

基于信誉推荐的 Ad Hoc 网络虫洞防御方案

郭华娟¹, 曹晓梅^{1,2}, 朱 杰¹

(1. 南京邮电大学 计算机与软件学院, 江苏 南京 210003;

2. 江苏省无线传感网高技术研究重点实验室, 江苏 南京 210003)

摘 要: 虫洞攻击是一种针对 Ad Hoc 网络路由协议的典型恶意攻击。两个恶意节点进行合谋协同攻击, 从而吸引大量数据包达到控制网络和紊乱路由机制的目的。为了解决这一问题, 提出信誉推荐算法—CRPFA (Credibility Recommended Path Flow Algorithm), 主要以三个步骤实现虫洞的防御, 包括信誉计算、节点聚类、节点推荐, 构建了新虫洞防御方法。该算法既不需要额外的硬件设备, 也不需要定位恶意节点具体位置, 且有效地克服了节点的自私性、欺骗性, 保证了数据包的安全传输。仿真结果表明, 该算法在传输距离、节点密度得到保证的情况下, 能够高效地防止恶意节点参加路由选择, 保证了数据包的有效传递。与 CERep 机制的仿真结果进行对比, 结果进一步验证了该方法的可行性和有效性。

关键词: Ad Hoc 网络; 虫洞攻击; 信誉; 聚类算法; 推荐值

中图分类号: TP31

文献标识码: A

文章编号: 1673-629X(2016)08-0083-05

doi: 10.3969/j.issn.1673-629X.2016.08.018

A Wormhole Defense Method for Ad Hoc Network Based on Credibility Recommendation

GUO Hua-juan¹, CAO Xiao-mei^{1,2}, ZHU Jie¹

(1. College of Computer and Software, Nanjing University of Posts and Telecommunications,
Nanjing 210003, China;

2. Key Laboratory of High-tech Wireless Sensor Network in Jiangsu Province, Nanjing 210003, China)

Abstract: The wormhole attack is a typical malicious attacks against Ad Hoc routing protocols. Two malicious nodes are conspiring to co-ordinated attack, attracting a large number of data packets to achieve the objective of controlling network and disordering routing mechanism. In order to solve this problem, a CRPFA (Credibility Recommended Path Flow Algorithm) is proposed which mainly divides into three steps to achieve the defense of the wormhole, including credit calculation, node aggregation and recommendation, construction of the new wormhole defense. This algorithm does not need additional hardware devices, also not need to locate malicious node location, and effectively overcomes the selfish and deceptive node, ensuring the safety of data packet transmission. The simulation results show that on the condition of guaranteeing in the transmission distance and the density of nodes, the algorithm proposed can efficiently prevent malicious nodes to participate in the routing and ensure effective transmission of the data packets. Compared with the CERep mechanism, the results show that the feasibility and validity of the method is further verified.

Key words: Ad Hoc network; wormhole attack; trust; aggregating algorithm; recommended value

0 引 言

Ad Hoc 网络是一种多跳的、无中心的、自组织无线网络, 又称为多跳网 (Multi-hop Network)。开放式的网络结构、有限的节点资源、动态的网络拓扑等特性, 使得 Ad Hoc 网络容易遭受各种各样的攻击^[1]。虫洞攻击^[2-3] 是一种针对路由协议发起的攻击, 特别是那些依赖接收对方的广播报文进行邻居探测的路由

协议, 是众多攻击中危害较为严重的一类。这种合作式攻击是一种通过建立高质量、高速率的私有通道, 将虫洞一端收集到的数据包在虫洞的另一端重放, 进行秘密通信并反复转发、篡改数据包的行为。近年来, 尽管许多研究人员根据路由协议提出了应对虫洞攻击的检测机制和防御机制, 但检测机制过分依赖同步时钟、GPS 等硬件设备, 而防御机制则忽视节点信任的主观

收稿日期: 2015-09-06

修回日期: 2015-12-23

网络出版时间: 2016-08-01

基金项目: 国家自然科学基金青年基金 (61202353); 国家自然科学基金资助项目 (60873231)

作者简介: 郭华娟 (1990-), 女, 硕士, 研究方向为网络信息安全; 曹晓梅, 副教授, 博士, 研究方向为无线网络安全、传感器网络安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20160801.0842.004.html>

