doi:10.3969/j.issn.1000-436x.2014.z2.029

基于信任评估的 Ad Hoc 网络关键节点选取算法

刘卓超[1]，杨力[1]，姜奇[1]，王巍[2]，曹春杰[3]

（1.西安电子科技大学 计算机学院，陕西 西安 710071；2. 中国电子科技集团 36 所
通信信息控制和安全技术重点实验室，浙江 嘉兴 314033；3. 海南大学 信息科学技术学院，海南 海口 570228）

摘 要：Ad Hoc 网络中存在关键节点，它们的失效会严重影响网络性能。为了有效地选取重要且可信的关键节点，给出了关键节点的定义，提出了一种基于信任评估的关键节点选取算法。首先利用节点收缩法计算节点的重要度，然后结合 D-S 证据理论，建立节点的信任评估模型，通过该模型得到节点的客观信任值来判断节点的可信度，最后综合考虑节点的重要度和可信度来选取关键节点。仿真实验结果表明，通过该方法得到的关键节点失效后将造成网络性能急剧下降。

关键词：Ad Hoc 网络；关键节点；节点收缩法；D-S 证据理论；信任评估
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0213-07

Critical nodes selection based on trust evaluation in Ad Hoc networks

LIU Zhuo-chao[1], YANG Li[1], JIANG Qi[1], WANG Wei[2], CAO Chun-jie[3]

(1.School of Computer Science and Technology , Xidian University, Xi'an 710071, China;
2. Science and Technology on Communication Information Security Control Laboratory, the 36th Research Institue of CETC, Jiaxing 314033, China;
3.College of Information Science and Technology, Hainan University, Haikou 570228 ,China)

Abstract: There are some critical nodes in Ad Hoc networks, and the failure of these critical nodes can critically affect the performance of the network. For the aim of selecting the important and trusted critical nodes in Ad Hoc networks, the definition of critical nodes is given, meanwhile, a critical nodes selection algorithm based on trust evaluation is proposed. By using the node contraction, the importance degree of the node is calculated. Then combined with D-S evidence theory, the trust evaluation model of critical node is presented, which is used to obtain the objective trust of the node and to judge the credibility of the node. Finally, the critical nodes are selected by considering of the importance degree and the credibility of the node. Simulation results show that when those critical nodes are failure, selected by the proposed algorithm, the network performance is decreasing significantly.

Key words: Ad Hoc networks; critical node; node contraction; D-S evidence theory; trust evaluation

1 引言

Ad Hoc 网络[1,2]不依靠任何基础设施，通过节点自组织、相互协作来实现网络通信。在 Ad Hoc 网络中会存在一些关键节点，这些节点的失效造成网络分割、节点通信的中断、数据分组的丢失等，极大地影响网络的连通性。同时，由于关键节点在网络中所处位置的关键性，一旦关键节点出现恶意行为[3]，将导致网络性能的急剧下降。因此，有效地发现关键节点能够为网络拓扑控制和安全防护提供必要

收稿日期：2014-07-02
基金项目：长江学者和创新团队发展计划基金资助项目（IRT1078）；国家自然科学基金资助项目（U1135002, 61202390, 61202389, 61173135, 61100230, 61100233）；陕西省自然科学基础研究计划基金资助项目（2012JM8025）；中央高校基本科研业务费基金资助项目（K5051303006）；信息保障技术重点实验室开发基金资助项目（KJ-14-109）
Foundation Items: The Program for Changjiang Scholars and Innovative Research Team in University(IRT1078); The National Natural Science Foundation of China (U1135002,61202390,61202389,61173135,61100230,61100233);The Natural Science Basic Research Plan in Shaanxi Province of China (2012JM8025);The Fundamental Research Funds for the Central Universities(K5051303006); The Foundation of Science and Technology on Information Assurance Laboratory(KJ-14-109)

的预知信息[4,5]。

现阶段关键节点的探测算法主要针对网络拓扑分割检测，文献[6]采用了集中式深度优先算法(DFS)查找网络中的关键节点，但所需的平均开销大，不适合大规模网络。文献[7]定义了 k 跳拓扑关键节点，将 k 跳拓扑关键节点作为全局关键节点，检测出关键节点的准确度与 k 有关，k 越大，准确度越高，但是额外的通信开销也会越大。文献[8]提出了一种基于中点覆盖圆的关键节点探测方法(DMCC)来探测局部关键节点，并论证中点圆半径为 $0.196r$ 时获得最大准确率，该算法开销小、检测速度快、适应动态拓扑。文献[9]针对网络中极易导致网络分割的关键节点，给出了关键节点存在的条件，提出了分布式拓扑分割探测算法(DPDP)，该算法有检测节点准确度高、开销小等特点，但是只适合平面化网络拓扑。

