基于级联失效的复杂保障网络抗毁性仿真分析*

李 勇, 邓宏钟, 吴 俊, 吕 欣, 刘 斌, 谭跃进
(国防科学技术大学 信息系统与管理学院, 长沙 410073)

摘 要: 通过引入流量强度指数 α和流量分布指数 β,建立了不同网络流量下的复杂负载网络级联失效抗毁性模型。基于该模型比较分析了无标度网络、随机网络和介于这两种网络之间的特定复杂保障网络在不同流量强度和流量分布下对单个节点的随机失效与故意攻击的抗毁性。结果表明,在考虑级联失效的条件下,复杂保障网络的抗毁性随着流量强度的增加急剧下降。此外,流量分布对复杂保障网络的抗毁性也具有显著影响,在流量强度一定的条件下改变网络的流量分布能有效提高网络的抗毁性。

关键词: 保障网络; 级联失效; 抗毁性; 流量强度
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2008)11-3451-04

Invulnerability simulation analysis of complex logistics networks based on cascading failure

LI Yong, DENG Hong-zhong, WU Jun, LV Xin, LIU Bin, TAN Yue-jin
(*School of Information Systems & Management, National University of Defense Technology, Changsha* 410073, *China*)

Abstract: By the analysis of characteristics of complex logistics networks, a simulation model based on cascading failure for its invulnerability was proposed. In this model, the intensity and distribution of network traffic was controlled by an α-index and a β-index, respectively. The variety of invulnerability was simulated under random failures and intentional attacks on different networks. Result shows that the invulnerability performance declines rapidly when the network traffic is increased. Furthermore, the distribution of network traffic also has a strong impact on the invulnerability performance.

Key words: logistics networks; cascading failure; invulnerability; network traffic

引言

几乎所有的复杂系统均可以抽象成网络模型,这些网络往往具有大量的节点,节点之间有着复杂的连接关系。复杂网络不仅仅指无标度网络,它还包括介于随机网络与无标度网络间的其他网络,把它们统称为复杂网络。随着人们对网络的依赖程度日益增高,一个广受关注的问题逐渐凸现出来:这些网络到底有多可靠?

日常生活中所涉及的大量网络,如何降低它们的失效概率,提高它们的抗毁性具有重要意义。例如,在 2008年的奥运会期间,在高负载、出现突发事件情况下,如何提高北京市的物资运输和人流输送网络的抗毁性、高效性,对于确保奥运会的正常进行,以及提高我国的形象和地位就具有极其重要的意义;对于生活中人们天天用到的通信网络,提高其抗毁性对确保人民的正常生活秩序,确保经济系统的正常运行,节约经济成本,提高经济效率与效益就有其重要的意义和实际的价值;对于大型企业的销售业务网,提高抗毁性就是提高企业的竞争力。生物领域也存在同样的问题,基因网络中的一些核心基因的故障会带来灾难性的后果。

以往的复杂网络抗毁性研究[1,2]主要关注的是静态的抗毁性,不考虑节点(边)失效的动态关联,即总是假设一个节点(边)的失效不会导致其他节点(边)的失效。这方面研究最重要的成果就是无标度网络的双重性:面对随机性的损伤,无标度网络比随机网络有着更好的抗毁性,但面对选择性打击,无标度网络却显得异常脆弱[2]。在这种假设下,少数几个节点的失效不会导致整个网络的崩溃,而事实并非如此。实际上大多数网络上是有负载的[3],这些负载可以是物质、信息或能量,可以是具体的,也可以是抽象的。网络上的负载是动态变化的,特别是当网络结构发生改变,如节点的加入、移除,网络上的负载将重新分配。一般来说,网络中节点承受负载的能力是有限的,即节点的容量是有限的。有限的容量和负载的重新分配使得负载网络的抗毁性问题变得更加复杂:一个节点的失效导致网络负载的重分配,负载的重分配可能使得某些节点上的负载超过其容量而失效,这些节点的失效又可能导致其他节点的级联失效(cascading failure)[4]。如果开始移除的是一个重要的关键节点,它的移除可能触发整个网络的崩溃,称之为级联崩溃(cascading breakdown)。这种现象[5,6]比故意攻击网络的后果更严重[2]。最典型的一个例子是 2003年北美电力网大崩溃事故。北美电力网就因为频率异动瞬间波及全网,导致级联崩溃。同样的问题也存在于因特网[7,8]、通信网[9]、交通

