻击规划库的基础上, 通过一系列关联分析技术来识别报警流中包含的与攻击规划库中的攻击规划相一致的攻击场景实例. Morin<sup>[10]</sup>将 Dousson 的纪事模型<sup>[11]</sup>应用于报警关联, 实现了一个能够对大量报警进行融合, 识别出其中存在的已知攻击模式的融合分析组件. Honeywell Lab 的 Geib 等人首

① 使用评测数据集: MIT Lincoln Laboratory, 2000 DARPA Intrusion Detection Scenario Specific Data Sets. [http://www.ll.mit.edu/IST/ideval/data/2000/2000\\_data\\_index.html](http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index.html), 2000

次应用规划识别技术来解决入侵检测中的报警关联问题<sup>[12,13]</sup>,提出了基于规划执行模型的报警关联算法.基于攻击规划库的报警关联方法是基于封闭世界假说,需要一个完整的攻击规划库作为支撑基础,但在实际环境中,由于攻击动作的多样性和攻击过程的随意性以及新的攻击工具和技术的不断出现,使得构建一个完善的攻击规划库极为困难.此外,由于存在并行的攻击场景,上述的各种方法对每个攻击场景维护中间的状态,从而导致其存储代价和计算代价都非常庞大.上述两个缺陷使得基于攻击场景库的报警关联方法难以在实际中得到广泛的有效应用.

基于攻击行为建模的报警关联方法的思想借鉴于人工智能领域自动规划问题中对动作的经典描述模型——STRIPS(Stanford Research Institute Problem Solver)模型<sup>[14]</sup>,通过对攻击动作的前提条件和造成的后果进行描述,构建攻击模型,如果一个攻击动作的后果使得另一攻击动作的前提条件得到满足,则认为这两个攻击动作之间存在因果关系.基于攻击行为建模的报警关联算法就利用这些因果关系将观察到的报警进行连接,构造出整个攻击场景.基于攻击行为建模构建的关联系统主要有 Cuppens 等人开发的报警关联模块 CRIM<sup>[15]</sup>和 Ning 的 TIAA 系统<sup>[5]</sup>等.基于攻击行为建模的报警关联方法不需要对所有可能的攻击规划进行描述和存储,只需要对单个攻击行为动作进行建模,准确刻画其所需的前提条件和造成的后果,因此攻击知识模型的构建和维护较为可行,另外构建的攻击知识模型存在较强的灵活性,能够对一些未知的攻击场景进行识别.

现有的入侵报警关联分析技术还存在着如下一些问题:首先,能够完成攻击规划识别的关联分析技术都需要有一个领域知识库的支撑,虽然目前在攻击关联知识模型方面有一些研究工作,但目前尚未有完整的、实际可行的网络攻防知识库的构建方案.攻防知识库构建的困难阻碍了关联分析技术的实际应用;其次,现有的入侵报警关联分析技术大多仅仅根据固定的模式对报警进行关联,而未对受监控系统以及攻击者的状态进行有效跟踪;第三,缺乏对攻击者意图的识别,无法为正确及时的响应提供支持;最后,由于在实际网络环境中很难获得攻击场景测试数据并准确地从背景网络流量中对其进行正确标识,因此对入侵报警关联分析技术的测试和验证普遍缺乏足够的攻击场景数据,这也使得目前大多数的入侵报警关联分析技术研究仅仅针对几个人工构造的攻击场景数据集,并不能够体现实用性.

### 3 网络攻防知识模型

从大量底层报警信息中识别攻击者的意图和规划,其本质上是要在网络攻防这一复杂的应用领域中研究和实现能够对大量攻击数据给出合理解释的专家系统.因此,我们首先要研究如何有效地对网络攻防领域中的知识进行建模和描述,并保证知识库构建的可行性、系统性以及可维护性.

知识表示方法的确定是知识模型构建的基础,对于复杂的网络攻防领域,我们以面向对象方法这一结构性的知识表示方法为基础,并结合一阶谓词逻辑来描述各种不同的知识对象之间的关联关系,以支持攻击规划识别算法.STRIPS 模型<sup>[14]</sup>是基于—阶谓词逻辑对特定应用领域中的世界状态、目标和动作的一个经典描述模型,我们将以其为基础,并针对网络攻防的领域特性和入侵行为关联分析问题的需求进行一些扩展,使之能够更加充分和准确地描述进一步推理所需的领域知识.

本文采用的网络攻防知识模型的整体框架由攻击知识模型和漏洞知识模型两部分组成,如图 1 所示.

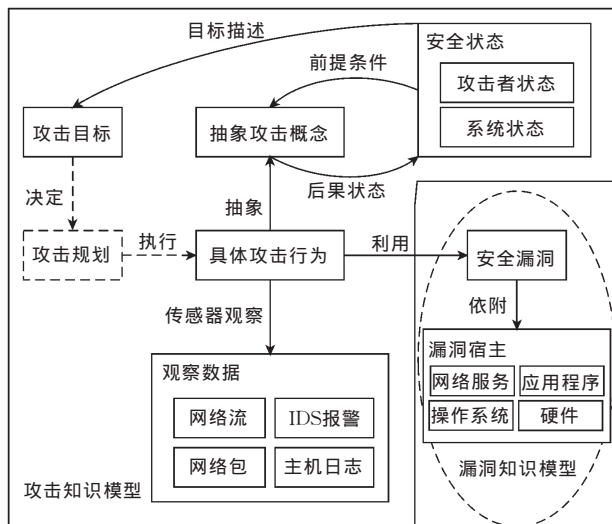


图 1 网络攻防知识模型整体框架

在攻击知识模型中,我们引入了攻击目标、安全状态、具体攻击行为、抽象攻击概念和观察数据五种对象类来对攻击过程进行描述.在知识内容的关联关系上,与基于攻击行为建模的报警关联方法类似,我们不对攻击规划进行显式的描述,而是在 STRIPS 模型的基础上进行扩展,引入以下特性对关联关系进行描述:

(1) 引入攻击行为模型的层次结构,分别定义具体攻击行为和抽象攻击概念,并维护之间的抽象—

具体关系,以保证整个攻击行为模型的结构性和可维护性;

(2)从网络攻防领域中存在的抽象攻击模式出发,在抽象攻击概念层面上定义它们的前提条件和后果状态,从而能够有效地降低攻击知识库构建的难度,并提高攻击知识结构的稳定性;

(3)将攻击行为与对攻击行为的观察事件分开考虑,通过维护它们之间的传感器观察关系对非确定性的观察进行应对处理.

在漏洞知识模型中,我们主要刻画安全漏洞的相关属性、内部操作方法和与其它知识内容之间的关联关系,包括安全漏洞和具体攻击行为的利用关系以及安全漏洞与漏洞宿主的依附关系.其中具体攻击行为对安全漏洞的利用关系将攻击知识模型和漏洞知识模型联系在一起.

