基于语义相似度的静态安全策略一致性检测

唐成华[1,2] 王丽娜[1,2] 强保华[2] 汤申生[3] 张 鑫[2]
(桂林电子科技大学广西信息科学实验中心 桂林 541004)[1]
(桂林电子科技大学广西可信软件重点实验室 桂林 541004)[2]
(西密苏里州立大学电子工程学院 圣约瑟夫 64507)[3]

摘 要 安全策略语义是人类控制安全行为意志的表达。针对策略语义在定义和转换过程中存在的冲突等问题,提出一种基于语义相似度的静态安全策略一致性检测模型与算法。首先建立策略领域本体并提取特征因子,给出基于本体中概念特征的语义相似度计算方法;继而以防火墙安全策略为例建立实例检测模型,运用静态安全策略一致性检测算法对冲突策略进行标记处理,并保证最终的策略规则库的一致性。实验结果表明,该算法具有较好的检测效果,为解决安全策略在定义、制定和映射等阶段的冲突提供了一种可行的途径。

关键词 安全策略,语义相似度,语义一致性,领域本体,特征因子
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.035

Static Security Policy Consistency Detection Based on Semantic Similarity

TANG Cheng-hua[1,2] WANG Li-na[1,2] QIANG Bao-hua[2] TANG Shen-sheng[3] ZHANG Xin[2]
(Guangxi Experiment Center of Information Science, Guilin University of Electronic Technology, Guilin 541004, China)[1]
(Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China)[2]
(Department of Engineering Technology, Missouri Western State University, St. Joseph MO 64507, USA)[3]

Abstract The security policy semanteme is the expression of human control safety behavior will. Aiming at the problem of the policy semantic conflicts existing in the definition and conversion process, a static security policy consistency detection algorithm based on the semantic similarity was proposed. Firstly, the domain ontology of the security policy is established, the characteristic factor is extracted, and then the calculation method of semantic similarity based on the ontology concept features is presented. Secondly, the firewall security policy is used as an example to establish a detection model, and the static security policy consistency detection algorithm is used to mark the confict policy, ensuring the consistency of the final policy rule base. Experimental results show that this method has better detection effect, and provides a feasible way to solve the security policy conflicts in the stage of definition, making and mapping.

Keywords Security policy, Semantic similarity, Semantic consistency, Domain ontology, Characteristic factor

网络安全策略用于指导网络信息系统安全的保护、检测、响应与恢复过程,反映了与系统安全相关的需求,是对人和资源进行安全控制的规则集合,是一种贴近人类思维的高层指导网络安全行为的方法[1]。策略语义则是这类行为规则对网络信息安全控制意志的表达,其形态过程影响到安全策略对网络与信息的安全保障能力。

从策略语义形态有效性的角度来看,安全策略语义的一致性问题是目前一个重要的研究课题。一般从不同角度或层面上研究如何保证策略语义在定义、转换和执行等形态过程中的一致性,如针对基于分类的授权策略提出的阵列模式的策略内部一致性和外部冲突检测算法[2];或者将策略模式化为半格形式,并通过动态编码生成授权策略,以确保授权策略在执行时的语义符合上下文[3];也有根据不同的策略目标,提出两种基于优先级的访问控制策略的非一致性冲突检测与消解方法[4]。文献[5,6]将策略描述框架定义成一种逻辑程序,并提出基于逻辑的策略语义一致性检测与自动修正方法,在统一良基语义下实现策略表达、语义查询和验证,在上下级相关策略本身无冲突的前提下实现相应的语义转换。文献[7]以网络级访问控制策略的定义和部署为例,用最先匹配原则解决语义冲突时的策略取舍问题。文献[8]设计了一组规则用于推理变化性、互斥、需要等约束,并基于描述逻辑实现对知识库中的语义特征建模及一致性等推理,该方法着重于将领域特征模型转换为描述逻辑知识库中的语义模型,而领域特征的抽取仍依赖于专家经验。近年来出现的基于语义相似

到稿日期:2014-08-26 返修日期:2014-11-24 本文受国家自然科学基金(61462020,61363006,61163057),广西自然科学基金(2014GXNSFAA118375),广西信息科学实验中心基金(20130329)资助。
唐成华(1974—),男,博士后,副教授,硕士生导师,CCF会员,主要研究方向为网络与信息安全,E-mail:tch@guet.edu.cn;王丽娜(1987—),女,硕士生,主要研究方向为网络信息安全;强保华(1972—),男,博士后,教授,主要研究方向为智能信息处理;汤申生(1969—),男,博士,主要研究方向为智能信息处理;张 鑫(1990—),男,硕士生,主要研究方向为网络信息安全。

