文章编号:1009-3087(2015)03-0101-07 DOI:10.15961/j.jsuese.2015.03.014

基于隐 Markov 过程的网络信任评估模型

郜 燕[1,2],刘文芬[1,2]
(1.解放军信息工程大学 网络空间安全学院,河南 郑州 450002;2.数学工程与先进计算国家重点实验室,河南 郑州 450002)

摘 要:为了快速精确地刻画实体行为的高动态性,提出一种基于连续时间隐 Markov 过程的信任评估模型。不同于离散时间隐 Markov 信任模型,该模型充分考虑到信任的时间相关性,结合交互记录之间的时间间隔,将实体信任评估问题归结为连续时间隐 Markov 过程的学习问题。进而利用改进的和声搜索算法,给出求解隐 Markov 过程最佳参数的算法,该算法有效地保证了全局搜索空间,能够获得更好的解。在此基础上,利用已有交互结果序列和最优参数组,对实体的信任度进行预测。仿真实验表明,该模型能够快速地反映出实体行为的动态性,具有较高的精确度,且能抵抗部分恶意攻击。

关键词:动态信任;隐 Markov 过程;和声搜索算法;信任度;微调空间
中图分类号:TP393 **文献标志码**:A

A Dynamic Trust Evaluation Model Based on Optimized Hidden Markov Process

GAO Yan[1,2], *LIU Wenfen*[1,2]
(1. School of Cyberspace Security, PLA Info. Eng. Univ., Zhengzhou 450002, China;
2. State Key Lab. of Mathematical Eng. and Advanced Computing, Zhengzhou 450002, China)

Abstract: In order to depict high dynamic of entity behavior quickly and accurately, a trust evaluation model based on continuous-time hidden Markov process was proposed. Different from the trust models on discrete-time hidden Markov chain, this model fully considered time dependence of trust, combined time intervals between the interactions and made the trust evaluation problem boil down to the learning problem of continuous-time hidden Markov process. Then an algorithm for solving the optimal parameters of hidden Markov process was given with the improved harmony algorithm, which could effectively guarantee the global search space and achieve a better solution. On this basis, the trust degree could be predicted using the existing interaction sequences and optimal parameters. Simulation results showed that the model is able to quickly reflect the dynamic of entity behavior, has high accuracy and resists the malicious attacks.

Key words: dynamic trust; hidden Markov process; harmony search algorithm; trust degree; adjustment space

随着网络新技术的快速发展,基于互联网的应用呈现出爆炸式的发展态势,电子商务、网上银行和社交网络等新的互联网应用得到广泛部署,SDN、云计算和 P2P 计算等新型分布式网络技术也使得互联网的应用更加简单高效。然而,当前网络的安全机制不够完善,因此所引发的安全可信任问题引起了人们的广泛关注。作为保障网络安全的一种"软安全"技术,信任问题的研究是安全基础理论的重要组成部分[1]。动态信任管理技术为解决开放网络环境中新应用形式的安全问题提供了新思路,是新一代互联网安全技术研究的热点问题[2]。

建立可靠的信任模型,对实体信任度进行评估和预测是动态信任管理技术的核心工作,所用到的方法主要包含加权平均法、概率统计方法、模糊逻辑方法和 D-S 证据理论等。概率信任模型主要利用贝叶斯方法、隐 Markov 模型(HMM)和因子图[3]等方法研究实体间的信任关系。Elsalamouny 等[4]指出贝叶斯信任模型适用于对稳定性较高的实体进行信任评估,而不足以用来描述高动态性的实体行为特征。Moe 等通过比较具有时间衰减性的贝叶斯信任

收稿日期:2014-07-03
基金项目:国家"973"计划重点项目资助(2012CB315905;2012CB315901)
作者简介:郜 燕(1986—),女,博士生.研究方向:信息安全和信任管理. E-mail:gaoyan_yangao@163.com

模型和HMM信任模型[5],说明利用HMM方法所建立的信任模型能够更准确地刻画高动态性实体间的信任关系。Liu等[6]构建了上下文环境感知的动态信任模型,通过将离散的信任评价集合作为嵌入Markov链的状态空间,选取与交互环境相关的特征子集合作为HMM的观测符号集合,将信任计算问题归结为HMM的解码问题。基于状态转移概率矩阵和观测矩阵的获取方法,给出了实体信任度的计算方法。文献[7]给出的PSOHMM信任模型通过将粒子群搜索算法和HMM模型结合,将HMM模型参数的局部最优解转化为全局最优解,进而建立了PSOHMM信誉评估模型,并将其应用于Amazon电子商务的信任评估。在文献[8]中,为了在尽可能减少存储、传输和计算等开销的条件下得到待评估实体行为的HMM模型参数,评估实体和反馈实体首先利用自身交互记录计算所对应的先验HMM参数,进而评估实体利用部分反馈交互信息,结合Jensen不等式和Lagrange乘子法等数学方法计算得到最优HMM参数,给出了一种基于离散时间HMM的分布式信任模型。

