节点信任度模型的算法研究与设计

马 力[1] 郑国宁[1] 孙 朋[2]

(海军91872部队 北京 102442)[1] (黑龙江省军区指挥自动化站 哈尔滨 150001)[2]

摘 要 节点信任反映的是网络中一个节点对另一个节点行为以及能力的综合评判。首先分析了信任模型现在的研究状况,并在研究本地信任、间接信任、综合信任的基础上,针对节点信任度模型的算法设计,引入概率论的相关知识来计算节点的可信程度。该方法针对节点信任度的多种影响因素,采用身份认证技术进行了节点信任度的模型设计,然后对其算法进行了设计实现。

关键词 节点,信任度,认证,设计

中图法分类号 N94 **文献标识码** A

Research and Design of Arithmetic Based on Node Trustful Model

MA Li[1] ZHENG Guo-ning[1] SUN Peng[2]

(No. 91872 Troops of PLA, Beijing 102442, China)[1]

(Military Command Automation Station in Heilongjiang Province, Haerbin 150001, China)[2]

Abstract Node trust reflects behavior and ability of a node against another node in the network. This article first analyzed the research status of trust model now. The algorithm design for node trust model is based on the research of local trust, recommendation trust, comprehengsive trust. The theory of probalbility knowledge was introduced to calculate nodal credible degree. This method in a variety of factors influencing the node trust, the identity authentication technology design and degree algorithm and degree algorithm was designed and realized.

Keywords Node, Trust, Certification, Design

信任这个概念在绝大多数人意识中都是一个模糊的概念,我们不能保证一个节点通过认证,它就一定是可信的,只能说在多大程度上是可信的。信任是一个复杂的概念,它涉及到诚实、真理、依赖性等多方面的概念,表达了关于人或所提供服务的诚实(Honesty)、可信(Truthfulness)、能力(Completeness)、可靠性(Reliability)等的信仰。而身份认证是保证用户身份合法的唯一途径,是系统安全中最重要的问题。信任度给身份认证一个平台,其结果就是对信任的量化表示。基于身份的认证一般有3种,即本地信任、间接信任和综合信任。本地信任和间接信任引用概率论的相关知识来计算一个节点的可信任程度。混合信任综合本地信任和间接信任并根据不同的系统为两者赋予不同的权重得出节点的最终信任值。只有当认证的结果达到了用户预先设定的阈值,我们才可以接受,这个阈值可以根据不同行业对于安全性的不同要求灵活地选择。

1 信任模型研究现状

对信任模型的研究开始于Blaze等人提出的信任管理的概念,它的基本思想是承认开放系统中安全信息的不完整性,系统的安全决策需要依靠中介机构提供的安全信息。典型的有Marsh的信任模型、基于Dempster-shafer理论的信任模型、Ginsberg模型。随后提出的Beth信任模型引入经验的概念来表述和度量信任关系,它将信任分为直接信任和推荐信任,以对交易结果的期望为基础,根据历史交易的经验计算实体的信任度,并给出了信任度的推导公式。

另外一种信任模型的基础是由A. Adul-Rahman等学者提出的主观信任模型,它从信任的概念出发,根据信任的内容和程度进行划分,从信任的主观入手,给出信任评估数学模型。主观信任是一种主观的判断,具有模糊性,因此主观信任模型的重点在于如何对主观性进行描述和如何对信任度进行评价。徐兰芳等人建立了基于灰色系统理论的主观信任模型,这种信任的评价方法也是基于模糊数学的。

2 信任度的影响因素

影响节点可信度的因素有很多,例如:节点的交易次数成功情况、节点的信誉值、节点的满意度评价、节点交易的衰减因素以及提供资源的类型等。在本文中,节点可信度主要根据节点的历史交易记录和中介节点反馈的可信程度来评定。

(1)节点的交易次数成功情况

网络中,节点的交互次数是影响节点可信性的一个很关键的因素,一个新加入的节点,它的交互次数为0,因此它的可信性处于一个不确定的状态。在这里我们假设两个场景,场景一:假设一个新加入的节点成功进行一次交易,它的交易次数为1,交易成功次数为1,认证概率为100%。场景二:任

