基于自适应遗忘机制的半环信任模型

喻 莉 李静茹* 刘祖浩
(华中科技大学电子与信息工程系 武汉 430074)

摘 要：半环代数由于可以很好地描述可信度计算规则问题，因此可用来计算节点间的可信度，而目前存在的半环信任模型并未定义基于时间的动态变化问题。该文提出了一种基于自适应遗忘机制的半环信任模型，刻画信任的动态性，并改进已有的半环信任模型，弥补了其未定义动态变化问题的缺陷。仿真结果表明，这种基于自适应遗忘机制的半环信任模型有效分辨正常节点和异常节点，并抵御开关攻击，从而可有效提高网络的安全性。

关键词：Ad hoc；信任模型；半环；遗忘机制；自适应
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2011)01-0175-05
DOI: 10.3724/SP.J.1146.2010.00221

Semiring Trust Model Based on Adaptive Forgetting Scheme

Yu Li Li Jing-ru Liu Zu-hao
(*Department of Electronics and Information Engineering,*
Huazhong University of Science and Technology, Wuhan 430074, *China*)

Abstract: Semiring algebra can be used to compute the trustworthiness between nodes, for it is a good description of the trustworthiness calculation rules issues. However, the existing semiring trust model does not define dynamic issues based on time. A semiring trust model based on the adaptive forgetting scheme is proposed to describe the dynamic of trust, and improve the existing semiring trust model, making up for its shortcoming of not defining dynamic issues. Simulation results show that proposed trust model distinguishes effectively between normal nodes and malicious nodes and resists on-off attacks, which improves the security of Ad hoc networks.

Key words: Ad hoc; Trust model; Semiring; Forgetting scheme; Adaptive

1 引言

由于Ad hoc网络缺乏中间服务器，因此网络中各个节点需要相互协作来实现网络功能。而节点间的协作十分脆弱，极容易被自私节点和恶意攻击等因素破坏，这造成了Ad hoc网络较差的安全性。因而，研究适用于Ad hoc网络的安全策略变得十分迫切。目前，将信任概念引入路由的可信路由机制是一种适用于Ad hoc网络的重要安全策略，因为这是一种分布式安全评价方法，非常适应于Ad hoc这种复杂环境，具有很强的鲁棒性。

近年来，国内外对信任机制的研究已取得许多进展。文献[1]基于beta函数计算直接信任，并运用一定模型计算间接信任，从而抵御各种恶意攻击。文献[2]采用贝叶斯方法，融合一手信息和二手信息，建立信誉系统，从而实现Ad hoc网络的自律。文献[3]还提出了一种基于熵(entropy)理论的信任模型。另外，文献[4]采用基于模糊逻辑的方法在Grid网络中建立了信任模型。

但是，这些模型都没有对可信度(信任的定量表示)计算规则给出明确说明。文献[5]提出了一种基于半环(semiring)代数理论的信任模型，它能很好地描述可信度计算规则，且可以很灵活地表示其他信任模型，因而成为目前一种非常重要的信任模型。文献[5]提出的半环信任模型适用于Ad hoc网络，他们之后出现了多种适用于其他情形的半环模型，这些半环模型大都以文献[5]的模型为基础。文献[6]运用文献[5]中的扩展Dijkstra算法，提出了信任路径搜索算法，建立了用于隐私保护的半环信任模型。但是文献[5]的半环信任模型仍然存在一些不足，比如它没有对基于时间的动态变化问题给出定义和描述。而Ad hoc网络的典型特点之一就是它的动态性，具体体现在，网络中的节点可以随处移动，也可以随时开机和关机。这样，网络的拓扑结构随时发生变化，从而引起节点间链路的变化(如链路的建立、取消等)，而节点的信任是通过节点间的链

2010-03-11 收到，2010-09-02 改回
国家 863 计划项目(2009AA01Z205)，国家实验室基金(P080010)和新世纪优秀人才计划(NCET070339)资助课题
*通信作者：李静茹 lijingru221@gmail.com

路进行传播和计算的，这样节点的信任也将随着拓扑结构的变化而具有动态变化性。因此，从客观的角度上，计算节点可信度的信任模型需要反映这种动态性，对节点行为的变化给予及时反映，提高自适应性。