这些最新的研究工作有效地推动了信任评估与预测研究的发展,但仍然存在一些问题。信任是与时间密切相关的一个动态变量,随着时间的演进而动态地发生变化。然而,现有基于离散时间HMM的信任模型均假设交互结果之间是等时间间隔的,在该假设条件下的信任模型就不足以体现信任的动态变化性。基于此,作者通过考虑信任的时间相关性,利用连续时间隐Markov过程建立了信任评估模型。由于实体行为是不断变化的,而该行为对评估者是隐含的,评估者只能通过交互结果来推测待评估实体的行为状态。通过将待评估实体的所有可能的行为状态集合看作隐Markov过程的状态空间,将实体间可能的交互结果看作隐Markov过程的观测符号集合,从而利用连续时间隐Markov过程建立了信任评估模型,将实体信任评估问题归结为连续时间隐Markov过程的学习问题,即从收集到的交互结果序列出发,估计隐Markov过程的最佳参数组。为了更有效地求解隐Markov过程的学习问题,利用改进的和声搜索HS算法给出了计算最优模型参数的具体算法,该算法保证了全局搜索空间,能够获得更好的解,提高了模型的准确度。在此基础上,利用已有交互结果序列及最优参数组,对当前及未来时刻待评估实体的信任度进行预测。

1 基于优化隐Markov过程的信任评估模型

1.1 利用隐Markov过程构建信任模型

在动态网络中,待评估实体的行为是不断动态变化的,所处状态会直接影响交互结果,而评估实体不能观测到待评估实体本身的行为状态,只能根据历史交互结果来推测它的行为动态以及未来时刻给出的交互结果,因此可利用隐Markov过程[9]对待评估实体建立信任评估模型。主要思想是从已收集到的交互结果序列出发,估计隐Markov过程的最优参数组λ,进而预测待评估实体的信任度。该模型能够适用于集中式或者分布式网络环境中。在集中式信任模型中,由管理器负责收集其他实体对待评估实体的交互结果;在分布式信任模型中,由评估实体通过一定的信任信息收集方式得到待评估实体的交互结果,进而建立信任评估模型。具体模型如下:

设$X(t)$为待评估实体在时刻t的行为状态,$\{X(t),t\geq 0\}$为连续时间Markov链,状态集合$S=\{1,2,\cdots,M\}$,初始分布$\boldsymbol{\pi}=\{\pi_i,i\in S\}$,密度矩阵为$\boldsymbol{Q}$。设随机变量$Y$表示评估实体(管理器)可观测到的交互结果,取值集合为Y,$|Y|=N$。对任意的$t\geq 0$,$i\in S$和$y\in Y$,在已知$X(t)=i$的条件下,观测符号为y的概率记为$b(y|i)=P(Y_t=y|X(t)=i)$,因此观测矩阵$\boldsymbol{B}=[b(y|i)]_{M\times N}$。为了叙述方便,隐Markov过程$\{(X(t),Y_t),t\geq 0\}$可用参数组$\lambda=(\boldsymbol{\pi},\boldsymbol{Q},\boldsymbol{B})$来表示。

设$\boldsymbol{y}^l=y_1y_2\cdots y_l$为长度$l$的交互结果序列,$y_i$所对应的交互时刻为$t_i$,其中,$y_i\in Y(1\leq i\leq l)$,$0=t_1<t_2<\cdots<t_l$。对任意的$1\leq k\leq l-1$,令$\Delta t_k=t_{k+1}-t_k$,则交互结果序列为$\boldsymbol{y}^l$的概率为:

$$P_\lambda(\boldsymbol{y}^l)=\sum_{s_1,s_2,\cdots,s_l\in S}P(s_1,s_2,\cdots,s_l,\boldsymbol{y}^l)=$$
$$\sum_{s_1,\cdots,s_l\in S}\pi_{s_1}b(y_1|s_1)\prod_{i=2}^{l}P_{s_{i-1}s_i}(\Delta t_{i-1})b(y_i|s_i)=$$
$$\sum_{s_1,\cdots,s_l\in S}\pi_{s_1}b(y_1|s_1)\prod_{i=2}^{l}(\mathrm{e}^{Q\Delta t_{i-1}})_{s_{i-1}s_i}b(y_i|s_i) \tag{1}$$

其中,对任意的$2\leq i\leq l$,

$P_{s_{i-1}s_i}(\Delta t_{i-1})=P(X(t_{i-1}+\Delta t_{i-1})=s_i|X(t_{i-1})=s_{i-1})$,且式(1)中最后一个等式由柯尔莫哥洛夫微分方程:

$P(\Delta t_{i-1})=(P_{jk}(\Delta t_{i-1}))_{M\times M}=\mathrm{e}^{Q\Delta t_{i-1}}$, $j,k\in S$

即可得到。

已知待评估实体的交互结果序列$\boldsymbol{y}^l$,寻找最佳

模型参数 $\lambda = (\boldsymbol{\pi}, \boldsymbol{Q}, \boldsymbol{B})$,可以转化为求解带约束条件的最大化问题:

$$\begin{cases} f(\boldsymbol{\lambda}) = \max\limits_{\boldsymbol{\lambda}} \log P_{\boldsymbol{\lambda}}(\boldsymbol{y}^l) \\ \text{subject to: } 0 \le \pi_i \le 1,\ 1 \le i \le M; \\ \sum\limits_{i=1}^{M} \pi_i = 1; \\ 0 \le b(y \mid i) \le 1,\ 1 \le i \le M, y \in Y; \\ \sum\limits_{y \in Y} b(y \mid i) = 1, 1 \le i \le M; \\ q_{ij} > 0,\ 1 \le i, j \le M, i \ne j; \\ q_{ii} = -\sum\limits_{j \ne i} q_{ij},\ 1 \le i \le M。 \end{cases}$$