马 力(1979—),女,硕士,主要研究方向为数据库与知识库;郑国宁(1970—),男,硕士,主要研究方向为网络安全;孙 朋(1979—),男,硕士,主要研究方向为数据库与知识库。

选系统中的一个节点，假设其交易次数为1000，成功交易次数为500，认证成功概率为50%。对比这两个场景，场景一的节点的认证度要远远高于场景二节点的认证度。但从实际情况中考虑，仅仅交易一次的节点即使交易成功，它的可信度仍然值得怀疑。因此，对节点交易次数的度量是考察节点可信度的一个重要因素。

(2)节点的信誉值

CA节点是基于第三方信任模型的可信机构，在对节点可信度的评估过程中，无论是直接信任还是间接信任都需要CA作为节点历史交易信息的中介。例如网络中的某个完全可信的终端节点，它的节点信息表存储在了一个恶意的CA的本地数据库中，这里的恶意CA主要指提供虚假的信息。假设对节点可信性的评估有3种情况，即{−1,0,1}，其中−1代表完全不可信，0代表可信性不确定，1代表完全可信。那么在对这个节点认证时，其可信度应该为1，但由于CA提供虚假的信息，也就是该CA反馈给上级CA的该节点的认证度为−1，因此节点不被认证。因此，在对节点认证可信度评估的过程中，考查CA的信誉值也是十分重要的。

(3)节点交易的衰减因素

节点的衰减因素主要考虑的是交易的时间问题，也就是一条交易记录的参考价值会随时间的流逝而有所变化。一般来说，交易时间越近的记录，其参考价值越大，反之，交易时间越远的记录其参考价值越小。在模型中引入衰减因子，可以增加最近交易记录的权重，以便更准确地计算节点的可信度。

(4)提供资源的类型

网络中存在着纷繁复杂的节点，每个节点提供资源的类型都有差异。在其擅长的领域内，提供资源的可信性会较高，因此我们在对节点信任度进行评估时要考虑节点提供资源的类型。

3 模型的信任度的计算

3.1 直接信任度

3.1.1 终端节点的认证度

直接信任值表示在网络中两个相互有过直接交易的节点的信任值。在实际评价交易结果中，应该存在很多必要因素，比如说反应速度、传输时间、交易结果的质量等等，需要分别对每一项进行评价，综合得到完整的直接信任值。然而已有的信任模型对直接信任值的计算往往都是靠主观的估算，主观性强，算法单一，不够准确，导致交易成功率低。

本文采用加权平均的方法来计算节点间的直接信任值，将多个因素的结果归一，运用对多次计算取平均值的方法，可以更准确地得到直接信任值。在以往的信任模型中，经常会因为一次交易失败就大幅度降低节点的信任值，有矫枉过正之嫌。很多节点因为一次传输错误，或者网络临时出现问题，并不是主观意愿导致交互失败，如果这时候就认为节点行为属于恶意行为，会严重影响信任值计算的准确性。

在认证过程中，根据认证发生的时间先后将认证值赋予不同的权重，发生时间越久远的交易记录时间权重越小，反之，越近交易的认证记录被赋予的权值越高。传统的身份认证模型都是将交易的记录按相同的时间间隔分段，将不同的时间段赋予不同的权重，但这种分类方法并不科学，因为认证记录随发生时间的渐远其参考价值也逐渐减小，新近发生的交易即使在同一个时间段其影响程度也有可能不同，所以对认证时间段的划分应该是不相同的。模型引入衰减函数来增加最近交易记录的权重，以便准确计算节点的可信度。假设T_{jk}为认证发生时的某个时间段，T_n为当前时间，衰减函数如下：

$$f(ID_{jk})=\rho^{T_n-T_{jk}} \tag{1}$$

式中，$f(ID_{jk})$为节点ID_{jk}与本地节点的当前交易记录的时间衰减函数，ρ为衰减因子，反映历史认证记录信息的重要程度($0<\rho<1$)。假设认证信息每过一小时，信任度衰减一半，即$\rho=0.5$，设当前时间为13:33，ID_{jk}与IDi交易记录时间为11:01，则$f(ID_{jk})=(0.5)^{13-11}=0.25$。

