·安全技术· 文章编号：1000-3428(2016)11-0165-05 文献标志码：A 中图分类号：TP309

基于信任度的自私用户协作激励机制

王 文[1]，黄开枝[1]，马 林[2]

（1. 国家数字交换系统工程技术研究中心，郑州 450002；2. 中国科学院上海微系统与信息技术研究所，上海 200050）

摘 要： 在多用户网络中，自私用户为节省自身能量和计算资源而拒绝为其他用户提供协作。针对这种消极行为，基于用户间信任度评价提出协作激励机制。中继通过与通信用户比较信任值来决定是否参与协作，自私用户信任值越低，其需要其他节点协作时遭到拒绝的概率越大，而积极参与协作的用户信任值越高，其获得其他节点协作的概率越大。通过信任值高低来激励用户积极参与协作提升自身信任度，以获取更多中继为已所用。仿真结果证明了所提方案的有效性，在信任度的激励下，自私用户积极参与协作提升自身的信任值，通信质量与无私中继协作转发相当。

关键词： 多用户网络；自私用户；信任度；信道容量；中继协作；协作激励

中文引用格式： 王 文，黄开枝，马 林. 基于信任度的自私用户协作激励机制[J]. 计算机工程，2016，42(11)：165-169，176.

英文引用格式： Wang Wen，Huang Kaizhi，Ma Lin. Cooperation Incentive Mechanism for Selfish Users Based on Trust Degree[J]. Computer Engineering，2016，42(11)：165-169，176.

Cooperation Incentive Mechanism for Selfish Users Based on Trust Degree

WANG Wen[1]，HUANG Kaizhi[1]，MA Lin[2]

（1. China National Digital Switching System Engineering and Technological R&D Center，Zhengzhou 450002，China；
2. Institute of Microsystem and Information Technology，Chinese Academy of Sciences，Shanghai 200050，China）

【Abstract】 In the multi-user network，selfish users refuse to provide other users with cooperation for saving their own energy and computing resources. In order to encourage selfish users to offer their resources，a cooperation incentive mechanism based on users trust degree evaluation is proposed. Relays decide whether to participate in the cooperation or not by comparing the trust value of communication users. The lower trust value of the selfish users，the more likely they will be rejected when they need cooperation. While the higher trust value of users，the more likely they will get cooperation. Simulation results demonstrate the effectiveness of the proposed scheme. The selfish users actively participate in the cooperation to increase their own trust value，and the communication quality is close to that of the cooperation with selfless relays.

【Key words】 multi-user network；selfish users；trust degree；channel capacity；relay cooperation；cooperation incentive

DOI： 10.3969/j.issn.1000-3428.2016.11.027

0 概述

对于通信用户来说，中继协作通信可以带来额外的分集增益，提高无线信道的传输速率及传输可靠性，增加系统覆盖范围和系统鲁棒性。在多用户网络中，利用空闲用户闲置的网络资源进行协作转发，可以进一步提高网络资源利用率，增加系统容量。

对于双向全双工中继通信的多用户网络，文献[1]提出一种最优资源分配方案，实现了网络吞吐量最大化，同时提出运算复杂度较低的次优资源分配方案。文献[2]对多用户网络中用户功率进行拍卖，通过竞标和定价策略实现整体效益最大，以此促进用户进行协作。近几年也兴起以博弈理论解决自私用户的拒绝协作问题，通过在用户和中继之间建立具有买卖关系的博弈模型，以虚拟货币的形式激励自私用户作为中继参与协作获得收益。文献[3]采用非协作博弈得到发送方和恶意窃听者之间的纳什均衡，并且给出窃听方协作的条件。文献[4]采用顺序第二价格博弈的方法解决多用户多天线的双向中继系统中多对用户与单中继协作的问题。文献[5]进一步研究了

基金项目： 国家“863”计划项目“未来无线接入物理层与系统安全通信技术研究”(2015AA01A708)；国家自然科学基金“基于博弈的物理层安全组网研究”(61379006)。

