Ad hoc网络中鲁棒信任机制的研究

孙玉星[1,2] 杜景林[2,3] 谢 立[2] 冯国富[1]

(南京审计学院信息科学学院 南京 211815)[1]

(南京大学计算机软件与新技术国家重点实验室 南京 210093)[2]

(南京信息工程大学电子与信息工程学院 南京 210044)[3]

摘 要 在Ad hoc网络中,报文转发依赖于各个分布节点间的协作。在分析了不同路由协议对信任模型的不同需求基础上,针对源路由协议特性,提出了鲁棒信任机制(RTM)。该机制基于OTMF模型,采用了基于确认机制从非邻接节点获取直接信息的方法,以及基于贝叶斯决策的推荐信任度修正方法,有效提高了信任评价的正确率。实验结果表明,RTM能较好地抵御针对信任模型的虚假推荐攻击并具有较快信任评价收敛速度。

关键词 Ad hoc网络,信任管理,信任模型,报文转发

中图法分类号 TP393 **文献标识码** A

On Robust Ttrust Mechanisms in Ad hoc Networks

SUN Yu-xing[1,2] DU Jing-lin[2,3] XIE Li[2] FENG Guo-fu[1]

(School of Information Science, Nanjing Audit University, Nanjing 211815, China)[1]

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]

(Information Engeering School, Nanjing University of Information Science & Technology Electronic, Nanjing 210044, China)[3]

Abstract *Packet delivery of Ad hoc networks depends on collaboration among distributed entities. Different needs on the trust models of varieties of routing protocols were analyzed separately. The robust trust mechanisms(RTM) were proposed to meet the new demands of source routing protocols for trust models. A new scheme for gathering first-hand trust information from non-neighbor nodes using acknowledgements was presented in paper. The RTM expands the OTMF by providing recommendation trust revision support, which is based on Bayesian Decision-Making theory and minimum-loss principle and promotes accuracy of trust value. Simulations show that compared with the OTMF, the RTM is helpful to reduce the impact of some threats on trust management and has better convergence.*

Keywords Ad hoc networks, Trust management, Trust model, Packet delivery

1 引言

Ad hoc网络是自组织网络在无线网络领域中的一个应用。由于Ad hoc网络缺乏固定的基础设施,节点拓扑结构具有高度的动态性,以及它的无中心性、自组织性、临时性等特点,因此其安全问题十分突出。传统的提供网络安全的做法常借用工具进行加密和验证,但是,基于加密的安全概念不能解决在Ad hoc网络中所遇到的新特征和新恶意行为(例如,如果路由中存在恶意或自私节点,则难以保证多跳路由上的报文可靠传递),因为加密技术不能防止内部对手或错误节点提供有意的和无意的错误服务。因此,信任模型的建立与管理越来越成为保障Ad hoc网络安全的重要部分。

信任模型虽然可以有效提高Ad hoc网络性能,并检测出恶意实体,但是它本身也是攻击者攻击的对象。除了一些常见的攻击手段,文献[1]总结了由于信任模型自身所采用的方法所引入的新的安全问题,例如错误推荐攻击、叛国者攻击、偏见攻击等。

本文针对Ruidong Li[2]提出的信任管理模型OTMF在抵御虚假推荐方面的缺陷,提出了鲁棒信任机制(Robust Trust Mechanisms),考虑了Ad hoc网络中源路由算法对信任模型的特殊需求,提出了非邻接节点直接信任信息获取方案,以及基于贝叶斯决策的推荐信任度修正方法,避免了虚假推荐对信任模型的正确性的不良影响。

本文第2节分析了OTMF信任模型缺陷及源路由协议对信任模型的新需求;第3节阐述了直接信任信息获取方案;第4节论述间接推荐信任度修正机制;第5节通过模拟实验

到稿日期:2009-09-15 返修日期:2009-12-28 本文受国家自然科学基金(No. 60673154),江苏省高校自然科学研究(No. 09KJD520005),江苏省自然科学基金(No. BK2009396)资助。

