ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.1, January 2008, pp.116−124
DOI: 10.3724/SP.J.1001.2008.00116

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无线网状网基于不确定性度量极小化信任模型*

丁旭阳+, 范明钰, 朱大勇, 王佳昊

(电子科技大学 计算机科学与工程学院 信息安全研究中心,四川 成都 610054)

Trust Model Based on Minimal Uncertainty Metric in Wireless Mesh Network

DING Xu-Yang+, FAN Ming-Yu, ZHU Da-Yong, WANG Jia-Hao

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)

+ Corresponding author: Phn: +86-28-83206618, E-mail: dingxuyang@tom.com

Ding XY, Fan MY, Zhu DY, Wang JH. Trust model based on minimal uncertainty metric in wireless mesh network. *Journal of Software*, 2008,19(1):116−124. http://www.jos.org.cn/1000-9825/19/116.htm

Abstract: In wireless mesh networks, the sample space of evidence may be not integrative or reliable because of the change of network topology and the occurrence of wireless collision. It makes the existing trust evaluation models inapplicable. To evaluate trust values of nodes and establish trust relationship in nodes, a trust model is proposed on the basis of the analyses of the existing trust models and the minimal principle of uncertainty metric. The model reduces the influence of the non-integrated and unreliable sample space through importing a credible parameter. According to the real situation of networks, the model can minimize the amendment of evaluation values in the whole scope. Contrasted with the evidence-based trust model, the simulation results show that the proposed model is effective.

Key words: wireless mesh networks; trust mode; uncertainty metric; minimal; evidence theory

摘 要: WMN(wireless mesh network)网络环境中,网络拓扑结构的改变或无线冲突的发生,都可能导致作为信任值评估证据的样本空间不一定完整和可靠,使得现有的信任评估模型不能应用其上.为了解决 WMN 网络节点间信任评估问题和建立信任关系,在研究现有信任模型并分析其存在问题的基础上,提出了基于不确定性度量极小化的信任模型.模型引入可信任度因子,根据网络实际情况,弱化证据样本空间不一定完整和可靠对信任值评估的影响,使得信任评估值的修正量在全局范围内达到最小.仿真实验与基于证据理论的信任评估模型进行了对比,表明模型是有效的.

关键词: WMN;信任模型;不确定性度量;极小化;证据理论

中图法分类号: TP393 **文献标识码**: A

WMN(wireless mesh network)是一种新型的宽带无线网络,网络结构与移动 Ad Hoc 网络相似,但总体来说,WMN 网络的节点移动性较弱,网络拓扑变化较小.由于 WMN 所存在的分布式的特点,它极易受到各种各样的攻击[1−4].为抵制攻击,在节点间建立合理的信任关系是一种有效的方法,它不仅有助于发现恶意节点,也有助于网络中的正常节点避免与信任值较小的节点合作,提高网络性能.

* Supported by the National Natural Science Foundation of China under Grant Nos.60673142, 60473090 (国家自然科学基金)
Received 2006-05-17; Accepted 2006-11-30

在网络范畴中,信任是指基于合理的证据或经验对所有参与某一协议的实体是否遵从预定规则集的评估[5].许多领域都涉及信任评估,如电子商务[6,7]、P2P 网络[8]、Ad Hoc 网络以及传感器网络[9,10]等.信任评估需要有一个合适的定量模型,用于计算或推定网络中节点的可信任度,称为信任模型.信任模型根据实现方式不同,可分为集中式与分布式两种[11].集中式是指由网络的可信任根进行节点信任值计算,并将各个节点的信任值提供给其他节点参考,如 PKI(public key infrastructure)[12];分布式是指以网络节点为中心,每个节点根据需要自行计算其他节点的信任值,如 PGP(pretty good privacy)[13].

由于 WMN 网络的特点,现有信任评估模型在其上的应用会受到 3 个方面的影响:(1) WMN 网络缺乏集中而统一的专用服务器,信任值计算不能依赖于第三方完成,导致集中式信任评估不可用;(2) WMN 网络拓扑结构改变或无线冲突发生都可能会使得作为信任值评估的证据空间不一定可靠和完整,导致基于证据理论或经验模型的信任评估模型在进行评估时可能出现较大误差;(3) WMN 网络中节点的计算能力参差不齐,信任值的计算复杂度不能过高,否则将影响网络性能.近年来,对 WMN 网络信任模型的研究并未能很好地解决以上问题[14],其根本原因在于信任评估模型不能有效消除证据空间不一定完整和可靠的影响.