作者简介： 王 文(1990—)，女，硕士，主研方向为移动通信物理层安全技术；黄开枝，教授、博士后；马 林，助理研究员、博士。

收稿日期： 2015-10-23 **修回日期：** 2015-12-03 **E-mail：** wenang555@126.com

三方博弈的场景。文献[6]提出两次报价博弈,抑制由中继自私性导致的欺骗行为。

除了虚拟货币这种收益形式,用户间的信任关系也是促进自私用户协作的重要手段。网络中用户间的信任度实质是对网络中某个用户身份和行为的可信度评估,同时也与这个用户所具有的能力和主观参与协作的积极性有关[7]。用户间的信任关系具有不确定性,通过周期性地观察彼此的交互转发行为,可以对节点间的直接信任度进行评估,并根据被评估节点的行为变化更新信任度[8-10]。文献[11]引入一种上下文感知的方法建立用户间信任度,文献[12]基于贝叶斯方法建立信任度,文献[13]则重点考量中继节点的协作策略。文献[14]为无线传感器网络提供一种有效的分布式网络节点信任度建立模型,同时保证传感器节点安全。文献[15]通过主观和客观相结合,观察节点的历史行为,用具体信任度评价值表示信任等级的高低,信任值随节点行为动态变化。

现有对用户信任关系之间的研究基本没有落实到物理层,也没有体现中继协作行为的具体效果,对用户身份的评估不够准确。中继协作用户转发的行为效果即所获得的信道容量增益是随瞬时信道状态而变的,每次通信都不相同,由此产生的贡献必然不同,只有将用户的贡献与物理层的信道状态联系在一起,才能更直观、准确地体现网络中用户的历史行为,也更有利于判别用户身份。本文将用户间信任度评价方法与用户协作通信得到的信道容量增益相结合,提出一种新的信任度评价方法,更直接地体现网络中用户历史行为对网络作出的贡献,从而使用户的通信质量保持在较高水平。

1 用户间信任度评价方法

假设在多用户通信网络中存在 N 个用户,如图 1 所示。发送用户与接收用户之间的通信可以通过直接链路(直线)或者间接链路(虚线)进行,在中继用户协作下的间接链路会为发送用户带来额外的信道容量增益,改善通信效果和用户体验。

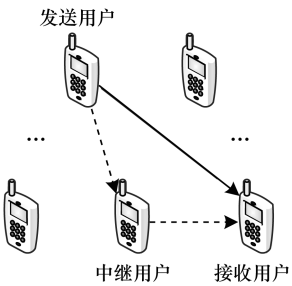

图 1 N 节点多用户通信网络通信路径

为了简化表达,发送用户用 S 表示,中继用户用 R 表示,接收用户用 D 表示。假设 S 到 D、S 到 R 以及 R 到 D 之间的信道增益分别为 h_{SD},h_{SR} 以及 h_{RD},信道噪声分别用 n_1,n_2 和 n_3 表示,都是均值为 0、方差为 σ^2 的加性高斯白噪声。

如果 S 选择通过直接链路与 D 进行通信时,设其发送信号为 x,发送功率为 P_S,则 D 接收到的信号为:

$$y_D = \sqrt{P_S}h_{SD}x + n_1 \tag{1}$$

因此,直接链路上的信道容量为:

$$C_{\text{direct}} = \text{lb}\left(1 + \frac{P_S \mid h_{SD} \mid^2}{\sigma^2}\right) \tag{2}$$

如果 S 选择间接链路与 D 进行通信,R 接收到 S 发送信号 x 之后进行解调并译码,采取一定的纠错手段降低误码率。然后将译出的正确信号重新编码发送给 D,因此该通信过程需要 2 个时隙。在第一个时隙,S 发送、R 接收,此时 R 接收信号为:

$$y'_R = \sqrt{P_S}h_{SR}x + n_2 \tag{3}$$

在第 2 个时隙内,R 对接收信号 y'_R进行解码并转发信号 x,发送功率为 P_R,此时 D 接收信号为:

$$y'_D = \sqrt{P_R}h_{RD}x + n_3 \tag{4}$$

文献[16]在译码转发模式下,对带直传和不带直传的 2 种多节点协作中继通信中信道容量的上下限进行了详细的分析和研究。在有限功率情况下,分析信道容量与中继节点数目之间的关系,给出容量随中继节点数目增加而提高所需的条件。理论分析和仿真结果证明:源到中继的信道条件较好时,只有当增加的新链路性能优于现有链路的平均值时才能提高信道容量。