在对节点信任度的纵向评估中，考虑每一个与之交易的节点的历史交易次数、历史交易的成功概率，以及交易的满意度。设$SNUM_{jk}$为节点ID_{jk}与节点ID_i成功交易的次数，NUM_{jk}为节点ID_{jk}与节点ID_i交易的总次数，则节点ID_{jk}与节点ID_i历史交易的成功概率为：

$$Psuccess(i,j)=\frac{SNUM_{jk}}{NUM_{jk}}\cdot\rho^{\frac{1}{SNUM_{jk}}} \tag{2}$$

节点的直接认证度将节点信息表中所有与之交易过的节点的历史认证度取加权平均值，并将此平均值与认证的满意度函数按照不同的权重加和。节点ID_i的直接认证度的计算公式如下：

$$NODET_i=\frac{1}{n}\sum_{k=1}^{n}[\alpha\cdot f(ID_{jk})\cdot T_{jk}+\beta\cdot Psuccess(i,j)\cdot SAT_{ji}] \tag{3}$$

式中，α,β为横向评估和纵向评估所占的权重。$\alpha,\beta\in(0,1)$且$\alpha+\beta=1$。

3.1.2 CA信誉相关的直接认证度

CA信誉相关的直接认证度是对中介CA信誉的考察，中介在把终端节点的认证度传递给高层CA的过程中，高层CA要首先考察中介CA的信誉。也就是说中介CA的信誉会影响终端节点的认证度。

Def1 CA的信誉：我们将CA的信誉理解为高层CA相信其可信的概率，记为：

$REP(CA_j)=P(CA_i\xrightarrow{believe}CA_j)$，其中$CA_i$为$CA_j$的严格上层CA。

Def2 节点的可信度：一个节点ID_i的可信度就是该节点被接受认证的概率。

$P(CA_j\xrightarrow{believe}ID_i)=NODET_i$。$CA_j$为$ID_i$的交易记录保存地点。

Def3 节点的直接信任度

$DT_{ki}=2\cdot NODET_i\cdot(1-2\cdot REP(CA_j))\cdot(1-NODET_i)+REP(CA_j)$

其中，DT_{ki}为CA_k对ID_i的直接信任度，CA_j为信任推荐CA。

证明：节点和CA间的拓扑结构关系如图1所示。

图1 拓扑关系图

(1)由定义 2，$DT_{1i}=P(CA_1 \xrightarrow{believe} ID_i)$

(2)由全概公式 $P(A)=P(A|B)P(B)+P(A|\overline{B})P(\overline{B})$ 知 $P(CA_1 \xrightarrow{believe} ID_i)=P(CA_1 \xrightarrow{believe} ID_i|NODET_i)\cdot NODET_i+P(CA_1 \xrightarrow{believe} ID_i|(1-NODET_i))\cdot(1-NODET_i)$。

在这里，$P(CA_1 \xrightarrow{believe} ID_i|NODET_i)$表示 ID_i 可信的情况下 CA_1 接受 ID_i 认证的概率，$P(CA_1 \xrightarrow{believe} ID_i|(1-NODET_i))$表示在 ID_i 不可信的情况下，CA_1 接受 ID_i 认证的概率。

(3)对于在 ID_i 可信的情况下 CA_1 接受 ID_i 认证的概率又可以分成两种情况，一种情况是 CA_2 接受 ID_i 的认证，并且 CA_1 认为 CA_2 也是可信的；另一种情况是 CA_1 认为 CA_2 是恶意 CA，因此它提供的节点的认证值也是不可信的。基于这两种情况，$P(CA_1 \xrightarrow{believe} ID_i|\mathrm{NODET_i})$的计算公式如下：

$$P(CA_1 \xrightarrow{believe} ID_i|NODET_i)=REP(CA_2)\cdot NODET_i+(1-REP(CA_2))\cdot(1-NODET_i)$$

同理，对于在 ID_i 不可信的情况下，CA_1 接受 ID_i 认证的概率也可以分成两种情况讨论，即 CA_1 相信 CA_2 提供的虚假信息和 CA_1 不相信 CA_2 提供的真实信息，$P(CA_1 \xrightarrow{believe} ID_i|(1-NODET_i))$的计算公式如下：

$$P(CA_1 \xrightarrow{believe} ID_i|(1-NODET_i))=(1-REP(CA_2))\cdot NODET_i+REP(CA_2)\cdot(1-NODET_i)$$