鉴于此,本文结合 WMN 网络的特点,提出了基于不确定性度量极小化的分布式信任评估模型.该模型对现有信任评估模型做了以下 3 个方面的改进:基于分布式构建,无须依赖可信的第三方;通过不确定度量极小化过程对证据空间进行适当调整,减少证据空间不一定可靠和完整对信任评估造成的扰动,并在全局范围内极小化信任评估误差;与现有的其他模型相比,采用了计算复杂度更小的信任评估函数,有利于改善信任评估对网络性能的影响.与证据理论模型的仿真对比实验表明,该信任评估模型能够有效消除证据空间不一定完整和可靠的影响,且具有较好的稳定性.

1 基于不确定性度量极小化的信任评估模型

分布式网络中的信任主要有以下特性:信任反映的是某实体对其他实体未来行为的主观期望;信任与周围环境密切相关;信任是经验的总结和统计上的分析结果[15,16].传统信任关系的建立大都通过概率统计或模糊理论估算出节点的信任值,而后根据信任值来建立彼此的信任关系.但需要注意的是,信任值往往是一个不确定量.事实上,一个理想而实用的不确定性度量,不仅应该是基于有穷经验、随着经验的积累动态可调的,而且应该是具有充分的直观可解释性,使度量可以从少数不涉及无穷的、明白而又自然的前提中逻辑地推导出来.

在信任评估模型中,节点间信任关系分为两类:一类为直接信任关系,即节点 A 直接有对节点 B 的某类经验,可作为可信度评估的依据(如图 1(a)所示);另一类为推荐信任关系,即节点 A 不具有对节点 B 的直接经验,但节点 A 有其他节点提供的关于节点 B 的某类可用作可信度评估依据的经验(如图 1(b)所示).

(a) (b)

Fig.1 Direct trust and recommendation trust

图 1 直接信任与推荐信任

我们知道,对信任关系进行评价的主要依据来源于相关的经验信息,而网络节点间的推荐信任关系主要表现为经验信息的传递和采纳.在经验传递过程中,由于中间节点的参与,需要判断中间节点是否诚实地提供了经验信息和决定对收到的推荐经验信息的采纳程度.因此,直接信任比推荐信任更客观,较容易建立合理和相对准确的数学模型,而推荐信任的处理则有更高的要求.

1.1 基于不确定度量极小化的直接信任评估

若将 WMN 网络中某一节点是否诚实对待下一时刻其他节点的请求看作一个命题 P,易知 P 为一个不确定命题,即 P 的正确性在不同时刻进行检验的结果可真可假,结果为真时检验值取 1,反之,检验值取 0.做一连串这样的检验,可得一个取值为 1 和 0 的序列,称为“经验”或“证据”.记这个序列为 $\{a_i|i=1,2,\ldots,n\}$,设它的前 n 次检验

中,命题 P 为真的次数为 $m=\sum_{i=1}^{n}a_i$.

在 WMN 网络环境中,网络拓扑的改变或无线冲突的发生都可能使得作为信任值评估的证据不一定完整和可靠,对节点可信任度的评估还必须考虑到证据空间扰动对不确定性度量的影响和折算问题,因此,引入证据可信任度因子λ,用于调整证据空间不完整或不可靠对信任值评估带来的影响[17,18].

将对命题 P 的正确性估计记为与 n,m 和λ有关的度量函数 $f_\lambda(n,m)$,并满足以下两个条件:

(i) $f_\lambda(0,0)=\frac{1}{2}$,为边界条件,表示在未做任何检验的情况下,一个认知主体对一个命题是无知的,因此对该命题的不确定性度量应该是无偏的.在 WMN 网络中,从主观概率的角度出发,该边界条件是成立的.

(ii) $0<f_\lambda(n+1,m)<f_\lambda(n,m)<f_\lambda(n+1,m+1)<1$,为顺序条件,表示在做了 n 次检验后再做第 n+1 次检验,结果为真,则度量值增加,结果为假,则度量值减少.但断言一个节点绝对可信或绝对不可信是不恰当的,因此,规定 0 和 1 这两个极端度量值只可逼近,不可到达.显然,顺序条件在 WMN 网络中也是成立的.

为使对命题 P 的不确定度量极小化,考虑泛函 $M[f_\lambda]$,如式(1)所示.

$$M[f_\lambda]=\max\left\{f_\lambda(n+1,0),\lambda\max_{0\le m\le n}[f_\lambda(n+1,m+1)-f_\lambda(n+1,m)],1-f_\lambda(n+1,n+1)\right\} \tag{1}$$

可证,当 $M[f_\lambda]$取得极小值 $\frac{\lambda}{n+1+2\lambda}$ 时,度量函数 $f_\lambda(n,m)$对命题 P 的度量值修正量在全局范围内达到最小,也即度量函数 $f_\lambda(n,m)$取得最优, $f_\lambda(n,m)=\frac{m+\lambda}{n+2\lambda}$.