针对现有关键节点的定义局限于导致拓扑分割的全局关键节点，没考虑到关键节点的可信度等不足，本文给出了关键节点的定义，并引入信任评估机制，提出一种基于信任评估的关键节点选取算法，该算法综合考虑节点在网络拓扑中的重要性和数据传输中的可信度，最终选取重要度大且可信的节点作为关键节点。

2 关键节点及重要度

2.1 关键节点定义

Ad Hoc 网络中的关键节点[5~8]定义为由于该节点失效会直接导致网络被分割成多个部分，这种关键节点是全局关键节点。如图 1 所示，节点 L 失效会导致网络分割成 2 个部分，则节点 L 是全局关键节点。

但是在图 1 中，节点 C、D 或节点 A、D 同时失效也会导致网络分割，从而对网络性能造成很大影响，本文也将节点 A、C、D 考虑为关键节点。同时，由于在网络中所处位置的关键性，一旦关键节点出现恶意行为，使数据的成功转发率下降，将直接导致网络性能下降。因此，本文引入信任评估机制[10,11]，利用 D-S 证据理论对节点进行信任评估，保证选取关键节点的可信度，从而保证整个网络的可靠性。

本文着重考虑关键节点的可信度以及关键节点失效对网络性能的影响，提出了关键节点集合概念，关键节点集合中的节点满足 2 个条件：1) 关键节点必须是可信节点；2) 关键节点的失效导致网络性能下降最大化。所谓的最大化，是随着失效的关键节点数目的增加，网络性能趋于平缓变化。

具体地，将关键节点定义为在网络中重要度大而且可信的节点。节点的重要度大反映了节点在网络拓扑中处于关键位置，确保了该节点失效后影响的节点数目多和通过该节点的路径数目多；而节点可信反映了节点在数据通信中处于关键传输位置，确保了该节点数据传输的成功转发率高，以及该节点的失效会导致传输路径的数据丢失率高。因此，关键节点的定义综合考虑了节点在网络拓扑中的重要性和数据传输中的可信度。

例如，在应急救灾网络中，需要依靠通信设备如终端等自组织构建网络，为了能够有效组建网络以及达到对网络的安全保护等目的，可以在网络拓扑以及数据传输的关键位置选用可信任节点，充分确保数据传输可靠性。

本文提出一种选取关键节点集合的算法，该算法是对全局关键节点探测算法的有效补充，可以选取重要且可信的关键节点。

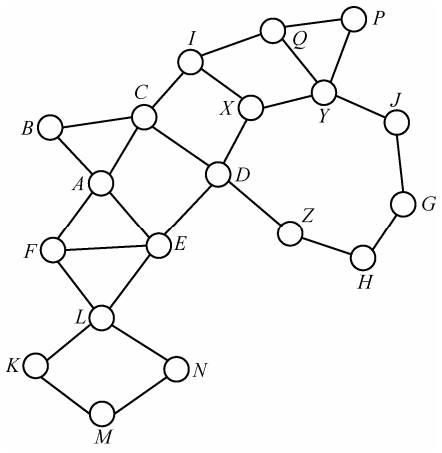

图 1 Ad Hoc 网络示意

2.2 重要度计算

为了确定节点在网络中的关键位置，本文利用节点重要度来衡量，并利用节点收缩法对重要度进行计算。所谓的节点收缩法[12]是将节点与相连接的邻居节点进行收缩融合，凝聚成一个节点。如果节点收缩后网络的凝聚度越大，则该节点越重要。

节点 L 的收缩过程如图 2 所示，将与节点 L 相连接的 E、F、K、N 都与 L 融合，即用新节点 L^* 代替，并将原来与它们连接的边都与新节点 L^* 相连接。

用图 G 来表示某网络，则图 G 的凝聚度[12]为

节点数目 n 与平均距离 l 乘积的倒数，用 $\partial(G)$ 表示。其定义如下。

$$\partial(G)=\frac{1}{nl}=\frac{1}{n\dfrac{\sum_{i\neq j\in V}d_{ij}}{n(n-1)}}=\frac{n-1}{\sum_{i\neq j\in V}d_{ij}} \tag{1}$$