性、自私性,使其在开放的网络环境下不成立。

文中提出基于信誉推荐路径流算法 (Credibility Recommended Path Flow Algorithm, CRPFA), 在不同的时间片内监测并统计链路层、网络层交互事件的满意度, 结合贝叶斯算法不断修正结果并发现稀疏矩阵, 利用聚类使整个通信网络区域分割成零散的安全簇, 并在簇区域内选择高推荐值的节点参加路由选择, 最终形成安全路径流。该算法既不需要额外的硬件设备, 也不需要定位恶意节点, 且有效克服了防御方法的单一性和节点的自私性、欺骗性, 保证了数据包的安全传输。

1 相关工作

国内外有关虫洞检测和虫洞防御的研究得到了不断发展, 也提出了较多的方案, 在封闭式小型网络环境中能够检测出虫洞的存在, 大致方法主要分为以下几种:

(1) 检测机制。

文献[4]提出一种 GPSR 方案, 在硬件设备 GPS 的基础上提出新算法, 网络中的拓扑频繁变化, 虽然 GPSR 可以使用本地拓扑信息快速找到正确的新航线, 但是需要借助硬件设备。Hu Yih-Chun 等^[5]提出一种称为“数据包限制”(packet leashes)的机制, 要求所有网络节点必须要具有严格同步的时钟和时间限制, 通常在几微秒甚至千万之一秒内, 并采用认证协议来检测虫洞攻击目的节点。目的节点可以根据接收时间和发送时间监测数据包传输的距离是否太长或者在数据包内设置一个有效时间, 超出这个有效时间, 则认为存在虫洞。文献[6]中提出一种利用节点路由表信息检测虫洞的方案。该方案通过链路使用频率统计和邻居节点验证的机制来找到虫洞链路, 但只适合小型网络中, 有一定局限。Deworm 方案^[7]利用节点邻居查询的路由信息来判定虫洞的存在, 但虫洞检测会带来较高的时间延迟和能量消耗。

(2) 信任防御机制。

通过收集和分析用户的历史行为来预测他们在未来的交互中可能发生的行为, 从而为交互对象的选择提供一定的依据, 成功规避风险。目前防御虫洞攻击的方法主要有五种: 包封装的方式、使用额外信道的方式、高能量传输方式、包接力的方式、使用协议偏差的方式^[8-10]。

EigenTrust^[11]、ManagingTrust^[12]和 LimitedReputation^[13]都采用服务信任的方法。这类方法没有专门的推荐可信度计算方法, 用提供服务的信任度来代替推荐可信度。其局限性在于, 节点可以通过提供高质量的服务维护高的信任值但同时不诚实节点操作也会颠

覆信誉系统。洪亮等^[14]提出基于邻居信任评估的虫洞防御机制, 节点之间基于直接交互经验形成直接信任评价, 方案中通过重新定义邻居的概念, 强调邻居作为节点信息转发的重要性, 引入 Marsh 信任模型, 将邻居的以往表现作为信任评估的经验来源, 并通过公式对邻居关系做出判定。虽然该机制能够一定程度上防御恶意节点参加路由选择, 但忽视了信任具有主观性、不确定性、历史经验依赖性、不对称性、动态性的缺点。

DevelopTrust^[15]和 Huynh^[16]提出的加权算法, 比较节点提供的推荐和实际交互结果之间的差异, 若差异越小, 则认为可信度越高。常俊胜等提出一种可信度增强的信誉机制 (CERep)^[17]。节点基于自身的经验产生的直接信任评价, 包含直接信任评价价值和关于此评价值的信心因子两部分。在此基础上, 提出了新的基于信誉的信任评价算法和推荐可信度计算模型, 并给出了信誉机制的分布式实现策略。但这类方法中节点的推荐基于少数的交互或者目标节点的服务质量变化很大, 导致诚实的推荐节点可能会被错误地划分为不诚实节点。

与 CRPFA 相比, 无论是基于同步时钟的“数据包限制”(packet leashes)方法, 还是基于时间和空间的检测方案, 虽然都能够准确定位恶意节点, 但在检测过程中对硬件要求较高; 而新阶段的信任防御机制, 往往难以应对不诚实推荐, 机制单一旦在开放性网络环境下总是不成立的。

2 信誉推荐路径流方案 (CRPFA)

2.1 信誉计算

文中提出的 CRPFA 算法主要由三个部分组成: 信誉计算、节点聚类和节点推荐路径流。基于信誉推荐的 CRPFA 考虑节点之间的两种信任关系: 全局信誉关系和局部信誉关系。局部信誉值的建立基于节点自身的经验, 全局信誉值来源于局部信誉关系。

