Journal of System Simulation

Volume 29 | Issue 8 Article 9

6-1-2020

Modeling and Analysis of Trust Attack Based on Object-oriented Petri Net

Guangqiu Huang
School of Management, Xi'an University of Architecture and Technology, Xi'an 710055, China;

Bai Lu
School of Management, Xi'an University of Architecture and Technology, Xi'an 710055, China;

Modeling and Analysis of Trust Attack Based on Object-oriented Petri Net

Abstract

Abstract: On the basis of trust attack graph, the object-oriented trust attack Petri net model was put forward, the dynamic model described the attack behaviors among components of trust entity object. *By introducing the object Petri net, the trust attack relations between trust entity objects and components were shown in the Petri net*, simulating the collaborative work between the components. *According to the new trust relation reconstruction rules, a trust attack path inference algorithm was proposed to make the attacker knowing the changes of harmfulness when attacking the components,* thus the attacker could decide the attack direction. *The maximal threat path* which could arrive at an attack goal could be searched out. An experiment shows that the model can describe the dynamic trust entity object attack relations between components, and accurately find the trust attack path in the trust environment.

Keywords

trust, trust attack, object Petri net, trust relation reconstruction, trust attack path

Recommended Citation

Huang Guangqiu, Bai Lu. Modeling and Analysis of Trust Attack Based on Object-oriented Petri Net[J]. Journal of System Simulation, 2017, 29(8): 1702-1711.

第 29 卷第 8 期 系统仿真学报© Vol. 29 No. 8
2017 年 8 月 Journal of System Simulation Aug., 2017

基于对象 Petri 网的信任攻击建模与分析

黄光球，白璐
（西安建筑科技大学管理学院，陕西 西安 710055）

摘要：在信任攻击图的基础上，提出了一种面向对象的信任攻击 Petri 网模型，该模型动态描述了攻击者在信任主体对象部件间的攻击行为。*通过引入对象 Petri 网，使信任主体对象和部件间的信任攻击关系在 Petri 网中展现*，从而模拟仿真了部件间协同工作的场景；*根据重新编写的信任关系重建规则，提出了信任攻击路径推理算法，使攻击者在进行攻击的同时掌握攻击部件的危害度变化*，从而决定进攻方向，找出到达攻击目标的*最大威胁度攻击路径*。最后用实例验证了该模型能够动态描述信任主体对象部件间的攻击关系，并准确找到信任环境中的信任攻击路径。

关键词：信任；信任攻击；对象 Petri 网；信任关系重建；信任攻击路径
中图分类号：TP393.08 文献标识码：A 文章编号：1004-731X (2017) 08-1702-10
DOI: 10.16182/j.issn1004731x.joss.201708009

Modeling and Analysis of Trust Attack Based on Object-oriented Petri Net

Huang Guangqiu, *Bai Lu*
(School of Management, Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: On the basis of trust attack graph, the object-oriented trust attack Petri net model was put forward, the dynamic model described the attack behaviors among components of trust entity object. *By introducing the object Petri net, the trust attack relations between trust entity objects and components were shown in the Petri net*, simulating the collaborative work between the components. *According to the new trust relation reconstruction rules, a trust attack path inference algorithm was proposed to make the attacker knowing the changes of harmfulness when attacking the components,* thus the attacker could decide the attack direction. *The maximal threat path* which could arrive at an attack goal could be searched out. An experiment shows that the model can describe the dynamic trust entity object attack relations between components, and accurately find the trust attack path in the trust environment.

Keywords: trust; trust attack; object Petri net; trust relation reconstruction; trust attack path

引言

随着网络应用的发展，互联网应用给人们的生活、工作带来了极大便利，但人们对网络信任的缺失也成为了影响互联网应用持续发展的主要原因之一。据中国互联网络信息中心(CNNIC)发布的第 35 次《中国互联网络发展状况统计报告》[1]显示，仅 2014 年就有约 46.3%的网民遇到过网络安全问题，其中，账号或密码被盗、消费欺诈所占比例分别为 25.9%和 12.6%。由此可见，信任安全问题的研究十分必要。

“信任管理”[2]是 Blaze M 等人于 1996 年为解决网络安全问题所提出的，并提出了多种信任模型。文献[3]对电子商务应用中分布式的声望管理

收稿日期：2015-09-24 修回日期：2015-12-08；
基金项目：陕西省自然科学基础研究计划(2015JZ010)，陕西省社会科学基金(2014P07)，教育部人文社会科学研究规划基金(15YJA910002)；
作者简介：黄光球(1964-)，男，湖南桃源，博士，教授，研究方向为网络与信息安全。

技术进行研究，利用节点自身的直接证据和其他节点提供的间接证据来评估目标节点的可信性。文献[4]提出一个信任的演化模型，基于节点的动态的行为进行信任的推理演化过程。针对无线网络，相关研究者提出了信任管理的攻击模型[5]和动态信任预测模型[6]，通过扩展模糊逻辑规则预测未来的行为。Li 等[7]利用可扩展反馈聚合覆盖网来增强反馈聚合机制的可扩展性、减少网络风险以及提高系统有效性。文献[8]提出了 SORT 信任机制，利用可用的局部信息构建信任网络。文献[9]建立了形式化的信任评价体系，对具有模糊性的主观信任进行有效地管理。文献[10]先是提出了一种安全协议 SPR，然后在文献[11]中提出 RATrust 模型研究声望信任的度量和推理演化问题，解决声望信任的度量和推理演化过程中的激励问题。文献[12]研究提出了 GoodRep 的攻击模型及其防御机制，从而帮助声誉系统排除 GoodRep 攻击组的干扰。文献[13-14]针对信任环境系统中的弱点，构建了信任攻击模型，后来又利用粗糙集理论，将信任环境中的信任主体按照属性划分等价类，从而快速搜索攻击图，找出最大威胁的攻击路径。文献[15]则基于多项式主观逻辑提出了扩展信任传播模型。

以上的模型均在各自领域得到应用，但仍有不足和局限。目前为止，信任攻击模型主要是由攻击图建立，虽然可以反应攻击者的各种攻击行为，但无法描述并发的协同式攻击，当节点信息量过大时，易产生状态节点的空间爆炸问题。并且模型中提到的信任关系传递闭包算法虽找到了所有可能的攻击路径，但由于不是按照攻击的时间顺序进行的，难以实现准确的信任攻击仿真。因此，本文将对象 Petri 网引入到信任攻击模型中，建立了面向对象的信任攻击 Petri 网，该模型将信任关系网转化成信任关系 Petri 网，增强了对攻击过程和网络状态的描述能力，利用重写的信任关系重建规则构建信任攻击 Petri 网，预测出可能的攻击路径，准确形象地模拟了信任攻击的场景，为安全政策的制定提供依据。

