doi:10.11887/j.cn.201401032 http://journal.nudt.edu.cn

一种可扩展的Cyber空间作战体系描述模型*

邓志宏,老松杨,白 亮,杨 征
(国防科技大学 信息系统与管理学院,湖南 长沙 410073)

摘 要:研究了Cyber空间作战体系模型构建技术,提出一种面向Cyber空间作战模拟的战争系统建模新思路,并以此为基础提出了Cyber空间作战体系一体化逻辑网络模型。将Cyber空间作战涉及到的敌我双方作战实体视为一个整体系统的组分,抽象为网络模型的实体节点,实体间的各种合作、协同、对抗等不同类型交互行为统一抽象为网络模型的逻辑边。针对网络模型的节点和边分别建立了基于本体的实体描述模型和基于OO-LAMBDA语言的行为描述模型。通过一个真实战例的仿真实验验证了本文提出的方法的有效性和正确性。

关键词:Cyber空间;Cyber空间作战体系;描述模型
中图分类号:E91 **文献标志码**:A **文章编号**:1001-2486(2014)01-0184-07

An extensible description model of cyber war system

DENG Zhihong, *LAO Songyang*, *BAI Liang*, *YANG Zheng*
(College of Information System and Management, National University of Defense Technology, Changsha 410073, China)

Abstract: The research is focused on the modeling technology of cyber war system. A new idea is proposed for cyber war simulation, based on which an integrated logical evolving network model of cyber war system is proposed. The model regards all of the entities which belong to different forces as components of a whole system, and represents them with verticals of the network, all kinds of interactive behaviors between distinct entities which include the cooperative behaviors, parallel behaviors and confrontational behaviors are represented with edges of the network uniformly. An entity description model based on ontology and a behavior description model based on OO-LAMBDA language are built to describe the verticals and the edges respectively. Finally, a simulation experiment is conducted by using a scenario of a real operation, the results of the experiment validate that our methods are validity and advantage.

Key words: Cyber space; Cyber war ystem; description model

Cyber空间和Cyber空间战是近几年新提出的概念,现已成为当前各军事强国发展和建设的热点之一[1-7]。战争的消耗性、破坏性、复杂性和不可重复性,使得基于实物和演习的研究方法不能为作战研究提供良好支持。作战模拟方法因其所具有的可重复性、易操作性和低成本的特点而成为作战研究的重要手段[8],对于Cyber空间作战研究也同样如此。作战模拟的主要思想就是通过建立一种现实作战系统的抽象表达,即对作战系统进行建模,利用模型对作战行为进行分析,从而达到认识、理解现实作战系统及其运行规律,并最终指导现实作战的目的。其中如何建立对现实作战系统的抽象表达,即作战系统模型的构建是作战模拟的基础工作,将直接决定作战模拟方法的正确性、有效性。

本文首先提出一种新的战争系统建模思路,其核心思想是将战争系统涉及的各方作战实体统一看作一个整体系统,从而使得以往多个系统间的交互行为转化为整体系统内部的系统演化行为。基于这种新的建模思路,本文提出Cyber空间作战体系一体化逻辑网络模型,并详细介绍了模型的两个主体部分,基于本体的实体描述模型和基于OO-LAMBDA语言的行为描述模型。

1 模型框架

Cyber空间战有着区别于传统动能作战的诸多特点,其中最主要的区别在于,传统单纯发生在物理域的动能作战是以直接能量输出达到毁伤敌对方作战平台为目标,而Cyber空间作战则是以争夺基于网络结构的信息运行控制权为目标,如

* **收稿日期**:2013-06-25
基金项目:国家自然科学基金资助项目(60902094)
作者简介:邓志宏(1986—),男,江西抚州人,博士研究生,E-mail:lingyu0207@gmail.com;
老松杨(通信作者),男,教授,博士,博士生导师,E-mail:songyanglao@sina.com