度计算及其在信息或事实陈述[9]、语义差异协调[10]和异构本体映射[11]等方面的应用研究也为语义转换和验证提供了一种思路。Kobra 等[12]针对本体在分割和分配到子分区时产生语义图的问题，提出一种基于距离的语义相似度计算方法，其模型较直观，但在本体产生加权图时，将直接相连结点之间边的权重记为相同值，没有考虑差异影响因素。Pirro[13]充分利用相似理论、信息理论和概率统计的知识，提出一种基于信息内容的语义相似度计算模型。Kunal 等[14]提出基于非功能性属性的语义相似度模型和算法，用于 Web 服务策略的匹配，其属性包括结构、句法，以及基于本体的策略制定意图等，通过域间策略关系来表达一种语义域模型，这有助于识别策略在规范和匹配过程中的不一致性，不过该计算模型依赖于本体中概念结点属性信息的丰富程度。

这些基于各种概念或属性特征的语义相似度计算方法可以用来实现策略语义形态的基本转换过程，亦可提高策略语义一致性冲突检测的准确性。本体由于能够准确描述概念含义和概念之间的内在关联，已成为语义相似度研究的基础。但现有语义相似度计算方法没有充分利用本体中的语义信息，且计算方法复杂。因此，本文提出一种基于本体中概念特征的语义相似度计算方法，根据概念在本体中的层次结构来确定特征集合，将相似度公式表示成更直观的形式，该方法计算简便，且接近于人类主观的判断值。另外，由于策略语义的一致性问题首先发生在策略制定的语法分析过程中，即静态语义冲突的检测与系统的即时状态无关；而动态策略语义冲突需要在系统运行期间对系统所有可能出现的状态进行动态分析以期发现冲突，适用于检测那些由于系统的某个特定状态而导致的冲突。尽管静态方法只能检测部分简单的策略冲突，而动态方法可以检测所有类型的策略冲突，但是过多的动态检测将会降低系统的运行效率，所以动态方法并不能替代静态方法，二者相辅相成，而且静态冲突是一种实际冲突，在策略制定、处于静态时就应首先予以解决。

1 基本概念

语义相似度是指两组概念之间的相似程度，说明两组概念之间具有某些相同的特性。语义相似度计算可以将规则概念之间不容易发现的共性、冲突等信息通过数字明确表示出来。

定义 1 静态安全策略语义一致性冲突是指高层语言的安全策略规范的不一致性引起的语义冲突，即高层管理人员制定的两条或两条以上的安全策略在主体、客体、动作行为上定义了不同的表示形式时发生的语义冲突。

静态安全策略语义一致性冲突主要表现为安全策略的各个概念、属性之间存在交集或是包含关系。因此，计算各安全策略特征属性之间是否存在某种关系，为语义一致性的检测提供了一种快速简便和有效的方法。

定义 2(韦氏字典规定[15]) 对于具有共同的严格的可比特征的度量，概念 W_1 和 W_2 的相似度 $sim(W_1,W_2)\in[0,1]$。若 $sim(W_1,W_2)=1$，则 $W_1=W_2$，表示两个概念相同；若 $sim(W_1,W_2)=0$，则 $W_1\neq W_2$，表示两个概念完全不同，即互不相关。

定义 3 特征因子是指领域本体中的概念和属性等，而且它们是可以区分的。

定义 4 安全策略中存在继承关系，策略 t_4 若继承策略 t_2，则可表示为 $t_2\rightarrow t_4$。

定义 5 安全策略包括多个领域，为其建立领域本体，将领域本体中的各个概念、属性作为特征因子，则基于本体的语义相似度为：

$$sim(P_1,P_2)=\frac{\sigma(P_1,P_2)}{\varphi(P_1,P_2)} \tag{1}$$

式中，$\sigma(P_1,P_2)$表示策略 P_1 和策略 P_2 包含的相同特征因子的个数；$\varphi(P_1,P_2)$表示策略 P_1 和策略 P_2 包含的全部特征因子的个数。