1 信任关系 Petri 网 TP 的构建方法

1.1 信任关系网转换 Petri 网

在信任关系网 *TN*(Trust Relation Net)中，每个节点代表信任主体的部件，用●表示主动节点，用○表示被动节点，用⊗表示中间节点，每条弧代表各部件之间的信任关系，弧上的数字为部件间的信任度。

将信任关系网转化为信任关系 Petri 网，用 Petri 网表示信任攻击中的结构以及逻辑关系，即用变迁 t 表示主体部件，库所 p 表示部件间的信任关系，弧 f 表示各部件间的信任关系。

为了使 Petri 网能动态表示信任攻击中的攻击路线和权限提升情况，制定如下扩充规则：

1. 为没有输入或输出库所的变迁添加输入或输出库所，这类库所属于部件关系库所；

2. 对于有弱点的部件，为其变迁添加输入库所表示弱点库所，用实心圆●表示；

3. Petri 网中的弧扩展为两种，实线弧既可表示攻击路径，又可表示部件间授权路径，虚线弧只能表示部件间授权路径。其中，由信任关系网转换过来的弧均为实线弧，在使用信任关系盗用规则时会出现虚线弧；

4. 根据弱点规则，为缺少约束权限限制的变迁添加约束关系库所。

1.2 信任关系 Petri 网命名规则

根据以上步骤，实现信任关系 Petri 网的转换。基于以上的 Petri 网，现制定信任关系 Petri 网命名规则：

1. 在信任关系 Petri 网中，变迁表示信任主体部件，如部件 a 记作 t_a；

2. 在部件关系库所中，从部件 a 到部件 b 之间的信任关系库所记作 p_{ab}，而从部件 a 到部件 b 之间的约束信任关系库所记作 p_{abi}，(i=1,2,...)，转化过程中为部件 a 添加的输入库所记为 p_{aS}，为部件 b 添加的输出库所记为 p_{bD}；

3. 在弱点库所中，部件 a 的弱点库所记为 p_a。

DOI: 10.16182/j.issn1004731x.joss.201708009

第 29 卷第 8 期 系统仿真学报 Vol. 29 No. 8
2017 年 8 月 Journal of System Simulation Aug., 2017

2 面向对象信任攻击 Petri 网模型的构建方法

2.1 对象 Petri 网

对象 Petri 网[16]是面向对象技术与 Petri 网相结合的产物，它将目标系统映射为一个相互协作的对象，并用 Petri 网来描述各个对象的行为以及对象之间的通信关系。利用对象的封装和继承等特性简化了模型，增强了其可重用性以及可维护性。

在信任环境中包含着多个信任主体，而不同类型的信任主体具有不同的部件和关系，在环境中处于不同的地位。因此，在信任攻击建模过程中，以信任主体为单位进行分类，对不同类型的信任主体建立抽象的类描述，通过 Petri 网描述信任环境中的动态行为和逻辑关系，大大降低了模型描述的复杂性，具体定义如下。

2.2 模型框架定义

定义 1 将信任环境系统定义为一个五元组有限自动机模型：

$$SYS=(S,S_0,\tau,S_{\text{authorized}},S_{\text{unauthorized}})$$

式中：S 代表信任环境系统的所有状态集合；S_0 代表该系统的初始状态集合；$\tau=S\times S$ 是该系统的状态变迁规则；$S_{\text{authorized}}\subseteq S$ 为信任已获取状态；$S_{\text{unauthorized}}\subseteq S$ 为信任未获取状态。这里的信任已获取状态与信任未获取状态是不同的信任主体根据不同需要及相关业务需求决定的，其满足基本关系：$S_{\text{authorized}}\cup S_{\text{unauthorized}}=S$，$S_{\text{authorized}}\cap S_{\text{unauthorized}}=\varnothing$，并且满足满射关系：$S_{\text{authorized}}\cup S_{\text{unauthorized}}\to S$。

定义 2 信任主体类是指在信任环境中具有相同属性和方法的信任主体的抽象，是每一个信任主体信息的封装体，结构定义如下：

Class Trust_Agent{

<attr,vid,C,Cr>；//部件，用来描述信任主体的信息(如提供的服务、应用程序、用户、文件等)，其中，*attr* 表示部件名；*vid* 为部件弱点；*C* 为部件的信任攻击复杂度，*Cr* 为部件在信任主体中的关键度

ATR；//信任主体对象部件间的关联关系

Ir；//信任主体对象性质

}

定义 3 信任主体对象部件间的关联关系 *ATR* (Access and Trust Relation)为一个二元组：

$$ATR=<AR,TR>$$

式中：*AR*(Access Relation)为信任环境中信任主体对象部件间的连接关系；*TR*(Trust Relation)为部件间的信任关系。用谓词公式 $Q(X)$来表示，其中 Q 为谓词，X 为参数，则有以下形式：

AR 记录形式为 $AccessR(O_i,attr_a,O_j,attr_b,r)$,表示信任主体 O_i 的部件 $attr_a$ 与信任主体 O_j 的部件 $attr_b$ 间的连接关系 $r\in Relation$={Y,N}。

TR 记录形式为 $TrustR(O_i,attr_a,O_j,attr_b,tr)$,表示信任主体 O_i 的部件 $attr_a$ 与信任主体 O_j 的部件 $attr_b$ 间的信任关系为 $tr\in Trust$={None-trusted, Trusted,Good-trusted,Very-trusted,Fully-trusted} ∪ { Take,Grant,Pervade}，其中，None-trusted、Trusted、Good-trusted、Very-trusted、Fully-trusted 分别表示不信任、信任、较信任、很信任和完全信任，且信任级别满足：None-trusted<Trusted<Good-trusted <Very-trusted<Fully-trusted,其中，Take、Grant、Pervade 为用于描述信任关系变化的特殊信任度。

定义 4 信任关系 Petri 网 *TP*（Trust relation Petri nets）为一个八元组：

$$TP=(O,P,T,F,Vid,Tr,C,H)$$

式中：O={O_1,O_2,O_3,...,O_N}是信任环境中信任主体的实例化对象集合，N 是信任主体对象的个数；P=$Pv\cup Pr$ 是一个库所的动态集合，并且弱点库所 Pv={p_1,p_2,p_3,...}表示部件弱点的状态集，部件关系库所 Pr={p_{12},p_{13},p_{14},...,p_{ij},...} ∪ {p_{121},p_{122}, p_{123},...,p_{ij1},p_{ij2},...} ∪ {p_{1S},p_{2S},...,p_{iS}} ∪ {p_{1D},p_{2D},...,p_{iD}} 表示部件间信任关系的状态、约束条件集和部件的输入、输出状态集，i,j=1,2,3,...,n 且 $i\neq j$；T={$O_1.t_1$，$O_1.t_2$，$O_1.t_3$，...，$O_2.t_i$，$O_2.t_{i+1}$,...,$O_N.t_{n-1}$,$O_N.t_n$}是一个变迁的有限集合，其中变迁 $O_i.t_j$ 表示信任主体对象 O_i 的具体部件 t_j，n 为信任环境中信任主体的部