何模拟这种基于网络结构的信息运行控制行为是 Cyber 空间作战模拟的核心任务。传统作战模拟主要突出的是对战争进程中的交战过程以及毁伤结果的模拟,这种方式难以满足对 Cyber 空间作战体系网络演化特性的模拟,为此本文提出一种面向 Cyber 空间作战模拟的战争系统建模思路。如图 1 所示,将交战对抗双方看作一个整体系网络系统,网络系统的拓扑结构代表了实体间的交互行为,从而将交战过程转化为整体网络系统的演化过程。

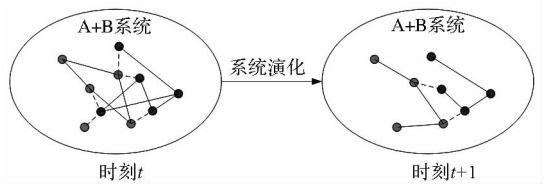


图 1　面向 Cyber 空间作战模拟的战争系统建模思路

Fig. 1　Idea for cyber war system modeling

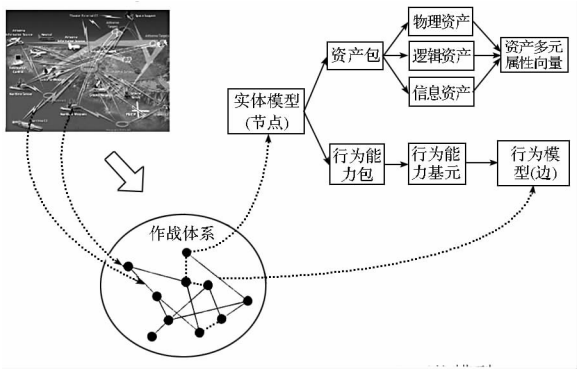


图 2　Cyber 空间作战体系一体化逻辑网络模型

Fig. 2　CWSILNM

基于图 1 建模思想,本文提出一种 Cyber 空间作战体系一体化逻辑网络模型(以下简称 CWSILN 模型)。如图 2 所示,其基本思想是构建一个整体的网络系统来描述 Cyber 空间作战体系,该网络系统的节点集表示包括敌我双方在内的作战实体,边集表示实体间的交互行为,这其中即包括与敌方节点的对抗行为,也包括各方内部的合作和协同行为,模型主体结构包括对实体节点描述的实体模型和对交互行为边描述的行为模型。

CWSILNM 模型一个主要特性是具有可扩展性,体现在以下两个方面:

(1)实体模型最核心的任务就是选取哪些特征描述实体状态,基于本体的实体描述模型可以灵活方便地管理实体资产概念空间,便于扩展。

(2)基于 OO-LAMBDA 语言的行为描述模型采用了面向对象的思想,Cyber 空间作战模拟中涉及的作战行为类型可以针对具体应用背景进行扩展。

2　基于本体的实体描述模型

节点表示的实体是战争中的行为主体在模型中的映射,是模型基本的、核心的组成元素。

定义 1　实体(Object)

$$O:=(ID,ASSet,BFSet)$$

其中,ID 为实体标识,*ASSet* 和 *BFSet* 分别表示实体资产包和实体行为能力包。实体资产包主要描述实体由什么构成,处于什么状态,是实体的物理结构划分。实体行为能力包主要描述实体具有哪些行为能力,是实体的逻辑功能划分。例如一架飞机按照物理结构划分得到其资产包包括机身、雷达、无线电、挂载武器等,对应的按照逻辑功能划分得到其行为能力包包括飞行能力、传感探测能力、通信能力、火力打击能力。

定义 2　实体资产包(Assets Set)

$$ASSet:=(PAS,LAS,IAS)$$

实体资产包包括三部分,实体物理资产包 *PAS*、实体逻辑资产包 *LAS* 和实体信息资产包 *IAS*。实体物理资产描述体现了 Cyber 空间中作战实体的物理存在基础,实体逻辑资产描述了节点与基于网络结构的信息运行过程相关的属性,实体信息资产是通过探测感知或接收其他节点传输的关于其他节点的信息集合,其中的元素可以视为对真实存在的节点的“仿制品”。