孙玉星(1977—),女,博士生,讲师,主要研究方向为无线网络、网络安全,E-mail:scholar_syx@yahoo.com.cn;杜景林(1974—),男,博士生,副教授,主要研究方向为分布式系统、无线传感器网络;谢 立(1942—),男,教授,博士导生师,主要研究方向为分布式计算、网络安全;冯国富(1977—),男,副教授,主要研究方向为分布式计算、计算机审计。

进行性能分析。

2 OTMF 信任模型与源路由协议的新需求

2.1 相关工作

近年来，对 Ad hoc 网络信任模型的研究成为当前安全领域的一个研究热点。各种信任计算模型层出不穷，有些信任模型是基于半环(semiring)代数理论[3,4]；有些信任模型是基于统计学的信任评估规则，文献[5]采用马尔科夫链证明了该方法的收敛性；还有一些信任模型是建立在传统的贝叶斯框架之下[2,6]，有些在此基础之上引入了信息熵(entropy)理论[7]。不同的信任模型计算方法在抵御针对信任模型攻击能力方面各有不同，文献[1]中已作分析。

本节主要分析了 OTMF 存在的问题以及 Ad hoc 网络中源路由协议的特性，由此提出了适应源路由协议的鲁棒信任机制。

2.2 OTMF 信任计算模型

定义 1 信任[8]是一个实体对另一个实体或团体将执行某种行为的一种特定的主观概率详细评定，这一评定是在实体可以观察到行为之前，并会影响他自己的行为。

本文中，信任是建立在两个节点之间对是否正确传递报文这一行为的主观概率测定。信任信息的获取可以通过直接和间接两个方式，直接信息是主体节点通过自身直接观察客体节点的报文传递行为来获取计算信任值。主体节点可以通过信任繁衍获得间接信息，本文中采用的信任繁衍方式是从其他节点请求推荐信任值，即从其他节点获取其他节点所知的直接信任值。在 OTMF 模型中直接信息被称为第一手信息，间接信息被称为第二手信息。

OTMF 模型融合了节点的自主信任观点和信誉信息，从结果可以看出，该模型对偏见式攻击有较好的抵御作用。

该模型使用 ITF 表示由原始数据产生的初始信任结构，例如 $ITF_{ij}=(\alpha_{ij},\beta_{ij})$，其中 α_{ij} 表示成功转发报文行为的次数，β_{ij} 表示未转发报文的次数。系统在计算信任评估时引入了信心值(confidence value)，信心值表示信任值计算的精确度，高信心值意味着目标实体已经经历了主体或者其他实体的多次检验。系统的执行过程可以分为以下四步：

S1：使用第一手信息更新 ITF。直接信息更新方式如式(1)所示。

$$\begin{aligned}\alpha_{ij}&=\alpha_{ij}+s\\ \beta_{ij}&=\beta_{ij}+1-s\end{aligned}\tag{1}$$

S2：分发和处理二手信息，各个节点周期性地根据直接信息产生二手信息并分发该信息。二手信息是从其他节点收集的关于目标节点的第一手信息，更新方式类似 ITF 的更新方法，由于只经历了一个时间段，因此处理的是该时间段内正常行为和错误行为的次数。

S3：根据 S1 和 S2 步骤得到 ITF 和二手信息，评估其他实体的基本观点由两个部分组成：信任值 $t\{i:j,action\}$ 和信心值 $c\{i:j,action\}$，计算方法如式(2)、式(3)所示。

$$t\{i:j,action\}=E(Beta(x,\alpha,\beta))=\frac{\alpha}{\alpha+\beta}\tag{2}$$

$$\begin{aligned}c\{i:j,action\}&=1-\sqrt{12}\sigma(Beta(x,\alpha,\beta))\\&=1-\sqrt{\frac{12\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}}\end{aligned}\tag{3}$$

S4：评估可信度，根据信任和信心值计算可信度，计算方法如式(4)所示。

$$T\{i:j,action\}=1-\frac{\sqrt{\frac{(t-1)^2}{x^2}+\frac{(c-1)^2}{y^2}}}{\sqrt{\frac{1}{x^2}+\frac{1}{y^2}}}\tag{4}$$

