移动自组网中基于推荐的信任模型

谭长庚,李 江
(中南大学 信息科学与工程学院,湖南 长沙 410083)

摘 要:作为对基于密码体系的安全手段的重要补充,信任管理对移动自组网的可靠运行和安全保障具有重要意义。由于节点间信任关系的建立有赖于第三方节点的推荐信息,节点的虚假推荐和不推荐行为是信任管理机制必须解决的问题。以移动自组网中信任管理为研究背景,提出一种基于推荐的信任模型,引入时间帧进行信任值合成计算,用推荐信任度来评价节点的推荐行为,可以有效解决恶意节点和自私节点的虚假推荐行为,以及自私节点的不推荐行为,同时提高了信任模型的动态适应能力。理论分析和仿真结果进一步验证了模型的合理性和可行性。

关键词:信任模型;虚假推荐;不推荐;推荐信任值
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)11-0068-04

Trust Model Based on Recommendation in Mobile Ad Hoc Networks

TAN Chang-geng, LI Jiang
(College of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: As an important supplement to cryptography based security solutions, trust management plays an important role in security and reliability of mobile ad hoc networks. However it can be cheated by the propagation of rumor produced by malicious or selfish node for using second-hand observation. Taking trust management as the background in mobile ad hoc networks, present a trust model based on recommendation mechanisms, provide a concrete and reasonable formula of trust value by the use of time-frame, and evaluate the recommender's feedback by the recommendation trust value. Our reputation mechanism shows effectiveness in distinguishing false recommendation of malicious and selfish node, and no-recommendation of selfish node, and it can evaluate the trust relationships between nodes more precisely. Through the theoretical analysis and simulated experiments, the rationality and the feasibility of this trust model is further confirmed.

Key words: trust model; false recommendation; no-recommendation; recommendation trust value

0 引 言

作为一种新型网络,移动自组网不仅具有传统网络包转发、链路交换的特点,而且通过引入移动通信的特性,极大延伸了计算机网络的应用领域。然而,这些特点同时也为移动自组网络体系结构的不同层面带来新的问题,使作为移动自组网络通讯管理核心的路由协议面临更为复杂的安全问题,并由此成为移动自组网络研究的重点[1-3]。

对移动自组网按需路由发现机制中节点的路由协作行为进行详细分析,可以看出作为相对独立实体间的协作行为,信任是整个路由协作行为的基础。在基于信任的移动自组网中,节点不仅根据自己与被评价节点的直接交互记录计算直接信任值,还可以通过第三方节点的推荐得到关于被评价节点的间接信任值[4-6]。使用间接信任值可以充分利用每个节点的信任记录,加速确定节点间的信任关系,从而更有效地检测不良节点。由于节点间信任关系的建立有赖于第三方节点的推荐,恶意节点为达到某种目的会在网络中散布虚假推荐信息[7],如果节点依据自身信任值以及被评价节点的信任值动态地对其他节点进行欺骗,或是与其他不良节点进行合谋攻击,这种行为将很难进行检测;另一方面,自私节点可能恶意提高其他节点的信任值,从而避免自身加入到路由或转发包等过程中去;另外,自私节点为节省自身能耗,只从其他节点处获取推荐信息而不愿为其他节点提供推荐服务,且出于同样原因,自私节点可以策略性改变自己的行为,从

收稿日期:2009-03-27;**修回日期**:2009-06-27
基金项目:国家自然科学基金(60673164);教育部博士点基金(20060533057)
作者简介:谭长庚(1963-),男,博士,副教授,CCF会员,研究方向为移动自组网的路由协议和性能评价。

而使其难以检测。

文中提出一种基于时间帧的信任值计算方法,用推荐信任值评价节点的推荐行为,提出低开销的邻居共享机制用于节点间交换信息,既可以解决节点策略性的虚假推荐和不推荐行为,又能够激励节点诚实推荐,同时对虚假推荐行为进行必要惩罚。

1　基于推荐的信任模型

假设节点总是信任自身,网络中多数节点是好的,且好节点偶尔的不良行为不会频繁发生。节点间信任关系的建立采用两种方式,一是节点在本地获取的关于被评价节点的信任信息,称为直接信任值;二是来自第三方节点的关于被评价节点信任信息的合成,称为间接信任值。推荐信任值属于直接信任值的一种特殊形式,用于描述一个节点对其他节点能否诚实提供推荐信息的主观性预测。