另外，文献[5]仅仅考虑了简单的节点行为，而未考虑较为复杂的攻击行为，如开关攻击、矛盾行为攻击等[1]。其中，进行开关攻击的恶意节点交替性地表现正常或异常，并且希望在对网络造成危害时不被检测到[1]。这种攻击对网络的损害是多方面的，比如降低QoS或提供虚假反馈等[7]。它需要由网络的自适应机制来克服[8]。而文献[5]的半环信任模型并不具备自适应机制，因而不能有效地克服开关攻击。

刻画动态性最常用的方法是引入遗忘因子[1]。本文将遗忘机制引入到传统的半环信任模型中，提出了一种基于自适应遗忘机制的半环信任模型，实时计算节点可信度，抵御开关攻击，从而提高异常行为监测能力和动态适应能力，增强Ad hoc网络的安全性。

2 信任的概念及计算

信任(trust)是一个节点基于对另一节点行为直接或间接的观察而托付它完成一项特定任务的相信程度[9]。这里将前一节点称作主节点，后一节点称作客节点。本文采用贝叶斯框架[10]来描述节点的信任。

可信度(trustworthiness)是信任的定量表示。根据节点对象，可信度可分为直接可信度和间接可信度。直接可信度是邻居节点间的可信度，通过对邻居节点的直接观察计算得到；而间接可信度是非邻居节点间的可信度，需要通过某种信任模型计算得到，本文中的半环信任模型就可以用来计算间接可信度。本文中，可信度(用 T 表示)用一个数值对 (t,c) 来刻画。其中，t 是信任值，表示主节点对客节点完成某项特定行为的信任估计，c 是置信值，刻画所计算信任值的精确性，二者计算如下[10]：

$$t=\mu(a,b)=\frac{a}{a+b} \tag{1}$$

$$c=1-\sqrt{12}\sigma(a,b)=1-\sqrt{\frac{12ab}{(a+b)^2(a+b+1)}} \tag{2}$$

其中 a 和 b 分别表示正常行为次数和异常行为次数，且 $t,c\in[0,1]$，故可信度空间为 $T=[0,1]\times[0,1]$。

3 基于自适应遗忘机制的半环信任模型

3.1 半环信任模型

3.1.1 半环 半环是一种代数结构 $(S,\oplus,\otimes)$，其中 S 是一个集合，$\oplus,\otimes$ 是是定义在 S 上的二元运算，且有以下性质。$\oplus$ 算子服从交换律、结合律，且存在一个中性元素 $0\in S$ (即 $\forall a\in S,a\oplus 0=a$)。$\otimes$ 算子服从结合律，且存在一个中性元素 $1\in S$ (即 $\forall a\in S,a\otimes 1=1\otimes a=a$)和一个吸收元素 0 (即 $\forall a\in S,a\otimes 0=0\otimes a=0$)。

在半环 $(S,\oplus,\otimes)$ 上定义偏序关系 $\preceq$，如果 $\preceq$ 关于两个算子单调，那么该半环结构称为有序半环 $(S,\oplus,\otimes,\preceq)$。

3.1.2 信任半环 算子 $\oplus$ 和 $\otimes$ 的以上性质使得有序半环代数可以很好地描述可信度计算的以下规则：

(1)可信度计算必须满足封闭性，具体来说，节点可信度是空间[0,1]×[0,1]上的点，对节点可信度经过计算后得到的可信度也必须在空间[0,1]×[0,1]中。由于半环运算中，参与运算的元素和计算结果同属于集合 S，因此半环代数可以保证封闭性。

(2)可信度的串联计算具有结合律性质，而且可信度不会增加。具体来说，串行可信度计算可以从一条路径的任意节点开始；另外，如图 1 所示，如果节点 A 对节点 B 的可信度为 T_{AB}，节点 B 对节点 C 的可信度为 T_{BC}，那么节点 A 对节点 C 的可信度小于 T_{AB} 和 T_{BC}。由于 $\otimes$ 算子服从结合律，那么在某一适当的偏序关系 $\preceq$ 下，$\otimes$ 算子符合以上可信度串联计算规则。

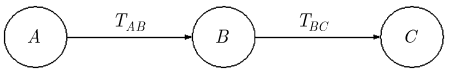


图 1 串行可信度计算

(3)可信度的多径传播具有交换律和结合律性质，同时可信度不会减少。具体来说，多径可信度计算中，不同路径可信度合并的起点和顺序都是不重要的；另外，如图 2 所示，一个节点 A 从不同的路径收到关于同一个节点 B 的多个可信度值，那么节点 A 对节点 B 的可信度不小于它们的最大值。由于 $\oplus$ 算子服从交换律和结合律，那么在某一适当的偏序关系 $\preceq$ 下，$\oplus$ 算子符合以上多径可信度计算规则。

