移动自组网的主观信任建模与仿真

王 健[1,2],刘衍珩[1,2],张 婧[1,2],刘雪莲[3]
(1.吉林大学计算机科学与技术学院,吉林长春 130012;
2.吉林大学符号计算与知识工程教育部重点实验室,吉林长春 130012;3.吉林大学软件学院,吉林长春 130012)

摘 要: 不同于以往只考虑最短路径或只依靠转发行为评价信任或基于推荐机制的传统路由算法,提出了一种兼顾通信可靠性和路径长度的主观信任路由模型.通过引入属性相似度概念将邻居选择、信任评估、数据转发等路由环节紧密相连,进一步建立一种新的动态包转发规则,并给出了一种计算属性相似度的推荐方法.实验结果表明主观信任路由模型较传统的 DSR(Dynamic Source Routing)协议和以往的信任路由协议表现出较高的抵抗黑洞攻击和行为改变攻击的能力,同时也不受诽谤攻击的影响.

关键词: 移动自组网;属性相似度;恶意节点;信任路由;动态源路由协议
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2011) 12-2813-07

Modeling and Simulating Subjective Trust in MANETs

WANG Jian[1,2], LIU Yan-heng[1,2], ZHANG Jing[1,2], LIU Xue-lian[3]
(1. *College of Computer Science and Technology, Jilin University, Changchun, Jilin* 130012, *China*;
2. *Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun, Jilin* 130012, *China*; 3. *College of Software, Jilin University, Changchun, Jilin* 130012, *China*)

Abstract: Different from most the past routing algorithms only considering the shortest path first, or evaluating the trust level solely on the forwarding behavior, or depending on recommendation-based trust mechanism, we propose a novel subjective trust routing model under consideration to both communication reliability and path length. We introduce the concept of attribute similarity to inherently bind neighbor selection, trust evaluation, packet forwarding, and other routing processes. Based on the similarity degree, we put forward a new forwarding behavior. We give a recommended method to calculate the similarity degree between attributes. Simulations show that the routing scheme behaves better than Dynamic Source Routing (DSR) protocol and previous trust-based routing protocols on standing against the blackhole attack and the on-off attack, and meanwhile is not affected by the slander attack.

Key words: mobile ad hoc networks; attribute similarity; malicious nodes; trusted routing; dynamic source routing

1 引言

移动自组网(Mobile Ad hoc Networks, MANETs)的路由协议和应用系统普遍假设所有移动节点都是可信赖和协作的[1~3].然而由于有限的资源和恶意行为导致事实并非如此,例如,恶意节点会发起中间人、黑洞、拒绝服务等攻击.另外,一些其他因素如可靠性和带宽也会被路由决策所考虑,而不仅仅是追求路径的最短距离.为节点对赋予一个局部信任级别不仅能够减轻恶意行为的影响,而且有望使通信只发生在相互信任的节点之间.因此,将信任性引入进移动自组网路由环节中是十分重要的,同时设计一种能够允许节点准确评估其他节点尤其是陌生节点信任级别的信任系统也是十分必要的.

在本文模型中,每个节点自身的运行状态和特征被称之为属性,并构成属性集合,例如,移动瞬时速度和方向,通信距离,环境干扰,隶属组织等,这些属性的取值决定了节点在网络中的路由行为.任意节点对之间对应属性的相似程度称为属性相似度.在以往提出的信任传播模型中[4,5],节点的转发行为是固定不变的.但是,在实际的移动自组网系统中,节点可能是智能的,它的包转发行为并不是固定的,它受节点转发时刻的自身状况、周围环境状况等因素影响.因此,本文定义了一种新的动态包转发规则:一个节点 i 决定是否转发来自其邻居节点 j 的数据包取决于节点 i 与节点 j 之间的属性相似度.另外,已有的大多数路由模型只追求路径长度的最短[6,7],这种策略在链路质量较稳定和安全性较高的有线网络较为适合,但是移动自组网开放的链路、不断的移动、易变的拓扑等特点均会造成单一的路径最短衡量指标不一定是最佳路由.因此,本文基于属性相似

收稿日期:2010-08-18;修回日期:2011-01-20
基金项目:国家自然科学基金(No.60973136, No.61073164);科技部国际科技合作与交流专项(No.2008DFA12140);欧盟 BTG 合作项目(No.155776-EM-1-2009-1-IT-ERAMUNDUS-ECW-L12);吉林大学研究生"985 工程"创新计划项目(No.20101029);吉林大学基本科研业务费项目(No.201103136)

度进一步提出了一种兼顾通信可靠性和路径长度的主观信任路由模型.