每个节点在特定时间点会接收不同邻节点转发的数据包, 同时, 在某一段时间片内也可以接收不同邻节点发来的数据包, 所以在不同的时间片内分别统计链路层和网络层中的数据帧和控制帧。为了得到每个节点准确的局部信任值, 通过测试包服务反馈评价, 并为每个节点设置一张数据结构为三元组的表 (R_{ij}^t, S_{ij}, t_i), 分别代表交易局部信誉值、满意度及时间片。同时为了提高数据的可靠性, 利用贝叶斯算法对收集的数据进行概率分析, 不断修正满意度 (作为节点 i 与节点 j 总共交互时间的满意度)。这里的满意度定义为:

$$S_{ij} = \text{sat}(i, j) - \text{usat}(i, j) \quad (1)$$

接收测试数据包的节点 i 对发送测试包的节点 j

的局部信誉值 R_{ij} 为:

$$R_{ij}^n = (1 - a) * R_{ij}^{n-1} + a * S_{ij}^n, 0 \leq R_{ij} \leq 1 \quad (2)$$

为了保证数据的客观性设置 $a = 0.5$, 在移动 Ad Hoc 的网络环境中, 每个节点根据多次交易来评价对方的信誉, 多次迭代计算局部信誉值 R_{ij} , 但在交易过程中, 总是存在数据篡改、不真实和不可靠等现象。在局部信誉值的基础上, 根据不同时间片、不同节点间交互的事件定义归一化的局部信誉值:

$$C_{ij} = \begin{cases} \frac{\max(R_{ij}, 0)}{\sum_j \max(R_{ij}, 0)}, & \text{if } \sum_j \max(R_{ij}, 0) \neq 0 \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

获得全局信誉矩阵:

$$C = \begin{pmatrix} 0 & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & 0 \end{pmatrix} \quad (4)$$

2.2 节点聚类

节点的自私性导致节点之间一旦确定相关身份之后不愿主动去刷新整个信誉系统, 甚至还会被恶意节点诋毁。为了增加节点的可信度, 利用信誉矩阵进行聚类分发。

邻域: 给定对象节点半径 r 内的区域称为该对象的 r 邻域。

直接信誉可达: 给定一个节点集合 D , 如果 p 在 q 的 r 邻域内, 且 q 是一个核心节点对象, 则认为节点 p 从节点 q 出发是直接信誉可达的。

信誉可达: 对于节点集合 D , 如果存在一个节点链 $p_1, p_2, \dots, p_n, p_1 = q, p_n = p$, 对于 $p_i \in D (1 \leq i \leq n)$, p_{i+1} 是从 p_i 关于 r 的直接信誉可达, 则节点 p 是从节点 q 关于 r 信誉可达的。

信誉相连: 如果存在节点 $o \in D$, 使节点 p 和 q 都是从 o 关于 r 信誉可达的, 那么节点 p 到节点 q 是关于 r 信誉相连的。

设 $M_{(i)} (i = 1, 2, \dots, n)$ 是 $D = \{d_1, d_2, \dots, d_n\}$ 区域上的动态节点集, i 被视为自变量。通常取 $M_{(i)}$ 为一个散列分布的函数集合, 由全局信誉矩阵组成, 隶属函数满足:

$$C_{ij} = \frac{\max(R_{ij}, 0)}{\sum_j \max(R_{ij}, 0)} \neq 0, \text{ 当 } \sum_j \max(R_{ij}, 0) \neq 0$$

信誉可达是直接信誉可达的传递闭包, 并且这种关系是非对称的, 然而, 信誉相连是对称关系, 所以需要通过信誉聚合找到信誉相连节点的最大集合。

2.3 推荐路径流

信誉值的计算得出各个节点信誉值矩阵, 并完成节点的聚类, 形成无数个簇区域。此时, 以上计算是在假设每次评价都是诚实的基础上进行的, 但在现实情

况下, 评价可能存在不诚实或恶意的现象。为了避免虫洞攻击, 利用推荐值计算公式推荐节点参加路由选择。在与其他服务评价对比中发现服务评价的可靠性与其通信区域内的信誉直达节点、通信块及所有节点具有一定的线性相关性, 于是提出节点推荐值 (Recommendation Value, RV) 公式:

$$RV = |C| - (RVC/N - \text{Chunk}/N) * 100\% \quad (5)$$

其中, RVC 为以中心节点为核心的簇区域内的节点数; N 为 r 通信区域内的所有节点数; Chunk 为聚类完成后的数据块, 只有选择推荐值最靠前的节点参与路由选择。

