高技术通讯 2010 年 第 20 卷 第 7 期:702 ~ 708

doi:10.3772/j.issn.1002-0470.2010.07.008

基于多路径路由的自组网节点合作方法①

郭建立② 刘宏伟 杨孝宗 吴智博 董 剑

(哈尔滨工业大学计算机科学与技术学院 哈尔滨 150001)

摘 要 为减小移动自组网中自私节点对网络性能的影响,提出了一种基于 TORA 协议的自组网节点合作方法 TORA _ CE。由于每个节点拥有多条通往目的节点的路径,在发现自私节点后,该方法能够快速切换路由,从而减小了数据传输过程中丢包的概率。TORA _ CE 具有更好的分布式特点,将自私节点引发的路由变化限制在自私节点附近较小的范围内,而且引入了共同邻居监听技术,并采用一跳信息计算节点的信誉值,提高了对自私节点的检测速度。使用 NS2 对 TORA _ CE 进行了仿真,实验结果显示,与基于 DSR 协议的节点合作方法相比,TORA _ CE 能够明显提高网络的吞吐率。

关键词 移动自组网(MANET),节点合作,信誉值,自私节点

0 引 言

在移动自组网[1]中,节点的无线通讯范围有限,两个相距较远的节点需要借助网络中其它节点的转发功能来实现数据通信。目前移动自组网中成熟的路由协议如动态源路由(dynamic source routing,DSR)协议[2]、Ad hoc 按需距离矢量(Ad hoc on-demand distance vector,AODV)路由协议[3]和临时按序路由算法(temporally ordered routing algorithm,TORA)协议[4,5],都假设自组网中的节点是合作的,它们乐意为网络中其它节点转发数据。

近年来,随着硬件技术的不断进步,民用自组网开始大规模出现。在这些网络中,各节点分别隶属于不同的个人或组织,缺乏共同的目的,节点间的合作无法得到保证,节点为了节省自己的资源(如能量),可能会丢弃待转发的数据,从而表现出自私行为。文献[6]运用博弈论从理论上证明了,在移动自组网中不存在自发的节点合作,需要使用外部机制来保证节点合作。而在移动自组网中,少数节点的自私行为将会对网络性能造成很大影响。文献[7]指出,如果网络中存在 10% ~ 40% 的自私节点,就会导致整个网络的性能下降 16% ~ 32%。

对于节点合作问题,研究者们提出了许多解决方案[8,9],但几乎都是基于 DSR 协议的,因而存在着以下问题:源节点不容易发现其所使用路由中的自私节点(尤其当自私节点距离源节点较远时);当自私节点附近的节点发现其自私行为后,需要通知每个使用该自私节点的源节点,为此需要建立信任管理机制;当源节点得知其所使用的路由中含有自私节点后,可能需要重新启动路由发现过程,增加了传输延迟。针对上面所存在的问题,本文提出了一种新的基于 TORA 协议的节点合作方法——TORA _ CE (TORA protocol with cooperation enhanced)。运用 TORA _ CE 方法时,当节点发现下一跳转发节点是自私节点后,由于其同时保存着多条到达目的节点的路由,因此会自动选择其它节点作为转发节点,既不需要通知源节点,也不需要重新发现路由,减小了丢包的概率。

1 相关工作

文献[7]第一次提出基于信誉[10]的节点合作方法,使用看门狗检测网络中的自私节点。文献[11]进一步提出采用二手信息(second-hand information)计算节点的信誉值,每个节点把自己的检测结果发送给朋友节点。文献[12]提出采用一跳信息(one-hop information)计算节点的信誉值,降低了系统的复杂度。文献[13]重点讨论了信誉值计算过程中所存在的安全问题,提出了一种安全与面向对象的基于

① 863 计划(2006AA01A103,2008AA01A201)和国家自然科学基金(60503015)资助项目。
② 男,1980 年生,博士;研究方向:移动自组网及感知网;联系人,E-mail: gjl@ftcl.hit.edu.cn
(收稿日期:2009-03-17)

