一种基于知识表示的多步攻击规划问题描述模型

努尔布力[1,4],解男男[2],刘志宇[3],胡 亮[2],柴 胜[2]
(1.新疆大学信息科学与工程学院,新疆乌鲁木齐 830046;2.吉林大学计算机科学与技术学院,
吉林长春 130012;3.公安部第一研究所,北京 100044;4. 新疆多语种信息技术重点实验室,新疆乌鲁木齐 830046)

摘 要: 网络入侵检测中,攻击的形式越来越多样化和复杂化,网络多步攻击成为当前攻击的主要形式.智能规划最早用于人工智能领域,将一个领域内的知识形成规划推理时的规划域,将待求解的问题对应于规划问题.将智能规划应用于多步攻击领域,用以对多步攻击进行识别,并以此为基础,提出一种基于知识表示的多步攻击规划问题描述模型,用以提供解决复杂网络攻击数据的形式化描述问题的一种探索.实验中规划问题采用PDDL语言进行描述,对所提模型进行可用性验证.

关键词: 多步攻击; 智能规划; 安全规划问题; PDDL
中图分类号: TP39 **文献标识码:** A **文章编号:** 0372-2112 (2013) 06-1101-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.06.010

A Multi-Stage Attack Planning Problem Description Model Based on Knowledge Representation

Nurbol[1,4], XIE Nan-nan[2], LIU Zhi-yu[3], HU Liang[2], CHAI Sheng[2]
(1. *School of Information Science and Engineering, Xinjiang University, Urumqi, Xinjiang* 830046, *China*;
2. *Computer Science and Technology College, Jilin University, Changchun, Jilin* 130012, *China*;
3. *The First Research Institute of the Ministry of Public Security of PRC, Beijing* 100044, *China*;
4. *Key Laboratory of Multi-Language Information Technology, Xinjiang University, Urumqi, Xinjiang* 830046, *China*)

Abstract: In network intrusion detection, the modes of attack are more and more complex and diversified. Network multi-stage attack has been the main form of current attack. Intelligent planning was used in artificial intelligence, makes the fields knowledge as planning domain, and the issues to be solved as planning problems. In this paper, intelligent planning was used in recognition of multi-stage attack, and based on this, a multi-stage planning problem recognize model was proposed, in order to provide an useful exploration of network attack data formal description. The model is described in PDDL, and evaluation shows the proposed model have well availability.

Key words: multi-stage attack; intelligent planning; security planning problem; PDDL

1 引言

根据CNCERT/CC 2010年互联网安全报告[1],网络安全事件的分类统计中,几乎所有的攻击都属于多步骤攻击.针对大型企业和政府部门的协作式、多阶段的网络入侵事件越来越多,造成的很大的社会负面影响.

入侵检测是目前应对网络环境中各种攻击的关键技术之一.Anderson将入侵定义为[2]:在没有授权的情况下,尝试访问信息、篡改信息、使系统不可靠或不可用.目前入侵检测系统针对复杂入侵行为的分析效果不佳,主要原因有两个方面,其一是入侵检测系统的警报信息量大并且孤立,难以进行有效的关联,其二是现有的多步攻击分析方法并不完善,而对于警报关联等多步攻击分析方法的研究和改进,是目前的研究热点.这使得入侵检测系统的检测率、误报率和漏报率并不理想.本文的研究出发点是通过智能规划来提升复杂入侵行为的分析效果.智能规划在问题的描述和问题的求解两方面有了新的突破[3],成为人工智能研究者普遍关心的一个重要领域.

本文工作以提升复杂网络攻击的识别效果为研究

收稿日期:2012-10-10;修回日期:2013-01-07
基金项目:国家重点基础研究发展计划(973计划)(No.2009CB320706);国家高技术研究发展计划(863计划)(No.2011AA010101);国家自然科学基金(No.61073009,No.61163052);吉林省重大科技攻关项目(No.2011ZDGG007);长春市国际合作项目(No.11GH12);新疆大学博士启动基金(No.BS110126)

目标,主要进行智能规划问题描述方面的工作.将智能规划的相关方法应用于攻击信息分析,首先需要解决入侵检测领域下规划域和规划问题描述模型的构建问题.针对入侵检测效果不佳的两个主要原因,我们的工作一方面通过形式化表示以达到消除信息孤立的目的,另一方面希望采用动态规划方法进行复杂网络攻击行为的分析.本文提出了一种基于知识表示的多步攻击规划问题描述模型,并通过实验验证描述方法的可行性.为下一步结合小组在规划域的形式化描述研究工作,实现应用规划方法分析复杂网络入侵,奠定基础.