2 相关工作

2.1 信任评估

文献[8]基于声誉机制扩展了源路由协议以便检测和惩罚移动自组网中的自私节点,不过他们没有考虑到如何计算声誉值.文献[9]通过贝叶斯方法评估节点主观信任,但是无法检测不诚实的推荐.文献[10]基于协作过滤机制提出了一种模糊信任推荐框架,但是没有考虑到信任演化的问题.文献[11]提出了一种客观信任管理框架,信任值的计算基于节点的直接观察和间接信息,但却忽视了推荐信任.

目前,大多数信任评估模型都是基于推荐评估方法学(观察,推荐,和知识)建立的.所以,评估结果的正确性严重依赖于转发行为检测的准确性和推荐者的诚实度.本文集成节点间信任的搜索、评估、传播和演化,建立了一种适用于环境受限的移动自组网的主观信任路由模型,并由此扩展动态源路由协议(Dynamic Source Routing,DSR).

2.2 信任路由

文献[12]在 DSR 协议中集成了信任和声誉机制实现了一种可靠路由,但是,没有考虑到如何阻止不诚实的推荐.文献[13]设计了一种分布式的信任路由框架,但是该框架依赖于第三方实体的帮助.文献[14]使用消息重发和冗余路由来检测和防御针对路由的攻击,但是在使用的信任模型中却忽略了如何阻止不诚实的推荐.文献[15]提出了一个与本文类似的信任评估方案(Trust-Aware Routing Protocol,TARP),将属性分为六类,源节点可以向直接邻居和间接邻居请求属性信息,并依据自身的信任规则进行匹配从而决定是否信任邻居节点.但是,该方案仅将属性信息简单地用于信任评估,并没有提出节点间的信任度和属性间的相似度概念,也没有将属性信息用于路由决策过程,本质上还是一种基于声誉机制的信任评估方法,并且在发包之前需要一个路由建立过程,增加了延迟.

尽管 AODV(Ad hoc On-Demand Distance Vector)协议较 DSR 协议在正常网络环境下具有较高的效率,但是,在资源受限的移动自组网环境里,AODV 协议的分组到达率下降了 30%,而 DSR 协议只下降了 10%[16],这是因为 DSR 协议具有路由缓存,因此较 AODV 协议具有更快的局部链路恢复过程.

3 问题描述

3.1 信任性定义

分布式网络中的信任概念源于社会科学,信任的一个普遍定义是:对于一个实体在具体环境中的可信、安全和可靠执行能力的坚定信念[17].本文主要考虑行为信任,由于信任是一个实体对于另一个实体行为的一种态度,因此本文认为移动自组网信任性是一个移动节点基于交互历史和属性相似性对于另一个节点未来行为的一种主观期望.

虽然目前基于推荐的信任度计算方法在分布式应用中被广泛采用,但本文提出信任度只与节点行为和属性相似性有关,前者决定着信任度的变化趋势,而后者意味着变化幅度.该信任模型属于主观信任,更适于节点频繁加入和离开的移动自组网环境.本文使用 $\Psi_{AB}(t)$ 表示节点 A 在时刻 t 对节点 B 的信任度,取值范围为(0,1).

3.2 相似性定义

在心理学范围内的一个普遍发现[18]是个体更易于同与自身有相似个性的其他个体交往.目前的很多研究正试图将这种相似吸引关系应用于人机交互中,但据作者所知,将相似性应用于移动自组网路由中的研究还很少.

由于评估相似性的能力与认知能力有关,因此本文考虑移动自组网相似性为一个移动节点基于自身偏好和立场对其他节点拥有的属性的一种主观判断.相似性表明了用户属性间的一种关系,当两个用户以往从未有关交互历史时,这种关系更为重要.相似性的引入适用于大规模动态网络,例如:移动自组网.因此,移动自组网相似性是移动实体间的一种个性评估,评估结果决定着移动实体间的转发行为.

一个具有 m 个属性的节点 A 的属性集合表示为 $\tau_A(a_1,a_2,\cdots,a_m)$.两个具有 m 个属性的节点构成的节点对 (A,B) 表示为 $(\tau_A(a_1,a_2,\cdots,a_m),\tau_B(a_1,a_2,\cdots,a_m))$,对应的属性之间具有一定的相似程度,称为属性相似度,表示为 $\Phi(\tau_A(a_i),\tau_B(a_i))$.本文实验中规定属性相似度的取值范围为(0,1),即 $\Phi(\tau_A(a_i),\tau_B(a_i))\in(0,1)$,其中 $1\leqslant i\leqslant m$.

