

一种支持 QoS 与信任值的启发式重路由机制

薛惠中¹, 王兴伟², 李 婕¹, 黄 敏³

¹(东北大学 计算机科学与工程学院 沈阳 110819)

²(东北大学 国家示范性软件学院 沈阳 110819)

³(东北大学 信息科学与工程学院 沈阳 110819)

E-mail: wangxw@mail.neu.edu.cn

摘 要: 随着网络规模持续扩大和新业务不断增长,用户对网络的服务质量(Quality of Service, QoS)提出了更高的要求. 用户数量增加、网络规模复杂、网络安全性差等因素使得网络元素(节点或链路)更加容易失效,从而导致重路由发生率增高. 本文在描述网络模型、用户需求以及满意度计算方法的基础上,根据带宽与信任值设计启发式函数,提出了一种支持 QoS 与信任值的启发式重路由机制(QoS and Trust value based heuristic ReRouting, QTRR). 仿真结果表明,当重路由由条件触发时,本机制能够快速建立一条可信且满足 QoS 需求的重路由路径.

关 键 词: 可信网络; 信任值; 服务质量; 重路由

中图分类号: TP391

文献标识码: A

文章编号: 1000-4220(2017)11-2432-05

QoS and Trust Value Supported Heuristic Rerouting Mechanism

XUE Hui-zhong¹, WANG Xing-wei², LI Jie¹, HUANG Min³

¹(School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China)

²(Software College, Northeastern University, Shenyang 110819, China)

³(College of Information Science and Engineering, Northeastern University, Shenyang 110819, China)

Abstract: With the continuous increase of the network scale and the number of new network applications, users need higher Quality of Service to satisfy their demands. Due to the increase of user quantity, expansion of the network scale and the poor security of networks, it is more prone to failure of network elements (e.g., routers or links). On the basis of network model analysis, user demands and degree of satisfaction, a QoS and Trust value supported heuristic ReRouting mechanism is proposed which is based on the required bandwidth and trusted values of links. The simulation results show that when the rerouting condition is triggered, a trusted and QoS rerouting path can be quickly established by this mechanism.

Key words: trusted network; trust value; QoS; rerouting

1 引 言

随着互联网技术的发展,人们的生活发生着巨大的改变. 智能家居、在线医疗、视频点播以及 IP 电话等应用对网络可信性^[1]和服务质量(Quality of Service, QoS)^[2-4]等需求提出了新的要求. 并且随着网络规模的扩大,互联网结构的日益复杂,网络节点或链路故障等原因引起的链路失效越来越频繁,因此,有关网络可信性、服务质量和路由机制的研究显得尤为重要.

文献[5]提出了在移动自组织网络(Mobile Ad hoc Network, MANET)中基于 QoS 和信任度的 TQR(Trust-based QoS Routing)路由机制,防止恶意节点的攻击,提高网络的安全性能. 文献[6]提出了基于信任值的 QoS 协议,对 MANET 进行路由优化,实现安全路由. 文献[7]提出了在无线传感器

网络(Wireless Sensor Network, WSN)中采用基于可信树的路由机制保证路由的安全性. 文献[8]提出了基于用户行为的信任值评价机制,在此基础上设计机会通信环境中的数据分发机制. 文献[9]基于网络的可信性和延迟提出了一种路由机制,能够准确地评价节点之间的信任关系并且有效地减少网络的延迟,但是没有考虑网络元素故障后的重路由问题. 文献[10]研究了机会网络的可信性和安全性,提出了恶意节点的检测算法,保证检测的准确度随检测时间的增加而增大. 上述研究成果主要针对 MANET、WSN 和机会网络路由机制进行研究. 在互联网主干网路由机制研究中文献[11]提出了一种共享健壮重路由 ShRR(Shared Robust Rerouting)策略,结合路径多样性、限制性恢复和全局重路由技术,减少网络开销,但该路由机制仅考虑了如何快速建立重路由路径,缺少对 QoS 和可信性的保证;文献[12]研究了节点故障情况下的重路由策略,提出了保证 QoS 的 ODUMR 算法,但是没有分析