2 知识表示、智能规划和多步攻击

2.1 知识表示

知识表示是人工智能领域的核心研究内容之一,目前并没有统一的标准定义.R Davis 等从知识表示解决的问题和涉及领域的角度给出了分析:知识表示是对事物或智能行为本身的描述,使得事物或事件能够通过理论分析而不是实践,来确定发展的方向或者轨迹,是智能推理、高效计算的一部分,它也是人类表达的一种,例如,人类语言就是一种对世界的知识表示[4].

王珏等将智能规划领域的知识表示研究分为知识表示方法的研究和表示观的研究两个层次.表示方法,即如何对知识进行表示,这些方法是研究者对智能行为的抽象模型.表示观是指对"什么是表示"这一类基本问题的回答.对于这个问题的不同理解,形成了不同的"表示观"流派,例如,认识论表示观,本体论表示观,知识工程表示观等[5].

知识表示需要满足充分的表达、有效的推理、方便的维护、易于理解等特性,基于这些特性的要求,传统知识表示方法主要有以下 5 种[6]:

(1)一阶谓词逻辑表示法.一阶谓词逻辑与人类自然语言比较接近,具有简单、自然、精确、灵活、容易实现等特点,一般形式为 $P(x_1,x_2,\cdots,x_n)$其中 P 是谓词,x 是常量、变量或者函数.这种谓词方法适用于表示事物的规则.局限在于难以表达不确定性、启发性知识,会出现状态爆炸,推理过程效率低.

(2)产生式表示法.基本形式为 if(前提 1)&(前提 2)&...then(结论 1)&(结论 2)….如果前提被满足,则可以推出结论或者执行所规定的动作.这种表达方法的优点依然是自然,灵活,清楚,模块性好,通用性强.缺点是难以表达具有结构性特征的知识,并且求解过程效率不高,容易造成组合爆炸.

(3)框架表示法.用以描述对象属性的一种数据结构,框架是知识表示的基本单元.通过属性之间建立联系,构成框架网络.善于表达结构性知识,继承性良好,缺点是对于过程性知识的表示有难度.

(4)脚本表示法.用于对某些专门知识的表达,结构类似于框架,用于描述固定的事件序列.

(5)语义网络表示法.用带有标识的有向图表示各种事物的语义关联和属性,灵活自然、易于实现,但是可能存在二义性.

近年来,知识表示的方法有了新的发展,在传统表示方法的基础上,提出了混合知识表示方法,例如,将谓词逻辑、产生式规则和过程式的融合.随着面向对象技术发展而出现的面向对象知识表示方法,随着模糊理论的发展产生的模糊技术的知识表示方法等.这些研究使得知识表示对事物的描述能力越来越精确,并且适应于不同的应用领域.Hornsby 等提出了一种基于知识表示的模型,能够根据所识别对象的变化进行描述.对实体识别的关键是对概念变化的追踪,文中提出的办法能够最小化识别模型需要的特征属性[7].基于地球与环境术语的语义网络(SWEET),是地学系统科学研究中非常重要的工具,已经开发形成了一个完整的地球和环境的本体系统,并用 OWL 完整表达.Raskin RG 等在文章中描述了地球科学系统和相应概念的知识空间,同时开发了一个搜索工具,用以发现可替换的搜索术语,并且扩展了搜索引擎的术语范围[8].在安全领域,诸葛建伟等针对网络攻防中攻击规划识别问题的特性,采用经典规划识别的方法对目标规划图进行进一步的扩充,形成了扩展目标规划图模型,并进一步提出了基于扩展目标规划图的攻击规划识别算法,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[9].

