

基于信任度评估的移动自组织网络路由协议

陈 园^{1,2}, 马 林¹, 郑 敏¹, 俞 凯^{1,3}

(1. 上海微系统与信息技术研究所, 上海 200050; 2. 中国科学院大学, 北京 100039;
3. 中科院南京宽带无线移动通信研发中心, 南京 211100)

摘 要: 针对移动自组织网络路由的可靠运行和安全保障问题, 提出一种基于 Dempster-Shafer 证据理论的节点信任评估模型。利用历史交互信息计算直接信任度, 通过邻居节点的推荐度量值获取间接信任度。对直接和间接信任度进行权重修正后根据 Dempster 组合规则合成, 得到节点全局信任度。利用该模型对优化链路状态路由协议的多点中继技术进行优化, 设计改进的路由协议 TOLSR。仿真结果表明, TOLSR 协议能发现和抑制网络的自私节点和恶意节点, 有效提高移动自组织网络的可靠性, 证明了该信任度评估模型的有效性和合理性。

关键词: 移动自组织网络; 自私节点; Dempster-Shafer 证据理论; 信任度评估; 优化链路状态路由协议; 多点中继节点

中文引用格式: 陈 园, 马 林, 郑 敏, 等. 基于信任度评估的移动自组织网络路由协议[J]. 计算机工程, 2015, 41(4): 135-139.

英文引用格式: Chen Yuan, Ma Lin, Zheng Min, et al. Routing Protocol for Mobile Ad Hoc Network Based on Trust Degree Evaluation[J]. Computer Engineering, 2015, 41(4): 135-139.

Routing Protocol for Mobile Ad Hoc Network Based on Trust Degree Evaluation

CHEN Yuan^{1,2}, MA Lin¹, ZHENG Min¹, YU Kai^{1,3}

(1. Institute of Microsystem and Information Technology, Shanghai 200050, China;

2. University of Chinese Academy of Sciences, Beijing 100039, China;

3. Nanjing Broad Band Wireless Communication Research Center, Chinese Academy of Sciences, Nanjing 211100, China)

[Abstract] Specific to reliability and security problems in Mobile Ad Hoc Network (MANET), a trust evaluation model based on Dempster-Shafer (D-S) evidence theory is proposed. Direct trust degree is calculated with historical interaction information and indirect trust is obtained from neighbor nodes' commendations. The direct trust degree and indirect trust are combined according to Dempster combination rule after being amended with weight, to obtain node's comprehensive trust finally. On this basis, it optimizes the Multi-point Relaying (MPR) technology in Optimized Link State Routing Protocol (OLSR), and proposes an improved routing protocol (TOLSR). Simulation result shows that the model can discoveries selfish nodes and malicious nodes, thus effectively improves the reliability of MANET, which also proves the validity and rationality of the trust evaluation model.

[Key words] Mobile Ad Hoc Network (MANET); selfish node; Dempster-Shafer (D-S) evidence theory; trust degree evaluation; Optimized Link State Routing Protocol (OLSR); Multi-point Relaying (MPR) node

DOI: 10.3969/j.issn.1000-3428.2015.04.025

1 概述

移动自组织网络 (Mobile Ad hoc Network, MANET) 通过节点间的相互协作来实现网络互联和信息交换, 而不依赖于任何固定的基础设施, 具有无

中心、自组织、可移动等特点, 因此被广泛应用在军事通信、灾难救援等应急通信领域。由于网络拓扑结构动态变化、无线信道对外开放、节点间缺乏必要的安全认证等原因^[1], 传统网络的可靠机制难以适用于移动自组织网络路由协议的设计, 移动 Ad hoc

基金项目: 中国科学院先导科技专项基金资助项目“服务于海云计算的无线传输技术研究”(XDA06011100); 上海市科委科技小巨人培育企业基金资助项目(13HX1180800); 上海市经信委战略性新兴产业基金资助项目(BY2JXA1001)。