4 可信传播算法

为表述方便,下文以图 1 为例,通过描述节点 A 如何将数据包路由至目的节点 F,以阐述本文提出的信任传播模型.下面为传播算法的四个基本步骤,每个步骤的具体细节将分别在本节中详细给出.

(1)节点 X 在其邻节点中选择下一跳节点并转发数据包(详见 4.1 小节);

(2)下一跳节点 Y 计算其与上一跳节点 X 之间的属性相似度(详见 4.2 小节);

(3)下一跳节点 Y 依照本文定义的包转发策略决

定是否转发上一跳发来的数据包(详见 4.3 小节);

(4)节点 X 识别下一跳节点 Y 是否正确地将数据包转发给其下游节点 Z(详见 4.4 小节).

4.1　路由路径选择

给定节点 x(源节点或中间转发节点),目的节点为 d,且节点 x 与节点 d 之间存在路径 $R=\{x=x_1,x_2,\cdots,x_{n-1},x_n=d\}$,其中 $n\geqslant 2$,有向边 l 是路径 R 上的一条边,即 $l\in R$,连接边 l 所对应的节点对在时刻 t 的信任度表示为 $\Psi_l(t)$,节点 x 与节点 d 之间的路径集合表示为 $R_{s,d}$,该路径集合中被节点 x 选定为向目的节点 d 发送数据包的路径表示为 R^*,则 R^* 是节点 x 与节点 d 之间的路径集合中具有最大链路平均信任度的路径,以尽量降低转发过程中节点转发失败的概率,即:

$$R^*=\max\left\{\left.\frac{\sum_{l\in R}\Psi_l(t)}{n_R}\right| R\in R_{x,d}\right\} \tag{1}$$

$$\text{s.t.}\quad R^*=\{x=y_1,y_2,\cdots,y_{n-1},y_n=d\} \tag{2}$$

其中,n_R 是路径 R 的长度.从式(1)和(2)中可以看出,本模型中路由路径的选择兼顾了信任度和链路长度二个因素,避免了由于简单的信任度加和算法造成的由过多跳数引发的不适当的最高信任度,同时也克服了单一追求最短距离而导致的不稳定通信链路,在链路可信度之和相同的情况下,跳数最少者被优先选择.

任意节点对之间的初始信任度设为 0.5,表示在没有发生任何合作之前,每个节点对其余节点的信任性保持中立.如图 1 第 1 步所示,每当有数据包要发送时,邻居节点间便进行信任信息交换,并保存在本地的信任度表中,以保证信任信息的实时更新,同时进行路由缓存,因此,仍属于一种按需路由协议.任意中间节点

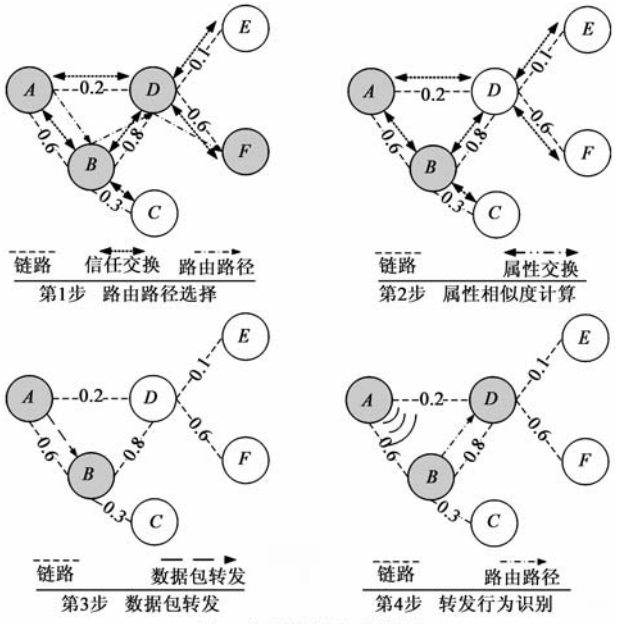

图1　主观信任路由模型

依据自身的信任度表决定下一跳的选择,而不是由源节点选定的节点列表.