(4)综上，

$$P(CA_1 \xrightarrow{believe} ID_i)=[REP(CA_2)\cdot NODET_i+(1-REP(CA_2))\cdot(1-NODET_i)]\cdot NODET_i+[REP(CA_2)\cdot(1-NODET_i)+(1-REP(CA_2))\cdot NODET_i]\cdot(1-NODET_i)=2\cdot NODET_i\cdot(1-2\cdot REP(CA_1))\cdot(1-NODET_i)+REP(CA_1)$$

，证毕。

举例说明，如图 1 所示，假设 ID_i 的节点信任度 $NODET_i=0.7$，CA_2 的信誉 $REP(CA_2)=0.8$，则

P(接受认证|ID_i 可信)=$P(CA_1$ 相信 $CA_2)*P(CA_2$ 相信 $ID_i)+P(CA_1$ 不相信 $CA_2)*P(CA_2$ 不相信 $ID_i)=0.8*0.7+0.2*0.3=0.62$；

P(接受认证|ID_i 不可信)=$P(CA_1$ 相信 $CA_2)*P(CA_2$ 不相信 $ID_i)+P(CA_1$ 不相信 $CA_2)*P(CA_2$ 相信 $ID_i)=0.8*0.3+0.2*0.7=0.38$；

$DT_{1i}=P$(接受认证|ID_i 可信)$*NODET_i+P$(接受认证|ID_i 不可信)$*(1-NODET_i)=0.62*0.7+0.38*0.3=0.548$。

3.2 间接信任度

间接信任的思想来源于人际网络，一个人不可能认识所有的人，当一个个体 A 想要了解另一个不太了解或者完全陌生的个体 B 时，A 通常会向自己熟悉的人群 C 咨询关于 B 的情况，然后综合 C 反馈回来的信息，得出对 B 的综合判断，这个结果一般与 B 的实际比较吻合。

为了防止恶意 CA 诋毁可信节点，阻止可信节点被认证，节点采用广播的方式询问其 friends 节点，获得被认证节点的间接认证值。节点的本地数据库中保存了其 friends 节点的历史认证记录，friends 节点库表结构如表 1 所列。

表 1 Friends 节点数据库

Friends ID	节点的上一次认证度	最后一次认证时间
ID_{j1}	$T_{j1}^{(k)}$	$TIME_{j1}$
ID_{j2}	$T_{j2}^{(k)}$	$TIME_{j2}$
……	……	……
ID_{jn}	$T_{jn}^{(k)}$	$TIME_{jn}$

节点的间接认证度可以表示为所有 Friends 节点的间接认证度加权平均值。节点从其 Friends 节点处获得的节点间接认证值理论上应该在某个范围内，但也可能出现偏差较大的值，在计算间接信任度时应将这些偏差较大的间接认证值删去，再计算加权平均值。$AVGT_i$ 表示剔除了偏差较大的间接值后对节点 i 的平均间接信任值。

$$AVG_j=\frac{\sum_{k\in set(ID_k)}(T_{kj}-\frac{1}{|Friends|}\sum_{m\in Friends}T_{mj})}{|set(ID_k)|},\quad (T_{kj}-\frac{1}{|Friends|}\sum_{m\in Friends}T_{mj}<\theta) \tag{4}$$

式中，$Friends=\{ID_1,ID_2,\cdots,ID_n\}$为节点 ID_i 的 Friends 节点库，|Friends|表示 Friends 节点库中节点的个数，set(ID)表示可用的间接信任值。Θ 为可接受的偏差。

那么节点 ID_i 对节点 ID_j 的间接认证度为：

$$IT_{ij}=\frac{\sum_{m\in Friends}T_{im}\cdot f(ID_m)}{|Friends|}\cdot AVG_j \tag{5}$$

