基于信任关系的 IP 网络容错容侵机制

纪俊杰　阳小龙　王 进　吴雄飚　林建人　隆克平
(电子科技大学光互联网及移动信息网络研究中心　成都　610054)

摘　要：目前 IP 网络受自身故障和网络攻击等异常行为影响较过去更深广。因此如何增强 IP 网络的容错和容侵能力显得尤为重要。但是目前很多的研究仅关注其中一个方面，而很少两者兼有，从而不能很好地兼顾安全性和可生存性。该文提出了一种有效的基于信任关系的容错容侵机制。该机制借用了社会网络中的信任关系思想，定量地描述了信任关系值与网络行为的对应关系——某节点的恶意行为会使得自己在其他节点处的信任值下降。然后，分析了该机制如何对 3 种网络异常，即自身故障、诋毁攻击和矛盾行为攻击的容忍能力。最后，仿真结果和分析表明该机制可以迅速而精确地检测到异常节点，并能有效地阻止这些异常对网络的攻击和破坏。

关键词：IP 网络；生存性；信任；容错；容侵
中图分类号：TN915.08　　**文献标识码**：A　　**文章编号**：1009-5896(2009)07-1576-06

An Efficient Fault-Tolerant and Intrusion-Tolerant Scheme Based on Trust Relationship for IP Networks

Ji Jun-jie　Yang Xiao-long　Wang Jin　Wu Xiong-biao　Lin Jian-ren　Long Ke-ping
(*Research Center for Optical Internet and Mobile Information Networks*,
Univ. of Electronic Science and Technology of China, *Chengdu* 610054, *China*)

Abstract: Nowadays, IP networks are suffering many faults and malicious attacks which greatly threaten its security and survivability. So it is an important issue that how to make the IP networks to be more robust under faults and attacks, i.e., to improve their tolerance abilities for both fault and intrusion. However recently, most of the researches focus on only one of them, and decouple the survivability and security each other. According to the trust model in social networks, this paper proposes an efficient fault-tolerant and intrusion-tolerant scheme based on trust relationship for IP networks. This scheme not only borrows the trust rating from the social links, but also qualitatively describes the relationships between the trust rating and the network behavior. Then, this paper analyses the scheme how to tolerate three known malicious behaviors, viz., self-faults, bad mouth attacks and conflict behavior attacks. Finally, the numeric simulation results show that the scheme can detect the malicious nodes fast and accurately and efficiently prevent these malicious behaviors in IP networks.

Key words: IP networks; Survivability; Trust; Fault-tolerant; Intrusion-tolerant

1　引言

目前 IP 网络受自身故障和网络攻击等异常行为影响较过去更深广，因此增强 IP 网络的容错和容侵能力显得尤为重要。但是目前很多研究仅关注其中一个方面，而很少两者兼有。比如：自愈、恢复[1,2]等机制是只从容错的角度来提高网络的容错能力；传统的确认、加密[3,4]和入侵检测[5]等技术则是只从容侵的角度来设计的。因此，如何提高 IP 网络的安全和生存性能，即既能容忍错误又容忍入侵就成为一个重要的研究课题。

人类社交活动中，任何一种用于建立个体之间联系的自然现象、社会活动或技术机制都可能形成一张网络，如：朋友关系、文献引用关系等。这些网络都有相应的机制(如：道德约束、行为规范或法律法规等)来处理个体之间的“信任关系”，对个体的差错行为(不管是无意识的或有意识的)进行内部处理和消化。IP 网络与这些人类社交网络有不少类似之处。因此，IP 网络可以基于社交网络模型，在信任与过滤基础上构建新容错容侵框架。

目前已有一些研究者将社会网络中的信任关系机制应用到通信网络中，以使网络能够既容错又容侵。Resinick 等的文献[6]中提出了一种集中式信誉系统。在该系统中，由一个中央节点来维护各个实体间的信任值表，每一个实体可以向中央节点查询