1.1　信任值描述与量化

Diego Gambetta 认为信任是主体对客体特定行为的主观可能性预测,取决于经验并随着客体行为的变化而不断修正[8]。主观判断具有主观性、不确定性和模糊性,文献[9]用信息论中熵的概念对实体的主观可能性进行定量描述,即

$$T\{p\} = \begin{cases} 1 - H(p), 0.5 \leqslant p \leqslant 1 \\ H(p) - 1, 0 \leqslant p < 0.5 \end{cases} \tag{1}$$

其中 T 表示主体对客体特定行为的信任程度,p 表示客体发生该行为的可能性,H 为熵函数:

$$H(p) = -p\log_2^p - (1-p)\log_2^{1-p}$$

为了提高信任评估的准确性和动态适应能力,把一段时间分为若干个时间帧。通常近期发生的交互行为具有更高的参考价值,因此为了减少信任值评价的时空开销,引入滑动窗口 W,滑动窗口大小是时间帧的整数倍。只有发生在滑动窗口内的交互行为才参与信任值的计算,且过期的交互行为将从滑动窗口中剔除。

1.1.1　直接信任值

若时间帧 t 内节点 subject 和节点 agent 有直接交互行为 action,用{subject: agent, action, trust_ value, t}记录此次交互行为,存储在直接信任值表中,trust_ value 标记交互成功与否。

设在第 i 时间帧内,节点 subject 与节点 agent 关于 action 行为交互成功 k_i 次,失败 j_i 次。假定在第 I 时间帧内节点 subject 需要计算节点 agent 关于 action 行为的直接信任值 $T^{\text{direct}}_{\{\text{subject:agent,action}\}}$,首先依据直接信任值表中的交互记录,由公式(2)计算客体发生该行为的可能性,然后由公式(1)计算直接信任值:

$$p = \frac{1 + \sum_{i=1}^{I} \beta_1^{-t_i} k_i}{2 + \sum_{i=1}^{I} (\beta_1^{-t_i} k_i + \beta_2^{-t_i} j_i)} \tag{2}$$

基于以下考虑引入时间消逝因子 β_1 和 β_2:

(1)通常近期发生的行为具有更高参考价值,因此应当弱化以往发生的交互行为对直接信任值的影响,同时加大近期行为在信任值合成中的比重。

(2)节点经一段时间积累了较好的信任值,但少数几次攻击行为就会使它的形象大打折扣,也就是说与好的行为相比,节点的攻击行为应该被淡忘的慢些,于是设定 $\beta_1 < \beta_2$。

1.1.2　间接信任值

间接信任值是通过节点间共享本地的直接信任值信息建立的,因此需要考虑以下问题:

(1)节点何时需要发起推荐请求?假设节点总是信任自身的,通常可以根据本地存储的信任值确定待评价节点是否可信,只有当本地节点没有存储待评价节点的信任值,或是存储的信任值不足以判定待评价节点是否可信时,节点才发起推荐请求。

(2)第三方节点如何确定?首先,推荐链路越长,虚假推荐的可能性就越大;即便推荐链路上不存在虚假推荐,由于信任是随推荐链路的延长而递减的,由此反馈来的推荐信息可参考性并不强,反而增加了系统开销。其次,直接信任值高的节点并不意味着它的推荐信息就值得信赖,毕竟推荐行为只是网络实体诸多行为中的一种。用推荐信任度来表示主体对客体推荐行为的可信程度,由此,本地节点只从其邻居节点中具有较高推荐信任度的节点那里获取推荐信息。

(3)如何合成间接信任值?节点可以从一个或多个邻居节点处获得推荐信息,前者称为单路推荐,后者称为多路推荐。用 $R_{\text{subject:recommender}}$ 表示节点 subject 对节点 recommender 的推荐信任值,用 $T^{\text{indirect}}_{\{\text{subject:agent,action}\}}$ 表示节点 subject 对节点 agent 关于行为 action 的间接信任值。