收稿日期: 2008-01-12; **修回日期**: 2008-03-28 **基金项目**: 国家自然科学基金资助项目(70501032, 70771111)

作者简介:李勇(1979-),男,湖南长沙人,博士研究生,主要研究方向为复杂网络抗毁性(stoneliyong@163.com);邓宏钟(1974-),硕导,博士,主要研究方向为复杂系统理论、分布式人工智能和遗传算法;吴俊(1980-),博士研究生,主要研究方向为复杂网络理论;吕欣(1984-),博士研究生,主要研究方向为复杂网络理论;刘斌(1982-),博士研究生,主要研究方向为复杂网络建模;谭跃进(1958-),博导,主要研究方向为系统理论与综合集成.

物流网以及其他社会经济系统网络中[10]。例如,2008年奥运会期间,突发事件就有可能造成北京交通网络的级联崩溃,即交通瘫痪。级联失效的本质是一种相关失效[11],而网络安全中的相关失效行为一直是一个非常棘手的问题,这源于对网络中相关失效机理知之甚少,特别是定量分析方法非常缺乏。复杂网络上的级联失效研究近年来得到了很大关注。2002年,Watts给出了一个级联失效过程的简单模型[5],它能转换到一类渗流模型之上,从而可以利用与针对简单顶点删除过程而言类似的生成函数方法来解。2002年,Holme等人[4,10]研究了演化网络上的级联失效,提出了一个基于负载重分配的级联失效模型,Motter等人[3]研究发现非同质拓扑结构中级联失效对选择性打击的敏感性,Moreno[12]; 2004年,Zhao Liang等人[13]研究了级联失效中的临界现象,Motter[14]研究了级联失效的防御和控制,Dobson等人[7~9]研究了电力网中的级联失效问题,Wang Xiao-fan等人[15]研究了耦合映像格子中的级联失效; 2006年,Wu和 Zhao等人[16]研究了具有群落结构的无标度网络的级联失效问题,并提出了一种新的路由规则来控制无标度网络的级联失效[17]。

这些已有的基于级联失效的网络抗毁性模型并不适合复杂保障网络:模型不能反映网络不同节点对之间发送不同的物资量;不同环境下的网络流量强度不同,模型不能反映这种不同的网络流量强度对抗毁性的影响。本文通过引入运载函数和流量强度指数等对网络流量强度、节点容量等进行了定义,建立了基于级联失效的复杂保障网络抗毁性模型,分析了复杂保障网络在不同流量强度和不同流量分布下的抗毁性。

基于级联失效的复杂保障网络抗毁性模型

复杂网络抗毁性研究中,用图 $G=(V,E)$来表示网络。假设 G是一个无向的加权连通图,有 n个节点,m 条边。其中:$V=\{v_1, v_2, v_3, \cdots, v_n\}$代表节点集合; $E=\{e_1, e_2, e_3, \cdots, e_m\}\subseteq V\times V$代表边的集合。

. 网络的节点和边

在复杂保障网络中,把所有的保障实体、交通枢纽抽象为节点。将连接节点间的公路、铁路、水路、航线、管线等抽象成网络的边。假设所有不同类型的节点都用 $v_i\ (i=1, 2, \cdots, n)$表示,所有不同类型的边都用 $e_j\ (j=1, 2, \cdots, n)$表示。