该模型认为偏见攻击主要产生的原因是实体只考虑了自身的直接观察信息，而自身观察与实际目标实体的表现有偏差，所以导致偏见攻击。为了抵制这样的攻击该系统考虑到将自身的观察和二手信息融合起来，但该模型的成功是建立在二手信息真实的基础之上的，如果二手信息不真实，那么该系统的作用将是有限的。

2.3 源路由协议对信任模型的新需求

传统的路由协议分类方法不足以体现不同路由算法对信任模型的不同需求。我们将 Ad hoc 路由协议分为两类：源路由协议和非源路由协议。源路由协议是路由协议在分组转发前已经全面了解从源端到目的端的完整路由信息，代表性的协议有 DSR，MSR 等。非源路由协议是指路由协议逐跳根据路由表信息转发报文，在转发报文前对完整路由信息没有认识了解，代表性的协议有 AODV，DSDV 等。

对于非源路由协议报文的转发只需要关注和邻接节点的交互，所以在可靠报文转发信任模型中只需要关心邻接节点的转发行为是否正常。在此类路由协议中，信任模型仅需获取邻居节点的直接观测信息即可，甚至无需从其他节点获取间接信息，即使为了避免偏见式攻击，使用了间接信息，也可以较简单地识别间接信息的真伪，所以对信任模型的功能要求较低。

对于源路由协议，由于报文转发前了解到完整路由信息，意味着选择路由前可以通过信任模型判断路径中各个中转节点的工作质量，即通过判断该路由中是否存在恶意节点或自私节点以避免不必要报文转发的延迟，提高网络带宽和资源的利用效率。但路由中的中继节点不一定是该节点的邻接节点，如何获取这些中继节点的信任值成为信任模型的一大挑战。常用思路是向邻接(或一定跳数范围内)节点发送请求，以获得间接信息，但是引入了新的安全问题，恶意节点可以通过发送伪造间接信息来达到攻击的目的。为了提高信任模型的鲁棒性，需要信任模型能获取非邻接节点的直接信息，并以此判断间接信息的真伪从而调整对某节点传达的间接信息的信任度，以减少虚假间接推荐的恶意影响。

3 直接信息获取

该鲁棒信任机制在传统的从邻接节点获取直接信息的基础上，采用基于确认机制的方法实现从非邻接节点获取直接信息。

3.1 获取邻接节点直接信息

无线信道侦听获取直接信息的方式类似 Watchdog[9]，假定节点间的链路都是双向通讯并且节点工作在混杂侦听模式下。节点发包之后，侦听下一跳节点的通信。如果在设定时间内，没有听到该包被继续传送到路径上的下一节点，那么认为下一跳节点自私丢包。我们的侦听方案中，如果节点没有将报文成功传递到下一跳，则将会被标识为失败行为。当然失败可能是由于节点的恶意行为或非恶意行为例如：网络拥塞、节点移动或节点故障造成的。无线信道监听只负责观测

邻接节点行为，而不区分是恶意或非恶意失败行为。

在该侦听方案下，节点 s 将保持计数器 A_{si}，C_{si} 的更新，其中下标 i 表示 s 节点的一个邻接节点，对于每一个邻接节点 i 都存在一对相应计数器$\{A_{si}, C_{si}\}$。其中计数器 A 记录了邻接节点 i 在一个观察时间窗内所接受到的需要转发的报文总数，计数器 C 记录了邻接节点 i 在一个观察时间窗内正确转发的报文总数，所谓正确转发是指正确传递到下一跳节点，而非丢弃或错误路由。计数器$\{A_{si}, C_{si}\}$的更新方法如下：当节点 s 观测到有一个报文需要从节点 i 转发到节点 j 时，路由信息如下$\{*, i, j\}$（$*$ 表示源端节点可以为 s 节点也可以不是），A_{si} 增一，同时计时器初始化。超时时隙值 t_{link} 大于邻接节点通讯的最大的往返延迟(Round-Trip Time)。如果在计时器超过 t_{link} 之前，节点 s 观测到报文拷贝由节点 i 传向下一跳节点 j，那么计数器 C_{si} 增一，否则计数器 C_{si} 不更新。

