doi:10.3969/j.issn.1000-436x.2013.09.009

基于动态贝叶斯网络的可信度量模型研究

梁洪泉，吴巍
（通信网络信息传输与分发技术重点实验室，河北 石家庄 050081）

摘 要：针对可信网络中亟需解决的可信度量模型展开研究，以社会学中的人际关系信任模型为基础，研究网络节点间的可信关系，提出了一种与时间因素关联的基于动态贝叶斯网络的可信度量模型。该模型充分考虑身份认证、网络交互行为对可信度量的影响，引入历史交互证据窗口、时效性因子和惩罚因子，同时给出了直接可信度和间接可信度的聚合方法，提高了模型的动态自适应能力以及计算的灵敏度和准确度，有效地抑制了异常实体的威胁。仿真实验结果表明，与传统的贝叶斯网络模型相比，该模型能够灵敏有效地进行可信度计算，同时具有良好的动态自适应性。

关键词：可信网络；可信度量；动态贝叶斯网络；条件概率分布
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)09-0068-09

Research of trust evaluation model based on dynamic Bayesian network

LIANG Hong-quan, WU Wei
(Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory, Shijiazhuang 050081, China)

Abstract: Trust evaluation model needs to be developed for trusted network. Based on interpersonal trust model in sociology, the trusted relationship between network nodes was researched, and a trust evaluation model based on dynamic bayesian network associating with time factor was proposed. The impact of authentication and network interaction behavior was fully considered, and historical interaction window, timeliness factor and penalty factor were introduced. Also, the polymerization method of the direct trust degree and indirect trust degree was given, and the dynamic adaptive ability of the model was improved as well as the calculation of the sensitivity and accuracy. Furthermore, the threaten of abnormal entity was effectively suppressed. Experimental results show that this model computes the trust degree more sensitively and effectively as well as better dynamic adaptivity compared with the traditional bayesian network model.

Key words: trusted network; trust evaluation; dynamic Bayesian network; conditional probabilistic distribution

1 引言

随着互联网的急剧膨胀，人们对互联网的要求也在不断提高。当前的网络体系正面临着严峻的安全和服务质量(QoS)保证等重大挑战。由于复杂网络环境的异构性、分布性、开放性、不确定性、动态性、欺骗性等特点，使可信问题成为下一代网络研究的新焦点。以往通过产品叠加式的“被动防御”方式已经远远不够，需要研究基于身份认证与网络行为相结合的新方法，迫切需要建立以准确、高效、动态可信度量模型为依据的可信网络新秩序。

过去互联网的安全可信大多是实现制定的安全策略，对终端系统进行安全检测，拒绝不安全系统的接入。针对用户侧的可信问题，国内外大多以可信计算为基础，在终端环境可信及终端对网络的可信接入等环节已取得了显著进展，如可信计算平台联盟(TCG)的可信网络连接(TNC)规范[1]、思科的

收稿日期：2012-10-21；修回日期：2013-03-25
基金项目：国防基础科研计划基金资助项目(B1120110001)
Foundation Item: The National Defense Basic Scientific Research Program of China (B1120110001)

网络接入控制(NAC)技术[2]及微软的网络接入保护(NAP)技术[3]等。

目前，学者们针对可信度量提出了多种建模与评估方法,且大多是以社会学中的人际关系信任模型为基础，主要包括基于证据和概率统计理论[4~6]、基于模糊集合理论[7]、基于信息熵的理论[8]、基于多属性决策理论[9]等。虽然已有的研究成果有效推动了可信度量的研究与发展，但在动态适应性及交互行为时效性等方面仍有待深入研究，主要呈现以下问题。

1) 现有基于概率统计的模型，在建模中做了各种主观的假设，缺少灵活性，使模型的准确性和动态自适应性受到影响。

2) 现有模型虽然考虑了实体交互的动态性及不确定性，但是没有考虑交互的时效性及根据交互上下文变化的动态自适应性，使可信度量模型的准确性与科学性受到影响。

3) 现有模型针对各种样式的网络攻击与欺骗，缺乏有效的防护机制及动态自适应性，导致模型缺乏顽健性，影响模型的安全性与可用性。

针对研究现状，本文提出了一种与时间相关的基于动态贝叶斯网络的可信度量模型，旨在提高模型的动态自适应性和灵敏性，降低不确定性。该模型将历史交互证据窗口、时效性因子、惩罚因子等应用到直接可信度量、间接可信度量及综合可信度量模型中，进而提高可信度预测的灵敏度和准确性，为后续网络资源的选择、调度及分配提供可信依据。

2　相关工作

1994 年，由 MARSH[10]首次提出了可信度量的数学模型，系统论述了可信度的规范化表示，并对可信度量的研究内容及可信程度的划分进行了阐述。1996 年，M BLAZE 等人[11]首次提出了“可信管理”的概念，其基本思想是承认开放系统中安全信息的不完整性，需要依靠可以信任的第三方提供额外的安全信息来保障决策安全。1997 年，ABDUL-RAHMAN 等人[12]首次提出用推荐机制来解决独立于上下文且具有主观性的可信管理概念；并于 2000 年再次提出将可信度量分为直接和推荐可信度量 2 部分的思想。