根据文献[16]结论可知,三节点中继系统间接链路的信道容量上限为:

$$C_{\text{relay}} \leqslant \min\left\{\text{lb}\left(1 + \frac{P_S \mid h_{SR} \mid^2}{\sigma^2}\right), \text{lb}\left(1 + \frac{P_R \mid h_{RD} \mid^2}{\sigma^2}\right)\right\} \tag{5}$$

因此,相比于直接链路,通过中继转发可以为发送用户带来的最大信道容量增益为:

$$\begin{aligned}\Delta C &= C_{\text{relay}} - C_{\text{direct}} \\ &= \min\left\{\text{lb}\left(1 + \frac{P_S \mid h_{SR} \mid^2}{\sigma^2}\right), \text{lb}\left(1 + \frac{P_R \mid h_{RD} \mid^2}{\sigma^2}\right)\right\} \\ &\quad - \text{lb}\left(1 + \frac{P_S \mid h_{SD} \mid^2}{\sigma^2}\right)\end{aligned} \tag{6}$$

定义 1 中继用户协作发送用户通信得到的信道容量增益 ΔC 定义为中继用户对于发送用户的当前贡献。拒绝协作的中继用户对于发送用户的贡献为 0。中继协作发送用户多次通信得到的信道增益总和称为历史总贡献,用 C 表示。

定义 2 在 N 个用户的多用户网络中,用户 j 的信任值定义为该用户当前时刻对于其他所有用户历史总贡献的总和,即:

$$T_j = \sum_{i \neq j}^{N} C_i \tag{7}$$

中继用户的历史总贡献体现了该用户的历史行

为,多次协作其他用户将为该中继带来较高的历史总贡献,由此也体现出该用户的可信度比较高,身份更加可靠。该中继对于其他所有用户的历史总贡献之和,即可得到该用户全部历史行为,以此全面体现该用户的信任值。

当用户为其他用户转发消息作出贡献时,需要消耗自身能量和计算资源,因此,为保证自身的性能,所有的用户一般只愿意接收网络资源而不愿意共享自身的资源和计算功能。此时,网络中的用户不愿意彼此帮助,这种自私行为降低了网络的吞吐量。因此,激励自私用户参与协作、共享资源以提高通信系统性能是目前无线网络物理层安全领域重要的研究内容之一。

2　本文机制

为了解决以上问题,本文提出了一种基于信任度的自私用户协作激励机制。首先,网络中所有用户的初始信任值设置为 0。之后,随着为其他用户提供转发作出贡献,信任值逐渐增加,拒绝转发的用户信任值不变。信任值高的用户更易于得到其他用户的协作,信任值低的用户被认为是自私用户,其他用户将拒绝为之提供转发服务。因此,为了获得其他用户协作转发带来的网络性能增益,各用户自身也将积极参与协作,为其他用户转发信息。该方法激励了网络中自私用户的协作行为,一定程度上提高了网络性能增益。

2.1　用户协作收益

网络中的全部用户在没有通信需求时都可以作为潜在中继用户,都可能为其他有通信需求的发送用户转发信息。用户根据自身在协作中是否获益来判断通信过程是否需要协作,不同身份的用户对是否协作的判决标准是不同的,下面分别从用户的2 个身份入手,分析其协作收益。

1)发送用户

网络中有发送需求的用户广播自己的协作请求,愿意与之进行协作组网的用户反馈该请求,发送用户计算协作通信中继链路的信道容量。假设有N 个用户响应发送用户的协作请求,则随后发送用户可以计算得到 N 个中继链路的信道容量为 $C_{\text{relay}}^{(1)}, C_{\text{relay}}^{(2)}, \cdots, C_{\text{relay}}^{(N)}$。发送者选择贡献最大的中继进行协作,此时为了防止某一个中继负载过大,发送者以概率 P 选择贡献最大的中继进行协作组网,以$(1-P)$的概率从其他中继中选择来进行负载均衡,如表 1 所示。