3.2 获取非邻接节点直接信息

通过 2.3 节的分析，针对 ad hoc 的源路由协议的新需求，在信任模型中，节点需要获取非邻接节点的直接信息。本文提出了基于确认机制的非邻接节点直接信息获取方案，该方案考虑到 Ad hoc 网络的特征，没有采用类似 TCP 的端到端的确认机制，而是采用近似逐跳确认机制，有效防止了 Ad hoc 网络链路不稳定导致确认报文的丢失所造成的误判。如图 1A 所示的路径，源端 s 将报文传递到目的端 d，途径 u, v_i $(1\leqslant i\leqslant n)$等节点。当节点 u 将报文转发给 v_1 时，将更新所有下游中继节点的计数器 A，如式(5)所示。

$$A_{uv_i}=A_{uv_i}+1 \quad 1\leqslant i\leqslant n \tag{5}$$

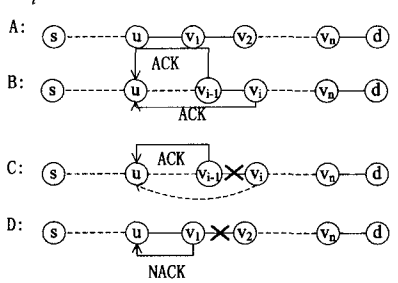

图 1 报文转发状态

若节点 v_i 收到 v_{i-1} 发来的报文将返回 ACK 报文，该 ACK 报文包含确认者、所确认正常点以及所确认正确传递的报文 ID 等信息，则该 ACK 报文将沿原途返回。如图 1B 所示，在时间片 t' 内，如果节点 u 收到节点 v_i 发来的 ACK 报文，则意味着该路径上节点 u 到节点 v_{i-1} 的中转节点都正确转发报文，节点 u 向上游转发时间片 t' 内所收到的最远节点 v_i 传来的 ACK 报文，同时将更新自己与节点 v_i 之间非邻接中继的计数器 C，如式(6)所示。

$$C_{uv_j}=C_{uv_j}+1 \quad 2\leqslant j\leqslant i-1 \tag{6}$$

由于节点 v_1 是节点 u 的邻接节点，对于节点 v_1 计数器的更新在 MAC 层的 3.1 节介绍的无线信道侦听阶段完毕。

如果在时间片 t' 前，节点 u 已经收到节点 v_k $(k<i)$传来的 ACK 报文，那么节点 u 将更新 v_k 与节点 v_i 之间非邻接中继的计数器 C，如式(7)所示。

$$C_{uv_j}=C_{uv_j}+1 \quad k\leqslant j\leqslant i-1 \tag{7}$$

如果节点 u 在超时时隙 t_{ack} 内(超时时隙 t_{ack} 应大于报文沿路径往返传递所需最长时间)，没有收到节点 v_i 传来的 ACK 报文，如图 1C 所示，那么节点 u 可以推断链路 v_{i-1}, v_i 之间出现问题，但是由于 v_{i-1}, v_i 并非节点 u 的邻接节点，因此节点 u 不能确定是节点 v_{i-1} 没有转发报文还是节点 v_i 是自私或恶意节点，所以只能同时对 v_{i-1}, v_i 实施惩罚。为了避免对节点 v_i 下游节点无谓的惩罚，这些节点的计数器 A 将做如式(8)的调整。

$$A_{uv_j}=A_{uv_j}-1 \quad i+1\leqslant j\leqslant n \tag{8}$$

对于路由$\{u, v_1, v_2\}$，如图 1D 所示，如果在计时器超过 t_{link} 之前，节点 v_1 没有通过 MAC 层无线信道侦听到报文由节点 v_2 传向下一跳节点，那么节点 v_1 可以发现邻居节点 v_2 没有正确转发报文，则在调整针对 v_2 计数器同时向上游节点转发 NACK 消息，NACK 报文中包含了所确认中断点、确认推断者以及所确认正确传递的报文 ID 等信息。节点 u 接受到节点 v_1 的 NACK 消息后，向上游转发 NACK 消息，同时对 v_2 下游的节点计数器 A 做如式(9)调整。