近年来，学者们使用了不同的数学模型和工具对可信度量展开研究，但到目前为止，还没有形成公认的理论模型和度量基准。其中，比较典型的有以下几种。

文献[4]采用改进的证据理论(D-S theory)对可信关系进行建模，可信度评估采用概率加权平均方法。文献[5]基于贝叶斯网络提出了一种使用 Kalman 方法的简化模型，通过引入衰减及奖惩机制，使模型具有一定的动态适应性，但在预测的准确性、灵敏性及时间连续性上存在不足，难以适应动态复杂的网络环境。文献[8]使用信息理论中熵的概念进行可信关系的建模。文献[13]将风险评估引入到可信度计算中，提出了适用于普适计算网络环境下基于可信度的安全服务发现模型。文献[14]提出了一种普适计算网络环境下通用的、基于交互上下文的可信度计算模型。文献[15]提出了一种适用于云计算环境下的基于多属性、多根源的可信度计算模型。文献[16]重点考虑可靠性和可用性 2 个因素，提出了一种适用于计算栅格环境下的可信度量模型，该模型具有较好的可扩展性。文献[17]提出了一种基于重复博弈的惩罚激励机制 PETrust，文献[18]提出了具有激励效果的分布式 P2P 可信管理模型 IMTM，这 2 个文献均没有考虑时间因素和动态环境的影响。文献[19]提出了一种基于时间窗的局部信任模型 TW-Trust，该模型通过反馈控制机制动态调节信任评估参数，提高了模型的动态适应能力。文献[20]提出了一种符合人类心理认知习惯的动态信任预测的认知模型，构建了自适应的基于有效历史交互证据窗口的总体信任决策方法，通过 DTT(direct trust tree)实现全局反馈信息的搜索与聚合，降低了网络带宽开销，提高了模型的可扩展性。

虽然这些研究成果有效推动了可信度量的研究与发展，但是仍然存在引言中指出的一些问题。本文的主要贡献是在深入分析可信度量的指标体系及系统架构的基础之上，给出了一种适用于动态不确定网络环境下的基于历史交互证据的可信度量模型，该模型以动态贝叶斯网络为理论依据，引入了时效性因子和惩罚因子，同时具有连续度测能力。

3　可信度量建模的相关内容

3.1　相关概念

定义 1　设当前网络中实体的可信度评价有 5 个等级 l_1、l_2、l_3、l_4、l_5，分别表示为完全不可信、不可信、未知可信、可信和完全可信，则称 $\boldsymbol{L}=\{l_1,l_2,\cdots,l_5\}$ 为可信等级集合。

定义 2 设集合 $\boldsymbol{X}=\{x_1, x_2,\cdots, x_n\}$表示当前网络中的 n 个自治实体，x 为当前实体,若 $\forall x_i \in X$ 且 $x \neq x_i$，存在交互证据 e_i，使 $e_i(x, x_i) \neq \varnothing$ 且 $e_i \in E$，则称集合 $\boldsymbol{E}=\{e_1,e_2,\cdots,e_n\}$为本地证据库。

定义 3 设 $\boldsymbol{E}=\{e_1,e_2,\cdots,e_n\}$为本地证据库，对于系统设定的窗口 H，若使 $\boldsymbol{E_H}=\{e_{n-H},e_{n-H+1},\cdots,e_n\}$作为目标实体可信度计算的有效证据，则称 H 为有效历史交互证据窗口。

定义 4 设 HEW 为有效历史交互证据窗口，t 为当前时间，则称 $C(HEW, t)$为 t 时刻有效历史交互证据窗口中相应的交互上下文条件。

3.2 数学建模方法的比较

根据以往可信度量数学建模方法的不同，大致可分为 3 种：基于概率统计理论、基于模糊集合理论和基于多属性决策理论等方法。

1) 基于概率统计的方法

该方法基于对实体间交互历史的统计，用概率来描述实体的可信度，具有较好的数学基础。此类模型虽然考虑了不确定性因素，但归根到底是依据精确的数学模型加以解决，其本质是把可信的主观性等同于随机性，且无法有效消除恶意推荐带来的影响。

2) 基于模糊集合理论的方法

该方法将概率论等精确的数学模型通过模糊集合理论进行扩展。可信的判断是通过实体对各可信模糊子集的隶属度构成的向量来描述的。该方法未综合考虑多属性也未给出确定可信属性权重因子的方法，因此不能很好地进行综合评判。同时，模糊隶属函数及具体的确定方法始终没有定论，而且模糊理论抛弃了对随机性的研究，显然对可信度量的研究不合适。

3) 基于多属性决策的方法

该方法在决策信息的基础上，通过一定的决策准则产生备选方案的综合评价值，并以此为依据决定各方案的优劣。该方法虽然综合考虑了上下文信息及候选服务提供者的多项属性，却未能体现可信的模糊性和不确定性，且在防范恶意实体蓄意破坏上存在一定的不足。

本文采用基于动态贝叶斯网络的推理方法，该方法有效结合了概率论和图论且具有天然的随机变量随时间演化的表示能力。优于以上 3 种方法的是动态贝叶斯网络的推理方法既考虑了时间因素下网络行为的随机性，又考虑了相互影响的随机变量间的依赖关系，充分体现了网络中的随机性、模糊性及动态性，同时能够有效地降低不确定性，提高计算的准确性。

4 基于动态贝叶斯网络的可信度量模型

4.1 动态贝叶斯网络理论

动态贝叶斯网络(dynamic Bayesian network)源于贝叶斯网络，其理论依据是贝叶斯定理及贝叶斯公式。动态贝叶斯网络将传统的贝叶斯网络与时序信息相结合，反映时间因素对事件概率的影响。