件总数，并且 $P\bigcup T\neq\varnothing$，$P\bigcap T=\varnothing$；$F$ 为有向边的集合，表示部件间的连接关系，且 $F=P\times T\bigcup T\times P$；$Vid=\{vid_1,vid_2,...,vid_n\}$与 Pv 中的元素一一对应，表示部件的弱点标识；$Tr=\{tr_{12},tr_{13},tr_{14},...,tr_{ij},...\}\bigcup\{tr_{121},tr_{122},tr_{123},...,tr_{ij1},tr_{ij2},...\}$与 Pr 中的元素部分对应，表示各部件间的信任度，Pr 中的输入库所和输出库所除外，只有当部件的输入库所或输出库所在信任攻击中转换成信任关系状态库所，才会被标识信任度，其中 $tr_{ij}\in Trust=${None-trusted, Trusted,Good-trusted,Very-trusted,Fully-trusted} ∪ { Take,Grant,Pervade}；$C=\{c_{12},c_{13},c_{14},...,c_{ij},...\}$为部件攻击复杂度，用于评估信任攻击的难易程度；$H=\{h_1,h_2,h_3,...,h_i,...\}$为部件危害度，表示被攻击部件变迁在整个信任环境中的受危害程度，与变迁 T 一一对应；其中，部件间的约束关系与其部件间的初始信任关系具有共同的 C，即 p_{ij} 与 p_{ij1} 的 c_{ij} 相同，但信任度不同，分别为 tr_{ij} 和 tr_{ij1}。

定义 5 将信任攻击 Petri 网定义 *TAP*(Trust Attack Petri net)为一个六元组：

$$TAP=(TP,RRP,S_0,S_{\text{authorized}},V_{\text{attack}},RT)$$

式中：*TP* 为信任环境中的信任关系 Petri 网；*RRP*={TakeP，GrantP，PervadeP}∪*VRRP*⊆*S*×*S* 是改写后的信任关系重建规则(Trust Relation Reconstruction Rule Petri nets)，用来表示信任环境系统中状态转移、信任关系传递以及信任攻击的过程；V_{attack}=(*A*,*t_A*,*TG*,*t_TG*)为攻击者和攻击目标的集合，*A* 代表攻击者所在变迁的输入库所，*t_A* 为攻击者所在的变迁，*TG* 代表攻击目标变迁的输出库所，*t_TG* 代表攻击目标变迁；*RT*=(*path*,*length*,*AT*,*RK*)记录信任攻击过程中的路径，*path*=(t_A, $dt_1,O_i.t_j,dt_2,...,dt_{\text{length}},t\_TG$)记录信任攻击中各路线所经过的部件变迁和触发变迁时的各指标集合，其中，当攻击者在 $O_p.t_i$ 进行信任攻击经由库所 p_{ij} 触发变迁 $O_q.t_j$ 时，$dt_k=<p_{ij},tr_{ij},c_{ij},h_j,\xi_k>$，$p_{ij}$ 为信任关系状态集，tr_{ij} 为信任度，c_{ij} 为部件攻击复杂度，h_j 为部件危害度，ξ_k 表示由初始库所 *A* 触发变迁 $O_q.t_j$ 时的部件威胁度，具体计算方法将在定义 7 中介绍，*length*∈[0,*Maxstep*]记录每条攻击路线的长度，其中，*Maxstep* 为信任环境中最大攻击长度，*AT*(Attack Threaten)为信任攻击所在路径的威胁度；*RK*=(*number*,*rank*)记录攻击路径总条数和威胁度排名。

定义 6 将信任攻击路径威胁度 *AT* 定义成一个二元组：

$$AT=<C,H>$$

式中：*C* 用来描述信任攻击的难易程度；*H* 表示攻击者进行攻击时对部件节点造成的危害，*H*=<*SF*,*NC*,*NI*>。以下是威胁度各指标的具体量化方法。

(1) 部件攻击复杂度 *C*(Complexity)根据文献[17]提出的弱点攻击复杂性的分级标准，量化为 7 个等级 E1-E7，*C*∈[0,1]。部件攻击的复杂度越低，越容易被广泛利用，对信任环境的安全威胁越大。

(2) 部件危害度 *H*（Harmfulness）由 *SF*(Safety Factor)、*NC*(Network Correlation)和 *NI*(Network Importance)共同决定，其中 *SF* 的量化需结合信任攻击过程中变迁 $O_i.t_j$ 的弱点状态来综合考量，具体表示方法如下：

$$SF(O_i.t_j)=\begin{cases}0 & \text{若变迁}O_i.t_j\text{不存在弱点}\\ SubT(vid_j) & \text{若变迁}O_i.t_j\text{存在弱点}vid_j\end{cases}$$

式中：*SF*∈[0,1]，且 $SubT(vid_j)$ 表示部件变迁 $O_i.t_j$ 的弱点 vid_j 被利用后所能盗取的信任度与当前信任度的级别差。

NC 表示了部件变迁在信任环境中的关联度，部件变迁的关联度越高，就越容易被攻击或者被攻击者利用，因此对信任环境的威胁性也就越大。具体的计算公式如下：

$$NC(O_i.t_j)=\frac{count(F(O_i.t_j))}{\sum_{p=1}^{N}\sum_{q=1}^{n}[count(F(O_p.t_q))]}$$

式中：$count(F(O_i.t_j))$ 表示与部件变迁 $O_i.t_j$ 相关联的连接弧的条数，这其中不包括约束库所和弱点库所所连接的弧。

NI 表示被攻击部件的重要程度，是一个二元组 *NI*=<*Ir*,*Cr*>。参照文献[18-19]对各类资产价值级

https://dc-china-simulation.researchcommons.org/journal/vol29/iss8/9
DOI: 10.16182/j.issn1004731x.joss.201708009

第 29 卷第 8 期 系统仿真学报 Vol. 29 No. 8
2017 年 8 月 Journal of System Simulation Aug., 2017

别的划分，将信任主体对象的性质 Ir 和主体对象部件的关键度 Cr 具体量化。

由以上的量化方法，可以得出对主体对象部件经行信任攻击时的所在路径的危害度，具体计算方法如下：

$$H(O_i.t_j)=a_1SF+a_2NC+a_3(b_1Ir+b_2Cr)$$

式中：a_1、a_2、a_3、b_1、b_2 为各指标所占的权重，a_1、a_2、a_3、b_1、$b_2\geqslant 0$，$a_1+a_2+a_3=1$，$b_1+b_2=1$，可以根据实际情况具体量化。