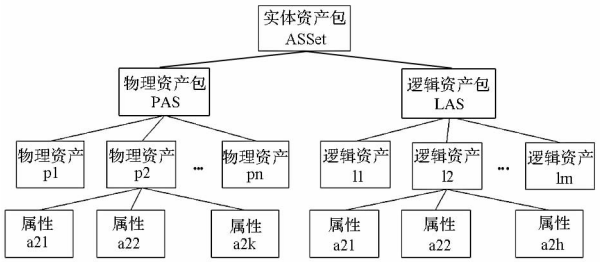


图 3　实体资产包树形结构

Fig. 3　Tree of entity assets

实体资产包中的物理资产包和逻辑资产包是一个树形结构。如图 3 所示,树形结构的叶子节点是具体的属性项,上层节点资产用其所有子资产属性集合表示。

针对 Cyber 空间模拟具体应用涉及的实体资产概念将会比较繁杂,很难一次就涵盖所有概念,因此模型中需要考虑扩展性,本文选用本体的方法对实体资产概念进行描述。

定义 3　实体资产概念领域本体

$$OASSet:=(C,T,R,A,\leqslant_C,\sigma_R,\sigma_A)$$

其中 C 表示资产概念集,T 表示资产概念取

值类型集，R 表示资产概念关系集，A 表示资产概念属性集。

$\leqslant_C$ 为概念集 C 上的偏序表示概念的层次结构，如果 $c_1 \leqslant_C c_2, c_1, c_2 \in C$，则称 c_1 是 c_2 的晚辈概念，c_2 是 c_1 的先辈概念，如果 $c_1 \leqslant_C c_2$ 且不存在 $c_1 \leqslant_C c_3 \leqslant_C c_2, c_3 \in C$，那么称 c_1 是 c_2 的子概念，c_2 是 c_1 的父概念，记为 $c_1 \prec c_2$；

$\sigma_R: R \rightarrow C^2$ 表示概念间的关系映射，描述概念集中概念对间存在关系 R。

映射 $\sigma_A: A \rightarrow C \times T$，用于属性的签名，即每一个属性明确属于哪个概念，该属性取值类型。图 4 所示为逻辑资产中描述主机系统的本体片段示例，其中，资产概念集 $C = \begin{Bmatrix} Host, IP, OS, Port, Protocol, \\ Service, Leak, LogicalWeapon \end{Bmatrix}$，资产概念取值类型集 $T = \{Integer, String\}$，资产概念关系集 $R = \begin{Bmatrix} has\_a, run\_on, use\_a, \\ install\_a, run\_a \end{Bmatrix}$，资产概念属性集 $A = \{name, id\}$，概念集上的偏序关系依次为图 4 中实心箭头方向，实心箭头上标签为资产概念关系，例如 $\sigma_R(run\_on) = (Service, Port)$，虚线箭头标签为概念属性签名，例如 $\sigma_A(host\_name) = (Host, String)$。