信誉的激励方法(a secure and objective reputation-based incentive scheme, SORI)。文献[14,15]认为基于看门狗的检测技术不够准确,提出了 two-hop ACKs 检测方法,更加精确地检测自私节点,但这种方法引入了大量 ACK 消息,严重占用网络带宽,使网络更容易发生拥塞。文献[10,16]对信誉值计算方法进行了分析和总结。

一些研究者还提出了基于虚拟货币的节点合作方法[17-20],通过为转发节点提供一定数量的虚拟货币作为转发数据的补偿,来激励节点进行合作。但是,在这类方法中,为了计算最优补偿方案,节点间需要交换大量信息,而且一旦网络拓扑结构发生变化,还需要重新计算最优补偿方案,阻碍了其在移动自组网中的应用。

2 基于 TORA 协议的节点合作方法(TORA _ CE)

2.1 TORA 协议简介

TORA[4,5]是一种多路径自组网路由协议,采用链路反转(link reversal)的分布式算法,创建一个从源到目的节点的有向无环路图(directed acyclic graphic,DAG)。每个节点有一个相对于目的节点的路由高度(route length),当相邻两节点能够直接通信时,具有较小高度值的节点被视为下行链路,数据包只能沿着下行链路传递,避免了路由环路的出现,如图 1所示。TORA 运行在互联网封装协议[21](Internet MANET encapsulation protocol,IMEP)之上,IMEP 用于提供控制消息的可靠传送,并向 TORA 协议报告链路的状态。

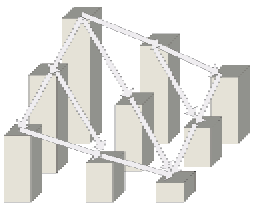


图 1 TORA 路由高度示意图

2.2 TORA _ CE 方法描述

TORA _ CE 方法的核心思想是将启私节点引发的路由变化限制在自私节点附近较小的范围内。每个节点通常保存多条到达目的节点的路径,一旦节点发现下一跳转发节点为自私节点,就立即选用其它可用路由继续发送数据,既不需要通知源节点,也不需要重新发现路由。对于自私节点,只要其邻居能够发现其自私行为,就能够把它从网络中隔离开,减小了自私节点对网络性能的影响。

下面用一个例子说明 TORA _ CE 对自私节点的处理过程。图 2(a)所示为 TORA 协议所创建的路由结构,每个节点都有多条路径到达目的节点,源节点 S 通过路由 S,A,F,C,D 把数据发送到目的节点 D。假定节点 C 是自私节点,总是丢弃数据包,节点 F 由于是其上一跳节点,因此能够快速发现其自私行为,并对其进行隔离,同时通过其它可用路由(如节点 G)继续向目的节点传输数据,整个过程不需要源节点 S 的参与,如图 2(b)所示。当节点 C 的所有邻居都得知其自私行为后,节点 C 就彻底被从网络中隔离开来,如图 2(c)所示。