收稿日期: 2016-10-12 收修改稿日期: 2016-11-10 基金项目: 国家杰出青年科学基金项目(71325002)资助; 国家自然科学基金项目(61572123, 61502092)资助; 中央高校基本科研业务费专项基金项目(N151604001)资助; 中国博士后科学基金项目(2016M591449)资助. 作者简介: 薛惠中,男,1992年生,硕士,研究方向为信息中心网络和软件定义网络; 王兴伟(通信作者),男,1968年生,博士,教授,博士生导师,CCF高级会员,研究方向为未来互联网、云计算、网络与信息安全等; 李 婕,女,1982年生,博士,副教授,CCF会员,研究方向为认知网络、移动计算等; 黄 敏,女,1968年生,博士,教授,博士生导师,研究方向为物流建模与优化、供应链系统等.

网络的可靠性对重路由路径的影响。

本文基于互联网主干网的服务质量需求,以及网络可信性评价指标,提出一种支持 QoS 与信任值的重路由机制 (QTRR, QoS and Trust value supported heuristic ReRouting mechanism)。该机制能够保证用户服务质量,同时具有可信性,当网络故障发生时,能够快速建立一条满足需求的恢复路径。

2 网络模型

网络模型可以抽象为无向连通图 $G(V, E)$ 。V 表示节点集合,代表网络中路由节点的集合,主要负责数据包的转发和节点可信性的评估。节点之间的可信性用信任值来度量,表示对该节点的信任程度。为了简化问题,将信任值与节点的延迟、延迟抖动、出错率一起归并到链路上。E 表示边的集合,代表网络通信链路的集合。

表 1 不同流量等级的 QoS 信息

Table 1 QoS information in different traffic level

网络负载	流量等级	相对带宽	相对延迟	相对延迟抖动	相对出错率
较轻	1	1	1	1	1
轻	2	0.8	1.07	1.05	1.02
一般	3	0.6	1.14	1.1	1.04
重	4	0.4	1.21	1.15	1.06
较重	5	0.2	1.28	1.2	1.08

本文考虑了网络负载对重路由机制的影响。通过改变链路在初始条件下的带宽、延迟、延迟抖动等 QoS 参数来模拟网络负载:当网络负载较轻时,每条链路提供其原始的 QoS 信息,此时用单位 1 表示;当网络负载增大时,每条链路提供其原始 QoS 信息的相对值,如表 1。

3 路由机制

3.1 用户需求

重路由请求由五元组组成,记为 $RReq(v_s, v_d, AP_i, TL, ID)$ 。v_s 表示源节点, v_d 表示目的节点。本文参考 DiffServ 模型区分出不同的网络应用类型,每种类型有特定的 QoS 需求区间。AP_i 表示第 i 种应用类型,其 QoS 需求为 $APR_i = (\Delta_{bw}^i, \Delta_{dl}^i, \Delta_{jitter}^i, \Delta_{loss}^i)$ 。其中, $\Delta_{bw}^i, \Delta_{dl}^i, \Delta_{jitter}^i, \Delta_{loss}^i$ 分别表示 AP_i 的带宽、延迟、延迟抖动、出错率的需求区间。TL 表示链路的信任等级,本文将信任划分为五个等级,不同的信任等级 1~5 对应不同的信任值区间:等级 5 为高度可信等级,信任值区间为 (0.8, 1]; 等级 4 为非常可信等级,信任值区间为 (0.6, 0.8]; 等级 3 一般可信等级,信任值区间为 (0.3, 0.6]; 等级 2 轻微可信等级,信任值区间为 (0, 0.3]; 等级 1 为无信任需求,信任值区间为 [0, 1]。重路由路径不仅需要满足 AP_i 的 QoS 需求,而且保证信任值不小于 TL 对应的信任值下限。ID 表示会话编号,保证重路由请求的唯一性。

3.2 算法设计

3.2.1 算法思想

本文设计的启发式重路由机制的思想是:通过将归一化

的链路带宽与信任值加权求和,将可信 QoS 重路由问题转化为单一权值问题。当重路由条件触发时,利用 D* Lite 算法^[13]在前 K 条最短路径中选择合适的最短路径。每当求得第 k 短路径时,检查该路径能否满足用户的 QoS 和信任值需求。如果满足,则该路径即为要寻找的最短路径,否则,求解第 k+1 短路径,直至找到满足需求的路径或者 k=K 为止。