证明:

I. 证明泛函 $M[f_\lambda]$的极小值为 $\frac{\lambda}{n+1+2\lambda}$.反证法.

如果泛函 $M[f_\lambda]$存在的极小值小于 $\frac{\lambda}{n+1+2\lambda}$,则存在一个 n,m 和λ的组合,使得式(2)~式(4)成立:

$$f_\lambda(n+1,0)<\frac{\lambda}{n+1+2\lambda} \tag{2}$$

$$\lambda\max_{0\le m\le n}[f_\lambda(n+1,m+1)-f_\lambda(n+1,m)<\frac{\lambda}{n+1+2\lambda} \tag{3}$$

$$1-f_\lambda(n+1,n+1)<\frac{\lambda}{n+1+2\lambda} \tag{4}$$

由式(3)可得: $\lambda\sum_{0\le m\le n}[f_\lambda(n+1,m+1)-f_\lambda(n+1,m)]\le\frac{(n+1)\lambda}{n+1+2\lambda}$,当$\lambda\neq0$ 时,可得下式:

$$\sum_{0\le m\le n}[f_\lambda(n+1,m+1)-f_\lambda(n+1,m)]\le\frac{n+1}{n+1+2\lambda},$$

即

$$f_\lambda(n+1,n+1)-f_\lambda(n+1,0)<\frac{\lambda}{n+1+2\lambda} \tag{5}$$

式(2)、式(4)、式(5)三式相加,可得: $1<\frac{\lambda+n+1+\lambda}{n+1+2\lambda}=1$,矛盾.故泛函 $M[f_\lambda]$的极小值为 $\frac{\lambda}{n+1+2\lambda}$.

II. 根据泛函 $M[f_\lambda]$表达式可知,当泛函 $M[f_\lambda]$取极小值时,度量函数 $f_\lambda(n,m)$对命题 P 的度量值修正量在全局范围内达到最小.下面证明当泛函 $M[f_\lambda]$取极小值时,度量函数 $f_\lambda(n,m)=\frac{m+\lambda}{n+2\lambda}$.

当泛函 $M[f_\lambda]$取得极小值时,那么必有:

$$f_\lambda(n+1,0)=1-f_\lambda(n+1,n+1)=\frac{\lambda}{n+1+2\lambda},$$

以及 $f_\lambda(n+1,m+1)-f_\lambda(n+1,m)=\frac{1}{n+1+2\lambda}$,$0\le m\le n$.

于是易得,

$$\begin{cases} f_\lambda(n+1,0)=\dfrac{0+\lambda}{n+1+2\lambda} \\ f_\lambda(n+1,1)=\dfrac{1+\lambda}{n+1+2\lambda} \\ \cdots \\ f_\lambda(n+1,n+1)=\dfrac{(n+1)+\lambda}{n+1+2\lambda} \end{cases}.$$

一般地,有 $f_\lambda(n+1,m)=\dfrac{m+\lambda}{n+1+2\lambda}$,考虑到 $f_\lambda(0,0)=\dfrac{1}{2}$,故有 $f_\lambda(n,m)=\dfrac{m+\lambda}{n+2\lambda}$,$0\le m\le n$. □

在实际 WMN 网络环境中,节点可以根据自身对网络的信任程度选取合适的λ,以调整对其他节点信任值的极小化度量.由式(6)可知,λ的取值如果太大,则掩盖了主体在原有证据基础上做出的不确定性极小化度量.因此,λ取值必须是基于原有证据基础之上的.为讨论λ值变化对信任值评估的影响,假定 n=100,$\lambda=\alpha n$(α=0,0.1,0.2,…,0.9,1),$\dfrac{m}{n}=0.1,0.2,...,0.9$.$\lambda$取不同值时对信任值评估的影响如图 2 所示.

$$\lim_{\lambda\to+\infty} f_\lambda(n,m)=\lim_{\lambda\to+\infty}\frac{\frac{m}{\lambda}+1}{\frac{n}{\lambda}+2}=\frac{1}{2} \tag{6}$$

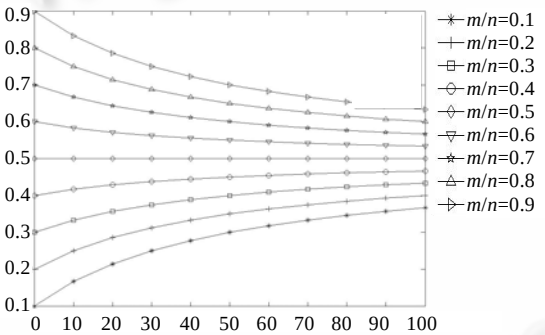


Fig.2 Infection of different λ to trust evaluation

图 2 λ取值不同时对信任值评估的影响

由图 2 可以看出,λ值越小,曲线逼近极端度量值$\left(\dfrac{m}{n}\right)$的速度越快,也即对网络信任的程度越高;反之,$\lambda$值越大,逼近极端值$\left(\dfrac{m}{n}\right)$的速度越慢,对网络怀疑的程度越大;而当信任评估值为$\dfrac{1}{2}$时,直观解释为信任评估主体对被评估主体的怀疑程度和可信程度相等,λ的取值不会左右其对信任值的判定.因此,λ可以看作是一个个性参数,它刻画了等量证据下不同认知主体做出的不同程度的内部调适.