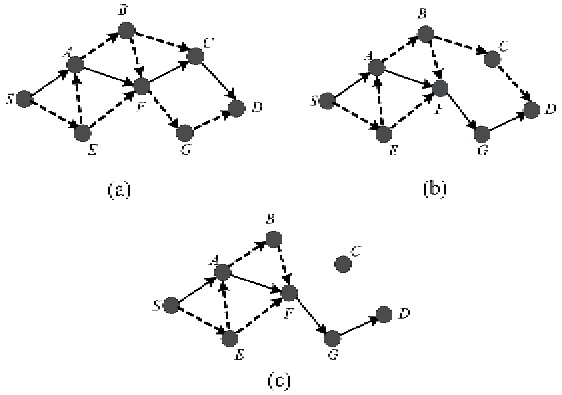


图 2 TORA _ CE 对自私节点的处理过程

TORA _ CE 主要对 IMEP 协议进行修改,位于网络层(TORA)和数据链路层之间,如图 3 所示,包含三个组件:看门狗、二次机会机制和信誉管理器。

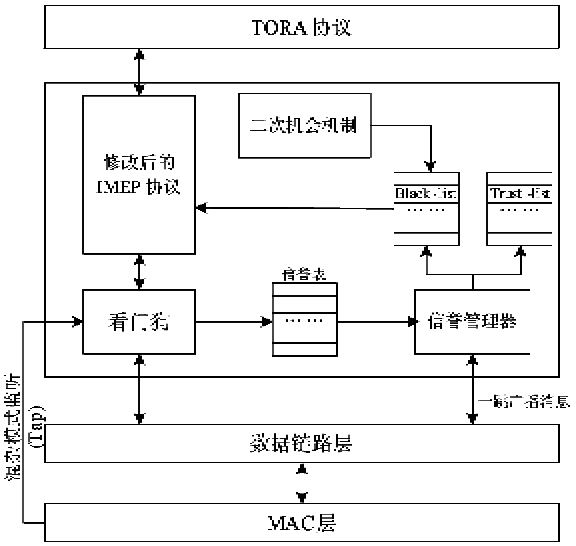


图 3 TORA _ CE 结构图

2.3 看门狗

看门狗主要对邻居节点进行监听，观察它们对数据的转发情况，以及在转发过程中是否修改了数据的内容。看门狗需要维护两个数据结构：信誉表和数据包监听缓存。

在信誉表中，每个邻居对应一个项，存放该节点的ID、信誉值和超时值。信誉值初始为0，取值范围为[-1,1]，定义两个阈值 $Thre_{\text{Trust}}=0.8$ 和 $Thre_{\text{Faulty}}=-0.5$，并规定信誉值大于 $Thre_{\text{Trust}}$ 的节点为可信节点，小于 $Thre_{\text{Faulty}}$ 的为自私节点，介于二者之间的为中立节点。

数据包监听缓存用于存放待监听的数据包，每个数据包对应一个项，在项中存放数据包的内容、下一跳转发节点的ID和超时值。路由层发出的数据，只要其下一跳节点不是目的节点，就被看门狗放入监听缓存中。看门狗在混杂模式下对网络监听，每捕获一个数据包，如果能在监听缓存中找到并且没有被篡改，就根据公式

$$RV_{\text{new}}=\begin{cases}RV_{\text{old}}\times\delta_1+RV_1 & \text{if } RV_{\text{old}}<Thre_{\text{Faulty}}\\ RV_{\text{old}}\times\delta_2+RV_2 & \text{if } RV_{\text{old}}>=Thre_{\text{Faulty}}\end{cases} \tag{1}$$

增加该转发节点的信誉值（其中 δ 为贴现率，RV 为增加或减少的信誉值，实验中取 $\delta_1=0.99$，$RV_1=0.01$，$\delta_2=0.9$，$RV_2=0.1$）。

如果直到监听缓存中的数据包超时，都没能观察到对其转发，或者发现转发节点对其进行篡改，就根据公式

$$RV_{\text{new}}=\begin{cases}RV_{\text{old}}\times\delta_3-RV_3 & \text{if } RV_{\text{old}}>=Thre_{\text{Trust}}\\ RV_{\text{old}}\times\delta_4-RV_4 & \text{if } RV_{\text{old}}<Thre_{\text{Trust}}\end{cases} \tag{2}$$

减小转发节点的信誉值（实验中取 $\delta_3=0.98$，$RV_3=0.02$，$\delta_4=0.9$，$RV_4=0.1$）。

式(1)和(2)使节点的信誉值具有如下性质：1)信誉值反映节点过去的行为；2)节点最近的行为对信誉值影响更大；3)节点的自私行为使其信誉值迅速低于 $Thre_{\text{Faulty}}$，从而被标记为自私节点；4)经过较长时间的合作才能使节点的信誉值大于 $Thre_{\text{Trust}}$，成为可信节点；5)自私节点的信誉值增加缓慢，要经过较长时间的合作才能使其成为中立节点，6)可信节点的信誉值减小缓慢，偶然连续丢失2~3个数据包并不会使其信誉值降到 $Thre_{\text{Trust}}$ 以下。