. 流量强度与流量分布

本模型中,定义网络流量强度为某一时刻进入网络的物资量总和,即在某一时刻所有节点发送物资量的总和。定义网络流量分布为网络中所有节点对之间发送物资量的空间分布。

网络流矩阵为

$$U=\begin{bmatrix} f_{11} & \cdots & f_{1k} & \cdots & f_{1n} \\ \cdots & & \cdots & & \cdots \\ f_{j1} & \cdots & f_{jk} & \cdots & f_{jn} \\ \cdots & & \cdots & & \cdots \\ f_{n1} & \cdots & f_{nk} & \cdots & f_{nn} \end{bmatrix} \tag{1}$$

其中:f_{jk}为运载函数,表示节点 v_j发送给节点 v_k的物资量。

流量强度 $NF=\sum f_{jk}$,表示所有发送物资量的总和。

定义

$$f_{jk}=\begin{cases} \alpha\times(d_j^{\beta}/2+d_k^{\beta}/2)\times n/\sum_{j=1}^{n}d_j^{\beta} & (j\neq k,\ 0\leq\alpha\leq 1) \\ 0 & (j=k) \end{cases} \tag{2}$$

其中:d_j和 d_k分别表示节点 v_j、v_k的度;α为流量强度指数,用来调节发送物资量的多少,当 $\alpha=1$, $f_{jk}=f_{jk}^{\max}$表示节点对 v_j、v_k之间发送最大物资量;β为流量分布指数,用来表示运载函数和度的关联程度。这样可以得到

$$NF=\sum f_{jk}=\alpha\times n(n-1) \tag{3}$$

流量强度 NF由网络的大小 n和流量强度指数 α决定,与β无关。这样改变 α的大小就可以改变流量强度。

当 $\beta>0$时,表示 f_{jk}与节点的度正相关,节点的度越大,该节点越重要,发送的物资量越多;当 $\beta<0$时,表示 f_{jk}与节点的度负相关,节点的度越大,该节点越不重要,发送的物资量越少;当 $\beta=0, \alpha=1$时,表示所有节点对之间发送的物资量都为一个单位,与已有模型的假设一致。本模型中,在流量强度 NF不变(α值不变)的条件下,改变 β值,可以改变网络的流量分布。

. 节点的负载量

本模型中,定义节点 v_i的负载量 $F_i\ (i=1, 2, 3, \cdots, n)$,为所有节点对 v_j、v_k之间按照最短路(如时间最短、距离最短)原则发送的物资,经过节点 v_i的流量和

$$F_i=\sum_{j\neq k}f_{jk}(i)\ (i=1, 2, 3, \cdots, n) \tag{4}$$

其中: $f_{jk}(i)$为节点对 v_j、v_k之间发送 f_{jk}的物资经过节点 v_i的流量。

. 节点的容量

节点的容量表示节点可以承受的最大负载量。本模型中,定义节点 v_i的容量

$$C_i=F_i^{\max}=\sum_{j\neq k}f_{jk}^{\max}(i)\ (i=1, 2, 3, \cdots, n) \tag{5}$$

$f_{jk}^{\max}(i)$表示所有节点对 v_j、v_k之间发送最大物资量 $f_{j\,k}^{\max}(\alpha=1)$时经过节点 v_i的流量。

. 负载的重分配策略

基于级联失效的抗毁性模型的负载重分配策略有很多形式,在本模型中,假设当某个节点或(和)边出现故障时,经过这些损坏节点或边的运输物资将按重新计算出来的新的最短路运输,实现了网络负载重分配。

. 级联失效过程

在本模型中,节点的初始攻击(initial damage)被处理为删除一个节点,初始节点的删除导致网络负载的重分配,因网络中节点的最大容量是确定的,重分配的负载可能会超过某些节点的容量,从而导致这些节点出现级联故障。这些故障节点也从网络中删除。这些级联故障节点的删除又可能产生下一轮的负载重分配,可能出现新的级联故障,该级联过程可延续到没有新的级联故障节点出现才停止。在剩余网络(节点删除以后的网络)中,网络可能被分割成一些不连通的子网和孤立节点,子网内部可实现相互间的物资发送,而孤立节点则不具备物资的发送和接收能力。