在上述网络攻防知识模型基础上,我们进一步引入对攻击行为和安全漏洞的星形多维分类方法保证知识库构建的系统性,并提供与其它网络攻防知识库如 Snort 特征库和 Nessus 安全漏洞库的索引机制,基于 XML Schema 定义攻击知识描述语言 AKDL 和漏洞知识描述语言 VKDL,以 AKDL 和 VKDL 语言对网络攻防领域的知识内容和关联关系进行描述,从而构建网络攻防知识库.

## 4 扩展目标规划图

规划图算法<sup>[3]</sup>是由 Blum 和 Furst 提出的经典自动规划算法,用于求解以 STRIPS<sup>[14]</sup>模型描述的领域规划问题. Hong 在规划图的基础上构建了目标规划图结构,并提出了一种目标识别算法<sup>[4]</sup>.目标识别是规划识别问题的一个特例,与传统的规划识别方法相比, Hong 提出的目标识别算法不需要一个显式构建规划库的支持,而只需给出类似 STRIPS 模型的目标集和动作集描述;另外,该算法采用了与规划图算法类似的目标规划图扩张和目标规划图分析两阶段方法来进行目标识别,而不是直接从规划空间中搜索结果; Hong 还进一步证明了该算法是稳固 (Sound) 的,且其时间和空间代价是多项式规模的.

在文献[4]提出的目标规划图模型的基础上,本节针对网络攻防领域规划识别问题的复杂性,在上节提出的网络攻防知识模型的支持下,对目标规划图进行进一步扩充,引入观察节点,将动作节点层分化为由具体动作层和抽象动作层组成的层次结构,并在抽象动作节点层上维护与状态节点的前提和后果条件,形成扩展目标规划图 (Extended Goal

Graph, EGG) 模型.

### 4.1 扩展目标规划图

定义 1 (扩展目标规划图). 扩展目标规划图 EGG (Extended Goal Graph) 定义为一个六元组  $\Gamma = \langle P, O, A, B, G, E \rangle$ , 其中:

$P$  为状态节点集合, 其中的每个元素表示为  $prop(p, i)$ ,  $p$  为一个状态实例, 其取值可以为“真”或者“假”,  $i$  为一个时间戳;

$O$  为观察节点集合, 其中的每个元素表示为  $obsv(o, i)$ ,  $o$  为一个观察实例;

$A$  为具体动作节点集合, 其中的每个元素表示为  $action(a, i)$ ,  $a$  为一个具体动作实例;

$B$  为抽象动作节点集合, 其中的每个元素表示为  $abstraction(b, i)$ ,  $b$  为一个抽象动作实例;

$G$  为目标节点集合, 其中的每个元素表示为  $goal(g, i)$ ,  $g$  为一个目标实例;

$E$  为边集, 包括如下六种不同类型的边:

$observation-edge(obsv(o, i), action(a, i))$ : 观察边, 表示观察节点  $obsv(o, i)$  是传感器对具体动作节点  $action(a, i)$  的观察事件.

$abstraction-edge(action(a, i), abstraction(b, i))$ : 抽象边, 表示具体动作节点  $action(a, i)$  可抽象为抽象动作节点  $abstraction(b, i)$ .

$precondition-edge(prop(p, i), abstraction(b, i))$ : 前提条件边, 表示状态节点  $prop(p, i)$  是抽象动作节点  $abstraction(b, i)$  的前提条件.

$postcondition-edge(abstraction(b, i), prop(p, i+1))$ : 后果状态边, 表示抽象动作节点  $abstraction(b, i)$  发生导致后果状态节点  $prop(p, i+1)$ .

$persistence-edge(prop(p, i), prop(p, i+1))$ : 状态保持边, 表示状态节点  $prop(p, i)$  保持到  $i+1$  新的时间片  $prop(p, i+1)$ .

$description-edge(prop(p, i), goal(g, i))$ : 目标描述边, 表示状态节点  $prop(p, i)$  是目标节点  $goal(g, i)$  的组成状态.

定义 2 (前提条件链). 定义状态节点  $p_i$  和抽象动作节点  $b_j$  之间存在前提条件链并记为  $precondition-path(p_i, b_j)$ , 当且仅当从  $p_i$  到  $p_j$  存在  $j-i$  条状态保持边, 并且从  $p_j$  到  $b_j$  存在前提条件边  $precondition-edge(p_j, b_j)$ .

定义 3 (后果条件链). 定义抽象动作节点  $b_i$  和状态节点  $p_j$  之间存在后果条件链并记为  $postcondition-path(b_i, p_j)$ , 当且仅当从  $b_i$  到  $p_{i+1}$  存在后果状态边  $postcondition-edge(b_i, p_{i+1})$ , 且从  $p_{i+1}$  到  $p_j$  存在  $j-i+1$  条状态保持边.

图 2 显示了一个扩展目标规划图的示例.

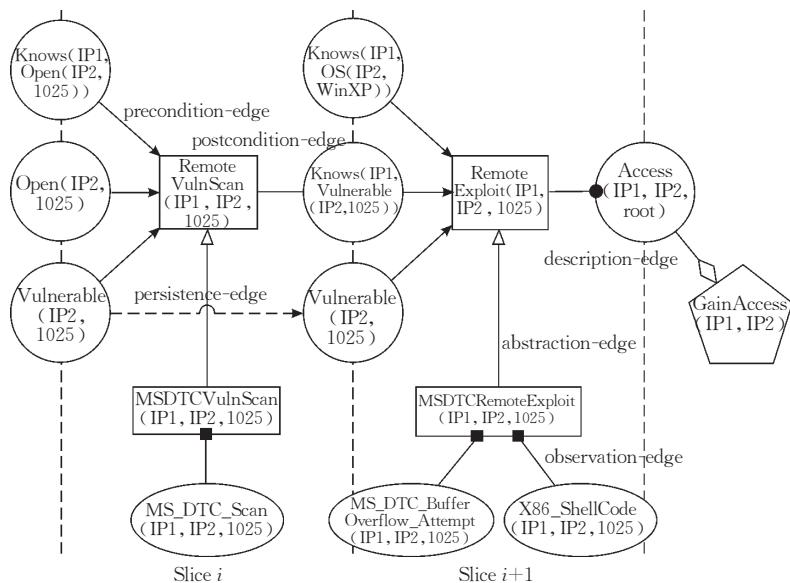


图 2 扩展目标规划图示例

#### 4.2 有效规划

在给出扩展目标规划图模型的定义后,首先我们给出因果链关系的定义,因果链体现了动作节点之间以及动作节点与目标节点之间的依赖关系,是攻击规划构建的基础.然后,我们给出在给定初始状态下能够达成某一目标的有效规划这一概念的定义.