在式(1)中取 $t_1 = 0$ 的原因:设当前时刻为 t,由于信任具有时间衰减性,只需考虑一段时间 $[t - T, t)(0 < T < t)$ 内的交互结果,而之前的交互结果对当前时刻信任度的影响可以忽略不计,因此在 $[t - T, t)$ 内第一个交互发生的时刻可记为 $t_1 = 0$,继而以 $t_1 = 0$ 为开始时刻记录之后发生的交互结果。

1.2　利用和声搜索 HS 算法求解隐 Markov 过程的参数

利用和声搜索 HS 算法[10-12]求解隐 Markov 过程的学习问题。首先,将矩阵 $\boldsymbol{Q}$ 和 $\boldsymbol{B}$ 改写为向量形式,即:

$$\boldsymbol{Q} = (q_{11}, \cdots, q_{1M}, \cdots, q_{M1}, \cdots, q_{MM}),$$
$$\boldsymbol{B} = (b_{11}, \cdots, b_{1N}, \cdots, b_{M1}, \cdots, b_{MN})。$$

由于隐 Markov 过程的参数 $\boldsymbol{\pi}$、$\boldsymbol{Q}$ 和 $\boldsymbol{B}$ 是互不影响的,因此可将其看作 HS 算法的 3 个向量变量,在所对应的定义域中通过随机选择、记忆库选择或者微调计算方式产生新解,进而得到最优模型参数。不同于原有 HS 算法的微调计算方式,该算法通过定义 3 个不同的微调空间,对 $\boldsymbol{\pi}$、$\boldsymbol{Q}$ 和 $\boldsymbol{B}$ 独立地进行微调。具体算法步骤如下:

步骤 1:给定待评估实体的交互结果序列 $\{(y_i, t_i), 1 \le i \le l, t_1 < t_2 < \cdots < t_l\}$,定义目标函数 $f(\lambda)$,向量变量 $\boldsymbol{\pi}$、$\boldsymbol{Q}$ 和 $\boldsymbol{B}$ 的定义域分别为 X_1,X_2 和 X_3 以及 HS 算法参数:和声记忆库的大小 HMS,记忆库取值概率 $HMCR$、微调概率 PAR、各向量变量的微调空间大小 $C_m(1 \le m \le 3)$、微调带宽 BW 以及迭代次数 $I_{\max}$,其中,$C_m \gg HMS$ 且 $C_m > BW$。

步骤 2:在各向量变量的约束条件下,随机生成和声记忆库和微调空间。由于 $\boldsymbol{\pi}$、$\boldsymbol{Q}$ 和 $\boldsymbol{B}$ 是互不影响的,因此可将其独立进行取值,进而生成和声记忆库。对任意的 $1 \le k \le HMS$,记:

$$\boldsymbol{\pi}^k = (\pi_1^k, \pi_2^k, \cdots, \pi_M^k),$$
$$\boldsymbol{Q}^k = (q_{11}^k, \cdots, q_{1M}^k, \cdots, q_{M1}^k, \cdots, q_{MM}^k),$$
$$\boldsymbol{B}^k = (b_{11}^k, \cdots, b_{1N}^k, \cdots, b_{M1}^k, \cdots, b_{MN}^k),$$

则和声记忆库

$$\boldsymbol{HM} = \begin{bmatrix} \boldsymbol{\pi}^1 & \boldsymbol{Q}^1 & \boldsymbol{B}^1 \\ \boldsymbol{\pi}^2 & \boldsymbol{Q}^2 & \boldsymbol{B}^2 \\ & \cdots & \\ \boldsymbol{\pi}^{HMS} & \boldsymbol{Q}^{HMS} & \boldsymbol{B}^{HMS} \end{bmatrix},$$

且当 $i \ne j$ 时,$\boldsymbol{HM}^i \ne \boldsymbol{HM}^j$,其中,$\boldsymbol{HM}^i$ 表示矩阵 $\boldsymbol{HM}$ 中第 i 行。

对任意的 $1 \le m \le 3$,分别在定义域 X_m 中随机选择 C_m 个向量构成所对应变量的微调空间,即随机选取 $\boldsymbol{\pi}_i \in X_1(1 \le i \le C_1)$,$\boldsymbol{Q}_i \in X_2(1 \le i \le C_2)$ 和 $\boldsymbol{B}_i \in X_3(1 \le i \le C_3)$,因此向量变量 $\boldsymbol{\pi}$、$\boldsymbol{Q}$ 和 $\boldsymbol{B}$ 的微调空间为:

$$\boldsymbol{G}_1 = (\boldsymbol{\pi}_1 \quad \boldsymbol{\pi}_2 \quad \cdots \quad \boldsymbol{\pi}_{C_1})^{\tau},$$
$$\boldsymbol{G}_2 = (\boldsymbol{Q}_1 \quad \boldsymbol{Q}_2 \quad \cdots \quad \boldsymbol{Q}_{C_2})^{\tau},$$
$$\boldsymbol{G}_3 = (\boldsymbol{B}_1 \quad \boldsymbol{B}_2 \quad \cdots \quad \boldsymbol{B}_{C_3})^{\tau}。$$