其中，d_{ij} 表示节点 i 和 j 间的最短跳数。当 n=1 时，$\partial(G)=1$。

定义节点 v_i 重要度为

$$IMC(v_i)=1-\frac{\partial(G)}{\partial(G_{v_i})} \tag{2}$$

其中，G_{v_i} 表示节点 v_i 收缩后所得到的图。

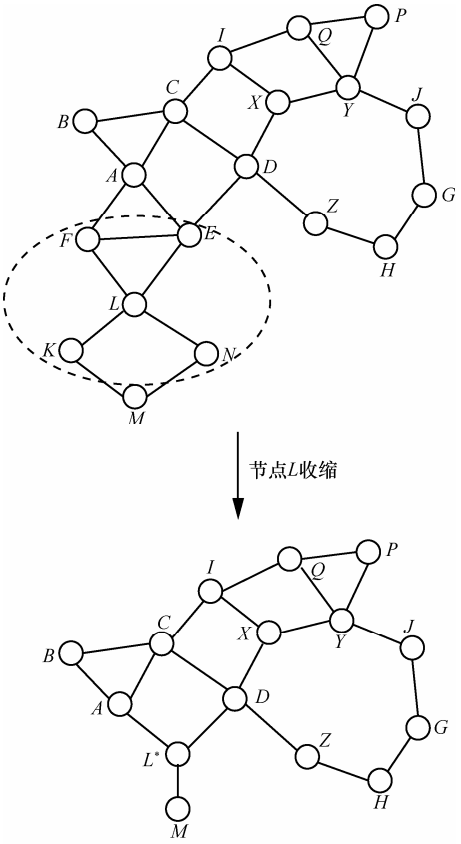

图 2　节点收缩过程

节点重要度的定义综合考虑了节点的连接度和通过该节点最短路径的数目。同时保证了该节点失效后影响的节点数目多以及影响通过该节点的路径数目多，能够比较客观地反映节点在网络中的重要程度。

3　基于 D-S 证据理论的信任评估

为了能够保证选取可信的关键节点，本文引入信任评估机制，利用 D-S 证据理论对节点进行信任评估。首先，对 D-S 证据理论的基本方法进行简要介绍，并给出本文所提出的基于 D-S 证据理论的信任评估模型。随后，通过该模型可以得到节点的客观信任值，并对客观信任值进行判断以确定节点是否可信。

3.1　D-S 证据理论

Dempster-Shafer(D-S)[13~15]证据可以有效解决信任评估中的随机性和主观不确定性，通过不断积累证据，能够在不需要先验分布的情况下，通过缩小假设集，为信任不确定信息的表达和合成提供了自然而强有力的方法。由于这些特点，D-S 证据理论在现阶段仍是进行信任评估的有效工具之一，本文采用 D-S 证据理论对节点进行信任评估。

3.2　信任评估模型

在 Ad Hoc 网络中，节点的邻居节点需要对该节点的直接信任值进行评估，即该节点转发邻居节点的数据分组的成功转发率。本文在评估直接信任的基础上，进一步评估节点的客观信任。这里的客观信任是综合考虑节点的所有邻居节点对它的直接信任值，由于邻居节点的主观性，对邻居节点的直接信任值进行修正，最后通过 Dempster 合成规则将所有邻居节点修正后的直接信任值进行合成，得到节点的客观信任值。客观信任值避免了邻居节点间主观判断带来的信任值错误，提供了相对客观的信任值来评价节点的可信度。

3.2.1　直接信任

在 Ad Hoc 网络中，节点的可靠性根据转发数据分组的成功率来评估，依据节点间直接交互历史计算节点的直接信任值。首先定义识别框架 θ={T,~T}，T 表示信任，~T 表示不信任。节点的直接信任值定义[16]为向量 $\boldsymbol{D}$，$\boldsymbol{D}$=(m({T}), m({~T}), m({T, ~T}))，其中，(m({T}), m({~T}), m({T,~T}))分别表示数据分组的成功转发率、拒绝转发率以及不确定是否成功转发率，它们的值分别用 α,β,γ 来表示，满足 0≤α,β,γ≤1, $\alpha-\beta-\gamma$=1。

由于节点直接信任值的动态性，节点的直接信任值在不同的时刻也会不同。初始时刻，邻居节点 i 和节点 j 间没有直接通信交互，因此节点 i 对节点 j 的直接信任向量 $\boldsymbol{D}_{i,j}(t_0)$=(0,0,1)。节点更新信任值的周期为 Δt（常量），当 t=t_n 时，$\boldsymbol{D}_{i,j}(t_n)$=($\alpha_n$,$\beta_n$,$\gamma_n$)，$\Delta t$ 以后，即 t=t_{n+j}=$t_n-\Delta t$，$\boldsymbol{D}_{i,j}(t_{n+1})$=($\alpha_{n+1}$,$\beta_{n+1}$,$\gamma_{n+1}$)。邻居节点 i 对节点 j 的直接信任值按照式(4)更新。

$$\boldsymbol{T}_{i,j}(t_{n+1})=(1-\omega)\boldsymbol{D}_{i,j}(t_n)+\omega\boldsymbol{D}_{i,j}(t_{n+1}) \tag{4}$$