2008-05-15 收到，2009-03-02 改回
国家 973 计划项目(2007CB310706)，国家杰出青年科学基金(60725104)和国家自然科学基金(60672045，60873263)资助课题

它与其它节点间的信任值。很明显，该系统存在瓶颈、可扩展性差，特别是当中央节点遭到恶意攻击或自身发生故障时，整个网络都会受到影响。CONFIDANT[7]是一种分布式的、对称地利用直接信任信息和间接信任信息来更新信任值的 MANET 路由协议。然而，如果不采取其它的限定措施而直接利用间接信任信息，则它很容易受到诋毁等形式的攻击。RFSN[8]是最早提出的专为传感器网络设计的基于信任的模型，并采用看门狗机制(watchdog)来建立信任值。但是，看门狗不可避免由于其自身故障所导致的异常行为，所以这个信任模型存在不可靠性。DRBTS[9]只是利用直接和间接信任信息在传感器定位网络中建立一个分布式的模型而已，没有进行较具体的研究。ATSN[10]是在传感器网络中基于移动代理的信任模型。传感器节点利用看门狗机制来监测其它节点的行为，利用移动代理来计算信任值和传播信任值信息。传感器节点收到信任值信息后利用其决定节点的行为。但它一方面没有充分共享节点间的信任信息；且另一方面因它采用了移动代理，而引入了移动代理自身固有的缺陷(如：三角路由等)。此外，移动代理方式也一定程度上增加了系统实现成本。

虽然利用信任关系机制来提高网络的容错容侵能力已取得了一些成果，但还处于初级阶段。一方面它们在提高网络的容错容侵能力上还不够完美，比如可扩展性差；另一方面它们只适用于特定的网络环境，比如无线传感器网络。本文提出了一种基于信任关系的 IP 网络容错容侵机制，将网络故障和入侵等异常事件统一处理来提高网络的容错容侵能力。

本文主要的贡献如下：首先，设计了一种分布式的、基于信任关系的容错容侵机制；其次，提出了一种在通用意义上的 IP 网络环境下，信任值的定义、更新及其传播机制；最后，通过仿真分析了几种网络异常情况下，该信任关系机制提高网络容错容侵的能力。

2　基于信任关系的容错容侵机制

2.1 基于信任关系的 IP 网络容错容侵机制构建

该机制对信任值进行了定义，制定了信任值在 IP 网络中的更新、传播和共享策略；并提出了信任值监测和更新机制的具体实现方案。该机制的结构图如图 1 所示。

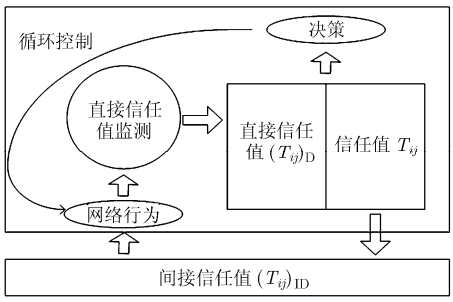


图 1 容错容侵机制结构图

2.2 信任值的定义和度量

本文利用 T_{ij} 来表示节点 i 所维护的关于节点 j 的信任值。它由两部分组成：一是直接对目标节点进行监测，一是接收其它相邻节点对它的评价。因此，其定义如下：

定义 1

$$T_{ij} = a(T_{ij})_{\mathrm{D}} + (1-a)(T_{ij})_{\mathrm{ID}} \tag{1}$$

其中 T_{ij} 取值范围为[0,1]，$(T_{ij})_{\mathrm{D}}$ 和 $(T_{ij})_{\mathrm{ID}}$ 分别称作直接信任值和间接信任值；$a\in[0,1]$为用户可以自行调节的常数，目的在于区分直接信任值与间接信任值对 T_{ij} 的不同贡献。当网络初始化时，假定任何节点的信任值都为 0.5。