1.2 推荐信任

直接信任是针对具有直接经验的节点的信任度评估,推荐信任是指网络中一个节点向另一个节点推荐其他节点的可信任值.对一个节点推荐的信任值,我们很难简单地划分为可信和不可信两种情况,即使进行划分,往往也会带有很大的随意性和主观性.另外,由于网络中节点对网络全局环境的主观信赖程度或收集的证据集的情况不同,即使是对同一节点的信任度的多次估算值也不一定相同.因此,节点间推荐信任关系的建立必须是相当谨慎的.

现有的信任模型对推荐信任关系评估的方法主要有贝叶斯网络、基于权重的合成、证据理论等[19−21].文献[19]中提出用贝叶斯网络解决推荐信任问题,但贝叶斯网络过于依赖专家经验,对经验的可靠性要求较高,且在

WMN 网络中,专家经验往往难于获取,很难保证其可靠性.文献[20]提出了基于权重的信任传递方法以解决推荐信任问题,但该方法中权重没有量化依据,在实际应用中难以确定.文献[21]提出基于证据理论来解决推荐信任问题,但由于 WMN 网络固有的特点,证据空间的不一定完整和可靠将导致信任评估出现较大误差.Abdul-Rahman 等人在文献[22]中将推荐信任划分为 6 个等级,用于标识不同节点的推荐可信程度,但事实上,过细的推荐信任划分会导致算法复杂度增加和可操作性降低.

考虑到推荐信任模型的可操作性和使用效率,我们引入可信系数 r 作为信任权重,用于刻画推荐路径上节点对推荐信任值的信任程度.推荐信任由直接信任值 t(根据与被评估节点有直接信任关系的节点计算得到)和对直接信任值的可信系数 r 组成,记为(t,r).

1.2.1 单路径信任推荐

如图 3(a)所示,设节点 A 对 B 的直接信任值为 t_{AB},节点 A 根据对节点 B 的直接信任值 t_{AB} 选取对节点 B 所推荐信任值可信任系数为 r_{AB},节点 B 向 A 推荐信任为(t_{BC},r_{BC}).节点 A 收到节点 B 的推荐信任后,按照式(7)对可信系数进行合成.

$$r_{AC}=r_{AB}\times r_{BC} \tag{7}$$

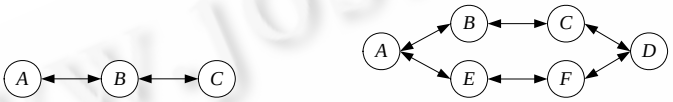


Fig.3 Combination of recommendation trust

图 3 推荐信任合成

在获得图 3(a)所示路径上 A 对 C 的可信系数以及 B 对 C 的直接评估信任值的基础上,根据公式(8)可得节点 A 接受的对 C 的推荐信任值.

$$t_{AC}=r_{AC}\times t_{BC} \tag{8}$$

当有多个中间信任推荐节点时,设节点序列为$\{M_1,M_2,\ldots,M_n\}$,合成可信系数及接受推荐信任值分别为

$$r_{M_1M_n}=\prod_{i=1}^{n-1} r_{M_iM_{i+1}} \tag{9}$$

$$t_{M_1M_n}=t_{M_{n-1}M_n}\times\prod_{i=1}^{n-1} r_{M_iM_{i+1}} \tag{10}$$

1.2.2 多路径信任推荐

在 WMN 网络中,通信节点对之间常常有多条路由.如图 3(b)所示,节点 A 与节点 D 之间存在两条推荐路径,path1:A-B-C-D 与 path2:A-E-F-D,设两条推荐路径上的推荐信任分别为$(t_{CD},r_{AD}1)$和$(t_{FD},r_{AD}2)$,则节点 A 对节点 D 的合成信任值可按照公式(11)计算得到.对多条路径的情况可以此类推.

$$t_{AD}=\frac{t_{CD}\times r_{AD}1+t_{FD}\times r_{AD}2}{r_{AD}1+r_{AD}2} \tag{11}$$

此外,我们还需注意到一个事实,当 A 从多条推荐路径获得推荐信任时,一些推荐路径的终点可能是同一个推荐节点,而从源自同一推荐节点的多条推荐路径上获得的推荐信任值总和不应大于最终推荐节点的直接信任值.直观上看,在最终推荐节点不同的情况下,按照公式(11)计算合成信任得到的结果是可接受的.但考虑到特殊情况,如图 4 所示,两条推荐路径的最终推荐节点是同一个节点 M,则无论这两条推荐路径上的可信系数如何,最终的合成信任值都等于最终推荐节点的直接信任值,这是不合理的.因此,我们需要对最终推荐节点相同的推荐路径上的可信系数进行合成,记为 $\bar{r}$.

