第 36 卷 第 2 期 计 算 机 工 程 2010 年 1 月
Vol.36 No.2 Computer Engineering January 2010
·安全技术· 文章编号：1000—3428(2010)02—0161—03 文献标识码：A 中图分类号：TP393

异构无线网络中基于实体可信度的信任模型

张 鹏，黄开枝，贺晓珺
(解放军信息工程大学国家数字交换系统工程技术研究中心，郑州 450002)

摘 要：针对异构无线网络的不确定性和动态性，提出一种基于实体可信度的动态信任模型。利用待测实体可信度和推荐主体可信度抑制恶意实体的破坏行为，采用信任时间戳标志信任信息的时间特性，突出近期信任信息的重要性。仿真结果表明，该模型能准确、有效地确定网络实体的信任度，较好抑制诋毁行为和协同欺骗行为。

关键词：异构无线网络；信任度；实体可信度

Trust Model Based on Entity Credibility in Heterogeneous Wireless Network

ZHANG Peng, HUANG Kai-zhi, HE Xiao-jun
(National Digital Switching System Engineering & Technological R&D Center, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】 Aiming at the characteristics of uncertainty and variability in heterogeneous wireless network, this paper proposes a dynamic trust model based on entity credibility. By introducing credibility of the candidate network and credibility of the evaluating entity, malicious behaviors of the dishonest entities are restrained effectively. Time stamp makes the evaluation pay much attention to the most recent performance records. Simulation result shows that the model can accurately evaluate the trustworthiness of the network and effectively restrain the acts of slander and co-fraud.

【Key words】 heterogeneous wireless network; trust worthiness; entity credibility

1 概述

无线网络的异构性和动态性对安全提出了新的要求，基于静态的传统认证和访问控制机制已经不能充分满足众多网络应用的安全需求。在实际中，恶意网络实体会伪装加入异构无线网络，损害用户利益。不诚实的网络实体可能对许诺的服务质量不能够可信地执行，从而影响用户的工作效率。因此，如何在异构环境下对网络实体的行为进行评判，有效控制移动用户对网络实体的访问和使用，已成为一个亟待解决的重要问题。

一种可行的解决方案是引入信任评判机制标志网络实体的善恶，用户选择网络时以信任度为依据，网络实体的信任度越高，认为其越安全，用户选择接入的几率便越大；反之，信任度越低，用户选择接入的几率越小。目前，对信任的研究主要包括 2 个方面的内容：(1)客观信任关系(如 PKI 中的证书)，这种关系基于证据，可以精确地描述、推理和验证；(2)实体之间的主观信任关系，这种关系是对实体的特定特征或行为的特定级别的主观判断，具有很大的主观性和不确定性，无法精确地加以描述和验证。

本文主要研究实体之间的主观信任关系。目前，典型的主观信任评估模型有 Beth 模型[1]和 Jøsang 模型[2]等，它们都试图用精确的概率模型解决信任模型中遇到的各种问题，忽略了信任的不确定性。针对该问题，文献[3]提出基于模糊集合理论的主观信任管理模型，认为主观信任作为一种认知现象，其主观性和不确定性主要表现为模糊性，为信任模型的研究提供了有价值的思路，但其概念比较抽象，缺少具体化的深入描述。因此，文献[4]引入隶属云理论对信任进行建模，给出信任评价云和信任等级云的定量描述，提出信任的计算、合成和综合更新等方法，并且对主体的信任等级做出评估。其不足是：该模型的前提假设不存在恶意评价行为，即认为主体的评价反馈都是诚实的。

综合考虑上述模型的优点和不足，本文提出一个基于实体可信度的动态信任模型(Dynamic Trust Model Based on Entity Credibility, DTMBEC)。仿真实验表明，该模型从安全角度出发，对异构无线网络接入选择进行了有益的探索和尝试。

2 异构无线网络中的信任机制

异构无线网络由多种采用不同接入技术的网络融合而成，为移动用户提供了随时随地的网络连接，并可最大限度地满足用户业务需求。但开放式的网络架构带来了新的安全隐患，为异构无线网络的安全增加了许多不确定性，如，恶意网络会伪装加入异构无线网络进行破坏活动，不诚信的网络也可能不执行许诺的服务质量。同时，开放式的互联系统使得异构无线网络具有动态性，网络实体或移动节点可以随时加入或离开异构无线网络。