为使看门狗建立的信誉值更准确，引入了共同邻居监听技术：对于看门狗在混杂模式下捕获的数据包，只要其当前转发节点和下一跳转发节点都是自己的邻居，就被放入数据包监听缓存中，进行监听。如图4所示，节点 S 通过 A、B、C 向节点 D 发送数据，节点 M 和 N 位于 B 和 C 的传输范围内。当 B 向 C 转发数据时，M 和 N 能够捕获该数据包，并发现其当前转发节点（B）和下一跳转发节点（C）都是自己的邻居，M 和 N 就把该数据包放入自己的数据包监听缓存中，监听节点 C 对其转发情况，并根据监听结果更新节点 C 的信誉值。

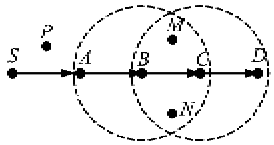


图4 共同邻居监听

2.4 信誉值管理器

信誉管理器周期地检查信誉表，把可信节点和自私节点放入一跳广播消息中，向邻居广播。信誉管理器还接收来自邻居的广播消息，把它们放入缓存中，周期地对其进行处理。信誉管理器把广播消息分为4类：自己发送的广播消息、来自可信节点的广播消息、来自中立节点的广播消息和来自自私节点的广播消息。

信誉管理器对广播消息的处理过程如下：

首先，认为来自自私节点的广播消息不可信，丢掉它们；其次，认为自己的检测结果最可信，所有与其相矛盾① 的广播消息都被认为是不可信的，丢掉它们；接着，认为来自可信节点的广播消息较可信，丢掉所有与其相矛盾的广播消息；最后，两个来自同级别的广播消息，如果内容相矛盾，则丢掉它们。剩下的广播消息被认为是有用的，把可信节点合并起来，更新Trust-list，把自私节点合并起来，更新Black-list。

2.5 二次机会机制

文献[7,17]指出多种原因会影响看门狗的检测结果，如信号冲突、网络拥塞和临时链路故障等，这些都会导致看门狗把合作节点错误地标记为自私节点（实验中发现，当网络负载较重、网络发生拥塞时，合作节点就可能被误判为自私节点）。另外，那些被系统检测出的自私节点，也可能在后期乐意表现出合作行为。为了让那些被标记为不合作的节点重新

① 自己认定某邻居节点是可信节点，而广播消息中却认为该节点是自私节点，或者相反。

返回到网络中,TORA_CE引入了二次机会机制:所有被放入Black-list中的节点,经过一段固定时间后,将被从Black-list中删除,但它们的信誉值不会被复位到0,而是保持当前值不变,目的是一旦这些节点继续表现自私行为,能够快速地被发现。

2.6 对IMEP的修改

TORA协议需要根据各邻居节点的链路状态(如LINK_BI,LINK_DOWN)实时更新路由,但是TORA协议自身是无法获得各邻居节点链路状态的,需要由IMEP协议协助完成。

TORA_CE对IMEP协议进行了修改,使得返回给TORA协议的自私节点所对应的链路状态为LINK_DOWN。于是,自私节点对TORA协议来说是透明的,尽管在物理位置上两节点可能是邻居,但经过IMEP处理后,TORA会认为自私节点不是自己的邻居,因此就不会选用自私节点作为下一跳转发节点。最后,作为对自私节点的惩罚,IMEP协议还需要过滤掉所有来自自私节点的数据(包括数据包和控制消息)。

3 协议正确性分析

在TORA协议中,自私节点可能会修改自己的路由高度,使自己成为局部最高,逃避替其他节点转发数据。下面通过一个定理指出,在TORA_CE中,节点不能随意更改自己的路由高度。

定理1 在TORA_CE中,自私节点不能随意修改自己的路由高度。

证明:TORA_CE并没有对TORA协议进行改动,而在TORA协议中,只有2个地方可以修改路由高度,下面将分别指出,如果自私节点不按照协议规定,随意地修改自己的路由高度,则其能够被邻居节点发现。

例1:在路由创建过程中,当节点的高度为NULL,并且有下行链路时,根据TORA协议,节点只能把自己的高度设置为比具有最小高度值的邻居的高度多1,如果节点设置一个较高的高度,将会被具有最小高度的邻居发现。