其中,对任意的 $1 \le i, j \le C_m$ 且 $i \ne j$,有 $\boldsymbol{\pi}_i \ne \boldsymbol{\pi}_j$,$\boldsymbol{Q}_i \ne \boldsymbol{Q}_j$ 和 $\boldsymbol{B}_i \ne \boldsymbol{B}_j$。在生成新的解变量过程中,若需要进行微调计算,则微调后变量在所对应的微调空间中进行选择。微调空间越大,搜索空间越大,所求解向量才会更优。

步骤 3:生成新的隐 Markov 过程参数。为表述方便,对任意的 $1 \le k \le HMS$,记 $\boldsymbol{\lambda}^k = (\boldsymbol{\lambda}_1^k, \boldsymbol{\lambda}_2^k, \boldsymbol{\lambda}_3^k)$,其中,$\boldsymbol{\lambda}_1^k = \boldsymbol{\pi}^k$,$\boldsymbol{\lambda}_2^k = \boldsymbol{Q}^k$ 和 $\boldsymbol{\lambda}_3^k = \boldsymbol{B}^k$。

首先,对任意的 $1 \le m \le 3$,λ_m^{new} 以概率 $HMCR$ 取自 $\boldsymbol{HM}$,而以概率 $1 - HMCR$ 在定义域 X_m 中随机选择,生成方式如下:

$$\boldsymbol{\lambda}_m^{\text{new}} \leftarrow \begin{cases} \boldsymbol{\lambda}_m^{\text{new}} \in \Omega_m, HMCR; \\ \boldsymbol{\lambda}_m^{\text{new}} \in X_m, 1 - HMCR。 \end{cases}$$

其中:

$$\Omega_1 = \{\boldsymbol{\pi}^i : 1 \le i, j \le HMS, \boldsymbol{\pi}^i \ne \boldsymbol{\pi}^j\},$$
$$\Omega_2 = \{\boldsymbol{Q}^i : 1 \le i, j \le HMS, \boldsymbol{Q}^i \ne \boldsymbol{Q}^j\},$$
$$\Omega_3 = \{\boldsymbol{B}^i : 1 \le i, j \le HMS, \boldsymbol{B}^i \ne \boldsymbol{B}^j\}。$$

其次,当新的和声 $\boldsymbol{\lambda}_m^{\text{new}} \in \boldsymbol{HM}$ 时,需以概率 PAR 在微调空间中对其进行微调,而以概率 $1 - PAR$ 保持不变。不妨设 $\boldsymbol{\lambda}_m^{\text{new}} = \boldsymbol{\lambda}_m^d, d \in \{1, 2, \cdots, HMS\}$,则

$$\boldsymbol{\lambda}_m^{\text{new}} \leftarrow \begin{cases} \boldsymbol{\lambda}_m^{\text{new}}, 1 - PAR; \\ \boldsymbol{\lambda}_m^{d^*} \in G_m, 0.5 \times PAR; \\ \boldsymbol{\lambda}_m^{d'} \in G_m, 0.5 \times PAR。 \end{cases}$$

其中,$d^* = d + BW - C_m \times \lfloor \dfrac{d + BW}{C_m + 1} \rfloor$,

$$d' = C_m + d - BW - C_m \times \lfloor \frac{C_m + d - BW}{C_m + 1} \rfloor,$$

$\lambda_m^{d^*}$ 和 $\lambda_m^{d'}$ 分别对应 G_m 中的第 d^* 和 d' 行元素。

步骤4:更新记忆库 $\boldsymbol{HM}$。令 $\boldsymbol{\lambda}^{\text{new}} = (\boldsymbol{\lambda}_1^{\text{new}}, \boldsymbol{\lambda}_2^{\text{new}}, \boldsymbol{\lambda}_3^{\text{new}})$,利用式(1)计算 $P_{\lambda^{\text{new}}}(\boldsymbol{y}^l)$。如果 $P_{\boldsymbol{\lambda}^{\text{new}}}(\boldsymbol{y}^l) > \min\limits_{1\le k\le HMS} P_{\boldsymbol{\lambda}^k}(\boldsymbol{y}^l)$,则更新和声记忆库 $\boldsymbol{HM}$,不妨设 $r = \arg\min\limits_{1\le k\le HMS} P_{\boldsymbol{\lambda}^k}(\boldsymbol{y}^l)$,则 $\boldsymbol{\lambda}^r = \boldsymbol{\lambda}^{\text{new}}$。否则 $\boldsymbol{HM}$ 保持不变。

