

# MEISRDL 静态图模型的一致性检查方法

郝 斐<sup>1</sup>, 蒋 鑫<sup>2</sup>, 董庆超<sup>2</sup>, 张 杰<sup>3</sup>

(1. 北京军区总医院 信息科, 北京 100049;

2. 解放军理工大学 指挥自动化学院, 江苏 南京 210007;

3. 总装备部驻 318 厂军事代表室, 北京 100053)

**摘 要:**复杂系统需求描述语言(MEISRDL)是一种基于业务特征的信息系统需求描述语言。由于该语言是一种半形式化语言,无法进行基于精确语义的模型检验,模型中容易存在语义上的矛盾或冲突。为了解决该问题,文章提出一种 MEISRDL 静态图模型的一致性检查方法。该方法采用描述逻辑 SHOIN(D)描述 MEISRDL 静态图图元,实现半形式化的 MEISRDL 模型的形式化转换,通过模型映射算法可以有效推理判断模型语义矛盾。实例证明:该方法解决了 MEISRDL 静态图模型无法进行精确语义模型检验的问题,为复杂系统需求模型的语义一致性检查工作,提供了可靠的技术支持。

**关键词:**MEISRDL;一致性检查;描述逻辑;SHOIN(D)

中图分类号:E917;TP391.9

文献标识码:A

文章编号:1673-629X(2011)10-0028-04

## Consistency Model Checking for MEISRDL Static Diagrams

HAO Fei<sup>1</sup>, JIANG Xin<sup>2</sup>, DONG Qing-chao<sup>2</sup>, ZHANG Jie<sup>3</sup>

(1. Department of Information, General Hospital of Beijing Military Region, Beijing 100049, China;

2. Institute of Command Automation, PLA University of Science & Technology, Nanjing 210007, China;

3. Military Representative office of General Armament Department in 318 Factory, Beijing 100053, China)

**Abstract:** MEISRDL is a kind of requirements description language to capture the characteristics of SoS business. But in such a way of semi-formal description, don't make a model consistency detection based on exact semantics, and therefore there could be some semantic conflicts in the models. To solve the problem, it suggests a method for consistency detecting of models based on the MEISRDL static diagrams. This main idea is to transform the components of MEISRDL static diagrams into formal models by using description logic SHOIN(D). Consistency of the transformed models can be automatically detected by automated reasoning systems. The experiment shows that the method can solve the problem of the model integrity checking based on exact semantics and guarantee consistency of multi-view models.

**Key words:** MEISRDL; consistency detecting; description Logic; SHOIN(D)

## 0 引言

复杂系统需求描述语言(MEISRDL)<sup>[1-3]</sup>是在复杂系统研制过程中用于顶层需求获取和分析的核心语言。它采用半形式化的建模方式较为准确地描述复杂系统需求的各要素,以便系统用户能够清晰地表达其要求,系统开发方的系统分析师能够正确理解核心业务,把握用户的需求,保证开发出来的系统能够真正满足用户的需求。MEISRDL 由业务框架描述(BFD)、技

术框架描述(TFD)和功能操作描述(FOD)三个方面的需求建模组成,这三个部分互为补充,分别从业务、技术和功能操作三个方面描述一个复杂系统的各种需求特征,为研发人员建立一个完整的需求概念。该语言不需要系统用户具备形式化的背景知识,它采用可视化的建模风格,直观地描述了系统用户的需求,为系统用户同系统分析师共同理解需求,提供了一个公共的平台。但是大型的系统模型中容易存在语义上的矛盾或者冲突,由于 MEISRDL 模型缺少形式化语义,无法进行基于精确语义的推理和验证,从而使模型中可能会存在一致性问题。

描述逻辑是目前语义 Web 领域的研究热点,并且为软件工程、系统工程、知识工程等相关领域广泛采用。描述逻辑最大的特点是一方面解决了知识表示的问题,另一个方面可以实现知识的推理和演绎。目前

收稿日期:2011-03-22;修回日期:2011-06-25

基金项目:国防预研基金项目(9140A06020206JB8101);"十一五"装备预先研究项目(513060102);国家高技术研究发展计划(863 计划)(2007AA01Z126)