式中，$f(ID_m)$表示节点 ID_m 交易时间的时间衰减函数。

3.3 综合信任度

综合信任值是通过直接信任值和间接信任值加权得到的。但是对于加权的系数应该考虑很多实际因素在里面，就像在人与人的实际交往中，当一个人与另一个人不太熟悉时，他对于这个人的了解更多地取决于其他人的介绍和评价，然而随着两个人的接触逐渐增多，了解也更加深入，对一个人的评价就越来越多地取决于自身，其他人的观点变得不那么重要，当两个人成为至交好友以后，对另一个人的评价也就不再和其他三个人有关了，完全取决于自己的判断。

对节点的贡献值的考量应从节点上传资源和下载资源以及间接其他节点的次数入手。一般来说，节点间接的次数越多对网络的贡献应该越大，节点上传资源属于对资源的聚集，下载资源属于对资源的消耗，因此贡献值与上传资源量应该成正比而与下载资源量应该成反比。据此，节点的贡献参数 AR_i 的计算公式如下：

$$AR_i=\xi\frac{U_i}{U_i+D_i}+(1-\xi)\cdot(\frac{U_i}{U_i+D_i}+\frac{INUM}{TNUM+INUM}) \tag{6}$$

式中，U_i 为节点 ID_i 上传资源的量，D_i 为节点 ID_i 下载资源的量，$INUM$ 和 $TNUM$ 分别表示节点间接次数和总交易次数，ξ 为权重因子，它控制上传资源、下载资源和间接次数对贡献值的比重。由公式可以看出，节点依靠上传资源获得的贡献值要远远大于仅依靠间接节点获取的贡献值，这将刺激

节点为网络贡献更多的资源，以维持系统的正常工作。

在获得了节点的贡献值之后，我们可以定义节点的综合信任度如下：

$$T_i=\alpha DT_i+\beta IT_i+\lambda AR_i \quad (7)$$

式中，α,β,λ 分别表示直接信任、间接信任和节点贡献值在综合认证值中占的比重，$\alpha,\beta,\lambda\in(0,1)$，并且 $\alpha+\beta+\lambda=1$。

4 算法设计

4.1 模型的设计框架

中介机构 CA 可以传递保存节点的认证信息，利用它对节点信任度的算法模型设计进行设计。模型的设计引入了聚类的思想，根据节点所提供资源类型的不同将节点分类，相同类型的节点用同一个 CA 记录其认证值。路径选择算法在提供同类型资源的节点中选取信任度较高的节点进行交易。反馈调节算法是在节点接受认证之后对节点提供信息的价值进行考量，若认为信息是有效的，则反馈认证成功的信息，反之反馈认证失败的信息。认证信息反馈给信任路径中的每一个 CA，每个 CA 根据反馈信息更新节点的认证信息。反馈算法根据节点在不同 CA 间接下的认证值的不同，决定节点应归属于信任值较大的 CA 所在的域中，这样使 CA 对节点的间接更可信，并且可以提高节点的信任度，使其更好地为网络提供服务。激励机制根据反馈信息判定节点对网络的贡献值以及节点的效用值，并以此决定节点的优先权，激励值越大的节点优先权越高，可以优先享受网络的资源，这样可以避免网络中资源枯竭、节点只享受资源而不提供资源的现象发生。模型的框架如图 2 所示。

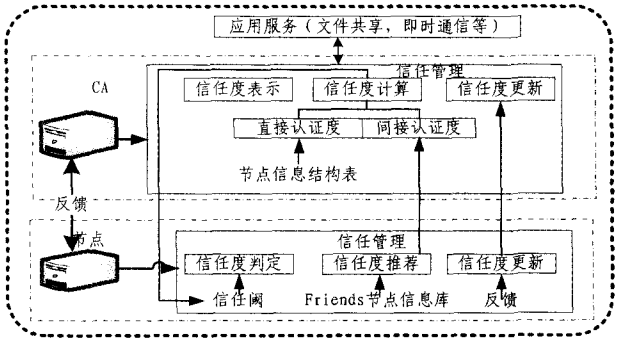

图 2 模型的总体架构

4.2 模型的算法实现

节点认证度包括直接认证度、间接认证度和综合认证度的计算。每一种计算方法封装为一个类，并将类的接口部分放于头文件中。其中直接信任度的计算类和间接信任度的计算类的实现方法都需要用到节点类的私有数据项，因此它们都继承自节点类。综合信任度的计算综合了直接信任度的计算和间接信任度的计算，并赋予权值，因此综合信任度的计算类有两个父类，分别是直接信任度的计算类和间接信任度的计算类。

