基于NN的空天网络行为信任模型

徐晏琦， 宋留勇， 王劲松
(信息工程大学,郑州,450002)

摘要 空天网络所具有的动态性、开放性、复杂性特点,使得空天网络需要更高的安全性。为解决空天网络实体间的信任问题,并充分利用先验知识,基于神经网络理论对空天网络实体的行为信任进行了建模。通过建立相识社区,利用相识者的直接信任,完成了推荐信任的计算,并采用BP神经网络的惩罚项理论解决了恶意推荐问题。为空天网络环境中的行为信任研究提供了新的思路。

关键词 神经网络;空天网络;行为信任;惩罚项
DOI 10.3969/j.issn.1009-3516.2016.01.005
中图分类号 V37;TP301 **文献标志码** A **文章编号** 1009-3516(2016)01-0024-05

A Behavior Trust Model in Aerospace Network Based on Neural Network Theory

XU Yanqi, SONG Liuyong, WANG Jinsong
(Information Engineering University , Zhengzhou 450002,China)

Abstract:In view of the characteristics of dynamic, openness and complexity, this makes aerospace network high in security .To make full use of prior knowledge, the neural network theory should be used to build up a model of the trust. Through the establishment of acquaintance community, recommending trust value is obtained. Lastly, the problem of malice recommendation is solved by BP neural network with penalty. The model proposed in this paper provides a new way for studying behavior trust in Aerospace Network.

Key words:neural network;aerospace network;behavior trust ;penalty

空天网络是指利用网络技术把外层空间、临近空间、航空空间中具有侦察、预警、监视、导航、中继、气象观测等功能的载荷设备如卫星、飞艇、预警机、无人机等连接而成的空天一体的信息网络。

如果把空天网络中的载荷设备看作一个个不同的实体用户,那么与现有网络相比,空天网络具有动态性、开放性、复杂性特点。此外空天网络还具有通信时延,工作环境多样等特征,这些特点和特征决定了空天网络实体用户之间的安全性要求更高,用户关系越来越复杂,并呈现出人类社会的特征:陌生用户之间的关系不能在交互前确定、不能在交互前互相充分了解。

利用信任理论解决复杂用户关系的安全问题始终是研究焦点。信任一般包括2种:一种是基于证据的信任,另一种是基于行为的信任,行为信任所强调的实体关系与空天网络用户间的关系非常相似,

收稿日期:2015-02-04
基金项目:国家自然科学基金(61309018)
作者简介:徐晏琦(1975—),男,河南滑县人,讲师,主要从事信息安全研究. E-mail:xyq_1@163.com

引用格式:徐晏琦,宋留勇,王劲松. 基于NN的空天网络行为信任模型[J]. 空军工程大学学报:自然科学版,2016,17(1):24-28. XU Yanqi, SONG Liuyong, WANG Jinsong.A Behavior Trust Model in Aerospace Network Based on Neural Network Theory[J]. Journal of Air Force Engineering University:Natural Science Edition,2016,17(1):24-28.

因此可用来解决空天网络用户间的关系问题。

有多位学者对行为信任进行了研究，如 Yu[1]等人利用证据理论将多个 Agent 的证据合并成一个 Agent 对其他 Agent 的评价；Song[2]基于模糊理论将权重由变量的模糊值确定，力图解决信息的不确定性；唐文[3]将信任的度量机制用模糊理论表示，从而完成对信任的建模工作，并引入形式化的方式对信任进行推理；Abdul-Rahmam[4]利用加权平均的方法形成信任评价；Sang[5]等人引入 evidence 空间和 opinion 空间来描述信任关系并提出主观逻辑算子完成信任度推导和综合运算；陈建刚[6]提出在网格中用贝叶斯网络对节点属性进行运算；桂劲松[7]基于证据理论对网格服务行为信任进行建模，解决了信任的度量、传递、组合问题；欧嵬[8]将用户对系统的服务请求映射为主体对客体的访问，通过定义模型的安全属性、安全策略约束用户行为；刘宴兵[9]采用事件触发检测与周期性检测相结合的方式计算综合信任值，并判断节点行为是否异常等等。

专门针对空天网络的信任研究有曹炳华[10]用自证明公钥理论完成了空天网络的身份认证。目前，空天网络行为信任的研究还处于空白之中。

1　信任

信任本是现实社会中人类的活动现象，不同的研究者根据自己的研究内容给出的信任定义都不尽相同。信息安全研究中的信任是以现实社会中的信任概念为基础建立的。本文针对空天网络实体间关系给出如下信任定义：