4.2　属性相似度计算

为计算方便起见,本文实验中只考虑三个属性(即 $m=3$):瞬时速度 v(赋值为实际速度值)、移动方向 o(赋值为节点在时刻 t 与时刻 $t-1$ 的位置移动向量与 0 度水平线间的顺时针夹角,因此移动方向的取值为[0,360))和隶属组织 m(随机赋值为 0 和 1 两个组织).瞬时速度和移动方向属性值随时间而变,瞬时速度和移动方向相近的移动节点容易在较长的时间里保持通信连通性,而隶属组织属性值是固定不变的,相同或相近的隶属组织更易于相互信任.两个节点 A 和 B 的瞬时速度 v_1 和 v_2 的相似度 $\Phi(\tau_A(v_1),\tau_B(v_2))=0.99-\left|\frac{v_1-v_2}{\max\{v_1,v_2\}}\right|$,移动方向 o_1 和 o_2 的相似度 $\Phi(\tau_A(o_1),\tau_B(o_2))=0.99-\left|\frac{o_1-o_2}{360}\right|$.隶属组织 m_1 和 m_2 的相信度 $\Phi(\tau_A(m_1),\tau_B(m_2))=\begin{cases}0.99, m_1=m_2\\0.01, m_1\neq m_2\end{cases}$.另外不同属性对整体相似性的贡献也不尽相同,例如,瞬时速度的相似性要重要于通信半径的相似性,这可以理解为不同属性对通信可靠性的影响程度不同,每个移动节点在计算整体属性相似度时可以侧重不同的属性.

节点 X 与节点 Y 的整体属性相似度定义为这两个节点所有属性对的相似度的加权平均值,即:

$$\Gamma(X,Y)=\sum_{i=1}^{m}(\omega_i\Phi(\tau_X(a_i),\tau_Y(a_i))) \tag{3}$$

$$\sum_{i=1}^{m}\omega_i=1 \tag{4}$$

其中,$\Gamma(X,Y)$表示节点 X 与节点 Y 之间的整体属性相似度,取值范围为(0,1),m 表示节点属性的个数,a_i 表示第 i 个属性,ω_i 表示第 i 个属性在整体相似度计算中所占的比重,可以根据不同的应用场景需要灵活设置,不失一般性,本文实验中所有属性采用相同的权重,即 $1/m$.

如图 1 第 2 步所示,每当有数据包要发送时,邻居节点间也会进行属性信息的交换,并按式(3)和(4)更新彼此间的属性相似度.该路由模型需要邻居节点之间交互各自的属性信息,表面看来可能会增加路由开销,但较 DSR 协议而言,却不必携带路径中间节点信息,所以增加的开销并不大.

4.3　数据包转发

如图 1 第 3 步所示,根据已经获得的属性相似度信息,节点 Y 将决定是否转发来自其上游节点 X 的数据包.按照移动自组网中的真实情况,节点 Y 是否转发来自节点 X 的数据包应该主要取决于这两个节点间的属

性相似度.设 $\Omega(Y,X)$表示节点 Y 转发来自节点 X 的数据包的概率,则 $\Omega(Y,X)$与这两个节点间的属性相似度成正比,即 $\Omega(Y,X)\propto\Gamma(Y,X)$.由于 $\Gamma(Y,X)\in(0,1)$,为降低计算的复杂度,本文在实验中设置正比例系数为 1,即 $\Omega(Y,X)=\Gamma(Y,X)$.

在该转发机制中,即便是正常节点也会依据属性相似度以一定的概率丢包,该概率随着属性的变化而不断改变,例如,移动速度、剩余能量等.这种设计方案不同于以往移动自组网路由模型中的尽力而为机制,体现了节点的智能转发行为,但是给准确识别邻居节点转发行为带来了一定的麻烦.

4.4 转发行为识别

采用网络层序号识别数据包,节点 X 工作在杂收模式,当节点 X 在超时时间以内检测到节点 Y 发出的数据包 q,节点 X 比对数据包 q 的序号和原始记录的序号是否匹配,而不再比对数据包中的节点列表.如在超时以后,节点 X 仍没有收到节点 Y 发出带有正确序号的数据包,则节点 X 认为节点 Y 此次没有正确转发数据包.(在移动自组网环境中,导致转发失败的原因众多,例如自私节点、不稳定链路、MAC 层冲突等,但以上原因均体现了不同程度的通信不可靠性,不过本文根据相似度的不同对节点失败转发的惩罚力度也不同)