异构无线网络如图 1 所示，异构无线网络的基本网络实体包括：AAA(Authentication Authorization and Accounting)服务器，可信第三方(Trust Third Party, TTP)和移动终端(Mobile

基金项目：国家“863”计划基金资助项目(2007AA01Z434)
作者简介：张 鹏(1982－)，男，硕士，主研方向：移动通信；黄开枝，副教授、博士；贺晓珺，硕士
收稿日期：2009-06-09 **E-mail：**zhangpengyining@163.com

Host, MH)。AAA 服务器主要用于对用户进行身份认证、授权和计费等；TTP 是网络内唯一可完全信任的实体，负责搜集、评估本域内网络实体的信任度，并为域内的网络实体颁发唯一的身份标志证书。其中，UMTS(Universal Mobile Telecommunications System)表示通用移动通信系统。

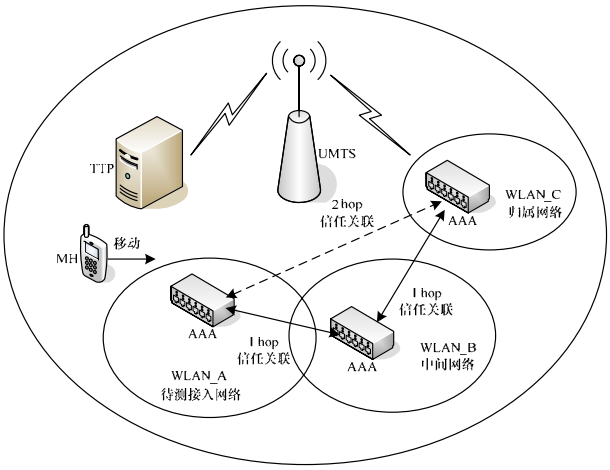

图 1　异构无线网络

对于任意一个网络 N，信任机制根据 N 执行过的服务情况，利用 DTMBEC 模型计算该网络的信任度。用户进行网络选择时以信任度为依据，信任度越高的网络具有的安全性越强，用户选择接入的概率越大。

3　DTMBEC 模型

针对异构无线网络的不确定性和动态性特点，提出 DTMBEC 模型。信任度的计算引入了直接信任度、推荐信任度、待测实体可信度、推荐主体可信度和信任时间戳 5 个参量，其中，直接信任度来源于终端与待测实体间的直接历史交互信息；推荐信任度来源于推荐主体的直接信任度。

在异构无线网络中，恶意网络可以通过策略性地改变行为方式对用户进行攻击，如恶意网络首先通过良好的服务建立较高的信任值，然后突然改变行为进行攻击，因此，直接信任度也存在一定的风险。在 DTMBEC 模型中，引入待测实体可信度对直接信任度进行赋权，可以较好地反映待测实体的近期行为，降低恶意网络策略性攻击带来的风险。恶意终端可能通过提交不诚实的评价降低善意网络或夸大恶意网络的信任度，即诋毁行为或协同欺骗行为。为抑制恶意终端的破坏行为，DTMBEC 模型定义了推荐主体可信度的概念，有效抑制了终端的恶意行为。最后，针对异构无线网络动态性的特点，DTMBEC 模型使用时间戳来标志信任的时间特性，重点突出了近期信任信息的重要性，并在设置有效时长 T 的基础上，引入先进先出(First In First Out, FIFO)策略淘汰过时的信任信息。

3.1　信任度的度量

设 $U=\{x\}$ 为研究论域，x 为待测实体集，T 为信任等级组成的模糊子集集合，包括不信任子集 T_1、一般信任子集 T_2、非常信任子集 T_3 和完全信任子集 T_4。对于 $\forall x\in U$，如果给定一个映射 $\mu_T: U\to[0,1], x\mapsto\mu_T(x)\in[0,1]$，则 $\mu_T(x)$ 为 x 对 T 的信任隶属度[5]。待测实体对各信任等级模糊子集的隶属度构成信任隶属向量，即 $\boldsymbol{R}=[\mu_{T_1}(x)\ \ \mu_{T_2}(x)\ \ \mu_{T_3}(x)\ \ \mu_{T_4}(x)]$。

在 DTMBEC 模型中，分别采用直接信任隶属向量和推荐信任隶属向量表示直接信任度和推荐信任度，而待测实体信任隶属向量根据直接信任隶属向量和推荐信任隶属向量由算法综合得到。最后，对待测实体信任隶属向量进行解模糊化，得到待测网络实体的信任度。