假定事件的变化发生在离散时间点之间，这些离散时间点由非负整数来索引。假定 $\boldsymbol{X}=\{X_1, X_2,\cdots, X_n\}$是随时间变化的属性集，$X_i[t]$表示在时刻 t 属性 X_i 的值，$X[t]$是随机变量 $X_i[t]$的集合。为表示整个过程中网络结构变化轨迹的度，需要在随机变量 $X[0]\cup X[1]\cup\cdots$上进行概率分布，假定整个变化过程满足马氏链模型：

$$P(X[t+1]\,|\,X[0],\cdots,X[t]) = P(X[t+1]\,|\,X[t]) \quad (1)$$

即 t+1 时的状态仅依赖于 t 时的状态。而网络的拓扑、变量集和变量间的因果关系在每个时间片都是相同的，因此建立一个动态贝叶斯网络，必须先定义先验网络及转移网络两部分：

1) 先验网络 B_0，表示初始时态 $X[0]$的分布；

2) 转移网络 $B\rightarrow$，表示所有时间 t 上的转移概率 $P(X[t+1]|X[t])$。

一个动态贝叶斯网络是由在符合变量 $X[0],\cdots, X[\infty]$上的无限的网络$(B_0, B\rightarrow)$来定义的，事实上，只需在有限区间 $0,\cdots,T$ 上进行推理即可。为此，可将上面的无限 DBN 转化为 $X[0],\cdots,X[t]$上的 DBN。在时间片 0 上，$X_i[0]$的父节点是那些在先验网络 B_0 中指定的节点；在时间片 t+1 上，$X_i[t+1]$的父节点是在时间片 t 的节点和时间片 t+1 上符合 $B\rightarrow$中 $X_i[t]$父节点的节点，用类似的方法可求得这些变量的条件分布。给定 DBN 的模型，$X[0],\cdots,X[t]$上的联合概率分布为

$$P(X[0],\cdots,X[t]) = P(X[0])\prod_{t=0}^{t-1} P(X[t+1]\,|\,X[t]) \quad (2)$$

其中，$P(X[t+1]|X[t])$可从转移网络模型中求得。动态贝叶斯网络通过网络拓扑结构反映变量间的概率依存关系及其随时间变化的情况，不但能够对变量所对应的不同特征之间的依存关系进

行概率建模，而且对特征之间的时序关系也能很好地加以体现。此外，还可以任意改变拓扑结构或增删变量以反映变量间的各种关联关系，而不影响算法本身，因此具有很好的可扩展性和灵活性。同时，动态贝叶斯网络还具有良好的可解释性，其拓扑结构具有精确及易理解的概率语义，通过对其进行分析可加深对不同变量间关联关系的理解。

动态贝叶斯网络利用采集到的样本更新网络结构、先验分布及条件概率，该方法在推理过程具有前后连续性从而更符合客观世界。采用概率方法结合专家知识、证据库及有效证据窗口对可信度进行描述，使其具有了知识累积和时间衰减特性，能更有效地降低不同层次信息融合中的不确定性，有效提高可信度量模型的准确性。

4.2　可信度量模型的形式化描述

1) 可信度量模型的指标体系

如图 1 所示，该指标体系由静态的实体身份可信和动态的实体行为可信 2 部分构成。其中，身份可信是可信度量模型的基础，目前，大多采用基于 CPK 的认证算法；而动态的行为可信能够提供比静态的身份可信更细粒度的安全保障。该指标体系通过逐层分解与细化，将复杂网络行为的可信度量问题转化为客观、可测量、可计算的基于交互证据的评估问题。

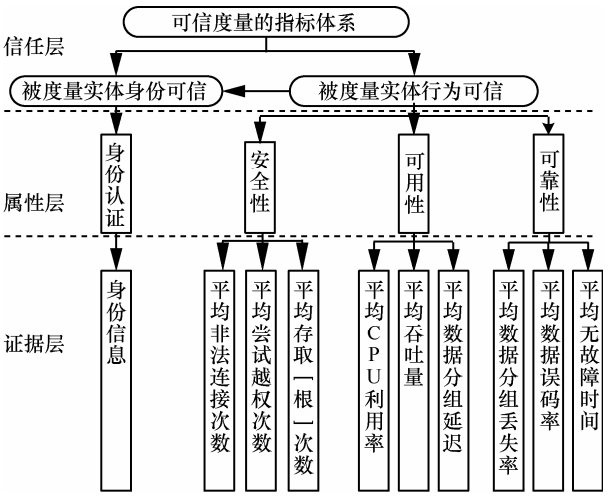

图 1　可信度量的指标体系

该指标体系的证据层列出了 10 种证据，考虑到证据采集的可行性及计算的复杂度，可以对证据层作进一步扩充或删减。

2) 可信度量模型的组成

如图 2 所示，可信度量模型组成包括知识库、证据库、可信认知模块、可信度量模块、可信决策模块及可信管理模块。

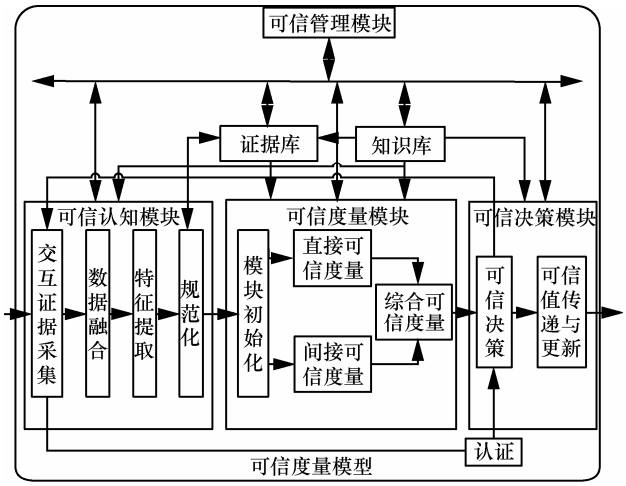

图 2　可信度量模型组成

① 知识库：本地用于存储并负责更新可信度量的策略与先验知识。

② 证据库：本地用于存储经过预处理和规范化后的有效证据，是可信度量计算的基础。

③ 可信认知模块：包括交互证据采集、数据融合、特征提取及规范化 4 个模块。交互证据采集用于监测网络行为、提取交互证据、接收信令携带的相关实体的间接可信度量值；数据融合完成信息处理、去冗余及数据关联；特征提取对数据融合后的信息完成特征析取；规范化对采集的交互证据完成等级划分及规范化表示。