定义 1　信任是对实体未来行为的可靠性、正确性、真实性的期望。

这个定义基本反映了呈现出社会化特点的空天网络实体对相互关系的认知。这里需要说明的是本文的信任特指行为信任。

2　信任评估

既然信任是对实体未来行为的期望，那如何评估信任就成了首要的任务。

实体间与信任相关的因素会不断发生变化，如果不利用先前形成的经验，则每一次对信任的评估都需要重新建立模型，这会存在许多重复的工作。所以，需要一种新的研究模型，能够自己进行“学习”，并将经验性的知识进行积累和利用，从而获得较为精确的信任值。

McCulloch 和 pitts 首次证明了人工神经网络可以逼近任何算术和逻辑函数，并且具有自学习、自适应和容错性强的特点，能够将经验性的知识积累并利用。本文将神经网络理论引入到行为信任研究中探讨空天网络行为信任。

2.1　信任网络

定义 2　对考察的空天网络实体某项行为 h 而言，令 $\{x_1,x_2,\cdots,x_n\}$ 表示 h 的评价属性向量，$\omega_i(i=1,2,\cdots,n)$ 为每一个评价属性在考察 h 时所具有的影响，则称以 $\{x_1,x_2,\cdots,x_n\}$ 为输入，以 $\omega_i(i=1,2,\cdots,n)$ 为输入权值，以 y 为输出的图 1 结构为信任元。其中 $\sum$ 是求和符号，α 是经过求和后的输出，f 是信任元的输出函数或者称为转移函数，θ 是信任元的阀值。

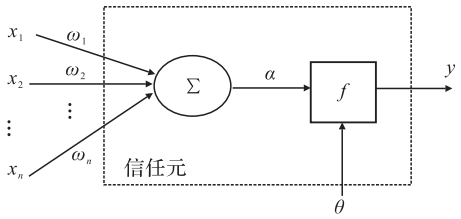

图 1　信任元

Fig.1　Trust element

信任元的输出为：$y=f(\boldsymbol{W}\boldsymbol{X}+\theta)=f(\sum_{i=1}^{n}\omega_i x_i+\theta)$ 其中 $\boldsymbol{W}=(\omega_1,\omega_2,\cdots,\omega_n)$，$\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$。输出 y 表示对实体行为 h 的信任程度称为信任度。

信任元的输入 X，表示对行为 h 属性的测算值。而行为的每一个属性对于实体信任值的影响都是不一样的，这种影响通过 W 来表现。如在空天网络应用中，直播卫星系统需要的数据量是很大的，这时对于数据传输行为而言，文件的完整性、传输的延迟时间和副本替换的安全性等属性对传输行为的影响要更大；而对于预警系统，同样是数据传输行为，排队时长、CPU 的利用率和通信带宽利用率等属性则更重要。

行为信任的复杂性决定了仅凭一个信任元计算的结果必然产生很大的误差，因此往往需要多个信任元并行形成一个层来工作，如果为了得到更精确的结果还需要形成由多层信任元组成的信任网络。但是层次也不是越多越好，已经证明三层网络可以完成任意精度的逼近[11]。

定义 3　多个信任元的并行排列结构称为一个信任层，由多个信任层组成的如图 2 所示结构称为信任网络。

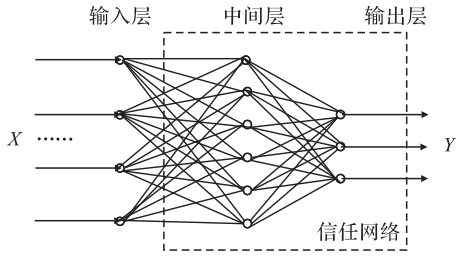

图 2 信任网络

Fig.2 Trust network

对于输入 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$ 而言,每一个都要与信任元相连。此时输出 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_m)$,对于每一个输出分量 y_j,仍可以表示为 $y_j=f(\boldsymbol{W}\cdot\boldsymbol{X}+\theta)$

2.2 归一化

行为 h 每一个属性值得到的方法、手段是多样化的,所以各属性具有不同的量纲且类型不同,也就是说属性间具有不可公度性。这种不可公度性就使得评估的结果误差较大,因此需要对各属性变量进行规范化处理——利用归一化的方法将属性变换到无量纲区间,使属性具有可比性。属性一般可分为:

