2021-2022学年春季学期

网络空间安全态势感知

Cyber security situation awareness

授课团队：刘宝旭 卢志刚 刘玉岭

助　　教：李　宁

网络空间安全态势感知

Cyber security situation awareness

[第6次课] 语义与本体表示技术

授课教师：刘玉岭

授课时间：2022.3.10

内容概要

互联网的发展过程

- **第一代互联网**（Web 1.0）
  - 通过超链接把资源联系在一起
  - 以HTML 、URL 和HTTP 等技术为标志，以静态页面的形式来展现信息
- **第二代互联网**（Web 2.0）
  - 动态的、允许用户与应用程序交互，动态的生成返回页面。
  - 以动态HTML 语言、Javascript、Ajax、JQuery、PHP、C#等技术为标志
- **第三代互联网**（Web 3.0）
  - 一个组成部分：语义网(Semantic Web)

现有的Web存在的问题

- Web信息在内容上不容易自动关联
- Web信息在内容上不容易自动理解
- 传统的Web 侧重信息的定位与展示，并不侧重内容的理解

语义网的目标

- 当前“机器可阅读”的万维网扩展为“机器可理解”的语义网

- 语义网（Semantic Web）
  - 万维网联盟的Tim Berners-Lee在1998年提出
  - Tim Berners-Lee：互联网之父、HTTP和HTML的发明人
  - 通过给万维网上的文档（如: HTML）加能够被计算机所理解的语义（Meta data），使整个互联网成为一个通用的信息交换媒介
  - W3C的提法：The Semantic Web provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries

设计目标：机器可自动处理
机器可理解

语义网络概念与内涵

- 基本概念

  语义网络是通过概念及其语义关系来表达知识的一种网络图,是一种“带标识”的有向图.

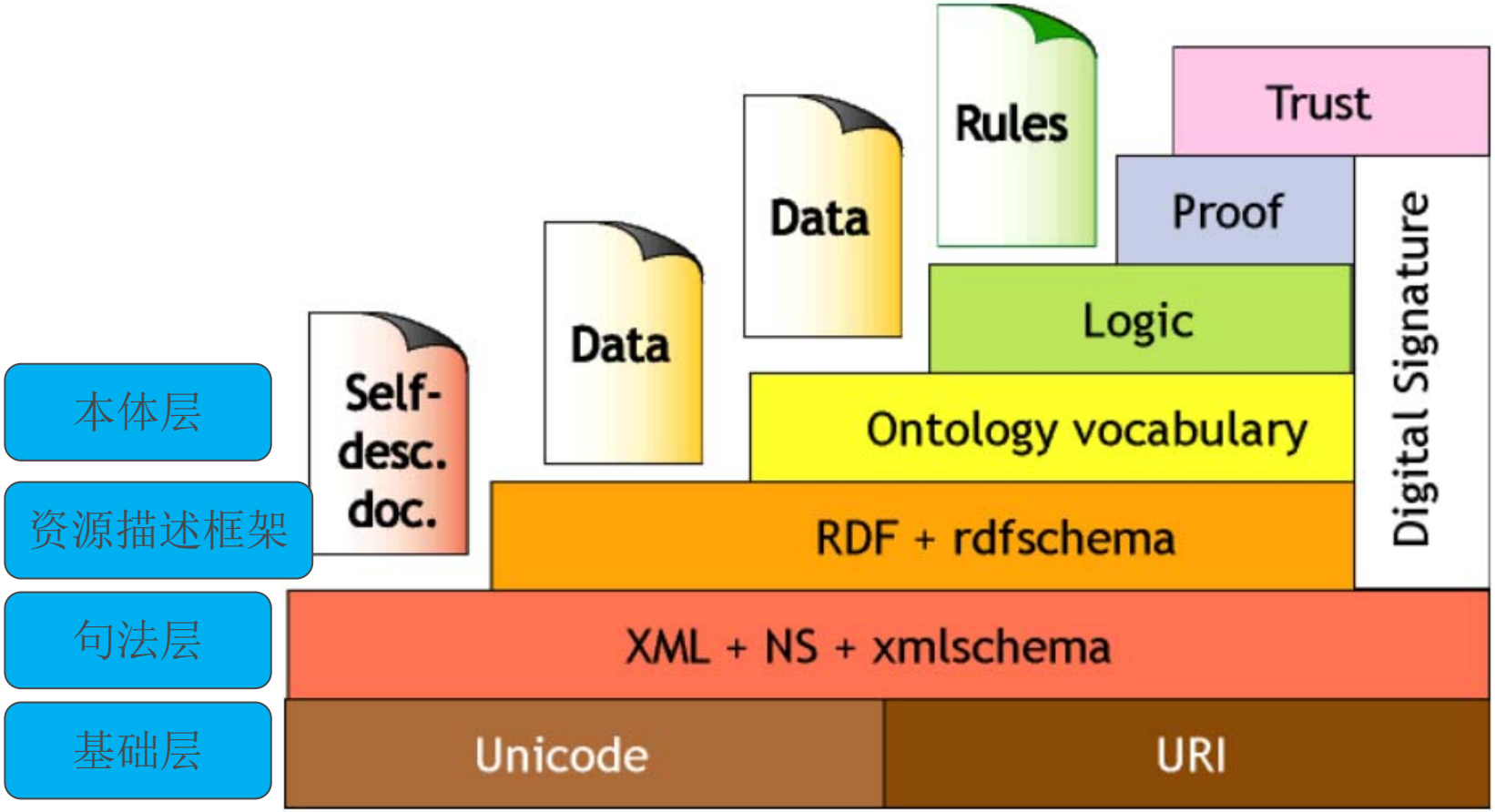
  节点表示各种事物,概念,情况,属性,动作,状态等.弧表示各种语义关系

  (节点1，弧，节点2)

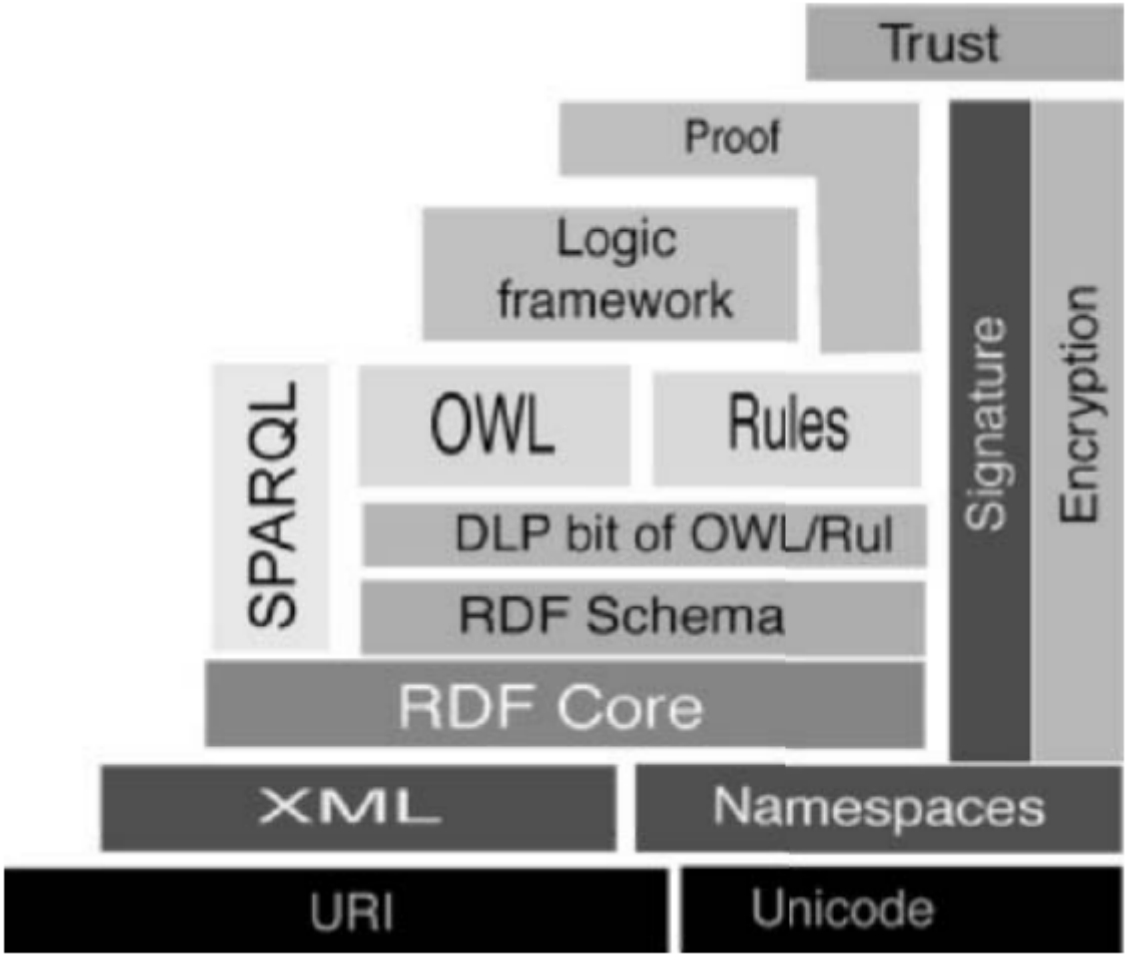
  也可表示为:

  当把多个基本的网络通过相应的语义关联在一起时,就得到一个语义网络

- 语义网体系结构
- Berners-Lee最初提出，Berners-Lee.Semanticweb-XML2000

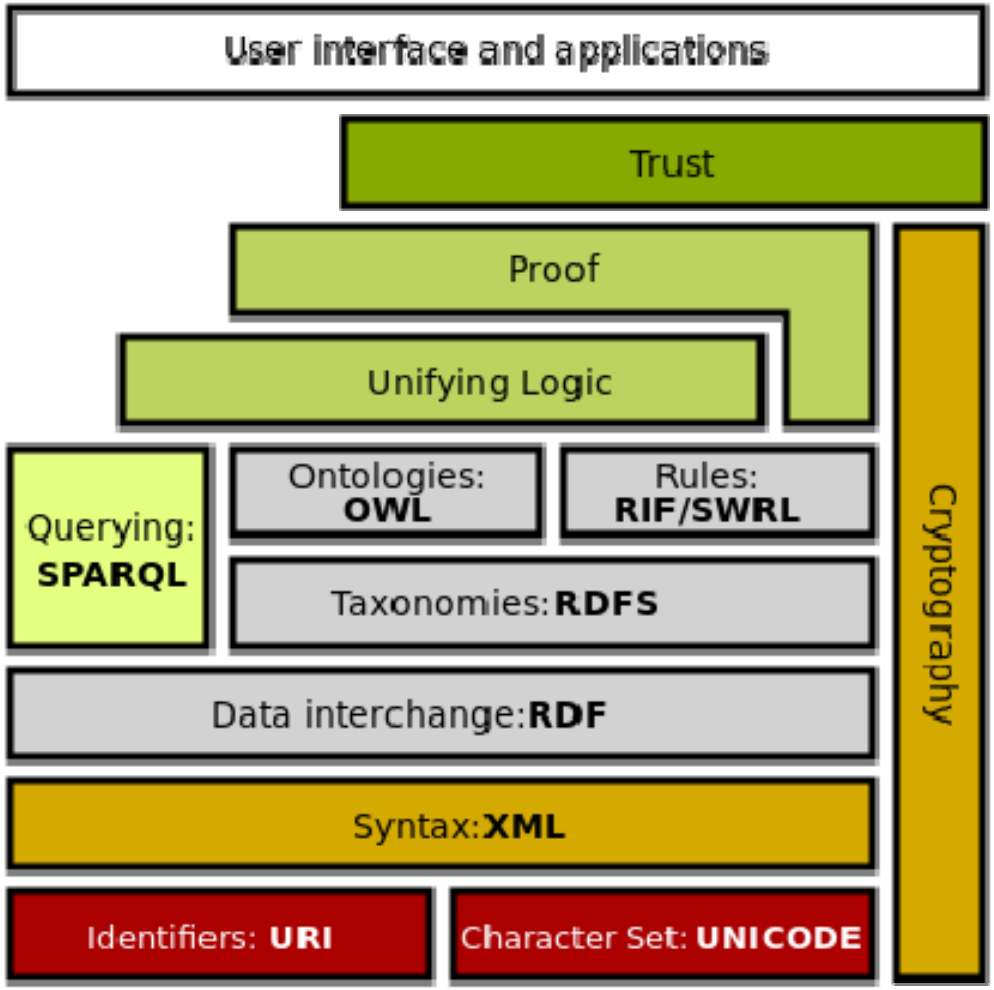


Grigoris Antoniou等提出的另一类体系结构



A Semantic Web Primer, G Antoniou

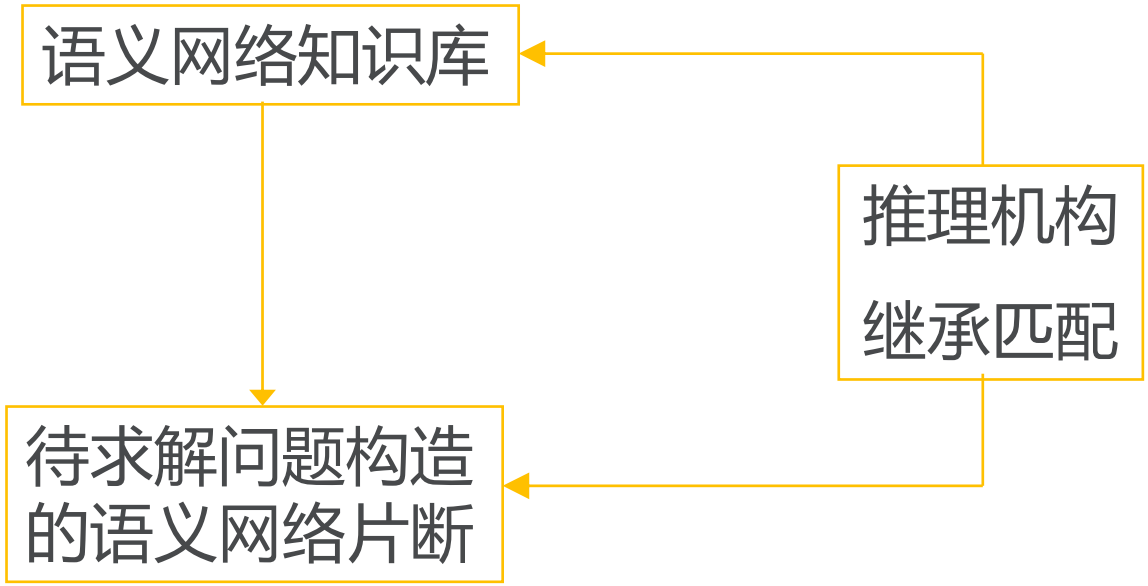
维基百科上的语义网堆栈



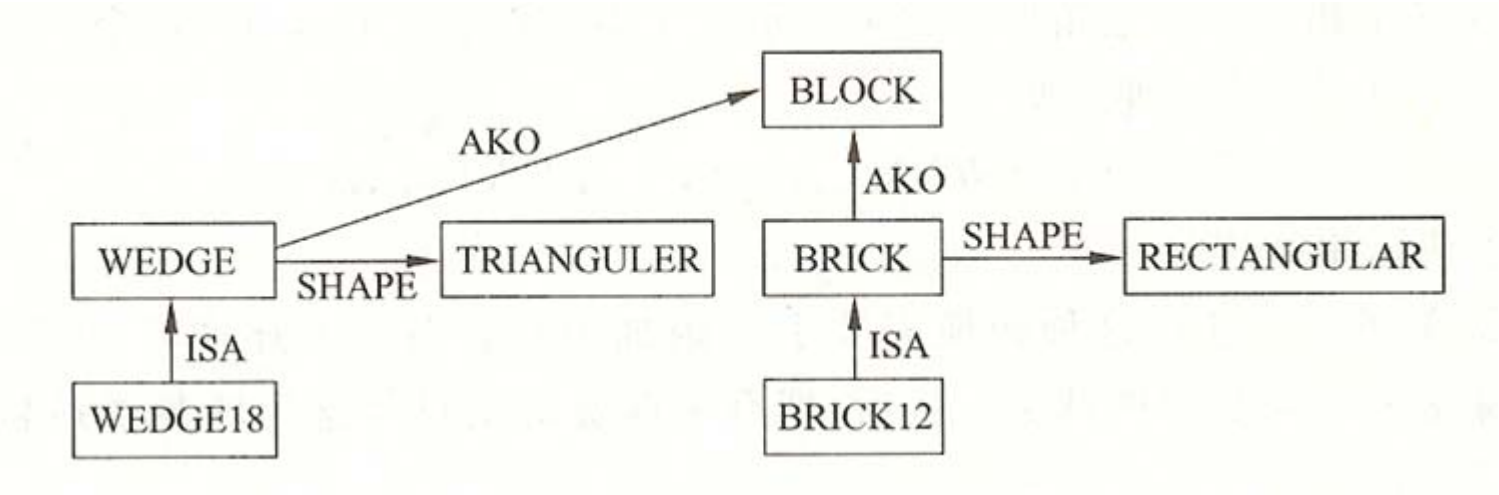
- RDF（Resource Description Framework）概念
  - 由W3C组织于1999年提出，于2004年2月成为W3C推荐标准
  - 是一种语义资源描述语言
  - 本质上是一种数据模型，涵盖数据结构、操作符、查询语言和完整性规则
- RDF基本数据模型
  - 资源（Resource）：能够使用RDF表示的对象，资源用唯一的URI来表示
  - 属性（Property）：用来描述资源的特征或资源间的关系
  - 断言（Statements）：为三元组<主体，属性，客体>
- RDFS (RDF Schema)
  - 定义了一组标准类及属性的层次关系词汇
  - 是一种模式语言，定义了特定领域的词汇的含义