对于图 1 所示的单路推荐,采用公式(3)计算间接信任值:

$$T^{\text{indirect}}_{\{A:C,\text{action}\}} = R_{A:B} \cdot T^{\text{direct}}_{\{B:C,\text{action}\}} \tag{3}$$

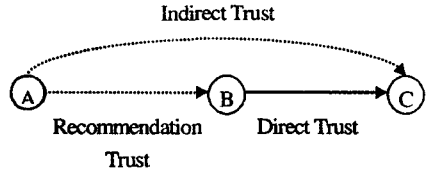

图 1　单路推荐

对于图 2 所示的多路推荐,采用公式(4)计算间接信任值:

$$T^{indirect}_{\{A:C,action\}} = w_1(R_{A:B} \cdot T^{direct}_{\{B:C,action\}}) + w_2(R_{A:D} \cdot T^{direct}_{\{D:C,action\}}) \quad (4)$$

其中 $w_1 = \frac{R_{A:B}}{R_{A:B} + R_{A:D}}, w_2 = \frac{R_{A:D}}{R_{A:B} + R_{A:D}}$

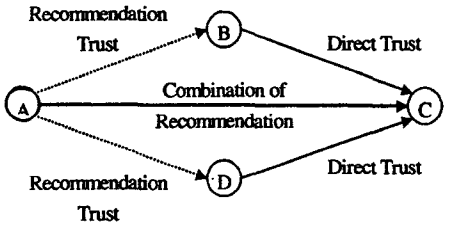

图 2 多路推荐

1.1.3 推荐信任值

当节点 recommender 接收到由节点 subject 发来的推荐请求后，首先将该推荐请求写入推荐请求信息表，然后依据直接信任值表计算待评价节点的信任值，并反馈给节点 subject。

假设在时间帧 t 内节点 subject 收到由节点 recommender 反馈来的关于被评价节点 agent 的信任值信息，用{recommender:agent,action, trust_ value,t}记录此条推荐信息并记录在推荐反馈信息表中。节点 subject 根据推荐反馈信息表中的信息，用公式(3)或(4)计算间接信任值，进而与直接信任值合成。在节点 subject 与节点 agent 建立信任关系并直接进行交互后，首先将此次交互行为写进直接信任值信息表，然后将推荐反馈信息表中的推荐信息和节点 subject 观察到的直接信任值进行偏离测试：

$$| T^{direct}_{\{subject:agent,action\}} - trust\_value | \leqslant \eta \quad (5)$$

如果偏离测试成功，则认为节点 recommender 的推荐诚实可靠，否则认为其进行虚假推荐。最后节点 subject 将此次推荐行为写进推荐信任值表：{subject: recommender, trust_ value,t}，trust_ value 标记此次推荐是否诚实，表的长度同样为滑动窗口的大小。

和直接信任值一样，用公式(1)和(2)计算推荐信任值。

1.2 基于推荐的信任模型

信任模型由四个模块组成：邻居监控、信息共享、信任评估与决策制定以及路由管理。邻居监控模块使用看门狗机制；信息共享模块主要包括初始化推荐请求信息 RREC、中间节点转发 RREC、目的节点回复 RRFB 以及源节点处理 RRFB；依据监控模块传递过来的监控结果和信息共享模块获得的关于待评价节点的推荐信息，信任评估与决策制定模块依据不同的事件即时计算信任值并作出相应决策；路由管理模块包括路由建立、选择及路由维护，这三个部分都是动态性、按需性的操作。

1.2.1 初始化推荐请求信息 RREC

当节点 A 无法依据直接信任值表确定某待评价节点集合是否可信时，首先查看推荐反馈信息表，对于有关该待评价节点集合的每条推荐信息，节点 A 需要计算该推荐信息的提供者的推荐信任值，若可信，则使用此条推荐信息，否则删除该记录。若无法依据推荐信息缓存表确定待评价节点集合中部分或是全部节点是否可信，则将待发送到数据包写入发送缓存，同时写入缓存的还有尚无法确定可信度的节点集合 U，然后设定一个计时器，并初始化推荐请求信息 RREC。RREC 信息包的格式如下：