定义 7 若 $t_1,t_2,t_3,...,t_l$ 为 $path$ 上所经过的部件变迁，则由初始变迁到触发变迁 $O_q.t_l$ 时所经路径 $path$ 的部件威胁度 ξ 计算方法如下：

$$\xi=\exp(-\sum_{i=1}^{l-1}c_i)(\alpha(1-c_l)+\beta h_l)$$

式中：α、β 为部件攻击复杂度和部件危害度两指标所占的权重，α、$\beta\geqslant 0$ 且 $\alpha+\beta=1$。$\exp(-\sum_{i=1}^{l-1}c_i)$ 为路径复杂度影响因子，$\sum_{i=1}^{l-1}c_i$ 表示攻击者由初始变迁到达目标变迁前的总复杂度。当总复杂度变大时，复杂度影响因子的值就会变小，攻击者选择该路径的概率就越低，该部件的威胁度也就越小。

定义 8 信任攻击路径威胁度 AT 为路径复杂度影响因子与攻击路径上每个信任部件威胁度和的乘积，即：

$$AT=\exp(-\sum_{i=1}^{l-1}c_i)\sum_{j=1}^{l}(\alpha(1-c_j)+\beta h_j)$$

2.3 重写信任关系重建规则

参照文献[13]可知，信任关系重建规则由两部分构成：(1) 信任关系盗用规则，用来表示因信任关系被盗用而导致信任度的提升、信任关系传递以及渗透与扩散的过程；(2) 弱点利用规则，用来表示因信任环境系统的弱点被利用所导致的信任关系状态的变化。根据以上的基本思想，重写信任关系重建规则，使它可以应用于 Petri 网中。

2.3.1 信任关系盗用规则

TakeP 规则：假设变迁 t_x、t_y 和 t_z 表示任意 3 个独立部件，库所 p_{xy}、p_{xy1} 和 p_{yz} 为部件间的信任关系和约束关系，p_y 为变迁 t_y 的弱点库所，其中，部件 x 为主动攻击部件。若 tr_{xy} 表示 t_x 到 t_y 的信任度级别为 $\gamma(\gamma\in Trust)$，tr_{yz} 表示 t_y 到 t_z 的信任度级别为 $\alpha(\alpha\in Trust)$，且 t_y 存在一个特殊弱点，p_y 中含有托肯，则对部件 y 进行攻击，使 x 到 y 信任度级别被提升为 $t(t\in Trust,\ t>\gamma)$，并增加从 t_x 到 p_{xy1} 的实线弧，从而增加了从 t_x 到 t_z 信任度级别为 α 的库所 p_{xz} 和两条虚线弧。具体过程如图 1 所示。

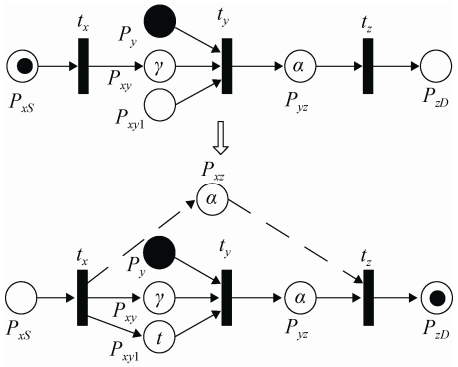

图 1 TakeP 规则
Fig. 1 TakeP Rule

TakeP 规则可以描述为部件 x 利用部件 y 的弱点进行攻击，盗取了到部件 z 的信任度为 α 的信任关系。在这一攻击过程中，攻击路线为 $x\rightarrow y\rightarrow z$。

GrantP 规则：假设变迁 t_x、t_y 和 t_z 表示任意 3 个独立部件，库所 p_{xy} 和 p_{xz} 为部件间的信任关系，p_x 为变迁 t_x 的弱点库所，其中，部件 y 为主动攻击部件。tr_{xz} 表示 t_x 到 t_z 的信任度为 $\alpha(\alpha\in Trust)$，且变迁 t_x 存在一个特殊弱点，若变迁 t_y 想要获得到达 t_z 的权限，则对部件 x 进行攻击，变迁 t_y 获得 t_x 的授权，且 tr_{xy} 的信任度为 $g(g\in Trust)$，从而导致增加一条自库所 p_{yD} 到变迁 t_z 的虚线弧，且 p_{yD} 的信任度为 α。具体过程如图 2 所示。

GrantP 规则可以理解为部件 x 因为自身的特殊弱点(主观弱点，如轻信他人，设置弱密码等)，将到部件 z 的信任度级别为 α 的信任关系转移给了部件 y。特别需要注意的是，t_x 到 t_y 的路径表示的为授权路线，而实际的攻击路线与之相反。因此，在这一攻击过程中，攻击路线为 $y\rightarrow x\rightarrow z$。

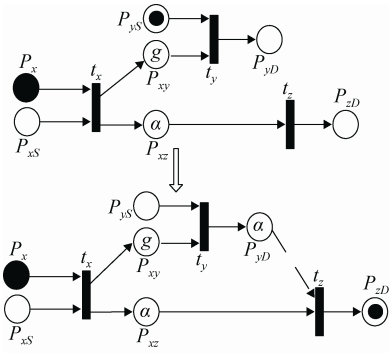

图 2 GrantP 规则
Fig. 2 GrantP Rule

PervadeP 规则：假设变迁 t_x、t_y 和 t_z 表示任意 3 个独立部件，库所 p_{xz} 和 p_{yz} 为部件间的信任关系，p_z 为变迁 t_z 的弱点库所，其中部件 x 为主动攻击部件。如果 tr_{xz} 表示 t_x 到 t_z 的信任度为 $\gamma(\gamma\in Trust)$，tr_{yz} 表示 t_y 到 t_z 的信任度为 $\alpha(\alpha\in Trust)$，且变迁 t_z 存在一个特殊弱点，则对变迁 t_z 进行攻击，使得 t_y 到 t_z 的信任关系被逆转为 $p(p\in Trust)$，并添加一条自 p_{zD} 到 t_y 的实线弧，从而导致 t_x 到 p_{yS} 增加了一条虚线弧且 p_{yS} 的信任度级别为 $\beta(\beta=\alpha$ 或 $\beta=\gamma)$。如图 3 所示。