Adida B, Birbeck M, McCarron S, et al. 2013. RDFa Core 1.1 - Second Edition

- 语义网络的推理过程
  - 用语义网络表示知识的问题求解系统包括：
    - 用语义网络构成的知识库
    - 用于问题求解的推理机构
  - 语义网络的推理过程主要有两种：继承，匹配



- 所谓继承就是对事物的描述从概念节点或类节点传递到实例节点，例如下图：



- 继承推理的三种继承模式
  - **值继承**：ISA链与 AKO（A Kind Of）链，常用知识传递方法
  - **“如果需要”（If - needed）链**：有时对不知道的槽值，可以计算得到，通过此计算程序得到知识的模式称为if - needed链，如通过体积与密度在需要时可以计算其质量
  - **“缺省”继承**：在对事务所作假设无十分把握时，可以加上“可能”字样，这种不肯定的值称为“缺省”值

内容概要

- 一、语义网络概念与内涵
- 二、本体概念与内涵
- 三、语义网与本体的应用
- 四、未来的挑战

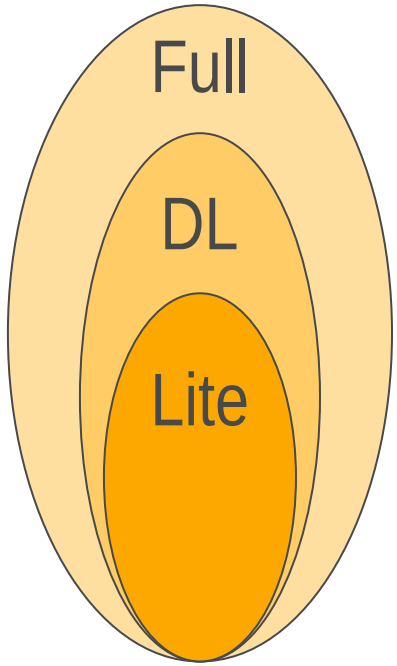
- 本体ontology
  - 斯坦福大学Tom Gruber：一种对于某一概念体系的明确表述（specification）
  - W3C：Ontology is about the exact description of things and their relationships
  - 德国学者Studer等人（1998）：“本体是共享概念模型的明确的形式化规范说明”

基本特征：概念化、形式化、可共享、明确、描述领域知识

- 本体描述语言
  - 基于谓词逻辑的本体描述语言：表示能力有限
  - 基于Web的本体描述语言：主流语言

特征	语言					
	SHOE	OML/CKML	RDF(S)	OIL	DAML+OIL	OWL
Horn 逻辑	是	否	否	否	否	否
描述逻辑	否	否/是	否	是	是	是
谓词逻辑	否	否	否	否	否	否
类的相等	支持	支持	不支持	不支持	支持	支持
属性/谓词相等	支持	支持	不支持	不支持	支持	支持
实例相等	不支持	不支持	不支持	不支持	支持	支持
本体分布定义	支持	不支持	支持	支持	支持	支持
本体扩展	支持	不支持	支持	支持	支持	支持
本体版本修订	支持	不支持	不支持	不支持	不支持	支持
计算特性区分	无	有	无	有	无	有

- OWL（Web Ontology Language）
  - OWL旨在提供一种可用于描述网络文档和应用之中所固有的那些类及其之间关系的语言，于2004 年2月成为W3C 的推荐标准
  - OWL提供了3种表达能力递增、计算效率递减的子语言：OWL Lite、OWL DL、OWL Full
    - OWL Lite：单一分类层次和简单约束，是OWL DL的子集仅支持部分的OWL语言要素
    - OWL DL：表达能力强大，与RDF不完全兼容
    - OWL Full：是OWL语言的全集，对推理的支持难以预测



- OWL（Web Ontology Language）

- 本体构造方法
  - 骨架法：基
  - IDEF5法：
  - 七步法：基
    用，应用广
  - METH-ON
  - TOVE法：
  - KACTUS法
    体
  - SENSUS法
  - 循环获取法
    术
  - 五步循环法

名称	生命周期	相关技术	方法细节	特点	应用领域
TOVE 法	非真正生命周期	不确定	少	基于问题	企业
METHON-TOLOGY 法	有	有 ,不全	详细	生命周期	化学、(Onto)2Agent
骨架法	非真正生命周期	不确定	少	指导方针	企业
KACTUS 法	没有	不确定	很少	知识复用	多用途复杂技术系统知识建模
SENSUS 法	没有	不确定	一般	启发式	电子科学、军事等
IDEF5 法	没有	有 ,不全	详细	结构化	企业
七步法	非真正生命周期	有	详细	系统	医学等

构造本体的要义

- Gruber在1995年提出的5条规则：

清晰（Clarity）

定义应该是客观的，形式化的

一致（Coherence）

它应该支持与其定义相一致的推理

可扩展性（Extendibility）

应该提供概念基础，支持在已有的概念基础上定义新的术语

编码偏好程度最小（Minimal encoding bias）

概念的描述不应该依赖于某一种特殊的符号层的表示方法

本体约定最小（Minimal ontological commitment）

本体约定应该最小，只要能够满足特定的知识共享需求即可。

内容概要

- 安全态势要素的表述
  - SNAP and SPAN:Towards Dynamic Spatial Ontology

$$\text{ExistsAt}(x, t) \equiv_{\text{def}} \exists\omega\,(\text{Snap}\Omega(\omega) \wedge \text{TemporalIndex}(\omega, t) \wedge \text{Constituent}(x, \omega))$$

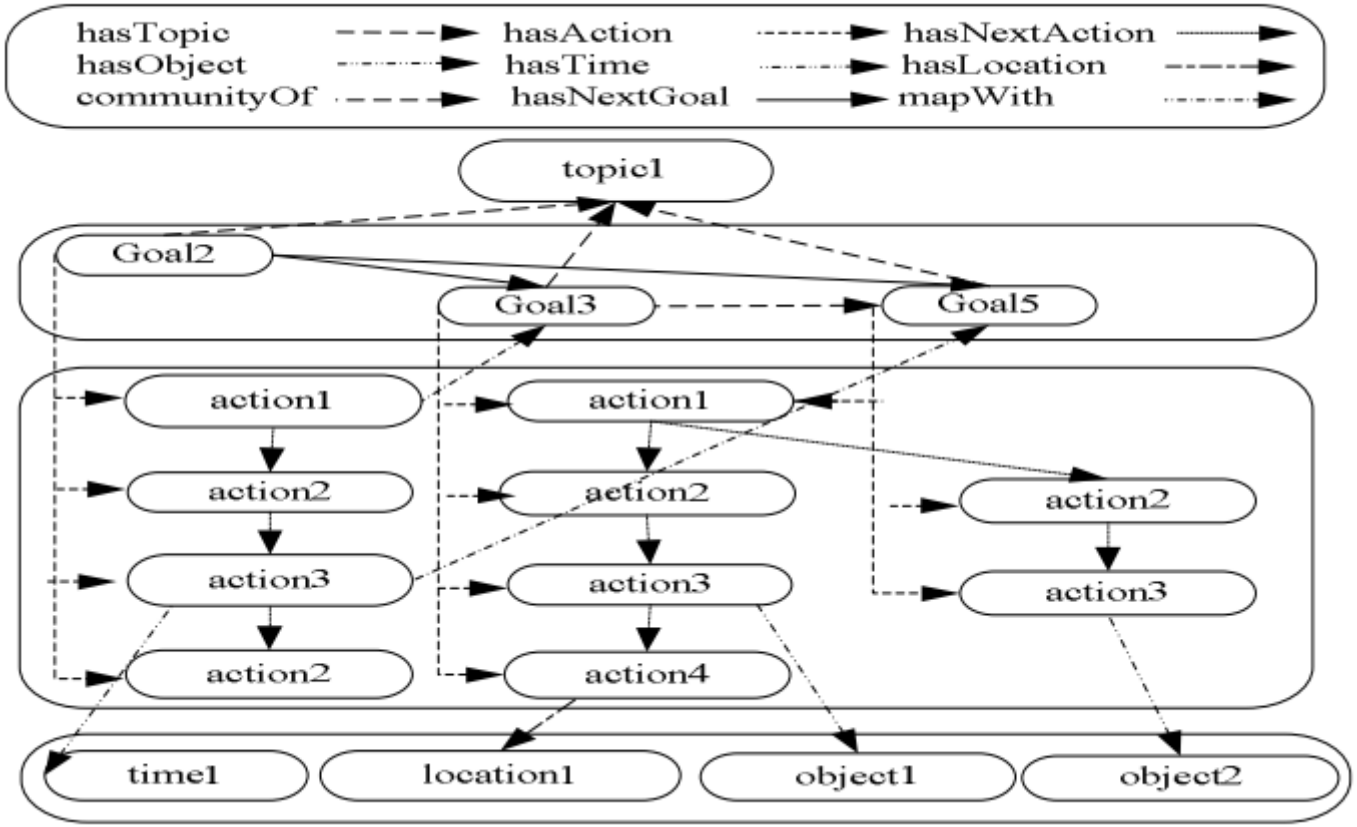
$$\text{ExistsDuring}(x, y) \equiv_{\text{def}} \text{TimeRegion}(y) \wedge \forall z\,((\text{TimeInstant}(z) \wedge \text{ProperPart}(z, y)) \rightarrow \text{ExistsAt}(x, z))$$