. 抗毁性的度量

在本文中,用级联失效后网络的最大连通片尺寸与网络尺寸之比[14]来度量复杂保障网络的抗毁性,即

$$R=N'/N \tag{6}$$

其中:N 表示复杂保障网络在攻击以前网络节点的数目;N 表示在攻击以后最大连通尺寸中节点的数目。

仿真分析

. 仿真设计

仿真设计主要包括网络结构、攻击形式的设计,以及对网络在不同流量强度和不同流量分布下抗毁性的比较分析。

1)网络结构　复杂保障网络是介于无标度网络和随机网络之间的一种网络。本文分别以 Barabasi的 BA模型[18]生成的无标度网络、ER模型[19]生成的随机网络和某保障网络作为研究对象。为了进行对比分析,三种网络的节点数均为 100,每种网络产生 10个。在本文中,BA网络初始节点 $n_0=2$,每个时间步增加一个节点和 $m=2$条边,平均度 $\overline{d_k}=4$。ER随机网络中任意两节点的连接概率 $p=0.04$,平均度 $\overline{d_j}=4$。保障网络由保障系统中的交通网络、存储网络和中转网络抽象而成,平均度 $\overline{d_i}=3.8$。

2)攻击形式　本文主要研究复杂保障网络在故意攻击和随机失效两种条件下的抗毁性。在仿真过程中故意攻击是指移除网络中负载量最大的单个节点;随机失效是指随机的移除网络中的单个节点。

3)比较设计　首先比较分析不同的流量强度下 (不同 α)每种网络对于单个节点移除的抗毁性;然后比较分析不同的流量分布下 (不同 β)每种网络对于单个节点移除的抗毁性。

. 仿真结果

1)不同流量强度下网络的抗毁性　不同流量强度下网络的抗毁性需要研究的是在网络流量分布均匀 (β=0)的条件下不同的流量强度对于抗毁性的影响。图 1(a)表示 ER随机网络在不同的流量强度下对于单个节点移除的抗毁性;图 1(b)表示 BA网络在不同流量强度下对于单个节点移除的抗毁性;图 1(c)表示复杂保障网络在不同流量强度下对于单个节点移除的抗毁性。其中,空心圆表示故意攻击 (intentional attacks);实心圆表示随机失效 (random failure)。图的横轴表示 α,用来度量流量强度;图的纵轴表示最大连通片比 R,用来度量网络的抗毁性。每种网络都对 10个具体网络的仿真结果进行平均,每一个网络都仿真 10次。

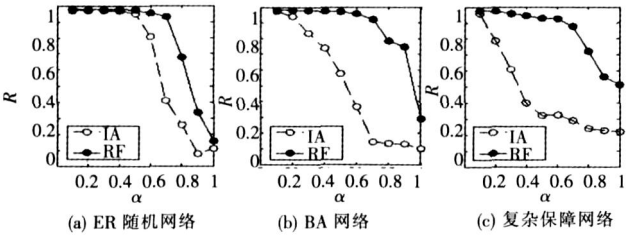

图 1　不同流量强度下网络的抗毁性

通过仿真结果分析发现:ER随机网络 (图 1(a))在流量强度不大时对单个节点的移除表现出很强的抗毁性,在 α的一段变化区间内 (α<0.5),网络随着 α的变化,抗毁性曲线几乎没有变化;随机失效和故意攻击都存在一个 α临界点 α^*,当 $\alpha<\alpha^*$,网络完好;当 $\alpha>\alpha^*$,网络开始级联失效,随机失效中 $\alpha^*\approx0.7$,故意攻击中 $\alpha^*\approx0.5$。BA网络 (图 1(b))中,网络对于随机失效和故意攻击的抗毁性差异很大,随机失效在 α=0.7时网络的抗毁性仍然很好 ($R>0.9$),甚至在网络接近饱和状态时 (α=0.9),网络的抗毁性指标还可以达到 70%以上;相反,故意攻击在流量强度很小时就出现级联失效 ($\alpha^*=0.2$),在 α=0.7时,网络几乎崩溃 ($R<0.15$)。复杂保障网络 (图 1(c))中,故意攻击的 α临界点在 α很小时就出现了 ($\alpha^*\approx0.1$),在 α=0.4时,网络抗毁性指标 (R)已经降到 40%以下;随机失效的 α临界点为 $\alpha^*\approx0.7$,在流量强度达到满负荷时 (α≈1),保障网络对于随机失效的抗毁性指标 (R)依然能达到 50%以上,这说明复杂保障网络对于随机失效有较好的抗毁性,对于故意攻击的抗毁性很差。