④ 可信度量模块：包括模块初始化、直接可信度量、间接可信度量及综合可信度量 4 部分。主要计算邻接实体的直接可信度，并将其与间接可信度进行综合，作为本实体对邻接实体综合可信度判定的唯一依据。

⑤ 可信决策模块：依据各邻接实体的综合度量值，维护并扩散本地可信关系列表，并对后续证据的采集产生指导。同时，对可信关系列表中度量值在阈值以下的网络实体进行隔离，限制其网络访问控制权限。

⑥ 可信管理模块：负责对其他模块的管理。

4.3　可信度量计算

可信度量是对目标实体满足预期程度的评价，是与实体交互相关的动态变量，具有主观性、上下文相关性、动态不确定性及时间滞后性的特点。可

信度量的计算包括直接可信度、间接可信度及综合可信度的计算 3 部分。

1) 直接可信度计算

定义 5 设 $\lambda(t)$表示时效性因子，其公式为

$$\lambda(t)=1-\frac{\Delta t\times\xi}{t-t_0} \tag{3}$$

其中，$\lambda(t)\in(0,1)$，$\xi\in(0,1)$，t_0 为计算的起始时刻，t 为当前时刻，Δt 为相邻 2 次计算的时间差。

ξ 用于调节衰减速率，其值越大，可信度衰减速度越快，反之衰减速度越慢。时效性因子充分考虑了可信度随时间动态衰减的影响，有效提高了可信度计算的准确性。

定义 6 设 δ 表示惩罚因子，其公式为

$$\delta=\begin{cases}1,\Delta DTD_n\geqslant 0\\ 0<\delta<1,\Delta DTD_n<0\end{cases} \tag{4}$$

其中，$\delta\in(0,1)$，DTD_n 为直接可信度，$\Delta DTD_n=DTD_n(t)-DTD_n(t-1)$。

当 $\Delta DTD_n<0$ 时要对可信度进行惩罚，δ 用于调节惩罚力度，其值越小，惩罚力度越大；反之惩罚力度越小。惩罚因子对提供虚假、恶意服务的实体进行严厉的惩罚，使其快速下降到可信阈值以下，并限制其网络访问控制权限，从而能够有效地遏制恶意实体的攻击。

定义 7 设 $\forall x_i\in X$，称 $DTD_n(x_i,x_j,C(hew，t),t)$ 为实体 x_i 对 x_j 在时刻 t 以及交互上下文 $C(hew，t)$ 条件下的直接可信度，令

$$DTD_n(x_i,x_j,C(hew,t),t)$$

$$=\begin{cases}\left(\frac{1}{n},\frac{1}{n},\cdots,\frac{1}{n}\right),t=0\\ DTD_n(x_i,x_j,C(hew,t-1),t-1)\cdot\lambda(t),\Delta C=\Phi\\ DTD_n(x_i,x_j,C(hew,t),t)\cdot\delta,\text{其他}\end{cases} \tag{5}$$

其中，x_i 与 x_j 分别表示本实体和目标实体，$C(hew,t)$表示时刻 t 之前实体 x_i 与 x_j 交互的上下文证据，HEW 表示有效历史交互证据窗口，hew 表示在历史交互证据窗口中 x_i 与 x_j 之间的有效证据，$\Delta C=C(HEW,t)-C(HEW,t-1)$，$\lambda(t)$表示时效性因子，$\delta$ 表示惩罚因子，$DTD_i(x_i,x_j,C(hew,t),t)$表示 x_i 对 x_j 在时刻 t 以及交互上下文 $C(hew,t)$条件下进行可信度量，且度量结果满足可信等级为 l_i 的概率，并且 $\sum_{i=1}^{n}DTD_i=1$。

综上所述，当模型初始化时，将邻接目标实体的直接可信度等概率均分为$(1/n,1/n,\cdots,1/n)$，允许邻接实体接入网络，分配基本的网络访问控制权，继续监视其交互上下文并进行度量；若时刻 t 与 $t-1$ 相比，并没有新的交互上下文证据，则当前时刻的直接可信度随时间推移而衰减；当直接可信度增量为正时，无需惩罚，当增量为负时，需要对可信度进行惩罚，使其快速下降到可信阈值以下，限制其访问控制权限。

2) 间接可信度计算

定义 8 设 $\forall x_i\in X$，称 $ITD_n(x_i,x_j,C(hew,t),t)$ 为实体 x_i 对 x_j 在时刻 t 以及交互上下文 $C(hew，t)$ 条件下的间接可信度。间接可信度的计算即将目标实体的邻接节点对其的综合可信度量传递到本实体，作为目标实体间接可信度计算的依据。令

$$ITD_n(x_i,x_j,C(hew,t),t)=\begin{cases}\left(\frac{1}{n},\frac{1}{n},\cdots,\frac{1}{n}\right),t=0\\ ITD_n(x_i,x_j,C(hew,t-1),t-1)\cdot\lambda(t),\Delta C=\Phi\\ \delta\cdot\dfrac{\sum_{Z\in X}DTD_n(x_i,x_k,C(hew,t-1),t-1)\times OTD_n(x_k,x_j,C(hew,t-1),t-1)}{\sum_{Z\in X}DTD_n(x_i,x_k,C(hew,t-1),t-1)},\text{其他}\end{cases} \tag{6}$$