Constituent: Entity x Ontology	TemporalIndex: Ontology x TimeRegion
Part: Entity x Entity	SpatialLocation: SnapEntity x SpaceRegion
InheresIn: SnapDependent x Substantial	
TemporalLocation: SpanEntity x TimeRegion	TemporalLocation: SpanEntity x SpacetimeRegion
Exists-At: SnapEntity x TimeInstant	ParticipatesIn: Substantial x Processual

Figure 3. Primitive relations and their signatures.

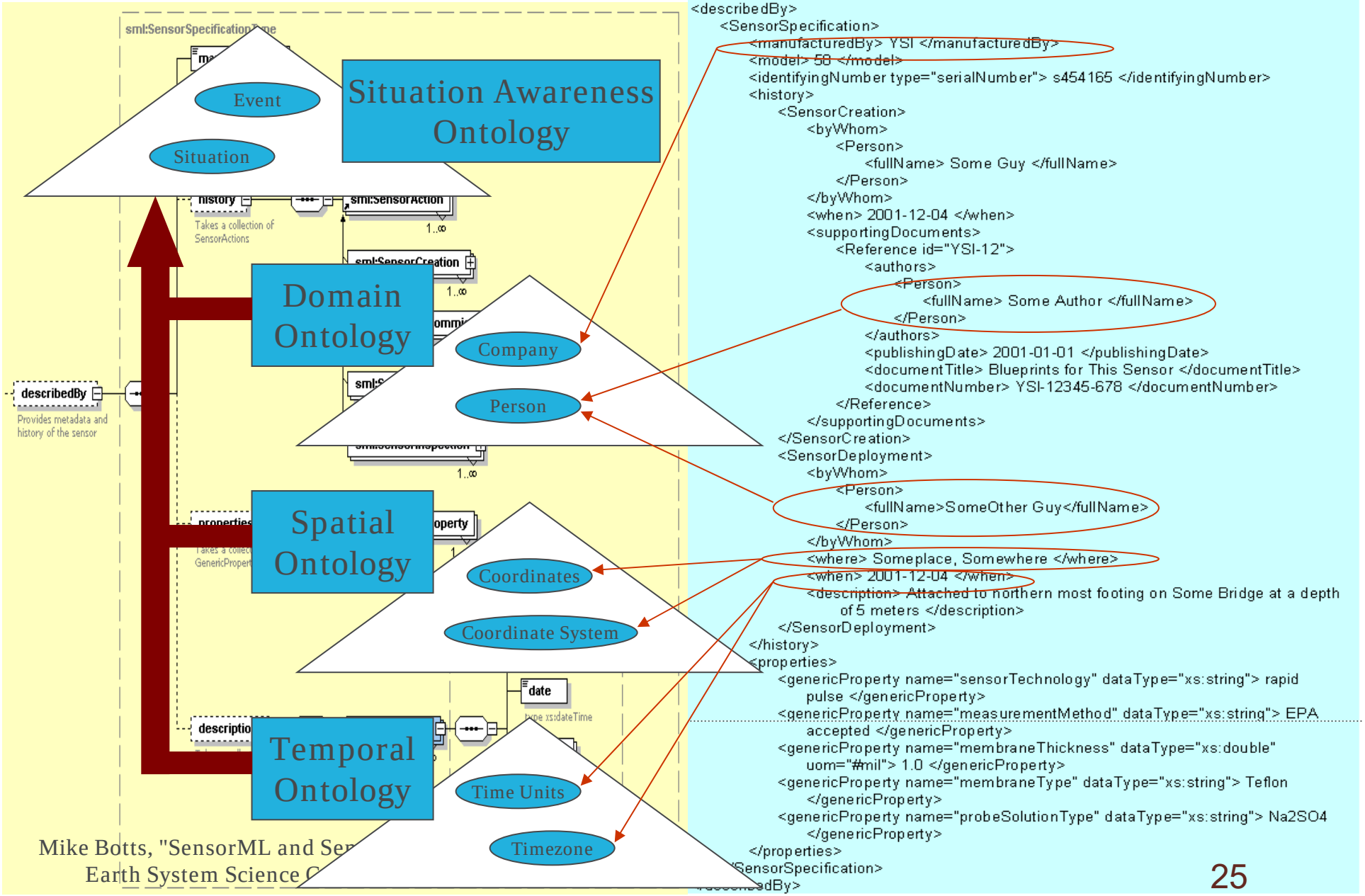
语义网与本体应用-数据表示（2）

- 一个扩展的态势本体模型：非网络安全



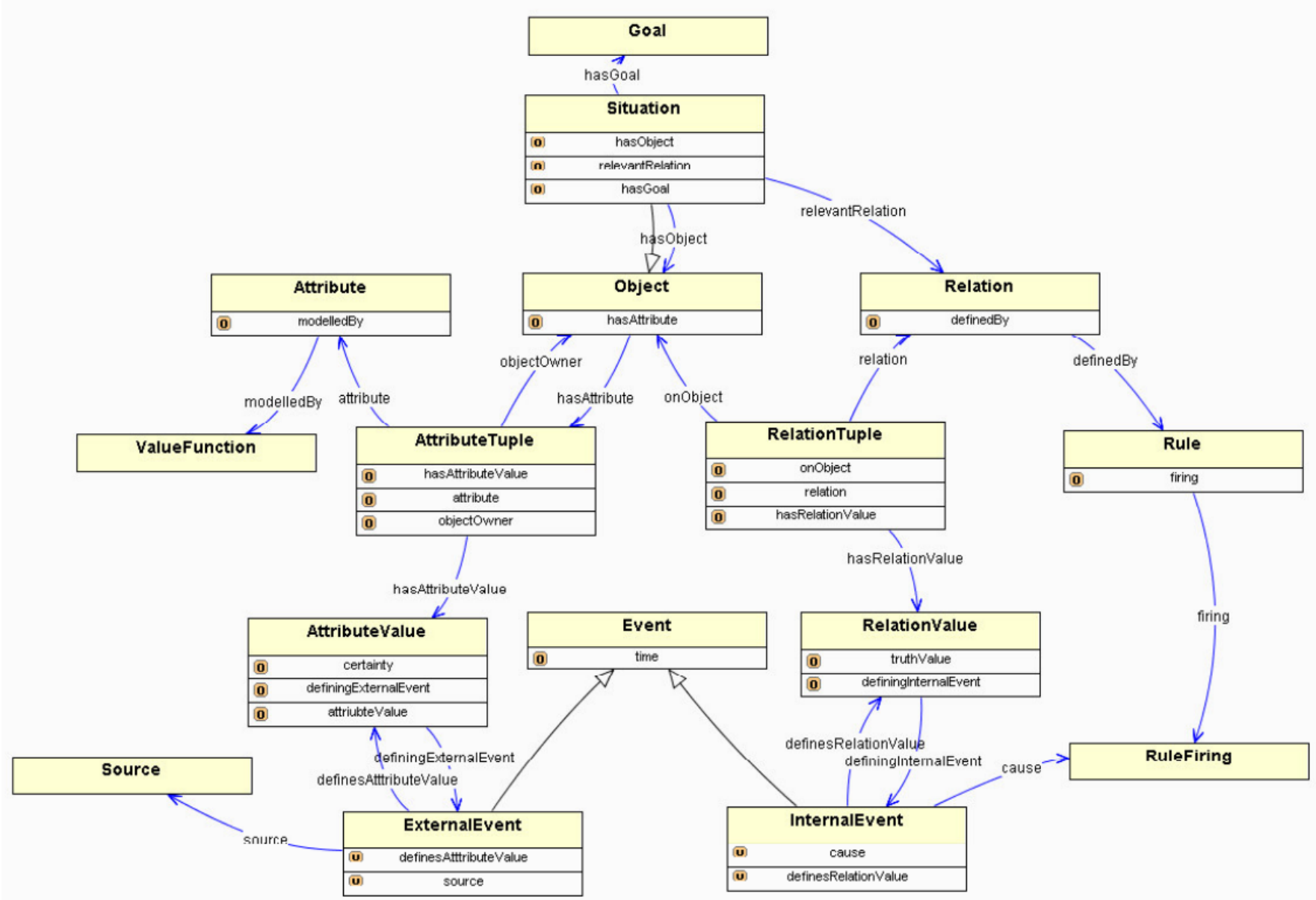
A Situation-Aware Method Based on Ontology Analysis of the Semantic Social Network