D* Lite 算法是在 LPA*^[14]算法的基础上提出来的,利用前向搜索来提高本次搜索的效率,利用启发式信息选择下一跳节点。如果在找路的过程中链路的权值发生改变, D* Lite 能够根据最新的链路信息寻找满足需求的最短路径。D* Lite 算法还具有搜索速度快等优点。

3.2.2 链路权值

由于求解多个 QoS 参数约束的路由问题是一个 NP 难问题,而且 QoS 参数之间具有一定相关性:在主干网中,处理延迟和传输延迟几乎可以忽略不计;排队延迟是由于链路带宽不足,数据在路由节点堆积导致阻塞引起的;节点阻塞还会导致分组丢失、出错率增大、延迟抖动增大。因此,链路提供的带宽是影响用户 QoS 体验的最主要因素。所以,本文重点考虑链路的可用带宽和信任值这两个参数来设计启发式重路由机制。由于带宽与信任值具有不同的量纲,因此需要对可用带宽进行归一化处理,如下:

$$bw_n^* = \begin{cases} 1 & bw_n \geq bw_H \\ \frac{bw_n - bw_L}{bw_H - bw_L} & bw_L < bw_n < bw_H \\ \varepsilon & bw_n \leq bw_L \end{cases} \quad (1)$$

其中 bw_n 表示第 n 条链路可用带宽, bw_L, bw_H 分别为应用带宽需求的下界和上界, ε 为很小的正数。

链路的权值表示为:

$$cost = \frac{\alpha}{bw_n^*} + \frac{\beta}{tru} \quad (2)$$

其中 tru 为链路的信任值, α 和 β 为带宽和信任值的调节因子 ($\alpha, \beta > 0$ 且 $\alpha + \beta = 1$)。

3.2.3 算法流程

在算法执行前需要设置一个计数器 k,记录寻找最短路径的次数。k 初始值为 1,当 $k > K$ (K 是查找次数的上限) 时算法结束。寻找最短路径之前需要根据网络的带宽和信任值,对每条边的权值 $c(u, v)$ 初始化,其中 $u, v \in V, (u, v) \in E$ 。final 表示当前节点,其初始值为起始节点 start。path 表示所求路径,初始值为空,当寻找到下一跳节点时,把当前节点 final 添加到 path 中。computeShortestPath(final, goal) (详细算法见 [9]) 方法表示估算出一条从当前节点 final 到目的节点 goal 的最短路径。findSuccessor(final) 方法表示根据估算的最短路径,找到当前节点 final 的下一跳节点,下一跳节点可能在估算的路径上也可能不在估算的路径上。updateVertex(u) 用于更新节点 u 到目的节点 goal 的最短路径的估计值。compute-qos(path) 计算路径 path 是否满足 QoS 约束,如果满足,则返回当前路径 path,否则重新计算下一条路径。

算法 1. 重路由 QTRR 算法

输入: 起始节点 start, 目的节点 goal。

输出: 路径 $path = \{v_1 = start, v_2, \dots, v_m = goal\}$

for $k = 1: K$

```

Initiate edge cost  $c(u, v)$ 
path =  $\emptyset$ 
final = start
path = path  $\cup$  final
computeShortestPath(final, goal)
while( final  $\neq$  goal)
final = findSuccessor(final)
path = path  $\cup$  final
if any edge cost changed
    update the edge cost  $c(u, v)$ 
    updateVertex(u)
computeShortestPath(final, goal)
if computeqos(path) is true
    return path
else
    k = k + 1

```

3.3 信任评估

在数据传输过程中,不同的恶意行为对网络链路的信任值产生不同的影响. 本文将信任危机行为划分成四个等级: 轻微危机, 包括网络元素(节点或链路)故障而引起的业务中断等行为; 中度危机, 包括窃听数据包信息及进行路由欺诈等恶意行为; 严重危机, 包括会话劫持、对数据包信息进行篡改和伪造等行为; 致命危机, 包括传播木马病毒、DoS 攻击等可能导致网络瘫痪恶意行为.