2)不同流量分布下的抗毁性　在复杂保障网络中,节点对之间发送的物资量与节点的重要性有关。模型中以度的函数 (运载函数 f_{jk})来表示这种关系,通过改变 β,可以改变网络流量分布。图 2(a)表示 ER随机网络在不同流量分布 (不同 β)下对于故意攻击的抗毁性;图 2(b)表示 ER随机网络在不同流量分布 (不同 β)下对于随机失效的抗毁性;图 2(c)表示 BA网络在不同流量分布 (不同 β)下对于故意攻击的抗毁性;图 2(d)表示 BA网络在不同流量分布 (不同 β)下对于随机失效的抗毁性;图 2(e)表示复杂保障网络在不同流量分布 (不同 β)下对于故意攻击的抗毁性;图 2(f)表示复杂保障网络在不同流量分布 (不同 β)下对于随机失效的抗毁性。图的横轴表示流量强度指数 α,用来度量流量强度,图的纵轴表示最大连通片比 R,用来度量网络的抗毁性。每种网络都对 10个具体网络的仿真结果进行平均,每一个网络都仿真 10次。

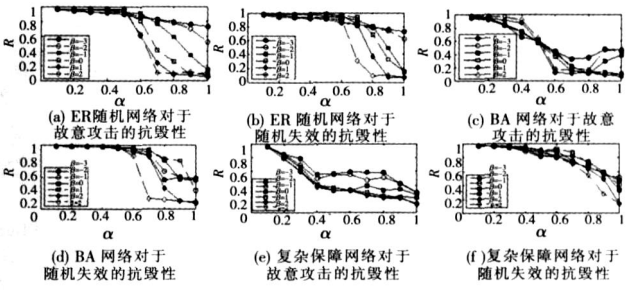

图 2　不同流量分布下的抗毁性

仿真结果表明,在 ER随机网络 (图 2(a)(b))中,在流量强度很小时 (α<0.5),无论是故意攻击还是随机失效,网络的抗毁性都很好 ($R>0.9$);随机网络对于故意攻击和随机失效的抗毁性曲线很相似,只是 α临界点 (α^*)有些差异,随机失效的 α^*比故意攻击的 α^*稍大,网络的抗毁性都随着 β的减小而递增,当 β=-3时,网络的抗毁性最好,即使网络满负荷运行 (α=1),网络的抗毁性指标 (R)均可以达到 80%以上。

在 BA网络中 (图 2(c)),存在一个故意攻击临界点 (α≈0.5),当 $\alpha<\alpha^{\#}$时,网络抗毁性随 β递增,β越大,网络抗毁性越好;当 $\alpha>\alpha^{\#}$时,网络抗毁性随 β递减,β越小,网络抗毁性越好;并且对于 β<0,网络抗毁性在流量强度未饱和时存在一个极小值点 (用 $\alpha^{\#}$表示流量强度未饱和点),如 β=-1时,极小值为 $R=0.15$, $\alpha^{\#}=0.8$;β=-3时,极小值为 $R=0.4$, $\alpha^{\#}=0.7$,在流量强度小于 $\alpha^{\#}$以前网络的抗毁性随着流量强度递增而变差,而在流量强度大于 $\alpha^{\#}$时网络的抗毁性随着流量强度的递增而变好。BA网络的随机失效 (图 2(d)),在流量强度较小时 (α<0.6),抗毁性指标 (R)在 80%以上,在 β=0时,抗毁性最好,即使流量强度接近满负荷 (α=0.9),抗毁性指标仍然能达到 70%以上。