如图 4 所示,设 path1:A-B-C-M-D 与 path2:A-E-F-M-D 为节点 A 和 D 之间的两条最终推荐节点相同的推荐路径,它们的推荐可信系数分别为 $r_{AD}1$ 和 $r_{AD}2$.此情形相当于有两个证据存在,表明推荐结论为真的可能性分别为 $r_{AD}1$ 和 $r_{AD}2$,那么根据概率论的方法,通过公式(12)计算可得合成可信系数 $\overline{r_{AD}}$.

$$\overline{r_{AD}} = 1-(1-r_{AD}1)\times(1-r_{AD}2) \tag{12}$$

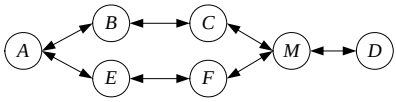


Fig.4 Combination of recommendation trust with the same final recommendation node

图 4 最终推荐节点相同的推荐信任合成

在推荐可信系数合成的基础上,设 $M_i(i=1,2,\ldots,m)$分别为推荐路径上各不相同的最终推荐者,$r_{ij}(i=1,2,\ldots,m;j=1,2,\ldots,n)$为一类以 M_i 为最终推荐节点的推荐路径的可信任系数,$t_i(i=1,2,\ldots,m)$为相应于 M_i 对被评估节点的直接信任值.定义 $\overline{r_i}$ 为以 M_i 为最终推荐节点的推荐路径的信任系数的合成,则合成推荐信任值 t 可按照公式(13)计算得到:

$$t = \frac{\sum_{i=1}^{m}(\overline{r_i}\times t_i)}{\sum_{i=1}^{m}\overline{r_i}} \tag{13}$$

2 仿真实验

为分析文中提出的信任评估模型,我们在 WMN 网络环境中对其进行了仿真测试.仿真工具选取 OPNET,仿真范围为 1000×1000m^2 的矩形区域,随机分布 50 个节点(根据可信度不同分为 4 类,见表 1),网络含有一个 FTP 服务器 G,位于网络物理中心(网络初始拓扑如图 5 所示,实线表示两节点在彼此通信覆盖范围内).无线节点通信覆盖半径均为 250m,MAC(media access control)层采用 IEEE 802.11 协议,路由协议采用 DSR(dynamic source routing)协议[23].

Table 1 The classification of simulation nodes

表 1 仿真节点分类表

Node classes	Number of node	Node ID	Trust value of node
Untrusty node	5	U1~U5	<0.1
Low-Trusty node	20	L1~L20	0.5
Medium-Trusty node	20	H1~H20	0.8
High-Trusty node	5	C1~C5	>0.9