根据传统的语义相似度计算方法，概念之间的相似程度与它们所包含的信息有关。两个概念共同拥有的信息越多，则它们就越相似；反之，如果两个概念所包含的不同的信息越多，它们的相似度就越小。有了特征因子的定义，则语义相似度的计算就是基于特征因子的比较。

定义 6 在安全策略被选择和执行时，遵循否定策略优先原则，即当主、客体相同的禁止策略和允许策略同时被触发时，优先选择禁止策略。

定义 7 基于范围规定安全策略的优先级，即在安全策略的继承层次里，禁止情况下范围大的优先保留，或者允许情况下范围小的优先保留。

2 静态安全策略语义一致性检测

2.1 基于语义相似度的静态策略语义一致性检测方法

由于在制定时存在动态环境变化等影响因素，高层语言制定的网络安全策略不可避免地存在语义上的冲突，在此阶段首先完成安全策略语义的一致性冲突检测将具有较高的实用性，并对安全策略的后续选择和执行带来积极作用。静态安全策略语义一致性检测的过程是：

(1)通过 Protégé 建立策略领域本体，且基于本体设定特征因子，如图 1 所示。

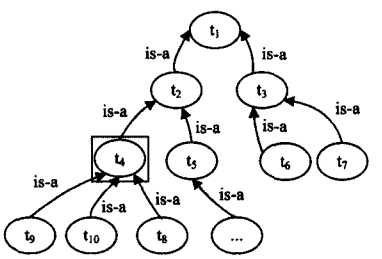

图 1 基于本体设定的特征因子

(2)提取策略 P_1 和策略规则库中的其他策略(如策略 P_2)的全部特征因子。根据定义 5 计算出所有特征因子总数 $\varphi(P_1,P_2)$，并对这些特征因子进行对比，选出策略 P_1 和策略 P_2 中相同的特征因子，并且计算出相同特征因子的个数 $\sigma(P_1,P_2)$。

(3)根据式(1)计算策略 P_1 和策略 P_2 的语义相似度。

(4)根据计算出的策略语义相似度以及各个领域中不同安全策略需求的不同，对两条策略进行后续相似处理(采用优先级原则，根据定义 6 和定义 7 采用否定策略优先和基于范围规定优先级的混合模式进行策略选择)，最终保留无冲突的策略，删除或标记冲突的策略。考虑到实际应用，本文对冲突的安全策略进行标记，以作为后期改进的目标。

2.2 静态安全策略语义一致性检测实例

以防火墙安全策略为例建立模型，针对高层语言的安全策略语义一致性冲突进行检测。防火墙的安全策略主要有两种：允许访问，是指在防火墙的安全策略中没有被列为允许访问的服务都是被禁止的，这意味着需要确定所有可以被提供的服务以及它们的安全特性，开放这些服务，并将所有其他未列入的服务排斥在外；禁止访问，则是指在防火墙的安全策略中没有被列为禁止访问的服务都是被允许的，这意味着首先确定那些被禁止的、不安全的服务，以禁止访问它们，而其他服务则被认为是安全的。

2.2.1 防火墙安全策略规则库

建立防火墙安全策略规则库，以此为例对静态策略语义一致性冲突进行检测，并根据需求将冲突部分删除或保留。防火墙安全策略规则库示例如表 1 所列。

表 1 防火墙安全策略规则

策略	动作	主体	客体
P_1	禁止	内部 IP2 访问	外网任意端口
P_2	允许	内部所有 IP 访问	外网的 TCP-80 端口
P_3	允许	内部所有 IP 访问	外网的 UDP-53 端口
P_4	允许	内部所有 IP 访问	外网任意端口
P_5	允许	内部 IP2 访问	外网任意端口
P_6	禁止	内部所有 IP 访问	外网的 TCP-25 端口
P_7	禁止	内部 IP2 访问	外网的 TCP-25 端口
P_8	禁止	内部所有 IP 访问	外网的 UDP-53 端口
P_9	允许	内部 IP2 访问	外网的 UDP 端口
P_{10}	禁止	内部 IP2 访问	外网的 TCP 端口

在表 1 中，策略 P_2 和策略 P_3 的特征因子分别为：允许，内部所有 IP 访问，外网的 TCP-80 端口；允许，内部所有 IP 访问，外网的 UDP-53 端口。根据式(1)，策略 P_2 和策略 P_3 的相似度计算就是对特征因子的比较，即 $sim(P_2,P_3)=2/3$。

