doi:10.3969/j.issn.1000-436x.2013.09.012

ad hoc 网络中一种基于信任模型的机会路由算法

王博，陈训逊
（国家计算机网络应急技术处理协调中心，北京 100029）

摘 要：由于 ad hoc 网络具有缺乏足够的物理保护、拓扑结构动态变化、采用分布式协作、节点的带宽和计算能力有限等特点，导致传统的路由安全机制不再适合 ad hoc 网络路由协议的设计。最近当前研究热点之一的机会路由能够在链路不可靠的情况下充分利用无线广播和空间多样性的特性提高网络的吞吐量。因此，考虑在机会路由中引入信任相似性概念设计信任机会路由，建立了基于节点信任度和最小成本的信任机会转发模型，提出了最小成本的机会路由算法 MCOR，并对算法进行了理论上的分析和证明。最后采用仿真实验对该算法进行验证，又与经典机会路由协议 ExOR 以及其他经典的信任路由协议 TAODV 和 Watchdog-DSR 进行性能对比。仿真结果表明，MCOR 算法能够防范恶意节点的攻击，在吞吐量、端到端时延、期望转发次数(ETX)和成本开销等方面都比其他 3 种协议表现出性能上的优势。

关键词：信任相似性；信任模型；信任度；机会路由；机会路由成本
中图分类号：TP393 **文献标识码：**A **文章编号：**1000-436X(2013)09-0092-13

Opportunistic routing algorithm based on trust model for ad hoc network

WANG Bo, CHEN Xun-xun
(CNCERT/CC, Beijing 100029, China)

Abstract: Due to the absence of enough physical protection, dynamic topology, distributed collaboration, the limited bandwidth and computing ability in ad hoc network, traditional routing security mechanism cannot adapt to the design of routing protocols. Recently, opportunistic routing is of the research hotspots, which can cope with the unreliable transmissions to improve throughput of the whole network by exploiting the broadcast nature of the wireless medium and spatial diversity of multi-hop wireless network. The concept of trust-based similarity in opportunistic routing for ad hoc network was incorporated, and a novel trusted opportunistic forwarding model based on trust degree of node and least cost of opportunistic routing were also built. Then a trusted minimum cost routing algorithm (MCOR) was proposed and the correctness and effectiveness of this algorithm from theoretical ana ysis were proved. Finally, MCOR algorithm was verified by simulation and was compared with the classic protocols: ExOR, TAODV and Watchdog-DSR. The simulation results show that MCOR scheme can detect and mitigate node misbehaviors. Furthermore, MCOR scheme outperforms the other protocols in terms of throughput, delay, expected ETX and cost of routing.

Key words: trust-based similarity; trust model; degree of trust; opportunistic routing; cost of opportunistic routing

1 引言

无线链路的动态、时变和丢失特性导致无线链路的质量较差且稳定性较低，这对提高 ad hoc 网络的吞吐量和传输的可靠性提出了挑战。另外，节点移动性带来的链路不稳定、节点能量的有限也给路由协议的设计及优化带来困难。然而，无线信道的广播特性具有其先天的优势，机会路由(opportunistic routing)[1~13]

收稿日期：2013-05-03；修回日期：2013-07-24
基金项目：国家自然科学基金资助项目(60633020,60970117)；国家高技术研究发展计划(“863”计划)基金资助项目(2011AA010707)
Foundation Items: The National Natural Science Foundation of China (6063 20, 60970117); The National High Technology Research and Development of China (863 Program) (2011AA010707)

正是利用了无线信道的这一特性提高无线网络的传输可靠性和端到端的吞吐量。但是，目前对机会路由的研究忽视了恶意节点对正常路由安全通信的攻击[16]，特别是当恶意节点对下一跳转发列表的确定、备选转发节点的选择及相应的优先级分配，以及后续机会路由成本的量化等方面都产生较大的影响。因此本文在对机会路由深入研究的基础上首次结合软安全中的信任思想增强网络的安全性能。

本文在对 ad hoc 网络中当前信任模型的研究基础上，创新性地将信任模型和机会路由进行综合分析，提出了一种基于信任度和最小成本机会路由的转发模型，给出了对应的最小成本信任机会路由算法 MCOR，并对该算法的有效性进行理论证明，最后通过仿真实验将该算法与经典的协议（ExOR[2]、TAODV[15]和 Watchdog-DSR[16]）进行性能对比，以此验证该算法的性能。仿真结果表明该算法能够抵制恶意节点加入到信任邻居转发列表，以及剔除恶意链路参与到信任机会路由的建立过程，并且在吞吐量、端到端时延、期望转发次数和成本开销等方面都有很大的性能提高。

2　相关工作

2.1　机会路由

当前对机会路由的研究主要集中在：下一跳备选节点集合(转发列表)的选取、列表中各个节点的优先级规定以及不同节点之间的高效协调机制避免重复发送数据分组 3 个方面。文献[3]对机会路由进行了数学理论的定义建模和分析，并把对应的一整套理论体系运用到当前其他机会路由的研究之中，具有很好的理论推广意义。文献[4]提出了基于一种新路由判剧 EAX (expected anycast transmissions) 的机会路由协议，并采用启发式算法计算转发备选节点集合，以及结合 EAX 的值确定节点的转发优先级。文献[5]考虑到把机会路由中各个节点转发数据分组时采用的单一确定速率延伸到多速率，进一步提高网络的吞吐量。文献[7]结合博弈论中效用函数的计算方法，取代 ExOR 协议利用 ETX[17]作为选择转发备选节点，以及优先级确定的度量参数，从而实现距离目的节点效用值较大的节点优先作为转发备选节点，最后保证采用该转发备选节点后，源节点获得的效用最大。文献[8]为每个节点配备一台 GPS 估算该节点距离目的节点的实际物理距离，进而选择转发列表和确定节点的优先级，同时也把该思想延伸到多速率的情况下进行设计。也有一些文献[10,11]把网络编码思想融入到机会路由中，从而减少由于转发列表中协调转发产生的时延开销以及节点之间重复转发数据分组的可能性。还有其他一些文献[6,9,12,13]对机会路由在其他方面(MAC 层信道分配减少最小重传次数等)进行改进。文献[37]首次针对节点之间的直接信任关系提出了一种避免恶意攻击的安全机会路由算法，从而提高了机会路由的安全性能。文献[38]在文献[37]的基础上提出了一种综合信任度的计算模型，以及设计了一种避免转发列表中存在恶意节点攻击的机会路由算法。

2.2　信任模型

当前基于信任模型的路由研究情况包括：LUO 等人在文献[18,19]中结合模糊数学来描述和定义信任值的度量，并对此建立信任模型。文献[20]也是基于贝叶斯理论对节点的信任关系进行建模，该模型可操作性较强，但对邻居节点的错误推荐缺少辨别能力。文献[21]提出了一种模糊信任推荐框架，该推荐算法是基于协同过滤思想来设计。文中信任模型的建立缺少对信任时效性和不确定性的考虑。文献[22]从当前信任模型的框架着手分析可能存在的攻击类型和脆弱性，进而提出了一种新的目标信任管理框架解决当前信任模型存在的不足。文献[23]基于信任图和门限密码学的思想设计了一种分布式公钥证书管理系统，该系统摒弃了传统采用集中式的管理和可信第三方，允许网络中的用户发布公钥证书，进而通过利用证书链实现节点的认证和鉴别功能。文献[24]采用当前广泛应用的交叉证明(cross-certification)思想设计基于 PKI 的信任模型，该文献中对该模型的具体实现和性能估计给出了详细的说明，以此验证该模型的有效性。文献[25]提出了一种减少信任不确定性的模型，该模型首先通过利用过去自身交互的有效信息增加节点评估信任关系的信心度，以及收集的信任信息减少节点自身主观评价的不确定性。此外，该文献也充分利用节点的移动性进一步减少评估过程中的不确定性和收敛性，从而确保该模型在时延、成本和不确定 3 个方面进行性能的折中分析。文献[26]针对当前 ad hoc 网络中出现的典型攻击行为提出了一种提高网络生存性的多维信任模型 RMTM。该模型主要基于 D-S 证据理论，根据节点的攻击情况将节点的攻击证据划分为多个维度，从而实现多维攻击证据和信任的复合增加信任模型评估的准确性和顽健性。但是该模型较复