**定义 4 (因果链).** 假设  $b_i$  和  $b_j$  是分别在时间片  $i$  和时间片  $j (i < j)$  发生的抽象动作节点,定义  $b_i$  和  $b_j$  间存在因果链并记为  $b_i \rightarrow b_j$ ,当且仅当:

$\exists p \mid postcondition-path(b_i, p) \wedge precondition-path(p, b_j)$ , 即  $b_i$  的某一后果状态  $p$  为  $b_j$  的前提条件状态,在  $b_i$  和  $b_j$  间包括一条  $b_i$  到  $p$  的后果状态边, 0 条或多条状态节点  $p$  的保持边以及一条从  $p$  到  $b_j$  的前提条件边.

定义具体动作节点  $a_i$  和  $a_j$  间存在因果链并记为  $a_i \rightarrow a_j$ ,当且仅当:

$\exists b_i, b_j \mid abstraction-edge(a_i, b_i) \wedge abstraction-edge(a_j, b_j) \wedge (b_i \rightarrow b_j)$ , 即存在  $a_i$  和  $a_j$  存在各自的抽象动作节点  $b_i$  和  $b_j$ , 且  $b_i$  和  $b_j$  间存在因果链.

定义具体动作节点  $a_i$  和目标节点  $g_j$  间存在因果链并记为  $a_i \rightarrow g_j$ ,当且仅当:

$\exists b_i, p \mid abstraction-edge(a_i, b_i) \wedge postcondition-path(b_i, p) \wedge description-edge(p, g_j)$ , 即  $a_i$  存在相应的抽象动作节点  $b_i$ , 且  $b_i$  的某一后果状态为目标  $g_j$  的描述.

在因果链关系和时序约束的基础上,我们可以定义如下能够达成某个目标的有效规划.

**定义 5 (有效规划).** 给定初始状态  $P_0$  和一个

目标  $g$ , 规划  $Plan = \langle A', C', L \rangle$ , 其中  $A'$  是一组动作,  $C'$  是在  $A'$  上的一组时序约束  $\{a_i < a_j\}$ ,  $L$  是在  $A'$  上的一组因果链关系  $\{a_i \rightarrow a_j\}$ , 称规划  $Plan$  是初始状态  $P_0$  下目标  $g$  的一个有效规划, 当且仅当:

在初始状态  $P_0$  下,  $A'$  中的动作可以任意满足时序约束  $C'$  的次序执行;

在初始状态  $P_0$  下, 目标  $g$  在  $A'$  中的动作以任意满足时序约束  $C'$  的次序执行后达成.

#### 4.3 一致性目标及一致性规划

在有效规划概念的基础上,我们将进一步定义与观察集合相一致的一致性目标和一致性规划,并根据这两个概念对攻击规划识别问题进行形式化定义.

**定义 6 (相关性动作).** 给定一个目标  $g$  和一组具体动作节点  $\langle A', C' \rangle$ , 称具体动作节点  $a \in A'$  在  $\langle A', C' \rangle$  上下文环境下与目标  $g$  相关, 当且仅当:

存在从具体动作节点  $a$  到目标  $g$  的因果链, 即  $a \rightarrow g$ ; 或者

存在具体动作节点  $a' \in A'$ ,  $(a \rightarrow a') \wedge (a < a') \wedge (a' \rightarrow g)$ .

**定义 7 (相关性观察).** 给定一个目标  $g$  和一组观察节点  $\langle O, C \rangle$ , 称观察节点  $o \in O$  在  $\langle O, C \rangle$  上下文环境下与目标  $g$  相关, 当且仅当:

存在具体动作节点  $a$ ,  $observation-edge(o, a)$ , 且  $a$  在  $\langle A', C' \rangle$  上下文环境下与目标  $g$  相关. 其中  $A' = \{a' \mid \exists o \in O, \exists observation-edge(o, a')\}$ ,  $C' = \{a < a' \mid \exists observation-edge(o, a) \wedge observation-edge(o', a') \wedge (o < o')\}$ .

**定义 8 (一致性目标).** 给定一组观察节点  $\langle O,$

$C\rangle$ , 称目标  $g$  是观察集  $\langle O, C \rangle$  的一致性目标, 当且仅当:

$\exists O' \sqsubseteq O, C' \sqsubseteq C, \forall o \in O'$  在  $\langle O', C' \rangle$  上下文环境下与目标  $g$  相关.

即存在观察集的子集  $O'$ ,  $O'$  中的每个观察与目标  $g$  均相关.

定义 9(一致性规划). 给定初始状态  $P_0$  和一组观察节点  $\langle O, C \rangle$ , 称规划  $Plan = \langle A', C', L_a \rangle$  与观察集  $\langle O, C \rangle$  相一致, 当且仅当:

存在观察集  $\langle O, C \rangle$  的一致性目标  $g$

$\forall a \in A', \exists o \in O, \exists \text{observation-edge}(o, a),$

$C' = \{a < a' \mid \exists \text{observation-edge}(o, a) \wedge \text{observation-edge}(o', a') \wedge (o < o')\}.$

规划  $Plan$  是初始状态  $P_0$  下目标  $g$  的一个有效规划.

将一致性规划记为  $\langle g, \langle A', C', L_a \rangle, L_g \rangle$ , 其中  $g$  为该规划所达成的目标,  $L_g$  为从  $A'$  中的具体动作节点  $a$  到目标  $g$  的因果链  $\{a \rightarrow g\}$  集合.

定理 1. 给定一组观察集  $\langle O, C \rangle$ , 初始状态  $P_0$ , 目标  $g$  为观察集  $\langle O, C \rangle$  的一致性目标, 且  $g$  完全达成或部分达成, 则必然存在观察集  $\langle O, C \rangle$  的一致性规划.

证明. 当目标  $g$  在观察集  $\langle O, C \rangle$  之后完全达成, 根据定义 8, 存在观察集的子集  $\langle O', C' \rangle$ , 目标  $g$  与  $\langle O', C' \rangle$  中的每个观察均相关, 根据定义 7, 存在规划  $\langle A', C'' \rangle$ , 其中  $A'$  为  $O'$  所观察到的具体动作节点集合, 目标  $g$  与  $\langle A', C'' \rangle$  中的每个动作节点均相关, 根据定义 6, 可以构造具体动作节点集合  $A'$  上的因果链集合  $L_a = \{a_i \rightarrow a_j\}$ , 最后根据定义 9 和定义 5, 在给定初始状态  $P_0$  下, 动作规划  $\langle A', C'', L_a \rangle$  与观察集  $\langle O, C \rangle$  相一致, 即存在观察集  $\langle O, C \rangle$  的一致性规划  $\langle g, \langle A', C'', L_a \rangle, L_g \rangle$ .