式(6)中，$\boldsymbol{Z}$ 表示与目标实体有邻接关系的实体集合。当模型初始化时，将邻接实体的间接可信度等概率均分为$(1/n,1/n,\cdots,1/n)$；若时刻 t 与 $t-1$ 相比，并没有新的关于目标实体的间接可信度推荐，则将当前的间接可信度随时间推移而衰减；若当前存在多个推荐，且交互上下文不断更新，则对目标实体的间接可信度计算需要综合考虑本实体与中间实体的直接可信度及中间实体对目标实体的综合可信度推荐，且当间接可信度增量为正时，无需惩罚，当增量为负时，需要对间接可信度进行惩罚，使其快速下降到阈值以下。

3) 综合可信度计算

定义 9 设 ω 表示直接可信度的权重因子，其公式为

$$\omega = \frac{HEW + hew}{2HEW} \tag{7}$$

其中，$\omega \in (0.5,1]$。

ω 是一个与交互上下文相关的变量，由于 $\omega \in (0.5,1]$，所以直接可信度的权重始终大于间接可信度的权重，使得综合可信度总是优先相信自己的直接判断，当证据充足时，无须考虑第三方推荐，从而能够尽可能地降低风险，这符合人类社会的认知习惯。

定义 10　设 $\forall x_i \in X$，称 $OTD_n(x_i, x_j, C(hew, t), t)$ 为实体 x_i 对 x_j 在时刻 t 以及交互上下文 $C(hew, t)$ 条件下的综合可信度量，简称可信度。令

$$OTD_n(x_i,x_j,C(hew,t),t) = \begin{cases} ITD_n(x_i,x_j,C(hew,t),t), C(hew,t) = \Phi \\ DTD_n(x_i,x_j,C(hew,t),t), C(hew,t) = C(HEW,t) \\ OTD_n(x_i,x_j,C(hew,t-1),t-1)\cdot\lambda(t), \Delta C = \Phi \\ \delta\cdot\left[\omega\cdot DTD_n(x_i,x_j,C(hew,t),t) + (1-\omega)ITD_n(x_i,x_j,C(hew,t),t)\right], \text{其他} \end{cases} \tag{8}$$

式(8)中，若时刻 t 与 $t-1$ 相比，综合可信度没有变化，则将其衰减；若当前交互上下文不断更新，则对目标实体的综合可信度计算需要综合考虑直接可信度和间接可信度，且当综合可信度增量为正时，无需惩罚，当增量为负时，需要对综合可信度进行惩罚，使其快速下降到阈值以下。

4.4　可信度量的更新

可信度量计算过程本身就是不断迭代更新的过程，度量结果对后续证据的采集产生指导意义，同时后续证据也会驱动可信度量的更新。此外，以可信度量为依据，路由和控制策略的实施及反馈结果同样能够驱动可信度量更新。

5　仿真实验

仿真建模工具采用 Genie，它是由匹兹堡大学决策系统实验室开发的一种基于决策理论的、图形化的建模开发工具。Genie 能够非常方便地进行静/动态贝叶斯网络建模，并能够进行先验概率的初始赋值及后验概率的计算，进行知识传递和积累。

仿真实验主要考虑 2 方面：1)本模型的有效性；2)本模型的优势，将传统贝叶斯网络模型(BNM)与文献[5]提出的基于贝叶斯网络的动态可信模型(BDTM)进行对比分析。

5.1　仿真实验设计

1) 提取变量

仿真实验根据如图 1 所示的可信度量指标体系提取变量。

2) 确定变量间的依赖关系

如图 3 所示，变量间的依赖关系通过单向箭头表示，箭尾对应变量依赖于箭头变量。

3) 确定变量间的条件概率分布

参照图 3 中变量间的依赖关系，通过可信认知模块，将证据库中的有效证据进行等级划分并规范化表示为区间[0,1]的数值，根据专家知识及交互上下文证据库，确定变量间的条件概率分布。当模型初始化时，由于证据不足，条件概率矩阵的形成更多地需要结合专家知识以及以往的经验值，虽然存在一定的假设和主观性，但是在运行过程中，随着