其中，ω 是常量，表示权重系数。在直接信任值的更新过程中，节点 i 将动态选择 ω 的值，如果 $\alpha_{n+1}-\alpha_n \geqslant \beta_{n+1}-\beta_n$，那么 $\omega=\omega_1$；否则，即 $\alpha_{n+1}-\alpha_n < \beta_{n+1}-\beta_n$，那么 $\omega=\omega_2$，其中，ω_1、ω_2 满足 $0\leqslant\omega_1\leqslant 0.5\leqslant\omega_2\leqslant 1$。当 $\omega_1<\omega_2$ 时，体现了当前时刻的直接信任值的影响大于前一时刻，这种策略能够抑制恶意节点快速提升自己的直接信任值，同时在关键节点的选择上也能够排除恶意节点。为了表述方便，下文中的 $\boldsymbol{T}_{i,j}(t_n)$ 简写成 $\boldsymbol{T}_{i,j}$。

3.2.2 修正直接信任

在 Ad Hoc 网络中，在获取所有邻居节点对节点的直接信任值时，由于网络中节点存在恶意行为，导致产生虚假的直接信任值[17]。虚假的直接信任值与其他直接信任值的证据发生冲突，导致信任证据合成时产生不合理结果[18]。本文采用了折扣系数[19]，有效地解决了该问题。

假定分别得到了 k 个不同的邻居节点 $\{n_1, n_2, \cdots, n_k\}$ 相对节点 j 的直接信任向量。

$$\boldsymbol{T}_{n1,j}=(m_{n1,j}(\{T\}), m_{n1,j}(\{\sim T\}), m_{n1,j}(\{T,\sim T\}))$$
$$\boldsymbol{T}_{n2,j}=(m_{n2,j}(\{T\}), m_{n2,j}(\{\sim T\}), m_{n2,j}(\{T,\sim T\}))$$
$$\boldsymbol{T}_{nk,j}=(m_{nk,j}(\{T\}), m_{nk,j}(\{\sim T\}), m_{nk,j}(\{T,\sim T\}))$$

通过证据距离公式[20]，计算得到任意 2 个直接信任向量 $\boldsymbol{p}$, $\boldsymbol{q}$ 的证据距离 $d_{p,q}$，$d_{p,q}$ 反映了第 p_{th} 个直接信任值与第 q_{th} 个直接信任值之间的冲突程度。$\boldsymbol{p}$,$\boldsymbol{q}$ 的相似度记作 $S_{p,q}$，那么 $S_{p,q}=1-d_{p,q}$，且 $S_{p,q}=1-S_{q,p}$。将所有的 $S_{p,q}$ 构建成 $k\times k$ 的相似度矩阵 $\boldsymbol{S}$。

$$\boldsymbol{S}=\begin{vmatrix} 1 & S_{1,2} & \cdots & S_{1,k} \\ S_{2,1} & 1 & \cdots & S_{2,k} \\ \vdots & \vdots & \vdots & \vdots \\ S_{k,1} & S_{k,2} & \cdots & 1 \end{vmatrix} \tag{5}$$

由 D-S 证据理论可以得知，当证据间发生冲突时。如果一个证据与其他大多数证据保持一致性，那么这个证据将对最终融合结果产生较大影响。因此，每个证据的权重与被其他证据的综合支持程度成正比。在得到证据的相似度矩阵 $\boldsymbol{S}$ 后，可以通过矩阵分析法来确定邻居节点中每个直接信任向量的权重[21]。

设第 p_{th} 个直接信任向量的支持度为 η_p，那么 $\eta_p=\sum_{q=1,q\neq p}^{k} S_{p,q}$，其标准权重系数 $\chi_p=\eta_p\Big/\sum_{q=1}^{k}\eta_q$，且满足 $\sum_{p=1}^{k}\chi_p=1$。选其中最大的系数 $\chi_{\max}$ 作为关键证据，可以根据 $factor=[f_1,f_2\cdots,f_k]=[\chi_1,\chi_2\cdots,\chi_k]\big/\chi_{\max}$ 得到每个向量的折扣系数。最后根据折扣系数 $factor$，节点 j 对邻居节点 $\{n_1,n_2,\cdots,n_k\}$ 的直接信任向量做如下修正。

$$\begin{cases} m'_{n_i}(A)=f_i m_{n_i}(A), A\subset\theta \\ m'_{n_i}(\theta)=1-f_i+f_i m_{n_i}(\theta)=1-\sum m'_{n_i}(A) \end{cases} \tag{6}$$