具体实例中, 区域 1、区域 2 和区域 3 是分别以 p_1 、 p_4 、 p_6 为中心的通信区域, 阴影部分则是核心节点的簇区域, 在簇区域里选择节点的具体步骤为: 第一步在核心节点的通信范围内寻找, 第二步在核心节点的簇区域内寻找。通过推荐值的计算, 当存在两个节点选择时, 选择推荐值最大者为下一跳节点参与路由选择, 最终该实例的路径流为 $p_1 - p_2 - p_4 - p_5 - p_6$ 。

3 仿真实验与结果分析

为了验证 CRPFA 在 Ad Hoc 网络下对虫洞攻击的防御效果, 仿真实验在 Windows 7+MATLAB 平台上完成。通过多次测试选择合适传输半径和节点密度, 在合适环境参数下, 从传输速率、能量消耗、动态性几个方面来评估 CRPFA 在 AODV 路由协议应对虫洞攻击的作用并与 CERep 机制的仿真结果进行对比。首先, 整个网络模拟场景大小为 $400 \text{ m} \times 500 \text{ m}$, AODV 协议下的节点随机分布各个节点, 其移动速度为 10 m/s , 运动方向随机, 数据包大小为 1 024。

节点密度为每百平方米 12 个节点, 10 个普通节点 ($P_1 \sim P_{10}$), 2 个恶意节点 ($N_1 \sim N_2$), 恶意节点相互之间执行虫洞攻击。节点在仿真环境下, 当 r 取不同值时, CRPFA 检测链路成功率和误判率的变化如表 1 所示。

表 1 仿真结果(1)

次数	半径 r/m	成功率/%	失败率/%
1	30	88	12
2	60	96.1	3.9
3	90	92.4	7.6
4	120	85.5	14.5
5	150	70.4	29.6

当 r 取值越大, 链路形成的成功率就越低, 失败率就越高, 如图 1 所示。当 r 取值大于 120 时链路形成成功率普遍低于 90%, 由于通信距离的加大, 增加了通信成本, 无论是在时间上还是在数据传输能力上都增

加了通信成本。所以当通信距离介于 60 ~ 150 之间,链路的成功率一直维持在一个较高水平,同时节约了时间与通信成本。

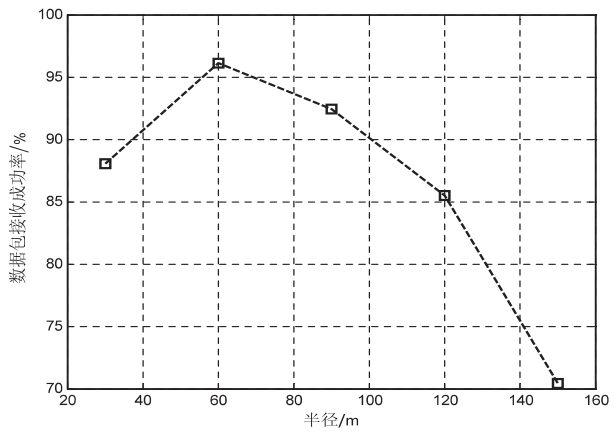


图 1 数据包接收成功率

当确定 $r = 60\text{ m}$ 和恶意节点 (N_1, N_2) , 以节点密度为变量, 比较数据包传输速率。当密度 s 取不同值时, 应用 CRPFA 节点的传输速率变化如表 2 所示。

表 2 仿真结果(2)

次数	通信半径 r/m	密度 $s\text{ (} n/\text{m}^2 \text{)}$	传输速率
1	125	100/11 304	不正常
2	125	200/11 304	不正常
3	125	300/11 304	不正常
4	125	400/11 304	不正常

由表 2 可知, 在存在虫洞攻击的情况下, 传输速率都无法呈现出正常状态, 所以研究相应防御机制是否能够有效防御虫洞攻击可以通过对比数据包的传输速率来确定。当通信半径 $r = 60$, 密度 $s = 400/11\ 304$ 时, 比较两者之间的传输速率、能力消耗和动态性, 如图 2 ~ 4 所示。