{pktType; requestID; subject; U; action; Z; Max_ Hop; transmit - path}

其中 pktType 表示包的类型，即 RREC；requestID 表示包的序列号；subject 表示发起该推荐请求的节点；U 表示待评价节点集合；action 表示待评价的节点的行为类型；Z 为 subject 确定的第三方节点集合；Max_ Hop 表示传输跳数，初始为允许的最大传输跳数；transmit - path 用于记录推荐请求的转发路径。

节点 A 初始化 RREC 信息后，采取洪泛的方式将推荐请求信息发送给它的邻居节点。

1.2.2 中间节点转发 RREC

中间节点 X 接收到 RREC 信息后，首先确认自己此前是否收到过该 RREC 信息，若已经收到过，则不予处理；否则将此信息写入推荐请求信息表中，然后判断 X 是否出现在集合 Z 中。若 X 不属于集合 Z，则 Max_ Hop 减 1，把 X 网络地址加入到 transmit - path 中，然后将 RREC 转发至自己的邻居节点；如果 X 属于集合 Z，则对源节点 A 的推荐信任度进行评价，若不可信，则不对此请求信息进行处理；若节点 A 的推荐信任度可信，则节点 X 依据其直接信任值表即时计算集合 U 中每个节点的直接信任值，如果节点 X 至今没有与集合 U 中某节点 u 直接交互过，则将其信任值标记为 UNKNOW，之后节点 X 进行两个操作：一是继续转发 RREC 至自己的邻居节点；二是初始化推荐反馈信息包 RRFB 并转发给节点 A。RRFB 信息包的格式如下：

{pktType; recommender; subject; rcmResult; action; Max_ Hop; transmit - path}

其中 pktType 表示包的类型，即 RRFB；recommender 表示推荐者；rcmResult 为推荐者反馈的信任值。

1.2.3 源节点处理 RRFB

源节点接收到 RRFB 包后，将其写入推荐信息缓存表，以供信任评估与决策制定模块使用。

1.3 有效性分析

(1)直接信任值和推荐信任值分开存储，只有进行

诚实推荐的节点才能获得较高的推荐信任值。

(2)推荐信任值既可以为本地节点确定第三方节点提供依据,同时作为权值参与间接信任值的合成。如果节点的推荐信任值并不是算高,那么它对合成的间接信任值不会有太大影响。

(3)节点收到邻居节点发送来的推荐请求后,首先计算该邻居节点的推荐信任度,若不可信,则不对该推荐请求进行响应。这样既是对节点的虚假推荐行为的惩罚,同时激励节点诚实推荐。

(4)对于节点的不推荐行为,可以扩大第三方节点的范围,方法是将出现在推荐请求信息表中但没有出现在推荐信任值表或推荐反馈信息表中的节点加入到第三方节点集合中。如果没有收到某节点反馈来的推荐信息,则重传推荐请求,并设置最大重传次数,如果已达到最大重传次数但仍未收到某节点的推荐信息,则认为该节点进行不推荐行为。

2　仿真分析

本节设置三个场景来验证信任模型的可靠性和可行性。

(1)部署 100 个节点,包含若干比例进行虚假推荐和不推荐行为的节点。由图 3 可以看出,虽然随着比例的增加,在使用和不使用信任的情况下,包成 功接收率都有明显下降,但与后者相比,前者对网络性能的改善是显而易见的。因为引入信任值可以更准确地评价节点行为,更快地构建信任关系。

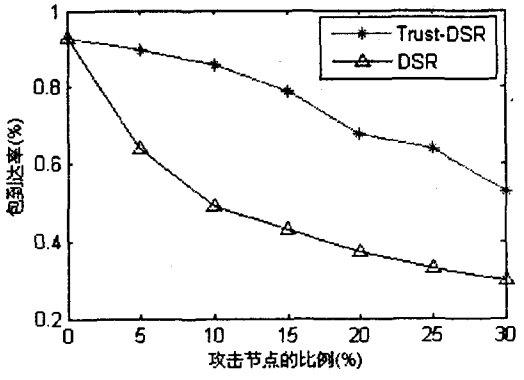

图 3　使用与不使用推荐情况下的包接收率

(2)部署 100 个节点,包含 20 个进行虚假推荐的节点组和 10 个进行不推荐行为的节点组 S,用于分析模型对不推荐行为的检测情况。将其他节点对 S 组节点的平均推荐信任值作为考量标准。实验分两次进行,一次是 S 组节点由始至终进行不推荐行为;一次是 S 组节点在 100 秒后开始进行诚实推荐。由图 4 可以看出,如果 S 组节点诚实推荐,其平均推荐信任值大体上是逐渐提高的;但在不推荐情况下,其平均推荐信任值是一直下滑的。