步骤5:检查算法结束条件,若达到结束条件,则算法终止,记 $h = \arg\max\limits_{1\le k\le HMS} P_{\boldsymbol{\lambda}^k}(\boldsymbol{y}^l)$,输出 $\boldsymbol{\lambda} = \boldsymbol{\lambda}^h$ 及其所对应的目标函数值 $f(\boldsymbol{\lambda})$,否则重复执行步骤3和4。

该算法通过随机选择、记忆库选择和微调3种计算方式产生的新解,不仅保留了已存在的较优解,且通过随机选择有效地扩展了全局搜索空间[11]。另外,通过定义微调空间,且保证微调空间中向量个数远远大于记忆库大小,在满足各向量分量约束条件的基础上,尽可能地提高微调搜索空间,从而能够获得更优的解,提高了算法的精确度。

1.3 信任度的预测及计算流程

设现在时刻为 t,$\Delta t_l = t - t_l$,则由式(1)可知,对任意的 $y \in Y$,时刻 t 观测值为 y 的概率为:

$$P_{\boldsymbol{\lambda}}(y|\boldsymbol{y}^l) = P_{\boldsymbol{\lambda}}(Y(t) = y|\boldsymbol{y}^l) = \frac{P_{\boldsymbol{\lambda}}(Y(t) = y, \boldsymbol{y}^l)}{P_{\boldsymbol{\lambda}}(\boldsymbol{y}^l)},$$

其中,

$$P_{\boldsymbol{\lambda}}(Y(t) = y, \boldsymbol{y}^l) = \sum_{s_1,\cdots,s_{l+1}\in S} \pi_{s_1} b(y_1|s_1) \prod_{i=2}^{l} (\mathrm{e}^{Q\Delta t_{i-1}})_{s_{i-1}s_i} b(y_i|s_i) \cdot (\mathrm{e}^{Q\Delta t_l})_{s_l s_{l+1}} b(y|s_{l+1}).$$

因此,t 时刻的交互结果即为使得 $P_{\boldsymbol{\lambda}}(y|\boldsymbol{y}^l)$ 取得最大值的观测符号,即:

$$y_{l+1} = \arg\max_{y\in Y} P_{\boldsymbol{\lambda}}(y|\boldsymbol{y}^l).$$

综上所述,利用隐Markov过程来构建信任评估模型(简记为HSO-HMP信任模型)的主要计算流程见图1。

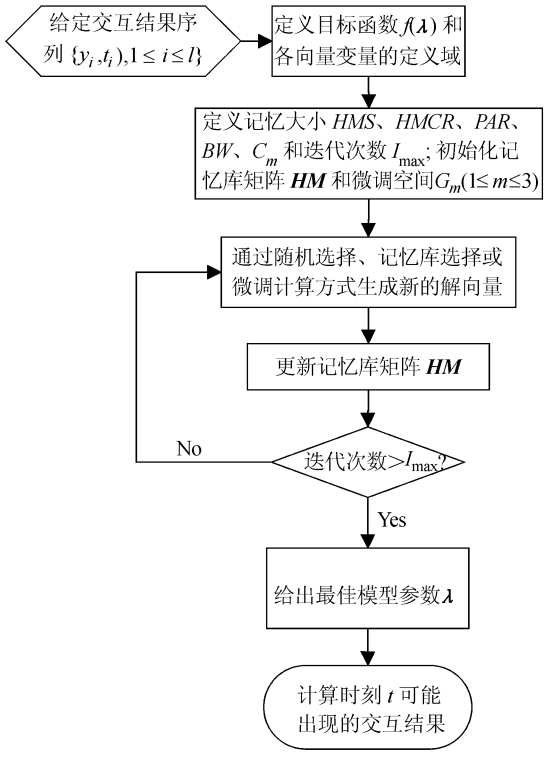

图1 HSO-HMP信任模型流程图

Fig. 1 Evaluation process of HSO-HMP trust model

表1 HSO-HMP信任模型参数

Tab. 1 Parameters of HSO-HMP trust model

模型参数	取值
记忆库大小 HMS	100
微调空间大小	1 000
记忆库取值概率 $HMCR$	0.9
微调概率 PAR	0.5
微调带宽 BW	1

2 仿真实验和结果分析

利用MATLAB软件对HSO-HMP信任模型进行仿真实验及分析,通过与已有PSO-HMM、BW-HMM等相关模型的比较,主要验证了所提HSO-HMP信任模型的有效性、准确性和动态安全性。

2.1 仿真实验参数设置

在利用改进的HS算法求解隐Markov过程参数及对信任度的预测中,需对HS算法的相关参数进行设置,其中所用算法参数如表1所示。

2.2 仿真结果及其讨论

实验1 模型的有效性

主要讨论本模型的有效性,将HSO-HMP信任模型与文献[7]中的PSO-HMM信任模型、BW-HMM信任模型进行对比分析。

首先设状态集合大小 $M = 5, N = 2$,随机生成10个序列长度为100、带时间间隔的交互结果序列 $\vec{\boldsymbol{y}}^k = y_1^k y_2^k \cdots y_{100}^k, 1 \le k \le 10$,而在PSO-HMM信任模型和BW-HMM信任模型中均假设每条序列中相邻交互结果之间是等时间间隔的。利用第1.2节给出的算法即可得到每条序列所对应的目标函数值。图2给出了在HSO-HMP、PSO-HMM和BW-HMM 3种信任模型中,10条随机序列所对应的最大目标函数值。