作者简介:郝 斐(1981-),男,山西原平人,助理工程师,CCF 会员,主要研究方向为指挥自动化理论。

描述逻辑已经派生了众多的子集,如 ALC、SHIN、SHOIN(D)等。这些子集的主要区别在于表达能力的强弱,鉴于文中应用环境的需要,选用描述逻辑 SHOIN(D)子系统实现需求的推理和论证。

为了解决 MEISRDL 静态模型语义一致性推理验证问题,文中参考国内外有关描述逻辑发展和应用的一些较新成果<sup>[4~8]</sup>,深入分析 MEISRDL 模型元素与描述逻辑系统构造子之间的语义映射联系,采用描述逻辑 SHOIN(D)描述 MEISRDL 静态图图元元素,实现 MEISRDL 静态图模型的形式化描述,并借助目前语义 Web 领域流行的自动推理机 Racer,实现模型自动的推理与验证。

## 1 静态图元的描述逻辑转换方法

MEISRDL 的静态图由情景分析用例模型、业务结果模型、业务角色模型、业务职能模型和业务资源模型组成。这些模型从系统功能、系统组成、作战结果等不同视角,全面地刻画了待建系统的静态特征。文献[1~3]详细介绍了上述模型的图元语义,本节主要介绍模型图元基于 SHOIN(D)的映射规则。

### 1.1 概念

MEISRDL 中的概念包括业务、系统、机构、人员、职能、结果和资源。这些抽象概念描述了组成复杂系统的不同要素,不同概念的实例集合之间不存在相交关系。这些概念与 SHOIN(D)的原子概念 concept 具有良好的对应关系,MEISRDL 中的概念在 SHOIN(D)中可以用原子概念描述。以假想的前沿区域防空系统目标发现与跟踪模型为例(如图 1 所示),应当添加以

下 SHOIN(D)概念:WarningRadarStation、WarningRadarSystem、TrackingRadarSystem、MissileLaunchingSystem、RadarAim、WarningRadar、RadarTransmitter。

### 1.2 一般关联关系 Binary association

MEISRDL 中一般关联关系借鉴于 UML 二元关联关系的语义。以图 1 为例,警戒雷达站与警戒雷达系统之间的操纵关系在 SHOIN(D)中描述为:

$\text{WarningRadarStation} \subseteq \forall \text{Control. AlertRadarSystem}$

其中警戒雷达站、警戒雷达系统分别用原子概念 WarningRadarStation、WarningRadarSystem 描述。操纵关系用原子关系 Control 描述,Control 的定义域是概念 WarningRadarStation,值域是概念 WarningRadarSystem。

关联双方的重数约束描述为:

$\text{WarningRadarStation} \subseteq \forall \text{Control. WarningRadarSystem} \cap (\geq \min \text{Control}) \cap (\leq \max \text{Control})$

$\text{WarningRadarStation} \subseteq \forall \text{Control}^-. \text{WarningRadarStation} \cap (\geq \min \text{Control}^-) \cap (\leq \max \text{Control}^-)$

(其中  $\text{Control}^-$  是 Control 的逆关系)

上述表达式的语义为:在有向一般关联关系 Control 中,定义域概念 AlertRadarStation 实例的重数大于最小值 min,小于最大值 max;值域概念 WarningRadarSystem 实例的重数大于最小值 min,小于最大值 max。

### 1.3 概括关系 Generalization

在 MEISRDL 中概括是一种继承关系,它是指两个模型元素之间存在一种抽象和具体的关系。概括使子概念可以继承父概念的全部公共特征,并且允许子概念拥有自己区别于父概念的个性存在。以假想的前沿

区域防空系统一雷达系统模型为例,预警雷达系统、跟踪雷达系统与雷达系统之间的概括关系在 SHOIN(D)中描述为:

$\text{WarningRadarStation} \subseteq \text{RadarSystem}$   
 $\text{TrackingRadarStation} \subseteq \text{RadarSystem}$