为了提高信任值评估的准确性, 反映信任值与时间的衰减特性, 本文引入了滑动窗口机制^[15]. 随着时间的推移, 远离当前周期的信任值的可信性逐渐下降, 最终被移出窗口.

3.3.1 直接信任值

在周期 i 内节点 A 记录与节点 B 交互行为的正面评价次数为 S_i 次, 轻微危机、中度危机、严重危机行为的负面评价次数分别为 F_{i1} 、 F_{i2} 、 F_{i3} . 如果出现一次致命危机行为, 则直接将节点关闭. 对不同的信任危机行为等级进行不同程度的“惩罚”, “惩罚”后的负面评价次数为:

$$F_i^* = \psi_1 F_{i1} + \psi_2 F_{i2} + \psi_3 F_{i3} \quad (3)$$

其中 $\psi_i (i = 1, 2, 3)$ 为惩罚因子, 对信任危机行为进行惩罚, 并且行为越恶劣惩罚尺度越大 ($\psi_1 < \psi_2 < \psi_3$).

节点 A 对 B 的期望信任值 exp ^[16] 为:

$$exp = \frac{1 + S_{de}}{2 + S_{de} + F_{de}} \quad (4)$$

其中 $S_{de} = \sum_{i=1}^N \beta_1^{t-t_i} S_i$, $F_{de} = \sum_{i=1}^N \beta_2^{t-t_i} F_i^*$. S_{de} 表示衰减后的正面评价次数, F_{de} 表示衰减后的负面评价次数. β_1 , β_2 为时间消逝因子, 且 $0 \leq \beta_1 \leq \beta_2 \leq 1$. t 为当前时间周期, t_i 为第 i 个时间周期, N 表示滑动窗口的大小.

上述 (3) 和 (4) 式具有一定的偶然性, 为了增强信任值评估的可靠性, 本文引入了可信度^[17]的概念. 可信度越接近于 1, 说明期望值 exp 的可信程度越大, 反之越小. 可信度 c 的定义如下:

$$c = 1 - \sqrt{\frac{12 S_{de} F_{de}}{(S_{de} + F_{de})^2 (S_{de} + F_{de} + 1)}} \quad (5)$$

节点 A 对节点 B 的直接信任值由期望信任值 exp 和可信

度 c 共同决定, 公式如下:

$$TV_{AB}^d = 1 - \frac{\sqrt{(exp - 1)^2 + r^2 (c - 1)^2}}{\sqrt{1 + r^2}} \quad (6)$$

其中 r 是 exp 与 c 之间重要程度的权值.

3.3.2 间接信任值

当可信度 $c < c_L$ (c_L 为可信度阈值) 时, 可信度不能真实地衡量节点之间的信任关系. 本文引入邻居节点推荐机制. 为了防止推荐的信任值与真实值差距较大还需要进行背离度测试, 计算公式如下:

$$|TV_{AB}^d - TV_{XB}^r| \leq \eta \quad (7)$$

其中 η 为背离度的阈值 $0 < \eta < 1$. TV_{XB}^r 为节点 A 的某个邻居节点 X 对 B 的推荐信任值. 如果推荐信任值与直接信任值接近则接受该推荐信任值, 否则拒绝.

假设接受推荐的信任值有 m 个, 则间接信任值的计算公式如下:

$$TV_{AB}^r = \frac{1}{m} \sum_{i=1}^m TV_{iB}^r \quad (8)$$

3.3.3 综合信任值

综合信任值可以由直接信任值与间接信任值计算得出, 公式如下:

$$tru = \alpha TV_{AB}^d + (1 - \alpha) TV_{AB}^r \quad (9)$$

其中 α 为直接信任权值, 一般取大于 0.5 的数值.

3.4 用户满意度

用户满意度反映了用户对路径的满意程度, 主要体现在带宽、延迟、延迟抖动、出错率和信任值等方面. 首先计算带宽的满意度. 假设路径 p 的可用带宽为 bw_p , 应用 AP_i 的带宽需求区间为 $\Delta_{bw}^i = [bw_L^i, bw_H^i]$, 则用户带宽满意度定义如下:

$$Sat(bw_p) = \begin{cases} 0 & bw_p < bw_L^i \\ \varepsilon & bw_p = bw_L^i \\ \frac{1}{2} + \frac{1}{2} BW & bw_L^i < bw_p \leq bw_H^i \\ 1 & bw_p > bw_H^i \end{cases} \quad (10)$$

其中 $BW = \sin \frac{\pi}{bw_H^i - bw_L^i} \left(bw_p - \frac{bw_H^i + bw_L^i}{2} \right)$.