1）节点头文件如下：

```
Struct Node
{
  int last_time;//上次交易发生的时间
  long ID;//发生交易节点的 ID
  int SAT;//满意度评价
  int NUM;//交易次数
  int SNUM;//满意次数
  double T;//当前认证度
}
  class Node
{
Node node;
  long ID;//节点 ID
int resouse_give;//提供资源数
int resouse_use;//消耗资源数
int INUM;//间接次数
};
```

2）模型函数的定义

```
/*计算 ID 为 i 的节点的节点认证度，并将其保存在 node_value 中。
  Trade_set 是一个保存交易过节点的集合，key 存储交易节点的
  ID，value 存储交易信息。*/
Trust_NODE_T(Node i,trade_set,double node_value)
/*计算 CAi 的信誉值，并保存到变量 rep 中。*/
  REP_CA(Node i,double rep)
/*计算节点的直接认证度，保存到变量 d_value 中*/
  Trust_D_T(Node i,REP_CA(Node i,double rep),double d_val-
  ue)
/*将 friends_set 节点的间接信息存储到 trust_vector 中*/
  Recommend_value(friends_set,Node_ID,trust_vector)
/*计算节点 i 的间接认证值，保存到变量 I_value 中。trust_vector 保
  存 friends 节点间接的认证值*/
  Trust_I_T(Node i,trust_vector,double I_value)
/*计算节点的综合信任值，存储到变量 T_value 中*/
  Trust_T(Count_D_T(Node i,REP_CA(Node i,double rep),
  double d_value),
  Trust_I_T(Node i,trust_vector,double T_value),double T_val-
  ue)
/*节点 i 对节点 j 的认证反馈信息*/
  Feedback(Node I,Node j,SAT)
/*在 set 中随机抽取节点 i*/
  Rand(Node i,set)
/*判断信任值是否满足节点的信任阈值。trust_domian 为信任阈
  */
  Greaterthan(Node i,Node j,double T_value,trust_domian)
/*判断直接认证值与节点的历史认证值的差异是否在可接受的范围
  之内。receive_domain 为可接受的差异阈*/
  IFreceive(Node i,Trust_D_T(Node i,REP_CA(Node i,double
  rep),receive_domain)
```

3）形式化算法描述

```
while(count<3000)//设置计数器进行次认证
{
Rand(Node i,set);//随机选取一个节点进行交易
Trust_NODE_T(Node i,trade_set,double node_value);
  //计算节点的节点认证度
REP_CA(Node i,double rep);//计算 CA 的信誉
Trust_D_T(Node i,REP_CA(Node i,double rep),double d_value);
  //计算节点的直接认证度
if (IFreceive(Node i,Trust_D_T(Node i,REP_CA(Node i,double
```

```
rep), receive_domain) &&Greaterthan(Node i, Node j, double T_
value, trust_domian));
//判断直接认证度是否达到信任阈并且获得的直接认证度与上次
  交易的认证度的差异在一个可以接受的范围之内
{
Feedback(Node I, Node j, SAT);//更新反馈信息
}
else
{
Recommend_value(friends_set, Node_ID, trust_vector);
//向 friends 节点询问被认证节点的认证度
Trust_I_T(Node i, trust_vector, double I_value);//计算间接认证度
Trust_T(Count_D_T(Node i, REP_CA(Node i, double rep), double
d_value), Trust_I_T(Node i, trust_vector, double T_value), double T
_value);
//计算综合认证度
if(Greaterthan(Node i, Node j, double T_value, trust_domian))
//判断认证度是否达到节点的认证阈值
{
Feedback(Node I, Node j, SAT);//更新反馈信息
}}}
```

5 可信信任度的演化测试模型

节点信任度测试用于验证基于中介机构的信任模型与传统的信任模型对于可信节点的认证度随认证次数的变化情况。模型随机选取一个可信节点为观察对象，分别记录这两个节点 3000 次交互之后在两种模型影响下的认证度。