当目标  $g$  在观察集  $\langle O, C \rangle$  之后部分达成, 令  $g'$  为目标  $g$  中已达成的部分, 则根据上述证明过程, 存在观察集  $\langle O, C \rangle$  的一致性规划  $\langle g', \langle A', C'', L_a \rangle, L_{g'} \rangle$ . 证毕.

定理 1 表明只要在扩展目标规划图中的目标节点层中存在一致性目标节点, 我们均可以找出一条达成这一目标节点的一致性规划. 定理 1 为基于扩展目标规划图的规划识别算法提供了完备性基础.

至此, 我们可以基于以上定义的一致性目标和一致性规划来形式化地定义本文关注的攻击规划识别问题, 即在初始状态  $P_0$  的情况下, 受监控网络中的传感器在一段时间内观察到的数据组成一个观察集  $\langle O, C \rangle$ , 攻击规划识别问题的任务就是识别出观

察集  $\langle O, C \rangle$  的一致性规划集合.

## 5 基于扩展目标规划图模型的攻击规划识别算法

### 5.1 两阶段算法介绍

在上节定义的扩展目标规划图模型的基础上, 本节开始描述从一组观察数据中识别出一致性规划集合的攻击规划识别算法. 算法在每个时间片执行两阶段的处理, 第一个阶段为扩展目标规划图的构建过程, 称为 EGG-Constructor 算法, 以前一个时间片的扩展目标规划图、观察数据集中该时间片的观察事件以及网络攻防领域知识库为输入, 根据观察事件对扩展目标规划图进行进一步扩张, 从而构建该时间片结束后新的扩展目标规划图; 第二个阶段称为 Plan-Recognizer 算法, 其目标是从新的扩展目标规划图中分析识别已达成或部分达成的目标, 并提取与观察数据集合相一致的攻击目标和规划.

### 5.2 EGG-Constructor 算法

EGG-Constructor 算法的初始输入为一个仅包括初始状态节点集的扩展目标规划图  $\Gamma_0 = \{P_0, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset\}$ , 初始状态集  $P_0$  可通过网络环境自动感知机制<sup>①</sup>获取或通过经验规则进行估计. EGG-Constructor 算法由两部分算法组成: 动作扩张算法 Action-Expansion 和目标扩张算法 Goal-Expansion, 而动作扩张算法根据第  $i$  个时间片的观察事件进行扩张, 生成第  $i$  个时间片结束后新的扩展目标规划图; 目标扩张算法对第  $i$  个时间片的状态层节点进行扩张, 将完全达成或部分达成的目标节点加入到第  $i$  个时间片的目标节点层.

动作扩张算法 Action-Expansion<sup>②</sup> 的描述如图 3: 动作扩张算法以第  $i$  个时间片的扩展目标规划图  $\Gamma_i$ 、第  $i$  个时间片的观察集  $O_i$  及攻击知识模型  $KB$  为输入, 算法首先根据观察集  $O_i$  中的每个观察事件  $o_i$ , 将此观察节点添加到第  $i$  个时间片的观察节点层; 通过观察事件的类型  $o_i$  从攻击知识模型中查询与该观察拥有传感器观察关系的具体攻击行为  $D$ , 并对具体攻击行为  $D$  进行实例化得到具体动作节点  $a_i$ , 将此具体动作节点添加到第  $i$  个时间片的具体动作层, 添加从观察节点  $o_i$  到具体动作节点的

① 如 N-Eye 系统, The Artemis Project, N-Eye Network Environment Apperceive Tool. <http://sourceforge.net/projects/n-eye/>, 2005.

② 本文对“假”值的描述方式与参考文献[4]不同, 动作扩张算法和目标扩张算法中的状态  $p$  的取值可为“真”或者“假”, 算法中统一对待  $p$  的取值为“真”或“假”的两种情况,  $\neg p$  表示  $p$  的取值取反, 而非非  $p$  的取值为“假”.



观察边;对具体攻击行为  $a_i$ , 进一步从攻击知识模型中查询与其拥有抽象关系的抽象攻击概念  $B'$ , 并实例化得到抽象动作节点  $b_i$  (包括其前提条件状态和后果状态);对每个抽象动作节点  $b_i$ , 将其添加入第  $i$  个时间片的抽象动作层, 联系具体动作节点  $a_i$  到抽象动作节点  $b_i$  的抽象边, 查看抽象动作节点  $b_i$  的前提条件状态是否在扩展目标规划图第  $i+1$  时间片的状态节点层中存在, 如果存在则连接之间的前提条件关系边, 对抽象动作节点  $b_i$  的后果状态节点, 则添加入第  $i+1$  个时间片的状态节点层. 动作扩张算法然后将第  $i$  个时间片状态节点层中未改变的所有状态节点都保持到第  $i+1$  个时间片, 并连接之间的状态保持边. 最后, 算法返回构建完毕的扩展目标规划图  $\Gamma_{i+1}$ .

Action-Expansion ( $\Gamma_i: \langle P, O, A, B, G, E \rangle, O_i, KB(W, G, D, B, O) \rangle; \Gamma_{i+1}$ )

1. For every  $o_i \in O_i$ 
  - a. Add  $obsv(o_i, i)$  to  $O$
  - b. Get  $O' = schema(o_i)$
  - c. For every  $D \in D \mid \exists R_{Obs}(D, O')$ 
    - c. 1 Instantiate  $D$  with  $o_i$  to get  $a_i$
    - c. 2 Add  $action(a_i, i)$  to  $A$
    - c. 3 Add  $observation-edge(obsv(o_i, i), action(a_i, i))$
    - c. 4 For every  $B' \in B \mid \exists R_{Abs}(D, B')$ 
      - c. 4. 1 Instantiate  $B'$  with  $a_i$  to get  $b_i$ , precondition set  $Pre(b_i)$  and effect set  $Effect(b_i)$  of  $b_i$
      - c. 4. 2 Add  $abstraction(b_i, i)$  to  $B$
      - c. 4. 3 Add  $abstraction-edge(action(a_i, i), abstraction(b_i, i))$
      - c. 4. 4 For every  $p \in Pre(b_i)$  if  $prop(p, i) \in P$  then  
Add  $precondition-edge(prop(p, i), abstraction(b_i, i))$
      - c. 4. 5 For every  $p' \in Effect(b_i)$   
Add  $prop(p', i+1)$  to  $P$   
Add  $postcondition-edge(abstraction(b_i, i), prop(p', i+1))$
2. For every  $prop(p, i) \in P$ 
  - If  $prop(\neg p, i) \notin P$  and  $prop(p, i+1) \notin P$  then  
Add  $prop(p, i+1)$  to  $P$   
Add  $persistence-edge(prop(p, i), prop(p, i+1))$
3. Return with  $\Gamma_{i+1}: \langle P, O, A, B, G, E \rangle$

图 3 动作扩张算法 Action-Expansion

目标扩展算法 Goal-Expansion(图 4)的描述如下:目标扩张算法以第  $i$  个时间片开始的扩展目标规划图  $\Gamma_i$  和网络攻击知识模型中的攻击目标集描述  $G$  为输入, 对每个攻击目标进行实例化, 获取其目标描述对应的安全状态集合, 然后查看这些安全状态是否存在于扩展目标规划图  $\Gamma_i$  的第  $i$  个时间片的状态层中, 如果存在, 则添加该目标节点到扩展目标规划图中, 并在状态节点和目标节点间添加目标描述边, 算法返回经过目标节点扩张的扩展目标规划图  $\Gamma_{i+1}$ .