在图2中,横坐标表示随机生成的10条交互结果序列,纵坐标表示不同算法所对应的对数似然函

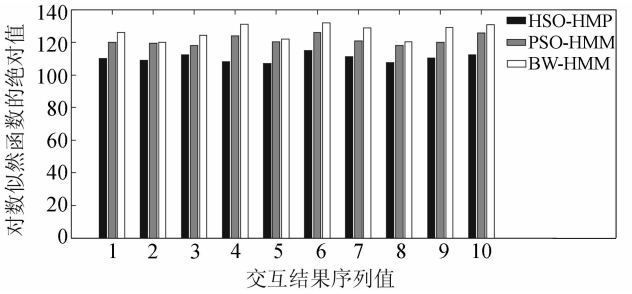

图 2　不同信任模型的似然函数值比较

Fig. 2　Comparison of likelihood functions of different trust models

数值的绝对值。从图 2 可以看出,与 PSO-HMM 信任模型和 BW-HMM 信任模型相比,HSO-HMP 信任模型具有更高的对数似然函数值,因此利用改进的 HS 算法能够更有效地求得每条随机序列所对应的最优模型参数,从而为进一步评估和预测实体的信任度奠定了良好的基础。

实验 2　模型的准确性

下面来验证该模型预测实体信任度的准确度。假设恶意实体所处状态分为 3 种:正常状态、中立状态和自私状态,其中,正常状态是指该实体能够提供高质量服务,中立状态是指实体只提供一般质量的服务,而实体在信誉提高之后就转化为自私状态,从而提供恶意服务。用 g、a 和 s 分别表示实体的正常状态、中立状态和自私状态,1、0 和 -1 分别表示高质量服务、一般质量服务和恶意服务,则状态集合为 $S=\{g,a,s\}$,交互结果取值集合 $Y=\{1,0,-1\}$,即 $M=3,N=3$,且

$$b(\rho\mid\sigma)=\begin{cases}1,(\sigma,\rho)=(g,1),(a,0),(s,-1);\\0,\text{else}。\end{cases}$$

因此观测矩阵为:

$$\boldsymbol{B}=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}。$$

恶意实体会在正常状态、中立状态和自私状态之间进行转换,然而评估者无法得知该恶意实体具体处在哪种状态,只能通过对收集到的交互结果序列进行分析,进而得到该实体的信任评价。

为了更有效地说明该模型的精确性,将 HSO-HMP 信任模型与文献[5]中的 HMM 信任模型进行对比分析。首先给定训练数据,即已知长度 $l=60$ 的交互结果序列 $\boldsymbol{y}=y_1y_2\cdots y_l$,其中,$y_i=1(1\leq i\leq 20)$,$y_i=0(21\leq i\leq 40)$,$y_i=-1(41\leq i\leq 60)$。由于观测矩阵 $\boldsymbol{B}$ 已知,则只需利用 HSO-HMP 信任模型得到模型参数 $\boldsymbol{\pi}$ 和 $\boldsymbol{Q}$。在此基础上,设实验数据 $\bar{y}=y_{l+1}y_{l+2}\cdots y_{2l}$,其中,$y_i=1(61\leq i\leq 80)$,$y_i=0(81\leq i\leq 100)$ 且 $y_i=-1(101\leq i\leq 120)$,并假设交互结果之间的时间间隔 $\Delta t_k\in(0,2)(1\leq k\leq 2l-1)$。通过实验分析,HSO-HMP 和 HMM 信任模型的准确性如图 3 所示。

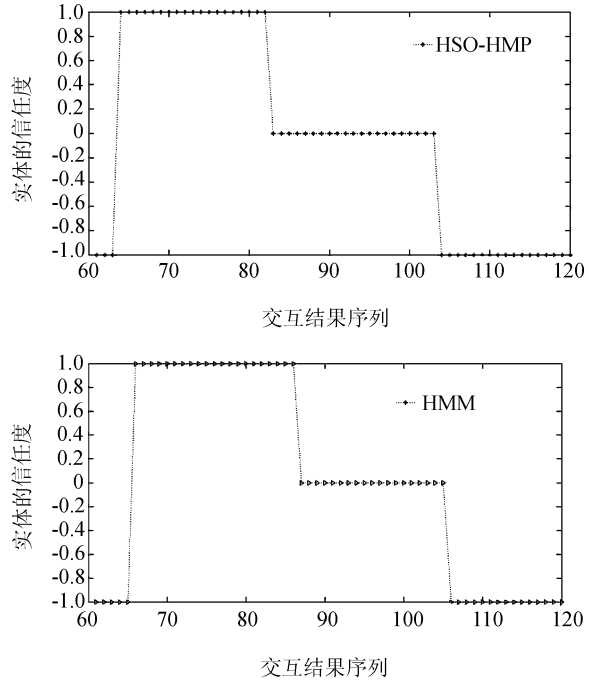

图 3　不同信任模型的准确性比较

Fig. 3　Aaccuracy of different trust models

在图 3 中,横坐标表示交互结果序列,纵坐标表示实体的信任度。从图 3 可以看出,HSO-HMP 信任模型经过大约 3 次就能够正确地监测到出恶意实体行为状态的变化,从而准确地判断该实体是否能够提供真实服务,进而及时地避免恶意服务。而 HMM 信任模型则需至少 5 次才能够反映出实体行为的变化,因此 HSO-HMP 信任模型更能够快速反映出实体行为的动态性,具有较高的准确度,并且能够抵抗该类策略实体的恶意攻击。