杂，可操作性不强。此外，需要集中式的可信第三方进行多维证据的收集，因此，该模型的扩展性也不强。

2.3 信任路由

而当前对信任路由的研究情况如下：文献[15]利用基于观点表示主观信任的信任模型延伸至 AODV 协议中，提出了基于信任管理机制的 TAODV 协议。文献[18]基于模糊理论，重点围绕模糊推理规则对信任评估和路由选择过程进行建模。最后将该模型在 DSR 协议中进行了实现和仿真对比。文献[27]充分考虑了信任的特性(时效性、不确定性和主观性等)，提出了一种动态信任机制高效地评估节点间的信任关系，最后将该机制在 AODV 和 DSR 协议中进行了实现和性能验证。文献[28]对当前无线网络中的信任和信誉管理机制进行了详细的介绍和分类。文献[29]在基于 AODV 协议上通过监视守卫(guard)节点辨别网络中的恶意节点。主要通过对邻居节点的信任水平进行评估，并与网络中的阈值进行比较，初步估计节点的恶意性。从而保证路由选择的有效性和安全性。文献[30]提出了一种多路径下的 ad hoc 网络信任路由协议 AOTDV。该协议基于一种简单的信任模型对邻居节点转发数据分组的能力进行评估，设计了多路径下的信任路径判据，从而摒弃了以往综合考虑跳数和信任值度量选择最优路由而产生关键节点负载过高的问题，提高了整个网络中恶意节点对路由选择产生的攻击影响。文献[31]提出了一种防范自私和恶意攻击的合作按需安全路由协议 COSR。该协议对节点的信誉度和路径信誉度给出了具体的定义，也对节点的转发能力给出了量化，解决了 DSR 协议中因过多选择信誉度高的节点而产生负载不均衡和安全等问题。

3 问题描述

本文通过对机会路由的原理思想进行分析发现：恶意节点可以通过伪装、监听和欺骗等攻击方式[16]加入到转发列表中，以此成为最优的转发节点。在此，网络中的恶意节点可能表现出 2 种典型的攻击行为。

情况 1：假设恶意节点在列表中的优先级较高，通过列表中的协调机制确定该节点为最优的转发节点，原则上该节点应该代替列表中的其他节点向下一跳转发数据分组。但是，该节点很可能表现出自私性，不转发数据分组，从而影响后续节点的正常通信。具体示例如图 1(a)所示。

情况 2：假设恶意节点本应该向下一跳节点转发数据分组，但是其虚报自身优先级的判据标准(例如 ETX)，导致列表中的其他备选节点成功转发此数据分组。具体示例如图 1(b)所示。

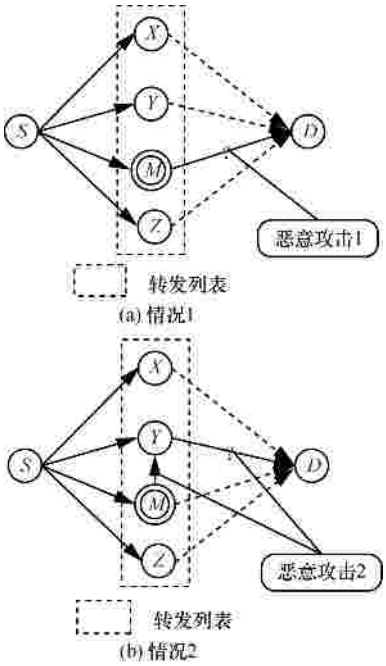

图 1 机会路由中出现的恶意攻击情况

本文基于以上 2 种情况的考虑，重点对机会路由中转发列表的安全性进行研究，在确保满足以下 2 个条件成立的前提下才对机会路由进行建模：1）只有可信的节点才能加入到转发列表中，即正常节点才有机会参与到为下一跳数据分组转发的过程中；2）综合度量列表中节点的转发优先级，即通过增加优先级的安全考虑，确保列表中优先级最高的节点优先转发数据分组，减少数据分组传输的重传次数以及增加数据分组在传输过程中的可靠性。

4 信任机会转发模型

当前对机会路由成本进行量化计算的相关研究很少，在机会路由中考虑安全因素的相关研究亦很少。因此，本文通过把两者有机结合起来进行研究，一方面结合机会路由自身的特性，另一方面利用信任机制弥补机会路由在安全方面存在的攻击隐患，以便为以后的研究工作提供相关的理论指导和分析。

结合 ad hoc 网络自身的特点，为了便于形式化地建模和分析，现对网络进行如下定义。

定义 1 （加权图表示）用加权有向图 $G=(V,E)$

表示 ad hoc 网络，其中，V 为网络的非空节点集合，E 为连接节点对的通信链路集合(相邻节点都在彼此的通信范围之内)，$|V|$和$|E|$分别表示该网络中节点和链路的数目。

4.1　基于信任相似性的信任模型

本文结合当前信任模型的研究基础[18~27]，需要保证信任定义的准确性、量化计算的简单性和模型设计的通用性。但是在 ad hoc 网路中，由于节点之间的信任关系具有不确定性，只有通过在周期性的时间内相互彼此观察各自的交互转发行为，才能对节点间的信任关系进行估计和判断，同时信任又具有主观性、非对称性和时效性等特点，因此本文考虑采用看门狗(watchdog)机制[18]监测节点的转发行为，根据实际的转发情况来定义节点的信任度，以此反映该节点当前转发行为的真实性和准确性。

定义 2　(直接信任度)：直接信任度是指节点 i 与邻居节点 j 在一段周期时间内根据直接交互行为历史（发送和接收数据分组的情况）信息所估计的直接信任水平。

用 $T^{\mathrm{d}}_{\mathrm{new}}(i,j)$ 表示节点 i 与节点 j 的直接信任水平。结合节点 i 的直接信任水平具有时效性，以及由于自身的转发行为而提供给该节点相应的奖励和惩罚等情况，给出如下计算公式

$$T^{\mathrm{d}}_{\mathrm{new}}(i,j)=\begin{cases}1-TF\cdot T^{\mathrm{d}}_{\mathrm{old}}(i,j) & ,s=0,f=0,T^{\mathrm{d}}_{\mathrm{old}}(i,j)>0\\ 1-TF\cdot(RF\cdot S-PF\cdot F)\cdot T^{\mathrm{d}}_{\mathrm{old}}(i,j)+TF\cdot(RF\cdot S-PF\cdot F) & ,s=0\text{或 }f=0,T^{\mathrm{d}}_{\mathrm{old}}(i,j)>0\\ 0 & ,\quad \text{其他}\end{cases}\tag{1}$$

其中，Δt 为当前时间与上次最后交互的时间间隔，TF 表示 Δt 时间内对直接信任度的时间影响因子，即 $TF=\Delta t/(\Delta t+1)$。$T^{\mathrm{d}}_{\mathrm{old}}(i,j)$ 为上次最后交互时两节点的直接信任度，$T^{\mathrm{d}}_{\mathrm{new}}(i,j)$ 为当前时间的直接信任度。RF 和 PF 分别为奖励和惩罚因子 $(1\geq RF>PF\geq 0, RF+PF=1)$，根据经验为对应的参数取值。$S$ 和 F 分别表示在 Δt 时间内，节点 i 成功转发和失败转发数据分组的概率，即 $S=s/(s+1)$，$F=f/(f+1)$，s 和 f 则为节点 i 向节点 j 实际转发数据分组成功的次数及失败的次数。很显然，$0<T^{\mathrm{d}}_{\mathrm{new}}(i,j)\leq 1$。

为了避免恶意节点不真实地虚报和私自掩饰自身的恶意转发行为，恶意节点之间通过共谋攻击故意欺骗善意节点来增加自身的信任度，以及诬陷善意节点具有恶意攻击的行为等攻击情况的发生，因此本文考虑采用第三方邻居节点的推荐机制来间接计算信任度，给出如下一系列定义。

定义 3　(信任相似性)：信任相似性是指节点 i 和节点 k 对其他节点如 u 信任度的相似程度。

当节点 i 和节点 k 信任相似程度越高，说明节点 i 和节点 k 对其他节点 u 的看法一致，即这 2 个节点具有相同的推荐水平 $s(i,k)$。具体的计算公式为

$$s(i,k)=\frac{\sum_{u\in CN(i,k)}(T^{\mathrm{d}}(i,u)-\overline{T_i})\cdot(T^{\mathrm{d}}(k,u)-\overline{T_k})}{\sqrt{\sum_{u\in CN(i,k)}(T^{\mathrm{d}}(i,u)-\overline{T_i})^2}\sqrt{\sum_{u\in CN(i,k)}(T^{\mathrm{d}}(k,u)-\overline{T_k})^2}}\tag{2}$$