综上所述，有序半环代数可用来描述可信度计算，于是便提出了信任半环。定义有序半环代数 $(S,\oplus,\otimes,\preceq)$，其中 S 表示可信度空间，$\otimes$ 算子表示可

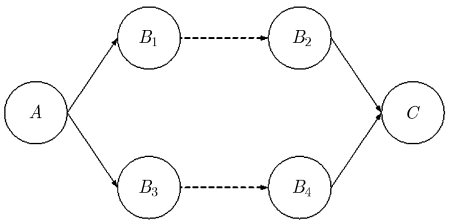


图 2 多径可信度计算

信度串联计算，$\oplus$ 算子表示可信度多径计算。于是图 1 和图 2 所示可信度计算规则可分别表示为：

(1) $a \otimes b \preceq a,b$ 。其中 a 表示节点 A 对 B 的可信度，b 表示 B 对 C 的可信度。

(2) $a \oplus b \succeq a,b$ 。其中 a 表示节点 B_1 传递给节点 A 的关于节点 C 的可信度，b 表示节点 B_2 传递给节点 A 的关于节点 C 的可信度。

本文提出如下的半环模型来计算节点可信度：

$$\left(t_{ik},c_{ik}\right)\otimes\left(t_{kj},c_{kj}\right)\to\left(t_{ik}t_{kj},c_{ik}c_{kj}\right) \tag{3}$$

$$\left(t_{ij}^{p_1},c_{ij}^{p_1}\right)\oplus\left(t_{ij}^{p_2},c_{ij}^{p_2}\right)\to\left(\frac{c_{ij}^{p_1}+c_{ij}^{p_2}}{\dfrac{c_{ij}^{p_1}}{t_{ij}^{p_1}}+\dfrac{c_{ij}^{p_2}}{t_{ij}^{p_2}}},\frac{c_{ij}^{p_1}+c_{ij}^{p_2}}{2}\right) \tag{4}$$

这样，运用式(3)进行串行可信度计算时，由于信任值和置信值都在[0,1]取值，所以二者都会下降。并且，当信任值取 0 时 t 的计算结果为 0，即 0 为信任值的吸收元素；而 1 为信任值的中性元素，因为 1 和任一信任值运算后仍等于该信任值。

进行多径可信度计算的式(4)中，t 的运算采用了文献[5]中距离半环的方法，即计算后的信任值为两个信任值分量的加权调和平均值，每个信任值的权重为对应的置信值。这样计算的结果处在两个信任值分量的中间，并且更靠近置信值高的一方信任值。并且，当一条路径的置信值为 0 时，该值将不会影响最终的置信值，故 0 为置信值的中性元素，且置信值计算具有封闭型，即结果在[0,1]区间取值。

3.2 自适应遗忘机制

由于网络情况是不断变化的，因此信任也具有动态性。那么，在以上半环信任模型基础上，还应定义基于时间的动态变化问题，刻画信任的动态性。

刻画信任的动态性是很重要的，同时它也是信任评估和可信性预测的最大挑战[11]。将信任的动态性融合入信任评价机制，将增强信任评价的实时性，更好地保证网络随时监测到异常行为，避免或减少网络受损。本文提出的自适应遗忘机制就是用来刻画信任的动态性的。

考虑到节点行为的影响随着时间的推移会逐渐降低，量化地表示此现象，则过去某时刻的可信度的权重要比最近某时刻的可信度的权重低。由此本文引入遗忘因子 $\beta(0<\beta\le 1)$，来刻画信任的动态性。具体地来说，若在 t_1 时刻某节点表现了 X 次异常行为，则它相当于在 $t_2\,(t_2>t_1)$ 时刻该节点表现 $X\beta^{t_2-t_1}$ 次异常行为。这样就描述了节点行为的影响逐渐降低的现象。β 反映了节点行为影响的衰减速率，在实际情况中，这种衰减速率是不固定的，随着节点行为的变化也在变动。比如，当节点行为变化较快时，β 应取较大的值，表示过去的行为对目前的影响较小；又如，当节点表现正常行为和异常行为时，β 也应取不同的值，这是因为，一次异常行为对信任形成的影响程度要比一次正常行为对信任形成的影响程度大，很多次正常行为才能弥补一次异常行为对信任的影响。因此，β 固定的遗忘机制不能抵御网络中某些攻击行为，如开关攻击[1]。综上所述，β 应是与信任值相关的变量，这种遗忘机制就是自适应遗忘机制。若 t 表示目前的信任值，则可选择 β 为

$$\beta=1-t \tag{5}$$

或

$$\beta=\begin{cases}\beta_1\ ,\ \ t\ge 0.5\\ \beta_2\ ,\ \ t<0.5\end{cases} \tag{6}$$