这样，就可以得到修正后直接信任值 $T'_{n_i,j}$。

由上述方法可知，邻居节点中的直接信任向量之间的冲突越严重，其折扣系数就越小，对客观信任值的最终合成的影响就越弱。这样可以有效地削弱恶意节点的直接信任值对客观信任值的影响，提高网络的可靠性。

3.2.3 客观信任

根据 Dempster 组合规则对修正后直接信任值 $T'_{n_i,j}$ 进行合成，得到节点 j 的客观信任值，其满足下述条件。

$$\begin{cases} m^*_j(A)=\left(m'_{n_1,j}(A)\oplus m'_{n_2,j}(A)\right)\oplus\cdots\oplus m'_{n_k,j}(A), A\subset\theta \\ m^*_j(\varnothing)=0 \end{cases} \tag{7}$$

在计算过程中，选取一个合适的常量 ε 作为阈值来判断节点是否可信。如果 $m^*_j(\{T\})\geqslant\varepsilon$，那么认为节点 j 可信。

4 关键节点选取算法

依据关键节点的定义，为了选出网络中处在关键位置且可信的关键节点。本文提出了基于信任评估的关键节点选取算法，该算法把节点的重要度和客观信任值作为选取关键节点的度量。采用节点收缩法计算节点的重要度，利用 D-S 证据理论来计算节点的客观信任值，并根据客观信任值判断节点是否可信，最终选取重要度大且可信的节点作为关键节点。

本算法假设已经获取网络的拓扑结构图，网络拓扑获取方法具体可参考文献[22,23]。在 Ad Hoc 网络中通过一个网关节点获取网络拓扑结构，并假设网关节点的计算处理能力足够强大，关键节点选取过程都在网关节点中进行。

算法具体过程如下。

1) 网关节点根据网络的点集合与边集合，获取节点之间最短距离的邻接矩阵，根据式(1)计算出网

络的凝聚度。同时，采用节点收缩法，依次计算节点收缩后的网络凝聚度。最后根据式(2)得到所有节点的重要度集合，并将重要度由大到小进行排序，得到节点重要度排序集合。

2) 网络初始化时，节点实时监测邻居节点集，收集对邻居节点的直接信任向量。一个时间间隔 T 后，根据式(4)计算节点的直接信任值并存储起来。网关节点间隔时间 T 向网络中广播信任值请求分组，所有节点收到信任值请求分组后，向网关节点发送包含直接信任值的回复分组。网关节点收到回复分组后，得到所有节点间的直接信任值，并按照 3.3.2 节依次修正直接信任值，最后得到所有节点的客观信任值。

3) 网关节点依次判断节点客观信任值是否大于 ε，如果是，则将节点加入到信任集合中。其中阈值 ε 根据网络中传输数据等级确定的：当传输数据等级为重要等级时，阈值 ε 的取值范围为[0.9,1]；当传输数据等级为次要等级时，阈值 ε 的取值范围为[0.8,1]；当传输数据等级为普通等级时，阈值 ε 的取值范围为[0.7,1]。

4) 从节点重要度排序集合和信任集合的交集中，重要度排序集合排在网络节点数前 $r\%$ 的节点选取作为关键节点，选取关键节点的数目根据网络规模确定，即关键节点失效后网络性能下降最大化时的数目。根据文献[6]，r 的取值范围为[5,30]。

本算法目前只适用于静态网络拓扑，如果考虑到网络拓扑动态变化，可以在步骤 1) 中间隔一个固定时间 T 重新获取网络拓扑，随后再依据算法进行计算。本算法对全局关键节点探测算法进行补充完善，可以选取出处在关键位置且可信的关键节点。同时对全局关键节点进行信任评估，当全局关键节点的信任值不满足要求时，不选取为关键节点。此时考虑网络的安全性，需要对全局关键节点进行替换补偿，可以从本算法的信任集合中选取信任补偿节点。

5　仿真实现与性能分析

5.1　仿真设置

为了验证本文所提出的关键节点选取算法的有效性，使用 NS3 [24]对算法进行实验仿真，并对仿真结果进行分析。在本实验仿真中，设定仿真场景为一个由 50 个无线节点随机分布在 1 000 m×1 000 m 的方形区域，每个节点都有 802.11 接口和全向天线，无线节点的传输范围 250 m，在选取关键节点时根据网络规模以及选定传输数据为普通等级，设定阈值 ε=0.7，r=20%。仿真参数如表 1 所示。