表 1　N 个中继被选中概率

中继	选中概率
$\max\{C_{\text{relay}}^{(1)}, C_{\text{relay}}^{(2)}, \cdots, C_{\text{relay}}^{(N)}\}$	P
其他	$(1-P)/(N-1)$

由此得到发送用户选择到中继协作时的信道容量用均值表示为:

$$C_{\text{relay}} = P \cdot \max\{C_{\text{relay}}^{(1)}, C_{\text{relay}}^{(2)}, \cdots, C_{\text{relay}}^{(N)}\} + (1-P)\left(\sum_{i=1}^{N} C_{\text{relay}}^{(i)} - \max\{C_{\text{relay}}^{(1)}, C_{\text{relay}}^{(2)}, \cdots, C_{\text{relay}}^{(N)}\}\right) / (N-1)$$

协作通信带来的信道增益 ΔC 为:

$$\Delta C = C_{\text{relay}} - C_{\text{direct}}$$

协作完成之后,发送用户更新中继对自己的贡献:

$$\Delta C(t+1) = \Delta C(t-1) + \Delta C(t)$$

其中,$\Delta C(t-1)$,$\Delta C(t+1)$分别表示更新前和更新后中继对该发送用户的贡献值。

2)中继用户

没有通信需求的用户接收到发送用户的协作请求之后,立即向网络中其他所有用户请求发送用户对其的贡献,并由式(7)计算得到发送用户 j 的信任值 T_j。同时,每个用户都存储自身对其他用户的贡献,由此可以得到自身信任值 T。

中继用户通过比较 T_j 和 T 来决定是否要参与协作:如果 $T_j \geqslant T$,则中继用户倾向于参与协作,参与概率为 $Q(0.5 < Q \leqslant 1)$,拒绝协作概率为 $\bar{Q} = 1 - Q$;反之 $T_j < T$ 时,中继用户倾向于不协作,此时拒绝协作的概率为 Q,参与协作的概率为 $\bar{Q}$。综上,中继用户愿意参与协作的判决条件如表 2 所示。可以看出,如果中继参与协作,为发送者带来的信道增益均值为 $Q \cdot \Delta C + \bar{Q} \cdot \Delta C$,即 ΔC。

表 2　中继用户决策及发生概率

ΔT	中继决策	概率	信道增益
$\Delta T \geqslant 0$	参与	Q	ΔC
	不参与	$\bar{Q}$	0
$\Delta T < 0$	参与	$\bar{Q}$	ΔC
	不参与	Q	0

对于网络中的用户,能量和计算资源有限且宝贵,如果参与协作则要消耗自身资源为其他用户服务,因此在没有任何激励措施的情况下,绝大多数理性用户都会拒绝参与协作。在本文所提的信任度的限制下,如果发送用户信任值 T_j 低于中继信任值 T,那么对于中继用户来说,协作会导致自身资源消耗,拒绝协作可以节约资源也不会对自身利益造成损害,因此,中继用户更加倾向与拒绝协作请求;但是当发送用户的信任值 T_j 高于中继自身的信任值 T 时,中继用户将面临风险:在两者身份交换的场景中,中继作为发送用户提出协作请求时遭到其他中

继用户拒绝的概率更大,影响通信质量和用户体验,因此,中继用户更倾向于与发送用户协作,以提高自身信任值,降低被拒的风险。

2.2 协作组网过程

经过以上分析可见,本文提出的基于信任度的自私用户协作激励机制能够增加中继用户的协作概率。当多用户网络中有用户产生通信需求时,具体的协作组网过程如下:

1)网络中一个用户 j 产生通信需求,向网络中空闲用户发出协作邀请。

2)收到邀请的空闲用户向网络中所有用户请求用户 j 和自身的贡献,计算得到信任值 T_j 和 T 并进行比较:

(1)如果 $T_j < T$,接收消息用户倾向于拒绝协作邀请,拒绝的概率为 Q,但仍有 $\bar{Q}$ 的概率接收协作邀请;