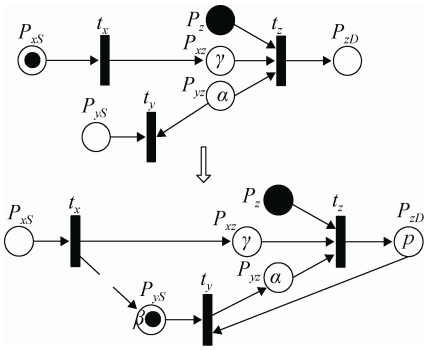

图 3 PervadeP 规则
Fig. 3 PervadeP Rule

PervadeP 规则可以看作是部件 x 利用其自身与子部件 z 的信任关系以及部件 y 与子部件 z 之间的信任关系，对部件 z 的弱点进行攻击，从而获取了对部件 y 的信任度为 β 的信任关系，实现了信任关系向高一级渗透并向其他相关联部件扩散的目的。在这一攻击过程中，攻击路线为 $x\rightarrow z\rightarrow y$。

重写的信任关系盗用规则中，攻击者为获取更高级别的信任度，利用中间被攻击部件的弱点盗取信任，从而达到目的。在该过程中库所产生了特殊信任度 t、g、$p(t$、g、$p\in Trust)$，它们分别是 Take、Grant、Pervade 的简写，而该库所对应的攻击复杂度与两部件变迁间原先的攻击复杂度相同。

2.3.2 弱点利用规则

定义 9 将弱点利用规则 *VRRP*(Vulnerability utilizing Rule)定义为一个四元组：

$$VRRP_{vid}=(VID,S_{\text{precond}},S_{\text{postcond}},V_{\text{active}})$$

其中：*VID* 为信任关系 Petri 网中某部件变迁 $O_i.t_j$ 的弱点标识 vid_j；S_{precond}=(P_{precond} , T_{precond} ; F_{precond}, Tr_{precond})，表示利用弱点 *VID* 进行信任攻击的前提条件；S_{postcond}=(P_{postcond} , T_{postcond} ; F_{postcond}, Tr_{postcond})，表示利用了弱点 *VID* 之后信任关系 Petri 网的状态；V_{active} 为主动攻击部件的集合。

定义 10 将信任关系重建规则的一次利用过程定义为一个五元组：

$$USE=(O_i,t_j,vid_j,RRP,V_a)$$

其中：信任主体对象 O_i 的部件 t_j 有弱点 vid_j；*RRP* 为{TakeP，GrantP，PervadeP}和 $VRRP_{vid}$ 的信任关系重建规则库；V_a 为 V_{attack} 的一个子集。

3 *TAP* 推理算法

根据以上模型的定义、转化规则、命名规则以及推理规则，得到以下 *TP* 生成算法和信任攻击路径推理算法。

3.1 *TP* 生成算法

算法：*TN_TP*

输入：网络拓扑结构图，网络部件信息，弱点信息，部件间关联信息

输出：*TP*

1. 根据定义 1，搭建信任环境 *SYS*，初始化信任主体对象 $O_1,O_2,O_3,...,O_N$；

2. 将网络拓扑结构信息转化成信任关系网 *TN*；

3. 根据信任关系转化规则，将信任关系网 *TN* 转化成相应的信任关系 Petri 网，并根据命名规则将对相应的库所和变迁进行命名，建立动态库所集 *P*、有限变迁集 *T* 以及有向边集合 *F*；

4. 根据弱点规则，向已建好的信任关系 Petri 网中添

DOI: 10.16182/j.issn1004731x.joss.201708009

第 29 卷第 8 期 系统仿真学报 Vol. 29 No. 8
2017 年 8 月 Journal of System Simulation Aug., 2017

加约束库所；

5. 根据网络部件信息，弱点信息，部件间关联信息，建立弱点集 *Vid*，信任度集合 *Tr*；

6. 根据定义 6，计算量化部件攻击复杂度 *C* 和部件危害度 *H*。

上述算法中，利用网络拓扑结构图，网络部件信息，弱点信息，部件间关联信息等构建了信任关系 Petri 网 *TP*，计算量化求得了部件攻击复杂度和部件危害度。利用以上结果和推理规则，可以得到信任攻击 Petri 网和攻击路径，具体的路径推理算法如下。

3.2 信任攻击路径推理算法

算法：*RT_TAP*

输入：信任关系 Petri 网 *TP*，Maxstep

输出：信任攻击 Petri 网 *TAP* 和攻击路径 *RT*

1. 添加攻击对象：将攻击对象和攻击目标记录在 V_{attack} 中，向 V_{attack} *.A* 中放入托肯。

2. 初始化攻击参数：

Maxstep=20；//为攻击长度设定合理值，这里设为 20

numb=1；//记录攻击路线条数

RT(numb).path={*t_A*} ， *RT*(numb).length=0 ， *RT*(numb).*AT*=0；//初始化信任攻击路径

len=0；//用于记录循环次数，即攻击长度

3. 根据信任关系重建规则对信任主体对象部件进行攻击：

While(！((*len*<=Maxstep AND *RT* 记录的全部路径中一部分到达攻击目标，另一部分为 NULL) OR (*len*>Maxstep))){

m=numb；//*m* 用来记录攻击路线条数

构建攻击队列 *VS*_queue；

For(*k*=1；*k*<=*m*；*k*++){

n=0；//*n* 用来记录当前攻击变迁 t_s 的立即可达变迁个数

If(*RT*(*k*).path！={NULL} AND *RT*(*k*)没有到达攻击目标){

搜索 *RT*(*k*).path 中的当前攻击部件变迁 t_s 的 *n* 个立即可达变迁；

If(*n*≠0){在原路径基础上添加 *n*–1 条攻击路径，并使新增加的攻击路径 *RT* 与当前攻击部件变迁 t_s 的 *RT* 相同，将这 *n* 个变迁及所对应的攻击线路 *RT* 加入到 *VS*_queue；

}Else{向队列 *VS*_queue 中加入 t_0 及 *RT*(k)；//t_0 代表不能到达攻击目标}

}Else If(*RT*(*k*).path！={NULL} AND *RT*(*k*)到达攻击目标){

向队列 *VS*_queue 中加入 *t_TG*；

}Else{向队列 *VS*_queue 中加入 t_0 及 *RT*(*k*)；}}//增加攻击路线

For(*k*=1；*k*<=numb；*k*++){

取出 *VS*_queue 中对应 *RT*(*k*)的一个被攻击变迁作为 *cur_VS*；

If(*cur_VS*！=t_0){//攻击者变迁 V_a 为 t_s，被攻击变迁 *cur_VS* 为 t_d

If(变迁 *cur_VS* 有弱点 vid_d){

If((*cur_VS* 模式与弱点利用规则 $VRRP_{vid_d}$，S_{precond} 匹配成功)OR(*cur_VS* 模式与信任关系盗用规则匹配成功)){