作者简介: 陈 园(1989-), 男, 硕士研究生, 主研方向: 信息安全, 移动网络; 马 林, 助理研究员、博士; 郑 敏, 副研究员、博士; 俞 凯, 研究员、博士。

收稿日期: 2014-05-26 **修回日期:** 2014-06-25 **E-mail:** Earthyuan@gmail.com

网络更容易遭受各种攻击。

优化链路状态路由协议 (Optimized Link State Routing Protocol, OLSR) 是一种基于 LS (Link State) 的先应式表驱动路由协议, 为了减少消息泛洪的开销, 只有多点中继 (Multi-point Relaying, MPR) 节点才能转发控制消息^[2]。但 MPR 节点周期性与其他节点交换信息, 难以适应网络拓扑结构的变化, 同时, 由于没有任何节点评估机制, 可能存在自私节点和恶意节点, 自私节点接收其他节点消息却拒绝充当 MPR 节点, 恶意节点广播大量虚假服务内容, 这些消极行为严重影响整个网络的工作效率。

针对自组织网络的路由问题, 国内外学者提出了诸多解决方案^[3,4]。文献[5]证明了最小 MPR 问题是 NP 完全问题。文献[6]用遗传算法寻找 OLSR 协议的最小 MPR 集, 能够在较短时间内找到最优解。文献[7]基于贝叶斯理论对节点的信任关系进行建模, 但对节点的错误推荐缺少辨别能力。文献[8]提出一种机会路由算法, 但该模型中忽略了信任度评估中的不确定性。

本文结合 MANET 特点, 建立基于 Dempster-Shafer (D-S) 证据理论的节点信任度评估模型, 提出转发代价模型和改进的路由协议 TOLSR。

2 基于 D-S 论据的信任度评估

2.1 证据理论

D-S 证据理论^[9]是建立在非空有限域 Ω 上的数学推理理论, 其主要特点是引入了对不确定性的描述和能够支持多个证据的融合。 Ω 称为问题 Q 的识别框架, 表示有限数目状态 $\{\theta_1, \theta_2, \dots, \theta_n\}$, 在自组织网络信任度评估中 $\Omega = \{T, \sim T\}$, 其中, T 表示表示节点对另一节点信任, $\sim T$ 则表示不信任。

定义 1 基本可信度函数

对于识别框架 $\Omega = \{T, \sim T\}$, 定义基本可信度函数 m 为幂集合 2^Ω 上的函数, 满足 $m(\Phi) = 0$ 且 $\sum_{A \subseteq \Omega} m(A) = 1$ 。

定义 2 信度函数

对于识别框架 Ω , m 为基本可信度函数, 如果 $Bel(A) = \sum_{B \subseteq A} m(B)$, 则称 Bel 为 Ω 对应于 m 的信度函数。

定义 3 似然函数

对于识别框架 Ω , m 为基本概率分配函数, 如果 $Pl(A) = \sum_{B \cap A \neq \emptyset} m(B)$, 则称 Pl 为 Ω 对应于 m 的似真函数。

$[Bel(A), Pl(A)]$ 为 A 的中性证据区间, 其宽度反映证据对命题 A 的不确定性程度, 常用测度函数有关区间的划分如图 1 所示。



图 1 D-S 理论函数基本区间的划分

定义 4 Dempster 规则

设 2 个推荐证据完全独立, 它们在识别框架 Ω 上对应的基本可信度函数分别为 m_1 和 m_2 , 定义函数 m_{12} 是识别框架上的一个基本可信度函数。

$$\begin{cases} m_{12}(\Phi) = 0 \\ m_{12}(A) = k \sum m_1(X) m_2(Y), X \cap Y = A \end{cases}$$