其中 $0<\beta_1<<\beta_2\le 1$。

3.3 自适应遗忘机制与半环信任模型的融合过程

第 2 节已述，根据式(1)和式(2)，可信度 (t,c) 可由正常行为次数 a 和异常行为次数 b 计算得到。根据自适应遗忘机制，在可信度更新计算时，遗忘因子 β 的引入将影响正常行为次数 a 和异常行为次数 b，从而影响可信度 (t,c) 的计算结果。假设在时刻 t_1 某节点“等效”已经表现了 a 次正常行为和 b 次异常行为，则相当于在 $t_2\,(t_2>t_1)$ 时刻该节点已经表现了 $a\beta^{t_2-t_1}$ 次正常行为和 $b\beta^{t_2-t_1}$ 次异常行为。又假设在时刻 t_1 和 $t_2\,(t_2>t_1)$ 之间，该节点又表现了 Δ_a 次正常行为和 Δ_b 次异常行为，那么在时刻 t_2，a 将更新为 $(a\beta^{t_2-t_1}+\Delta_a)$，$b$ 将更新为 $(b\beta^{t_2-t_1}+\Delta_b)$。更新后的 a 和 b 根据式(1)和式(2)计算 t 和 c，得到当前时刻 t_2 该节点的可信度 (t,c)。进而根据 3.1.2 节中的信任半环即式(3)和式(4)，该可信度参与到相应节点所在路径的串行可信度计算以及多径可信度计算，得到网络中某两个节点间的可信度，这样便完成了自适应遗忘机制与半环信任模型的结合。整个融合过程可用图 3 表示。

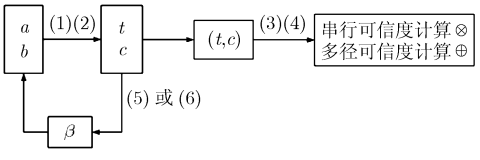


图 3　自适应遗忘机制与半环信任模型的融合过程

4 仿真实验与结果分析

4.1 节点设置和仿真细节

在仿真实验中，设一部分节点为正常节点，它们根据自己的传输协议正常地发送、接收和转发数据包，但鉴于 Ad hoc 网络的固有特性，也可能会由于网络拥塞、无线信道性质差(如信道质量差、带宽不够等)而产生正常丢包等异常行为；并设另一部分节点为异常节点，这些异常节点又分为一般异常节点(丢包率为 90%的节点)和一种特殊异常节点——进行开关攻击的节点。正常节点和异常节点的身份在拓扑形成时就形成。本实验对开关攻击这一特定的攻击行为进行模拟，并检验本文提出的基于自适应遗忘机制的半环信任模型对它的抵御效果。

随着仿真的进行，某一节点对其他正常节点和异常节点的可信度评价应按如图 4 所示趋势变化，这是仿真希望达到的效果。

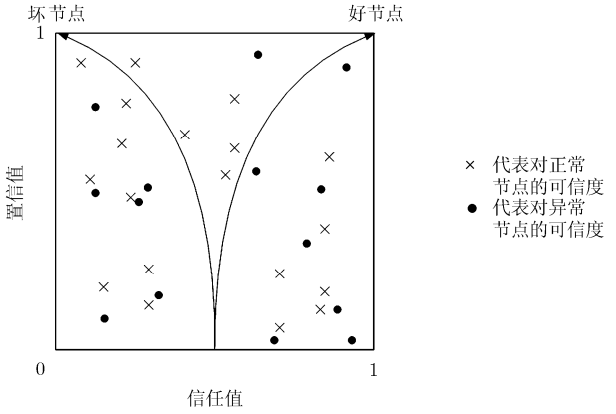


图 4 可信度变化趋势

仿真实验中共设置 50 个节点，25 个为正常节点，10 个为一般异常节点，15 个为开关节点(进行开关攻击的异常节点)。可信度初始值设为：初始信任值在(0.45,0.55)区间，初始置信值在(0.05,0.15)，即中等的信任值和较低的置信值。实验中设置一定的仿真周期，并按此周期进行计算结果的统计。