(3)部署 100 个节点,用分组 G1 表示 20 个进行虚假推荐的节点集合,用分组 G2 表示 20 个进行诚实推荐的节点集合。该场景用于分析模型对节点虚假推荐行为的检测情况,同样用节点组的平均推荐信任值进行考量。设定从 100 秒开始,G1 组节点进行诚实推荐,而 G2 组节点转为虚假推荐。由图 5 可以看出,G1 组节点的平均推荐信任值在 300 秒处已经有很好改善,但 G2 组节点的平均推荐信任值已经在初始信任度以下。

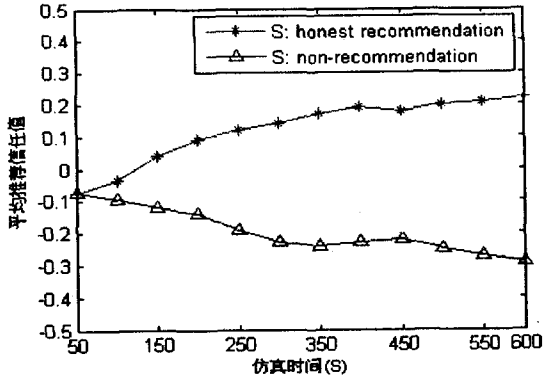

图 4　诚实推荐与不推荐情况下的平均推荐信任值

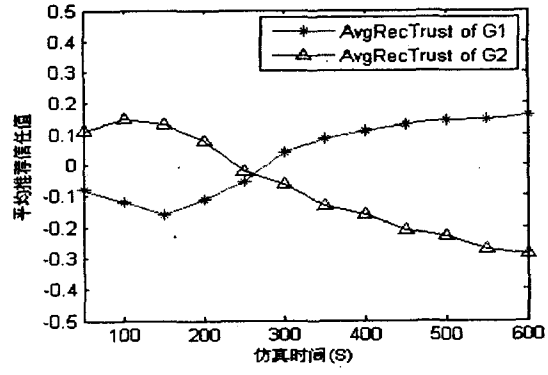

图 5　策略性攻击情况下的平均推荐信任值

3　结束语

基于移动自组网中信任机制本身存在的安全问题,文中提出一种基于推荐的信任模型,采用时间帧优化信任值计算,用推荐信任值评价节点的推荐行为,提高了模型的动态适应能力,同时有效解决了虚假推荐和不推荐行为。理论分析和仿真结果进一步验证了模型的合理性和可行性。

参考文献:

[1]　臧婉瑜,于　勐,谢　立,等.按需式 Ad Hoc 移动网络路由协议的研究进展[J].计算机学报,2002,25(10):1009-1017.

(下转第 75 页)

对于 QoS 组件的 QoS 管理功能的设计可以采用传统的 QoS 管理框架设计方法,可以根据响应时间、可靠性、吞吐量等具体的侧重不同制定相应的 QoS 模型。QoS 信息的采集可以采用基于 JAX-RPC 和 JAX-WS 规范所提供的"截取器"(handler)机制。在 QoS 信息存储方面,由于删除和修改操作很少,可以采用普通文件加索引的方式存储[11,12]。一般而言,BPEL 流程的执行效率是最重要的,因此,QoS 算法可以根据响应时间和吞吐量为依据设计。QoS 管理功能可以作为独立的模块来进行设计,它的改变不会影响 Web 服务动态组合和 BPEL 流程的执行,使 QoS 组件易于扩展。

3　结束语

动态 Web 服务组合是 Web 服务领域中一个重要发展方向。结合 BPEL 和 UDDI 提出了一种基于 QoS 组件的 Web 服务组合新框架,该框架具有在业务流程运行阶段动态绑定和选择 Web 服务的能力,具有很好的可扩展性和可恢复性,并增强了 Web 服务的业务组合能力。为增强该架构的实用性,将进一步研究业务流程的安全、业务流程模板中的服务粒度划分等问题。另外,对于动态绑定的策略和 Web 服务的替换策略的研究也是今后工作的重点。

参考文献:

[1] Modafferi S, Mussi E, Maurino A, et al. A Framework for Provisioning of Complex e-Services[C]//Services Computing, 2004 IEEE International Confernce on (SCC'04). Shanghai, China: IEEE Computer Society Press, 2004: 81-90.