其中子概念预警雷达系统、跟踪雷达系统分别用原子概念 WarningRadarSystem、TrackingRadarSystem 描述,父概念雷达系

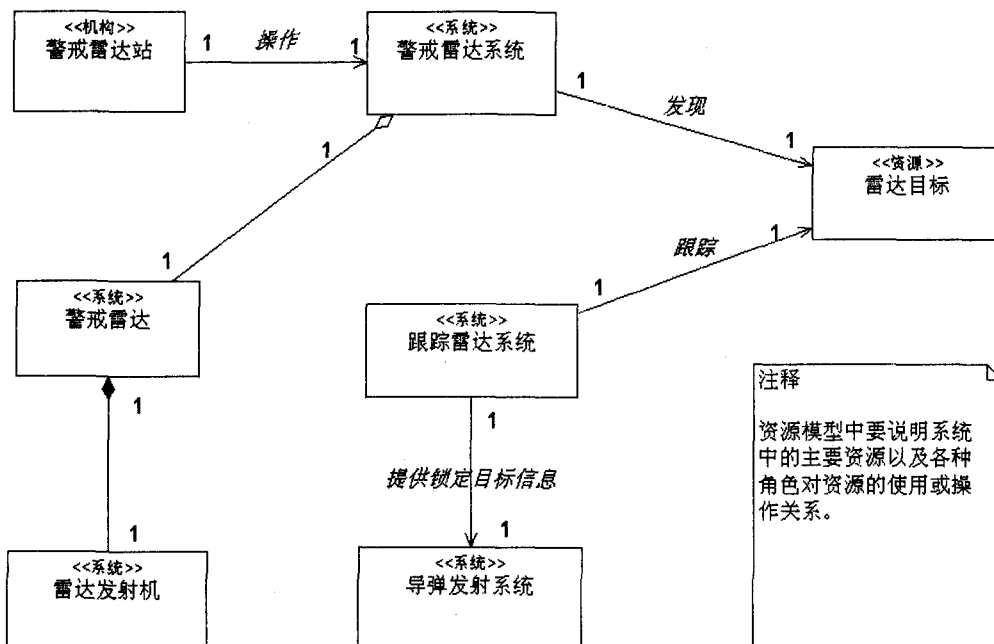


图 1 目标发现与跟踪模型

统用原子概念 RadarSystem 描述。

#### 1.4 弱聚合关系 Aggregation

在 MEISRDL 中弱聚合关系描述了一种不同概念之间存在的整体与成员之间的关系。MEISRDL 约定在弱聚合关系中,一个成员实例可以同时聚合于多个整体实例中,并且整体实例和成员实例都可以脱离对方而独立存在。以假想的前沿区域防空系统业务职能模型为例,导弹攻击功能与前沿区域防空系统之间的弱聚合关系在 SHOIN(D) 中描述为:

$$FAAD \subseteq \forall A. \text{MissileAttack} \cap (=1A)$$

$$\text{MissileAttack} \subseteq \forall A. FAAD$$

其中整体部分前沿区域防空系统编码为原子概念 FAAD,成员部分导弹攻击功能编码为原子概念 MissileAttack,前沿区域防空系统与导弹攻击功能之间的弱聚合关系编码为原子关系 A, A 的定义域是原子概念 FAAD,值域是原子概念 MissileAttack, SHOIN(D) 表达式的语义是:一个整体 FAAD 实例强聚合一个成员 MissileAttack 实例;一个 MissileAttack 实例可以同时聚合于多个整体 FAAD 实例之中,并且成员实例能够脱离整体实例而独立存在。该语义满足 MEISRDL 对弱聚合的约束要求。

#### 1.5 强聚合关系 Composition

在 MEISRDL 中强聚合关系描述了一种较弱聚合关系更加强的整体-成员关系。MEISRDL 约定在强聚合关系中,一个成员实例仅能聚合于唯一的整体实例中,并且成员实例不能够脱离整体实例而独立存在。以雷达与雷达发射机之间的强聚合关系为例,该强聚合关系在 SHOIN(D) 中描述为:

$$\text{Radar} \subseteq \forall \text{Agg}. \text{RadarTransmitter} \cap (=1\text{Agg})$$

$$\text{RadarTransmitter} \subseteq \forall \text{Agg}. \text{Radar} \cap (=1\text{Agg})$$