$$A_{uv_j}=A_{uv_j}-1 \quad 3\leqslant j\leqslant n \tag{9}$$

在此方案中，采用两种方式探测报文在链路上未被正常转发从而获取非邻接节点直接信息：1)通过超过时隙 t_{ack} 未收到 ACK 报文，推断报文未被正常转发；2)通过观测到非正常转发行为，节点向上游通告 NACK 消息。非邻接节点直接信息获取方案中采用了这两种方法互为弥补，提高精确性。

4 间接信息的信任度修正

由于在该鲁棒信任机制中使用了间接信息，恶意节点可以通过虚假推荐达到各种攻击目的，因此在该机制中使用了基于贝叶斯决策的对间接信息的信任度修正机制[10]，以减少虚假间接推荐信息对信任模型建立正确的信任评价的影响。

4.1 推荐偏差度

定义 2（间接推荐偏差度） 假设 T_{ik} 表示节点 i 通过直接观察所计算出对节点 k 正确转发报文行为的主观概率评价。R_{ik}^{j} 表示节点 i 从节点 j 那里获取的间接推荐值，即节点 j 对节点 k 正确转发报文行为的主观预期。那么间接推荐偏差度 D_{ik}^{j} 表示 R_{ik}^{j} 与 T_{ik} 之间的偏差，如式(10)所示。

$$D_{ik}^{j}=R_{ik}^{j}-T_{ik} \tag{10}$$

如果 D_{ik}^{j} 大于 0，表示节点 j 的推荐比节点 i 实际观察到的情形要好。如果 D_{ik}^{j} 小于 0，表示节点 j 的推荐比节点 i 实际观察到的情形要糟糕。推荐偏差度的取值范围介于$[-1, 1]$。

4.2 推荐偏差度的贝塔分布

贝塔分布是为取之于某有限区间$[a, b]$的随机现象建立模型的有效工具。它是定义在$[a, b]$区间上的连续概率分布，形状的变化取决于贝塔分布的两个参数 p 和 q。本文中定义了随机变量为推荐偏差度的贝塔分布。贝塔分布的一般概率密度函数如式(11)所示。

$$f(x)=\frac{(x-a)^{p-1}(b-x)^{q-1}}{B(p,q)(b-a)^{p+q-1}} \quad a\leqslant x\leqslant b; p, q>0 \tag{11}$$

式中，p, q 是形状参数，a, b 是上下限，其中 $B(p,q)$ 是贝塔函数，其计算方法如式(12)所示。

$$B(p,q)=\int_0^1 t^{p-1}(1-t)^{q-1}\,\mathrm{d}t \tag{12}$$

推荐偏差度的后验分布可以通过融合间接推荐值偏差的先验分布与新的偏差度而获得。通过基于贝叶斯理论的方法，可以及时通过使用新的偏差值来修正推荐信任值偏差的分布，从而对未来的趋势作出预期判断。本文假设每次获得

的间接推荐偏差度有相同的置信度，即 p,q 的和为一个固定值 k，可得如式(13)的关系。

$$d=\frac{p}{p+q};k=p+q \tag{13}$$

因此贝塔分布 p,q 参数计算如式(14)所示。

$$p=dk;q=k-dk \tag{14}$$

式中，d 为推荐信任偏差度。针对两种不同谎言对信任系统产生的不同影响，以及所需的惩罚程度各不相同，本文将两个贝塔分布分别用以区分不同的撒谎行为。

定义 3（偏差度的贝塔分布） 如果 $d>0$，那么偏差度的概率密度函数为 $f_+(x|p^+,q^+)$，如果 $d<0$，那么偏差度的概率密度函数为 $f_-(x|p^-,q^-)$，其中元组对 (p,q) 包含了推荐信任度偏差的所有历史信息。下标+，−区分元组对 (p,q) 是正偏差度 f_+ 还是负偏差度 f_- 的参数。