很显然，$0<s(i,k)\leq 1$。其中，$CN(i,k)$ 为节点 i 和节点 k 之间所公有的邻居节点，$T^{\mathrm{d}}(k,u)$ 和 $T^{\mathrm{d}}(i,u)$ 分别为节点 k、节点 i 和节点 u 之间的直接信任度。通过观察节点 k、节点 i 与 $CN(i,k)$ 的交互情况，可以计算出节点 k 和节点 i 的平均直接信任度 $\overline{T_k}$ 和 $\overline{T_i}$。

通过利用定义 3 的计算公式可以计算出节点 i 和其每一个邻居节点的相似性，通过对这些信任相似性进行排序，节点 i 就可以获知与其相似性至少达到一定阈值为 t　$(t\geq 0.6)$ 的邻居节点集合(m 个节点)，因此，计算节点 i 与节点 j 信任水平可以根据节点 i 与这 m 个最相似的节点推荐信任水平间接计算，进而得出定义 4。

定义 4　(间接信任度)：间接信任度是指与节点 i 具有较高信任相似性的邻居节点所推荐的直接信任度。通过综合权衡具有较高信任相似性的各个邻居节点的直接信任度，能够更可靠、真实和准确地反映出推荐的信任水平。

即间接信任度 $T^{\mathrm{r}}(i,j)$ 的计算公式为

$$T^{\mathrm{r}}(i,j)=\frac{\sum_{k\in m}T^{\mathrm{d}}(k,j)s(i,k)}{\sum_{k\in m}s(i,k)}\tag{3}$$

其中，$0<T^{\mathrm{r}}(i,j)\leq 1$。

如果节点由于资源受限或链路的不稳定性导致不能直接观察邻居节点的转发行为，那么推荐信任度的引入可以加快整个信任模型的评估过程。此外，引入推荐信任度的计算具有如下优势：一方面，

节点可以监测出周围邻居节点是否存在恶意行为，避免将需要转发的数据分组转发给该恶意节点；另一方面，通过选择信任度较高的节点转发数据分组能够提高网络中节点的合作性。

定义 5 （信任度）：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。

根据定义 2 和定义 4 的计算公式可以得出节点 i 和节点 j 之间的总信任度为

$$T(i,j)=a\cdot T^{\mathrm{d}}(i,j)+b\cdot T^{\mathrm{r}}(i,j) \tag{4}$$

其中，$0\le T(i,j)\le 1$，$a+b=1$。根据实际的网络情况对 a 和 b 进行折中取值。如果当前的网络状况更倾向于直接信任度的估计，则设置 $1>a>b>0$。在网络的初始状态下，各个节点之间由于缺少直接交互经验的信息，节点的信任度无法通过定义 2 和定义 4 进行估计和确定，对节点的信任度则可以采取折中考虑，初始分配为 0.5（取值为 0.5 表示不确定状态）。

4.2 信任机会路由成本计算

在 4.1 节中，网络中的节点可以通过利用基于信任相似性的信任模型来判断周围邻居节点的转发行为：如果存在恶意攻击行为，那么恶意节点将被剔除网络，而剩下的其他节点都可以认为是可信的节点。因此，在本节中，本文假定通过上节的计算模型对恶意节点进行筛选过滤，只在可信的网络安全环境中考虑机会路由成本的计算情况，以及转发列表的选择和列表中节点优先级的确定。因此，在此环境下，所提到的机会路由可以称之为信任机会路由。

定义 6 （有序图表示）：也可以用有序图 $X=(V,e)$ 表示 ad hoc 网络，其中，V 仍为网络的非空节点集合，e 为有序链路集合。一条有序链路可以用有序节点对 (i,J) 来表示，其中，$i\in V$，$(i,J)\in e$，J 为包含节点 i 所有邻居节点 $N(i)$ 的非空子集，$J\subseteq N(i)$（机会路由中的邻居转发列表）。

定义 7 （信任邻居转发列表）：该列表中包含的下一跳邻居节点中都具有较高的信任度，并且其成本距离目的节点较小。

本文用 $J(i)$ 表示节点 i 的信任邻居转发列表 $(J(i)\in J)$，其中，对任何一个节点 $j(j\in J(i))$，保证 j 是信任度较高的节点，即 $T(i,j)>T_{\text{threshold}}$。其中，$T_{\text{threshold}}$ 为网络中节点的信任度阈值。

定义 8 （信任转发列表）：在节点 i 到目的节点的路由中，依次从中间节点的信任邻居转发列表中有序选择的最终转发节点所组成的集合。

信任邻居转发列表是每个节点在转发数据分组时优先考虑转发给下一跳备选节点的集合。而信任转发列表是整个路由在建立过程中，最终从中间节点的信任邻居转发列表中选出的转发节点的集合。因此，信任转发列表是整个路由建立过程中的中间节点的信任邻居转发列表并集的子集。也即当此路由是最小成本机会路由时，转发列表为所有下一跳被确定的中间节点所组成的集合。

由于无线链路具有信道干扰的特点，通过对链路质量进行评估来计算机会路由成本。由文献[19]可知，通过在一定周期内节点检测发送探测数据分组的情况，计算该链路的期望传输次数(*ETX*)来评估链路质量。因此 G 中的任意一条链路的传输概率都可以采用此方法得出。

定义 9 （前向链路成本）：当节点 i 向信任邻居转发列表 $J(i)$ 发送数据分组时，$J(i)$ 中至少有一个节点接收到该数据分组的概率为 $p_{i,J(i)}$，此时所对应的期望传输次数即为前向链路成本。

用 $d_{i,J(i)}$ 表示节点 i 的前向链路成本，即 $d_{i,J(i)}=\dfrac{1}{p_{i,J(i)}}$。

假设节点 i 和节点 $j(j\in J(i))$ 之间的传输概率为 $p_{i,j}$。由于节点 i 和 $J(i)$ 中任何节点的链路之间发生占用链路信道资源产生干扰事件是相互独立的，因此可以得出：$p_{i,J(i)}=1-\prod_{j\in J(i)}(1-p_{i,j})$。

很显然，机会路由中一条信任路由的成本计算可以通过对路径中所有有序链路 $(i,J(i))$ 的前向链路成本求和获得。

定义 10 （信任路由成本）：即当前信任机会路由中存在的其中一条信任路由的成本。

设 R 为当前存在的机会路由集合，其中的一条路由为 r：$r=(s,n_1,n_2,\mathrm{L},n_k,d)$，$r\in R$，$C_r$ 为 r 的成本，$(s,n_1),(n_1,n_2),\cdots,(n_k,d)$ 为信任路由中包含的链路，$\{n_1,n_2,\mathrm{L},n_k,d\}$ 为节点 S 的信任转发列表。即

$$C_r=\sum_{i\in r}d_{i,J(i)}=d_{s,J(s)}+d_{n_1,J(n_1)}+\mathrm{L}+d_{n_k,J(n_k)} \tag{5}$$

其中，$J(i)$ 为 r 的中间节点 i $(i\in\{n_1,n_2,\mathrm{L},n_k,d\})$ 的信任邻居转发列表。实际上，式(5)的计算方式是通过中间节点利用定义 7 的信任邻居转发列表选择转

发节点，以此重复此过程，直至到达目的节点。

从式(5)中可以看出，信任路由成本的计算公式是通过确定中间节点的转发节点最终利用前向链路成本求和得出。即信任机会路由成本的量化计算可以通过基于前向链路成本进行进一步扩展前向链路成本和剩余路径成本。因此，信任机会路由的成本（见定义 12）也可以通过采用对应节点距离目的节点的成本距离来表示。

定义 11　（剩余路径成本）：$J(s)$ 中任意节点 j 到达目的节点的权重成本之和即为从节点 s 到目的节点的剩余路径成本。用 $R_{s,J(s)}$ 表示剩余路径成本。