在诸如医疗、科学和工程等领域,由于持续的发展,其中的知识往往是动态变化的.因此,设计基于知识的系统,能够适应知识的动态变化具有重要的使用意义.Li X 等提出了一种用于专家系统的模糊 Petri 网模型 AFPN.这种模型不仅包含模糊 Petri 网的特征,还包括神经网络的学习能力.经过训练之后,AFPN 模型能够应用于动态的知识表示和推理[10].

2.2 智能规划

智能规划(Artificial Intelligence Planning)是人工智能研究中的一个重要领域,同时也是一门涵盖知识表示、自动推理、非单调逻辑、人机交互和认知科学等方面的多领域交叉性学科[11].智能规划的研究最早起源于自动推理与知识表示,在 20 世纪 90 年代以前,一直采用逻辑演绎的方法予以求解,主要侧重于经典逻辑下的各种推理技术的利用.1996 年,Blum 等人设计的基于规划图的 Graphplan 规划系统很好的解决了知识表示过程中的指数级空间爆炸问题,使得智能规划领域逐步得

到相关研究者的重视[12].

智能规划通常研究的是一类领域问题,需要领域专家将一个领域内的常识以及本质的知识形成规划推理时的知识库—规划域,而需要向规划推理方法提供的另一个输入就是在对应知识库上进行求解的规划问题.由于受到规划域的限制,对应的规划问题通常是几类对应的领域问题.规划系统把规划方法集成在其中,规划域给出领域问题的可用的资源和资源约束,并通过可以采取的动作进行推理,求解出问题的规划路径,它通常是以动作序列的形式表现的.

近年来,智能规划的应用领域更加广泛.Marchetta MG 等提出了一种基于智能规划的混合程序和知识表示,其中探讨了对制造业中经典的特征解释和特征表示问题[13].von Mayrhauser A 等将智能规划应用于黑盒测试中的测试目标生成,应用于待测试系统的 UML 类图中.将生成的规划域和规划问题作为规划器的输入,从而产生出相应的测试样本[14].蒋志华等提出了一种基于智能规划的 Parlay X 电信业务设计方法 APBPTSD,用标准后处理动作处理容错,用等待事件动作处理异步响应,用本地动作处理变化推理[15].智能规划在安全领域的应用目前并不多见,典型的研究有王桢珍等为了评估网络信息系统的安全风险,提出了基于智能规划的信息安全风险过程建模方法,最后通过规划渗透图表现系统安全风险过程[16].

智能规划领域常用的描述语言有 Strips[17]、ADL 和 PDDL.由于智能规划大赛的出现,PDDL 语言虽然出现较晚,却是为 IPC 专门设计的比赛使用语言,这也是为了便于智能规划的领域知识的统一表示,同时也可以将不同的规划器的解决问题的能力进行统一的比较了.PDDL 语言随着 IPC 的不间断举行,语言本身历届都会被进一步改进,使得 PDDL 的描述能力已经超出了规划所能处理的范围[18].

2.3　多步攻击

多步攻击是单步攻击按照一定逻辑关系的排列,在特定的时间和空间条件下,形成一个攻击序列,从而实现对目标主机的攻击过程.典型的多步攻击通常具有以下特点:攻击方式多样性,例如使用缓冲区溢出漏洞、利用数据库注入或者利用主机某些服务的漏洞来完成攻击;攻击过程多步骤,例如攻击者会先搜寻一个网络中开启的主机的信息,然后根据这些信息确定准备攻击的多个主机,再通过一些工具确定这些目标主机的漏洞和脆弱性,之后再根据不同的主机弱点执行攻击行为;攻击步骤顺序性,一个攻击步骤的完成就意味着下一个攻击步骤的开始,这些攻击步骤对应着不同的攻击行为,存在着一定的先后时序关系.

警报关联是目前多步攻击领域研究的主要问题,用来解决多步攻击警报数据繁多并且孤立的问题.目前,国内外对于警报信息的研究是以警报关联的方法或算法为主,对于警报数据规则化描述的研究较少.典型的警报关联方法主要包括基于属性相似度的警报关联,基于已知场景的警报关联,基于因果关系的警报关联,基于关联规则的警报关联,基于统计分析的警报关联等[19].穆成坡等提出了一种基于模糊综合评判的方法来处理入侵检测系统的报警信息、关联报警事件,通过确信度来对报警信息进行过滤,力求降低误报率和重复报警[20].法国 France Telecom 公司的 Benjamin Morin 等对 IDS 警报关联进行研究,提出了一种形式化的数据模型 M2D2,其中包含四种信息类型:与监控信息系统的特征相关的信息,监控系统脆弱性的信息,与监控系统使用的安全工具相关的信息,以及观察事件的信息.用 M2D2 对警报数据进行规范化描述,可以进行进一步的警报关联[21].