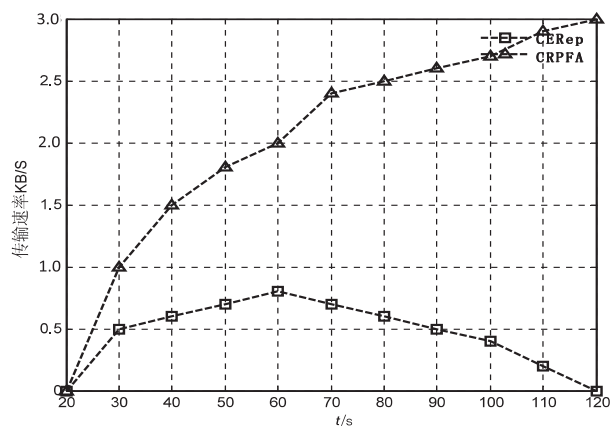


图 2 传输速率

由图 2 可知, CRPFA 下的 AODV 在传输速率上呈现持续上升的态势, 而没有应用该算法的协议接收的流量在 120 s 后显现为 0 的状态, 由于没有相关的反馈机制和监测机制, 这一错误无法纠正, 致使数据包的传

输一直为零。在一组恶意节点攻击的影响下, 网络的加载量不断增加、恶性循环。应用 CRPFA 的节点传输速率呈持续增长趋势, 也就意味着在 AODV 协议下, 目的节点都可以找到一条正确到达目标节点的路径, 起到防御虫洞攻击的作用。

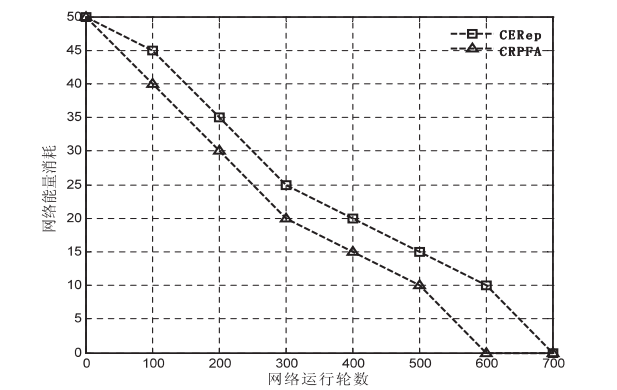


图 3 网络能量消耗

从图 3 可以看到, 随着时间的增加, 能量的消耗呈现降低的趋势, 相比 CERep 机制有更好的表现效果, 有效遏制了恶意节点对 Ad Hoc 网络能量方面的巨大威胁, 在消耗少量能量的前提下做到了对网络安全的提升, 同时验证了 CRPFA 可以有效防范节点利用间接信息进行诽谤攻击。

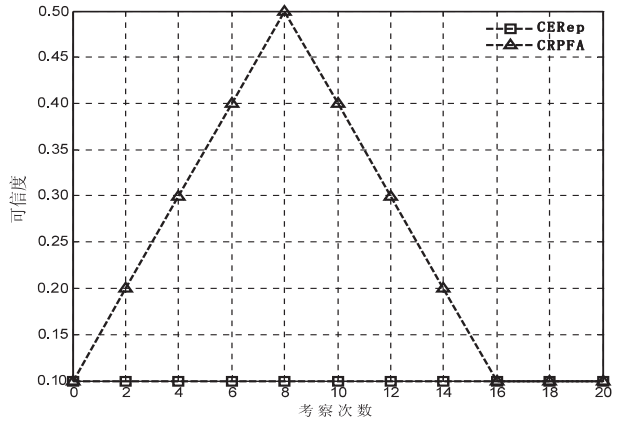


图 4 可信度考察

从图中可以看到, 节点的初始信誉值为 0.5, 通过异常行为的累计, 逐渐将节点可信度降低, 并且这个过程是一个加速的过程, 而 CERep 机制对于可信度的考察结果却是一成不变的。说明 CRPFA 对于任何随机进行恶意诽谤的恶意节点, 其可信度随着行为性质的变化而动态变化, 能够有效地防范恶意节点的诽谤行为。

4 结束语

虫洞攻击是目前影响移动 Ad Hoc 网络发展的重大威胁之一。针对目前探测虫洞的方法过于注重地理位置而忽视信誉的表现, 文中提出 CRPFA 防御移动

Ad Hoc 网络中的虫洞攻击,综合局部声誉和全局声誉的优点,结合权重机制区别对待各个节点,构建新的信誉计算算法。为了保证节点信誉的可信度、减少通信量与数据量,应用贝叶斯算法和信誉聚合算法,以源节点为中心,在其簇区域内选择误差范围内的可直接通信节点。在仿真中观察 AODV 路由协议下 CRPFA 对虫洞节点的影响,仿真结果表明,邻居信誉值防御虫洞攻击是有效的。