其中, $k^{-1} = \sum m_1(X) m_2(Y), X \cap Y \neq \emptyset$, 它反映 m_1 和 m_2 对应的 2 个推荐证据对命题 A 的联合支持程度, 其中 k 为组合系数, 保证 m_{12} 的值域归一化到标准空间 $[0, 1]$ 上。

2.2 信任度模型

ITU-T 推荐的 PKI 标准 X.509 中给出信任的定义: 若实体 A 认定实体 B 将严格地按 A 的期望进行行动, 则 A 信任 B ^[10]。由此可见, 信任是一种主观概念, 取决于经验, 并随着客体行为的结果变化而不断修正。MANET 中节点间的信任关系具有不确定性^[11], 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进行更新; 其次, 评估节点收集其他节点对被评估节点的推荐信任度, 形成间接信任度, 信任关系模型如图 2 所示。

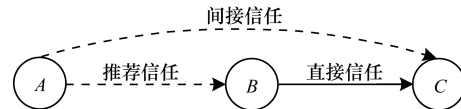


图 2 信任关系定义模型

(1) 直接信任度

直接信任度是两节点根据交互历史记录给对方评估的信任度值, 定义直接信任度向量 DT_{ij} 表示节点 i 与节点 j 的直接信任度。

$$DT_{ij} = [m_{i,j}(\{T\}), m_{i,j}(\{\sim T\}), m_{i,j}(\{T, \sim T\})]$$

其中, $m(\{T\})$ 和 $m(\{\sim T\})$ 分别表示对信任和信任的支持程度; $m(\{T, \sim T\})$ 表示信息缺乏导致的不确定性程度。统计 ΔT 内 i, j 节点间交互次数 S_{ij} , 其中通信成功次数 α_{ij} 、失败次数 β_{ij} , 计算各命题的基本置信度, 即可得到各节点的基本信任度 $D_{i,j}$ 。

$$m_{i,j}(\{T\}) = \alpha_{ij}/S_{ij}$$

$$m_{i,j}(\{\sim T\}) = \beta_{ij}/S_{ij}$$

$$m_{i,j}(\{T, \sim T\}) = 1 - \alpha_{ij}/S_{ij} - \beta_{ij}/S_{ij}$$

每个节点对节点信任度评估后, 可以得到直接可信度函数矩阵 $V_{n \times (n-1)}$:

$$V_{n \times (n-1)} = \begin{bmatrix} T_{12} & T_{13} & \cdots & T_{1n} \\ T_{21} & T_{23} & \cdots & T_{2n} \\ \vdots & \vdots & & \vdots \\ T_{n1} & T_{n2} & \cdots & T_{n(n-1)} \end{bmatrix}$$

(2) 间接信任度

间接信任度是指其他节点对某节点信任度的推

荐度量值,根据其他节点对该节点的反馈评估值而得出。为了减少自组织网通信负荷,同时避免推荐递归和简化计算,间接信任度的推荐限制在节点之间进行,且不采用信任的传递迭代,即推荐节点只能将自己对被评估节点的直接信任度发送给评估节点,不能把收到的推荐信息再推荐给其他节点。

如图3所示,假设A与节点B间存在公共节点 C_1, C_2, \dots, C_n ,记节点A与 C_1 的通信成功概率: $P_{AC_1}^{(0)} = \partial_{AC_1}/S_{AC_1}$,失败概率 $P_{AC_1}^{(1)} = \beta_{AC_1}/S_{AC_1}$;节点 C_1 与B的通信成功概率: $P_{C_1B}^{(0)} = \partial_{C_1B}/S_{C_1B}$,失败概率 $P_{C_1B}^{(1)} = \beta_{C_1B}/S_{C_1B}$ 。