2.2.2 建立领域本体

通过 Protégé 建立防火墙安全策略本体，并将本体中的概念、属性等作为计算防火墙安全策略语义相似度的特征因子，如图 2 所示。

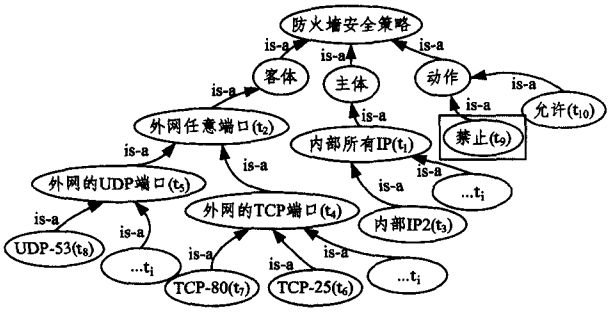

图 2 基于策略本体设定的特征因子

其中防火墙安全策略各特征因子的表示如下：

t_1：内部所有 IP；

t_2：外网任意端口；

t_3：内部 IP2；

t_4：外网的 TCP 端口；

t_5：外网的 UDP 端口；

t_6：外网的 TCP-25 端口；

t_7：外网的 TCP-80 端口；

t_8：外网的 UDP-53 端口；

t_9：禁止；

t_{10}：允许。

由图 2 可知，特征因子 t_1 和 t_2 属于同一层，t_3、t_4 和 t_5 分属 t_1、t_2 的下一层，即子集与自身之间具有继承关系；t_6、t_7、t_8 属于 t_3、t_4、t_5 的下一层也即是它们的子集，它们之间同样具有继承关系。由定义 4 有：$t_1 \rightarrow t_3$，$t_2 \rightarrow t_4$，$t_2 \rightarrow t_5$ 等。

2.2.3 静态安全策略一致性检测算法及应用

利用基于本体语义相似度的静态策略语义一致性检测方法对防火墙策略进行冲突检测处理，如图 3 所示。首先读取防火墙安全策略规则库(以表 1 为实例)中的两条策略，对它们进行特征因子的比较分析，并计算出两条策略中所有特征因子数以及相同的特征因子数。然后根据式(1) 计算出两条策略的语义相似度，相似度为 0 的保留，不为 0 的进行标记。另外，为了保证防火墙的安全性能，对同为允许的或者同为禁止的并且相似度为 0 的两条策略进行处理：两条策略动作都为允许时，标记特征因子范围大的策略，保留范围小的策略；动作均为禁止时，标记特征因子范围小的策略，保留范围大的策略。否则对同为允许的或者同为禁止的且相似度不为 0 的两条策略进行处理：若同为禁止且主体或客体相同，另外一对范围不同时，则保留范围大的策略，标记小的策略；若同为允许，则相反。当语义相似度为 1 时，若动作不同，则保留禁止策略，标记允许策略；当语义相似度为 1.0/3.0 时，若动作不同且主体或客体相同，另外一对范围不同时，则保留禁止策略。