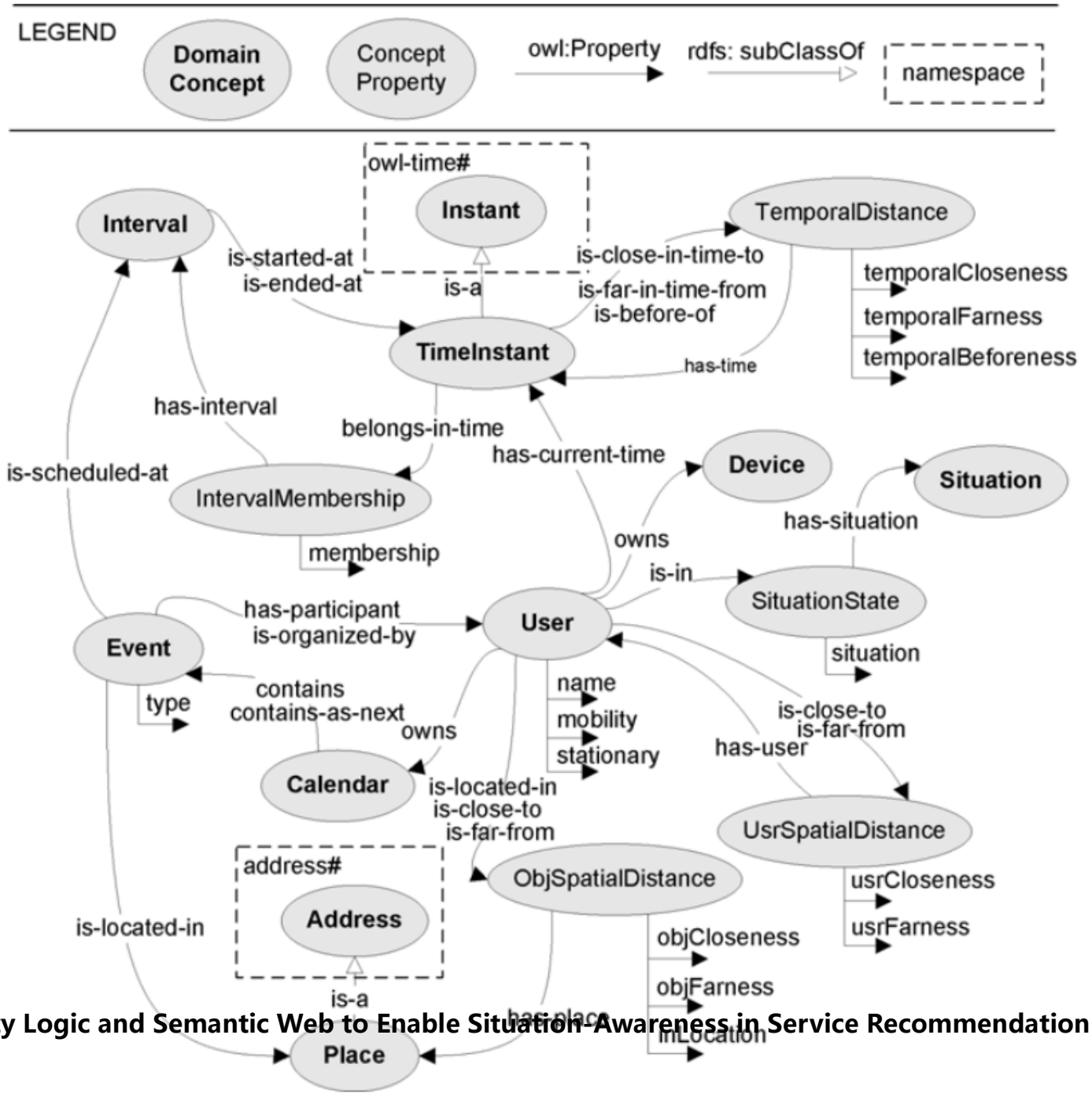
语义网与本体应用-数据表示（3）



Mike Botts, "SensorML and Sen
Earth System Science C

语义网与本体应用-数据表示（4）





Combining Fuzzy Logic and Semantic Web to Enable Situation-Awareness in Service Recommendation