当可用带宽在最小带宽 bw_L^i 附近时, 增加网络的带宽仅能满足应用的最低需求, 因此用户的满意度较低; 当超出最小带宽 $\frac{bw_H^i - bw_L^i}{2}$ 时, 应用的需求很大程度得到满足, 因此用户满意度较高; 当可用带宽在最大带宽 bw_H^i 附近时, 应用的需求全部得到满足, 因此用户的满意度达到最大.

类似计算延迟满意度. 假设路径 p 提供的延迟为 dl_p , 应用 AP_i 延迟需求区间为 $\Delta_{dl}^i = [dl_L^i, dl_H^i]$, 则用户延迟满意度定义如下:

$$Sat(dl_p) = \begin{cases} 0 & dl_p > dl_H^i \\ \varepsilon & dl_p = dl_H^i \\ \frac{1}{2} - \frac{1}{2} DL & dl_L^i \leq dl_p < dl_H^i \\ 1 & dl_p < dl_L^i \end{cases} \quad (11)$$

其中 $DL = \sin \frac{\pi}{dl_H^i - dl_L^i} \left(dl_p - \frac{dl_H^i + dl_L^i}{2} \right)$.

然后计算延迟抖动、出错率和信任值的满意度. 如果路径提供的延迟抖动、出错率、信任值分别为 jt_p 、 ls_p 、 tr_p , 应用 AP_i 延迟抖动需求区间、出错率需求区间、信任值需求区间分别 $\Delta_{jt}^i = [jt_L^i, jt_H^i]$ 、 $\Delta_{ls}^i = [ls_L^i, ls_H^i]$ 、 $\Delta_{tr}^i = [tr_L^i, tr_H^i]$ 则按照式 (10) 可以定义用户信任值满意度 $Tsat(tr_p)$ 按照式 (11) 可以定义用户延迟抖动满意度 $Sat(jt_p)$ 和出错率满意度 $Sat(ls_p)$.

用户的综合满意度 sat :

$$sat = \lambda Qsat + (1 - \lambda) Tsat(tr_p) \quad (12)$$

$$Qsat = w_{bw} Sat(bw_p) + w_{dl} Sat(dl_p) + w_{jt} Sat(jt_p) + w_{ls} Sat(ls_p) \quad (13)$$

其中 $w_{bw} + w_{dl} + w_{jt} + w_{ls} = 1$, w_{bw} 、 w_{dl} 、 w_{jt} 、 w_{ls} 分别表示带宽、延迟、延迟抖动、出错率的权重. λ 为 QoS 满意度权重, 介于 0.5 与 1 之间.

4 仿真实验与性能评价

4.1 仿真策略

本文在 VC++ 平台上对所提出的支持 QoS 与信任值的重路由机制 (QTRR) 进行仿真实现, 并与文献 [18] 中提出的路由算法进行对比分析. 在实验时, 带宽和信任值的调节因子分别取值为 $\alpha = 0.5$ 、 $\beta = 0.5$, 轻微危机、中度危机、严重危机的惩罚因子分别取 $\psi_1 = 1.2$ 、 $\psi_2 = 1.4$ 、 $\psi_3 = 1.6$, 时间消逝因子 $\beta_1 = 0.8$ 、 $\beta_2 = 0.9$. 本文选用 CERNET2、INTERNET2 拓扑作为仿真拓扑用例. 随机生成链路的初始带宽、延迟等链路状态信息. 在这两种拓扑下, 设定 5 种不同的流量等级, 通过随机选定源节点和目的节点, 产生 100 个不同应用类型和信任等级的路由请求. 并随机设定不同节点或链路故障来运行上述 QTRR 重路由算法, 求解出满足用户 QoS 需求的可信路径. 记录算法的运行结果并与基准算法进行比较.