直接信任值 $(T_{ij})_{\mathrm{D}}$ 取决于用户对特定应用的需求。比如，语音业务希望延迟尽可能小，而邮件业务却要求低丢包率。该机制使得用户可以根据自身业务的需求自定义直接信任值。其定义如下：

定义 2

$$\begin{aligned}\left(T_{ij}\right)_{\mathrm{D}} &= c_1 f_1(\cdot) + c_2 f_2(\cdot) + \cdots + c_i f_i(\cdot) + \cdots \\ &\quad + (1 - c_1 - c_2 - \cdots - c_{n-1}) f_n(\cdot)\end{aligned} \tag{2}$$

其中 $c_1 + c_2 + \cdots + c_n = 1$。$c_i\in[0,1]$为常数，可以由用户据各个信任映射函数对信任值的贡献程度来进行设置。n 为用户定制的信任映射函数的总个数，$f_i(\cdot)$为第 i 个信任映射函数。

间接信任值 $(T_{ij})_{\mathrm{ID}}$ 是由各个节点之间广播交互而得到的间接信任值信息。某些节点对特定节点非常信任，而有的节点却不信任，所以我们要区别对待。它可以定义如下：

定义 3

$$(T_{ij})_{\mathrm{ID}} = \frac{1}{N_i}\sum_{l=1}^{l=N_i} w_{il}\cdot T_{lj} \tag{3}$$

其中 l 是节点 i 邻节点的下标，N_i 为与节点 i 邻节点总数。w_{il} 是一个权值，其具体表达式如下：

$$w_{il} = \begin{cases} \text{常数}, & \forall T_{il} \ge \mathrm{TH} \\ \dfrac{1}{2^k} + \dfrac{1}{2^t}, & \forall T_{il} < \mathrm{TH} \end{cases} \tag{4}$$

其中 $l \in N_i$。当节点本身所维护的关于其它某节点的信任值大于一个特定门限值 TH 时，就认为该节点是合作的，即完全可信任的。相反，则反之。式

(4)中常数代表与之处于合作关系时节点所贡献的关于其它节点的间接信任值的权重。$1/2^k+1/2^t$ 表示与之不合作关系时节点所贡献的关于其它节点的间接信任值的权重。

由式(4)显见该动态函数有两个参数 k 和 t。k 表示节点的度数(即节点的分支数)，t 表示一定时器所设定的时间长度。在 RFSN[8]信誉机制中，只是接收正常节点的间接信任值信息。其实，即使有些节点被攻击、被控制或自身出现故障，它们发布的间接信任值对计算信任值也是有一定积极贡献的。所以，本文与 RFSN[8]的机制相比较无论是什么样的节点(好或坏)，都接收它们发布的间接信任值信息，只是在权重上有所区分。这样既可以充分共享一切有利用价值的信息，又不以牺牲安全性为代价。本文通过权值对下列情形予以区别对待：(1)好的节点和不好的节点；(2)节点由于自身故障或被恶意攻击控制两种情况下所发布的间接信任值的有用性；(3)在节点被恶意控制或攻击的前提下，该节点的度数较大或较小的不同。

2.3 自适应信任值更新策略

在该机制中，信任值是实时更新的。受 TCP 拥塞控制理论的启发，将 TCP 拥塞控制中的慢启动与冲突避免策略加以改进以实现对信任值的更新。具体的更新策略是：假定一个监测时间间隔窗口，设 W_t 为 t 时刻时间间隔，窗口最大值为 $W_{\max}$，窗口初始值为 W_0。当直接监测计算得到的信任值 T 大于某特定门限时，忽略其它节点所传来的间接信任值信息，用直接信任值作最终信任值，并将节点自身监测计算信任值的时间间隔 W_t 成指数形式增加。当增加至 $W_t=W_{\max}$ 后，监测时间间隔将保持为 $W_{\max}$ 不变。一旦直接监测到的直接信任值 T 低于该门限值时，开始根据定义式 1 来考虑间接信任值，并将监测时间间隔降为最大值的一半。若 T 开始高于门限值，则忽略间接信任值并使 W_t 就以每次 1 s 的方式增加，直到增加到最大值。若 T 仍未高于该门限值，则 W_t 继续降为上一次间隔的一半，继续根据定义式 1 来考虑间接信任值来得到最终信任值…。