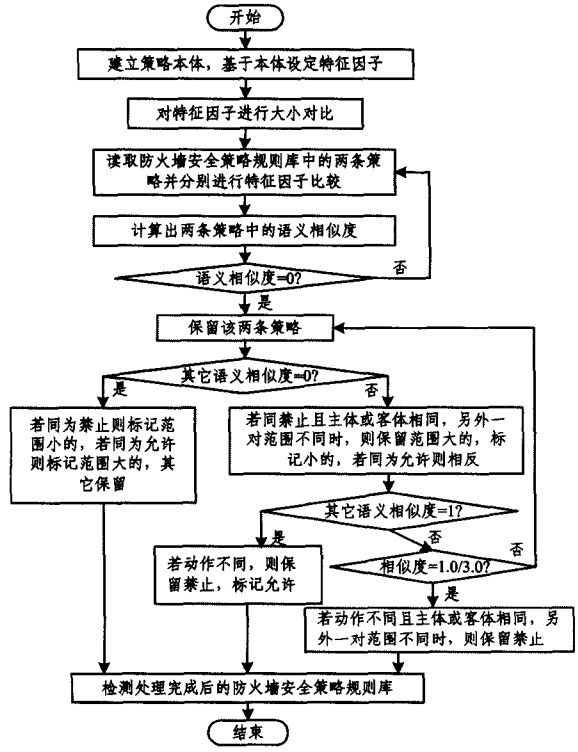

图 3 静态防火墙安全策略语义一致性检测流程

算法 1 静态防火墙安全策略语义一致性检测

Input：特征因子 characteristic，防火墙安全策略规则库 Rules

Output：一致性的防火墙安全策略规则库

Begin {

1. I=Rules. length / * 规则库里的策略数 * /

2. for i=0 to I do

```
3.  CharacteristicFactorComparision [Rules(i),Rules(i+1)]
    /*每两条策略进行特征因子比较*/
4. end for
5. for i=0 to I do
6.  while(sim(Rules(s),Rules(s+1))=0) do
/*sim 计算语义相似度*/
7.  ProcessedRules=retain(Rules(i),Rules(i+1))
/*若两条策略的相似度为 0,则保留这两条策略*/
8. end for
9. for i=0 to I do
10. while(sim(ProcessedRules(i+1),ProcessedRules(i))=0) do
    /*动作相同时其他特征因子的语义相似度为 0*/
11.  if(flag(ProcessedRules(i+1),ProcessedRules(i))
/*flag 若为真,则两条策略的动作都为禁止,否则为允许*/
12.  ProhibitRules(ProcessedRules(i+1),Processed Rules(i))
     /*若动作同为禁止,则标记特征因子范围小的,保留大的*/
13.  else
14.  PermitRules(ProcessedRules(i+1),Processed Rules(i))
     /*若动作同为允许,则标记特征因子范围大的,保留小的*/
15.  end if
16. end for
17. for i= 0 to I do
18. while(sim(ProcessedRules(i+1),ProcessedRules(i))≠0) do
    /*动作相同时其他特征因子的语义相似度不为 0*/
19.  if(flag(ProcessedRules(i+1),ProcessedRules(i))
     /*flag 若为真,则两条策略的动作都为禁止,否则为允许*/
20.  ProhibitRules1(ProcessedRules(i+1),Processed Rules(i))
     /*若同为禁止,且主体或客体相同,另外一对范围不同时,则
     保留范围大的,标记小的,其余情况保留*/
21.  else
22.  PermitRules1(ProcessedRules(i+1),Processed Rules(i))
     /*若同为允许,且主体或客体相同,另外一对范围不同时,则
     保留范围小的,标记大的,其余情况保留*/
23.  end if
24. end for
25. AfterProcessFirewallPolicyRule=Getretain()}
    /*输出处理后的防火墙安全策略*/
End
```

3 实验结果及分析

在 Java 平台下应用算法 1 对表 1 中防火墙安全策略规则编程计算后,得出处理后的防火墙安全策略,如表 2 所列。

表 2 处理后的防火墙安全策略

策略	标识	策略	标识	策略	标识
P_1	0	P_5	1	P_9	1
P_2	0	P_6	0	P_{10}	1
P_3	1	P_7	1	—	—
P_4	1	P_8	0	—	—
P_4	1	P_8	0	—	—

表 2 中标识为 0 的策略表示处理后没有冲突而保留下来的策略,标识为 1 的策略表示处理后存在冲突的策略。通过对比分析表 2 与表 1 可知,对于静态安全策略语义一致性冲突检测,应用算法 1 使得安全策略语义中存在冲突的策略尽可能地被标记,具有很高的准确率。另外,实验显示,当策略数分别为 50、100 和 1000 时,算法 1 仍然具有很好的效果。

应用算法 1 对规则数在 10,20,…,100 时的防火墙安全策略进行处理的准确率以及处理时间如表 3 所列。

表 3 算法 1 处理策略的准确率以及处理时间

策略数	10	20	30	40	50	60	70	80	90	100
准确率(%)	90	90	85	82.5	85	83.3	88.5	96.2	86.7	87
处理应用时间(ms)	3	6	10	14	17	21	25	28	31	33

文献[16]在人工参与的基础上将防火墙安全策略分为禁止和允许两类,提出了一种静态冲突检测算法,其核心思想是:同为禁止或允许的两条策略进行比较,检测出主体/客体有冲突的,标记为主体/客体关联冲突策略;或者同时有主客体冲突的,则标记为主客体关联冲突策略。