复杂保障网络对于故意攻击 (图 2(e))的抗毁性在流量

强度很小时 (α = 0. 1)就出现了级联失效。随着流量强度的增加,网络的抗毁性不断下降。并且,发现网络的抗毁性随着 β的减小而增加,当 β = - 3时,在 α变化的大部分区间内 (α < 0. 85),网络的抗毁性指标均能保持在 50%以上。复杂保障网络 (图 2(f))对于随机失效的抗毁性较好,在 α = 0. 6时,网络的抗毁性指标 (*R*)可以达到 80%以上,网络的抗毁性对于 β的变化不明显,当 β = 0时,网络的抗毁性最好。从图 2(e)与 (f)比较可知,复杂保障网络对于随机失效有较好的抗毁性,而对于故意攻击的抗毁性较差,通过改变网络的流量分布 (β = - 3),可以提高复杂保障网络的抗毁性。

结束语

本文提出了基于级联失效的复杂保障网络抗毁性模型,仿真分析了复杂保障网络在不同流量强度和不同流量分布条件下的网络抗毁性,发现复杂保障网络对于故意攻击在流量强度很小时就出现级联失效。在流量强度较大时,更可能使得网络整体崩溃,而对于随机失效却表现出很好的抗毁性,即使在网络满负荷运行时,网络抗毁性也能达到 50%以上。不同的流量分布也能使得网络的抗毁性发生变化,找到合适的流量分布,可以提高网络的抗毁性。

参考文献:

[1] BROADBENT S R, HAMMERSLEY J M. Percolation processes: I crystals and mazes [J]. Proc Cambridge Philos Soc, 1957, 53: 629-641.

[2] ALBERT R, JEONG H, BARABÁSI A L. Error and attack tolerance of complex networks [J]. Nature, 2000, 406 (6794): 378-382.

[3] MOTTER A E, LAI Y C. Cascade-based attacks on complex networks [J]. Phys Rev E, 2002, 66 (6): 065102.

[4] HOLME P. Edge overload breakdown in evolving networks[J]. Phys Rev E, 2002, 66 (3): 036119.

[5] WATTS D J. A simple model of global cascades on random networks [J]. Proc Natl Acad Sci, 2002, 99 (9): 5766-5771.

[6] MORENO Y, GÓMEZ J B, PACHECO A F. Instability of scale-free networks under node-breaking avalanches[J]. Europhys Lett, 2002, 58 (4): 630-636.

[7] DOBSON I, CARRERAS B A, LYNCH V E, *et al* Estimating failure propagation in models of cascading lackouts[C]//Proc of International Conference on Probabilistic Methods Applied to Power Systems 2004.

[8] DOBSON I, CARRERAS B A, NEWMAN D E. A probabilistic loading-dependent model of cascading failure and possible implications for blackouts[C]//Proc of the 36th Hawaii International Conference on System Sciences. Hawaii: IEEE Computer Society, 2003.

[9] DOBSON I, CARRERAS B A, NEWMAN D E. Probabilistic load-dependent cascading failure with limited component interactions[C]//Proc of International Symposium on Circuits and Systems 2004.

[10] HOLME P, KIM B J. Vertex overload breakdown in evolving networks [J]. Phys Rev E, 2002, 65 (6): 066109.

[11] 李翠玲,谢里阳. 相关失效分析方法评述与探讨 [J]. 机械设计与制造, 2003 (3): 1-3.

[12] MORENO Y, PASTOR-SATORRAS R, VÁZQUEZ A, *et al* Critical load and congestion instabilities in scale-free networks[J]. Europhys Lett, 2003, 62 (2): 292-298.