此外，为了进一步加强信任，增强网络的可靠性。本文对收到的间接信任值做进一步地处理后再代入定义式 1 进行加权更新。具体的处理过程为：我们定义一个门限值，也就是每个节点发的间接信任值信息与相应节点收到的其它节点传来的间接信任值进行比较。如果与接收到的其它的间接信任值的平均值之差超过某个门限值，则认为它是假信息而忽略。但是，如果有 N 个节点的间接信任值信息，就要计算 N 次平均值。可是，因为现实网络中一般节点的度并不大，而且节点的度较大的节点的数量很有限[11]。

2.4 信任值绑定传播策略

本文假定每个路由器节点都维护一张相邻节点的信任值表。这个表其实不是独立的一张表，而是和路由表结合在一起的。这里暂且称它为改进的路由表，即在路由信息的后面相应的位置上，添加一个信任值字段。信任值与路由信息是绑定在一起利用改进了的路由协议来向外传播的。信任值与路由信息一起存储、一起传播，既可以借鉴利用现有的成熟的路由信息存储、更新机制，又以较少的代价使原有路由器的功能得到扩展和增强。我们假定每个节点只维护相邻节点的信任值信息。当然，这些信任值是可以传递到很多跳以外的。但为了简化机制，此种情况在本文中不予考虑。

3 容错容侵机制的具体实现

该机制的实现如下：节点混合监听、收集信任信息，然后根据定义式(2)来计算直接信任值 T_{ij}。根据 T_{ij}，节点 i 可以决定如何处理节点 i，j 之间的行为。此外，借助于改进的路由表，节点 i 将 T_{ij} 以间接信任值的身份向其它节点传播。其传播是利用改进的路由协议。关于改进的路由协议在 2.4 节已经详细论述。此外，我们亦可不对路由协议进行改进，而单独对信任信息进行传播。单独对信任值进行传播显然增加了额外的网络开销。本文采用与路由信息绑定传播策略。

混合监听和数据收集模块的功能在第 3 节的开头已经提及。该监听机制实时地监测相邻节点的行为，并计算直接信任值。直接信任值由用户定制的信任映射函数库中的一个或多个函数进行加权计算得到。各个函数都是用户自定义的，比如：可以将第 1 个函数定义为包投递率，第 2 个定义为延迟函数，第 3 个定义为吞吐量函数以及其它的。用户可以根据自己的喜好和对各网络性能指标的关注度，来选取信任映射函数的种类，数量及函数具体实现方式。此外，用户还可以自己决定各个信任映射函数在直接信任值中的权重，即 c_i 值，它可以由用户在[0,1]内调节。当然里面的“1”表示该信任映射函数被选用，“0”表示未被选用。直接信任值的监测过程如图 2 所示。

4 机制的容错容侵能力分析

4.1 节点故障引起的异常

网络节点有可能突然断电或因人为等因素使得节点的部分或全部功能失效。那么该机制会根据定

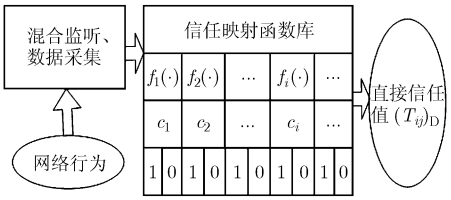


图 2 直接信任值的监测图

义式(2)计算得到直接信任值为“0”或很低。因为其它节点所保存的信任值信息也是实时更新的。再考虑到式(4)对间接信任值权值的降低，会使各个节点向外发布的间接信任值迅速下降。此外，因为计算最终信任值时几乎没有了直接信任值项，所以各个节点所维护的关于该节点的信任值会迅速收敛至“0”。从而有效地达到阻止异常的目的。