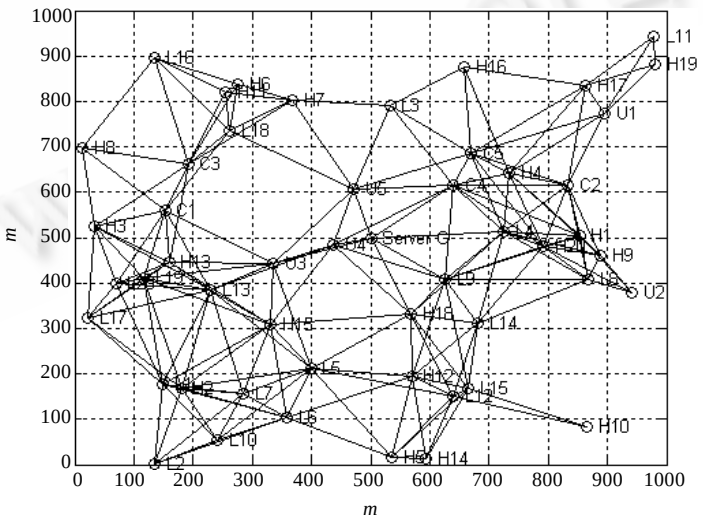


Fig.5 The topology of original network

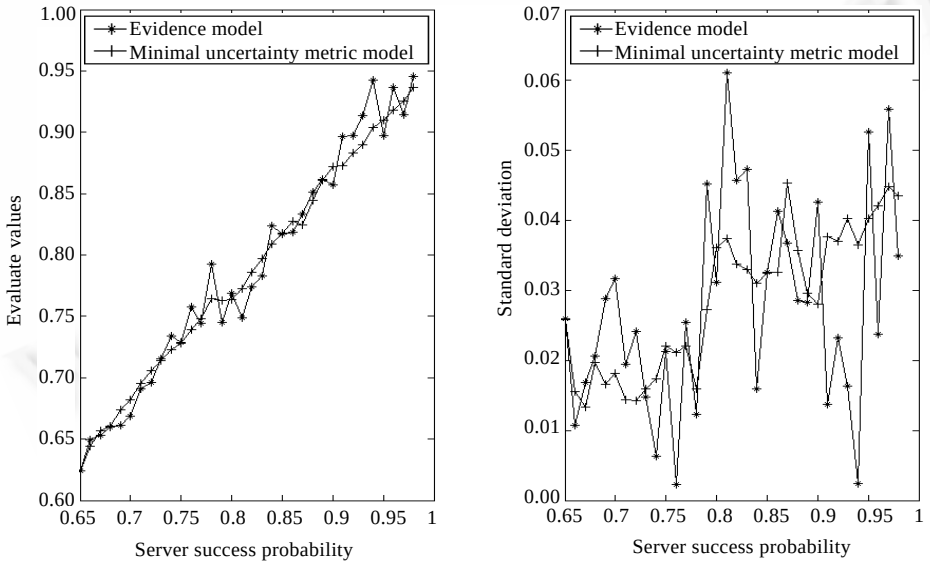
图 5 网络初始时刻拓扑结构

为使仿真实验更接近实际情况,信任评估主体只有在对被评估节点缺乏直接经验时,才需要从其他节点获取信任值信息.在仿真实验中,设定服务器 G 在固有成功率 p 不同的情况下(p 从 0.65~0.98,间隔为 0.01),网络中节点随机向服务器 G 发起 1 000 次下载请求,服务器 G 根据其固有成功率,服从(0-1)分布($P\{x=k\}=p^k(1-p)^{1-k}$, $0<p<1,k=0,1$),随机接受或拒绝一个请求.由于无法确切地了解信任推荐者的行为,在仿真实验中设信任推荐者所提供的推荐信任值的误差程度服从正态分布 $N(u,0.004u)$,其中,u 为推荐者自身的客观可信任度.

仿真实验中,模型选用了启发式算法对不确定因子λ的值进行渐近调整.在仿真初始时刻,用户对网络其他节点的可信任状况是无知的.但无论用户是否乐意,在这种情形下,它只能姑且乐观地信任网络其他节点所提供的所有信息.因此,在初始时刻,设定不确定因子λ=0.随着用户对网络中其他用户信息的积累,逐渐对信任模型的不确定因子进行调整,以期适合于网络的真实状况.用户每收集到一定的证据量 n(仿真中取值为 50),根据新的证据统计情况,对不确定因子λ进行调整.例如,在时刻 t_0,假设用户根据证据样本计算得到的可信任度为 0.9,而在时刻 t_1,用户根据自身统计得到的证据样本计算得到的可信任度为 0.8,则用户认为在该推荐路径上的可信任度存在 0.1 的误差,相应地调整不确定因子λ=0.1n.

仿真实验在静态 WMN 网络和动态 WMN 网络(节点随机移动,速度范围设定为 0~15m/s)环境下,统计网络中节点在证据理论模型[21]和不确定性度量极小化模型下,对服务器 G 的信任评估值(取估算节点估算值的算术平均).仿真结果如图 6 和图 7 所示.

对于静态 WMN 网络,从图 6(a)所示的仿真结果可以看出,不确定性度量极小化模型对服务器 G 的信任值评估曲线较证据理论模型更平滑.证据理论模型对服务器 G 的信任评估值围绕 G 的固有成功率 p 上下波动;不确定性度量极小化模型对服务器 G 的信任评估值略小于 G 的固有成功率 p,这是由于受到可信任度因子λ的影响.由图 6(b)的标准差曲线可以看出,不确定性度量极小化模型估算信任值与服务器 G 的固有成功率 p 的差值较为稳定,在 0.01~0.05 之间发生变化;证据理论模型估算信任值与服务器的固有成功率 p 的差值波动较大,在 0~0.07 之间变化.这说明,不确定性度量极小化模型能够较好地克服网络环境的影响,客观地给出一个合理的信任估算值,使得估算值与实际值之间的差值较为稳定.即达到了不确定性度量极小化的目的:在全局范围内,使度量值的修正量达到最小.