Goal-Expansion ( $\Gamma_i: \langle P, O, A, B, G, E \rangle, i, G \rangle; \Gamma_{i+1}$  Goal-Expanded)

1. For every  $G_k \in G$ 
  - For every instance  $g$  of  $G_k$ 
    - a. Get a set of goal descriptions  $S_g$ , instantiate  $S_g$  to get  $S'_g$
    - b. For every  $p_g \in S'_g$ 
      - If  $prop(p_g, i) \in P_i$  then  
Add  $goal(g, i)$  to  $G$   
Add  $description-edge(prop(p_g, i), goal(g, i))$  to  $E$
2. Return with  $\langle P, O, A, B, G, E \rangle$  as  $\Gamma_{i+1}$  Goal-Expanded

图 4 目标扩张算法 Goal-Expansion

### 5.3 Plan-Recognizer 算法

当 EGG-Constructor 算法中出现新达成的目标节点时, 进入攻击规划识别的第二阶段扩展目标规划图分析算法——Plan-Recognizer 算法(图 5), 算法描述如下: Plan-Recognizer 算法对第  $i$  个时间片新达成的每个目标节点  $g_i$ , 找出与  $g_i$  拥有目标描述边的状态节点, 并添加到一个状态节点队列  $P'$  中; 算法接着对队列  $P'$  中的每个状态节点, 找出后果状态为该状态节点的抽象动作节点  $b'$  及其对应的具体动作节点  $a'$ , 将  $a'$  添加到攻击规划的具体动作集合中, 并将具体动作节点直接对目标节点的因果链关系添加到  $L_g$ ; 继续找出抽象动作节点  $b'$  的前提条件状态节点集合, 将这些状态节点添加到队列  $L_g$ , 从而进一步查找导致这些状态节点的具体动作, 同时维护攻击规划中的时序约束和具体动作间的因果链关系. 循环结束后, 即对目标节点  $g_i$  可以找出完整的一致性规划  $\langle g_i, \langle A', C', L_a \rangle, L_g \rangle$ .

Plan-Recognizer ( $\Gamma_i: \langle P, O, A, B, G, E \rangle, i, G \rangle; GoalPlan$ )

1. For every  $g_i \in G_i$ 
  - a.  $A' = \emptyset, C' = \emptyset, L_a = \emptyset, L_g = \emptyset, P' = \emptyset$
  - b. For every  $p_i \in P_i \mid \exists description-edge(p_i, g_i)$  enqueue( $P', p_i$ )
  - c. While  $P' \neq \emptyset$  do
    - c. 1  $p' = deque(P')$
    - c. 2 get  $b' \in B \mid \exists postcondition-path(b', p')$   
If  $b' = \emptyset$  then continue
    - c. 3 get  $a' \in A \mid \exists abstraction-edge(a', b')$ ,  $A' = A' \cup \{a'\}$   
If  $\exists description-edge(p', g_i)$  then  $L_g = L_g \cup \{a' \rightarrow g_i\}$
    - c. 4 for every  $p'' \mid \exists precondition-edge(p'', b')$  enqueue( $P', p''$ )  
If  $\exists a'', b'', abstraction-edge(a'', b'') \wedge postcondition-path(b'', p'')$   
 $C' = C' \cup \{a'' \leq a'\}, L_a = L_a \cup \{a'' \rightarrow a'\}$
  - d. Add  $\langle g_i, \langle A', C', L_a \rangle, L_g \rangle$  to  $GoalPlan$
2. Return with  $GoalPlan$

图 5 规划识别算法 Plan-Recognizer

### 5.4 算法分析

可以证明本节提出的扩展目标规划图的扩张算法及分析算法都是稳固的 (Sound) 和完备的 (Complete).

定理 2 (EGG-Constructor 算法的稳固性与完备性). EGG-Constructor 算法是稳固的: 在任何时间片  $i$  加入扩展目标规划图的任何目标节点在时

间片  $i$  的世界状态中一定是完全或部分达成的; EGG-Constructor 算法是完备的: 在所有可能的目标均在知识库已经描述的假设前提下, 如果一个目标由时间片  $i$  之前观察到的具体动作完全达成或部分达成, 那么 EGG-Constructor 算法一定在时间片  $i$  将该目标添加到扩展目标规划图中。

证明。

(稳固性) 扩展目标规划图的时间片 1 状态层仅包括初始状态节点, 表示没有任何观察到的具体动作时的世界状态, 通过 EGG-Constructor 算法将时间片  $i-1$  观察到具体动作对应的后果状态加入到时间片  $i$  的状态节点层中, 并将其它时间片  $i-1$  状态层中未改变的状态节点通过状态保持边复制到时间片  $i$  的状态节点层, 因此扩展目标规划图在时间片  $i$  的状态节点层中反映了当前的世界状态, 而在时间片  $i$  加入扩展目标规划图的目标节点是在时间片  $i$  的状态节点层中完全达成或部分达成的, 因此在时间片  $i$  的世界状态中也一定是完全或部分达成的。

(完备性) 假设一个目标在时间片  $i$  已经由从时间片  $1, 2, \dots, i-1$  的具体动作完全或部分达成, 那么该目标在扩展目标规划图中时间片  $i$  的状态层中已经完全或部分达成, 根据 EGG-Constructor 算法的动作扩张和目标扩张过程, 所有在知识库中的目标模板的所有在时间片  $i$  的状态层中已经完全或部分达成的目标实例节点都将添加到时间片  $i$  的目标节点层中, 基于知识库中的攻击目标完备性假设, 该目标也是知识库中某个目标模板的一个实例, 因此 EGG-Constructor 算法必然会将该目标添加到时间片  $i$  的目标节点层中。