语义网与本体应用-数据表示（6）

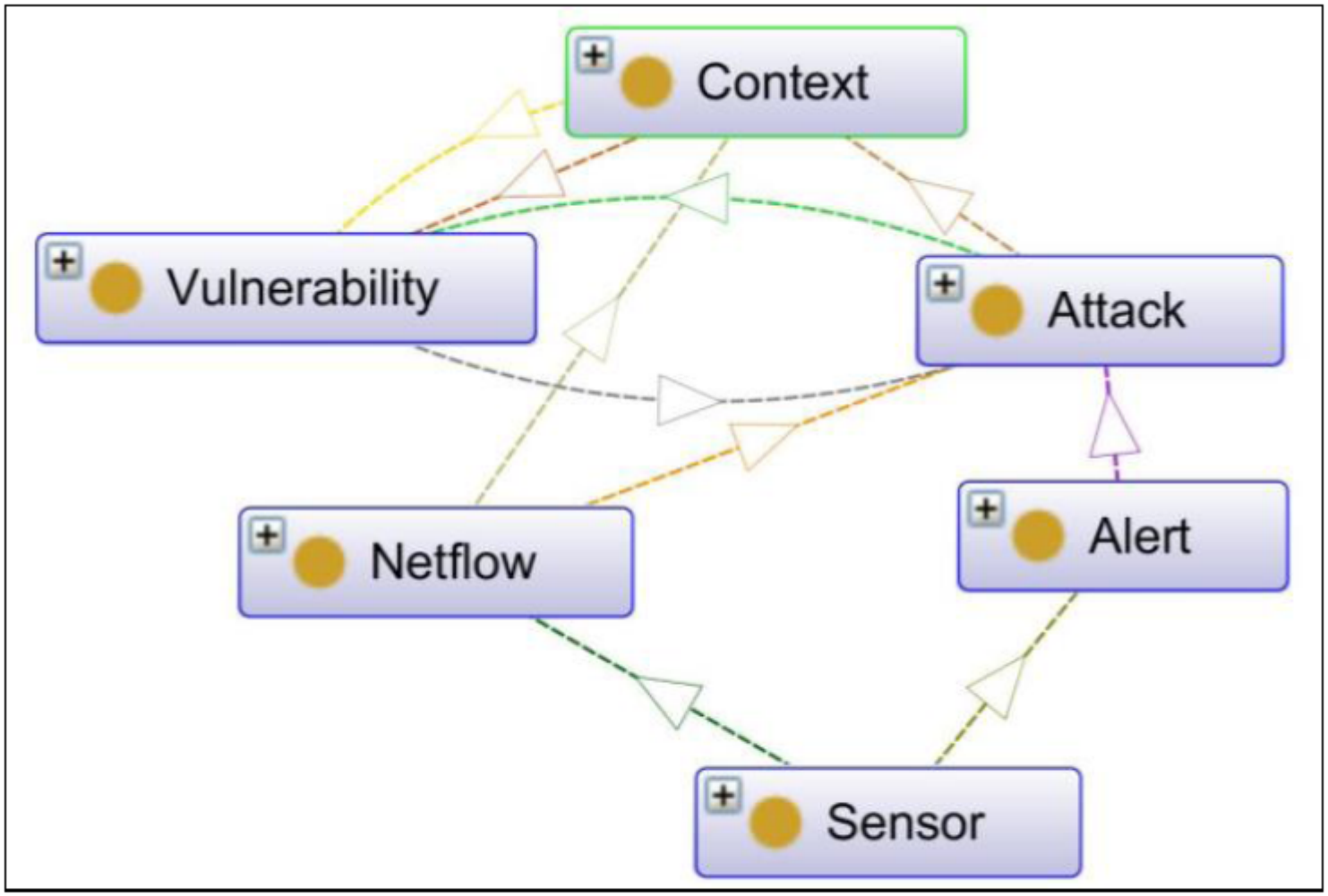
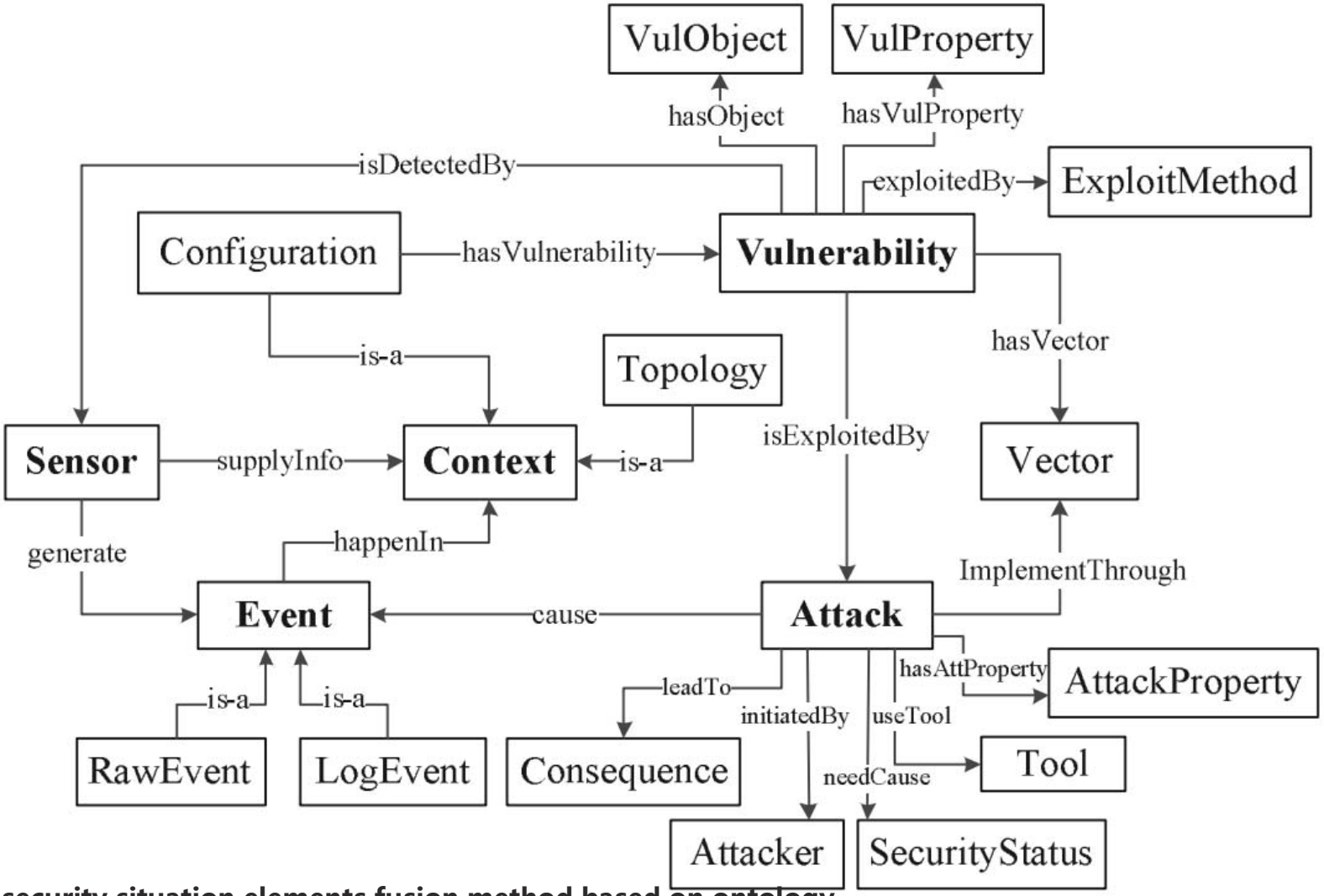


FIGURE 5. Top classes of the NSSA ontology model.

Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things

语义网与本体应用-数据表示（7）



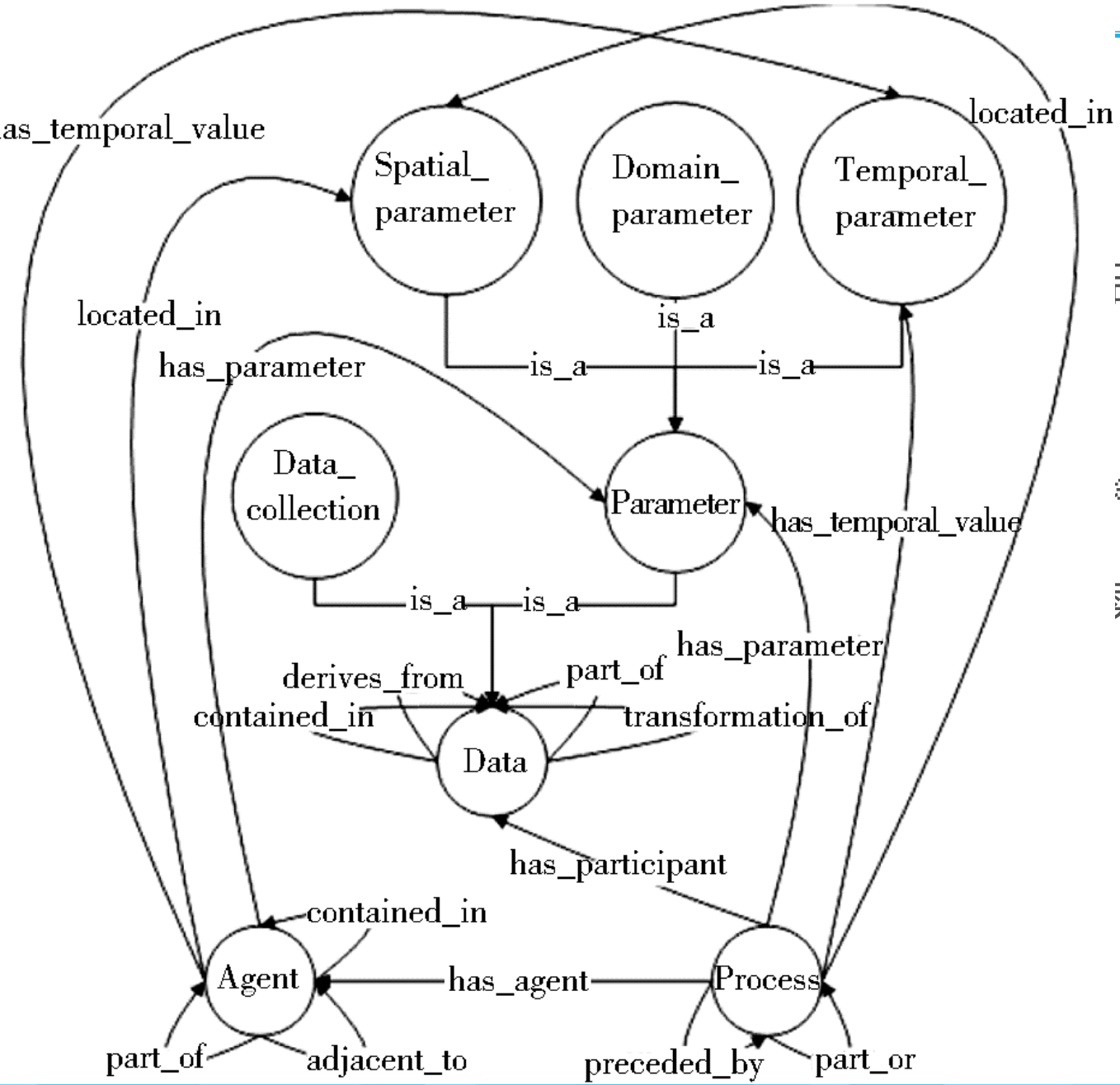
Network security situation elements fusion method based on ontology