$USE=(O_i, cur\_VS, vid_d, RRP, V_a)$；//根据 $VRRP_{vid_d}$ 中的规则或者匹配的信任关系盗用规则，向 *TP* 中添加弧、库所以及复杂度 c_{sd}、信任度 tr_{sd} 和攻击方式 g_{sd}

触发变迁 *cur_VS*，向后移动托肯；

RT(*k*).length++；//增加攻击长度

根据定义 7，计算 ξ_{length}；

$dt_{\text{length}}=(p_{sd}, tr_{sd}, c_{sd}, h_d, g_{sd}, \xi_{\text{length}})$；

RT(*k*).path=*RT*(*k*).path+ dt_{length} +*cur_VS*；//添加攻击路径

}Else{//有弱点，但模式匹配不成功的路径

RT(*k*).length=*0* ； *RT*(*k*).*path*={NULL} ；

Break；}

}Else If(满足变迁 *cur_VS* 触发条件){

触发变迁 *cur__VS*，向后移动托肯；

RT(*k*).*length*++；计算 ξ_{length}；

$dt_{\text{length}}=(p_{sd}, tr_{sd}, c_{sd}, h_d, g_{sd}, \xi_{\text{length}})$；

RT(*k*).path=*RT*(*k*).path+ dt_{length} +*cur_VS*；//添加攻击路径

}Else{//无弱点，又不满足攻击条件的路径

RT(*k*).length=*0*; *RT*(*k*).*path*={NULL}; Break; }
}Else{//攻击路径不通的路线跳出循环
RT(*k*).length=*0*; *RT*(*k*).path={NULL};
Break; }}//对每一条攻击路径进行更新
len++; }

4. 整理攻击路线，剔除未完成和路径不通的路线;
5. 根据定义 8 计算攻击路线的攻击威胁度并排名;
6. 输出 *RT*

3.3 *TAP* 模型系统分析框架

网络系统→配置扫描工具→攻击图→Petri 网(*TP* 模型)→动态分析(信任关系重建规则)→*TAP* 模型→攻击者的攻击路径→最佳攻击路径

4 实例验证

为了说明信任攻击模型的建立和分析，由拓扑结构图生成了相应的信任关系网，如图 4 所示。图中，网络为交换网络，共有 5 台计算机，其中，IP1 上开放 Apache、HTTP 和 TELNET 服务，IP2 和 IP4 均为内部用户，IP3 上提供 SSH、MySQL 和 FTP 服务，IP4 上运行着 SMB 服务。假设攻击者 Eve 的攻击目标是要获得 IP4 上 File 的访问权限。

构建信任关系对象，其中：O_1 代表 Eve，O_2 代表 IP1，O_3 代表 IP2，O_4 代表 IP3，O_5 代表 IP4，并且在表 1 中，t_1 与 Eve 对应，t_2 与 IP1 对应，t_3 与 Apache 对应，t_4 与 HTTP 对应，t_5 与 TELNET 对应，t_6 与 IP2 对应，t_7 与 IE 对应，t_8 与 User2 对应，t_9 与 IP3 对应，t_{10} 与 SSH 对应，t_{11} 与 MySQL 对应，t_{12} 与 FTP 对应，t_{13} 与 IP4 对应，t_{14} 与 User1 对应，t_{15} 与 File 对应，t_{16} 与 SMB 对应。信任主体对象部件间属性如表 1。

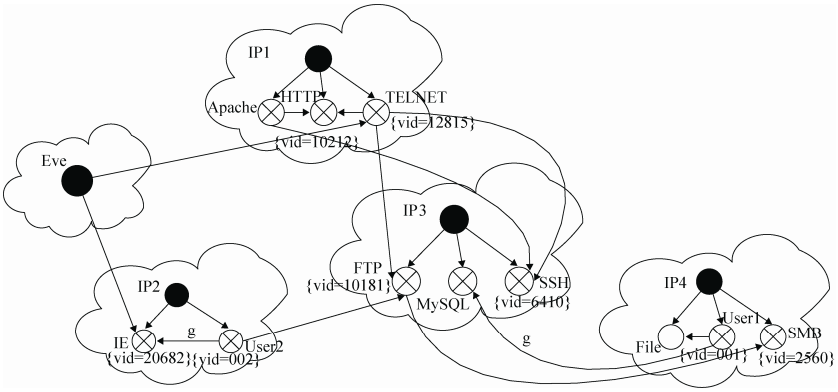

图 4 信任关系网
Fig. 4 Trust relation net

表 1 信任主体对象部件间的属性
Tab. 1 Attribute of trust entity object between components

对象及重要度	部件及关键度	信任关系及攻击复杂度
O_1,0.2	t_1,0.5	Trust$R$(O_1,t_1,O_2,t_5,Good-trusted)；0.05 Trust$R$(O_1,t_1,O_3,t_7,Trusted)；0.1
O_2,0.5	t_2,0.8 t_3,0.5 t_4,0.5 t_5,0.8	Trust$R$(O_2,t_2,O_2,t_3,Fully-trusted)；0.8 Trust$R$(O_2,t_2,O_2,t_4,Fully-trusted)；0.5 Trust$R$(O_2,t_2,O_2,t_5,Fully-trusted)；0.5 Trust$R$(O_2,t_3,O_4,t_{10},Very-trusted)；0.2 Trust$R$(O_2,t_3,O_2,t_4,Very-trusted)；0.1 Trust$R$(O_2,t_5,O_2,t_4,Good-trusted)；0.2 Trust$R$(O_2,t_5,O_4,t_{10},Good-trusted)；0.5 Trust$R$(O_2,t_5,O_4,t_{12},Trusted)；0.6
O_3,0.4	t_6,0.5 t_7,0.5 t_8,0.1	Trust$R$(O_3,t_6,O_3,t_7,Fully-trusted)；0.1 Trust$R$(O_3,t_6,O_3,t_8,Fully-trusted)；0.2 Trust$R$(O_3,t_8,O_3,t_7,Grant)；0.05 Trust$R$(O_3,t_8,O_4,t_{12},Very-trusted)；0.5
O_4,0.5	t_9,0.8 t_{10},0.8 t_{11},0.5 t_{12},0.5	Trust$R$(O_4,t_9,O_4,t_{10},Fully-trusted)；0.2 Trust$R$(O_4,t_9,O_4,t_{11},Fully-trusted)；0.6 Trust$R$(O_4,t_9,O_4,t_{12},Fully-trusted)；0.5 Trust$R$(O_4,t_{12},O_5,t_{16},Good-trusted)；0.6
O_5,0.7	t_{13},0.8 t_{14},0.5 t_{15},0.8 t_{16},0.5	Trust$R$(O_5,t_{13},O_5,t_{14},Fully-trusted)；0.2 Trust$R$(O_5,t_{13},O_5,t_{15},Fully-trusted)；0.6 Trust$R$(O_5,t_{13},O_5,t_{16},Fully-trusted)；0.5 Trust$R$(O_5,t_{14},O_4,t_{11},Grant)；0.2 Trust$R$(O_5,t_{14},O_5,t_{15},Very-trusted)；0.6