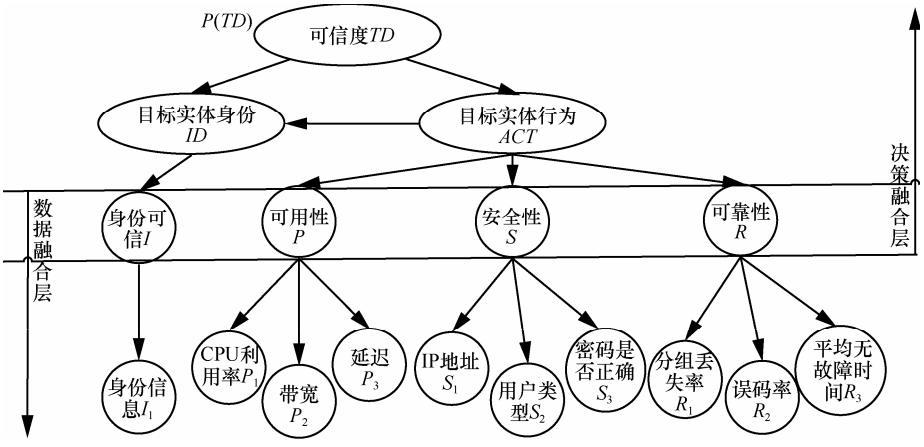

图 3　变量间的依赖关系

表 1 初始状态时变量 *TD*、*I*、*ID*、*ACT*、*C*、*P*、*S*、*R* 间的条件概率分布

P(*A*|*B*)	*P*(*A*=*H*|*B*=*H*)	*P*(*A*=*H*|*B*=*M*)	*P*(*A*=*H*|*B*=*L*)	*P*(*A*=*M*|*B*=*H*)	*P*(*A*=*M*|*B*=*M*)	*P*(*A*=*M*|*B*=*L*)	*P*(*A*=*L*|*B*=*H*)	*P*(*A*=*L*|*B*=*M*)	*P*(*A*=*L*|*B*=*L*)
P(*ID*|*TD*)||*P*(*ACT*|*TD*)||*P*(*I*|*ID*)	0.8	0.4	0.1	0.15	0.5	0.2	0.05	0.1	0.7
P(*P*|*ACT*)||*P*(*S*|*ACT*)||*P*(*R*|*ACT*)	0.9	0.5	0.1	0.1	0.4	0.3	0	0.1	0.6
P(*R*1|*R*)||*P*(*R*2|*R*)||*P*(*R*3|*R*)	0.9	0.5	0.1	0.05	0.4	0.4	0.05	0.1	0.5
P(*P*1|*P*)||*P*(*P*2|*P*)||*P*(*P*3|*P*)	0.8	0.4	0.2	0.1	0.5	0.3	0.1	0.1	0.5
P(*S*1|*S*)||*P*(*S*2|*S*)||*P*(*S*3|*S*)	0.7	0.3	0.1	0.2	0.4	0.2	0.1	0.3	0.7

交互上下文证据的不断补充和更新，通过迭代计算，可以对条件概率矩阵进行不断调整，以提高评估结果的准确性和可信性。如表 1 所示，列出了初始状态时变量间的条件概率分布，其中，*B* 表示先验交互证据，分为高、中、低 3 种等级，分别用 *H*、*M*、*L* 表示，*P*(*A*/*B*)则表示 *B* 发生条件下 *A* 发生的概率。

4) 仿真实验参数设置

仿真实验参数说明及设置如表 2 所示。

表 2 仿真实验参数设置说明

参数	默认值	描述
HEW	1 000	历史交互证据窗口所包含证据数
hew	200	本实体与目标实体的有效证据数
L	3	交互证据分为 3 个等级(*H*、*M*、*L*)
N	10	本实体的邻接实体数量
ξ	0.05	调节衰减速率的常量
Θ	0.3	综合可信度阈值
T	10	仿真迭代次数

5.2 仿真实验 1：本模型的有效性

按照图 3 及 5.1 节的描述进行配置，构建基于动态贝叶斯网络的可信度量模型，通过 10 个步长的仿真实验，来验证本模型的动态自适应性及计算的准确性。

1) λ 及 δ 的取值对模型的影响

如图 4 所示，显示了<λ,δ>取值分别为<0.95,0.3>、<0.95,0.2>、<0.9,0.3>及<1,1>时的对比曲线图，<1,1>取值下表示模型时效性因子和惩罚因子无效。其中，圆形相连表示<0.95,0.3>时的曲线，菱形相连表示<0.95,0.2>时的曲线，正方形相连表示<0.9,0.3>时的曲线，三角形相连表示<1,1>时的曲线。整个仿真过程为 10 个步长，采集到特定目标实体的证据等级依次为 *H*、*H*、*L*、*M*、*H*、*H*、*Φ*、*Φ*、*Φ*、*Φ*。在 *T*=0,1 时，分别采集到等级为 *H* 的证据，此刻，对该目标实体的综合可信度在缓慢增加；在 *T*=3 时，采集到等级为 *L* 的证据，此时除三角形曲线外其他曲线的综合可信度均迅速下降到 0.1 以下，远远低于系统设定的综合可信度阈值 0.3，而三角形曲线下降至 0.3；此后，在 *T*=4、5、6 时，均采集到等级为 *H* 的证据，所有曲线均不同程度上升；在 *T*=7、8、9、10 时，未收集到任何证据，此时除三角形曲线保持不变外，其他曲线均缓慢下降。