应用文献[16]中的算法编程对规则数在 10,20,…,100 时的防火墙安全策略进行处理的准确率以及处理应用时间如表 4 所列。

表 4 文献[16]算法处理策略的准确率以及处理时间

策略数	10	20	30	40	50	60	70	80	90	100
准确率(%)	70	70	65	72.5	67	70	72.5	76.2	72.2	63
处理应用时间(ms)	5	8	9	10	10	12	10	11	12	12

在不同策略数量情况下,将算法 1 与文献[16]中的静态冲突检测算法就检测准确性和时间效率进行对比,结果如图 4 和图 5 所示。需要说明的是,文献[16]的算法仅考虑了检测环节,而策略分析过程人工完成,本文算法 1 则是从策略分析到一致性冲突检测的完整过程。

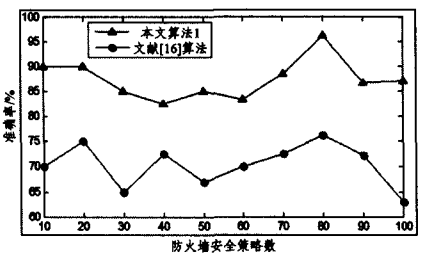

图 4 两种算法的检测准确率

从图 4 可知,作为防火墙安全性能保证的安全策略,在其一致性冲突检测方面,利用本文算法的检测结果准确率明显高于对比算法的准确率,本文算法在实际运用中更具有应用价值。

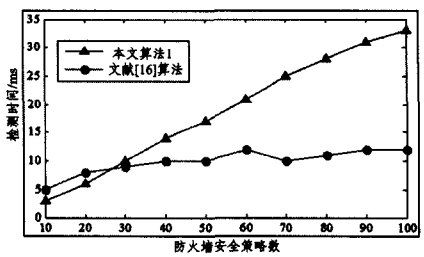

图 5 两种算法的运行时间

从图 5 可知,在策略数较少时,本文算法从策略分析到冲突检测的运行时间比文献[16]中仅考虑检测环节的时间还要短,但随着策略数量的增加,算法 1 的运行时间也呈递增的趋势。尽管进行 100 条策略规则一致性检测的时间大约 30ms,但本文算法整合了策略语义特征提取、相似度计算和一致性检测等过程,所以其仍有可取之处。

(下转第 197 页)

[3] Gedik B, Liu Ling. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms [J]. IEEE Transactions on Mobile Computing, 2008, 7(1): 1-18

[4] Gruteser M, Grunwald D. Anonymous usage of locationbased services through spatial and temporal cloaking [C] // ACM/USENIX MobiSys. 2003: 1-8

[5] Lu Zhao, Lin Xin. A Data Privacy-Oriented Multi-Parities Location Collect Scheme in Location Based Services [C] // 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology. 2009: 964-969

[6] Ghinita G, Kalnis P, Skiadopoulos S. PRIVE: anonymous location based queries in distributed mobile systems[C] // Proceedings of International Conference on World Wide Web (WWW'07). Banff, Alberta, Canada, 2007: 1-10

[7] Tang Ming, Wu Qian-hong, Zhang Guo-ping, et al. A New Scheme of LBS Privacy Protection [C] // 5th International Conference on WiCom'09. 2009: 1-6

[8] Gallery E, Mitchell C J. Trusted Mobile Platform[M] // Foundations of Security Analysis and Design IV. Springer, 2007: 282-323

(上接第 169 页)

与其他策略静态语义处理的实验对比表明，本文算法具有很高的准确率且消耗时间少，即时间复杂度小，因此实用性强。

结束语 安全策略语义的一致性检测效果直接影响到安全策略的正确执行，并体现安全策略对网络与信息安全的保障能力是否有效。因此保证安全策略语义一致性至关重要。本文在研究静态安全策略语义冲突的基础上提出一种语义相似度计算模型，利用本体提取特征因子，在计算其语义相似度后，对安全策略进行处理，对是否具有冲突的安全策略进行不同的标记，来作为管理者后期改进的目标，从而保证安全策略规则库的一致性。该模型和算法计算简单且有效，检测结果具有很高的准确率，使得安全策略对网络与信息具有很好的安全保障能力。本文仅研究了一般网络环境下的静态安全策略语义一致性检测，进一步的工作是优化算法的过程以提高其时间效率，以及策略执行环节中的动态检测研究。