4.2 结果及分析

实验中，首先通过计算源节点对开关节点的可信度，验证了加入自适应遗忘机制的半环信任模型对开关攻击的抑制效果。图 5 为加入自适应遗忘机制前后，源节点对开关节点的可信度评价。

应用自适应遗忘机制刻画信任的动态性，是为了更好地保证网络随时监测到开关攻击等异常行为。由图 5(a)可见，未加入自适应遗忘机制时，虽然开关节点表现了攻击行为，但是源节点对它的可信度评价仍然朝(1,1)方向靠近，即不能很好地检测并抑制开关攻击。而由图 5(b)可见，加入自适应遗忘机制后，虽然开关节点依然表现出一定的开关行为，但是源节点对它的可信度评价总体是朝着(0,1)靠近的，即自适应遗忘机制可以检测并抑制开关攻击。由此可见，基于自适应遗忘机制的半环信任模型可以较好地检测并抑制开关攻击。

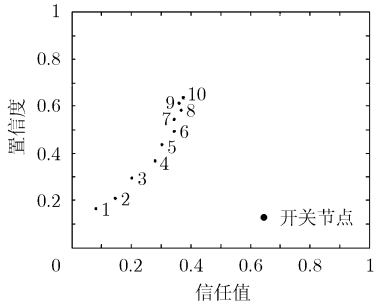
再从源节点对其他所有节点的可信度评价来看本文信任模型的节点分类效果和抑制攻击效果。图 6 和图 7 分别为未加入自适应遗忘机制时和加入自适应遗忘机制时，源节点对其他所有节点的可信度评价。

由图 6 可看出，未加入自适应遗忘机制时，随着开关节点开始进行攻击，源节点不能较好地分辨正常节点和异常节点，对两种节点的可信度评价混合，无法明显分辨正常节点和异常节点。而由图 7 可看出，加入自适应遗忘机制后，虽然当开关节点开始进行攻击后，源节点无法明显分辨出正常节点和异常节点，但是过一段时间后，源节点便能够有效地分辨出两种节点，再次验证了基于自适应遗忘机制的半环信任模型可以较好地抑制开关攻击。分析原因，这是因为自适应遗忘机制可以有效地“惩罚”节点的异常行为，这样，即使异常节点再表现正常行为，也需要较长的时间才能“补偿”之前的异常行为。这样可使源节点对开关节点的可信度评价依然朝着(0,1)的异常节点标准靠近，有效地抑制了开关攻击。

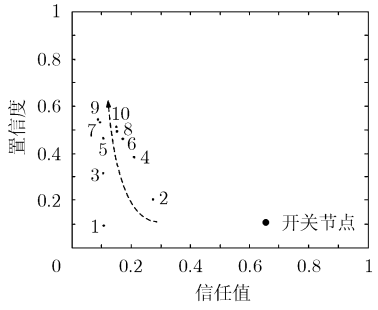
由以上实验结果和分析可得，本文基于自适应遗忘机制的半环信任模型可以有效地对正常节点和异常节点进行分类，并能有效地抑制开关攻击。

5 结论

本文提出了一种基于自适应遗忘机制的半环信任模型，核心思想是运用半环代数计算节点间的可信度，并将自适应遗忘机制融合入该信任模型中，用来刻画信任的动态性。仿真结果表明，基于自适应遗忘机制的半环信任模型可以有效地对正常节点和异常节点进行分类，并能有效地检测并抑制开关攻击。运用这种信任模型可以使节点及时、准确地检测到异常节点，并进行预防和抵制，有效地保护 Ad hoc 网络不受异常节点的侵害。

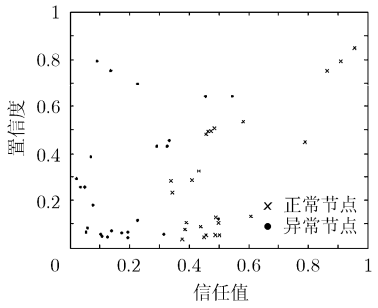


(a) 未加入自适应遗忘机制

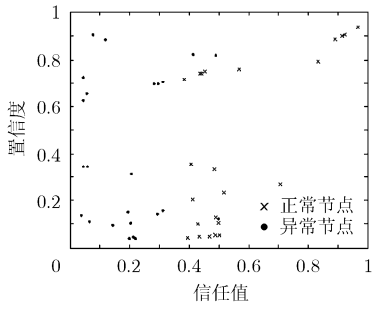


(b) 加入了自适应遗忘机制

图 5 加入自适应遗忘机制前后，源节点对开关节点的可信度评价 (图中数字为仿真周期的序号)