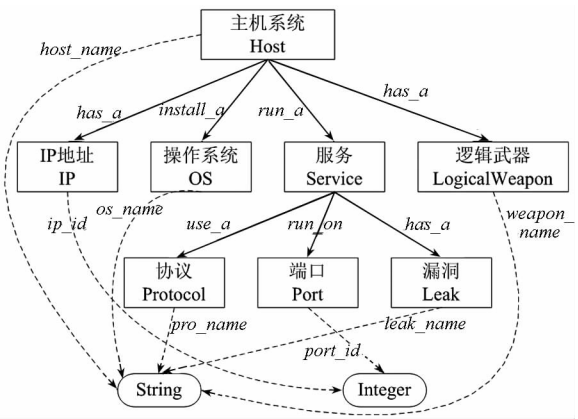


图 4 描述主机系统的本体片段

Fig. 4 Ontology of host

定义 4 实体行为能力包（Behavior Faculties Set）

$$BFSet \subseteq ABFSet$$

ABFSet 是指所有可能行为能力集，实体节点行为能力包是其子集，*ABFSet* 中的元素为行为能力基元，行为能力基元是行为模型中需要重点描述的。

3 基于 OO-LAMBDA 语言的行为描述模型

以往作战模拟一个难点就是对于不同类型的网络，如传感网、指控网、火力网，无法统一处理，因此只能单一以一种网络作为研究对象。但是这种人为将不同类型网络进行分割处理必然导致不同类型网络间的相互影响无法得到体现，而本文提出的 CWSILN 模型则能很好地解决这个问题。CWSILN 模型一个核心思想就是将不同类型的交互行为，如通信行为、指控行为、探测行为、对抗行为统一抽象为节点间的连边，交互行为的差别则通过描述连边的行为模型来体现。通过这种方式就能够从本质上解决异构网络的问题，这其中的关键就是如何合理描述不同类型的交互行为。本文借鉴网络信息安全领域用于网络攻击建模的一种形式化描述语言——LAMBDA 语言的基本思想[11]，提出一种基于面向对象思想的改进 LAMBDA 语言 OO-LAMBDA，用于 CWSILNM 模型中的行为描述。

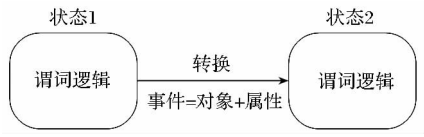


图 5 LAMBDA 语言基本思想

Fig. 5 LAMBDA language

LAMBDA 语言基本思想如图 5 所示，主要包括三部分：

第一部分为状态描述（State Description），用来描述攻击事件前提条件和后果，具体方式是采用谓词逻辑来描述与攻击事件相关的状态属性。

第二部分为连接事件（Combining Events），主要通过符号“&”来描述攻击事件涉及的多个步骤，可以看作子事件。

第三部分为转换描述（Transition Description），用来描述第二部分中涉及的各事件属性。

运用 LAMBDA 语言对一个完整攻击事件进行描述时往往包含了多个攻击步骤，也就是多个攻击行为的组合描述。这种方式在以指定攻击事件为描述对象时是合适的，但对于 Cyber 空间作战体系而言，由于涉及的实体及行为数量往往较多，如果对每个攻击事件都采用这种复合描述方式，必然会导致逻辑混乱。另外，LAMBDA 语言描述的是以攻击者为视角的指定攻击事件，不便于动态事件的扩展。针对这些问题，本文对 LAMBDA 语言进行改进，提出 OO-LAMBDA 语言。

首先给出两个关键定义。

定义 5 实体行为能力基元（Behavior Faculties）

$$BF := (O_I, O_P, f, \eta)$$

其中 O_I 是行为主体，是发起行为的实体节

点;O_P 是行为客体,是行为的作用对象节点;$f:O^2\rightarrow O^2$ 是行为的效用函数,用来描述行为将会对节点 O_I 和 O_P 产生何种影响;η 是行为的执行约束集,用来描述行为能力在满足哪些条件前提下才可能被执行。

定义 6　实体行为(Behavior)

$B:=(BF, BF\_Arg, OccurTime, DurationTime)$

行为是实体间发生的具体交互动作,是实体行为能力基元 *BF* 的实例化。行为能力基元实例化为行为时,需要相关的行为参数 *BF_Arg*。另外,行为具有时间属性,时间属性包括行为开始时间 *OccurTime* 和行为持续时间 *DurationTime*。

OO-LAMBDA 语言的基本思想如图 6 所示,采用面向对象的思想,建立行为能力基元类结构。以谓词逻辑描述的实体状态 1 作为行为能力基于实例化的判断依据。另外,指定实体状态中某些属性项作为行为能力基元实例化参数,最后实例化所得行为,依据行为能力基元中描述的行为效用函数(同样用谓词逻辑描述)以及实例化所用参数来改变目标实体状态。

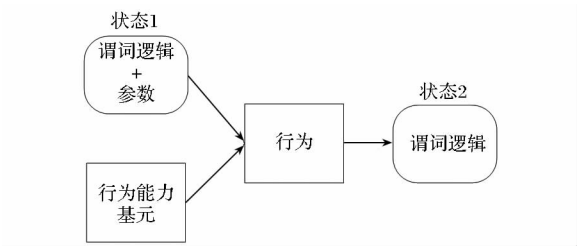


图 6　OO-LAMBDA 语言基本思想

Fig. 6　OO-LAMBDA language

BehaviorFaculty *BFNAME*
Args(O_I, O_P, *OccurTime*, *DurationTime*, *Arg*1, *Arg*2, …)
Pre:
Eff:

(a) 行为能力基元描述语法

BFNAME *Bname*
ArgValues:
$O_I = O_x$;
$O_P = O_y$;
OccurTime = *t*1
DurationTime = *dt*
…

(b) 行为描述语法

图 7　OO-LAMBDA 语言两种基本语法

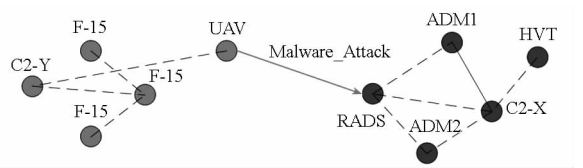
Fig. 7　Two basic grammar of OO-LAMBDA

OO-LAMBDA 语言包括两种语法,行为能力基元描述语法和行为描述语法,如图 7 所示。

行为能力基元描述语法中,BehaviorFaculty 为关键字,BFNAME 为行为能力基元名称,Args 为行为能力基元参数项,其中固有参数包括行为主体实体、行为客体实体、行为发生时间和行为持续时间,Pre 描述行为能力基元执行约束集,Eff 描述行为能力基元效用函数,Pre 和 Eff 均用谓词逻辑表示。

行为描述语法中,BFNAME 为行为对应的个体行为能力基元名称,BNAME 为具体行为名称标识,ArgValues 为行为能力基元参数项对应取值。

图 8 为一个简单的 OO-LAMBDA 语言运用示例,图中描述了红方一架隐形无人机 UAV 向蓝方防空雷达 RADS 进行蠕虫病毒攻击的行为,图 8(a)中的红色连边即表示该次病毒攻击行为,其对应的行为能力基元为图 8(b)中所示“病毒攻击”行为能力基元,其中描述了该行为的执行约束是攻击节点已经入侵了被攻击节点,行为的效用函数是使得被攻击节点感染攻击所使用的病毒。图 8(c)描述了该次具体攻击行为,其中指明了攻击节点为红方 UAV 节点,被攻击节点为蓝方



(a) 逻辑网络图

BehaviorFaculty *VIRUSATTACK*
Args(O_I, O_P, *OccurTime*, *DurationTime*, *VirusType*)
Pre:
InbreakTo(O_I, O_P)
Eff:
VirusInfect (*OP*, *VirusType*)

(b) “病毒攻击”行为能力基元描述

VIRUSATTACK *Worm _attack*
ArgValues:
$O_I = UAV$;
$OP = RADS$;
OccurTime = "10:03:46"
DurationTime = 2*s*
VirusType = "*Worm*"

(c) UAV 向 RADS 实施的“蠕虫病毒攻击”行为

图 8　OO-LAMBDA 语言描述示例

Fig. 8　An example of OO-LAMBDA

RADS 节点,攻击行为发生时间是“10:03:46”,攻击行为持续时间是 2s,攻击行为所使用的病毒类型为蠕虫病毒。

4　综合仿真实验验证

仿真程序包括两个主要部分:

首先是想定描述,运用本文方法对实验想定进行描述,包括对各实体的资产包和行为能力包进行描述。

其次是仿真运行,仿真运行包括实体资产属性更新和实体间行为生成,即更新 Cyber 空间作战体系网络节点属性并生成新的连边。节点属性更新以前一时刻网络拓扑结构为依据,对每条边(即行为)连接的两个实体节点按照行为的效用函数更新节点属性。新的连边生成则通过检查各节点行为能力的执行约束条件,如果实体资产属性满足其行为执行约束条件,则该行为能力实例化为可执行行为。如果一个节点有多个可执行行为,则需要按照某种行为选择机制选择其中某个行为作为下一时刻实体的待执行行为。节点行为选择机制不是本文研究重点,本文实验中采用最简单的行为队列方式,取队列中第一个行为作为待执行行为。

为了验证本文方法,以一个真实战例作为实验想定。2007 年 9 月 6 日,以色列空军使用“舒特”机载网络攻击系统,成功突防了叙利亚先进的第三代地空导弹武器系统,对叙境内纵深目标(事后叙方称该目标是一个“科学研究中心”,而一些西方国家官员认为是叙利亚化武库所在地)成功实施了突击,在进入和撤出过程中叙军毫无察觉。针对该战例制定的实验想定如图 9 所示。