表 1　　仿真环境参数

参数	值
场景	1 000 m×1 000 m
MAC 类型	IEEE 802.11
信道类型	Wi-Fi Channel
路由协议	AODV
移动模型	Constant Position
传输数据类型	CBR
仿真时间	300 s
通信距离	250 m
数据分组大小	512 byte
数据分组发送速率	4 packet/s
节点数	50

5.2　仿真结果及分析

5.2.1　网络数目变化

随机生成 30 个 Ad Hoc 网络拓扑，在上述仿真环境下，分别得到全局关键节点以及本文选取的关键节点。然后对这些网络的全局关键节点以及本文选取的关键节点进行攻击，使其失效。选择节点失效后网络的分组投递率作为网络性能指标。

图 3 给出了不同网络数目下全局关键节点和本文关键节点失效后网络分组投递率的比较，从图中可以看出，本文关键节点失效导致分组投递率基本保持在 20%~30%左右，比全局关键节点要低很多。这验证了本文选取的关键节点比全局关键节点对网络性能影响更大。同时两者失效导致的分组投递

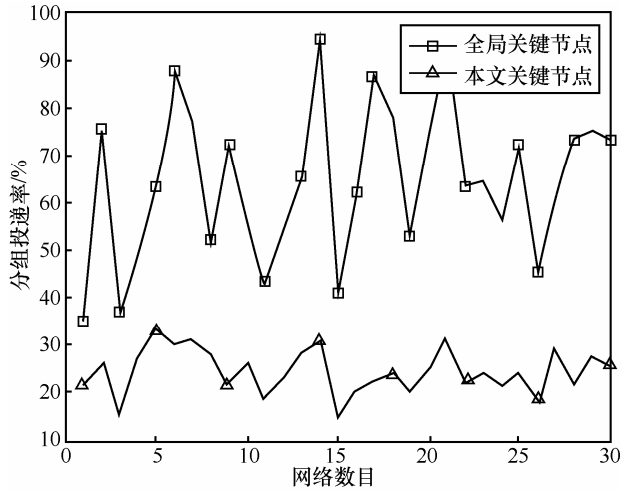

图 3　分组投递率比较

率变化波动比较大，这是由于网络的拓扑结构不同，全局关键节点的数目也不同。这也进一步表明对于不同的 Ad Hoc 网络受到攻击的难易程度有很大不同。

5.2.2 失效节点数目变化

随机生成一个 Ad Hoc 网络拓扑，对网络中普通节点与关键节点进行攻击，使其失效，选择分组投递率、丢失率、吞吐量参数作为网络指标，通过对比在不同数目下，关键节点与普通节点失效后网络性能的变化。

图 4 给出了不同数目的关键节点和普通节点失效后网络分组丢失率的比较。从图中可以看出，当失效的节点数量较少时，网络具有较小的分组丢失率，随着失效节点的数目的增加，两者的分组丢失率都增加。普通节点失效后导致分组丢失率变化不大，而关键节点失效后导致分组丢失率的增加幅度要远远大于普通节点的。说明关键节点失效，导致更多链路断裂，节点通信中断，节点间数据传输丢失率高，导致分组丢失率急剧增加。

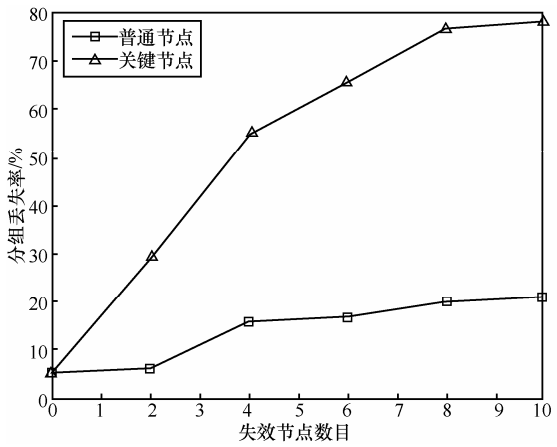

图 4　分组丢失率比较

图 5 给出了不同数目的关键节点和普通节点失效后网络分组投递率的比较。从图中可以看出，随着失效节点数目的增加，分组投递率都呈现下降趋势。但是普通节点的失效对网络的性能影响不大，保持在 80%左右，而关键节点的失效导致分组投递率迅速下降，直到 20%左右，且两者的差距十分明显。