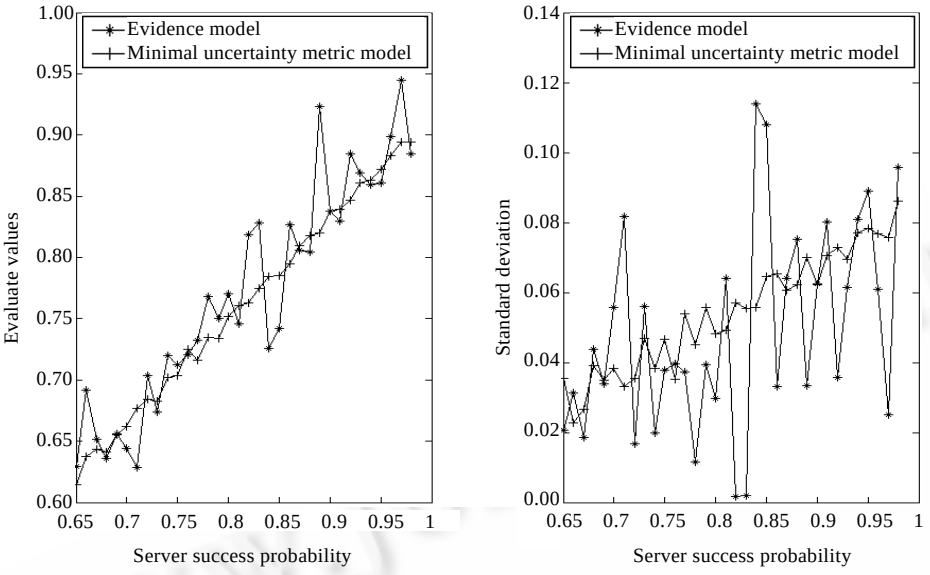


(a) Model estimates (a) 模型估算值

(b) The standard deviation of estimates (b) 估算值标准差

Fig.6 Static wireless mesh network

图 6 静态 WMN 网络



(a) Model estimates (b) The standard deviation of estimates

(a) 模型估算值 (b) 估算值标准差

Fig.7 Dynamic wireless mesh network

图 7 动态 WMN 网络

值得注意的是,在有线网络环境中,基于证据理论的信任评估模型的仿真结果的准确度要优于在 WMN 网络环境中的仿真结果.这是由于,在 WMN 网络环境中,网络拓扑结构的改变或者无线冲突的发生,可能引起通信过程中数据包丢失或通信失败,在信任评估时导致作为信任值评估的证据样本不一定完整和可靠.因此,基于证据理论的评估模型由于受到证据空间扰动的影响,其信任评估值的波动较大.

在动态 WMN 网络环境中(图 7),与图 6 相比,证据理论模型对服务器 G 的信任评估值较静态网络环境下波动得更为剧烈,而不确定性度量极小化模型却仍能保持相对较好的稳定性.虽然由于动态 WMN 网络中因节点移动带来的证据空间有更为剧烈的扰动,使得两种模型对服务器 G 的信任评估值与 G 的固有成功率 p 之间的差值增大,如图 7(b)所示,但从仿真结果可以看出,不确定性度量极小化模型能在一定程度上消除 WMN 网络中证据空间扰动对信任评估的影响,其稳定性优于基于证据理论的评估模型.

综上所述,在 WMN 网络环境中,不确定性度量极小化模型通过不确定性度量极小化过程,使得信任评估值在全局范围内的修正量达到最小,且在合理评估信任值的同时使得稳定性能优于证据理论模型.

3 结 论

本文深入研究了 WMN 网络环境中节点直接信任值评估以及推荐信任的传递和合成问题,分析了现有的信任评估模型,例如基于贝叶斯网络推理、基于权重以及证据理论等的信任评估模型,指出了其中存在的问题,并在借鉴这些信任评估模型的基础上,从信任的定义、度量、信任传递和综合计算等方面出发,给出了一个基于不确定性度量最小化的信任评估模型.主要工作有:(1) 从信任的定义出发,使用不确定性度量最小化原理对直接信任关系的度量进行解释,并给出了一个直接信任值计算公式,计算结果可直接用于信任决策;(2) 分析了现有模型中信任传递过程中的优缺点,并在此基础上提出了信任传递模型,通过引入可信任系数对信任关系做出较客观和合理的评价;(3) 将该模型与证据理论模型分别在静态和动态 WMN 网络环境中进行了仿真实验,实验结果验证了模型的合理性.

References:

[1] Zhou L, Haas ZJ. Securing ad hoc networks. Network IEEE, 1999,13(6):24−30.