4.2 重路由成功率

如图 1、图 2 所示, 两种重路由机制的成功率随着流量级别的增加而下降. 随着网络负载增大, 可用的网络资源减少, 因而导致重路由所选的路径无法满足用户 QoS 需求而导致重路由失败. 当重路由条件触发时, 基准算法主要关注路径的延迟是否满足 QoS 需求, 而忽略了带宽在 QoS 中的主要作用. 同时基准算法没有考虑网络的可信性. 而 QTRR 算法以带宽和信任值作为链路的权值同时兼顾了延迟、延迟抖动、出错率等因素, 当网络节点或链路故障时从起始节点重新寻路, 因而更能找到满足需求的路径. 所以, 当流量级别增大时, 基准算法重路由成功率下降的更快一些.

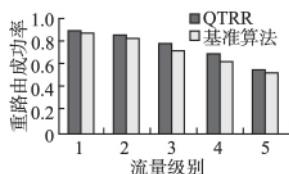


图 1 CERNET2 拓扑下重路由成功率

Fig. 1 Success rate of rerouting in CERNET2

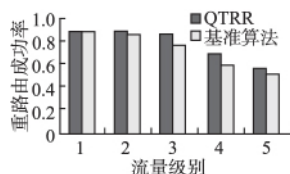


图 2 INTERNET2 拓扑下重路由成功率

Fig. 2 Success rate of rerouting in INTERNET2

在相同流量等级下, QTRR 算法在 CERNET2 拓扑下的重路由成功率相对稍低, 原因在于 CERNET2 拓扑环路较少,

路径多样性较差. 因此, 拓扑环路越多、节点度数越大, 重路由成功率越高.

4.3 用户满意度

如图 3、图 4 所示, 用户的满意度随着流量等级的增加而下降. 当网络流量增大时, 同时满足可信性和 QoS 需求的路径逐渐减少, 用户的应用需求难以得到满足, 因此用户的满意度都呈现下降的趋势. 基准算法以延迟为主要因素寻找满足 QoS 需求的路径, 这就导致网络重载时求得的路径难以满足其他 QoS 参数需求, 因此用户满意度下降的更快一些.

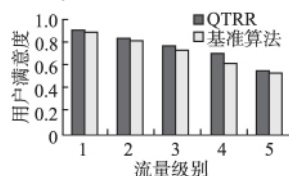


图 3 CERNET2 拓扑下用户满意度

Fig. 3 User satisfaction in CERNET2

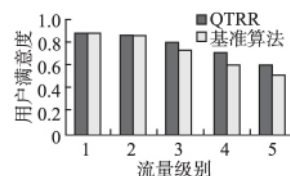


图 4 INTERNET2 拓扑下用户满意度

Fig. 4 User satisfaction in INTERNET2

QTRR 算法主要考虑了带宽和信任值, 当网络负载较重时, QTRR 优先选择满足带宽和可信性的路径. 这样的路径能够在网络重载时满足用户的基本应用需求, 因此满意度会稍高一些. 此外, D^* Lite 算法能够根据网络的动态变化选择相应的路径, 有效地避免负载较重的节点, 因此更能满足用户的 QoS 和可信性需求.

4.4 重路由时间

如图 5, QTRR 算法是基于 D^* Lite 算法的扩展, 重路由时间短. 基准算法需要生成 Steiner 树来寻找满足需求的路

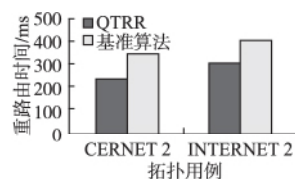


图 5 两种拓扑下重路由时间

Fig. 5 Rerouting time in CERNET2 and INTERNET2

径. 在生成 Steiner 树时, 基准算法需要在 QoS 参数和构建树的代价之间权衡: 选择满足 QoS 参数的路径时, 生成树的代价将会增大; 减小生成树的代价, 求得的路径的难以满足 QoS 需求. 因此, 基准算法的重路由时间长一些. 因为 INTERNET2 拓扑结构更加复杂, 所以 QTRR 算法在 INTERNET2 拓扑下重路由时间比 CERNET2 重路由时间稍长.