该防御方法的显著优点在于动态防御、聚类速度快,在降低节点对硬件要求的同时,准确找出安全链路,大大减少了维护节点信息而产生的开销,具有较高的效率和鲁棒性。随着 Ad Hoc 网络的不断发展和日益成熟,它将会被部署在更为特殊和复杂的应用环境中,在安全链路得到满足的情况下,定位恶意节点也显得更加重要,因此提出一种新颖的方案探测恶意节点的具体位置,并保证安全路由的需求也变得尤为突出。

参考文献:

- [1] Yang Hao, Luo Haiyun, Ye Fan, et al. Security in mobile ad hoc networks: challenges and solutions [J]. IEEE Wireless Communications, 2004, 11(1): 38–47.
- [2] Hu Y, Perrig A, Johnson D B. Wormhole attacks in wireless networks [J]. Selected Areas in Communications, 2006, 24(2): 370–380.
- [3] Mahajan V, Natu M, Sethi A. Analysis of wormhole intrusion attacks in MANETS [C]//Proc of military communications conference. [s. l.]: IEEE, 2008: 1–7.
- [4] Brad K, Kung H T. GPSR: greedy perimeter stateless routing for wireless networks [C]//Proceedings of the 6th annual international conference on mobile computing and networking. Boston, Massachusetts, USA: [s. n.], 2000: 243–254.
- [5] Hu Yih-Chun, Perrig A, Johnson D B. Packet leashes: a defense against wormhole attacks in wireless networks [C]//Proc of twenty-second annual joint conference of the IEEE computer and communications. [s. l.]: IEEE, 2003: 1976–1986.
- [6] Khan Z A, Islam M H. Wormhole attack: a new detection technique [C]//Proc of international conference on emerging technologies. Islamabad: IEEE, 2012: 1–6.
- [7] Hayajneh T, Krishnamurthy P, Tipper D. DeWorm: a simple protocol to detect wormhole attacks in wireless ad hoc networks [C]//Proc of 2009 third international conference on network and system security. [s. l.]: IEEE Computer Society, 2009: 73–80.
- [8] Mármol F G, Pérez G M. TRMSim-WSN, trust and reputation models simulator for wireless sensor networks [C]//Proc of IEEE international conference on communications. [s. l.]: IEEE, 2009: 1–5.
- [9] Al-Karaki J N, Kamal A E. Routing techniques in wireless sensor networks: a survey [J]. IEEE Wireless Communications, 2004, 11(6): 6–28.
- [10] Hales D. From selfish nodes to cooperative networks—emergent link-based incentives in peer-to-peer networks [C]//Proc of fourth international conference on peer-to-peer computing. [s. l.]: IEEE, 2004: 151–158.
- [11] Kamvar S D, Schlosser M T, Garcia-Molina H. EigenRep: reputation management in p2p networks [C]//Proceedings of the twelfth international world wide web conference. Budapest, Hungary: [s. n.], 2003: 123–134.
- [12] Aberer K, Despotovic Z. Managing trust in a peer-2-peer information system [C]//Proc of CIKM. New York, USA: ACM, 2001: 310–317.
- [13] Marti S, Garcia-Molina H. Limited reputation sharing in p2p systems [C]//Proceedings of the 5th ACM conference on electronic commerce. [s. l.]: ACM, 2004: 91–101.
- [14] 洪亮, 洪帆, 彭冰, 等. 一种基于邻居信任评估的虫洞防御机制 [J]. 计算机科学, 2006, 33(8): 130–133.
- [15] Yu B, Singh M P, Sycara K. Developing trust in large-scale peer-to-peer systems [C]//Proceedings of first IEEE symposium on multi-agent security and survivability. [s. l.]: IEEE, 2004: 1–10.
- [16] Huynh T D, Jennings N R, Shadbolt N. On handling inaccurate witness reports [C]//Proceedings of 8th international workshop on trust in agent societies. [s. l.]: [s. n.], 2005: 63–77.
- [17] 常俊胜, 庞征斌, 徐炜遐, 等. CERep: 一种可信度增强的信誉机制 [J]. 国防科技大学学报, 2014, 36(2): 105–112.