(2)反之,如果 $T_j \geqslant T$,用户以概率 Q 积极参与协作转发,以 $\bar{Q}$ 的概率拒绝协作。

3)用户 j 遍历计算潜在中继协作贡献,以 P 概率选择贡献最大的中继,以(1 - P)的概率选择其他中继进行协作。

4)通信完成后,用户 j 更新协作中继贡献。

3 仿真结果分析

本节使用 Matlab 对所提的自私用户协作激励机制进行仿真验证其有效性和可靠性。假设无障碍网络中有 5 对用户对,用户间的信道为瑞利衰落信道,同时信号传输受到大尺度衰落的影响。用户位置随机分布,但所有用户信道增益满足 $h_{SD} \sim CN(0, 0.001\ 2)$,$h_{SR} \sim CN(0, 0.001\ 5)$ 以及 $h_{RD} \sim CN(0, 0.001)$。为简单起见,令 $P = Q = 1$,噪声方差为 1,同时所有用户的发送功率都是 100 mW。

图 2 ~ 图 4 分别表示进行 10 次、100 次和 1 000 次通信时的信道容量以及用户信任值变化。

在图 2(a)中,无方案上、下限指的是不采用本文方案时,用户通过中继协作或无协作情况下直接发送等所有通信可能性中,可以得到的信道容量的最大值和最小值,这是在用户之间无私提供协作的情况下得到的结果。对于自私用户来说,通信的信道容量水平将接近下限。而对于本文所提的激励自私用户参与协作的方案来说,可以看到,信道容量接近并可以达到容量界上限,这为用户的通信质量带来一定的提高。在图 2(b)中,可以清楚看到:1)在某次通信之后作为中继的用户自身信任值的提高;2)在某次通信之后如果所有用户信任值都没有变化(如第 4 次通信),那么说明本次通信中的发送用户没有通过中继协作通信,而是与接收用户直接链路通信;3)信任值低的用户积极参与协作,信任值高的用户拒绝协作。

图 3(a)与图 2(a)结论相同,都体现了本文方案的有效性以及对通信质量的提升。从图 2(b)中可以看到,5 个用户的信任值交替上升,信任值低的用户积极参与协作,证明了本文方案能够很好地促进自私用户积极协作。

从图 4(a)中可以看到,在本文方案下进行的通信,大多数信道容量接近容量界上限,1/1000 的几率信道容量较低,体现了本文方案的有效性。

从图 4(b)中可以看到,5 个用户的信任值非常接近,并且都在不断上升。这体现了在本文所提自私中继协作激励机制作用下,所有自私用户都参与协作提升自身信任值,同时使得网络中用户的信任值比较均衡。如果出现信任值较低的用户,那么为了能得到其他用户的协作,他必须提升自身信任值,就需要该用户自身参与协作以提升自己的信任值;反之,如果出现信任值高的用户,自身可以得到其他用户协作,但是拒绝协作其他用户,其信任值将维持不变,就会很快被其他用户超越,使其信任值相对较低,从而对其协作造成威胁。