1)开销型属性。这类属性是对资源、成本的一种消耗,对这类属性的评定值一般是越小越好。如 CPU 时间的消耗等,因此对于此类属性可选取归一化函数如下:$F=(\max_j-x_i)/(\max_j-\min_j)$,其中 $\max_j$ 为该类属性的最大值、$\min_j$ 为该类属性的最小值;

2)贪婪型属性。这类属性值越大越好,如数据带宽、下载速度,对于这类属性可选取如下归一函数:$F=(x_i-\min_j)/(\max_j-\min_j)$,其中 $\max_j$ 为该类属性的最大值、$\min_j$ 为该类属性的最小值;

3)稳定型属性。此类属性以稳定在某一个值为最好,如空天网络中大型设备的电压。这类属性的归一函数为:$F=\mathrm{mid}_j/(|x_i-\mathrm{mid}_j|+\mathrm{mid}_j)$,其中 mid_j 为该类属性的稳定值或最合适的值。

2.3 信任的评估

对属性进行归一化处理后,可以通过信任网络完成对空天网络实体的信任评估。这种计算是对空天网络实体行为的分析、计算,涉及的因素主要有:

2.3.1 评估结果

评估结果即对被评价实体所进行的信任评判,即信任网络的输出。由于评价结果可以有多种类型如离散型,连续型,二值型,所以评估结果既可以是用连续值表示,也可以转换为离散值表示。用离散值表示时往往选择{完全信任,很信任,一般信任,有点信任,不信任}。

2.3.2 权重

权重体现了各个属性对评价结果的影响程度,即信任网络中的 ω_j。权重初始值是由主体根据经验和自身要求给出,但是在信任网络中经过训练后会收敛在一个特定值附近。

2.3.3 学习规则

学习规则是修改信任网络权重的方法和过程,即如何训练信任网络完成对信任的评估。学习规则直接决定了信任评估的具体过程。学习规则有多种,本文选取 BP 算法作为信任网络的学习规则。

2.3.4 评估过程

评估信任的过程可分为 2 个阶段,第 1 个阶段是训练信任网络,训练的目的是使权重收敛在一个特定值;第 2 阶段是评估,即将属性值 X 输入训练完毕的信任网络中,产生评估结果。整个过程如下:

1)权值初始化;

2)确定样本指标;

3)归一化处理;

4)依次计算隐层,输出层各神经元的输出;

5)计算误差;

6)满足需求开始评估,否则修正各层的权值和偏置值返回到 4)。

定义 4 直接信任,称由信任网络得出的信任度为直接信任度,简称直接信任,用 $d(p)$ 表示,其中 p 为被评估信任的实体。

3 推荐信任

3.1 推荐信任值的计算

2 个空天网络实体进行了一次或若干次交互后会产生一个较稳定的直接信任。但是,当 2 个没有任何联系的实体需要交互的话怎么办呢?一般而言有 2 种方法:一种方法是先给陌生的实体一个初始值,大家慢慢试探;另一种就是通过其他实体推荐后,进行一次交易,交易完后可以获得对方的直接信任,这样,下次再交互就可以根据直接信任进行判断。显然这和人类社会比较类似,2 个陌生人交往时一种就是找与之熟悉的人进行询问,一种就是抱着试试看的态度与之交往,两者比较可能通过熟悉的人推荐所获得的安全性更好。

定义 5 陌生者,实体 a 与实体 b 没有任何交往,则称实体 a 与实体 b 互为陌生者。

定义 6 相识者,实体 a 与实体 b 至少有一次交往,则称实体 a 与实体 b 互为相识者。

定义 7 推荐信任,实体 a 与实体 b 互为陌生者,称实体 a 获得的其他实体 c 关于实体 b 的信任度为推荐信任度简称推荐信任,用 $r(c,b)$ 表示。

在人类社会中,每个人都有自己的交往范围,或

者称为生活圈。在多数情况下，人更多接触的是这个圈子中的人，在对某人进行评价时，他们的意见是比较重要的。与此类似，每个空天网络实体都属于一个区域。

定义 8　相识社区，空天网络实体 b 的全部相识者组成的集合 $A=\{a_1,a_2,\cdots,a_n\}$ 称为相识社区，b 称为相识社区的中心，用 $b\rightarrow A$ 表示。