$$f_+(x|p^+,q^+)=\frac{x^{p^+-1}(1-x)^{q^+-1}}{B(p^+,q^+)}$$

$$0\leqslant x\leqslant 1;p^+,q^+>0 \tag{15}$$

$$f_-(x|p^-,q^-)=\frac{(x+1)^{p^--1}(-x)^{q^--1}}{B(p^-,q^-)}$$

$$-1\leqslant x\leqslant 0;p^-,q^->0 \tag{16}$$

4.3 对间接推荐的信任修正

若节点 i 接收到节点 j 的间接推荐值，通过将所得推荐值与自身观察所得的直接信息相对比则可刻画出节点 j 的间接推荐偏差分布，这时节点 i 需根据分布情况调整对节点 j 的间接推荐的信任程度，以减少今后偏差过大的推荐信任对信任模型建立正确的信任评价的不良影响，这个过程即为对间接推荐的信任修正。

对间接推荐的信任修正方法是基于贝叶斯决策理论，如果要根据推荐偏差的后验分布修正对推荐的信任程度，则需要以下三要素：

• 状态集：信任偏差 d 的偏差范围，介于[1,−1]之间，如果 $d>0$，则 d 的概率密度函数为 $f_+(d|p^+,q^+)$；如果 $d<0$，则 d 的概率密度函数为 $f_-(d|p^-,q^-)$。

• 行为集：对推荐信任度的信任程度在[0,1]之间。0 表示完全不信任，1 表示完全信任。

• 损失函数 $L(t,d,a)$：如式(17)、式(18)，用于计算当信任偏差度为 d、所观测到的真实信任度为 t、对推荐信任的信任度为 a 时所可能造成的损失。

$$L_+(t,d,a)=(g(a,(t+d))-t)^2 \quad d\geqslant 0 \tag{17}$$

$$L_-(t,d,a)=\theta(g(a,(t-d))-t)^2 \quad d<0 \tag{18}$$

式中，$g(.)$ 表示已知间接推荐值和对推荐信任的信任度前提下得到的信任值的函数。L_+ 表示虚假赞扬时的损失函数，L_- 表示诽谤行为的损失函数。在已知行为集、状态集、损失函数的前提下，对间接推荐信任度的修正就是找到一个推荐信任的信任度 a 使得损失函数期望最小。a_+ 和 a_- 分别代表了从最小化损失期望函数 $\varphi_+(a)$ 和 $\varphi_-(a)$ 得到的值，其中 θ 表示偏差度。

$$\varphi_+(a)=\int L_+(t,\theta,a)f_+(\theta\mid p^+,q^+)\mathrm{d}\theta \quad \theta\geqslant 0 \tag{19}$$

$$\varphi_-(a)=\int L_-(t,\theta,a)f_-(\theta\mid p^-,q^-)\mathrm{d}\theta \quad \theta<0 \tag{20}$$

最后依据式(21)，综合考量 a_+ 和 a_- 完成最终的对推荐信任的信任度的修正。

$$\begin{cases} a_+, & \text{if } \dfrac{p^++q^+}{p^-+q^-}\geqslant r \\ a_-, & \text{if } \dfrac{p^-+q^-}{p^++q^+}\geqslant r \\ \dfrac{(p^-+q^-)a_-+(p^++q^+)a_+}{p^-+q^-+p^++q^+}, & \text{else} \end{cases} \tag{21}$$

5 性能评价

OTMF 模型通过性能分析表现出对偏见式攻击具有一定的防御能力，但是前提是系统中所提供的间接信息（二手信息）是真实可信的。OTMF 没有考虑恶意节点提供虚假间接信息对信任模型作出正确信任评价的影响。RTM 针对 OTMF 的弱点以及源路由协议的特性提出了改进措施。模拟实验中采用小世界网络模拟 Ad hoc 网络拓扑结构：节点的总个数为 50，大部分节点邻接节点数目较少，少数节点有大量邻接节点，平均入度为 5。