3.2　待测实体可信度

用户在进行网络选择时，接入网络与归属网络之间应存在一定信任关联，以实现接入网络 AAA 服务器对用户的身份认证。对于用户而言，归属网络是完全诚实可信的，因此，待测网络实体与用户归属网络之间的信任相关程度可用来表示待测实体的可信度，并由 2 个网络之间的信任关联跳数(Trust Association Hop, TAH)得到。如图 1 所示，假设待测网络实体和归属网络分别与中间网络存在信任相关路径为 1 的直接信任关系，则待测实体与用户归属网络之间存在 TAH 为 2 的间接信任关系。

设 $\mathfrak{R}$ 表示待测实体可信度，H_n 表示待测网络实体与用户归属网络之间的 TAH，随着 H_n 的增加 $\mathfrak{R}$ 将逐渐降低，即近距离的网络比远距离的网络有更强的可信度。由于中间网络的增加使得可靠性和不确定性大大增加，因此随着 H_n 的增加，$\mathfrak{R}$ 降低速度越来越快，式(1)形象地表述此关系：

$$\mathfrak{R}=\psi\times[\frac{\pi}{2}-\arctan(H_n-H_{\max})] \tag{1}$$

其中，ψ 为常数，ψ 的取值应使 $0<\mathfrak{R}\le 1$；$H_{\max}$ 是允许的最大路径长度，当 $H_n>H_{\max}$ 时，认为待测网络实体与归属网络之间不存在信任关联，用户不考虑接入此网络，当 $H_n<H_{\max}$ 时，使用待测实体可信度 $\mathfrak{R}$ 对用户直接信任度进行赋权，可以有效减少恶意网络策略性攻击行为造成的影响。

3.3　推荐主体可信度

假设 2 个向量 $\boldsymbol{A}=(a_1,a_2,\cdots,a_n)$ 和 $\boldsymbol{B}=(b_1,b_2,\cdots,b_n)$，分别进行归一化运算，$\boldsymbol{A}'=(a_1',a_2',\cdots,a_n')=(a_1\Big/\sum_{i=1}^{n}a_i, a_2\Big/\sum_{i=1}^{n}a_i,\cdots, a_n\Big/\sum_{i=1}^{n}a_i)$，$\boldsymbol{B}'=(b_1',b_2',\cdots,b_n')=(b_1\Big/\sum_{i=1}^{n}b_i, b_2\Big/\sum_{i=1}^{n}b_i,\cdots,b_n\Big/\sum_{i=1}^{n}b_i)$，则 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 的最大最小贴近度函数[5] $N_M(\boldsymbol{A},\boldsymbol{B})$ 为

$$N_M(\boldsymbol{A},\boldsymbol{B})=\frac{\sum_{i=1}^{n}(a_i'\wedge b_i')}{\sum_{i=1}^{n}(a_i'\vee b_i')} \tag{2}$$

其中，$\wedge$ 和 $\vee$ 为扎德 max 算子和扎德 min 算子；$0\le N_M(\boldsymbol{A},\boldsymbol{B})\le 1$，$N_M(\boldsymbol{A},\boldsymbol{B})$ 越大，说明 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 2 个向量越接近。

在异构无线网络中，假设用户 C 根据用户 D 的推荐信任隶属向量 $\boldsymbol{rt}_{D(t)}^{E\leftarrow C}$ 接入网络 E，用户 C 接受网络 E 的服务后向 TTP 反馈网络直接信任隶属向量为 $\boldsymbol{dt}_{C(t)}^{E\leftarrow C}$，由式(2)可得两者的贴近度 $N(\boldsymbol{rt}_{D(t)}^{E\leftarrow C},\boldsymbol{dt}_{C(t)}^{E\leftarrow C})$。若 $0\le N(\boldsymbol{rt}_{D(t)}^{E\leftarrow C},\boldsymbol{dt}_{C(t)}^{E\leftarrow C})<0.5$，认为该次推荐失败；若 $0.5\le N(\boldsymbol{rt}_{D(t)}^{E\leftarrow C},\boldsymbol{dt}_{C(t)}^{E\leftarrow C})\le 1$，认为该次推荐成功。