由以上定义可以得出：s 到目的节点 d 的信任机会路由成本 D_s 包括两部分：从 s 到 $J(s)$ 的前向链路成本和从 $J(s)$ 到目的节点 d 的剩余路径成本（具体如图 2 所示）。即

$$D_s = d_{s,J(s)} + R_{s,J(s)} \tag{6}$$

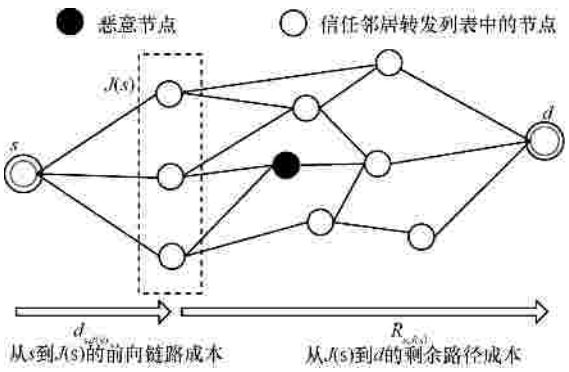

图 2　信任机会路由成本表示示例

而 $R_{s,J(s)}$ 的计算方法为

$$R_{s,J(s)} = \sum_{j \in J(s)} w_j D_j$$

其中，$\sum_{j \in J(s)} w_j = 1$。

权重 w_j 表示节点 j 成为转发节点的概率，D_j 为节点 j 到目的节点的成本。当 $J(s)=\{1,2,\cdots,n\}$ 时，各个节点距离目的节点的成本有如下关系：$D_1 < D_2 < \cdots < D_n$，则 $J(s)$ 中其他节点优先级比节点 j 高的备选节点都没有机会成为有效转发节点的概率为 $p_j(1-p_{j-1})(1-p_{j-2})\cdots(1-p_1)$，$w_j = \dfrac{p_j \prod_{k=1}^{j-1}(1-p_k)}{1-\prod_{j \in J(i)}(1-p_j)}$。

鉴于一条路由中各个节点可能受当前网络无线信道资源、拓扑动态变化和各个节点剩余能量等网络状况的影响，因此一条路由 r 可能以特定的概率出现，同时又由于无线网络具有广播特性，当信任转发列表中的节点接收到数据分组后，可能产生相应的 R 条可选机会路由，对这 R 条路由进行综合计算，得出如下的定义。

定义 12　（信任机会路由成本）：即在一对节点之间所有可能出现的信任路由成本之和。即

$$COR(R) = \sum_{r \in R} p(r) C_r \tag{7}$$

由于网络的动态变化以及无线链路的时变性，导致各条信任路由的建立具有一定的概率。因而，节点在选择路由时可能表现出一定的机会性，正与机会路由的思想一致。因此本文也是基于此思想来设计信任机会路由转发模型。具体 $p(r)$可以根据实际的网络情况进行近似估计(当前网络的拥塞情况、发送数据分组的速率、信道的干扰情况)。在本文中，假定 R 中的所有信任路由的 $p(r)$ 都设置为 1。当 $p(r)$ 都为 1 时，此时定义 12 对机会路由的成本量化和式(6)的计算思想是相同的。

4.3　信任机会转发模型

1)　备选转发节点选择机制

最优转发节点机制的设计需要对以下问题进行折中考虑：一方面，选择过多的备选节点将减少整个数据分组的转发成本（数据分组发送给任何一个备选节点的成本计算）；另一方面，从每一个信任邻居转发列表中选择的备选节点对于最优路由的选择没有给网络的性能带来实质性的提高。因此，利用较多的备选转发节点可能增加数据分组不选择此最优路由传输的概率。本文通过利用节点 i 到目的节点 d 的成本距离表示从 $J(i)$ 中确定最优的备选转发节点和该节点对应的转发优先级。但是需要注意的前提条件为：从信任邻居转发列表 $J(i)$ 中挑选出作为备选节点的信任度必须大于网络中的信任度阈值 $T_{\text{threshold}}$，以此避免恶意节点加入 $J(i)$ 中，并且减少恶意节点对整个网络的攻击。

本文采用一种简单的备选转发节点选择机制，具体的思想如下。当节点 i 发送数据分组时，针对 $J(i)$ 中存在不同的转发节点情况，可进行如下策略选择：如果 $J(i)$ 中只有一个转发节点，则该转发节点作为备选节点向下一跳节点转发数据分组；如果 $J(i)$ 中存在多个转发节点，这些转发节点中对应的与目的节点 d 成本距离最小的节点将分配最高的转

发优先级，那么该节点就优先考虑作为最优的转发节点。很显然，成本距离越小的节点，其对应的转发优先级越高，则该节点成为备选节点转发数据分组的可能性就越大。但是，如果当前优先级最高的节点不能及时地转发数据分组，则转发优先级次高的节点则成为最优的节点来进行数据分组转发。整个过程中需要采用一种高效的协调机制对备选节点之间的协作转发提供保证。如果 $J(i)$中的任何一个节点都没有接收到对应的数据分组，则节点 i 需要对该数据分组进行重传以提高整个机会路由中数据分组传输的可靠性。具体实现见第 5 节的 MCOR 算法。

2) 模型建立

在保证转发列表中节点都是可信的基础上，对列表中的转发节点进行成本距离优先级排序，最后根据定义 12 选择机会成本最小的路由。因而既保证了机会转发路由的成本最小，又避免恶意节点对网络的攻击。综合以上节点信任度和机会路由成本的计算思想，建立信任机会转发模型。即目标函数为

$$\min \forall r \ COR(R)$$

对应的约束条件为：对于任意一条信任路由 r 的任意中间节点 i 的信任邻居转发列表为 $J_{r\in R}(i)$，存在任何节点 $k \in J_{r\in R}(i)$，k 必须满足：$T(i,k) > T_{\text{threshold}}$。$T_{\text{threshold}}$ 为信任度阈值。即在信任邻居转发列表中只有优先级和信任度较高的节点才可以参与数据分组的机会转发过程。

当 $COR(R)$ 取得最小值时，即从当前所建立路由中的中间各个节点的信任邻居转发列表中所选择的转发节点形成信任转发列表。

为了详细地描述信任最小成本机会路由的建立过程，本文在第 5 节给出了路由算法的形式化描述。

5 MCOR 路由算法

5.1 算法描述

本算法结合 ad hoc 网络的特点考虑采用分布式算法求解。图 3 给出了信任最小成本机会路由算法的整体框架。整个框架包含了 3 个部分：信任管理、信任机会转发模型和最小成本的信任机会路由算法 MCOR。MCOR 算法在设计过程中所涉及的假设条件如下：任何节点之间的链路都是双向连接，每个节点将自身设置为混杂监听模式，以此监听邻居节点数据分组的转发行为。另外，为防止由于网络中链路的不稳定性影响数据分组传输的效率，对邻居节点行为的监测也可以通过被动确认(passive ack)方式[32]进行实现。ad hoc 网络中各条链路的传输概率通过周期性地发送探测分组来进行估计。关于节点间信任度计算的形式化算法如图 4 和图 5 所示。

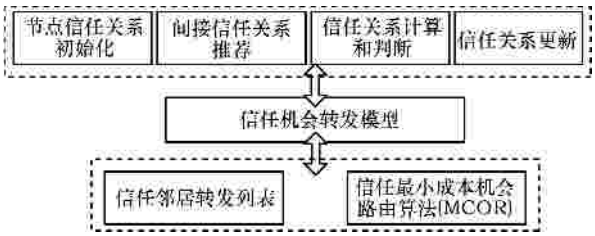

图 3 MCOR 算法框架

算法 1 Calculating TrustDegree (i,j)

1) //对节点 i 和邻居节点 j 之间的信任度进行初始化
2) 节点 i 通过收集周围邻居节点相关链路情况构建局部拓扑
3) 从本地保持的邻居节点列表中获取周围邻居节点历史数据分组转发行为情况，节点 i 可以计算出与节点 j 的直接信任度
4) If (节点 i 和节点 j 之间不存在交互信息)
then
5) 节点 i 和节点 j 之间的信任度可以通过直接信任度进行初始化计算，具体为

$$T(i,j) \leftarrow T^{d}(i,j) \leftarrow 0.5$$

6) 节点 i 对节点 i 与节点 j 之间的直接信任度和当前时间等信息进行本地保存
7) Else if (节点 i 和节点 j 之间存在交互信息 j) then
8) Updating DirectTrustDegree(i,j)
9) 节点 i 对节点 i 与节点 j 之间的直接信任度和当前时间等信息进行本地保存
10) 节点 i 通过利用信任相似性的计算公式(2)对周围邻居节点的信任推荐能力进行评估
11) 节点 i 通过根据上一步信任推荐能力较强的邻居节点利用公式(3)计算间接信任度
12) 根据第 10)步和第 11)步的计算情况，利用式(4)计算出节点 i 和节点 j 之间的信任度
13) Else
14) $T(i,j) \leftarrow 0$
15) End if
16) Return $T(i,j)$

图 4 CalculatingTrustDegree 算法

算法 2　Updating DirectTrustDegree (*i*,*j*)