图 6 给出了不同数目的节点失效后网络吞吐量的变化。从图中可以看出，随着失效节点数目的增加，关键节点和普通节点失效后网络的吞吐量都下降，普通节点失效后的下降幅度不大，而关键节点失效后的下降幅度更大。这是因为关键节点处在网络中的关键位置，有更大的连接度，失效后影响更多节点间的数据传输，导致网络中的数据传输能力减弱，从而导致吞吐量急剧下降。

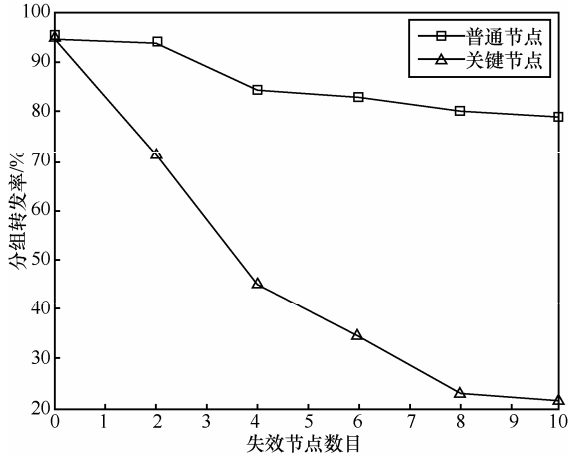

图 5　分组转发率比较

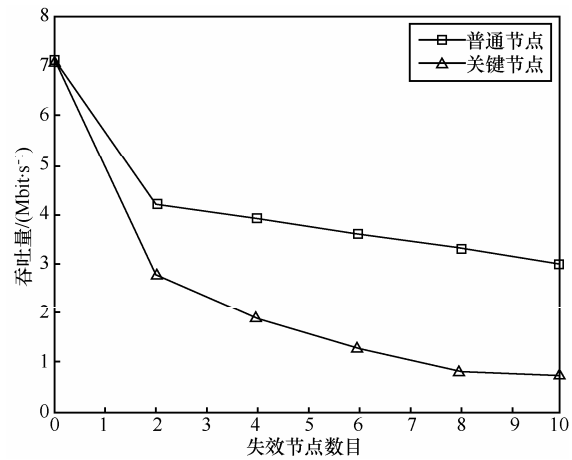

图 6　吞吐量比较

6　结束语

针对现有关键节点的选取局限于导致拓扑分割的全局关键节点，且没考虑到关键节点的可信度，本文给出了关键节点的定义，提出了基于 D-S 证据理论的关键节点选取算法，该算法综合考虑了关键节点在网络拓扑中的重要性和数据传输中的可信度，选取出重要且可信的关键节点。通过仿真实验结果表明，本算法选取的关键节点的失效导致网络分组投递率和吞吐量急剧下降。同时也表明对 Ad Hoc 网络攻击，重点选择攻击比随机攻击的效果要好。

本文所做的工作，进一步可以在网络拓扑控制上为全局关键节点替换补偿提供信任节点的选取，在网

络安全防护上为通过保护少部分节点（如本文提出的关键节点）来保护整个网络提供了一种新思路。

参考文献：

[1] RAMANATHAN R, REDI J. A brief overview of Ad Hoc networks: challenges and directions[J]. IEEE Communication Magazine, 2002, 40(5) : 20-22.

[2] YANG H, LUO H, YE F. Security in mobile Ad Hoc networks: challenges and solutions[J]. Wireless Communications, IEEE, 2004, 11(1): 38-47.

[3] BASU P, REDI J. Movement control algorithms for realization of faultolerant Ad Hoc robot networks[J]. IEEE Network, 2004, 18(4): 36-44.

[4] SHEN Z, CHANG Y L, CUI C. A fault-tolerant and minimum-energy path-preserving topology control algorithm for wireless multi-hop networks [A]. International Conference on Computational Intelligence and Security (CIS)[C]. Xi'an, China, 2005.864-869.

[5] GOYAL D, CAFFERY J. Partitioning avoidance in mobile Ad Hoc networks using network survivability concepts[A].The 7th IEEE Symposium on Computers and Communications (ISCC)[C]. Taormina, Italy, 2002. 553- 558.

[6] JORGIC M, HAUSPIE M, SIMPLOT-RYL D. Localized algorithms for detection of critical nodes and links for connectivity in Ad Hoc networks[A]. Proceedings of 3rd IFIP Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET 2004)[C]. Turkey, 2004.12.