在 DTMBEC 模型中，设 $P_D=\dfrac{S_D}{S_D+I_D}$ 代表推荐主体 D 的可信度，其中，S_D 和 I_D 分别表示累计推荐成功次数和累计推荐失败次数；P_D 取值越大说明推荐主体越可信，其诚实评价的可能性越大。与此同时，TTP 将以 P_D 的概率接收推荐主体 D 的推荐，这在一定程度上抑制了恶意终端的诋毁行为和协同欺骗行为。

3.4　信任时间戳

在异构无线网络中，一定比例的网络实体或移动节点离

开域后将不再重新接入，保持这些实体之前长时间的历史信任信息将严重浪费 TTP 存储资源。因此，在 DTMBEC 模型中仅考虑距离当前时刻有效时间 T 内的信任信息。同时，针对信任的遗忘性特点，引入信任时间戳使得距离当前时间越近的交互记录越有参考性。设 t 时刻交互记录的时效值 $\Delta T_t = T_{now} - t + 1$，其中，$T_{now}$ 为当前日期时间；设置 τ_t 为时间戳，不失一般性，可设 $\tau_t = 1/\Delta T_t$。t 时刻信任隶属向量为

$$\boldsymbol{R}^{'} = \tau_t \times [\mu_{T_1}(x)\ \ \mu_{T_2}(x)\ \ \mu_{T_3}(x)\ \ \mu_{T_4}(x)] \tag{3}$$

同时规定，在有效时间 T 内单个终端对一个网络实体的最多评价次数为 N。在 DTMBEC 模型中以有限长度的表格保存网络实体的信任信息，运用 FIFO 策略淘汰陈旧的信任资源。

这样，根据有效时间 T 内有限次的信任反馈计算信任度，可以在有效计算的前提下节省 TTP 的维护开销。

3.5 信任联合算法

基于上述分析，提出适用于 DTMBEC 模型的信任联合算法(Trust Combining Algorithm, TCA)，设 $\boldsymbol{O}_{i(t)}^{j\leftarrow i}$ 表示 t 时刻终端 i 对待测实体 j 的信任隶属向量：$\boldsymbol{DT}_{i(t)}^{j\leftarrow i} = [\boldsymbol{dt}_{i(t_1)}^{j\leftarrow i}\ \boldsymbol{dt}_{i(t_2)}^{j\leftarrow i}\cdots\boldsymbol{dt}_{i(t_m)}^{j\leftarrow i}]^{\mathrm{T}}$ 表示终端 i 对待测实体 j 的直接信任向量，$\boldsymbol{RT}_{h(t)}^{j\leftarrow i} = [\boldsymbol{rt}_{h(t_1)}^{j\leftarrow i}\ \boldsymbol{rt}_{h(t_2)}^{j\leftarrow i}\cdots\boldsymbol{rt}_{h(t_k)}^{j\leftarrow i}]^{\mathrm{T}}$ 表示终端 h 对待测实体 j 的推荐信任向量，则

$$\boldsymbol{O}_{i(t)}^{j\leftarrow i} = \alpha \times \mathfrak{R}_{(t)} \times \frac{\sum_{p=1}^{m} \boldsymbol{dt}_{i(t_p)}^{j\leftarrow i}}{m} + \beta \times \frac{\sum_{h=1}^{n} P_{h(t)} \times \frac{\sum_{q=1}^{k} \boldsymbol{rt}_{h(t_q)}^{j\leftarrow i}}{k}}{n} \tag{4}$$

其中，$\boldsymbol{dt}_{i(t)}^{j\leftarrow i}$ 和 $\boldsymbol{rt}_{h(t)}^{j\leftarrow i}$ 分别表示 t 时刻终端 i 对待测实体 j 的直接信任隶属向量和终端 h 对待测实体 j 的推荐信任隶属向量，由式(3)可得；m 和 k 分别表示直接信任隶属向量和推荐信任隶属向量总数，有 $m \le N$，$k \le N$；n 表示推荐主体数量；$\mathfrak{R}_{(t)}$ 表示 t 时刻待测实体可信度，由式(1)可得；$P_{h(t)}$ 表示 t 时刻推荐主体 h 的可信度。

在 TCA 中，α 和 β 为权重值，分别表示 $\boldsymbol{DT}_{i(t)}^{j\leftarrow i}$ 和 $\boldsymbol{RT}_{h(t)}^{j\leftarrow i}$ 在信任隶属向量 $O_{i(t)}^{j\leftarrow i}$ 中所占比重，有 $\alpha + \beta = 1$。对一个刚愎的用户而言，可设 $\alpha = 1,\ \beta = 0$，这时用户只相信自身的交互历史。对于一个无主见的用户而言，可设 $\alpha = 0,\ \beta = 1$，这时用户完全依靠推荐主体的意见决定取舍。一般 $\alpha > \beta$，即直接信任度的权重大于推荐信任度的权重，就是说用户更相信自身的评判结果。