- 开放溯源模型（Open Provenance Model，OPM）

关系名称	起点	终点	指代含义
Used	活动	实体	活动使用实体
Was Generated by	实体	活动	活动产生实体
Was Informed by	活动	活动	两个活动之间存在实体的交流
Was Derived by	实体	实体	活动使用的实体与产生的实体之间的关系，主要适用涉及活动未知或者不关注的情况
Was Attributed to	实体	代理	代理对实体承担责任
Was Associated with	活动	代理	代理在活动中承担责任
Acted on Behalf of	代理	代理	承担不同责任代理之间的关系

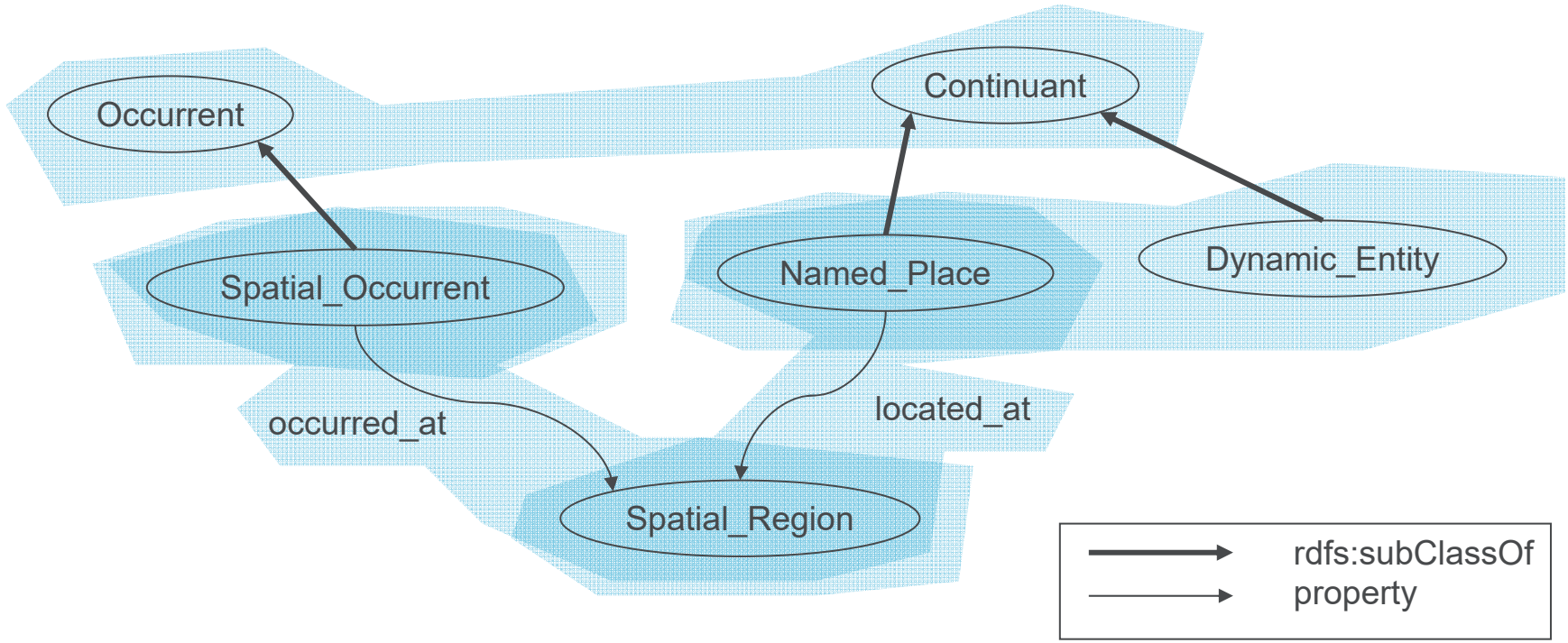
语义网与本体应用—数据溯源（2）

- Pr
  -



The Open Prover

语义网与本体应用-数据溯源（3）



Occurrent: Events – happen and then don't exist

occurred_at: Links Spatial_Occurents to their geographic locations

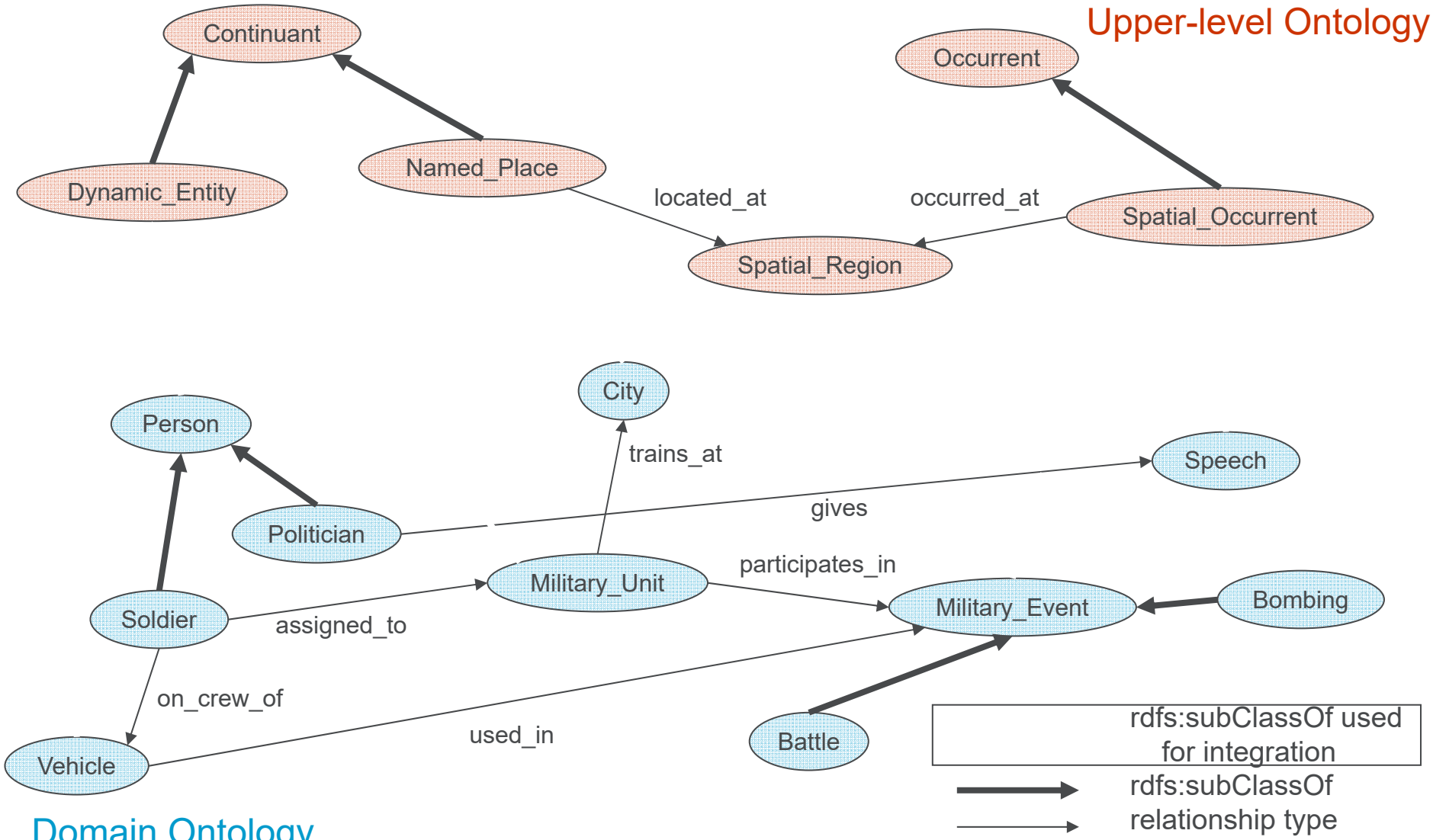
Spatial_Occurrent: Events with concrete spatial locations (e.g. a speech)

located_at: Links Named_Places to their geographic locations

Dynamic_Entity: Those entities with dynamics spatial locations (e.g. person)