例2:在路由维护过程中,只有当节点失去最后一个下行链路后,才能修改路由高度,否则将被下行链路所连接的节点发现。

在其他情况下,如果节点修改了路由高度,就会被下行链路连接的节点发现。

4 仿真及结果分析

本节中,将采用NS2[22]对TORA_CE进行验证,并观察其对网络性能的影响。仿真中采用Random Waypoint运动模型,卡内基梅隆大学(Carnegie Mellon University,CMU)的数据流产生工具并不能满足要求,需要对cbrgen.tcl进行修改,使得产生的恒定比特率(constant bit rate,CBR)数据流满足:每个连接的源节点和目的节点在网络中随机分布,连接的开始时间在[0s,1000s]中均匀分布,连接的持续时间在[200s,600s]中均匀分布。仿真基本参数设置如表1所示。

表1 仿真基本参数

仿真持续时间	1000s
节点传输范围	250m
节点接收范围	250m
载波监听范围	550m
传输速率	2Mbits/s
节点最大运动速度	10m/s
节点最大停留时间	100s
数据流类型	CBR
数据包大小	512byte
发送速率	2pkt/s

主要采用以下两个参数对协议性能进行评价:

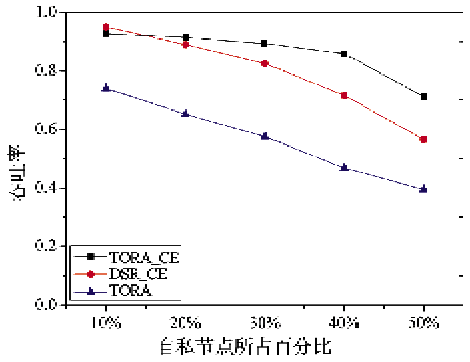
(1)吞吐率(throughput):节点发出的能够顺利到达目的节点的数据包的个数与节点发出的总的数据包个数的比值。

(2)平均路由长度(average routing length):数据包从源节点到目的节点所经过的路由的平均长度(仅统计那些能够顺利到达目的节点的数据包,中途被丢弃的数据包不参与统计)。

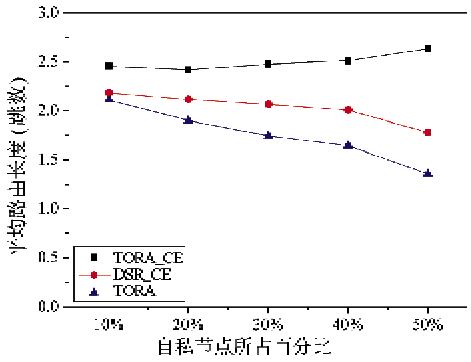
首先观察自私节点对网络性能的影响。仿真区域为670m×670m,30个节点在仿真区域中随机分布,CBR连接数为30,自私节点在网络中随机选取。每组参数运行10次仿真过程,结果取平均值。仿真结果如图5所示,其中DSR_CE表示基于DSR协议的节点合作方法(对自私节点的检测方法与TORA_CE完全相同)。

图5(a)所示为协议的吞吐率,从中可以看出,TORA协议的吞吐率最低,要明显低于TORA_CE和DSR_CE。当自私节点所占比例为10%时,TORA_CE的吞吐率略低于DSR_CE,主要是因为DSR协议的性能要略好于TORA协议,而当自私节点所占

比例较小时，自私节点对网络性能的影响较小，TORA _ CE 未能充分发挥作用。随着网络中自私节点所占比例的提高，TORA _ CE 的优势变得越来越明显。主要有三个原因使得 TORA _ CE 的吞吐率高于 DSR _ CE：1）当发现自私节点后，TORA _ CE 一般不需要重新发现路由；2）在 TORA _ CE 中，自私节点被发现后，所有经过自私节点的连接都会自动绕开它，而在 DSR _ CE 中，需要发送 route error 消息分别通知每个源节点；3）在 IMEP 协议的帮助下，TORA _ CE 能够更快发现链路故障，更早采用新路由。