1) //对节点 *i* 和邻居节点 *j* 之间的直接信任度进行更新
2) 根据当前网络的拓扑情况，节点 *i* 判断与节点 *j* 的链路情况
3) 节点 *i* 从本地缓存的信息表中提取出相关信息（上次与节点 *j* 的直接信任度、上次存储时间、*s* 和 *f* 等）；
4) If (节点 *i* 与节点 *j* 的链路存在&& $T_{old}^{d}(i,j)>0$) then
5) $T_{new}^{d}(i,j)$ 可以通过式(1)进行计算更新
6) Else if (节点 *i* 与节点 *j* 的链路不存在&& $T_{old}^{d}(i,j)\le 0$) then
$T_{new}^{d}(i,j)\leftarrow 0$
7) Else
节点 *i* 在一定周期时间 *T* 内通过发送 HELLO 探测分组获取周围邻居节点的存活情况和链路情况
8) End if
9) Return $T_{new}^{d}(i,j)$

图 5　UpdatingDirectTrustDegree **算法**

在设计 MCOR 算法之前，采用 Filtering Neighbor MNodes 算法(如图 6 所示)过滤掉任何节点 *i* 周围邻居节点中包含的恶意节点，形成信任邻居转发列表，并删除恶意节点与节点 *i* 的所有链路。MCOR 算法描述了 *G* 中任意节点到目的节点 *d* 最小机会成本的计算思想。其中，*EXTRACT-LEAST-COST* 函数表示从当前节点集合中选择距离目的节点 *d* 成本最小的节点。*S* 为在遍历过程中保存当前存在最小成本机会路由时所经过的节点。算法形式化描述如图 7 所示。

算法 3　Filtering NeighborMNodes (*G*,*i*)

1) For each edge (*i*, *j*) in *E*
2) Do
3) If (Calculating TrustDegree (*i*, *j*) $\le T_{threshold}$) then
4) $E\leftarrow E-edge(i,j)$
5) $V\leftarrow V-\{j\}$
6) End if
7) End for

图 6　Filtering NeighborMNodes **算法**

5.2　算法的有效性分析

定理 1　（无环性）：MCOR 算法保证一定不会出现环。

算法 4　Minimum-cost OR (*G*, *d*)

1) For each node *i* in *V*
2) Do Filtering NeighborMNodes (*G*, *i*)
3) $D_i\leftarrow\infty$
4) $F_i\leftarrow f$
5) End for
6) $D_d\leftarrow 0$
7) $S\leftarrow 0$
8) $Q\leftarrow V$
9) While $Q\neq f$
10) Do $j\leftarrow EXTRACT\text{-}LEAST\text{-}COST(Q)$
11) $S\leftarrow S\cup\{j\}$
12) For each edge (*i*,*j*) in *E*
13) Do $J\leftarrow F_i\cup\{j\}$
14) If ($D_i>D_j$) then $D_i\leftarrow d_{i,J}+D_J$
15) $F_i\leftarrow J$
16) End if
17) End for
18) End while

图 7　MCOR **算法**

证明　采用反证法进行证明。假如网络中至少存在一条环。设环为$(i,j,k,\cdots,l,i)$，环中包含的所有节点都是信任度较高的节点，如图 8 所示。

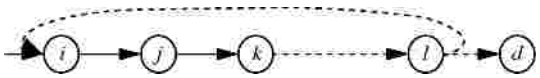

图 8　存在一条环的网络示意

由于(i,j,k,L,l,i)环为有序序列，环中各个节点到目的节点 *d* 的最小机会路由成本为：D_i^*、D_j^*、D_k^*、D_l^*。很显然，$D_i^*>D_j^*>D_k^*>D_l^*$。由于节点 *i* 和 *l* 之间存在环，节点 *l* 在计算到节点 *d* 的机会路由成本时，必然考虑了信任邻居转发列表 $J(l)$ 中节点 *i* 对路由成本的影响。由于 $D_i^*>D_l^*$，如果把节点 *i* 从 $J(l)$ 中删除，则更新 $D_l^{*\prime}$，且存在如下计算关系：$D_l^{*\prime}\le D_l^*$。这与假设 D_l^* 为从节点 *l* 到节点 *d* 为机会路由的最小成本相矛盾，因此算法一定在执行过程中不出现环。证毕。

定理 2　（最优性）：MCOR 算法一定能够得到最优解。

证明　假设节点 *i* 的信任邻居转发列表为 $J(i)$，则节点 *i* 到目的节点 *d* 存在最小成本的机会路由为

D_i^*。仍然采用反证法。假设存在的最小成本路由为 $D_i^{*\prime}$ 而不是 D_i^*，对应采用的信任邻居转发列表为 $J'(i)$，则 $D_i^{*\prime} \le D_i^*$，即 $d_{i,J'(i)} + R_{i,J'(i)} \le d_{i,J(i)} + R_{i,J(i)}$。然而由于 D_i^* 不是最小成本的机会路由，$J(i)$ 中至少存在一个类似的节点 m，使得 $D_m \ge D_i^*$，从而可以通过删除类似的节点最终形成新的信任转发列表 $J''(i)$，从而可以得到节点 i 到节点 d 的其他最小成本机会路由 $D_i^{*\prime\prime}: D_i^{*\prime\prime} = d_{i,J''(i)} + R_{i,J''(i)}$。这与假设的条件相矛盾($D_i^{*\prime}$ 为最小成本的机会路由)。因此，算法一定能够得到最优解。证毕。

5.3 算法的时间复杂性分析

定理 3 （算法开销）：MCOR 算法的时间复杂性为 $O(|V|\log|V|+|E|)$。

证明 该算法的时间复杂性主要取决于从第 9)步~第 18)步 while 循环中 Q 的执行效率。第 10)步的时间开销主要体现在函数 *EXTRACT-LEAST-COST* 中。假如在本算法中采用 Fibonacci 堆，则第 10)步的时间开销对应为 $O(|V|\log|V|)$。接着从第 12)步~第 17)步的时间开销主要花费在 for 循环中遍历 G 中所有的边集合 E，其中包括 S 集合、各个节点到 d 的最小机会成本和信任转发列表的更新和计算，大致的时间花费为 $O(|E|)$。因此，本算法的时间复杂性为以上两部分之和，即 $O(|V|\log|V|+|E|)$。证毕。

6 仿真与分析

6.1 仿真环境设置

为了验证 MCOR 算法的有效性，采用 Nsclick[34] 和 Madwifi[33] 扩展分组进行真实模拟测试。Nsclick 仿真分组是结合当前流行的 NS2[35] 和 Click Modular Router[34] 框架整合在一起的扩展分组，以便在真实的无线网络中设计路由协议时进行移植开发。

本文的仿真环境基于 MAC 层使用 IEEE 802.11b 的 DCF，移动模型采用 random waypoint，以及将 CBR(constant bit rate)作为传输流量模型，发送数据分组的速率为 4 packet/s，每个数据分组可以随机地从一个源节点传输到另一个随机地目的节点，移动速度在 0～20 m/s 之间任意选择。到达目的节点后，经过一个暂停时间(0～100 s)再开始新的传输过程。仿真过程中一共生成 25 种随机拓扑，每种情况对应 5 种，最后的数据为 5 种拓扑所产生数据的平均值。

本文的拓扑结构采用改进的 Waxman[36] 方法思想，它可以产生实际网络的拓扑结构。具体 Waxman 方法的思想为：网络中随机产生 N 个节点，并将这些节点均匀地分布在一定拓扑区域中，任意 2 个节点 i 和 j 之间按一定的概率建立连接，节点间连接概率的取值具体由节点间的欧拉距离决定，从而将节点间链路的存在是否与节点间的距离进行关联。而链路的产生概率可以通过如下公式进行计算。

$$p(i,j) = w_1 \exp\frac{-Dis(i,j)}{w_2 L_{\max}}$$

其中，$Dis(i,j)$ 表示节点 i 和节点 j 之间的欧式距离，$L_{\max}$ 表示整个网络中任意节点间的最大距离，w_1 和 w_2 为对应的动态调整参数（$0<w_2<1, 0<w_1<1$）。当 w_2 逐渐增大时，网络中边的密度也在增大，而当 w_1 减少时，网路中节点间距离较小的边相对于距离较大的边的密度也在增大。通过对参数 w_1 和 w_2 进行调整，使得距离较小的边存在的概率大于较长边存在的概率，并且使得图中的节点平均密度为 4~6。基于此，在假定各个节点的传输半径是相同的前提条件下，根据节点间的距离与传输半径进行对比情况，优化 Waxman 拓扑思想，并结合参数 w_1 和 w_2 的调整，使得彼此节点位于各自传输半径范围内，确保距离较小的边对应的链路连通性较高，以及整个网络的密度适中，最终实现网络拓扑图的连通性。通过实验得到的网络拓扑结构如图 9 所示（初始网络中各个节点的信任水平都取值适中，不对节点的恶意和正常行为进行区分）。