其中整体部分雷达编码为原子概念 Radar,成员部分雷达发射机编码为原子概念 RadarTransmitter,雷达与雷达发射机之间的强聚合关系编码为原子关系 Agg, Agg 的定义域是原子概念 Radar,值域是原子概念 RadarTransmitter, SHOIN(D) 表达式的语义是:一个整体 Radar 实例强聚合一个成员 RadarTransmitter 实例;一个成员 RadarTransmitter 实例只能聚合在唯一的整体 Radar 实例中,并且任何 RadarTransmitter 实例都不能够脱离 Radar 实例而独立存在。

#### 1.6 约束条件

不相交约束在 SHOIN(D) 中描述为:

$$C_i \subseteq \cap_{j=i+1}^n C_j \quad 1 \leq i \leq n-1$$

SHOIN(D) 表达式的语义为:任何不相交的概念之间,它们的实例集合交集为空。

覆盖约束在 SHOIN(D) 中描述为:

$$C \subseteq \cup_{i=1}^n C_i$$

SHOIN(D) 表达式的语义为:概念 C 是一系列相关概念集合并集的子集。

借助上述映射转换算法,可以将 MEISRDL 模型转换为相应的描述逻辑本体,进而借助 Racer 引擎,推理判断本体中各个概念之间的包容、蕴涵、冗余关系。

## 2 方法可以解决的几类不一致性问题

文献[9]区分定义了三种本体一致性问题,即结构一致性、逻辑一致性和用户自定义一致性。

结构一致性是指本体遵守本体语言语法。

逻辑一致性是指本体内部语义逻辑不冲突,不矛盾。

用户自定义一致性指本体满足用户根据应用环境需要,而预先定义的一些一致性条件。

文中介绍的模型映射规则遵守了 SHOIN(D) 语法,因此模型映射变换后不存在结构一致性问题;同时,所讨论的 MEISRDL 模型是一种环境无关模型,因此用户自定义一致性问题也可以忽略。这里重点分析模型的逻辑一致性问题。文献[4,10]指出对于逻辑一致性,Tableaux 算法可以解决以下问题:

本体逻辑一致性:要求本体是可以满足的,不含矛盾信息。

概念的一致性:要求本体中的任意概念不是空集。

概念的包容关系:概念间的包容是一种抽象与继承关系,与面向对象中的继承关系语义一致。

概念等价关系:概念间的等价说明概念之间存在相同的实例集合,即两个概念完全相同。

隐含的不一致性:概念之间存在关联,在实例层,概念的实例可能会违反关联中基数数量的约束。

在推理过程中,上述五种一致性问题都可以转化成概念可满足问题<sup>[4]</sup>。推理引擎执行 Tableaux 算法判断概念的可满足性,该算法通过一系列的扩展规则,试图构建本体的一棵 Tableaux 树,即本体的一个可满足解释。如果无法构建 Tableaux 树,则说明概念不可满足,本体含有语义矛盾。扩展规则主要包括:

(1)  $\cap$  规则。

$S \rightarrow \{x:C_1, x:C_2\} \cup S$ , 如果  $x:C_1 \cap C_2$  属于  $S$ , 且  $x:C_1$  和  $x:C_2$  不属于  $S$ ;

(2)  $\cup$  规则。

$S \rightarrow \{x:D\} \cup S$ , 如果  $x:C_1 \cup C_2$  属于  $S$ ,  $x:C_1$  和  $x:C_2$  不属于  $S$ , 且  $D = C_1$  或者  $D = C_2$ ;

(3)  $\exists$  规则。

$S \rightarrow \{x:P_1y, \dots, sP_ky, y:C\} \cup S$ , 如果  $x:\exists R.C$  属于  $S$ ,  $R = P_1 \cap \dots \cap P_k$ , 没有  $z$  使得  $xRz$  属于  $S$ , 且  $z:C$  属于  $S$ ,  $y$  为一个新变量。