目前的警报关联系统大都是基于规则库的,依赖于专家知识,容易出错.还有基于统计的模型,这些模型往往难以发现安全事件之间的因果关系.Alserhani Faeiz 等提出了一种警报关联的框架,用以解决上述的问题,将一种改进的因果关系模型和统计模型结合,用以提高检测率,降低误报率,基于知识表示的模型用以提供可管理的和有意思的图.通过 DARPA2000 测试证明了所提方法的有效性[22].Strayer WT 等在 SPIE 的基础上将其扩展,提出了一种多步攻击回溯的知识框架 STARLITE,将单一的网络包回溯和多步攻击过程检测结合,并建立原型,用以解决传统的 IP 包难以解决多步攻击回溯的问题[23].

虽然网络以及主机的安全防护能力在不断的提升,但是攻击者的攻击手段也在不断演进,更加的难以防范和追查.一种典型的多步攻击识别模型如图 1 所示[24].

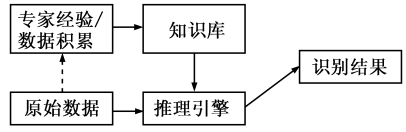

图1　一种典型的多步攻击识别模型

图 1 中,专家通过观察分析原始数据形成经验的积累,同时存储具有研究价值的数据,最终以专家经验和领域数据形成识别攻击的知识库.在后续的攻击识别中,原始数据作为输入传递给核心部分—推理引擎,推理引擎使用内置的推理计算算法比结合知识库,从原始数据中得出识别攻击的结果.

智能活动就是获取知识和运用知识的过程,按照上面的分类标准,将智能规划应用于多步攻击数据的

描述领域,是知识表示领域中的一种产生式表示法.根据智能规划的定义,对于完整的多步攻击的描述,分为规划域和规划问题两部分.其中,规划域是用规则化的描述语言描述的知识库,而规划问题是同样规则化描述的待解决的问题.

3 多步攻击规划问题描述模型

考虑多步攻击模型和智能规划领域的关联,提出一种攻击识别和智能规划的关联模型,用以描述智能规划领域和攻击识别领域的对应关系.后文中基于知识表示的多步攻击规划问题描述模型,是这一模型中的组成部分.攻击识别和智能规划的关联模型如图2所示.

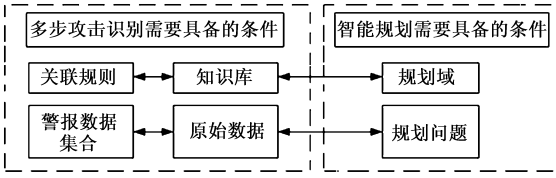

图2 攻击识别和智能规划的关联模型

图2中,多步攻击识别需要具备的条件有知识库和原始数据,原始数据对应于警报数据的集合,知识库即是关联规则库,根据其中的关联规则,建立单条警报之间的关系.其中,知识库对应智能规划中的规划域概念,而原始数据对应的是规划问题.根据知识库建立规划域,再将多步攻击警报描述为规划问题,从而实现多步攻击警报关联.

规划问题的问题文件包含两部分:初始状态(initial state)和目标状态(goal state).规划器从初始状态出发,利用相应的规划域中提供的知识和推理规则来进行计算推理,找出能够到达目标状态的路径,从而得出相应的规划解.因此,规划问题文件的生成就需要提供初始和目标状态的描述,而这些信息就是根据提供的警报数据而生成的.基于知识表示的多步攻击识别的安全规划问题描述模型如图3所示.