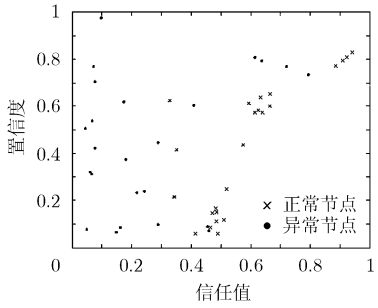


(a) 少数几个仿真周期后的计算结果

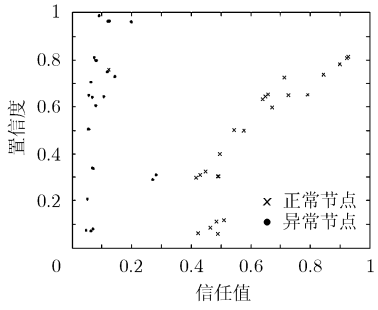


(b) 多个仿真周期后的计算结果

图 6 未加入自适应遗忘机制时，源节点对其他所有节点的可信度评价



(a) 少数几个仿真周期后的计算结果



(b) 多个仿真周期后的计算结果

图 7 加入自适应遗忘机制时，源节点对其他所有节点的可信度评价

参 考 文 献

[1] Sun Yan (Lindsay), Han Zhu, and Liu K J R. Defense of trust management vulnerabilities in distributed networks[J]. *IEEE Communications Magazine*, 2008, 46(2): 112–119.

[2] Buchegger S and Le Boudec Jean-Yves. Self-policing mobile Ad hoc networks by reputation systems[J]. *IEEE Communications Magazine*, 2005, 43(7): 101–107.

[3] Sun Yan (Lindsay), Yu Wei, Han Zhu, and Liu K J R. Information theoretic framework of trust modeling and evaluation for Ad hoc networks[J]. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 305–317.

[4] Liao Hong-mei, Wang Qian-ping, and Li Guo-xin. A fuzzy logic-based trust model in grid[C]. International Conference on Networks Security, Wireless Communications and Trusted Computing(NSWCTC '09), Wuhan, China, April 25–26, 2009, 1: 608–614.

[5] Theodorakopoulos G and Baras 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.

[6] Zhang Ming-wu, Yang Bo, and Zhang Wen-zheng. A semiring privacy protect model[C]. IFIP International Conference on Network and Parallel Computing Workshops, Dalian, China, 2007: 255–262.

[7] Zhang Yun-chang, Chen Shan-shan, and Yang Geng. SFTrust: a double trust metric based trust model in unstructured P2P system[C]. Source, IPDPS archive Proceedings of the 2009 IEEE International Symposium on Parallel&Distributed Processing(IPDPS 2009), Rome, Italy, May 25–29, 2009: 1–7.

[8] Perrone L F and Nelson S C. A study of on-off attack models for wireless Ad hoc networks[C]. First IEEE International Workshop on Operator-Assisted (Wireless Mesh) Community Networks (OpComm 2006), Berlin, Germany, Sept. 2006: 1–10.

[9] Li J, Li R, and Kato J. Future trust management framework for mobile Ad hoc networks[J]. *IEEE Communications Magazine*, 2008, 46(4): 108–114.

[10] Zouridaki C, *et al*.. A quantitative trust establishment framework for reliable data packet delivery in MANETs[C]. Proc. 3rd ACM Wksp. Sec. Ad hoc and Sensor Networks, Alexandria, Virginia, USA, Nov. 7, 2005: 1–10.

[11] Chang E, Thomson P, Dillon T, and Hussain F. The fuzzy and dynamic nature of trust[C]. LNCS 3592, Berlin, Springer-Verlag, 2005: 161–174.

喻　莉：女，1970 年生，教授，博士生导师，武汉光电国家实验室(筹)宽带中心主任，研究方向为计算机网络与多媒体通信.

李静茹：女，1987 年生，博士生，研究方向为可信路由.

刘祖浩：男，1986 年生，博士生，研究方向为可信路由.