第 29 卷第 8 期 系统仿真学报 Vol. 29 No. 8
2017 年 8 月 Journal of System Simulation Aug., 2017

根据信任关系盗取规则和弱点利用规则，利用 *RT_TAP* 算法生成信任攻击 Petri 网 *TAP* 及信任攻击路线 *RT* 如图 5 所示。

在信任攻击过程中，攻击者 Eve 根据扫描得到的弱点对部件进行攻击，如攻击者对 TELNET 上的弱点 12815 进行攻击，即触发变迁 t_5 上的弱点 p_5，获得了更高的攻击权限，即 Eve 对 TELNET 的信任度由 Good-trusted 提升到 Very-trusted，致使信任节点 IP1 上的部件 TELNET 可以访问 IP3 的部件 SSH。但由于 TELNET 提升后的权限不够高，攻击 IP3 上的部件 FTP 的弱点 10181 很难获取更高的权限 $p_{5\ 12\ 1}$，因此，t_{12} 不能通过 t_5 的攻击路径进行触发，即 TELNET 很难利用 FTP 的弱点进行下一步攻击。

根据定义 6 中的量化计算公式，可得到部件的攻击复杂度和危害度。在本例中，威胁度计算公式中的各权重均相等，即 $\alpha=\beta=1/2$，$a_1=a_2=a_3=1/3$，$b_1=b_2=1/2$。根据信任攻击路径推理算法及路径威胁度的计算公式，设定最大攻击路径长度为 10，可以得到 8 条攻击路径，具体如表 2。其中，A=p_{1S}，t_A=$O_1.t_1$，TG=p_{15D}，t_TG=$O_5.t_{15}$。

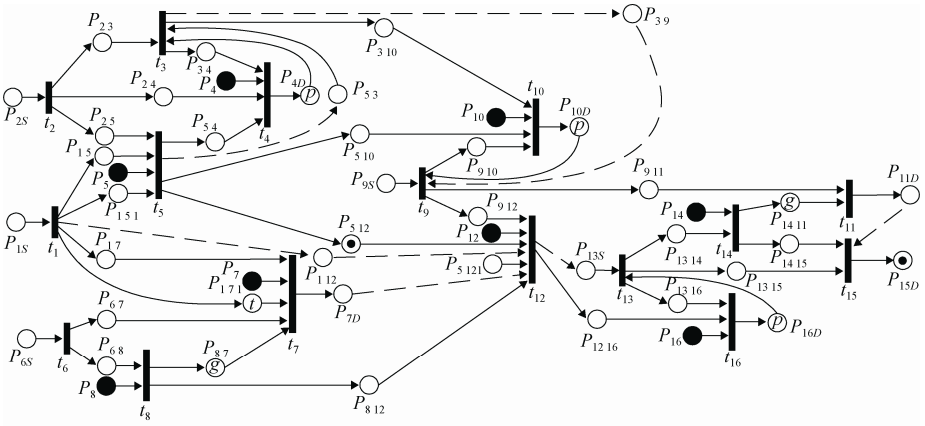

图 5 信任攻击 Petri 网
Fig. 5 Trust attack petri net

表 2 信任攻击路径
Tab. 2 Trust attack path

RT	path	length	AT	RK
1	(t_A,dt_1,$O_2.t_5$,dt_2,$O_2.t_4$,dt_3,$O_2.t_3$,dt_4,$O_4.t_{10}$,dt_5,$O_4.t_9$,dt_6,$O_4.t_{11}$,dt_7,$O_5.t_{14}$,dt_8,t_TG)	8	0.844	(8,1)
2	(t_A,dt_1,$O_2.t_5$,dt_2,$O_2.t_4$,dt_3,$O_2.t_3$,dt_4,$O_4.t_{10}$,dt_5,$O_4.t_9$,dt_6,$O_4.t_{12}$,dt_7,$O_5.t_{16}$,dt_8,$O_5.t_{13}$,dt_9,t_TG)	9	0.415	(8,5)
3	(t_A,dt_1,$O_2.t_5$,dt_2,$O_2.t_4$,dt_3,$O_2.t_3$,dt_4,$O_4.t_{10}$,dt_5,$O_4.t_9$,dt_6,$O_4.t_{12}$,dt_7,$O_5.t_{16}$,dt_8,$O_5.t_{13}$,dt_9,$O_5.t_{14}$,dt_{10},t_TG)	10	0.382	(8,6)
4	(t_A,dt_1,$O_2.t_5$,dt_2,$O_4.t_{10}$,dt_3,$O_4.t_9$,dt_4,$O_4.t_{11}$,dt_5,$O_5.t_{14}$,dt_6,t_TG)	6	0.578	(8,2)
5	(t_A,dt_1,$O_2.t_5$,dt_2,$O_4.t_{10}$,dt_3,$O_4.t_9$,dt_4,$O_4.t_{12}$,dt_5,$O_5.t_{16}$,dt_6,$O_5.t_{13}$,dt_7,t_TG)	7	0.219	(8,7)
6	(t_A,dt_1,$O_2.t_5$,dt_2,$O_4.t_{10}$,dt_3,$O_4.t_9$,dt_4,$O_4.t_{12}$,dt_5,$O_5.t_{16}$,dt_6,$O_5.t_{13}$,dt_7,$O_5.t_{14}$,dt_8,t_TG)	8	0.210	(8,8)
7	(t_A,dt_1,$O_3.t_7$,dt_2,$O_3.t_8$,dt_3,$O_4.t_{12}$,dt_4,$O_5.t_{16}$,dt_5,$O_5.t_{13}$,dt_6,t_TG)	6	0.470	(8,3)
8	(t_A,dt_1,$O_3.t_7$,dt_2,$O_3.t_8$,dt_3,$O_4.t_{12}$,dt_4,$O_5.t_{16}$,dt_1,$O_5.t_{13}$,dt_6,$O_5.t_{14}$,dt_7,t_TG)	7	0.462	(8,4)

从表 2 可以看出，Eve 到 File 的最佳攻击路径 Eve→IP1.TELNET→IP1.HTTP→IP1.Apache→IP3.SSH→IP3→IP3.MySQL→IP4.User1→IP4.File，该路径威胁度为 0.844 0。Eve 通过 TELNET 服务登录到 IP1 上，利用 HTTP 上的畸形密码内存破坏漏洞获得到 Apache 的访问权限，信任度为 Good-trusted，通过 SSH 上的 NULL 字符远程缓冲区溢出漏洞获得到主机 IP3 信任度为 Good-trusted 的权限，伪装成正常用户骗取了 IP4 上 User1 的信任，获得了从 MySQL 上访问 File 的授权，完成攻击任务。

5 结论

本文提出了一种面向对象的信任攻击 Petri 网的攻击模型，该模型利用对象 Petri 网协同性，根据重写的信任关系重建规则和信任攻击路径推理算法动态生成了 *TAP* 模型并给出了威胁度最大的攻击路径，更直观地模拟了攻击者的信任攻击行为和攻击场景。

参考文献:

[1] 中国互联网信息中心. 中国互联网络发展状况统计报告 [EB/OL]. (2015-02-03) [2015-09-24]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/201502/P020150203551802054676.pdf.