[2] Zhang Y, Lee W. Intrusion detection in wireless ad-hoc networks. In: Proc. of the ACM MOBICOM. 2000. 275−283. http://portal.acm.org/citation.cfm?doid=345910.345958

[3] Marti S, Giuli T, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In: Proc. of the 6th Annual ACM/IEEE Int'l Conf. on Mobile Computing and Networking. 2000. 255−265. http://portal.acm.org/citation.cfm?id=345910.345955

[4] Hu YC, Perrig A, Johnson DB. Ariadne: A secure on-demand routing protocol for ad hoc networks. In: Proc. of the 8th ACM Int'l Conf. on Mobile Computing and Networking. 2002. 12−23. http://www.geocities.com/prashthy/secure_routing_ad_hoc.html

[5] Eschenauer L, Gligor VD, Baras J. On trust establishment in mobile ad hoc networks. In: Proc. of the 10th Int'l Workshop on Security Protocols. 2002. 47−66. http://dblp.uni-trier.de/rec/bibtex/conf/spw/EschenauerGB02

[6] Manchala DW. Trust metrics, models and protocols for electronic commerce transactions. In: Proc. of the 18th Int'l Conf. on Distributed Computing Systems. 1998. 312−321. http://portal.acm.org/citation.cfm?id=850926.851678

[7] Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. In: Proc. of the Decision Support Systems. 2005. http://citeseer.ist.psu.edu/738255.html

[8] Yu B, Singh MP, Sycara K. Developing trust in large-scale peer-to-peer systems. In: Proc. of the 1st IEEE Symp. on Multi-Agent Security and Survivability. 2004. 1−10. http://jmvidal.cse.sc.edu/lib/yu04a.html

[9] Buchegger S, Boudec JL. Performance analysis of the confidant protocol. In: Proc. of the IEEE/ACM Symp. on Mobile Ad Hoc Networking and Computing. 2002. 226−236. http://portal.acm.org/citation.cfm?id=513828

[10] Theodorakopoulos G, Baras JS. Trust evaluation in ad-hoc networks. In: Proc. of the 2004 ACM Workshop on Wireless Security. 2004. 1−10. http://portal.acm.org/citation.cfm?id=1023648

[11] Theodorakopoulos G. Distributed trust evaluation in ad hoc networks [MS. Thesis]. University of Maryland, 2004.

[12] Housley R, Ford W, Polk W, Solo D. RFC 2459, Internet X.509 public key infrastructure, 1999.

[13] Beth T, Borcherding M, Klein B. Valuation of trust in open networks. In: Proc. of the 3rd European Symp. on Research in Computer Security. 1994. 3−18. http://www.informatik.uni-trier.de/~ley/db/conf/esorics/esorics1994.html

[14] Theodorakopoulos G, Baras JS. On trust models and trust evaluation metrics for ad hoc networks. IEEE Journal on Selected Areas in Communications, 2006,24(2):318−328.

[15] Mui L, Mojdeh M, Ari H. A computational mode of trust and reputation. In: Proc. of the 35th Hawaii Int'l Conf. on System Sciences. 2002. 2431−2439. http://portal.acm.org/citation.cfm?id=821158

[16] Zand D. Trust and managerial problem solving. Administrative Science Quarterly, 1972,17:229−239.

[17] Carnap R, Jeffrey RC. Studies in Inductive Logic and Probability, Vol.1. Berkeley: The University of California Press, 1971.

[18] Niiniluoto I. On a *k*-dimensional system of inductive logic. Philosophy of Science Association, 1976,2:425−477.

[19] Wang Y, Vassileva J. Bayesian network-based trust model. In: Proc. of the IEEE/WIC Int'l Conf. 2003. 372−378.

[20] Guha R, Kumar R, Raghavan P, Tomkins A. Propagation of trust and distrust. In: Proc. of the Int'l World Wide Web Conf. 2004. 17−22. http://citeseer.ist.psu.edu/guha04propagation.html

[21] Yu B, Munindar P. An evidential model of distributed reputation management. In: Proc. of the Int'l Conf. 2002. 294−301.

[22] Abdul-Rahman A, Hailes S. Using recommendations for managing trust in distributed systems. In: Proc. of the IEEE Malaysia Int'l Conf. on Communication'97. 1997. http://citeseer.ist.psu.edu/360414.html

[23] Johnson DB, Maltz DA, Hu YC. The dynamic source routing protocol for mobile ad hoc networks (DSR). 2004. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

丁旭阳(1981－),男,贵州遵义人,博士生,主要研究领域为无线网络,信息安全.

朱大勇(1977－),男,博士,讲师,主要研究领域为网络通信,系统仿真.

范明钰(1962－),女,博士,教授,博士生导师,主要研究领域为网络与信息安全.

王佳昊(1979－),男,博士生,主要研究领域为无线传感器网络,信息安全.