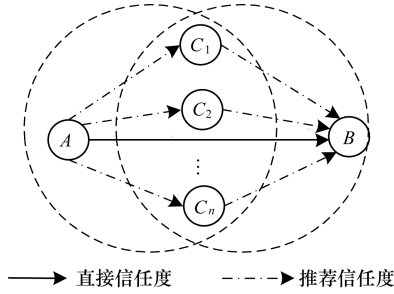


图3 间接信任度计算模型

定义间接信任度向量 $IT_{A,B}$ 表示节点A与节点B的间接信任度:

$$IT_{A,B} = [m_{A,B}(\{T\}), m_{A,B}(\{\sim T\}), m_{A,B}(\{T, \sim T\})]$$

间接信任度 $IT(i,j)$ 的计算公式为:

$$\begin{cases} m_{A,B}(\{T\}) = \frac{\sum_{k \in n} P_{AC_k}^{(0)} P_{C_kB}^{(0)}}{\sum_{k \in n} P_{C_kB}^{(0)}} \\ m_{A,B}(\{\sim T\}) = \frac{\sum_{k \in n} P_{AC_k}^{(1)} P_{C_kB}^{(1)}}{\sum_{k \in n} P_{C_kB}^{(1)}} \\ m_{A,B}(\{T, \sim T\}) = 1 - m_{i,j}(\{T\}) - m_{i,j}(\{\sim T\}) \end{cases}$$

由于节点分布的随机性,可能会出现图4所示的特殊情况,两节点间没有共同节点,这种情况下不计算节点间的间接信任度,全局信任度用直接信任度表示。

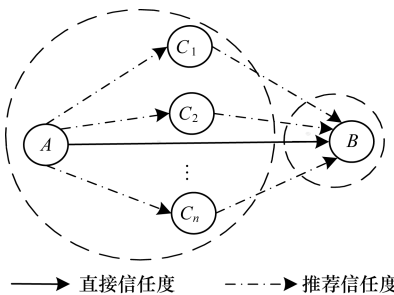


图4 间接信任度计算模型的特殊情况

(3) 全局信任度

全局信任度是指包含节点之间的直接信任度和

间接信任度的综合信任水平,由直接信任度和间接信任度加权计算得到。根据Dempster组合规则,节点 i 与节点 j 之间的总信任度为:

$$T(i,j) = \partial \times DT(i,j) + \beta \times IT(i,j)$$

其中, $0 \leq T(i,j) \leq 1, \partial + \beta = 1$ 根据实际的网络情况对 ∂ 和 β 进行折中取值。

3 基于信任度评估的TOLSR路由协议

3.1 转发代价模型

OLSR路由协议的执行过程大致可以分为4个阶段,即邻居发现、MPR选择、MPR信息分发和路由计算。传统路由中节点转发主要以最短路径(或最小跳数)作为选择标准,对于移动自组织网而言,节点可能处于运动状态,转发节点、转发路径的选择都会影响到消息广播的可靠性^[12]。

由第2节分析可知,节点的信任度值较高意味着该节点转发成功的概率较大,因此,引入信任度作为转发节点选择标准;同时,为了有效地控制网络中信息泛滥,应考虑节点的连通度,计算出尽可能小的MPR集合。因此提出基于信任度、连通度的转发代价模型。假定 i 是MANET的某个节点,函数定义如表1所示。

表1 转发代价模型函数

符号	物理意义
$CFP(i)$	i 节点转发数据包开销
$N_1(i)$	i 节点一跳节点
$N_2(i)$	i 节点二跳节点
$N_{1,2}(i)$	$N_1(i) \cup N_2(i)$, 节点一二跳节点
$CF(i)$	i 节点的转发代价

$$(1) \text{ 连通度模型: } CF_c(i) = \frac{CFP(i)}{|N_1(i)|};$$

$$(2) \text{ 信任度模型: } CF_t(i) = \frac{CFP(i)}{|TR(i)|};$$

(3) 混合模型TOLSR:

$$CF(i) = \frac{CFP(i)}{|TR(i)| \times |N_1(i)|}$$

3.2 MPR节点选择

节点A的MPR集合是满足下面条件的节点集:
(1)MPR中的每个节点都是A的一跳节点;(2)通过MPR中的节点,A可以将信息传播到所有的二跳节点。建立转发代价模型后,提出改进的路由协议TOLSR,主要思想是尽可能减少MPR节点个数,进而提高网络的整体控制能力。MPR选择流程可以分为4个阶段:

第1阶段:利用Hello消息建立两节点间的对称链路,获取一跳、二跳节点状态信息。

第2阶段:信任度评估值初始化。根据信任度

评估模型对每个节点的信任度进行评估,生成转发代价值并组播给节点。

第3阶段:选举 MPR_0 节点。每个节点选择一跳节点中转发代价最小的节点作为 MPR 节点,记为 MPR_0 。

第4阶段:选择 MPR 节点覆盖其他节点。如果此时在节点集中还存在没有被 MPR 覆盖的节点,那么重复以下步骤,使得所有的节点都能通过 MPR 到达:

(1) 遍历三跳 MPR_0 间存在的可能路径,计算每条路径的转发代价值。

(2) 选择代价值最小路径上的节点,如果有多个满足条件的节点,选择节点 ID 小的节点,将节点加入 MPR ,然后将能够通过 MPR 到达的节点从未被覆盖节点集中移除。

3.3 算法设计

每个节点选择具有最小转发代价 $CF(i)$ 的邻节点(可以是自身节点),选举产生 MPR_0 节点。为表述方便,假定 k 是已确定的 MPR_0 节点, N 跳 MPR_0 形式化定义如下:

一跳 MPR_0 :

$$CH_1(k) = \{i \in N_1(k) \mid H = 1 \text{ in } Hello(i)\}$$

二跳 MPR_0 :

$$CH_2(k) = \{i \in N_2(k) \mid H = 1 \text{ in } Hello(i)\}$$

三跳 MPR_0 :

$$CH_3(k) = \{j \mid \exists i \in N_2(k) \& \& i \text{ vote for } j\} N_{1,2}(k)$$

覆盖度:

$$CH(k) = CH_3(k) \cup CH(k)_2 \{j \mid \exists i \in$$

$$CH_1(k) \& \& j \in N_1(i)\}$$

Hello 消息需要进行若干处修改,第1处是增加 H 标志, $H=1$ 时表示本节点已被选为 MPR_0 ,第2处是增加类型标志 H_NEIGH , $H_NEIGH=1$ 表示有邻节点已经被选为 MPR_0 。对于每个节点,可以通过监测选举信息,来获悉本节点是否当选 MPR_0 。这些修改会使 Hello 消息数量加倍,但是相对于广播的 TC 消息,增加的 HELLO 消息对网络拥塞的影响微不足道。 MPR 节点选择算法具体描述如下:

算法1 MPR_0 选择 $MPR_0_Selection(G, E)$

i 是 MANET 的节点;

若 $k \in N_1(i) \cup \{i\}$ 且 $CF(k) = \min \{CF(j) \mid k \in N_1(i) \cup \{i\}\}$;

节点 i 选择节点 k ;

节点 k 当选 MPR_0 。

算法2 连通 $CH_3(k)$ 节点 $CH_3(k)_Cover(k, 1)$

当 $CH(k) \cap CH_3(k) \neq \emptyset$;

令 $l \in CH(k) \cap CH_3(k)$;

遍历路径 $k, x, y, l, \min \{CF(x) + CF(y)\}$;

若存在2种或者多种最小代价路径,选择 x, y

节点 ID 较小的路径;

置 x 为 MPR 节点;

$CH(k)$ 剔除 l 节点和 $x \in CH_2(k)$ 。

算法3 连通 $CH_2(k)$ 节点 $CH_2(k)_Cover(k, l)$

当 $CH(k) \neq \emptyset$;

$l \in CH(k) \cap CH_2(k)$;

遍历路径 $k, x, l, \min \{CF(x)\}$;