图 9　实验想定

Fig. 9　Scenario for experiment

想定描述:以色列(*Y* 国)突袭叙利亚(*X* 国)高价值目标;

想定涉及作战实体:

- *Y* 国

指控节点 C2 - Y、一架搭载了“舒特”网络攻击系统的隐形无人机(UAV)、一个由 3 架 F - 15 战斗机组成的攻击编队;

- *X* 国

指控节点 C2 - X、由一部防空雷达(RADS)和两个地空导弹发射平台(ADM1、ADM2)组成的防空系统、高价值目标 HVT。

针对上述想定,本文设计了两个实验:

实验一:*Y* 国 UAV 未搭载“舒特”网络攻击系统,F - 15 编队直接突防对 *X* 国 HVT 实施打击;

实验二:*Y* 国 UAV 搭载“舒特”网络攻击系统,F - 15 编队在 *X* 国 RADS 被入侵之后对 HVT

```
Object UAV
    Physical_Assets:                          %物理资产
        Fuselage:                             %机身
            Arg1(type Int)(default 0)
            Arg2(type Int)(default 0)
            ...
        ...
    Logical_Assets:                           %逻辑资产
            HostName(type string)(default "")          %主机名
            IPAdress(type string)(default "")          %主机 IP 地址
            Service:                                   %主机运行的服务
                Sev_name(type string)(default "")      %服务名
                Sev_protocol(type string)(default "")  %服务使用的协议
                Sev_port(type int)(default 0)          %服务使用的端口
                Sev_leak:                              %服务的漏洞
                    Leak_id(type int)(default 0)       %漏洞编号
                    Leak_type(type string)(default "") %漏洞类型
            LogicalWeapons:                            %逻辑武器
                Weapon1(type Malware)(default virus)   %病毒
                Weapon2(type Malware)(default Trojan)  %木马
    Information_Assets                        %信息资产
            InforOFObject_RADS(                        %敌方防空雷达的信息
                Physical_Assets:...
                Logical_Assets:...
                Information_Assets:...)
            InforOFObject_HVT(                         %敌方指控节点的信息
                Physical_Assets:...
                Logical_Assets:...
                Information_Assets:...)
            ...
```

(a) UAV 实体资产包

```
Object UAV
    Behavior_Faculties_Set:                                          %行为能力包
        Fly:                                                         %飞行能力
            Effectiveness:
                Location = new_Location(Location, speed, direction, time)
            Precondition:
                Fuselage.status == normal
                Energy.status == normal
        Wireless_Inbreak(ObjTarget):                                 %无线入侵能力
            Effectiveness:
                Linkages.Add( new Linkage( ObjTarget.IPAdress,
                              ObjTarget.Sev_protocol, ObjTarget.Sev_port) )
            Precondition:
                ObjTarget.IPAdress != null
                ObjTarget.Sev_protocol != null
                ObjTarget.Sev_port != null
        Malware_Attack(ObjTarget, logical_weapon):                   %恶意程序攻击能力
            Effectiveness:
                Malware.Infect(ObjTarget, logical_weapon)
            Precondition:
                Linkages.ObjectLinkTo.IPAdress.Contain(ObjTarget.IPAdress) = True
                Authorities.Contain(ObjTarget.IPAdress, access) = True
        Information_Assets_Tamper(ObjTarget, ObjProtect):            %信息篡改能力
            Effectiveness:
                TamperInformation(ObjTarget.InforOFObjProtect)
            Precondition:
                Linkages.ObjectLinkTo.IPAdress.Contain(ObjTarget.IPAdress) = True
                Authorities.Contain(ObjTarget.IPAdress, root) = True
```