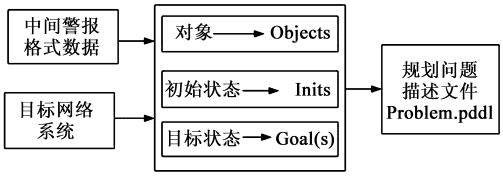

图3 基于知识表示的多步攻击规划问题描述模型

3.1 数据结构

规划问题的数据结构定义如下:

定义1 将处理后的中间警报格式数据作为数据源,那么这些数据包含的信息包含有如下属性:源IP、目的IP、协议类型、端口信息、警报时间、警报安全类型等等.

定义2 如果用∑表示这些警报数据模型,∑是一个八元组.

∑=(IS,PS,ID,PD,P,S,T,E);其中:

IS和ID分别表示警报中包含的源IP地址和目的IP地址,这里指的都是IPv4地址.

PS和PD,分别表示警报中包含的源端口和目的端口,其取值范围都是0~65535.

P表示协议类型

S表示警报的安全状态.

T表示警报的时间戳记录.

E表示其他扩展项.若∑的E项没有具体内容,则此∑项可以设置为NULL,不予处理.

3.2 处理机制

规划问题的处理机制定义如下:

定义3 对于一条警报数据可以将其根据定义2中的模型∑=(IS,PS,PD,ID,S,T,E)转换成智能规划的表示形式.转化方法如下:

(1)若E=NULL,(IS,PS,T)→Object,(ID,PD,T)→Object,(IS,P,S)→(Inits and Goals)Predicate,(ID,P,S)→(Inits and Goals)Predicate.

(2)如果E≠NULL,(IS,PS,T,E)→Object,(ID,PD,T,E)→Object,(IS,P,S,E)→(Inits and Goals)Predicate,(ID,P,S,E)→(Inits and Goals)Predicate.

定义4 由定义3中得出Inits和Goals,再引入作为推理知识库的规划域的名称,形成一个完整的规划Problem.

PDDL语言是一种以动作为中心的规划域描述语言,更加接近自然语言,从整体上扩展了Strips和ADL表示范围,在智能规划领域得到了长足的发展,已成为一种标准的规划描述语言,本文将使用PDDL语言对规划问题进行描述.

采用PDDL语言描述DDos攻击的规划问题如下:

```
(define(problem DDosattack1)
  (:domain DDosattack)
    (:objects Echo-ICMPEcho a z = HostAsset Good
      receivestatus sadmindpingStatus sadmindOver-
      FlowStatus ZTelnetStatus-Status)
    (:init (sendToIcmpecho Echo)
           (is receivesatus Good))
    (:goal (attack a z)))
```

4 实验评估

本文对提出的模型进行可用性的评价,在一定的实验环境下,提出的描述模型能够达到有效识别多步

攻击的目的.

4.1 实验环境

(1)系统平台:Linux(ubuntu-10.04).

(2)数据集:这里的入侵检测数据采用 MIT 的 DARPA2000 数据集[25].

以 DARPA2000 中的拒绝服务攻击为例,攻击过程如图 4 所示.

(3)规划器:FF v2.3 版

FF 规划器是 Fast Forward 的缩写,此规划器参与了 IPC-2000,在 IPC-2000 的比赛上,表现突出,解决的问题用时都比较少,而且求出的解是最优解或者接近于最优解.而且参与了 IPC-2002,并获得了最优表现奖.

(4)评价指标说明:传统入侵检测一般应用检测率、误报率和漏报率作为评价指标,这里为了证明描述的有效性,采用针对 LLDOS 1.0 中五个攻击阶段的单个步骤的识别情况作为评价分析的标准[26].

4.2 结果分析

对于规划问题的验证,与规划域有必然的联系.规划域(Planning Domain)在国内外的有关文献中并没有严格的定义描述,它是智能规划中可用规划来解决的领域问题的抽象描述,根据研究和实际问题的需要,提炼出与问题解决有重大关系的要素,在此基础上结合实际附加一些假定条件,从而形成的对一个领域内问题的全局条件的描述.在这个描述体系中,只有与规划问题相关的元素.在与本文工作关联的另一篇文献中,对 DARPA2000 多步攻击规划域进行了描述,本文实验中采用上文中定义的规划问题.