[2] Supadulchai P, Aagesen F A. A Framework for Dynamic Service Composition[C]//First International IEEE WoWMoM Workshop on Autonomic Communications and Computing (ACC'05). Taormina, Italy: IEEE Computer Society Press, 2005: 527-531.

[3] Takemoto M, Oh-ishi T, Iwata T, et al. A Service-Composition and Service-Emergence Framework for Ubiquitous-Computing Environments[C]//Symposium on Applications and the Internet-Workshops (SAINT 2004 Workshops). Tokyo, Japan: IEEE Computer Society Press, 2004.

[4] Piccinelli G, Zirpins C, Lamersdorf W. The FRESCO Framework: An Overview[C]//Symposium on Applications and the Internet Workshops (SAINT 2003 Workshops). Florida, USA: IEEE Computer Society Press, 2003.

[5] Zeng L, QoS-aware middleware for Web services composition [J]. IEEE Transactions on Software Engineering, 2004, 30(5): 311-327.

[6] 马　骞,虞建杰,马晓星,等.一种基于运行时体系结构的 BPEL 支撑环境[J].电子学报,2006,34(12A):2361-2365.

[7] 杨　鑫,陈俊亮.WSC/ADL:Web Services 组合系统体系结构描述语言[J].软件学报,2006,17(5):1182-1194.

[8] 赵俊峰,谢　冰,张　路,等.一种支持领域特性的 Web 服务组装方法[J].计算机学报,2005,28(4):731-738.

[9] 陈彦萍,李增智,郭志胜,等.Web 服务组合中基于服务质量的服务选择算法[J].西安交通大学学报,2006(8):897-900.

[10] 陈彦萍,李增智,郭志胜,等.一种满足马尔可夫性质的不完全信息下的 Web 服务组合方法[J].计算机学报,2006,29(7):1076-1083.

[11] 邵凌霜,李　田,赵俊峰,等.一种可扩展的 Web services QoS 管理框架[J].计算机学报,2008,31(8):1458-1470.

[12] 王　莉,刘厚泉,吴雪峰.基于 BPEL 的业务流程管理系统架构的研究与应用[J].计算机工程与设计,2006,27(18):3507-3510.

(上接第 71 页)

[2] 李金鹏,吕光宏,王立平,等.移动 Ad hoc 网络安全路由协议研究[J].计算机技术与发展,2008,18(7):24-28.

[3] 刘志远,杨植超.Ad hoc 网络及其安全性分析[J].计算机技术与发展,2006,16(1):231-233.

[4] Buchegger S, Le J Y, Boudec J L. Performance analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in distributed Ad-hoc networks[C]// Proc of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC2002). EPFL Lausanne, Switzerland: [s. n.], 2002: 226-236.

[5] 洪　亮,洪　帆,张明猛,等.移动 Ad hoc 网络中一种信任评估模型[J].计算机科学,2006,33(7):31-33.

[6] 谭长庚,陈松乔,王建新.移动自组网中一种优化的局部声誉系统[J].计算机工程与应用,2008,44(9):20-23.

[7] Buchegger S, Boudec J L. Coping with False Accusations in Misbehavior Reputation Systems for Mobile Ad-Hoc Networks[R]. EPFL tech. rep, 2003.

[8] Gambetta D. Can we trust trust[M]. Trust: Making and breaking cooperative relations, electronic edition. Oxford: University of Oxford, 1988: 213-237.

[9] Sun Y. A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense against Attacks[C]// Proc of the 25th IEEE International Conference on Computer Communications (INFOCOM 2006). Barcelona, Spain: [s. n.], 2006: 1-13.