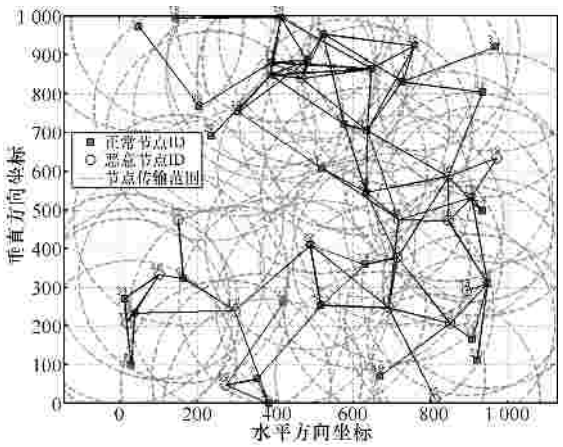

图 9 仿真过程中网络的拓扑结构

图 9 中存在 35 个正常的善意节点(benevolent node)和 15 个恶意节点(malicious node)。对恶意节

点攻击进行模拟假设如下：恶意节点随机选择性地在[0.4~0.8]概率范围内丢失接收到的数据分组。其他的参数设置如表 1 所示。

表 1　仿真参数设置

参数	表示的意义	取值
Area	网络拓扑区域	1 000 m × 1 000 m
N	网络中的节点个数	50
r	节点的传输半径	250 m
S	节点的最大移动速度	20 m/s
P	数据负载大小	512 byte/packet
a	$T^d(i,j)$的权重因子	0.6
ß	$T^r(i,j)$的权重因子	0.4
$\triangle t$	信任更新周期	0.2 s
T	仿真时间	500 s
M	恶意节点个数	1~20
$T_{threshold}$	网络中的信任度阈值	0.6
RF	成功交互的奖励比例	0.8
PF	失败交互的惩罚比例	0.2

6.2　性能对比参数

为了验证 MCOR 算法的性能，并与 ExOR、TAODV 和 Watchdog-DSR 协议进行实验对比，本文将围绕以下几个参数进行分析。

1) 吞吐量：定义为每秒钟从源节点向目的节点发送的数据分组个数或字节数。

2) 平均机会路由成本：定义为网络中所有节点与确定的目的节点的机会路由成本之和的平均值。

3) 平均期望传输次数：定义为根据各个链路的实际情况，所有链路中发送数据分组的平均期望传输次数。

4) 恶意检测概率：定义为网络中通过监听和发送确认的方式正确检测出恶意节点的数目与当前节点总数的比值。本节引入这个参数的目的主要是将 MCOR 算法的思想与当前研究中典型的 2 种对恶意攻击防范措施—TAODV[15]和 Watchdog-DSR[16]进行对比。

5) 端到端的平均时延：包括路由查找时延、数据分组在接口队列中的等待时延、传输时延及 MAC 层的重传时延，反映了路由的有效性。端到端的平均时延=S (接收到数据分组的时间- 发送数据分组的时间)/发送数据分组的个数。

6.3　仿真结果与分析

图 10 和图 11 显示了在不同条件下 MCOR 算法与 ExOR 协议在吞吐量、平均机会路由成本、平均期望传输次数、平均转发列表大小方面的性能对比情况。图 10(a)给出了当恶意节点数在不断增加时吞吐量的对比情况：总体来说，2 种算法的吞吐量都在逐步递减，但 MCOR 算法的吞吐量(从 176 kbyte/s 降为 60 kbyte/s)略高于 ExOR 协议(从 160 kbyte/s 降为 40 kbyte/s)，其原因在于随着恶意节点的逐渐增多，通过利用本文所提出的信任模型来对各个节点信任度判断，从而将恶意节点和恶意边剔除网络，减少了恶意节点对网络吞吐量的影响，因此各个节点利用无线网络的广播特性，结合预先形成的信任邻居转发列表，可以加快数据分组的转发速率，从而提高网络的吞吐量。然而 ExOR 协议没有考虑增加对恶意攻击的防范措施，因而其吞吐量的性能略低一些。

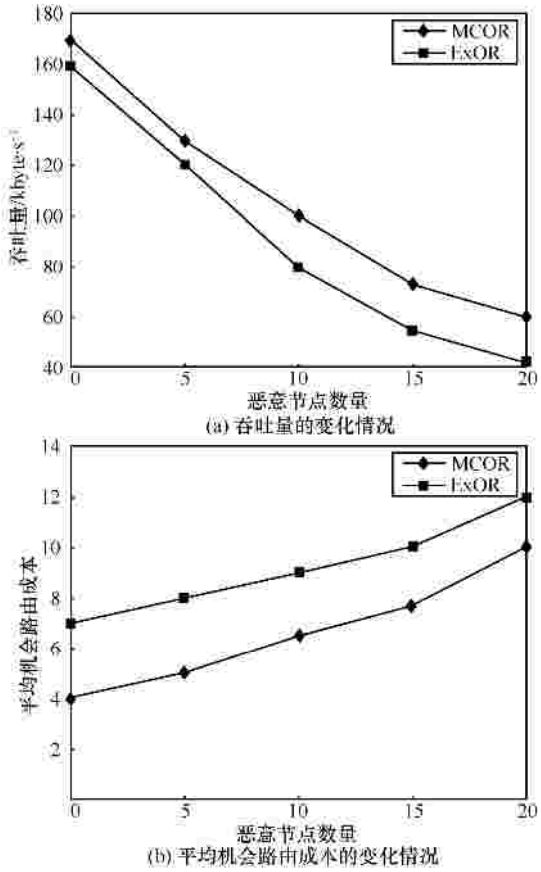

图 10　在不同恶意节点数量下，2 种算法在吞吐量和平均机会路由成本方面的对比情况

图 10(b)采用与图 10(a)相同恶意节点数的条件下进行平均机会路由成本的对比：ExOR 协议的平均机会路由成本从 7.8 增加到了 12，而 MCOR 算法对

应从 4.5 增加到 11.7，ExOR 协议的路由成本开销略高于 MCOR 算法，产生原因为：本文的机会路由成本思想充分利用信任邻居转发列表并发转发数据分组，以及结合列表中的节点距离目的节点的剩余成本进行加权计算剩余路径成本，联合前向链路高可靠转发概率形成前向链路成本，通过递归回溯计算最小的机会路由成本，但是由于恶意节点的增多增加了机会路由成本中节点协调转发的开销，相对而言，MCOR 算法性能略高于 ExOR 协议。

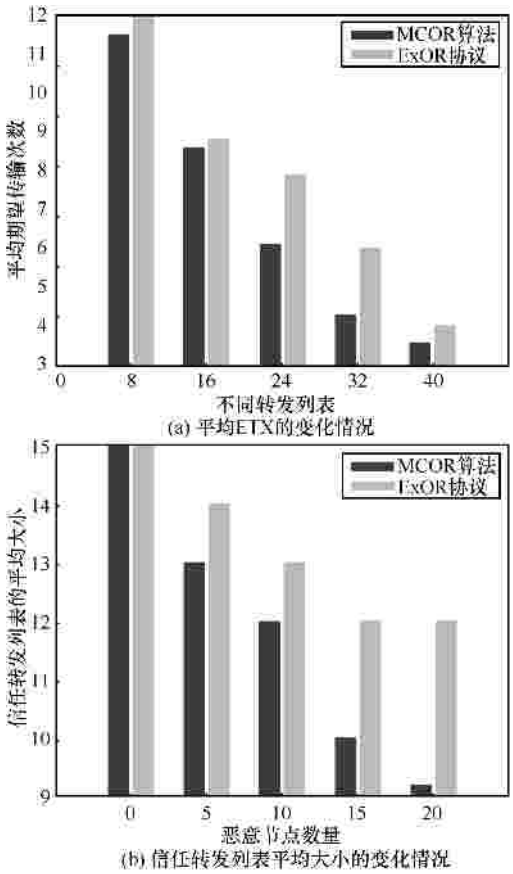

图 11 2 种算法在不同转发列表和不同恶意节点数量下的对比情况

为了更有效地验证 2 种协议模式下信任列表中各个节点对各条链路 ETX 的影响，本文在信任邻居转发列表大小设置为 8~40 时进行仿真实验，图 11(a)最后给出了实验对比结果。该结果的产生与图 10 的原因类似，为了防范恶意攻击对网络的影响，引入节点信任度的计算方法，过滤掉原来邻居转发列表中的恶意节点和恶意链路，从而更新各个节点的期望传输次数以及平均 ETX，而 ExOR 协议没有考虑恶意节点的影响，从而得出：ExOR 协议的平均 ETX 略高于 MCOR 算法。本文也进一步考虑了恶意节点对信任转发列表的影响并进行了仿真，如图 11(b)所示。图 11(b)表明了随着恶意节点数的增加，虽然减少了信任转发列表中的节点数，影响了机会转发的概率，但在这种情况下，MCOR 算法中的信任机制能够利用现有为数不多的可信节点加入信任邻居列表中，以此形成有效的信任转发列表，维持恶意攻击较为严重情况下的安全通信，提高了网络正常转发数据分组的效率，减少了网络中出现通信中断的可能性。