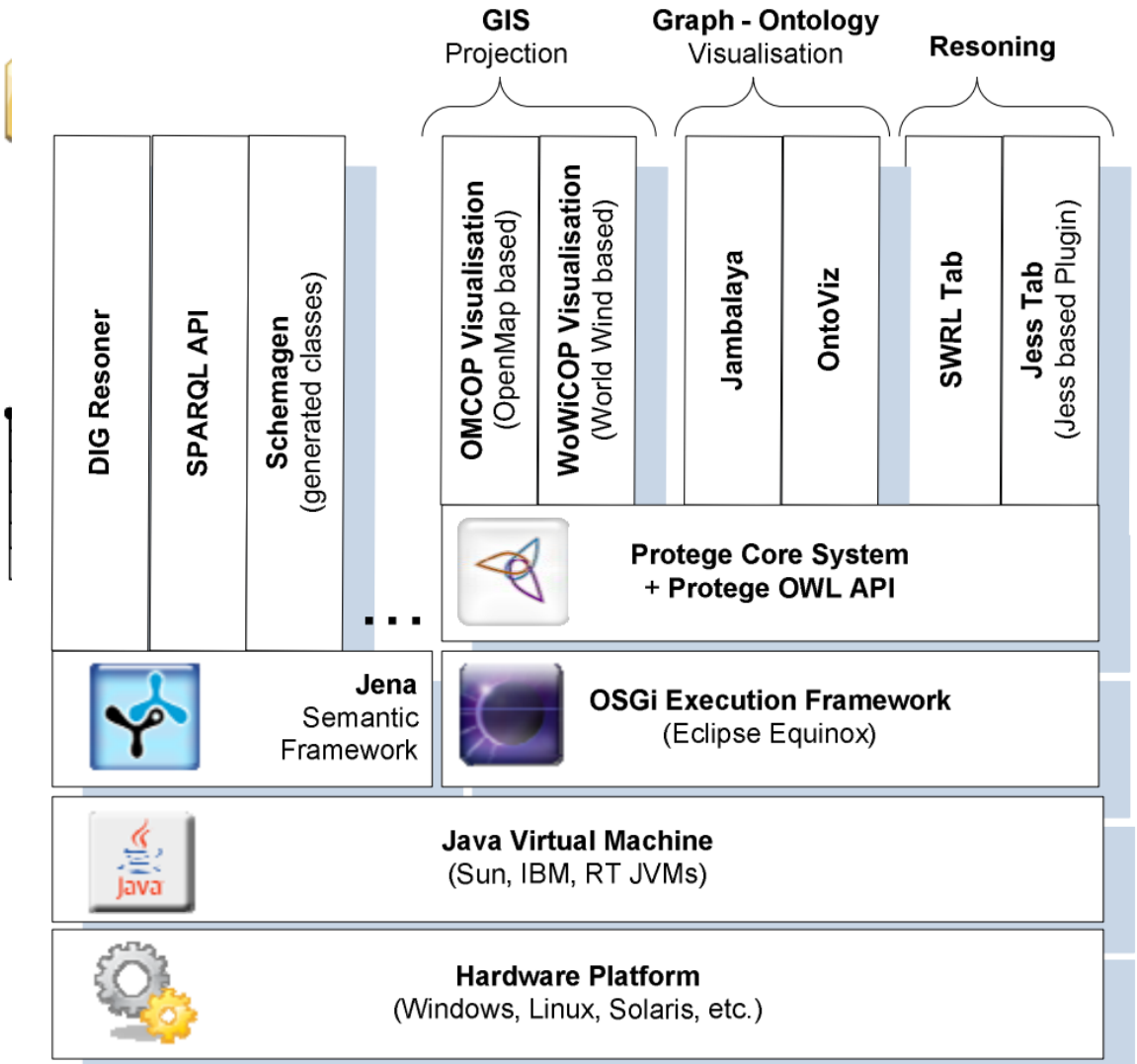
dynamic entities get spatial properties indirectly through relationships with spatial entities

语义网与本体应用-数据溯源（4）



dynamic entities get spatial properties indirectly through relationships with spatial entities

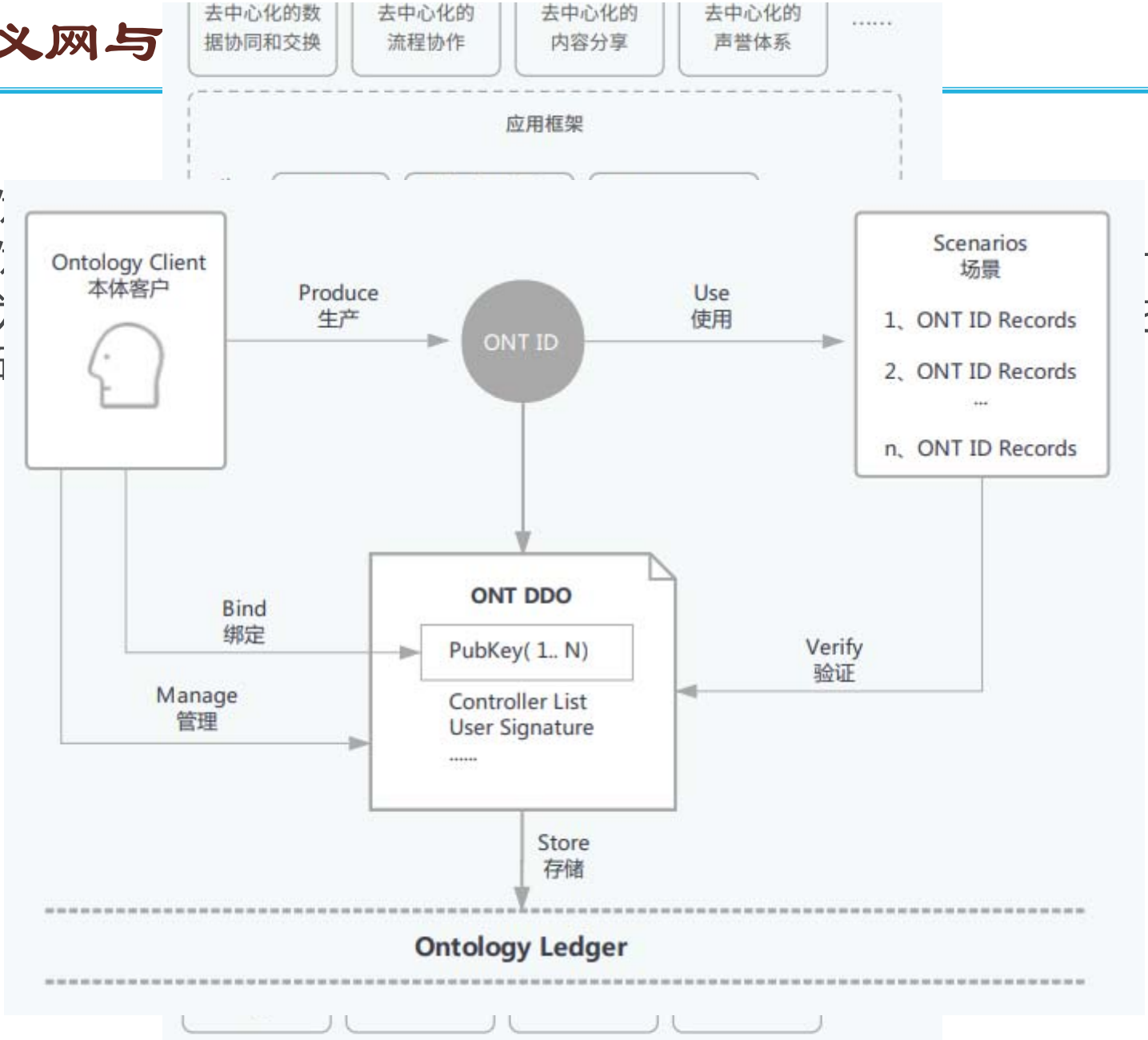
语义网与本体应用-决策辅助（1）



Ontology Applications for Achieving Situation Awareness in Military Decision Support Systems

- 本
- 本
  、
  基

协同
技术



https://icodrops.com/ontology-network/

内容概要

- 一、语义网络概念与内涵
- 二、本体概念与内涵
- 三、语义网与本体的应用
- 四、未来的挑战

未来的挑战

- 网络数据智能语义化
  - 智能标记
  - 语义理解
  - …
- 网络主体的智能推理
  - 精准的机器推理（学习）
  - 语义表达模型扩展
  - 本体的时空动态演变
  - …
- 安全与隐私
  - 能力表达与隐私泄露是一对矛盾体

语义与本体