证毕。

定理 3 (Plan-Recognizer 算法的稳固性与完备性)。Plan-Recognizer 算法是稳固的: Plan-Recognizer 算法在时间片  $i$  识别得到的规划  $\langle g, \langle A', C', L_a \rangle, L_g \rangle$  都是到时间片  $i$  观察集  $\langle O, C \rangle$  的一致规划; Plan-Recognizer 算法算法是完备的: 给定一组到时间片  $i$  观察集  $\langle O, C \rangle$ , 初始状态  $P_0$ , 目标  $g$  为观察集  $\langle O, C \rangle$  的一致性目标, 若  $g$  在时间片  $i$  完全达成或部分达成, 则通过 Plan-Recognizer 算法能够识别获得达成  $g$  的一致规划  $\langle g, \langle A', C', L_a \rangle, L_g \rangle$ 。

证明。

(稳固性) 首先, EGG-Constructor 算法是根据观察集  $\langle O, C \rangle$  构建扩展目标规划图中的观察节点层, 并根据观察边构建具体动作层, 因此由 Plan-Recognizer 算法识别出来的规划中的具体动作行为均是观察集相对应的, 即  $\forall a \in A', \exists o \in O, \exists ob-$

servation-edge  $(o, a)$ ; 其次, 由 Plan-Recognizer 算法的特性, 将目标  $g$  描述的状态节点以及依赖的中间状态节点逐层添加入状态节点队列  $P'$ , 并逐步提取以这些状态节点为后果状态的具体动作添加入所识别的规划中, 直至队列  $P'$  为空, 由此过程得到的规划  $\langle A', C', L_a \rangle$  中的每个动作均是目标  $g$  的相关动作, 同时将初始状态  $P_0$  改变到使得目标  $g$  达成的世界状态, 根据定义 5, 规划  $\langle A', C', L_a \rangle$  是在初始状态  $P_0$  下目标  $g$  的一个有效规划; 最后根据定义 8、定义 7 和定义 6, 规划  $\langle A', C', L_a \rangle$  的达成目标  $g$  与  $A'$  中的动作均是相关的, 与  $A'$  的观察集  $O'$  也均是相关的, 因此目标  $g$  是观察集  $\langle O, C \rangle$  的一个一致性目标。综合上述三个推论, 根据定义 9, 由 Plan-Recognizer 算法识别得到的  $\langle g, \langle A', C', L_a \rangle, L_g \rangle$  均为观察集  $\langle O, C \rangle$  的一致性规划。

(完备性) 首先, 根据定理 2 中 EGG-Constructor 算法的完备性, 对于在时间片  $i$  完全达成或部分达成的目标  $g$ , EGG-Constructor 算法一定在时间片  $i$  将该目标添加到扩展目标规划图中; 而 Plan-Recognizer 算法过程对每个目标节点都将生成一个规划  $\langle A', C', L_a \rangle$ , 该规划中包括扩展目标规划图中与目标  $g$  相关的具体动作节点, 而根据 Plan-Recognizer 算法的稳固性, 生成的规划  $\langle g, \langle A', C', L_a \rangle, L_g \rangle$  为到时间片  $i$  观察集  $\langle O, C \rangle$  的一致规划; 综合上述条件, 即对每个在时间片  $i$  完全达成或部分达成的目标  $g$ , 通过 Plan-Recognizer 算法能够识别获得达成  $g$  的一致规划  $\langle g, \langle A', C', L_a \rangle, L_g \rangle$ , 因此 Plan-Recognizer 算法是完备的。证毕。

## 6 实验分析

我们实现了上节中提出的基于扩展目标规划图的攻击规划识别算法, 并基于 DARPA 2000 入侵场景关联评测数据以及在蜜网环境中捕获的实际僵尸网络场景对其进行了实验验证。

### 6.1 DARPA 2000 数据集实验

DARPA 2000 数据集是 DARPA 资助 MIT 林肯实验室构造的入侵场景关联评测数据集, 被普遍应用于入侵报警关联算法的有效性验证<sup>[5,16,17]</sup>, 但目前公开的文献, 只有 Ning 等人的 TIAA 系统<sup>[5]</sup>给出了对此数据集的完整实验结果, 因此本节将给出本文算法对此数据集的关联结果, 并与 TIAA 的关联结果进行对比, 以说明本文提出的算法较传统报警关联方法的优势。该数据集包括两个攻击场景实例: LLDOS 1.0 和 LLDOS 2.0.2。在



LLDOS 1.0 攻击场景中,攻击者通过 Solaris sadmind 服务漏洞攻陷并控制了“Eyrie”空军基地网络中的三台主机,上传了 Mstream 分布式拒绝服务攻击工具,并对某一美国政府网站发动了分布式拒绝服务攻击. LLDOS 2.0.2 攻击场景与 LLDOS 1.0 类似,不同的是攻击者对漏洞主机的发现以及 Mstream 分布式拒绝服务攻击的上传都采用了更为隐蔽的方法,从而验证关联算法在底层入侵检测系统存在漏报情况下的关联效果.

为了保证关联结果的可比较性,本文使用了与 Ning 等人相同的报警数据文件(Realsecure 对两个场景原始数据报文的报警信息文件),同时也采用了 Ning 等人提出的关联分析算法评测指标:关联完备

性(正确关联报警数与相关报警数的比值)和关联有效性(正确关联报警数与被关联报警数的比值).

通过第 4 节描述的扩展目标规划图的构建算法以及从扩展目标规划图中识别得到的达成目标的攻击规划算法,对 DARPA 2000 LLDOS 1.0 攻击场景得到的最终攻击关联场景图如图 6 所示,与 TIAA 系统关联结果相比,除了通过对安全状态的跟踪与达成攻击目标规划的精确识别过程消除了 TIAA 系统关联结果中存在的 3 个错误关联外,还详细体现出了 172.16.115.20 上安装的 Mstream handler 和其它主机上安装的 Mstream agent 的协同过程,从而使得分析人员能够更清晰地理解该数据集中 Mstream DDoS 攻击的全过程.