(4)  $\forall$  规则。

$S \rightarrow \{y: C\} \cup S$ , 若  $x: \exists R. C$  属于  $S$ ,  $xRy$  属于  $S$ , 且  $y: C$  不属于  $S$ 。

下面举例说明算法过程:

假设 TBox 中公理集包括:  $\{C \subseteq B, B \subseteq R. D, D \subseteq E, E \subseteq A \cap F, F \subseteq \neg A\}$ , 判断概念  $C$  的可满足性过程如下:

- (1)  $a: \{C\}$ ;
- (2)  $a: \{C, B\}$ ;
- (3)  $a: \{C, B, \exists R. D\}$ ;
- (4) 利用  $\exists$  规则得出  $R(a, b), b: \{D\}$ ;
- (5)  $b: \{D, E\}$ ;
- (6)  $b: \{D, E, A \cap F\}$ ;
- (7) 利用  $\cap$  规则得  $b: \{D, E, A \cap F, A, F\}$ ;
- (8)  $b: \{D, E, A \cap F, A, F, \neg A\}$ 。

此时发现集合中同时包含  $A$  与  $\neg A$ , 发现冲突, 即概念  $C$  不可满足。需要说明的是上述推理步骤虽然复杂, 但是 Racer 推理引擎完全支持推理算法的自动执行并返回推理判断结果。

### 3 模型一致性检查实例

本节采用一个雷达组成模型验证案例(见图 2), 分析论证本方法的现实可行性。前沿防空系统 FAAD 是一个人机交互系统, 装备于防空旅, 用于前沿阵地或中心城市等重点保护对象的低空防御。雷达组成模型描述了各种雷达之间的继承关系及其内部组成结构。

首先通过模型映射算法获取需求本体:

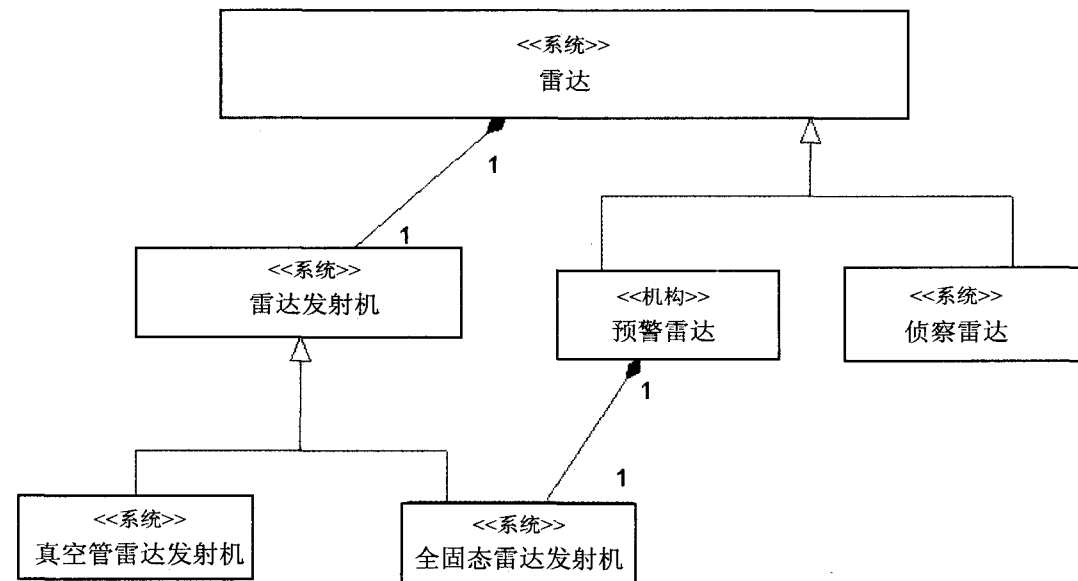


图 2 雷达组成模型

$\text{WarningRadar} \subseteq \text{Radar}$

$\text{TrackingRadar} \subseteq \text{Radar}$

$\text{SolidRadarTransmitter} \subseteq \text{RadarTransmitter}$

$\text{VaccumTubeRadarTransmitter} \subseteq \text{RadarTransmitter}$

$\text{Radar} \subseteq \forall \text{Composition. RadarTransmitter} \cap (= 1 \text{Composition})$