实验 3　HSO-HMP 信任模型的动态安全性

为了考察 HSO-HMP 信任模型的动态安全性,以更复杂的恶意实体为例来进行验证。假设恶意实体只有 2 种状态,即正常状态 g 和自私状态 s,且恶意实体在正常状态时以概率 $b(g)$ 提供高质量服务,概率 $1-b(g)$ 提供恶意服务,其中,$b(g)\in[0,1]$。而当实体由正常状态转化为自私状态之后,则只提供恶意服务。用1和0分别表示高质量服务和恶意服务,则 $b(1\mid g)=b(g)$,$b(0\mid g)=1-b(g)$,$b(1\mid s)=0$,$b(0\mid s)=1$,因此观测矩阵

$$\boldsymbol{B}=\begin{bmatrix}b(g)&1-b(g)\\0&1\end{bmatrix}。$$

下面分析 HSO-HMP 和 HMM 信任模型分别在 $b(g)=0.6,0.7,0.8,0.9$ 时的动态安全性。首先给定训练数据,即已知长度 $l=40$ 的交互结果序列 $\boldsymbol{y}=y_1y_2\cdots y_l$,其中,$y_i=1(1\leq i\leq 20)$,$y_i=0(21\leq i\leq 40)$,实验数据长度 $\tilde{y}=y_{41}y_{22}\cdots y_{140}$,其中,

$$y_i=\begin{cases}1, & i\in[41,60]\cup[81,100]\cup[121,140];\\ 0, & i\in[61,80]\cup[101,120]。\end{cases}$$