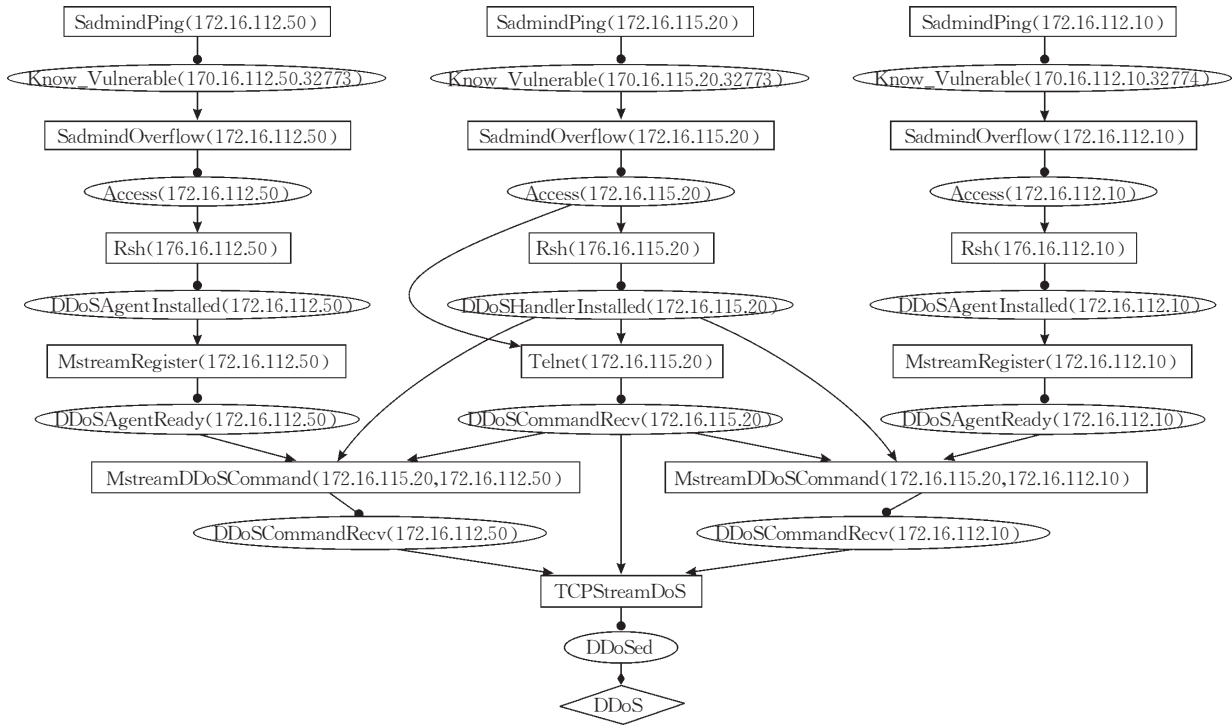


图 6 对 DARPA 2000 LLDOS 1.0 攻击场景的关联结果

本文算法与 TIAA 系统最终的结果对比如表 1 所示,本文算法对 LLDOS 1.0 和 LLDOS 2.0.2 均取得了 100% 的完备性,即所有与攻击场景相关的报警都被关联到最终得到的攻击场景图中,在 LLDOS 2.0.2 场景中,由于存在 Email\_Ehlo 和

Email\_Turn 误报警并达成攻击目标 GainAccess 导致错误的关联,因此关联有效性分别为 75% 和 88.9%. 对比结果显示,对每个测试数据集,本文算法均达到了比 TIAA 更优的关联完备性,而关联有效性则与 TIAA 相当.

表 1 Athena 关联分析原型系统对 DARPA 2000 数据集的关联结果统计并与 TIAA<sup>[5]</sup> 的对比

		关联结果					
		本文算法			TIAA <sup>[5]</sup>		
		相关报警数	关联报警数	正确关联	完备性(%)	有效性(%)	完备性(%)
LLDOS 1.0	DMZ	57	58	57	100	98.3	94.7
	Inside	44	44	44	100	100	93.2
LLDOS 2.0.2*	DMZ	6	8	6	100	75	100
	Inside	16	18	16	100	88.9	92.3

\* Ning 等人<sup>[5]</sup>认为误报警 Email\_Ehlo 和 Email\_Turn 的关联是正确关联,而本文认为这两个报警与实际发生的攻击场景无关,不应计入相关报警数和正确报警数内,本文将这两个误报警的关联计入了错误关联数.

6.2 实际僵尸网络场景识别实验

为了进一步验证本文算法在实际环境中的有效性,我们使用在互联网上部署的蜜网环境中捕获的实际僵尸网络攻击场景数据对本文算法进行了进一步测试,图 7 给出了本文算法在实际蜜网环境中从 2006 年 1 月 16 日到 2006 年 1 月 29 日间的关联结果数据统计,从每天超过 1000 条观察数据中能够准确地关联出 1~10 个规模的成功攻击场景,而与这些成功攻击场景相关的观察事件数也在 10~100 个这一量级规模.图 8 显示了一个典型的僵尸网络成功攻击场景,利用 RPC、NetBIOS 等 Windows 系统常用服务中的系统漏洞进行溢出攻击得到访问权,并通过 FTP 方式上传僵尸程序体,僵尸程序激活后,连接僵尸网络的控制信道,从而接收攻击者的进一步控制指令.

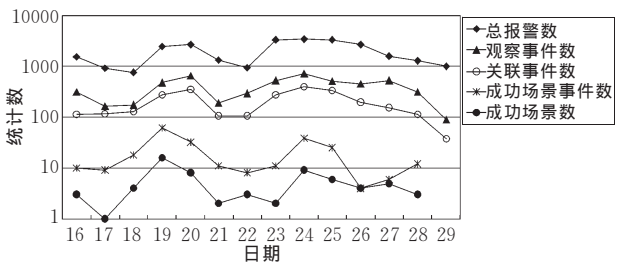


图 7 本文算法对实际蜜网环境中捕获的僵尸网络攻击场景的关联分析效果

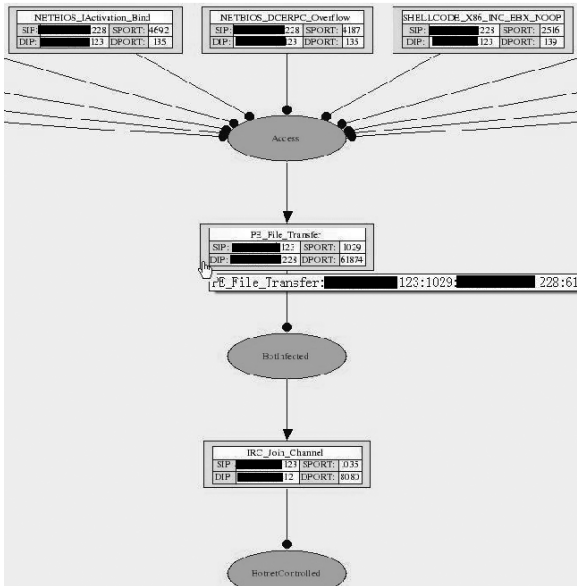


图 8 本文算法对蜜网捕获的一个典型僵尸网络攻击场景的关联结果图

从上述实验结果可以看出,本文算法能够有效地达到对网络攻击规划的识别,辅助安全分析人员对实际发生的网络安全威胁进行快速有效的理解,从而帮助其更好地应对这些安全威胁.