(b) UAV 实体行为能力包

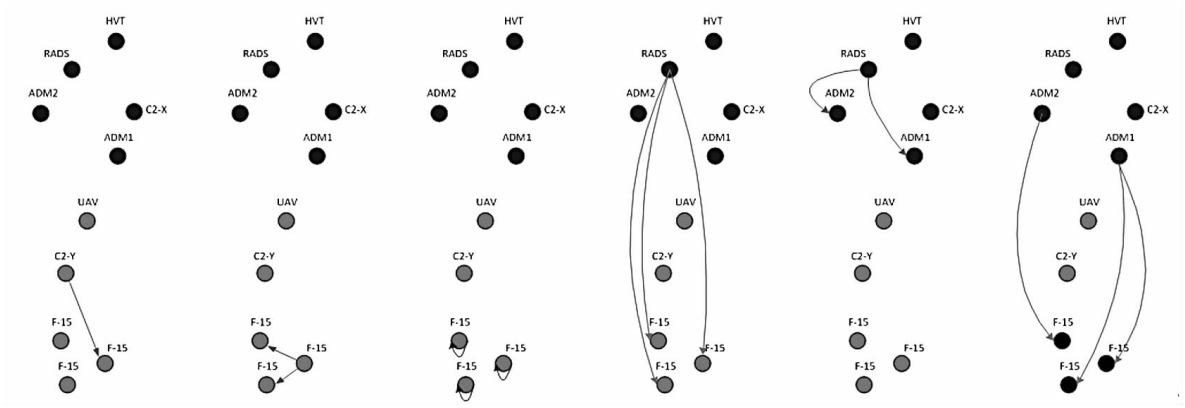
图 10　UAV 描述数据

Fig. 10　Description data of UAV

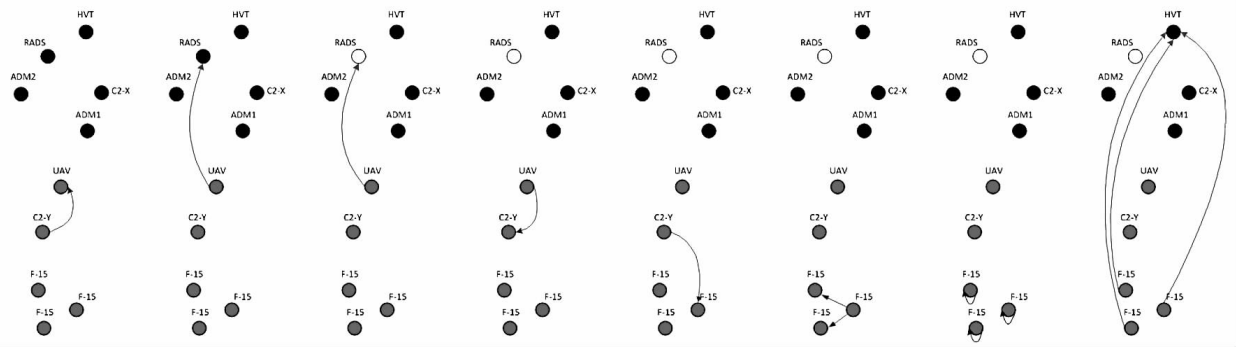
实施突袭。

实验一是一个传统空战的纵深突袭的想定,实验二则是涉及 Cyber 空间的作战行动,其中 UAV 搭载的“舒特”网络攻击系统代表了 Cyber 空间特有的作战能力。

实验以想定初始描述数据为输入(介于篇幅限制,图 10 仅列出了对 *Y* 国 UAV 节点的实体资产包和实体行为能力包的描述),以作战体系逻辑网络拓扑演化序列为输出(本质上就是交战过程的行为序列),图 11 显示了两个实验的实验结果。实验结果表明本文描述 Cyber 空间作战体系的方法,对于 Cyber 空间作战模拟能够起到支撑作用。