$\text{RadarTransmitter} \subseteq \forall \text{Composition} - 1. \text{Radar} \cap (= 1 \text{Composition} - 1)$

$\text{WarningRadar} \subseteq \forall \text{Composition. SolidRadarTransmitter} \cap (= 1 \text{Composition})$

$\text{SolidRadarTransmitter} \subseteq \forall \text{Composition} - 1. \text{WarningRadar} \cap (= 1 \text{Composition} - 1)$

假设在需求获取阶段, 系统分析师忽略了雷达概念与预警雷达概念之间的继承关系。由此, 可以发现模型错误地将雷达发射机同时建模为雷达和预警雷达概念的成员概念, 此时模型含有隐含不一致性问题。为了便于直观理解, 采用本体编辑工具 Protégé 加载上述本体, 并借助 Racer 推理引擎的推理服务, 获取的需求本体推理结果与预期结果一致。测试结果也表明这种基于描述逻辑推理的 MEISRDL 模型验证方法, 可以将系统分析师从繁杂的模型手工检测中脱离出来, 使得复杂系统的需求模型质量得到可靠保证。

### 4 结束语

文中采用描述逻辑 SHOIN(D) 描述 MEISRDL 静态图图元, 确定了模型由 MEISRDL 到 SHOIN(D) 的映射规则, 借助该规则可以实现 MEISRDL 静态图模型的形式化描述, 为 MEISRDL 静态图模型赋予形式化语义, 同时借助自动推理引擎提供的逻辑推理服务, 该方法解决了 MEISRDL 模型由于缺乏形式化语义, 而无法

进行精确语义检查的问题。

下一步将结合文献 [11~13] 的主要思想, 将领域特定规则推理技术与本方法结合起来, 进一步验证复杂系统需求模型的合理性和完整性问题。

### 参考文献:

- [1] 王智学. 一种业务概念模型驱动的需求分析与获取方法

(下转第 35 页)

层测试板卡的1、2端口进行数据的接收与转发仿真测试。图中椭圆标志的区域中,从上往下,1、2端口的第一、二、四层指示灯为绿色,说明1、2端口上不仅物理连接UP,而且两端口间相互转发的数据流都能正常接收,测试结果即表示两端点发送的数据流均能通过TPE间的MS-PW转发给对端,实现了该MS-PW类型多段PW的组网方式。

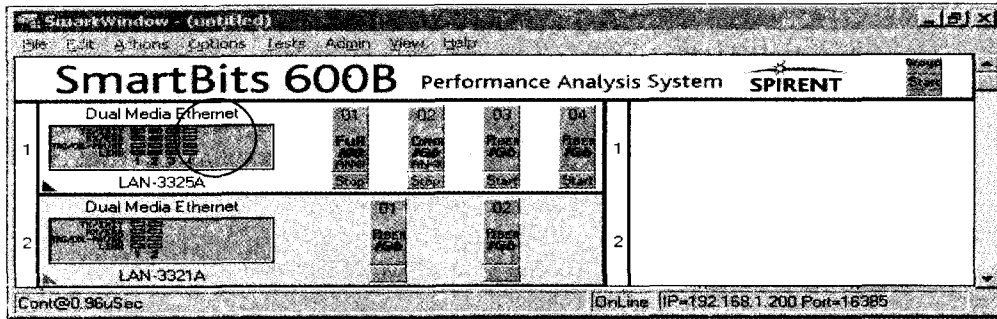


图4 SmartBits的数据转发图

### 3 结束语

通过各种类型多段PW的仿真测试结果的分析可知,对多段PW的组网方式的实现是正确、可行的。多段PW的实现不仅可以灵活组网,而且可以降低庞大网络组网的复杂度,提高PSN网络的安全性<sup>[12]</sup>。但目前多段PW技术并未形成国际通用的RFC协议文档,因此今后还得注意多段实现的技术向正式的协议靠近。