7 结 论

本文在人工智能领域中规划识别方法的基础上,针对网络攻防领域中规划识别问题的特性,对目标规划图进行进一步扩充,引入观察节点以区分规划者动作以及识别者对动作的观察,将动作节点分化为由具体动作层和抽象动作层组成的层次结构,并根据抽象攻击模式在抽象攻击层面上维护与安全状态节点的前提和后果条件,形成扩展目标规划图(Extended Goal Graph,EGG)模型;并进一步提出基于扩展目标规划图的攻击规划识别算法,通过两阶段的扩展目标规划图构建和分析算法,从大量底层入侵报警信息中识别背后蕴藏的攻击者意图及规划.通过 DARPA 2000 数据集和实际僵尸网络攻击场景的实验表明,本算法具有:能够对攻击规划过程中的状态变化进行有效跟踪,从而有效消除错误关联并清晰体现攻击规划的流程;能够保证关联结果的完备性;知识库构建具有可行性和易维护性,对实际发生攻击场景的关联具有更强的实用性等优势.

本文下一步研究方向包括:(1)引入不确定知识表示方法和推理机制对关联分析过程中存在的不确定性进行处理;(2)研究对未达成目标的攻击规划的预测算法;(3)针对实际环境中更多类型的网络攻击场景,在网络攻防知识库中刻画其抽象攻击模式,并对本文算法进行更加深入的测试和验证,从而提高本文算法的实用性.

参 考 文 献

1 Amoroso E. , Intrusion detection—An introduction to Internet surveillance, correlation, trace-back, traps, and response. Intrusion. Net Books, 1999

2 Axelsson S. . The base-rate fallacy and its implications for the difficulty of Intrusion Detection. ACM Transactions on Information and System Security (TISSEC), 2000, 3(3): 186~205

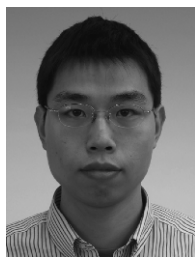
3 Blum A. L. , Furst M. L. . Fast planning through planning graph analysis. Artificial Intelligence, 1997, 90: 281~300

4 Hong J. . Goal recognition through goal graph analysis. Journal of Artificial Intelligence Research, 2001, 15: 1~30

5 Ning P. , Cui Y. , Reeves D. S. , Xu D. . Techniques and tools for analyzing intrusion alerts. ACM Transactions on Information and System Security (TISSEC), 2004, 7(2): 274~318

6 Debar H. , Wespi A. . Aggregation and correlation of intrusion detection alerts. In: Lee W. , Me L. , Wespi A. eds. Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID). Lecture Notes in Computer Sci-

- ence 2212. Springer-Verlag, 2001, 85~103
- 7 Dain O. , Cunningham R. K. . Building scenarios from a heterogeneous alert stream. In: Proceedings of the IEEE SMC Information Assurance Workshop, West Point, NY, 2001
  - 8 Porras P. A. , Neumann P. G. . EMERALD: Event monitoring enabling responses to anomalous live disturbances. In: Proceedings of the 20th National Information Systems Security Conference, Baltimore, Maryland, 1997, 353~365
  - 9 Valdes A. , Skinner K. . Probabilistic alert correlation. In: Lee W. , Me L. , Wespi A. eds. Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID). Lecture Notes in Computer Science 2212. Springer-Verlag, 2001, 54~68
  - 10 Morin B. , Debar H. . Correlation of intrusion symptoms: An application of chronicles. In: Vigna G. , Jonsson E. , Krugel C. eds. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID). Lecture Notes in Computer Science 2820. Springer-Verlag, 2003, 94~112
  - 11 Dousson C. . Extending and unifying chronicles representation with event counters. In: Proceedings of the 15th European Conference on Artificial Intelligence (ECAI 2002), Lyon, France, 2002, 257~261
  - 12 Geib C. W. , Goldman R. P. . Plan recognition in intrusion detection systems. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX II'01), Anaheim, California, 2001
  - 13 Geib C. W. , Goldman R. P. . Probabilistic plan recognition for hostile agents. In: Proceedings of the 14th International Florida Artificial Intelligence Research Society Conference, 2001, 580~584
  - 14 Fikes R. , Nilsson N. . STRIPS: A new approach to the application of theorem proving to problem solving. Artificial Intelligence, 1971, 2: 189~208
  - 15 Cuppens F. , Miège A. . Alert correlation in a cooperative intrusion detection framework. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, USA, 2002
  - 16 Yan W. , Hou E. , Ansari N. . Extracting attack knowledge using principal-subordinate consequence tagging case grammar and alerts semantic networks. In: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04), 2004
  - 17 Bao Xu-Hua, Dai Ying-Xia, Feng Ping-Hui, Zhu Peng-Fei, Wei Jun. A detection and forecast algorithm for multi-step attack based on intrusion intention. Journal of Software, 2005, 16(12): 2132~2138(in Chinese)  
(鲍旭华,戴英侠,冯萍慧,朱鹏飞,魏 军. 基于入侵意图的复合攻击检测和预测算法, 软件学报, 2005, 16(12): 2132~2138)



**HAN Xin-Hui**, born in 1969, Ph. D. candidate, assis-

**ZHUGE Jian-Wei**, born in 1980, Ph. D., assistant professor. His main research interests include intrusion detection and correlation, honeypot and honeynet technologies, malware analysis and prevention technologies.

tant professor. His main research interests include honeypot and honeynet technologies, malware analysis and prevention technologies.

**YE Zhi-Yuan**, born in 1963, senior engineer. His main research domain is network and information security.

**ZOU Wei**, born in 1964, professor. His main research domain is network and information security.

## Background

This work is supported by the China Information Security Project, named "Botnet Monitor System Research based on the Honeynet Technology", under grant of No. 2005C32.

As well known, botnets have raised more and more threats to the Internet security. This project focuses on the discovery, tracking and treatment of the active botnets on the Internet using distributed honeynet technology. The recognition and reconstruction of botnet attack scenarios is essential to this project, and it also belongs to the attack plan recognition problem in the network attack and defense domain.

With the foundation of classical planning graph and goal graph model in the domain of artificial intelligence, for dealing with the complexity of network attack and defense problem, this paper defines the EGG (Extended Goal Graph) model formally, and presents attack plan recognition algorithm based on

the proposed EGG model. Furthermore, through the experiments using DARPA 2000 intrusion scenario correlation benchmark dataset and in-the-wild botnet scenarios data captured in the honeynet, the results show the completeness and soundness of the proposed algorithm. The proposed algorithm has been implemented as a botnet scenario recognition subsystem of the botnet monitor system.

This work is done with The Artemis Project, initiated by Institute of Computer Science and Technology, Peking University, which is the only participant of world-wide Honeynet Research Alliance in China, and is known as Chinese Honeynet Project. The research direction of The Artemis Project is the measurement, analysis and treatment of practical and serious Internet treats based on honeypot and honeynet technologies.