为了进一步对本文提出的基于信任相似性的信任模型进行验证和分析。本节也将 MCOR 与 TAODV 和 Watchdog-DSR 在恶意攻击的检测概率上进行了对比和分析，具体如图 12(a)所示。随着恶意节点数的增加，3 种方式的检测概率都在下降。从这个过程中可以看出，当恶意节点数增加到 20 时，网络遭受恶意攻击的程度最高，3 种算法对恶意攻击的检测能力基本上维持在最低的水平。但是相对来说，MCOR 算法对恶意攻击的检测概率上还是略高于 TAODV 和 Watchdog-DSR 算法。导致产生这种现象的原因与各自对恶意攻击的防范机制有关：Watchdog-DSR 算法是利用直接观察邻居节点的转发行为为辨别恶意攻击提供依据(Watchdog 机制)，TAODV 是基于 Josang[65]等人提出的主观逻辑思想，用观点(opinion)作为辨别恶意攻击的经验信息，而 MCOR 算法是基于直接和推荐信任的思想，此外避免在获取推荐信任信息的过程中获取的信息存在较大差异，增加了推荐节点推荐能力的相似性估计。很显然，Watchdog-DSR 算法中存在监测过程中观测信息的不全面性，容易产生误判情况；而 TAODV 在 ad hoc 网络中的可操作性不强。因此，MCOR 算法能够在整个恶意攻击的检测过程中增加检测的可靠性和准确性。

针对图 12(a)的分析情况，在 MCOR 算法和 ExOR 协议的对比基础上，增加 TAODV 和 Watchdog-DSR 算法的时延开销分析。具体的对比情况如图 12(b)所示。图 12(b)给出了在恶意节点数逐渐增多的情况下，端到端时延开销的对比情况。由于 MCOR 算法增加了对节点度的计算、判断和更新的过程，需要增加额外控制信息的开销，此外，以信任转发列表中节点之间的协调转发机制对节点优先级和最优转发节点进行确定，以上过程和机制的额外维护开销是 MCOR 算法时延开销的主要来源，因此 MCOR 算法的时延开销比 TAODV 和 Watchdog-DSR 这 2 种算法的略高。ExOR 协议缺少对恶意攻击的防范能力，恶意

节点的增多严重地影响了通信的正常进行，导致网络出现了分割的可能，在这种情况下断裂处的转发节点可能误以为与下一跳节点的链路发生断裂，不断地重传需要转发的数据分组。因此，数据分组的重传时延和在本地缓存队列中产生的等待时延增加了 ExOR 协议的时延开销。

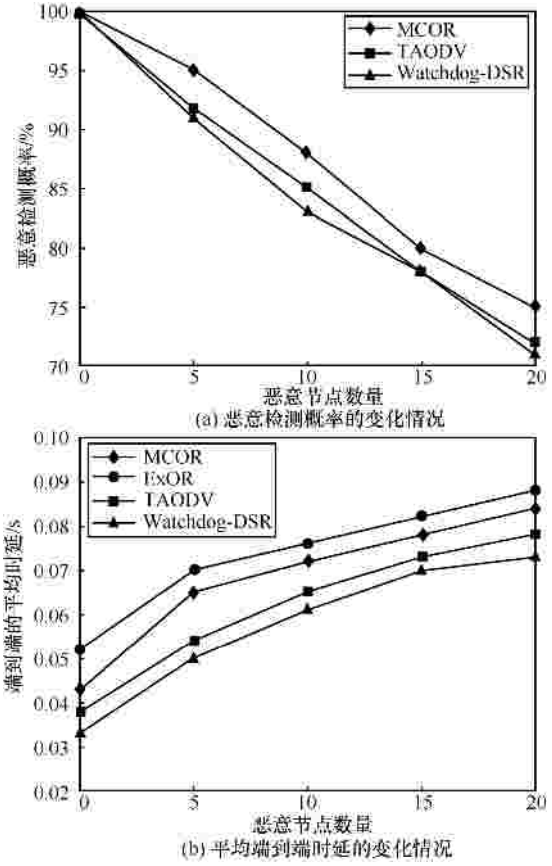

图 12　在不同恶意节点数下，各个算法在恶意检测概率和时延方面的对比情况

最后，本文也针对式(4)中权重因子 a 和 b ($a+b=1$)的不同变化情况，来验证本文提出的基于信任相似性的信任模型的有效性：一方面，本文从不同仿真时间环境下给出不同权重因子对应的信任度对比情况(如图 13(a)所示)；另一方面，本文也在不同信任更新周期环境下给出不同权重因子对应的信任度对比情况(如图 13(b)所示)。从图 13(a)中可以看出：随着仿真时间的增加，3 种权重因子 $a=0.2$、$a=0.5$ 和 $a=0.8$ 所对应的信任度也在相应增加。产生此情况的主要原因是由于仿真时间的增加将提供给节点更多熟悉和频繁交互的机会，提高节点之间信任度的准确性。但是权重因子 $a=0.8$ 高于其他 2 种情况主要是因为节点之间直接交互而产生的直接信任度决定了节点转发列表中节点信任度的计算，较为客观、真实地反映节点当前的信任度。此外，从图 13(b)中可以看出：随着节点信任更新周期的不断递增，3 种权重因子所对应的信任度在逐渐递减。产生此现象的主要原因是：节点频繁移动和节点间交互次数的增加，需要在节点信任更新周期较短的时间内对节点的信任度进行更新，以便反映出网络中节点最新的信任度，从而提高节点转发列表中对恶意节点剔除的检测概率。然而，由于权重因子 $a=0.8$ 的信任度主要由直接信任度来计算，可以避免间接信任度更新不及时而产生的信任度计算误差，因而其信任度的整体趋势要高于其他 2 种情况。

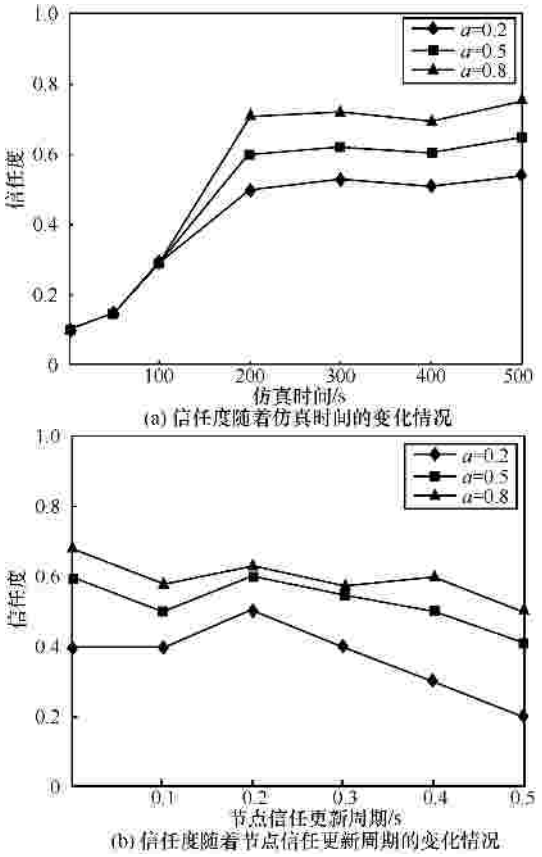

图 13　不同权重因子计算出的信任度在不同环境下的对比情况

7　结束语

本文重点探讨软安全中信任模型的问题，以及结合当前研究热点之一的机会路由，通过进行综合分析，建立了一种基于节点信任度和机会路由成本的信任机会转发模型，提出了 MCOR 算法，并对该算法进行了理论上的证明，最后通过 Nsclick 仿真软件进行实现和验证，又与经典的机会路由协议

ExOR，以及信任路由协议 TAODV 和 Watchdog-DSR 进行了性能上的对比。仿真结果验证了 MCOR 算法的有效性，以及在防范恶意节点攻击及机会路由成本方面性能上的显著改进。在未来的工作中，将更深入地对该算法进行性能测试，并考虑利用网络编码进一步提高机会路由的吞吐量和数据分组的转发效率，提供 QoS 保证的多媒体服务应用(快速文件上传/下载)以及考虑在转发列表中设计节点高效协调机制，以减少网络数据分组的传输时延。

参考文献：

[1] 田克，张宝贤，马建等. 无线多跳网络中的机会路由[J]. 软件学报，2010, 21(10):2542-2553.
TIAN K, ZHANG B X, MA J,*et al*. Opportunistic routing protocols for wireless multihop networks[J]. Journal of Software, 2010, 21(10): 2542-2553.