#### 参考文献:

- [1] Xiao Xipeng, Hannan A, Bailey B, et al. Traffic engineering with MPLS in the Internet[J]. IEEE Network, 2000, 14(2): 28-33.
- [2] 曹玉群. 多段伪线路技术[J]. 通信技术, 2010(10): 92-94.
- [3] Rasiah P, Chung Jong-Moon. Traffic engineering optimal routing for LSP setup in MPLS[C]//Midwest Symposium on Circuits and Systems. [s. l.]: [s. n.], 2002: 272-275.
- [4] Zhang R, Bartell M. BGP设计与实现[M]. 北京:人民邮电出版社, 2005.
- [5] O'Shea D. Pseudo wire, real bridge [J]. Telephony, 2005, 246(2): 24-25.
- [6] 蔡芸芸. 基于MPLS网络的PWE3实现研究[D]. 南京:南京航空航天大学, 2008.
- [7] 宋庆, 刘彦明, 朱永升. MPLS技术的研究[J]. 电子科技, 2007(2): 76-82.
- [8] 方圆. IP/MPLS流量标识与业务质量控制[J]. 数据通信, 2009(1): 40-45.
- [9] 李缓, 安宁. MPLS VPN的关键技术及其应用[J]. 科技信息, 2008(35): 497-604.
- [10] 傅德胜, 肖洁岑. MPLS VPN的实现机制及其配置[J]. 南京信息工程大学学报(自然科学版), 2010(6): 567-572.
- [11] Palmieri F, Fiore U. Securing the MPLS control plane[J]. Lecture Notes in Computer Science, 2005, 3726: 511-523.
- [12] 陈业芳. MPLS技术及发展前景分析[C]//海南省通信学会学术年会论文集. 出版地不详: 出版者不详, 2006.

(上接第31页)

- [1]. 军事运筹与系统工程, 2006, 20(1): 18-22.
- [2] 王聪. 军事综合电子信息系统需求建模方法研究[D]. 南京: 解放军理工大学, 2004.
- [3] 李宗勇, 王智学. 面向业务概念框架的可视化需求获取与建模工具[C]//中国电子学会电子系统工程分会第十三届信息化理论学术研讨会. 安徽, 黄山: 出版者不详, 2006: 268-271.
- [4] 陆建江. 语义网原理与技术[M]. 北京: 科学出版社, 2007.
- [5] Na Hong-Seok, Choi O-Hoon, Lim Jung-Eun. A Method for Building Domain Ontologies Based on the Transformation of UML Models[C]//SERA2006. New York: IEEE, 2006: 332-338.
- [6] Na Hong-Seok, Choi O-Hoon, Lim Jung-Eun. A Metamodel-Based Approach for Extracting Ontological Semantics from UML Models [C]//WISE 2006. Chongqing: Computer Science, 2006: 411-422.
- [7] van der Straeten R. Inconsistency Management in Model-Driven Engineering - An Approach Using Description Logics [D]. Brussel: Vrije Universiteit Brussel, 2005.
- [8] Berardi D, Calvanese D, Giacomo G D. Reasoning on UML class diagrams [J]. Artificial Intelligence, 2005, 168: 70-118.
- [9] Peter H, Ljiljana S. Consistent Evolution of OWL Ontologies [C]//Proceedings of ESWC 2005. Heraklion: [s. n.], 2005: 182-197.
- [10] Horrocks I, Sattler U. A tableau decision procedure for SHOIQ [J]. Journal of Automated Reasoning, 2007, 39(3): 249-276.
- [11] 董庆超, 王智学, 张爱辉, 等. 基于UML类图模型的一致性检查方法[J]. 计算机技术与发展, 2008, 18(10): 85-89.
- [12] 王智学, 董庆超, 陈彬, 等. 基于UML模型的C4ISR系统能力需求分析与验证[J]. 系统工程与电子技术, 2009, 31(9): 2167-2171.
- [13] 张爱辉, 王智学, 李宗勇. 基于领域知识的模型检验方法[J]. 系统工程与电子技术, 2008, 30(8): 1561-1565.