[13] ZHAO Liang, KWANGHO P, LAI Y C. Attack vulnerability of scale-free networks due to cascading breakdown[J]. Phys Rev E, 2004, 70 (3): 035101.

[14] MOTTER A E. Cascade control and defense in complex networks[J]. Phys Rev Lett, 2004, 93 (9): 098701.

[15] WANG Xiao-fan, XU J. Cascading failures in coupled map lattices [J]. Phys Rev E, 2004, 70 (5): 056113.

[16] WU Jian-jun, GAO Zi-you. Cascade and breakdown in scale-free networks with community structure [J]. Phys Rev E, 2006, 74 (6): 066111.

[17] ZHAO Hui, GAO Zi-you. Cascade defense via navigation in scale free networks [J]. Eur Phys J B, 2007, 57: 95-101.

[18] BARABÁSI A L, ALBERT R, JEONG H. Mean-field theory for scale-free random networks [J]. Physica A, 1999, 272: 173-187.

[19] ERDÖS P, RÉNYI A. On the evolution of random graphs[J]. Publ Math Inst Hung Acad Sci, 1960, 5: 17-60.

(上接第 3450页)

$R^{(1)}$ if T_{ij}^{a} is $\widetilde{Z}$ then T_{ij} is $\widetilde{D}\widetilde{T}$

$R^{(2)}$ if T_{ij}^{a} is $\widetilde{PS}$ then T_{ij} is $\widetilde{D}\widetilde{T}$ or $\widetilde{T}$

$R^{(3)}$ if T_{ij}^{a} is $\widetilde{PM}$ then T_{ij} is $\widetilde{D}\widetilde{T}$ or $\widetilde{T}$

$R^{(4)}$ if T_{ij}^{a} is $\widetilde{PB}$ then T_{ij} is $\widetilde{T}$ or $\widetilde{HT}$

结束语

由于 MANETs自身的特点,其容易受到攻击。本文分析了 MANETs中的节点自私性问题,结合模糊数学的知识,提出了一种 MANETs环境下的模糊信任模型方案。该方案能有效地解决自私性问题,刺激节点参与路由和数据包转发,提高了路由信息的完整性。利用 NS-2作一系列的仿真实验来对该方案进行评估。仿真结果表明,该方案在多数情况下能发现节点自私行为率高达 85. 5%,且并没有引入过多的系统开销。同时提高了包的吞吐量至少 8%,误确认概率低于 3. 6%。但是自私节点篡谋和其他一些恶意节点联合攻击对该模型有一定的影响。节点的假信任推荐在网络中传播问题也是值得进一步研究的。

参考文献:

[1] XU Li, LIN Zhi-wei, YE A-yong. Analysis and countermeasure of selfish node problem in mobile Ad hoc network[C]//Proc of the 10th Computer Supported Cooperative Work in Design, International Conference. 2006: 1-4.

[2] LI Jing-tao, JING Yi-nan, XIAO Xiao-chun, *et al* A trust model based on similarity-weighted recommendation for P2P environments [J]. Journal of Software, 2007, 18 (1): 157-167.

[3] TANG Wen, CHEN Zhong. Research of subjective trust management model based on the fuzzy set theory [J]. Journal of Software, 2003, 14 (8): 1401-1408.

[4] YU Fa-jiang, ZHANG Huan-guo, YAN Fei. A fuzzy relation trust model in P2P system [C]//Proc of Computational Intelligence and Security International Conference. 2006: 1497-1502.

[5] TAL A, DOLEV D, HOD B. Cooperative and reliable packet-forwarding on top of AODV [C]//Proc of the 4th International Symposium on Modeling and Optimization in Mobile, Ad hoc and Wireless Networks. 2006: 1-10.

[6] GRIFFITHS N, CHAO Kuo-ming, YOUNAS M. Fuzzy trust for peer-to-peer systems[C]//Proc of the 26th IEEE International Conference on Distributed Computing Systems Workshops. 2006: 73.