[2] Blaze M, Feigenbaum J. Decentralized trust management [C]// Proceedings of the 17th Symposium on Security and Privacy. USA: IEEE Computer Society Press, 1996: 164-173.

[3] Yu B, Singh M P. Distributed reputation management for electronic commerce [J]. Computational Intelligence (S1860-949X), 2002, 18(4): 535-549.

[4] Almenárez F, Marín A, Díaz D, et al. Trust management for multimedia P2P applications in autonomic networking [J]. Ad Hoc Networks (S1570-8705), 2011, 9(4): 687-697.

[5] Yu Y, Li K, Zhou W, et al. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures [J]. Journal of Network and Computer Applications (S1084-8045), 2012, 35(3): 867-880.

[6] Xia H, Jia Z, Li X, et al. Trust prediction and trust-based source routing in mobile ad hoc networks [J]. Ad Hoc Networks (S1570-8705), 2013, 11(7): 2096-2114.

[7] Li X, Zhou F, Yang X. Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management [J]. IEEE Transactions on Parallel and Distributed Systems (S1045-9219), 2012, 23(10): 1944-1957.

[8] Can A B, Bhargava B. SORT: A Self-Organizing Trust Model for Pee-to-Peer Systems [J]. IEEE Transactions on Dependable and Secure Computing (S1545-5971), 2013, 10(1): 14-27.

[9] 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究 [J]. 软件学报, 2003, 14(8): 1401-1408. (Tang Wen, Chen Zhong. Research of Subjective Trust Management Model Based on the Fuzzy Set Theory [J]. Journal of Software (S1000-9825), 2003, 14(8): 1401-1408.)

[10] 胡建理, 周斌, 吴泉源. 一种 P2P 信任管理安全性协议 [J]. 计算机科学, 2011, 38(10): 64-67, 90. (Hu Jianli, Zhou Bin, Wu Quanyuan. Security Protocol for Protecting the P2P Trust Information Management [J]. Computer Science (S1002-137X), 2011, 38(10): 64-67, 90.)

[11] 胡建理, 周斌, 吴泉源. P2P 网络环境下基于信誉的分布式抗攻击信任管理模型 [J]. 计算机研究与发展, 2011, 48(12): 2235-2241. (Hu Jianli, Zhou Bin, Wu Quanyuan. A Reputation Based Attack-Resistant Distributed Trust Management Model for P2P Networks [J]. Journal of Computer Research and Development (S1000-1239), 2011, 48(12): 2235-2241.)

[12] 冯景瑜, 张玉清, 陈深龙, 等. P2P 声誉系统中 GoodRep 攻击及其防御机制 [J]. 计算机研究与发展, 2011, 48(8): 1473-1480. (Feng Jing-yu, Zhang Yu-qing, Chen Shen-long, et al. GoodRep Attack and Defense in P2P Reputation Systems [J]. Journal of Computer Research and Development (S1000-1239), 2011, 48(8): 1473-1480.)

[13] 陆秋琴, 和涛, 黄光球, 等. 信任攻击建模方法 [J]. 计算机工程与应用, 2012, 48(12): 129-135. (Lu Qiuqin, He Tao, Huang Guangqiu, et al. Trust attack modeling [J]. Computer Engineering and Applications (S1002-8331), 2012, 48(12): 129-135.)

[14] 陆秋琴, 和涛, 黄光球, 等. 面向对象粗糙信任攻击威胁感知模型 [J]. 计算机工程与应用, 2012, 48(30): 103-176. (Lu Qiuqin, He Tao, Huang Guangqiu, et al. Object-oriented rough trust attack threat perception model [J]. Computer Engineering and Applications (S1002-8331), 2012, 48(30): 103-176.)

[15] 田俊峰, 吴丽娟. 基于多项式主观逻辑的扩展信任传播模型 [J]. 通信学报, 2013, 34(5): 12-19. (Tian Junfeng, Wu Lijuan. Multinomial subjective logic based extended trust propagation model [J]. Journal of Communications (S1000-436X), 2013, 34(5): 12-19.)

[16] 舒远仲, 刘炎培, 彭晓红, 等. 面向对象 Petri 网建模技术综述 [J]. 计算机工程与设计, 2010, 31(15): 3432-3435. (Shu Yuanzhong, Liu Yanpei, Peng Xiaohong, et al. Survey on object-oriented Petri net modeling [J]. Computer Engineering and Design (S1000-7024), 2010, 31(15): 3432-3435.)

[17] 吴迪, 冯登国, 连一峰, 等. 一种给定脆弱性环境下的安全措施效用评估模型 [J]. 软件学报, 2012, 23(7): 1880-1898. (Wu Di, Feng Dengguo, Lian Yifeng, et al. Efficiency Evaluation Model of System Security Measures in the Given Vulnerabilities Set [J]. Journal of Software (S1000-9825), 2012, 23(7): 1880-1898.)

[18] 陈锋, 刘德辉, 张怡, 等. 基于威胁传播模型的层次化网络安全评估方法 [J]. 计算机研究与发展, 2011, 48(6): 945-954. (Chen Feng, Liu Dehui, Zhang Yi, et al. A Hierarchical Evaluation Approach for Network Security Based on Threat Spread Model [J]. Journal of Computer Research and Development (S1000-1239), 2011, 48(6): 945-954.)

[19] 王玥, 蔡皖东, 段琪. 基于遗传算法的网络脆弱性计算方法 [J]. 系统仿真学报, 2009, 21(6): 1628-1632. (Wang Yue, Cai Wandong, Duan Qi. Computing Vulnerability of Network Based on Genetic Algorithm [J]. Jounal of System Simulation (S1004-731X), 2009, 21(6): 1628-1632.)

DOI: 10.16182/j.issn1004731x.joss.201708009