实验交互过程如下：

- 在一段时间间隔中随机选择一个节点提出认证请求。
- 新节点的初始认证度为 0.5，表示可信度不确定。
- 认证结果分布在(0,1)之间。

结果图 3 所示。

从实验结果可以看出，基于中介机构第三方信任模型的可信节点其认证度变化较传统的信任模型上升较快，并且认证度也有较大的提高。可信节点经过较少的认证次数即可达到一个较高的平衡值，收敛速度较快。

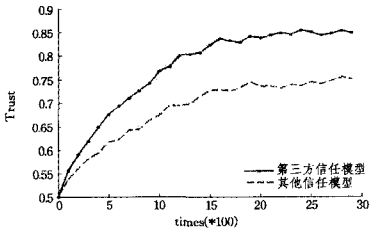

图 3 可信节点的信任度变化趋势

结束语 本文对基于节点信任度模型的算法部分进行了设计，根据模型的设计思想分析了影响认证度的几种因素，设计实现了模型的直接认证度算法、间接认证度算法和综合认证度算法。本文提出的认证度评估模型对可信节点的认证度较以往的信任模型有所提高。可信节点认证成功发生交易的可信性增大，有利于网络中资源的有效利用。

参 考 文 献

[1] 戚文静，张素，于承新，等. 几种身份认证技术的比较及其发展方向[J]. 山东建筑工程学院学报，2004，6：85-87

[2] 来学嘉. 基于挑战——响应的认证协议安全的必要条件[J]. 中国科学院研究生院学报，2002，19(3)：246-253

[3] 龙毅宏. 可信计算中的数字证书[Z]. Netinfo Security，2004

[4] 鲍宇，曾国荪，曾连荪. P2P 网络中防止欺骗行为的一种信任度计算方法[J]. 通信学报，2008，10：215-222

[5] 田祥宏，严浩，严筱永. P2P 环境下的一种混合式信任模型[J]. 计算机工程与应用，2009，45(31)：73-76

[6] 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(9)：1401-1408

[7] Zhang Shi-bin, He D. Fuzzy model for trust evaluation[J]. Journal of Southwest jiaotong University, 2006, 14(1): 23-28

[8] Manchala D W. Trust metrics, models and protocols for electronic commerce transactions [C] // Inthe 18th International Conference on Distributed Computing Systems. 1998: 3-12

[9] 徐兰芳，张大圣，徐凤鸣. 基于灰色系统理论的主观信任模型[J]. 小型微型计算机系统，2007，28(5)：801-804

(上接第 53 页)

则来实现 XSS 漏洞的静态分析，并通过定义概念攻击字符串的常见变换来实现净化单元的动态检测，由此来实现 Web 应用跨站脚本(XSS)漏洞检测。分析表明该方法能有效发现 Web 应用程序中的跨站脚本(XSS)漏洞。

但是，本文目前针对净化单元的动态测试主要是手动测试，如何构建变换测试知识库，然后实现自动化动态测试净化单元是下一步的工作重点。

参 考 文 献

[1] 石华耀，等. 黑客攻防技术宝典[M]. 北京：人民邮电出版社，2009

[2] Open Web Application Security Project. Testing Guide 2008 V3.0

[3] Open Web Application Security Project. A guide to building secure Web applications

[4] 董启雄，韩平，程永敬，等. 安全编程：代码静态分析[M]. 北京：机械工业出版社，2008

[5] Petukhov A, Kozlov D. Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing [J]. OWASP Application Security Conference, 2008(3)

[6] 朱辉，沈明星，李善平. Web 应用中代码注入漏洞的测试方法[J]. 计算机工程，2010(10)

[7] Livshits B, Lam M S. Finding Security Vulnerabilities in Java Applications with Static Analysis[C]//Proceedings of the 14th conference on USENIX Security Symposium(SSYM'05). Volume 14

[8] Ragle D. Introduction to Perl's Taint Mode[EB/OL]. http://www.webreference.com/programming/perl/taint

[9] Wassermann G, Su Zhen-dong. Static Detection of Cross-Site Scripting Vulnerabilities [C] // Software Engineering, ACM/IEEE 30th International Conference on, ICSE '08. 2008

[10] Open Sourced HTML filtering utility for Java[EB/OL]. http://xss-html-filter.sourceforge.net/