设实体 q 向实体 p 请求服务，q 与 p 是陌生者，$p\rightarrow P$，p 要获得关于 q 的推荐信任。可以看出如果仅将 P 中实体的推荐值输入信任网络，参与的实体太少，缺少一般性，如果采取向空天网络中全部实体都发送推荐请求，则信任网络的输入规模又过于庞大，计算复杂，时间耗费长，协调也困难。本文采用了如下方法解决这一矛盾，p 获得关于 q 的信任值的过程如下：p 向相识社区 P 中的全体实体 $p_n(n=1,2,\cdots,m)$ 发出推荐请求，然后 p 的相识社区中的每一个实体 $p_n(n=1,2,\cdots,m)$ 形成一个以自己为中心的相识社区的推荐值作为 $p_n(n=1,2,\cdots,m)$ 的推荐值 $r(p_n,q)$，该推荐值作为 p 的信任网络的输入。设 $d_n(n=1,2,\cdots,m)$ 为 p 对 $p_n(n=1,2,\cdots,m)$ 中每个相识者的直接信任，将 $d(p_n)$ 作为 p 的信任网络的权值，这里称 $d(p_n)$ 为口碑。最后经过 p 的信任网络的运算得出 $r(p,q)$。计算过程见图 3。

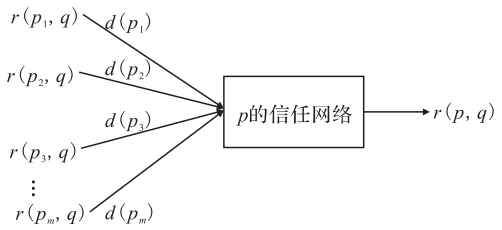

图 3　推荐信任计算过程

Fig.3　The computational process of recommendation trust

3.2　恶意推荐的处理

虽然利用推荐是与陌生空天网络实体交往的一种有效途径，但是这种方法存在着安全风险，即恶意推荐。

定义 9　设空天网络实体 g_1、g_2，推荐信任值为 $r(g_1,g_2)$，设存在一个正实数 ε，及直接信任 $d(g_2)$。若 $|r(g_1,g_2)-d(g_2)|>\varepsilon$，则称实体 g_1 对实体 g_2 的推荐为恶意推荐，推荐信任值 $r(g_1,g_2)$ 为恶意推荐值。

恶意推荐的存在引起了空天网络中许多安全问题及效率问题的发生，如终端 g_1 需要从空天网络中某导航卫星下载数据，如果在恶意推荐的引导下从被敌方俘获控制的卫星下载，要么增加下载时间，要么会下载错误信息，这都会损害终端安全。由此可见，对于行为信任研究而言，如何消除恶意推荐的影响是保证信任模型鲁棒性的重要环节。

下面以神经网络的惩罚项理论为基础提出一种新的消除恶意推荐的方法。

在图 3 的信任网络中假设存在 s 个恶意实体，如何消除它们的推荐影响呢？最直接的方法就是让恶意推荐不能进入信任网络。如果恶意实体的推荐所对应的权值为 0 的话，则该恶意实体的推荐就没有可能进入信任网络，也就失去了对最终推荐信任值的影响力。现在问题的关键就转换为如何使权值为 0。惩罚项理论就是一种通过训练使权值收敛为 0 的方法。

具体原理如下：

在传统的误差函数中加入一个衡量信任网络输入恶意程度的“惩罚项”，该项在计算信任度的过程中起到使恶意实体的推荐输入所对应的权值减小到 0 的作用，从而达到将恶意实体的推荐输入排除出信任网络的目的。

设图 3 的信任网络中采用的误差函数为 E。

为了消除恶意推荐，将误差函数 E 定义为 $E=\tilde{E}+\dfrac{\omega_i^2/((I-y)^2+\varepsilon)}{1+\omega_i^2/((I-y)^2+\varepsilon)}$。$\tilde{E}$ 是 BP 神经网络的原误差函数；$\boldsymbol{\omega}$ 是权值向量；I 是第 i 个输入；y 是最终的输出；ε 是一个足够小的正数。

图 4 直观地说明了这种方法可以使恶意推荐的权值收敛为 0。对于误差函数 E 的第 2 项而言，如果 $((I-y)^2+\varepsilon)>>|\omega_i|$，即第 i 个输入与最终输出的误差很大，可以判定第 i 个输入为恶意推荐，此时误差函数 E 的第 2 项接近为 0，也就表明对于推荐信任来说第 i 个权值是不可信的，应该从信任网络中删除，反之，当 $((I-y)^2+\varepsilon)<<|\omega_i|$ 时，即误差较小，此时误差函数 E 的第 2 项接近为 1，也就表明对于推荐信任来说第 i 个权值是重要的、可信赖的，应该保留。可见惩罚项起到了将恶意推荐剔除出信任网络的作用。