则 HSO-HMP 和 HMM 信任模型的动态安全性如图4所示。

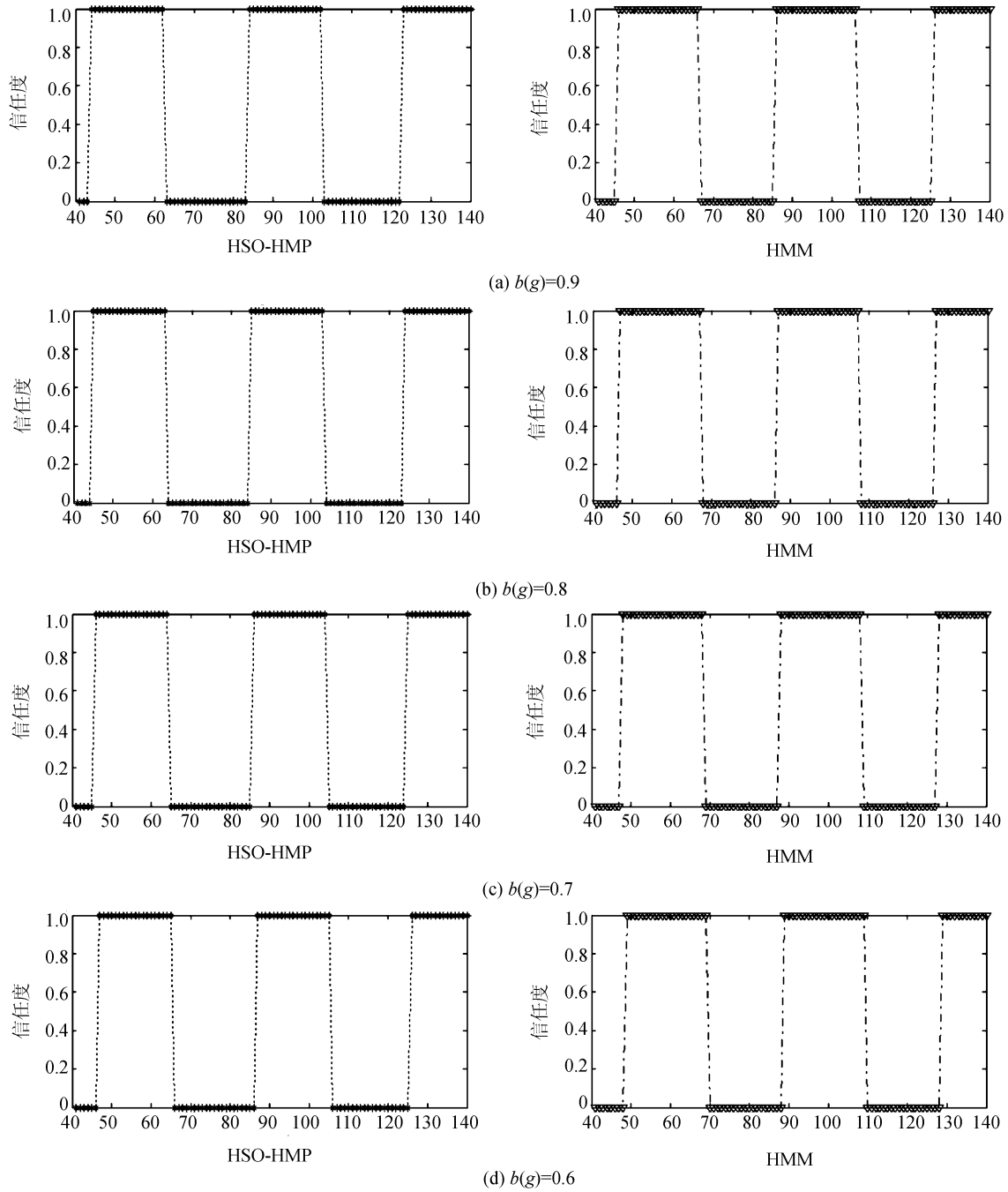

图4 不同信任模型的动态安全性

Fig. 4 Ddynamic of different trust models

在图4中,横坐标表示交互结果序列,纵坐标表示实体的信任度。从图4可以看出,随着 $b(g)$ 的逐渐减小,即恶意实体的动态不确定性逐渐加强,则 HSO-HMP 信任模型和 HMM 信任模型都能够检测出实体行为状态的变化。在 HSO-HMM 信任模型中,可控制在至多5次就可以检测到实体行为的变化,而 HMM 信任模型在相对稳定的实体,即 $b(g)=0.9$ 时就需要5次,并且随着 $b(g)$ 减小到0.6,即

实体行为表现出高动态性时,则需要将近 10 次交互才能反映出实体行为状态的变化,由此可知 HSO-HMP 信任模型能够更快速地反映出实体行为的高动态性变化,从而准确地预测该实体可能的交互结果,进而有效地避免恶意服务,提高安全性。

3　结　论

主要给出了一种基于连续时间隐 Markov 过程的网络信任模型。考虑到离散时间 HMM 模型不足以刻画信任随着时间变化的动态性,因此引入了连续时间隐 Markov 过程,通过结合交互结果之间的时间间隔,构建了网络信任评估模型。该模型将实体信任度计算问题转化为求解连续时间隐 Markov 过程的学习问题。为了得到隐 Markov 过程的最佳参数,通过定义微调空间,利用改进的和声搜索 HS 算法进行了求解,该算法有效地扩展了全局搜索空间和微调空间,能够获得更优的解,从而提高了模型的精确度。分析和仿真结果表明,该模型能够快速反映出实体行为的动态变化,具有较高的精确性,且能抵抗部分恶意攻击。下一步工作一方面是如何比较各反馈实体所提供的交互序列所对应的模型参数,剔除虚假反馈,能够抵抗共谋攻击等较为复杂的攻击方式;另一方面是将其应用于可重构网络的可信服务承载网的构建中,从而保障可重构网络的安全。

参考文献:

[1] Wang Jingpei, Sun Bin, Niu Xinxin, et al. Distributed trust model based on parameter modeling[J]. Journal on Communications, 2013, 34(4): 47 – 59. [汪京培, 孙斌, 钮心忻, 等. 基于参数建模的分布式信任模型[J]. 通信学报, 2013, 34(4): 47 – 59.]

[2] 桂小林, 李小勇. 信任管理与计算[M]. 西安: 西安交通大学出版社, 2011.

[3] Ayday E, Fekri F. Iterative trust and reputation management using belief propagation[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(3): 375 – 386.

[4] Elsalamouny E, Krukow K T, Sassone V. An analysis of the exponential decay principle in probabilistic trust models[J]. Theoretical Computer Science, 2009, 410: 4067 – 4084.

[5] Moe M E G, Helvik B E, Knapskog S J. Comparison of the beta and the hidden Markov models of trust in dynamic environments[C]//Trust Management III, IFTP Advances in Information and Communication Technology 300. Berlin: Springer, 2009: 283 – 297.

[6] Liu X, Datta A. Modeling context aware dynamic trust using hidden Markov model[C]//Proceedings of the 26th AAAI Conference on Artificial Intelligence. 2012: 1938 – 1944.

[7] Liu C, Yacine O, Antoine N, et. al. The reputation evaluation based on optimized hidden Markov model in E-commerce[J]. Mathematical Problems in Engineering, 2013, 2013: 1 – 11.

[8] Elsalamouny E, Sassone V. An HMM-based reputation model[J]. Advances in Security of Information and Communication Networks, 2013, 381: 111 – 121.

[9] Turin W. Continuous time HMM[M]//Performance analysis and modeling of digital transmission systems. New York: Springer, 2004.

[10] Geem Z W, Kim J H, Loganathan G V. A new heuristic optimization algorithm: Harmony Search[J]. Simulation, 2001, 76(2): 60 – 68.

[11] Geem Z W, Sim K B. Parameter-setting-free harmony search algorithm[J]. Applied Mathematics and Computation, 2010, 217: 3881 – 3889.

[12] Mun S, Cho Y H. Modified harmony search optimization for constrained design problems[J]. Expert Systems with Applications, 2012, 39: 419 – 423.

(编辑　杨　蓓)