[7] SHENG M, LI J D, SHI Y. Critical nodes detection in mobile Ad Hoc network[A]. IEEE the 20th International Conference on Advanced Information Networking and Applications (IEEE AINA)[C]. Vienna, Austria, 2006.336-340.

[8] 李建东, 田野, 盛敏. 大规模 Ad Hoc 网络拓扑分割探测研究[J]. 通信学报, 2008, 29(9): 54-61.
LI J D, TIAN Y, SHENG M. Partition detection for large scale Ad Hoc networks[J]. Journal on Communications , 2008, 29(9): 54-61.

[9] MARTI S, GIULI T J, LAI K, *et al*. Mitigating routing misbehavior in mobile Ad Hoc networks[A]. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking[C]. ACM, 2000.255-265.

[10] GOVINDAN K, MOHAPATRA P. Trust computations and trust dynamics in mobile Ad Hoc networks: a survey[J]. Communications Surveys & Tutorials, 2012, 14(2): 279-298.

[11] CHO J H, SWAMI A, CHEN R. A survey on trust management for mobile Ad Hoc networks[J]. Communications Surveys & Tutorials, 2011, 13(4): 562-583.

[12] 谭跃进, 吴俊, 邓宏钟. 复杂网络中节点重要度评估的节点收缩方法[J]. 系统工程理论与实践,2006,26(11): 79-83.
TAN Y J,WU J, DENG H Z. Evaluation method for node importance based on node contraction in complex networks[J]. Journal of Systems Science and Information, 2006, 26(11):79-83.

[13] DEMPSTER A P. Upper and lower probabilities induced by a multi-valued mapping[J]. The Annals of Mathematical Statistics, 1967, 38(2): 325-339.

[14] SHAFER G. A Mathematical Theory of Evidence[M]. Princeton: Princeton University Press, 1976.

[15] AHMED M R, HUANG X, SHARMA D. A novel misbehavior evaluation with dempster-shafer theory in wireless sensor networks[A] Proceedings of the thirteenth ACM international symposium on Mobile Ad hoc Networking and Computing[C]. ACM, 2012.259-260.

[16] 叶阿勇, 马建峰. 一种移动自组网中信任评估模型的设计[J].计算机研究与发展, 2008, 45(5): 765-771.
YE A Y, MA J F. A trust valuation model in MANET[J]. Journal of Computer Research and Development, 2008, 45(5): 765-771.

[17] ING Q, TANG L CHEN Z. Trust management in wireless sensor networks[J]. Journal of Software, 2008, 19(7):1716-1730.

[18] ZADEH L A. A simple view of the Dempster-Shafer theory of evidence and its implication for the rule of combination[J]. AI Magazine, 1986, 7(2): 85-90.

[19] MURPHY C K. Combining belief functions when evidence conflicts[J]. Decision Support Systems, 2000, 29(1):1-9.

[20] JOUSSELME A L, MAUPIN P. Distances in evidence theory: Comprehensive survey and generalizations[J]. International Journal of Approximate Reasoning, 2012, 53(2): 118-145.

[21] 陈一雷, 王俊杰. 一种 D-S 证据推理的改进方法[J].系统仿真学报, 2004, 16(1): 28-30.
CHEN Y L, WANG J J. An improved method of D-S evidential reasoning [J]. Journal of System Simulation, 2004, 16(1):28-30.

[22] WEI J, GUO W, SU J, *et al*. Mobile agent based topology discovery in mobile Ad Hoc networks[A]. Wireless Communications, Networking and Mobile Computing 2009[C]. 2009.1-4.

[23] MIGAS N, BUCHANAN W J, MCARTNEY K A. Mobile agents for routing topology discovery, and automatic network reconfiguration in ad-hoc networks[A]. Engineering of Computer-Based Systems,2003. Proceedings. 10th IEEE International Conference and Workshop on the IEEE[C]. 2003.200-206.

[24] NS3[EB/OL]. http://www.nsnam.org.

作者简介：

刘卓超（1990-），男，湖北武汉人，西安电子科技大学硕士生，主要研究方向为无线自组织网络路由协议及安全技术等。

杨力（1977-），男，陕西乾县人，西安电子科技大学副教授、硕士生导师，主要研究方向为无线网络安全、可信计算、应用密码学等。

姜奇（1983-），男，安徽全椒人，西安电子科技大学副教授、硕士生导师，主要研究方向为安全协议及无线网络安全技术。

王巍（1980-），男，河北张家口人，中国电子科技集团 36 所高级工程师，主要研究方向为网络安全、网络对抗等。

曹春杰（1977-），男，河北衡水人，海南大学副教授，主要研究方向为信息安全、应用密码学。