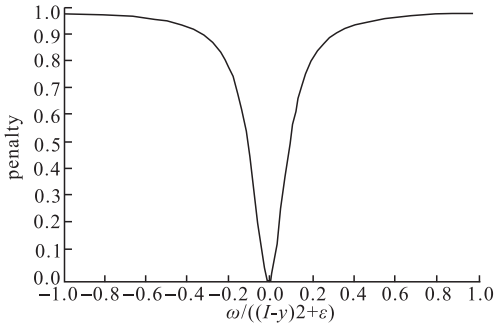

图 4　惩罚项

Fig.4　Penalty

文献[12]已经证明误差函数 E 收敛：

$$\lim_{k\to\infty} \| E_W(W^k) \| = 0$$

4 结语

本文的信任模型对空天网络行为信任的自学习、容错性进行了研究,充分利用先验知识,改变了已有信任模型当相关因素变化时需要重新修改或建立模型的状况。本文还在惩罚项理论的基础上提出了一种新的解决恶意推荐的方法。此外,利用分割的相识社区降低了推荐信任的计算规模。本文的信任模型可以作为一种智能、有效的分析工具,用于空天网络行为信任的计算中并对其它开放网络环境的相关信任研究提供借鉴。

参考文献(References):

[1] Bin Yu, Munindar P Singh. An Evidential Model of Distributed Reputation Management [C]//Proceedings of the 1st International Joint Conference on Autonomous Agents and MultiAgent Systems (AAMAS). Italy, 2002: 82-93.

[2] S Song, K Hwang, R Zhou. Trusted P2P Transactions with Fuzzy Reputation Aggregation[J]. Internet computing, 2005, 9(6): 24-34.

[3] 唐文.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. Research of Subjective Trust Management Model Based on the Fuzzy Set Theory[J]. Journal of Software, 2003, 14(8): 1401-1408.(in Chinese)

[4] Abdul-Rahman, S Hailes. UsingRecommendations for Managing Trust in Distributed System[C]//Proceedings of the IEEE Malaysian International Conference on Communication, 1997.

[5] Sang A. A Logic for Uncertain Probabilities. International Journal of Uncertainty [J]. Fuzziness and Knowledge-based Systems, 2001, 9(3): 279-311.

[6] 陈建刚,王汝传,王海燕.网格资源访问的一种主观信任机制[J].电子学报,2006,34(5):818-821.
CHEN Jian'gang, WANG Ruchuan, WANG Haiyan. A Subjective Trust Mechanism of Resource Access in Grid[J]. Acta lectronica Sinica, 2006, 34(5): 818-821.(in Chinese)

[7] 桂劲松,陈志刚,邓晓衡,等.基于 D-S 证据理论的网格服务行为信任模型[J].计算机工程与应用,2007,43(2):25-27.
GUI Jinsong, CHEN Zhigang, DENG Xiaoheng, et al. Bebavior Trust Model for Grid Services Based on D-S Evidence Theory[J]. Computer Engineering and Applications, 2007, 43(2): 25-27.(in Chinese)

[8] 欧鬼,王勇军,韩文报. 基于用户行为的可信模型研究[J].计算机工程与科学,2013,35(5):46-50.
OU Wei, WANG Yongjun, HAN Wenbao. Research on Trustworthy Model Based on User's Behavior[J]. Computer Engineering & Science, 2013, 35(5): 46-50.(in Chinese)

[9] 刘宴兵,龚雪红,冯艳芬.基于物联网节点行为检测的信任评估方法[J].通信学报,2014,35(5):8-15.
LIU Yanbing, GONG Xuehong, FENG Yanfen. Trust System Based on Node Behavior Detection in Internet of Things[J]. Journal on Communactions, 2014, 35(5): 8-15.(in Chinese)

[10] 曹炳华,孟凡涛.一种适用于空天网络的身份认证框架[J].现代军事通信,2011,19(1):50-53.
CAO Binghua, MENG Fantao. Authentication Framework for Space Network[J]. Journal of Modern Military Communications, 2011, 19(1): 50-53.(in Chinese)

[11] Robert Hecht Nielsen. Theory of Back Propagation Neural Network[C]// Proceedings of IJCNN, 1989: 593-604.

[12] 邵红梅.带惩罚项的 BP 神经网络训练算法的收敛性[D].大连:大连理工大学,2006.
SHAO Hongmei. Convergence of BP Algorithms with Penalty for FNN Training[D]. Dalian: Dalian University of Technology, 2006.(in Chinese)

(编辑:姚树峰)