图 5 中所描述的规划域是本文前期工作的一部分,是采用 PDDL 语言描述的多步攻击规划域.其中,define 定义了描述域的名称,requirement 标签内定义了该描述域能够解决问题的能力范围,types 定义了这个域内的一些类型,constants 根据实际问题定义了不变量,predicate 标签内定义用于逻辑推理的逻辑谓词,action 标签内定义的是关于这类实际问题所应该具有的实际行为.其中,IPscan 是攻击动作之一的 IP 扫描,针对上文中介绍的 DDOS 攻击,其相应的攻击动作还有端口探测,根权限获取,登陆安全攻击软件,以及发动攻击,这些动作的定义方式与 IPScan 类似.采用 FF 规划器生成了规划结果,对上文中提到的 DDOS 攻击规划问题进行实验,得出结论如图 6.

对于 DARPA 2000 中的 DDOS 攻击,能够识别出结果,如图 7.

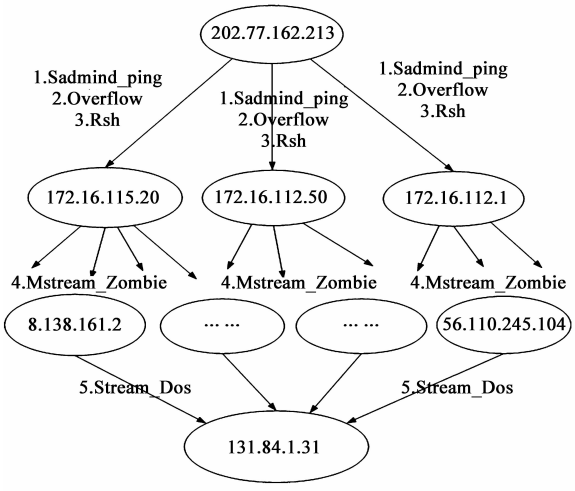

图4　DARPA2000中LLDOS1.0攻击过程

```
Step:
        0: IPSCAN Z ECHO RECEIVESATUS GOOD GOOD
        1: DETECTSERVICE Z A GOOD GOOD
        2: CONNECTSERVICE Z A GOOD TELNETSTATUS
        3: GETACCSESS Z A GOOD GOOD GOOD
        4: ATTRACK Z A GOOD GOOD
time spent:
    0.00 seconds instantiating 970 easy, 0 hard action templates
    0.00 seconds reachability analysis, yielding 43 facts and 970 actions
    0.00 seconds creating final representation with 42 relevant facts
    0.01 seconds building connectivity graph
    0.00 seconds searching, evaluating 6 states, to a max depth of 1
    0.01 seconds total time
```

图6　FF规划器识别结果

```
Define(domain DDosattrack)
(:requirement :strios :adl :universal -precondition :existential -precongdition
:condition-effects
                :equal)
(:types ICMPEcho Status HostAsset ServiceAsset)
(:constants (Good -Status ))
(:predicate (OpenInformation ?b -HostAsset)
              (KnowStatus ?b -HostAsset ?k -Status)
               (KnowService ?b -HostAsset ?k -serviceAsset)
               (Connect ?m -HostAsset ?n -HostAsset)
               (receivesatus ?z -Status)
               (send-to-icmpecho ? Echo -ICMPEcho)
                (sadmindpingStatus ?z -Status)
                (sadmindOverFlowStatus ?z -Status)
                (AccessRightStatus ?z -Status)
                (TelnetStatus ?z -Status)
                 (AttrackStatus ?z -Status)
(:action IPScan
        :parameters( ? Echo -ICMPEcho ?z -Status)
        :precondition(and(send-to-icmpecho ? Echo)(=(receivesatus ?z) Good))
        :effects(and(OpenInformation (?z)(=(sadmindpingStatus ?z) Good)))
)
```

图5　多步攻击规划域的描述样例

	ICMP_Reply	Ping_Sadmind	OverFlow_Target	Telnet	MS_Install	MM_Install	DDos_Attack
172.16.112.10	✓	✓	✓	✓	✓	✓	
172.16.112.50	✓	✓	✓	✓	✓	×	
172.16.112.100	✓	×	×	×	×	×	
172.16.112.105	✓	×	×	×	×	×	
172.16.112.194	✓	×	×	×	×	×	
172.16.113.50	✓	×	×	×	×	×	
172.16.113.105	✓	×	×	×	×	×	
172.16.113.148	✓	×	×	×	×	×	
172.16.115.20	✓	✓	✓	✓	✓	×	
172.16.115.87	✓	×	×	×	×	×	
131.84.1.31							✓