（a）吞吐率



（b）平均路由长度

图 5　自私节点对网络性能的影响（30 节点）

图 5（b）所示为协议的平均路由长度，可以看出，TORA _ CE 对应的平均路由长度要明显高于 DSR _ CE，原因在于 DSR _ CE 总是选用最短路由发送数据，而 TORA _ CE 并没有选用最短路由，尤其当网络拓扑发生频繁变化时（由节点的移动或者自私节点引起），TORA _ CE 所采用的路由会更加偏离最短路由，因此随着自私节点所占比例增大，TORA _ CE 的平均路由长度也在变大。另外，DSR _ CE 和 TORA 的平均路由长度会随着自私节点所占比例增大而减小，这主要因为：在 DSR _ CE 和 TORA 中，到达目的节点的数据包中路由长度为 1 的数据包所占比例较高，减小了 DSR _ CE 和 TORA 的平均路由长度，如表 2 所示。

表 2　路由长度为 1 的数据包所占比例（30 节点）

	10%	20%	30%	40%	50%
TORA _ CE	0.335883	0.334651	0.331548	0.322615	0.380793
DSR _ CE	0.331119	0.363863	0.382106	0.404539	0.542556
TORA	0.425369	0.500806	0.546352	0.600782	0.736382

接下来观察网络负载对吞吐率的影响。选用的仿真区域为 670m × 670m，节点数量为 30，自私节点所占比例为 30%，CBR 连接数在 10 ~ 50 之间变化。仿真结果如图 6 所示。可以看出，当网络负载较小时，TORA _ CE 的吞吐率要明显高于 DSR _ CE，而当连接数大于 40 后，TORA _ CE 的吞吐率急剧下降，甚至低于 DSR _ CE。主要原因是，TORA _ CE 的平均路由长度较大，更容易发生网络拥塞。另外，在发生网络拥塞时，合作节点更容易被误判为自私节点，从而进一步降低了网络的吞吐率。

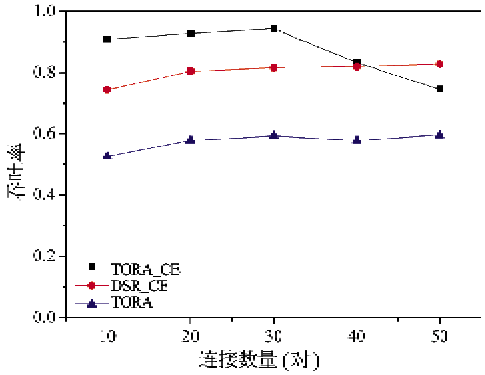


图 6　负载对吞吐率的影响

观察节点运动速度对吞吐率的影响。仿真区域为 670m × 670m，节点数为 30，自私节点所占比例为 30%，CBR 连接数为 30，节点运动速度在 5 ~ 20m/s 之间变化，节点停留时间为 0s。仿真结果如图 7 所示。可以看出，TORA _ CE 的吞吐率最高，但随着节点运动速度增加，TORA _ CE 的吞吐率明显降低。主要原因是，当节点运动速度增大后，网络拓扑更容易发生变化，而在 TORA _ CE 中，只要节点有指向目的节点的路由，就不会重新运行路由发现过程，使得所采用的路由越来越偏离最优路由，因此就更容易发生数据包丢失情况，降低吞吐率。