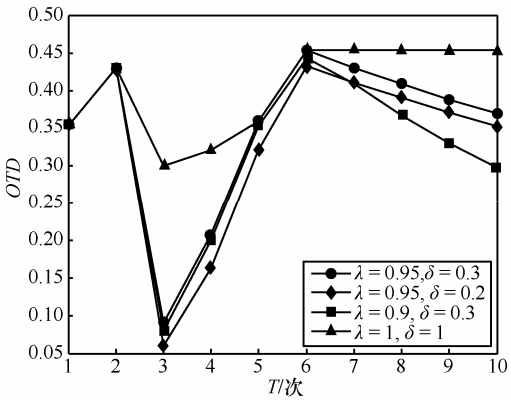

图 4 λ 及 δ 的取值对模型的影响

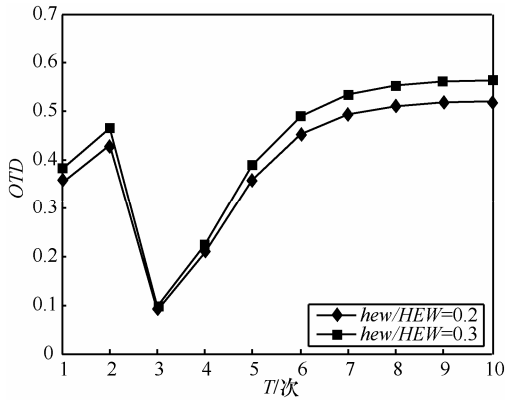

图 5 *hew*/*HEW* 的取值对模型的影响

通过对比实验得出，在引入时效性因子 λ 和惩罚因子 δ 后，本模型能够对交互上下文做出敏捷反应，针对异常行为使其综合可信度快速下降到阈值

以下，限制其资源调配与访问控制权限，从而有效抑制了异常实体的威胁；当没有有效证据时，目标实体的综合可信度慢慢衰减，知识库逐渐老化，更加符合人类认识的习惯。此外，λ 和 δ 对模型的灵敏度以及准确度具有调节作用，在 $\lambda\to1$ 的过程中，说明模型知识的新陈代谢越慢，适用于交互较少的系统；在 $\delta\to0$ 的过程中，说明模型对不可信行为的惩罚力度越大，适用于对安全可信要求高的系统。

2) *hew/HEW* 的取值对模型的影响

如图 5 所示，在采集证据等级依次为 *H*、*H*、*L*、*M*、*H*、*H*、*H*、*H*、*H*、*H* 情况下，菱形相连的曲线为 *hew/HEW*=0.2 时的综合可信度迭代情况，正方形相连的曲线为 *hew/HEW*=0.3 时的综合可信度迭代情况。从图 5 中可以得到，在对目标实体进行可信度量时，有效交互证据数量占历史交互证据窗口的比例越大，确定性信息越多，越有利于进行综合可信度评估。在 *hew/HEW*→1 的过程中，随着本地证据和知识的累积，能够越来越清晰、准确地刻画综合可信度，这与人类社会的认知习惯一致。

5.3　仿真实验 2：与其他模型的对比分析

本节以图 3 的指标体系及 5.1 节的实验方案为依据，通过对比分析传统贝叶斯网络模型(BNM)及基于贝叶斯网络的动态可信模型(BDTM)[8]，验证本模型的优越性和有效性。

1) 当 *hew/HEW*=0.2 时，本模型与 BNM、BDTM 的对比

如图 6 所示，在 *hew/HEW*=0.2 且<λ,δ>取值为<0.95,0.3>时，采集到特定目标实体的证据等级依次为 *H*、*H*、*L*、*M*、*H*、*H*、*H*、*H*、*H*、*H* 情况下，菱形、正方形、三角形相连的曲线分别表示本模型与 BNM、BDTM 的迭代情况。通过对比可知，在 *T*=3 时，采集到等级为 *L* 的证据，本模型的综合可信度下降最快，由 0.43 迅速下降至 0.09，BDTM 次之，由 0.424 迅速的下降为 0.107，BNM 下降最缓慢且存在延迟，由 0.424 下降为 0.355，在 *T*=4 时进一步的下降至 0.254；在 *T*=7、8、9、10 时，采集证据等级均为 *H*，3 种模型的综合可信度均缓慢增加，本模型由 0.45 缓慢的增加到 0.515。本组实验体现了本模型对威胁行为能够迅速作出反应，且当不断采集到有利证据时，其综合可信度缓慢增加；而传统的贝叶斯网络模型，针对异常交互，明显的反应滞后，针对有利证据，其增速的变化率要高于本模型。另外，菱形、正方形两组曲线对比得出，在<λ,δ>取值一定的情况下，本模型比 BDTM 具有更好的灵敏性和准确性。该实验表明本模型在稳定性、灵敏性以及准确性上均优于 BNM 和 BDTM。

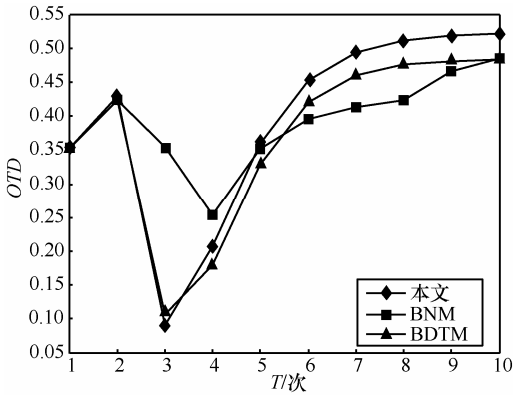

图 6　*hew/HEW*=0.2 时本模型与 BNM、BDTM 的对比

2) 当 *hew/HEW* = 0.3 时，本模型与 BNM、BDTM 的对比

如图 7 所示，反映了在 *hew/HEW*=0.3 且<λ,δ>取值为<0.95,0.3>时，采集到特定目标实体的证据等级依次为{*H*、*H*、*L*、*M*、*H*、*H*、*H*、*H*、*H*、*H*}情况下，本模型与 BNM、BDTM 的对比情况。结合图 6 的实验相比得出，随着有效交互证据数量占历史交互证据窗口比例的增大，相应确定性信息的增多，更加有利于进行综合可信度评估，计算的灵敏性和有效性也越来越高，进一步验证了本模型与 BNM、BDTM 相比具有更好的动态适应性、灵敏性、有效性和连续度测能力。

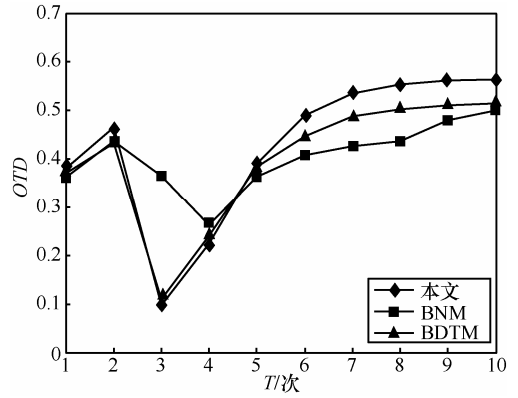

图 7　*hew/HEW*=0.3 时本模型与 BNM、BDTM 的对比

通过以上仿真实验及分析，得出以下结论：当有利证据逐渐增多时，通过动态贝叶斯网络的推理方法，被评估实体的综合可信度值缓慢增加，符合人类社会行为规范，说明基于动态贝叶斯网络的可信度量模型是有效的。同理，针对不利证据的收集，