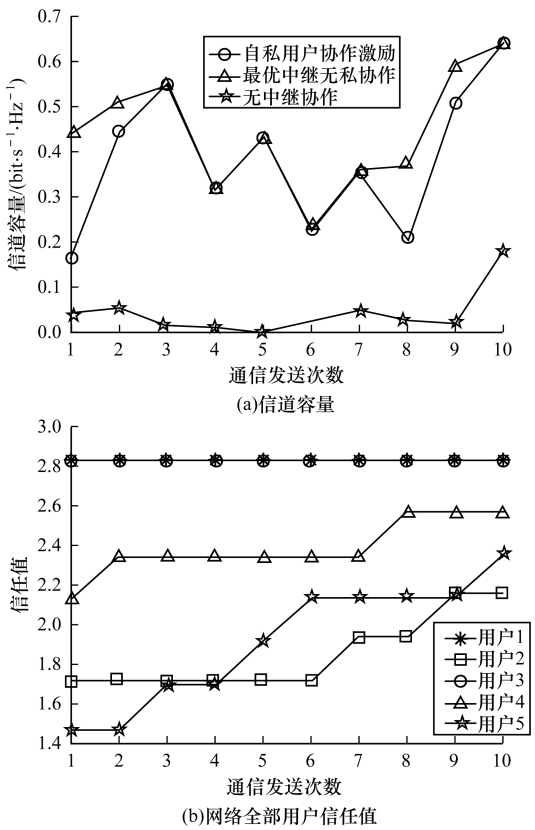

图 2 10 次通信时的信道容量及用户信任值变化

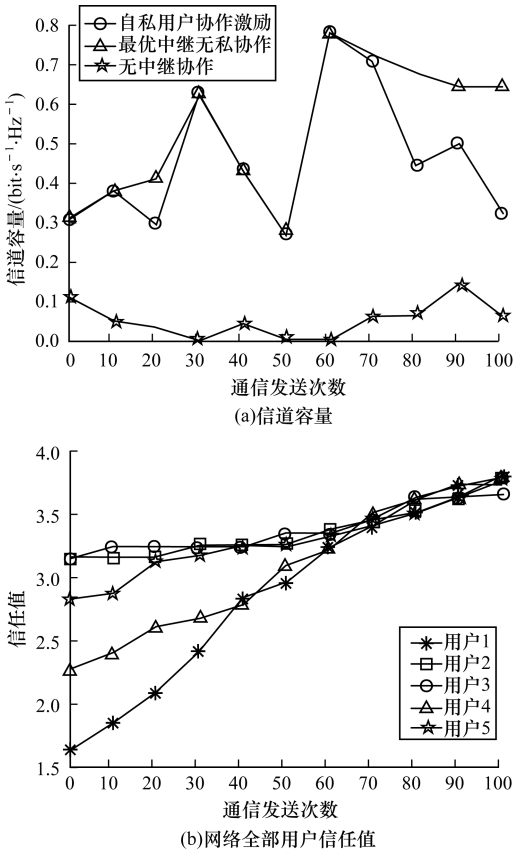

图 3　100 次通信时的信道容量及用户信任值变化

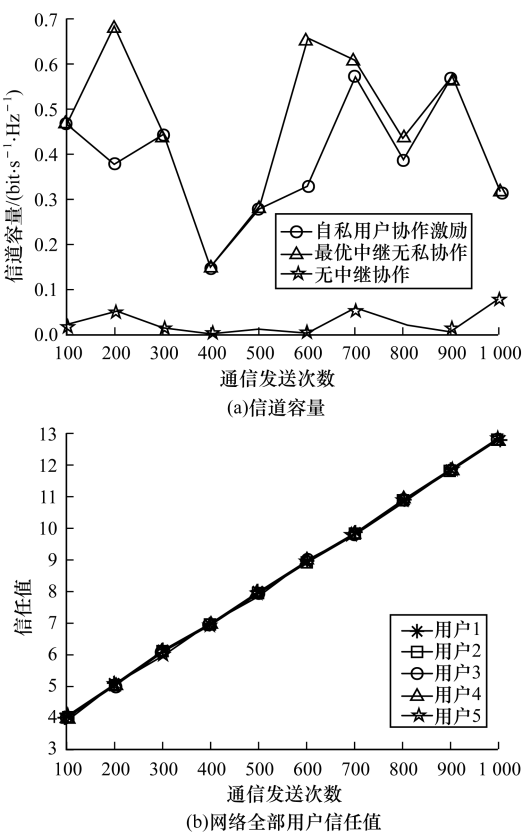

图 4　1 000 次通信时的信道容量及用户信任值变化

P 值越小,表示为了均衡中继负载,发送者以越大的概率选择非最优中继。从图 5 中可以看出,随着 P 值减少,用户信道容量随之降低。

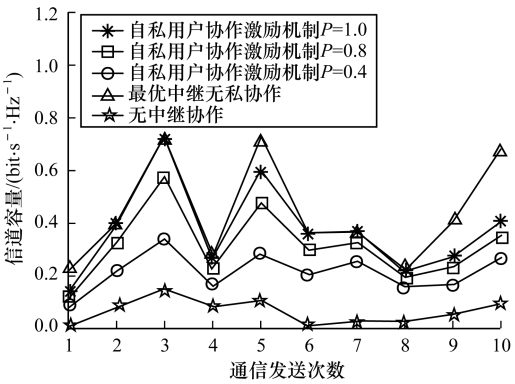

图 5　参数 P 对用户通信性能增益的影响

4　结束语

在多用户网络中,用户之间通过相互协作扩大通信范围,提升通信质量和用户体验。但是用户终端若受资源、能耗等方面限制不愿意为其他用户转发,则会影响网络性能。为激励自私用户积极参与协作,本文提出一种基于用户间信任度评价的协作激励机制。首先为网络中所有用户定义一个信任度初始值,随着通信的发生,信任值动态变化。信任值较高的用户拒绝协作,信任值较低的用户必须积极协作才能提高自身信任值以获取其他用户的协作。经过几次通信后,原本拒绝协作的用户信任值不变,参与协作的用户信任值越来越高。因此,用户之间的信任值将发生交替上升,彼此促进参与协作,提高自身信任值。仿真实验证明了本文机制的有效性。下一步将对该机制进行完善,加入安全速率等更多考量指标,在保证通信质量的情况下提升通信安全性能,实现用户更优质的通信。

参考文献

[1] Li Zexu,Li Yong,Wang Jun,et al. Resource Allocation for Multiuser Two-way Full-duplex Relay Networks[C]// Proceedings of IEEE International Conference on Communications. Washington D. C.,USA:IEEE Press,2015:3299-3304.

[2] Liu Yuan,Tao Meixia,Huang Jianwei. Auction-based Optimal Power Allocation in Multiuser Cooperative Networks[C]//Proceedings of IEEE Global Telecommunications Conference. Washington D. C.,USA:IEEE Press,2011:1-5.

[3] Cho P,Hong Y,Kuo J. A Game Theoretic Approach to Eavesdropper Cooperation in MISO Wireless Networks[C]//Proceedings of IEEE International Conference on Acoustics,Speech and Signal Processing. Washington D. C.,USA:IEEE Press,2011:3428-3431.

(下转第 176 页)

参考文献

[1] 国家互联网应急中心. 2015 年 8 月互联网安全威胁报告[EB/OL]. (2015-09-23). http://www.cert.org.cn/publish/main/45/2015/20150923135135572858862/20150923135135572858862_.html.