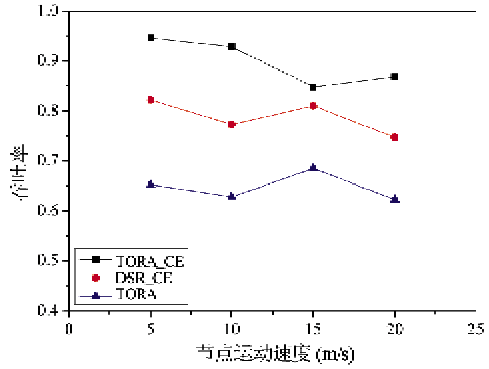


图 7　节点运动速度对吞吐率的影响

最后,观察自私节点对中等规模网络性能的影响。仿真区域为 1000m × 1000m,节点数为 60,CBR 连接数为 30,自私节点所占比例在 10% ~ 50% 之间变化,仿真结果如图 8 所示。从图 8(a)中可以看出 TORA _ CE 的吞吐率要高于 DSR _ CE,而 TORA 的吞吐率最低。当自私节点所占比例为 50%时,由于发生网络拥塞,使得 TORA _ CE 的吞吐率大幅度下降。在图 8(b)中,TORA _ CE 的平均路由长度最大,并且随着自私节点的增多而减小。主要原因是:在 TORA _ CE 中,随着自私节点比例增大,到达目的节点的数据包中路由长度为 1 的数据包所占比例迅速增大了。

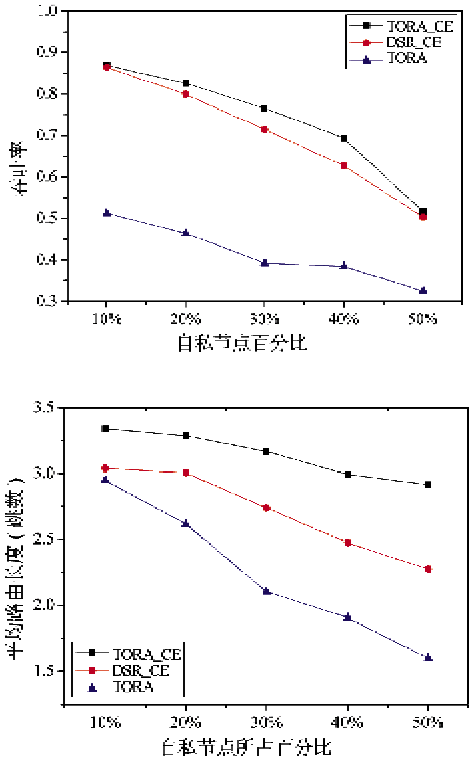


图 8　自私节点对网络性能的影响(60 节点)

5　结　论

本文提出了 TORA _ CE 方法,这是一种基于 TORA 协议的多路径自组网节点合作方法,能够快速检测出网络中的自私节点,并快速切换路由,减小了自私节点对网络性能的影响。与基于 DSR 协议的方法相比,TORA _ CE 具有更好的分布式特点,把对自私节点的检测工作限制在自私节点的附近区域。TORA _ CE 还引入了共同邻居检测技术,并采用一跳信息计算节点的信誉值,使得自私节点附近的节点能够快速发现它,并对其进行隔离。NS2 仿真结果显示,当网络中存在自私节点时,TORA _ CE 能够明显提高网络的吞吐率。

在仿真过程中,发现 TORA _ CE 对网络负载非常敏感,较易发生网络拥塞,使网络性能大幅下降。主要原因有两个:TORA _ CE 不能发现最短路由,增加了数据包的平均路由长度;TORA _ CE 总是选择具有最小高度的邻居节点作为下一跳转发节点,使得网络负载都流向个别的节点,从而引起网络拥塞。我们正在尝试选用其它路由策略(如负载均衡策略、随机选择策略等),以使网络负载均衡,减小网络出现拥塞的可能。

参考文献

[1] Basagni S, Conti M, Giordano S, et al. Mobile Ad Hoc Networking. New Jersey: Wiley-IEEE press, 2004

[2] Johnson D B, Maltz D A, Hu Y C. The dynamic source routing protocol for mobile ad hoc networks (DSR). http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt, Internet Draft, IETF MANET Working Group, 2004

[3] Perkins C E, Royer E M. Ad-hoc on-demand distance vector routing. In: Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications. New Orleans: IEEE press, 1999. 90-100

[4] Park A D, Corson M S. A highly acaptive distributed routing algorithm for mobile wireless networks. In: Proceedings of the IEEE International Conference on Computer Communications. Kobe, Japan: IEEE Computer Society Press, 1997.3. 1405-1413

[5] 刘强,匡镜明,王华. TORA 路由协议详解及性能分析. 见:2005 年海峡两岸三地无线科技学术会论文集, 2005, 北京.499-503

[6] Feleqyhazi M, Hubaux J P, Buttyan L. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 2006, 5(5): 463-