4 仿真分析

在仿真过程中，假设网络分为善意网络、恶意网络和随机网络 3 种类型。善意网络指交互中提供诚信服务的网络；恶意网络在交互过程中提供不诚信的服务，而随机网络提供的服务具有一定随机性，此类网络有时提供诚信服务，有时提供不诚信的服务。

按照终端对网络服务的评价反馈将终端分为诚信终端、共谋终端和诋毁终端。诚信终端指双方交互后终端提交的反馈评价真实合理。共谋终端交互后对同谋网络提交的评价偏高，对非同谋网络的评价偏低。诋毁终端交互后对服务网络提交的评价总是较低。

4.1 有效性验证

假设异构无线环境中存在 3 个网络，分为善意网络、恶意网络和随机网络，初始信任度均为 0.5。无线环境中所有的终端均为诚信终端。

网络信任度变化趋势如图 2 所示。随着时间的推移，善意网络因为良好的服务质量使得信任度逐渐上升，恶意网络因为服务质量较差，其信任度随时间快速降低，随机网络信任度随服务质量的变化表现出相应的变化趋势。这充分说明了 DTMBEC 模型的有效性。

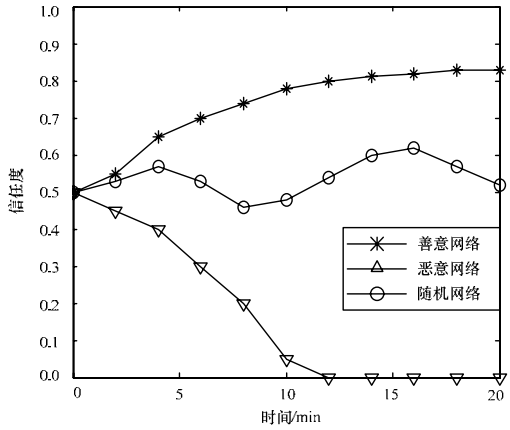

图 2 网络信任度变化趋势

4.2 对比分析

本节从抑制诋毁行为和协同欺骗行为 2 个方面与基于实体声誉的 PeerTrust 模型[6]和基于信任评价云的隶属云信任模型[4]进行对比分析。假设异构无线环境中存在一个信任度为 0.8 的善意网络，随着诋毁终端比例的增加，图 3 显示了 3 种模型下网络信任度的变化趋势。

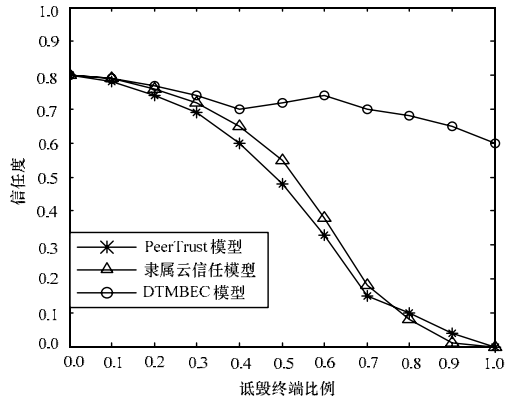

图 3 诋毁行为对比分析

PeerTrust 模型完全依赖其他实体的评价信息来计算待测实体的信任度，没有参考自身的交互历史，计算出的信任值始终与网络的真实信任值有一段距离，并且随着诋毁终端的增加，信任度将迅速降低。隶属云信任模型假设对实体的评价是诚实的，不存在恶意评价行为，因此，随着诋毁终端的增加，信任度也迅速降低。DTMBEC 模型借鉴了推荐主体的推荐信任，还参考了自身直接的历史交互经验，并且通过设置推荐主体可信度，使恶意终端的诋毁行为很难发挥作用。因此，在 DTMBEC 模型中，诋毁终端的数量对信任度的影响有限。

假设在异构无线网络中存在一个初始信任度为 0.5 的恶意网络，共谋终端企图通过频繁的业务交互来夸大恶意网络的信任度。随着共谋终端比例的增加，图 4 显示了 3 种模型

(下转第 166 页)