4.2 诋毁攻击引起的异常

节点对外发布虚假信任值来诬陷好的节点，却提高坏的节点的信任值来对外传播[8]。这样的攻击叫做诋毁攻击。关于信任管理或信誉系统的文献[8,12]对这种攻击进行过论述。

首先，在本文的机制中，当每个节点接收到关于某节点 A 的间接信任值后都要与接收到的其它节点传来的关于节点 A 的间接信任值的统计平均值进行比较，当差值超过我们设定的门限值时，就忽略该间接信任值。其次，当差值没有低于假定的门限值却低于式(4)中的门限值时，那么对间接信任值进行的权值为 $1/2^k+1/2^t$，参见式(4)。对它的加权会综合考虑其节点自身的度数和低于门限值的时间 t。原因在于：(1)可以设想当恶意节点度数很大的时候，它如果恶意地向外发布虚假信任值信息，那么它对网络的恶意影响程度较大，为了确保网络安全，尤其是全局安全，本文考虑到利用一个特殊的加权策略来处理。那么利用根据以节点的度数作为负指数，按照负指数规律递减的方式会使度大的节点传来的间接信任值迅速趋于“0”，这样兼顾了安全和效率，如式(4)中所示。(2)对恶意节点，它的权重都初始化为“1”。并设定一个定时器 $t=T_t\,(T_t>0)$，T_t 时间过后，若该节点恢复正常则其权重值加倍且使其小于等于 1，若还未恢复正常则将权重降为初始权重的 1/2，另外定时器重设为 t=2,T_t,…。一旦权重有加倍动作，则将定时器置 0。这样便有效地阻止了这种攻击引起的异常的破坏。

4.3 矛盾行为攻击引起的异常

矛盾行为攻击是信任管理系统中另一种攻击。恶意节点能够通过使某好节点对其它不同节点有不同的行为表现达到消减该好节点信任值的目的。比如，恶意节点 i 可以始终表现得对节点 j 友好却对节点 k 不友好。这样，节点 j 和节点 k 对节点 i 的评价就会正好相反，造成冲突。在本文的信任机制中，采用的多种加权策略可以有效地阻止这种类型的攻击所引发的网络异常。应对这种异常的具体方法和 4.2 节中所述基本相同。

5 仿真

5.1 整体仿真环境

为了简化仿真，本文在仿真中只利用两个信任映射函数 $f_1(\cdot)$ 和 $f_2(\cdot)$。$f_1(\cdot)$ 定义为包投递率，它的表达式如下：

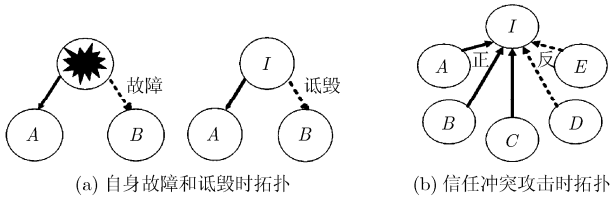
$$f_1(\cdot)=\frac{\text{目的节点接收包的总数}}{\text{发送节点发送包的总数}} \tag{5}$$

$f_2(\cdot)$ 定义为一个关于延迟的函数，它的表达式如下：

$$f_2(\cdot)=\mu\frac{\text{延迟超过}\beta R_{tt}\text{的包数}}{\text{发送节点发包数}} \tag{6}$$

其中 μ 是一个与网络应用业务对延时敏感度相关的系数，用户可以自己调节。比如，语音、视频会议等业务对延时敏感度较强，那么就可以把这个系数调得大一些；而对延时相对不太敏感的业务，比如大文件传输等，可以将该系数调得稍小些。