[2] Antonakakis M, Perdisci R, Dagon D, et al. Building a Dynamic Reputation System for DNS[C]//Proceedings of USENIX Security Symposium. Washington D. C., USA: USENIX, 2010: 273-290.

[3] Ghafir I, Prenosil V. DNS Traffic Analysis for Malicious Domains Detection[C]//Proceedings of Conference on Signal Processing and Integrated Networks. Washington D. C., USA: IEEE Press, 2015: 613-618.

[4] Nazario J, Holz T. As the Net Churns: Fast-flux Botnet Observations[C]//Proceedings of Malicious and Unwanted Software MALWARE Conference. Washington D. C., USA: IEEE Press, 2008: 24-31.

[5] Guerid H, Mittig K, Serhrouchni A. Collaborative Approach for Inter-domain Botnet Detection in Large-scale Networks[C]//Proceedings of International Conference on Collaborative Computing: Networking, Applications and Worksharing. Washington D. C., USA: IEEE Press, 2013: 279-288.

[6] Bilge L, Kirda E, Kruegel C, et al. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis[C]//Proceedings of the 18th Annual Network & Distributed System Security Conference. [S. l.]: ISOC, 2011: 1-17.

[7] Zou Futai, Zhang Siyu, Rao Weixiong. Hybrid Detection and Tracking of Fast-flux Botnet on Domain Name System Traffic[J]. China Communications, 2013, 10(11): 81-94.

[8] 康 乐, 李 东, 余翔湛. 基于 SVM 的 Fast-flux 僵尸网络检测技术研究[J]. 智能计算机与应用, 2011, 1(1): 24-27.

[9] 张永斌, 陆 寅, 张艳宁. 基于组行为特征的恶意域名检测[J]. 计算机科学, 2013, 40(8): 146-148.

[10] Yadav S, Reddy A, Reddy A, et al. Detecting Algorithmically Generated Malicious Domain Names[C]//Proceedings of the 10th ACM SIGCOMM Conference. New York, USA: ACM Press, 2010: 48-61.