5.1 抵御虚假推荐攻击性能比较

在模拟环境中，不可信任节点可以对其他节点作出真实或虚假的推荐。为了能够反映模型对各种虚假推荐攻击的抵御能力，我们对不可信任节点做如下分类：1）独立型，不可信任节点之间彼此互不了解，对所有节点都提供坏的间接推荐；2）协作性，不可信任节点彼此相互了解，对同盟者给出高评，而对非同盟者给低评；3）随机型，不可信任节点对所有节点提供随机高评或恶评。虚假推荐攻击策略如表 1 所列。

表 1 模拟中环境参数及行为策略

	Parameter	Value
正常节点比率	网络中节点总数	50
节点类型	10～90%	
	不可信节点比率	0～80%
	恶意节点比率	0～10%
	推荐偏差度	0.5,0.9
行为策略	正常节点：提供可靠传递并提供可靠间接推荐 不可信节点：分为三类独立型、协作性、随机型（具体行为见上文） 恶意节点：拒绝提供可靠传递，并对正常节点提供低评，对恶意节点提供好评	

为了评价系统的性能，引入了一种评价标准信任评估正确率 $P_{correct}$。假设 ρ_{ij} 表示通过 RTM 计算出的节点 i 认为节点 j 进行可靠传递信任度，μ_j 表示节点 j 在实际工作中可靠传递的频率。M_i 表示节点 i 计算了可靠传递信任度的所有节点的集合。$P^i_{correct}$ 表示节点 i 的信任评估正确率，如式(22)所示。

$$P^i_{correct}=\frac{\sum_{j\in M_i}(1-\frac{|\rho_{ij}-\mu_j|}{\mu_j})}{|M_i|} \tag{22}$$

$P_{correct}$ 为整个系统的信任评价正确率：

$$P_{correct}=\frac{\sum_{i\in N}P^i_{correct}}{|N|} \tag{23}$$

图 2 显示了该机制在 5 种攻击模式下，不可信节点的数目由 0%到 80%时，信任模型信任评价正确率的变化情况。从图 2 中可以看出在 OTMF 模型下基本不具备对虚假推荐的抵御能力，随着不可信节点的增加，系统中因无法识别不可信节点，导致系统信任评估正确率急剧下降。而在 RTM 中，由于采用了从非邻接节点获取直接信息的机制，并且启用了对间接推荐节点的信任修正机制，使得恶意推荐的影响尽量最小化。当然在不可信节点急剧增加并且采用了联合攻击机

制后，信任评价的正确率也会受到一定影响。

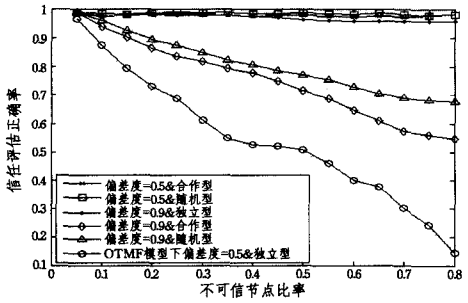

图 2　不可信节点比率 vs. 信任评估正确率

5.2　收敛性比较

由于 OTMF 模型采用了间接推荐的机制，因此信任度收敛速度比一般信任模型已经有了较大的提高，但 OTMF 模型的收敛速度是在没有考虑虚假推荐攻击下的。图 3 反映了在不可信节点占 10%，虚假推荐偏差度不超过 0.5，采用随机型的虚假攻击方式下，OTMF 模型和 RTM 之间在收敛性能上的差异。