网络仿真节点拓扑结构如图 3 所示。其中图 3(a)对应节点故障和诋毁攻击引起的网络异常。情形 1：节点 I 发生自身故障；情形 2：节点 I 对节点 A 表现正常，对节点 B 的信誉进行恶意诽谤。图 3(b)对应矛盾行为攻击引起的异常。节点 I 对节点 A，节点 B，节点 C 总是友好的，对节点 D，节点 E 始终是恶意的。所以节点 A，节点 B，节点 C 对节点 I 的评价是正面的，而节点 D，节点 E 对节点 I 的评价是反面的。



(a) 自身故障和诋毁时拓扑　　(b) 信任冲突攻击时拓扑

图 3 仿真节点拓扑结构图

5.2 网络仿真评价目标、仿真结果及分析

本文利用各个节点所保存的某特定节点的信任值随时间的变化来反映该节点的好坏行为。进而为隔离、修复等措施提供定量的决策依据。针对这 3 种异常的仿真结果进一步证实了该机制具有容错容侵的能力。

对于图 3(a)情形 1，节点 I 发生故障，根据本文中信任值的定义，节点 A 和节点 B 所保存的节点 I

的信任值都会立即下降，其过程如图 4 所示。因此，节点 A 和节点 B 均与 I 断绝友好关系。

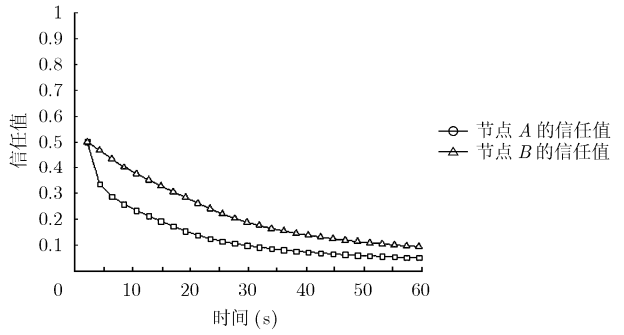


图 4 对节点自身故障的容错能力

对于图 3(a)情形 2，I 节点对节点 A 始终保持好的行为，而对节点 B 保持不好的行为。节点 A 所维护的关于节点 I 的信任值迅速升高，而节点 B 所维护的关于节点 I 的信任值会下降很快。因此，节点 A 会继续与节点 I 保持友好往来，而随着 I 的信任值在节点 B 处的下降，B 会断绝与 I 的往来。根据本文中信任值的定义，节点 A 和节点 B 保存的节点 I 的信任值变化趋势如图 5 所示。对于图 3(b)的情形，节点 A，节点 B，节点 C 所监测到的信任值很高，节点 D，节点 E 监测到的信任值很低。直接信任值比间接信任值在信任值计算中的权重要高。它们之间共享间接信任值后各个节点所保存的关于节点 I 的信任值变化趋势如图 6 所示。

6 结论

本文提出了一种基于信任关系的 IP 网络容错容侵机制，并定量地描述了节点的信任值与节点行为之间的对应关系。当节点表现异常威胁其它节点时，它的信任值就会迅速降低。每个节点独立地监测相邻节点的行为，并将信任值与路由信息绑定对外传播。我们的信任机制可以对网络异常行为，比如：节点自身故障、诋毁攻击和信任关系冲突攻击