若存在2种或者多种最小代价路径,选择 x 节点 ID 较小的路径;

置 x 为 MPR 节点;

$CH(k)$ 中剔除 $CH_2(k)$ 可以通过 x 到达的节点。

假设网络节点拓扑如图5所示,各节点转发代价如表2所示。

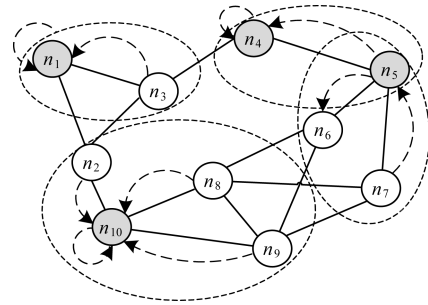


图5 代价转发模型流程

表2 转发代价

节点	开销	节点	开销
n_1	3	n_6	7
n_2	3	n_7	6
n_3	6	n_8	7
n_4	4	n_9	8
n_5	5	n_{10}	1

按照 MPR 计算步骤,获取节点信任度值后,各节点选择转发代价最小的邻节点作为 MPR_0 ,完成后 MPR 节点集有 $\{n_1, n_4, n_5, n_{10}\}$ 。以 n_{10} 为例开始选择其他 MPR 节点, $CH_1(n_{10}) = \emptyset$; $CH_2(n_{10}) = \{n_1\}$; $CH_3(n_{10}) = \{n_5\}$, 因为 $N_2(n_{10})$ 中没有节点选择 n_4 , 所以 $n_4 \notin CH_3(n_{10})$ 。

首先需要覆盖三跳 MPR_0 节点 $CH_3(n_{10})$, 算法2给出从节点 n_{10} 到 n_5 的最小代价路径计算方法,有4条可供选择的路径: $\{n_9, n_7\}$, $\{n_9, n_6\}$, $\{n_8, n_7\}$, $\{n_8, n_6\}$, 经计算可知 $\{n_8, n_7\}$ 具有最小转发代价,因此选择 n_8, n_7 作为 MPR 节点。接下来需要覆盖二跳 MPR_0 节点 $CH_2(n_{10}) = \{n_1\}$, 只有一条路径 $\{n_2\}$ 。所有计算完成后,最后 n_{10} 选择 $\{n_8, n_2\}$ 作为 MPR ; n_1 选择 n_2 , n_5 选择 n_7 作为 MPR 节点。

4 仿真与性能分析

性能仿真实验采用 Network Simulator 2 平台,场景设置为 $500 \text{ m} \times 500 \text{ m}$ 的区域,场内随机分布有

50个节点,其中有若干自私节点,节点间的通信距离250 m;信道传输速率1 Mb/s。实验主要收集2种数据:端到端平均时延和分组成功交换率,仿真结果如图6和图7所示。

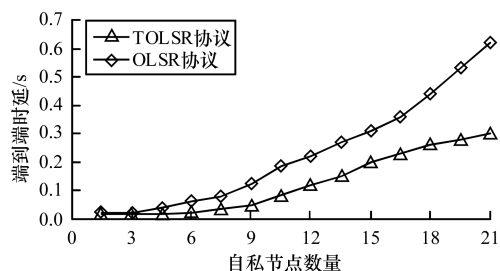


图6 TOLSR和OLSR协议的端到端平均时延对比1

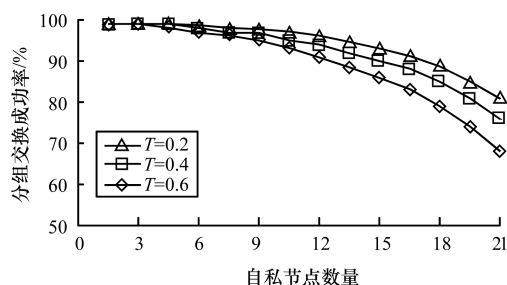


图7 不同周期下TOLSR协议的分组成功交换率

由图6可以看出,随着自私节点数量增加,节点端到端平均时延增大,OLSR协议时延增加更快,这是由于自私节点拒绝充当MPR节点,影响了整个网络的工作效率。TOLSR协议的平均时延也有所增加,一方面是因为自私节点的增加导致平均转发代价增加,另一方面Hello消息增加也导致协议开销增大。