图7　识别结果

输出结果为对 DARPA2000 中 LLDOS 的五步攻击过程,给出了各个步骤的名称和状态,以及整个问题通过搜索算法计算时所耗费的时间.图 7 给出的是对于攻击类型的识别结果,可以看出此多步攻击由 3 条攻击路径组成,最终的攻击目标只有一个就是主机 131.84.1.31.对于其他机器的攻击,都是多步攻击的一部分,目标是最终的主机.由于 Mstream 工具的主控制端只需要在一个主机上安装就可以控制其他的服务器端,因此在 MM_Install 列只有 172.16.112.10 安装了.上述实验结果显示,本文提出的模型能够有效地描述多步攻击的规划问题,具有较好的可用性.

5 结束语

目前国内外现有的研究,在复杂网络入侵行为的分析识别方面有了大量工作,主要通过警报的关联这一角度进行.其中警报关联的前提是信息融合,而信息融合的前提是警报信息的规范化和描述.警报信息的规范化方面美国国防高级研究计划署(DARPA)和互联网工程任务组(IETF)等已经提出了相关的规范和标准;在警报信息描述方面,主要研究对象是对警报数据进行形式化表示.本文的研究针对的是多步入侵行为,通过知识表示进行知识层面的警报关联分析,提出一种基于知识表示的多步攻击规划问题描述模型,是将智能规划应用于入侵检测多步攻击领域的有效尝试,通过可行性验证证明了所提模型的可用性.下一阶段工作中,我们计划将研究小组规划域和规划问题描述的研究成果进行结合,以便于进一步开展基于动态规划的复杂网络入侵分析和识别的研究工作.

参考文献

[1] 国家互联网应急中心.中国互联网网络安全报告[DB/OL]. http://www.cert.org.cn/UserFiles/File/2010%20first%20half.pdf,2011-4-22.

[2] James P Anderson Company. Computer Security Threat Monitoring and Surveillance[R]. Fort Washington, Pennsylvania: James P Anderson Company,1980.

[3] Carla P Gomes. Artificial intelligence and operations research: challenges and opportunities in planning and scheduling[J]. The Knowledge Engineering Review,2000,15(1):1 – 10.

[4] R Davis,H Shrobe,P Szolovits. What is a knowledge representation[J]. AI Magazine,14(1):17 – 33,1993.

[5] 王珏,袁小红, 石纯一,郝继刚.关于知识表示的讨论[J].计算机学报,1995,18(3):212 – 224.

[6] 年志刚,梁式,麻芳兰,李尚平.知识表示方法研究与应用[J].计算机表示方法研究与应用,2007,24(5):234 – 236.

[7] Hornsby K, Egenhofer MJ. Indentity-based change: A foundation for spatio-temporal knowledge representation[J]. International Journal of Geographical Information Science, 2000, 14(3):207 – 224.

[8] Raskin RG, Pan MJ. Knowledge representation in the semantic web for earth and environmental terminology(SWEET)[J]. Computers & Geosciences,2005,31(9):1119 – 1125.

[9] 诸葛建伟,韩心慧,叶志远,邹维.基于扩展目标规划图的网络攻击规划识别算法[J].计算机学报,2006,29(8):1356 – 1366.

[10] Li X, Lara-Rosano F. Adaptive fuzzy petri nets for dynamic knowledge representation and inference[J]. Expert Systems with Applications,2000,19(3):235 – 241.

[11] Fikes RE, Nilsson N. STRIPS: A new approach to the application of therorem providing to problem solving[J]. Artificial Intelligence,1971,2(3-4):189 – 208.

[12] Blum AL, Furst ML. Fast planning through planning graph analysis[J]. Artificial Intelligence,1997,90(1-2):281 – 300.

[13] Marchetta, MG, Forradellas, RQ. An artificial intelligence planning approach to manufacturing feature recognition[J]. Computer-Aided Design,2010,42(3):248 – 256.