476

[7] Marti S, Giuli T, Lai K, et al. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston: ACM press, 2000. 255-265

[8] Marias G F, Georgiadis P, Flitzanis D, et al. Cooperation enforcement schemes for MANETs: a survey. *Wireless Communications and Mobile Computing*, 2006, 6(3): 319-332

[9] Yoo Y, Agrawal D P. Why does it pay to be selfish in a MANET?. *IEEE Wireless Communications*, 2006, 13(6): 87-97

[10] Buchegger S, Mundinger J, Boudec J Y L. Reputation systems for self-organized networks. *IEEE Technology and Society Magazine*, 2008, 27(1): 41-47

[11] Buchegger S, Boudec J Y L. Self-policing mobile ad hoc networks by reputation systems. *IEEE communications magazine*, 2005, 43(7): 101-107

[12] 郭建立,吴智博,刘宏伟等. OIECE:基于一跳信息转发的自组网节点合作协议.高技术通讯. 2009,19(5):901-906

[13] He Q, Wu D P, Khosla P. A secure incentive architecture for ad hoc networks. *Wireless Communications & Mobile Computing*, 2006, 6(3): 333-346

[14] Liu K J, Deng J, Varshney P K, et al. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE transactions on mobile computing*, 2007, 6(5): 536-550

[15] Djenouri D, Badache N. Struggling against selfishness and black hole attacks in MANETs. *Wireless communications and mobile computing*, 2008, 8(6): 689-704

[16] Hu J Y. Cooperation in Mobile Ad Hoc Networks. http://www.cs.fsu.edu/research/reports/TR-050111.pdf, Computer Science Department, Florida State University, January 2005

[17] Anderegg L, Eidenbenz S. Ad-hoc-VCG: a truthful and cost efficient routing protocol for mobile ad-hoc networks with selfish agents. In: Proceedings of the 9th Annual International Conference on Mobile Computing and Networking, San Diego, CA, USA: ACM press, 2003: 245-259

[18] Wang Y W, Singhal M. On improving the efficiency of truthful routing in MANETs with selfish nodes. *Pervasive and Mobile Computing*, 2007, 3(5): 537-559

[19] Eidenbenz S, Resta G, Santi P. The COMMIT protocol for truthful and cost-efficient routing in Ad hoc networks with selfish nodes. *IEEE Transactions on Mobile Computing*, 2008, 7(1): 19-33

[20] 郭建立,吴智博,刘宏伟等. 基于机制设计理论的自组网节点合作协议. 计算机学报. 2009, 32(3):483-492

[21] Corson M S, Park V. An Internet MANET Encapsulation Protocol (IMEP) Specification. Internet-Draft, draftietf-manet-imep-spec-00.txt, technical report, 1998

[22] Fall K, Varadhan K. The ns Manual(formerly ns Notes and Documentation). The VINT Project, 2008, http://www.isi.edu/nsnam/ns/doc/index.html

A hode cooperation scheme for mobile Ad hoc networks based on multipath routing

Guo Jianli, Liu Hongwei, Yang Xiaozong, Wu Zhibo, Dong Jian

(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001)

Abstract

To stimulate selfish nodes in mobile Ad hoc networks to participate in the network cooperation, this paper proposes the TORA _ CE scheme, a new node cooperation scheme for mobile ad hoc networks based on the temporally ordered routing algorithm (TORA) protocol. Because each node has a number of paths leading to the destination, after the discovery of selfish nodes, the scheme can quickly switch routes, reducing the probability of packet loss in the data transmission phase. With its distributed features, TORA _ CE can restrict the route changes caused by selfish nodes in a smaller range. The TORA _ CE can increase the selfish node detection rate because of its introduction of a common neighbor monitoring technology and the use of one-hop information for computing the node reputation. The NS2 was used to simulate TORA _ CE, and the experimental results show that the TORA _ CE can significantly improve the network throughput, compared with the cooperation scheme based on the dynamic source routing (DSR) protocol.

Key words: mobile Ad hoc networks (MANET), node cooperation, reputation, selfish node