参 考 文 献

[1] David B, Vincent J, Felix K, et al. Enforceable security policies revisited [J]. ACM Transactions on Information and System Security, 2013, 16(1): 31-56

[2] Mohan A, Blough D M, Kurc T, et al. Detection of conflicts and inconsistencies in taxonomy-based authorization policies [C] // Proceedings of the IEEE International Conference on Bioinformatics and Biomedicine. Atlanta, GA, 2011: 590-594

[3] Li Zang, Chu Chao-hsien, Yao Wen. A semantic authorization model for pervasive healthcare [J]. Journal of Network and Computer Applications, 2014, 38: 76-87

[4] 李瑞轩，鲁剑锋，李添翼，等. 一种访问控制策略非一致性冲突消解方法[J]. 计算机学报，2013，36(6)：1210-1223
Li Rui-xuan, Lu Jian-feng, Li Tian-yi, et al. An approach for resolving inconsistency conflicts in access control policies [J]. Chinese Journal of Computers, 2013, 36(6): 1210-1223

[5] Bao Yi-bao, Yin Li-hua, Fang Bin-xing, et al. A novel logic-based automatic approach to constructing compliant security policies [J]. Science China: Information Sciences, 2012, 55(1): 149-164

[6] 包义保，殷利华，方滨兴，等. 基于良基语义的安全策略表达与验证方法[J]. 软件学报，2012，23(4)：912-927
Bao Yi-bao, Yin Li-hua, Fang Bin-xing, et al. Approach of security policy expression and verification based on well-founded semantic [J]. Journal of Software, 2012, 23(4): 912-927

[7] Basile C, Cappadonia A, Lioy A. Network-level access control policy analysis and transformation [J]. IEEE/ACM Transactions on Networking, 2012, 20(4): 985-998

[8] 沈国华，张伟，黄志球，等. 基于描述逻辑的特征语义建模及验证[J]. 计算机研究与发展，2013，50(7)：1501-1512
Shen Guo-hua, Zhang Wei, Huang Zhi-qiu, et al. Description-logic-based feature modeling and verification [J]. Journal of Computer Research and Development, 2013, 50(7): 1501-1512

[9] 王腾，朱青，王珊. 基于语义相似度的 Web 信息可信分析[J]. 计算机学报，2013，36(8)：1668-1681
Wang Teng, Zhu Qing, Wang Shan. Fact statements verification based on semantic similarity [J]. Chinese Journal of Computers, 2013, 36(8): 1668-1681

[10] 程勇，黄河，邱莉榕，等. 一个基于相似度计算的动态多维概念映射算法[J]. 小型微型计算机系统，2006，27(6)：975-979
Cheng Yong, Huang He, Qiu Li-rong, et al. Similarity-based dynamic multi-dimension concept mapping algorithm [J]. Mini-Micro Systems, 2006, 27(6): 975-979

[11] 郑晓洁，张琳. 本体映射中相似度计算的改进[J]. 计算机科学，2013，40(12)：108-112
Zheng Xiao-jie, Zhang Lin. Modification of similarity computation in ontology mapping [J]. Computer Science, 2013, 40(12): 108-112

[12] Kobra E, Amin R D, Mahmoud N. Overlapped ontology partitioning based on semantic similarity measures [C] // Proceedings of the 5th International Symposium on Telecommunications. Tehran, Iran, 2010: 1013-1018

[13] Pirro G. A semantic similarity metric combining features and intrinsic information content [J]. Data & Knowledge Engineering, 2009, 68(11): 1289-1308

[14] Kunal V, Rama A, Richard G. Semantic matching of web service policies[C] // Proceedings of the 2nd International Workshop on Semantic and Dynamic Web Processes. Orlando, USA, 2005: 1-12

[15] Gruber T R. A translation approach to portable ontology specifications [J]. Knowledge Acquisition, 1993, 5(2): 199-220

[16] 倪俊，陈晓苏，刘辉宇，等. 网络安全策略求精一致性检测和冲突消解机制的研究[J]. 计算机科学，2011，38(2)：32-37
Ni Jun, Chen Xiao-su, Liu Hui-yu, et al. Research on network security policy refinement consistency of detection and conflict resolution mechanisms [J]. Computer Science, 2011, 38(2): 32-37