采用惩罚策略使目标实体的综合可信度快速下降到可信阈值以下，并进行有效隔离，从而降低其对网络的威胁和破坏。

6 结束语

针对目前可信度量模型动态自适应能力差的问题，本文提出了基于动态贝叶斯网络的可信度量模型，充分考虑了交互上下文的时效性，通过引入了历史交互证据窗口、时效性因子和惩罚因子，能够灵敏、有效地计算出网络实体间的可信度量值，仿真实验结果表明本模型在动态不确定网络环境下具有连续的可信度量能力，为基于可信度量的可信连接、可信管理及可信决策的研究奠定了较好的基础。下一步的工作是对本模型做进一步的完善，并对基于可信度量的可信连接展开研究。

参考文献：

[1] Trusted Computing Group TCG Trusted Network Connect TNC Architecture for Interoperability Specification Version 1.2[S]. 2007.

[2] Cisco Systems, Inc network admission control introduction[EB/OL]. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html, 2007.

[3] Microsoft Corporation. Introduction to network access protection[EB/OL]. http://technet.microsoft.com/en-us/network/cc984252, 2008.

[4] ALMENAREZ F, MARIN A, DIAZ D. Developing a model for trust management in pervasive devices[A]. Proc of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security (PerSec 2006)[C]. Washington DC, USA, 2006. 267-272.

[5] MELAYE D, DEMAZEAU Y. Bayesian dynamic trust model[A]. LNCS 3690[C]. Berlin: Springer-Verlag, Germany, 2005.480-489.

[6] FENG R J, XU X F, ZHOU X. A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory[J]. Sensors, 2011, 11:1345-1360.

[7] BHAVNA G, HARMEET K, NAMITA. Trust based access control for grid resources[A]. International Conference on Communication Systems and Network Technologies[C]. Jammu, India, 2011.678-682.

[8] SUN Y, YU W, HAN Z. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, Selected Areas in Communications, 2006, 249(2):305-319.

[9] 李小勇, 桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报, 2009, 32(3):405-416.
LI X Y, GUI X L. Trust quantitative model with multiple decision factors in trusted network[J]. Chinese Journal of Computers, 2009, 32(3):405-416.

[10] MARSH S. Formalising Trust as a Computational Concept[D]. Stirling: University of Stirling, 1994.

[11] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[A]. Proceedings of the 17th Symposium on Security and Privacy Oakland[C]. Oakland, CA, 1996.164-173.

[12] ABDUL-RAHMAN A, HAILES S. Using recommendations for managing trust in distributed systems[A]. Proceedings of IEEE Malaysia International Conference on Communication[C]. Kuala Lumpur, Malaysia, 1997. 1-7.

[13] AHAMED S I, SHARMIN M. A trust-based secure service discovery(TSSD) model for pervasive computing[J]. Journal of Computer Communications, 2008, 31(18):4281-4293.

[14] AHAMED S I, HAQUE M M. Design, analysis and deployment of omnipresent formal trust model(FTM) with trust bootstrapping for pervasive environment[J]. Journal of Systems and Software, 2010, 83(2):253-270.

[15] HABIB S M, RIES S, MÜHLHÄUSER M. Towards a trust management system for cloud computing[A]. IEEE 10th International Conference[C]. Changsha, China, 2011. 933-939.

[16] RANGASAMY K, SOMASUNDARAM T S. Trust management system for computational grids[J]. European Journal of Scientific Research, 2012, 79(1):15-23.

[17] 桂春梅, 蹇强, 王怀民. 虚拟计算环境中基于重复博弈的惩罚激励机制[J]. 软件学报, 2010, 21(12):3042-3055.
GUI C M, JIA Q, WANG H M. Repeated game theory based penalty-incentive mechanism in internet-based virtual computing environment[J]. Journal of Software, 2010, 21(12):3042-3055.

[18] 胡建理, 周斌, 吴泉源. P2P 网络中具有激励机制的信任管理研究[J]. 通信学报, 2011, 32(5):22-32.
HU J L, ZHOU B, WU Q Y. Research on incentive mechanism integrated trust management for P2P networks[J]. Journal on Communications, 2011, 32(5):22-32.

[19] 石志国, 刘冀伟, 王志良. 基于时间窗反馈机制的动态 P2P 信任模型[J]. 通信学报, 2010, 31(2):120-129.
SHI Z G, LIU J W, WANG Z L. Dynamic P2P trust model based on time-window feedback mechanism[J]. Journal on Communications, 2010, 31(2):120-129.

[20] 李小勇, 桂小林. 动态信任预测的认知模型[J]. 软件学报, 2010, 21(1):163-176.
LI X Y, GUI X L. Cognitive model of dynamic trust forecasting[J]. Journal of Software, 2010, 21(1):163-176.

作者简介：

梁洪泉（1981-），男，河北石家庄人，通信网络信息传输与分发技术重点实验室博士生、工程师，主要研究方向为可信网络、通信系统与网络仿真。

吴巍（1956-），男，重庆忠县人，硕士，通信网络信息传输与分发技术重点实验室研究员、博士生导师，主要研究方向为通信网技术。