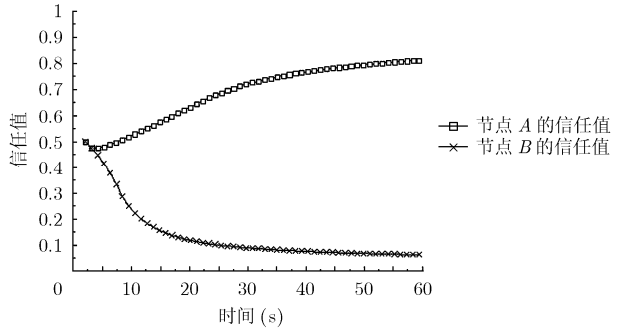


图 5 对诋毁攻击的容忍能力

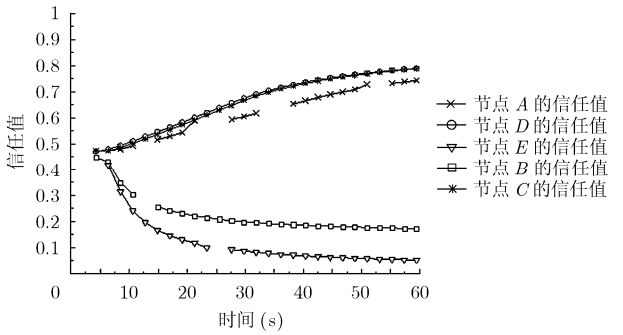


图 6 对矛盾行为攻击的容侵能力

等具有容错容侵的能力，从而有效地提高了 IP 网络的生存性。此外，还可以迅速而精确地定位异常节点的位置，以便对其采用隔离和修复等策略。

参 考 文 献

[1] Kodian A A. Advances in p-cycle network design. [Ph.D. dissertation]. Department of Electrical and Computer Engineering, University of Alberta. Spring 2006.

[2] Cholda P and Jajszczyk A. Reliability assessment of optical p-cycles. *IEEE/ACM Transactions on Networking*, 2007, 15(6): 1579–1592.

[3] Chen Hai-guang, Han Peng, and Yu Bo, *et al*.. A new kind of session keys based on message scheme for sensor networks. The Seventeenth Asia Pacific Microwave Conference (APMC 2005), Suzhou, China, Dec. 4-7, 2005: 1–4.

[4] Karlof C, Sastry N, and Wagner D. TinySec: A link layer security architecture for wireless sensor networks. Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), Baltimore, Maryland, USA, 2004: 162–175.

[5] Chen Hai-guang, Han Peng, and Zhou Xi, *et al*.. Lightweight anomaly intrusion detection in wireless sensor networks. PAISI, 2007, LNCS 4430: 106–116.

[6] Resnick P and Zeckhauser R. Trust among strangers in internet transactions: empirical analysis of Ebay's reputation system. Advances in Applied Microeconomics: The Economics of the Internet and E-Commerce, (Michael R B. ed.) Amsterdam: Elsevier/JAI Press, 2002, 11: 127–157.

[7] Buchegger S and Le Boudec J Y. Performance analysis of the CONFIDANT protocol (cooperation of nodes-fairness in dynamic ad-hoc networks). Proceedings of MobiHoc 2002, Lausanne, CH, June 2002: 226–236.

[8] Ganeriwal S and Srivastava M B. Reputation-based framework for high integrity sensor networks. SASN'04, Washington, D.C., USA, October 25, 2004: 66–77.

[9] Srinivasan A, Teitelbaum J, and Wu J. DRBTS: Distributed

reputation-based beacon trust system. The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), Indianapolis, USA, 2006: 277–283.

[10] Chen Hai-guang, Wu Hua-feng, and Zhou Xi, *et al*.. Agent-based trust model in wireless sensor networks. DOI 10.1109/SNPD. 2007, 122: 119–124.

[11] Newman M E J. The structure and function of complex networks. *SIAM Review*, 2003, 45(2): 167–256.

[12] Dellarocas C. Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems. Proceedings of ICIS, Brisbane, Australia, 2000: 520–525.

纪俊杰：男，1982年生，硕士生，研究方向为IP网络生存性理论与技术.

阳小龙：男，1970年生，教授，博士，研究方向为光互联网、宽带网络理论与技术.

王　进：男，1980年生，博士生，研究方向为光互联网、宽带网络理论与技术.

吴雄飚：男，1981年生，硕士生，研究方向为IP网络生存性理论与技术.

林建人：男，1982年生，硕士生，研究方向为IP网络生存性理论与技术.

隆克平：男，1968年生，教授，博士，研究方向为宽带网络理论及技术、无线信息网络、网络安全与电信应用等.