5 结论

本文设计了一种支持 QoS 和可信性需求的重路由机制, 该机制易于实现, 能够动态计算节点的信任值, 提高检测效率, 从而增强网络安全性能. 在仿真平台上对该重路由机制进行了实现, 并基于两种不同的网络拓扑进行了性能分析, 验证了该机制在保证用户服务质量的同时保证了节点的可信性, 提高了用户的满意程度. 未来的研究工作考虑如何更好的均衡重路由各项性能指标, 进一步提高重路由机制的性能.

References:

- [1] Lin Chuang ,Peng Xue-hai. Research on trustworthy networks[J]. Chinese Journal of Computers 2005 28(5) : 751-758.
- [2] Wang Xing-wei ,Cheng Hui ,Huang Min. QoS multicast routing protocol oriented to cognitive network using competitive coevolutionary algorithm[J]. Expert Systems with Applications 2014 41 (10) : 4513-4528.
- [3] Wang Xing-wei ,Qu Da-peng ,Huang Min ,et al. Multiple many-to-many multicast routing scheme in green multi-granularity transport networks[J]. Computer Networks 2015 93(P1) : 225-242.
- [4] Wang Xing-wei ,Cheng Hui ,Huang Min. Multi-robot navigation based QoS routing in self-organizing networks [J]. Engineering Applications of Artificial Intelligence 2013 26(1) : 262-272.
- [5] Wang Bo ,Chen Xun-xun ,Chang Wei-ling. A light-weight trust-based QoS routing algorithm for ad hoc networks [J]. Pervasive and Mobile Computing 2014 13: 164-180.
- [6] Zafar S ,Soni M K. Trust based QoS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET [C]. International Conference on Optimization ,Reliability and Information Technology 2014: 173-177.
- [7] Hu Zhi ,Bie Yu-xia ,Zhao Hong. Trusted tree-based trust management scheme for secure routing in wireless sensor networks[J]. International Journal of Distributed Sensor Networks 2015(3) : 1-13.
- [8] Li Jie ,Wang Xing-wei ,Yu Rui-yun ,et al. Reputation-based incentives for data dissemination in mobile participatory sensing networks[J]. International Journal of Distributed Sensor Networks , 2015(2015) : 1-13.
- [9] Wang Na ,Wang Tian-hua. A trusted QoS routing model for wireless sensor networks [C]. International Conference on Computer Science & Education 2015: 627-630.
- [10] Alajeely M ,Doss R. Establishing trust relationships in OppNets using Merkle trees[C]. 8th International Conference on Communication Systems and Networks 2016: 1-6.
- [11] Fundo A ,Bashllari A ,Nace D ,et al. A hybrid rerouting scheme [J]. Telecommunication Systems 2014 56(1) : 69-78.
- [12] Heydarian M. A high performance optimal dynamic routing algorithm with unicast multichannel QoS guarantee in communication systems[J]. Journal of Supercomputing 2012 62(1) : 315-344.
- [13] Koenig S ,Likhachev M. D* lite [C]. Eighteenth National Conference on Artificial Intelligence 2002: 476-483.
- [14] Ratner D ,Pohi I. Joint and LPA: combination of approximation and search [C]. National Conference on Artificial Intelligence Philadelphia ,1986: 173-177.
- [15] Wang Xing-wei ,Wang Jun-wei ,Huang Min. Hunting search based trustworthy QoS routing algorithm[J]. Journal of Northeastern University Nature Science 2012 33(10) : 1385-1389.
- [16] Denko M K ,Sun T ,Woungang I. Trust management in ubiquitous computing: a Bayesian approach [J]. Computer Communications , 2011 34(3) : 398-406.
- [17] Zouridaki C ,Mark B L ,Hejmo M ,et al. E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks[J]. Ad Hoc Networks 2009 7(6) : 1156-1168.
- [18] Kim M ,Choo H ,Mutka M W ,et al. On QoS multicast routing algorithms using k-minimum Steiner trees[J]. Information Sciences , 2013 238(7) : 190-204.

附中文参考文献:

- [1] 林 闯 ,彭雪海. 可信网络研究[J]. 计算机学报 2005 28(5) : 751-758.
- [15] 王兴伟 ,王军伟 ,黄 敏. 基于狩猎搜索的可信 QoS 路由算法 [J]. 东北大学学报: 自然科学版 2012 33(10) : 1385-1389.