(a) 实验一



(b) 实验二

图 11　实验结果

Fig. 11　Experiment results

5　结论

作战模拟方法是 Cyber 空间作战研究的重要手段。Cyber 空间作战体系建模是 Cyber 空间作战模拟的基础工作,但目前已有的战争系统建模方法对于 Cyber 空间作战而言,都存在诸多缺陷,不能有效描述 Cyber 空间作战体系的相关特点。为此,本文首先提出一种新的战争系统建模思路,有别于以往将战争系统划分为多个对立系统的思想,该思想将战争系统涉及的各方实体都纳入到一个整体系统内,从而将对立节点间的对抗行为、己方节点内部的合作和协同行为都统一转化为整体系统内部的交互行为。基于这种思想,本文提出了一种可扩展的 Cyber 空间作战体系一体化逻辑网络模型,模型将 Cyber 空间作战体系抽象为一个一体化的逻辑网络。为了描述网络的节点和边,也即 Cyber 作战体系的实体和交互行为,分别建立了基于本体的实体描述模型和基于 OO-LAMBDA 语言的行为描述模型。本文所作工作为运用作战模拟方法研究 Cyber 空间作战奠定了良好基础。基于本文所提出的 Cyber 空间作战体系描述模型,针对作战体系的动态特性,通过研究系统演化行为来辅助作战人员认识、理解 Cyber 空间作战规律和掌控战争演变过程,以期望获得关于 Cyber 空间作战的规律性知识,并最终用于指导真实战争是本课题未来研究的主要方向。

参考文献(References)

[1] The White House. Cyberspace policy review assuring a trusted and resilient information and communications iInfrastructure[R]. Washington D. C,2009.

[2] Chairman of the Joint Chiefs of Staff. National military strategy for cyberspace operations (NMS－CO)[R]. Washington D C, 2006.

[3] Joint Publication 1－02, DoD Dictionary of Military Terms[R]. Washington D. C, Joint Doctrine Division, J－7, October

17, 2008.

[4] 胡晓峰,王艳正,司光亚. Cyberspace 的建模与仿真研究综述[J]. 中国电子科学研究院学报, 2011,6(3):226 – 229.
HU Xiaofeng, WANG Yanzheng, SI Guangya. Summarizing of research on modeling&simulation about cyberspace[J]. Journal of CAEIT, 2011,6(3): 226 – 229. (in Chinese)

[5] 仇建伟. 赛博空间作战研究[J]. 中国电子科学研究院学报, 2011,6(3):252 – 255.
QIU Jianwei. The research on the cyberspace operations[J]. Journal of CAEIT, 2011,6(3): 252 – 255. (in Chinese)

[6] 周光霞,孙欣. 赛博空间对抗[J]. 指挥信息系统与技术, 2012,2(3):6 – 10.
ZHOU Guangxia, SUN Xin. Study on cyberspace operations[J]. Command Information System and Technology, 2012,2(3): 6 – 10. (in Chinese)

[7] 余永林,王刚,赵炯,丁未. 赛博空间攻击关键技术体系研究[J]. 中国电子科学研究院学报, 2012,7(1):107 – 110.
YU Yonglin, WANG Gang, ZHAO Jiong, et al. Research on key technology architecture of cyberspace attack[J]. Journal of CAEIT, 2012,7(1): 107 – 110. (in Chinese)

[8] 李伯虎, 柴旭东, 朱文海, 等. 现代建模与仿真技术发展中的几个焦点[J]. 系统仿真学报, 2004, 16(9): 1871 – 1878.
LI Bohu, CHAI Xudong, ZHU Wenhai, et al. Some focusing points in development of modern modeling and simulation technology[J]. Journal of System Sirnulation, 2004, 16(9): 1871 – 1878. (in Chinese)

[9] 谭东风. 基于演化网络的体系对抗效能模型[J]. 国防科技大学学报, 2007,29(6):93 – 97.
TAN Dongfeng. An evolving network model for effectiveness of combat between SoSs[J]. Journal of National University of Defense Technology, 2007,29(6): 93 – 97. (in Chinese)

[10] 谭东风,鲍鲜鲲,胡定磊. 模拟体系对抗价值链的网络同步模型[J]. 国防科技大学学报, 2010,32(5):143 – 176.
TAN Dongfeng, BAO Xiankun, HU Dinglei. A model of network synchronization for value chain of combat of SoSs[J]. Journal of National University of Defense Technology, 2010, 32(5): 143 – 176. (in Chinese)

[11] Cuppens F, Ortalo R. LAMBDA: A language to model a database for detection of attacks[C]//Proceedings of Third International Workshop on Recent Advances in Intrusion Detection(RAID 2000), 2000:197 – 216.