[11] 李青山, 陈 钟. Domain-flux 僵尸网络域名检测[J]. 计算机工程与设计, 2012, 33(8): 2915-2919.

[12] 张 鹏, 谢晓尧. 基于熵的二叉树多类支持向量机的漏洞分类[J]. 计算机应用, 2014, 34(11): 3283-3286.

[13] Rosen B E. Ensemble Learning Using Decorrelated Neural Networks[J]. Connection Science, 1996, 8(3/4): 373-384.

[14] Dietterich T G. The Handbook of Brain Theory and Neural Networks[M]. 2nd ed. Cambridge, USA: MIT Press, 2002: 110-125.

[15] Breiman L. Random Forests[J]. Machine Learning, 2001, 45(1): 5-32.

[16] Svetnik V, Liaw A, Tong C, et al. Random Forest: A Classification and Regression Tool for Compound Classification and QSAR Modeling[J]. Journal of Chemical Information and Computer Sciences, 2003, 43(6): 1947-1958.

[17] Prasad N, Patro K R, Naidu M M. A Gini Index Based Elegant Decision Tree Classifier to Predict Precipitation[C]//Proceedings of Modelling Symposium. Washington D. C., USA: IEEE Press, 2013: 46-54.

[18] Knauer U, Meffert B. Evaluation Based Combining of Classifiers for Monitoring Honeybees[C]//Proceedings of Conference on Applications of Computer Vision. Washington D. C., USA: IEEE Press, 2009: 1-6.

编辑 金胡考

(上接第 169 页)

[4] Wang Tianyu, Zhang Rongqing, Song Lingyang, et al. Power Allocation for Two-way Relay System Based on Sequential Second Price Auction[J]. Wireless Personal Communications, 2012, 67(1): 47-62.

[5] Walid S, Zhang Xiangyun, Behrouz M. Tree Formation with Physical Layer Security Considerations in Wireless Multi-hop Networks[J]. IEEE Transactions on Wireless Communications, 2012, 11(11): 1536-1276.

[6] 洪 颖, 黄开枝, 罗文宇, 等. 一种基于两次报价博弈机制的安全中继选择方法[J]. 信息工程大学学报, 2014, 15(5): 1671-1673.

[7] Manchala D W. E-commerce Trust Metrics and Models[J]. Internet Computing, 2000, 4(4): 476-487.

[8] 王 博, 陈训逊. Ad Hoc 网络中一种基于信任模型的机会路由算法[J]. 通信学报, 2013, 34(9): 92-104.

[9] Ahn J H, Lee T J. Multipoint Relay Selection for Robust Broadcast in Ad Hoc Networks[J]. Ad Hoc Networks, 2014, 17(1): 82-87.

[10] 袁禄来, 曾国荪, 王 伟. 基于 Dempster-Shafer 证据理论的信任评估模型[J]. 武汉大学学报: 理学版, 2006, 52(5): 627-630.

[11] Shankaran R, Varadharajan V, Orgun M, et al. Context-aware Trust Management for Peer-to-Peer Mobile Ad-hoc Networks[C]//Proceedings of the 33rd Annual IEEE Computer Software and Applications Conference. Washington D. C., USA: IEEE Press, 2009: 188-193.

[12] Wang Junshe, Li Xiaolong, Zhang Yun. Research of P2P Network Trust Model[C]//Proceedings of the 5th International Conference on Intelligent Human-machine Systems and Cybernetics. Nanjing, China: [s. n.], 2013: 70-73.

[13] Changiz R, Halabian H, Yu F R, et al. Trust Establishment in Cooperative Wireless Networks[C]//Proceedings of Military Communications Conference. Washington D. C., USA: IEEE Press, 2010: 1074-1079.

[14] Jiang Jinfang, Han Guangjie, Wang Feng, et al. An Efficient Distributed Trust Model for Wireless Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(5): 1228-1237.

[15] 周贤伟, 吴启武. 基于可信度的 MANET 路由协议综合评估[J]. 计算机工程, 2009, 35(6): 20-22.

[16] 黄 英, 魏急波, 雷 菁. 多节点协同中继信道容量分析及功率分配[J]. 解放军理工大学学报, 2012, 13(2): 119-123.

编辑 金胡考