由图7可以看出,随着自私节点数量的增加,TOLSR协议分组交换成功率有所降低,且信任度评估周期越长,转发成功率降低越快,主要是因为评估周期变长,有些自私节点没能及时发现,这些自私节点导致信道上的无线干扰和冲突也相应加剧,导致丢包率增大。

将仿真场景中的自私节点改为恶意节点,这些节点或转发虚假服务内容,或因链路状态等原因参与转发却不能完成任务。实验结果如图8所示。

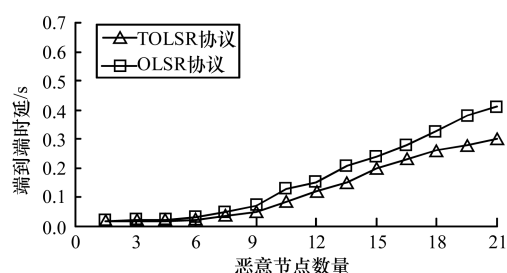


图8 TOLSR和OLSR协议的端到端平均时延对比2

可以看出,节点端到端平均时延随着恶意节点数量增加而增大。因为恶意节点大量广播虚假服务

内容,导致路由中TC消息泛滥、网络拥塞,因而端端的平均时延急剧上升,OLSR协议时延增加更快。同时由于TOLSR协议能够识别网络中的恶意节点,因此时延增加较为缓慢。

5 结束语

针对MANET路由的可靠运行和安全保障问题,本文建立一种基于D-S证据理论的节点信任度评估模型,解决了信任度评估中的不确定性问题。仿真结果验证了TOLSR协议的有效性,以及在防范自私节点和路由成本方面性能上的显著改进。下一步将对该协议进行性能测试,研究如何在保证网络路由可靠性的同时,降低协议开销,为自组织网络提供更好的QoS路由方式。

参考文献

- [1] Abolhasan M, Wysocki T, Dutkiewicz E. A Review of Routing Protocols for Mobile Ad Hoc Networks[J]. Ad Hoc Networks, 2004, 2(1): 1-22.
- [2] Clausen T, Jacquet P, Adjih C, et al. Optimized Link State Routing Protocol (OLSR)[S]. RFC 3626, 2003.
- [3] Robert J M, Otrok H, Chriqi A. RBC-OLSR: Reputation-based Clustering OLSR Protocol for Wireless Ad Hoc Networks[J]. Computer Communications, 2012, 35(4): 487-499.
- [4] 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.
- [5] Qayyum A, Viennot L, Laouiti A. Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks, RR-3898[R]. INRIA, 2000.
- [6] 张信明, 曾依灵, 干国政, 等. 用遗传算法寻找OLSR协议的最小MPR集[J]. 软件学报, 2006, 17(4): 932-938.
- [7] Gong Wei, You Zhiyang, Chen Danning, et al. Trust Based Routing for Misbehavior Detection in Ad Hoc Networks[J]. Journal of Networks, 2010, 44(5): 551-558.
- [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] Xu Congfu, Geng Weidong, Pan Yunhe. Review of Dempster-Shafer Method for Data Fusion[J]. Acta Electronica Sinica, 2001, 29(3): 393-396.
- [10] Kamvar S D, Schlosser M T, Garcia-Molina H. The Eigentrust Algorithm for Reputation Management in P2P Networks[C]//Proceedings of the 12th International Conference on World Wide Web. New York, USA: ACM Press, 2003: 640-651.
- [11] 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.
- [12] 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.

编辑 金胡考