[14] von Mayrhauser A, France R, Scheetz M, Dahlman E. Generating test-cases from an object-oriented model with an artificial-intelligence planning system[J]. IEEE Transactions on Reliability,2000,49(1):26 – 36.

[15] 蒋志华,饶东宁,姜云飞,江洪.基于 AI Planning 的 Parlay X 电信业务设计[J].计算机学报,2011,34(2):304 – 317.

[16] 王桢珍,武小悦,刘忠.一种基于智能规划的信息安全风险过程建模方法[J].电子学报,2008,36(12A):76 – 80.
WANG Zhen-zhen, WU Xiao-yue, LIU Zhong. A planning-based method of risk process modeling for information security [J]. Acta Electronica Sinica, 2008, 36(12A): 76 – 80. (in Chinese)

[17] Fikes R E, N J Nilsson. STRIPS: A new approach to the application of theorem proving to problem solving[J]. Artificial Intelligence,1971,2(3-4):189 – 208.

[18] Fox M, Long D. PDDL2.1: An extension to PDDL for expressing temporal planning domians[J]. Journal of Artificial Intelligence Research,2003,20(SI):61 – 124.

[19] 努尔布力,柴胜,李红炜,胡亮.一种基于 Choquet 模糊积分的入侵检测警报关联方法[J].电子学报,2011,39(12):2741 – 2747.
Nurbol, CHAI Sheng, LI Hong-Wei, HU Liang. Intrusion detection alert correlation based on choquet fuzzy integral[J], Acta Electronica Sinica,2011,39(12):2741 – 2747. (in Chinese)

[20] 穆成坡,黄厚宽,田盛丰,林友芳,秦远辉.基于模糊综合评判的入侵检测报警信息处理[J].计算机研究与发展,2005,42(10):1679 – 1685.

[21] Benjamin Morin, Ludovic Mé, Hervé Debar, Mireille Ducassé. M2D2: a formal data model for IDS alert correlation

[A]. RAID'02 Proceedings of the 5th International Conference on Recent Advances in Intrusion Detection[C]. Berlin, Heidelberg: Springer-Verlag, 2002. 115 – 137.

[22] Alserhani Faeiz, Akhlaq Monis, Awan Irfan U. Mars: Multi-stage attack recognition system[A]. 24th IEEE International Conference on Advanced Information Networking and Applications[C]. Perth, Australia: IEEE Press, 2010. 753 – 759.

[23] Strayer WT, Jones CE, Schwartz BI, Mikkelson J, Livadas C. Architecture for multi-stage network attack traceback[A]. 30th Conference on Local Computer Networks [C]. Washington, DC, USA: IEEE Computer Society, 2005. 776 – 783.

[24] 何金山. 基于智能规划的多步攻击识别方法的研究[D]. 长春:吉林大学,2012.

[25] MIT 林肯实验室. DARPA Intrusion Detection Data Sets [EB/OL]. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html ,2012 – 04.

[26] 努尔布力. 基于数据挖掘的异常检测和多步入侵警报关联方法研究[D]. 长春:吉林大学,2010.

作者简介

努尔布力　男,1981 年出生,哈萨克族,新疆大学副教授,硕士生导师,兼院士科研助理,新疆大学校级创新团队"网络与多语种内容安全"带头人,自治区工业控制信息安全专家组成员. 2010 年获得吉林大学计算机科学与技术学院系统结构专业博士学位. 主要研究方向为网络安全和数据挖掘方法. 现主持国家自然基金 1 项,其他科研类项目 4 项. 曾获教育部高等学校科学研究科技进步奖一等奖,中国商业联合会科技进步奖一等奖,中国商业联合会科技创新奖一等奖等奖项和荣誉. 在国内外重要期刊和会议上发表学术论文 20 作篇,其中 SCI 检索两篇,EI 检索 10 余篇.

解男男(通信作者)　女,1987 年出生,在读博士生,2010 年于吉林大学软件学院获学士学位,同年攻读软件学院硕士研究生,于 2012 年推荐免试吉林大学计算机学院博士. 作为学生主要参与国家自然科学基金 1 项,主要研究方向为网络安全.

E-mail: jienn10@mails.jlu.edu.cn