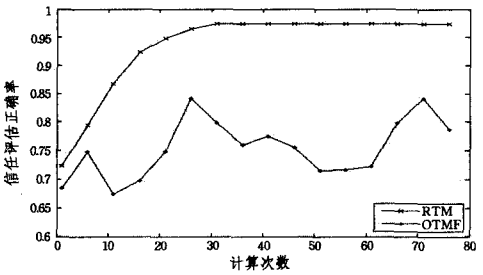

图 3　计算次数 vs. 信任评估正确率

由于 RTM 具备对不可信节点的识别能力，在有限次信息交互后，对不可信节点的间接推荐基本采取极低信任度，即不可信节点的间接推荐将对模型的信任值不会产生影响，因此在该模型下信任评估会逐步达到稳定的状态。而 OTMF 不具备对不可信节点的识别能力，所以系统的评估正确率不会随着间接推荐的增加而趋于稳定，而会随着不可信节点的随机攻击性而出现不稳定的状态，基本信任评估正确率在[0.65，0.85]区间徘徊。

结束语　针对 Ad hoc 网络中源路由的特性，在 OTMF 模型基础之上提出的鲁棒信任机制(RTM)提升了对虚假推荐的抵御能力并且加快了信任值的收敛速度。但通过性能分析表明，该系统在恶意节点和不可信节点协作攻击下，系统的评估正确率有待进一步提高，这些将是我们今后研究工作的重点。

参 考 文 献

[1]　孙玉星，黄松华，等. 自治网络中信任/信誉模型的安全现状的研究[J]. 计算机科学，2009，36(4)：5

[2]　Li Ruidong，Li Jie，Liu Peng，et al. An Objective Trust Management Framework for Mobile Ad hoc Networks[C]// Vehicular Technology Conference，VTC 007-Spring. April 2007：56-60

[3]　Theodorakpoulos G，Baras J S. On Trust models and trust evaluation metrics for ad-hoc networks [J]. IEEE Journal on Selected Areas in Communications，2006，24(2)：318-328

[4]　Theodorakpoulos G. Distributed trust evaluation in ad-hoc networks[D]. Maryland：University of Maryland，2004

[5]　Jiang Tao，Baras J S. Trust Evaluation in Anarchy：A Case Study on Autonomous Networks [C]// Proceedings of the 25th Conference on Computer Communications. Barcelona，Spain，April 2006

[6]　Buchegger S，Le Boudec J-Y. A Robust Reputation System for P2P and Mobile Ad-hoc Networks[C]// Proceedings of P2PEcon 2004. Harvard University，Cambridge MA，U. S. A. http：// www. sonja. ws/robust. pdf

[7]　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，2006，249(2)：674-679

[8]　Lamsal. Understanding trust and security[J/OL]. http：//www. cs. helsinki. FI/u/lamsal/papers/

[9]　Marti S，Giuli T J，Lai K. Mitigating routing misbehavior in mobile ad hoc networks[C]// Proceedings of the 6th annual international conference on Mobile computing and networking. Boston，Massachusetts，United States，2000：255-265

[10]　Sun Yu-xing，Huang Song-Hua，et al. Bayesian Decision-Making Based Recommendation Trust Revision Model in Ad hoc Networks [J]. 软件学报，2009，20(9)：2574

(上接第 14 页)

[64]　Ohno A，Murao H. Measuring Source Code Similarity Using Reference Vectors[J]. Proceedings of International Conference on Innovative Computing，Information and Control (ICICIC' 06)，2006，2(30-01)：92-95

[65]　Mann S，Frew Z. Similarity and originality in code：Plagiarism and normal variation in student assignment[C]// Proceedings of the 8th Australian conference on computing education. 2006，52：37-58

[66]　Ji J H，Park S-H，Woo G，et al. Source code similarity detection using adaptive local alignment of keywords[C]// Proceedings of 8th International Conference on Parallel and Distributed Computing，Applications and Technologies. 2007：179-180

[67]　Cosma G，Joy M. Towards a definition of source-code plagiarism [C]// Proceedings of IEEE Transactions on Education. 2008，51：195-200

[68]　Fowler M，Beck K，Brant J，et al. Refactoring：Improving the Design of Existing Code [M]：63

[69]　Gamma E，Helm R，Johnson R，et al. Design patterns：Elements of reusable object-oriented software[M]. Addison-wesley，1997