[2] BISWAS S, MORRIS R. ExOR: opportunistic multi-hop routing for wireless networks[A]. Proceedings of ACM SIGCOMM[C]. Pennsylvania, USA, 2005. 133-144.

[3] LU M M, WU J. Opportunistic routing algebra and its applications[A]. Proceedings of INFOCOM[C]. Riode Janeiro, Brazil, 2009. 2374-2382.

[4] DUBOIS-FERRIERE H, GROSSGLAUSER M, VETTERLI M. Least-cost opportunistic routing[A]. Proceedings of 2007 Allerton Conference on Communication, Control, and Computing[C]. Monticello, USA, 2007. 1-8.

[5] ZENG K, LUO W, ZHAI H. On end-to-end throughput of opportunistic routing in multirate and multihop wireless networks[A]. Proceedings of IEEE INFOCOM'08 Conference[C]. Phoenix, USA, 2008. 1490-1498.

[6] ZHONG Z, NELAKUDITI S. On the efficacy of opportunistic routing[A]. Proceedings of SECON '07[C]. San Diego, USA, 2007.18-21.

[7] LU M, LI F, WU J. Efficient opportunistic routing in utility-based ad hoc networks[J]. IEEE Trans Reliability, 2009, 58(3):485-495.

[8] ZENG K, LOU W, ZHANG Y. Multi-rate geographic opportunistic routing in wireless ad hoc networks[A]. IEEE Milcom[C]. Orlando, USA, 2007.1-7.

[9] YANG Z Y, ZENG K, LOU W J. FSA: a fast coordination scheme for opportunistic routing[A]. Proceedings IEEE ICC 2009[C]. Dresden, Germany, 2009.1-5.

[10] CHACHULSKI S, JENNINGS M, KATTI S, *et al*. Trading structure for randomness in wireless opportunistic routing[A]. Proceedings of ACM SIGCOMM[C]. Kyoto, Japan, 2007. 169-180.

[11] CUI T, CHEN L, HO T, *et al*. Opportunistic source coding for data gathering in wireless sensor networks[A]. Proceedings of MASS[C]. Pisa, Italy, 2007.1-10.

[12] ZUBOW A, KURTH M, REDLICH J P. Multi-channel opportunistic routing[A]. Proceedings of IEEE European Wireless[C]. Paris, France, 2007.1-7.

[13] LI Y H, CHEN W, ZHANG Z L. Optimal forwarder list selection in opportunistic routing[A]. Proceedings of MASS[C]. Pisa, Italy, 2007. 670-675.

[14] ZHANG C, ZHOU M C, YU M. ad hoc network security: a review[J]. Int J Commun Syst, 2007, 20(8):909-925.

[15] LI X Q, LYU M R. A trust model based routing protocol for secure ad hoc networks[A]. Proc of IEEE Aerospace Conference[C]. Big Sky, Montana, USA, 2004. 1266-1295.

[16] MARTI S, GIULI T, LAI K, *et al*. Mitigating routing misbehavior in mobile ad hoc networks[A]. Proc of MobiCom'00[C]. New York: ACM, USA, 2000. 255-265.

[17] COUTO D D, AGUAYO D, BICKET J, *et al*. A high-throughput path metric for multi-hop wireless routing[A]. Proc of IEEE/ACM MOBICOM[C]. San Diego, USA, 2003.134-146.

[18] LUO J H, LIU X, FAN M Y. A trust model based on fuzzy recommendation for mobile ad-hoc networks[J]. Computer Networks, 2009, 53(14):2396-2407.

[19] LUO J, LIU X, ZHANG Y, *et al*. Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks[A]. Proc of the 33rd IEEE Conference on Local Computer Networks (LCN 2008)[C]. Montreal, Canada, 2008. 305-311.

[20] GONG W, YOU Z Y, CHEN D N, *et al*. Trust based routing for misbehavior detection in ad hoc networks[J]. Journal of Networks, 2010, 5(5):551-558.

[21] DAI H J, JIA Z P, QIN Z W. Trust evaluation and dynamic routing decision based on fuzzy theory for MANETs[J]. Journal f Software, 2009, 4(10):1091-1101.

[22] LI J, LI R, KATO J. Future trust management framework for mobile ad hoc networks[J]. IEEE Communications Magazine, 2008, 46(4):108-114.

[23] OMAR M, CHALLAL Y, BOUABDALLAH A. Reliable and fully distributed trust model for mobile ad hoc networks[J]. Computer Security, 2009, 28(3):199-214.

[24] MILLAN G L, PEREZ M G, PEREZ G M, *et al*. PKI-based trust management in inter-domain scenarios[J]. Computer Security, 2010, 29(2):278-290.

[25] LI F, WU J. Uncertainty modeling and reduction in MANETs[J]. IEEE Transaction on Mobile Computing, 2010, 9(7):1035-1048.

[26] 陈深龙，张玉清. 增强 ad hoc 网络可生存性的健壮多维信任模型[J]. 通信学报，2010, 31(5):1-9.
CHEN S L, ZHANG Y Q. Robust multi-dimensional trust model for improving the survivability of ad hoc networks[J]. Journal on Communications,2010,31(5):1-9.

[27] PENG S C, JIA W J, WANG G J, *et al*. Trusted routing based on dynamic trust mechanism in mobile ad-hoc networks[J]. IEICE Trans on Information and Systems, 2010, E93-D(3):510-517.

[28] ESCH J. A survey of trust and reputation management systems in wireless communications[A]. Proceedings of the IEEE[C]. 2010. 98(10):1755-1772.

[29] RAZA I, HUSSAIN S A. Identification of malicious nodes in an AODV pure ad hoc network through guard nodes[J]. Computer Communications, 2008, 31(9):1796-1802.

[30] LI X, JIA Z, ZHANG P, *et al*. Trust-based on-demand multipath routing in mobile ad hoc networks[J]. IET Information Security, 2010, 41(4):212-232.

[31] WANG F, WANG F R, HUANG B X, *et al*. COSR: a reputation-based secure route protocol in MANET[J]. EURASIP Journal on reless Communications and Networking, 2010, 2010:1-10.

[32] PIRZADA A A, MCDONALD C, DATTA A. Performance comparison of trust-based reactive routing protocols[J]. IEEE Transactions on Mobile Computing, 2006, 5(6):695-710.

[33] LETOR N, CLEYN P D, BLONDIA C. Enabling cross layer de : adding the mad Wi-Fi extensions to nsclick[A]. Proc the First International Workshop on Network Simulation Tools 2007[C]. Nantes, France, 2007. 1-10.

[34] KOHLER E, MORRIS R, CHEN B, *et al*. The click modular router[J]. ACM Trans on Computer Systems, 2000, 18(3):263-297.

[35] The network simulator-ns-2[EB/OL]. http://www.isi.edu/ nsnam/ns/, 2012.

[36] WAXMAN BERNARD M. Routing of multipoint connections[J]. IEEE Journal on Selected Areas in Communications, 1988, 6(9):1617-1622.

[37] WANG B, CHEN X X. An efficient trust-based opportunistic routing for ad hoc networks[A]. Proc of WCSP 2012, IEEE Communications Society[C]. Huangshan, China, 2012.1-7.

[38] WANG B, HUANG C H. Trust-based minimum cost opportunistic routing for ad hoc networks[J]. Journal of Systems and Software, 2011, 84(12):2107-2122.

作者简介：

王博（1982-），男，河南漯河人，博士，国家计算机网络应急技术处理协调中心工程师，主要研究方向为计算机网络与通信、信息安全。

陈训逊[通信作者]（1972-），男，山东庆云人，博士，国家计算机网络应急技术处理协调中心教授，主要研究方向为计算机系统结构、计算机网络与信息安全。E-mail: cxx@cert.org.cn。