如图 1 第 4 步所示,当节点 X 在时刻 $t-1$ 检测到当前转发节点 Y 没有正确地转发数据包,X 将在时刻 t 减小对节点 Y 的信任度;反之,则增大对节点 Y 的信任度.增大与减小信任度按式(5)计算:

$$\Psi_{XY}(t)=\begin{cases}\Psi_{XY}(t-1)-\Psi_{XY}(t-1)\mathrm{e}^{\frac{\Gamma(X,Y)}{\Gamma(X,Y)-1}}, & \text{dec.}\\ \Psi_{XY}(t-1)+(1-\Psi_{XY}(t-1))\mathrm{e}^{\frac{\Gamma(X,Y)-1}{\Gamma(X,Y)}}, & \text{inc.}\end{cases}\tag{5}$$

其中,$\Gamma(A,B)\in(0,1)$.从式(5)中可以看出,在 $t-1$ 时刻节点 X 对其邻节点 Y 与 Z 有相同的信任度,但节点 X 与节点 Y 之间具有比与节点 Z 之间更高的属性相似度,即 $\Psi_{XY}(t-1)=\Psi_{XZ}(t-1)$,$\Gamma(X,Y)>\Gamma(X,Z)$.若节点 X 检测到节点 Y 与节点 Z 都未正确地转发数据包,则节点 X 对节点 Y 的信任度的减小幅度要小于对节点 Z 的信任度的减小幅度,即 $\Psi_{XY}(t)>\Psi_{XZ}(t)$.信任度增加的情况与之相反,因此,当节点 X 与节点 Y 之间的属性相似度接近于 1 时,信任度的减幅接近于 0,即设 $\Delta\Psi_{XY}(t)=\Psi_{XY}(t)-\Psi_{XY}(t-1)$,则 $\lim\limits_{\Gamma(X,Y)\to1}\Delta\Psi_{XY}(t)=0$;而相似度接近于 0 时,信任度的减幅接近于 100%.当节点间的属性相似度接近于 0 时,信任度的增幅也接近于 0,即 $\lim\limits_{\Gamma(X,Y)\to0}\Delta\Psi_{XY}(t)=0$;而相似度接近于 1 时,信任度增加至接近于 1.

式(5)的设计是源于人类信任关系网中的情形,对自己好朋友偶然犯的一次错误的信任度惩罚力度应低于对一般人犯错误的惩罚力度.例如,若节点 X 和节点 Y 之间的属性相似度为 0.9,则节点 Y 每丢弃一个数据包节点 X 对其信任度的减少量为 0.012%.这样设计的另一个考虑是本文应用场景中节点是完全的自组织工作模式,如 4.3 节所述,当前转发节点是否转发上游节点发来的数据包仅取决于二者的属性相似度,而非预先设定.这样节点应尽可能同与自己属性相似度高的节点合作,以期获得较高的转发成功率,这在未来高度自治移动模式中是合理的.本文也考虑到了由于 MAC 层冲突导致的误判断情况,所以节点之间的信任度越高,意外的失败转发导致信任度降低的程度就越小,二者之间的信任度在后续的评估过程中恢复得也越快,由此尽可能地降低误判带来的影响.

5 实验结果与分析

N 个移动节点被随机放置在 1000m × 400m 的实验区域内,移动节点随机运动且停留时间为 0.关注的模型参数主要有:通信半径(R),移动速度(S)和节点总数(N).每个节点顺序地从其余 $N-1$ 个节点中随机地寻找一个节点作为目的节点产生一次 FTP 通信(分组产生的平均到达间隔符合泊淞分布),每秒钟发送 10 个长度为 512 字节的数据包,N 个节点重复地执行该过程直至模拟时间结束.为每个节点设置一个最高速度和一个最低速度,节点在移动过程中速度保持不变,而到达一个新位置时节点会在最高速度和最低速度之间随机选取一个新速度继续移动.每个场景下实验结果的采样间隔均为 20s.每个实验结果对应 50 次以上模拟结果的平均值.主要关注的性能指标有分组到达率:目的节点收到的来自非恶意节点的数据分组数量与源节点发送的数据分组数量的比值;吞吐量:单位时间内从非恶意节点到达目的节点的数据包量;平均延迟:所有从非恶意节点发出的数据包到达目的节点的时刻与源节点发包时刻之差的平均值;抖动:从非恶意节点发出的相邻数据包的延迟差与相邻数据包的序号差之比.

5.1 黑洞攻击

图 2 给出了原始 DSR 协议、TARP 协议和改进后 DSR 协议在没有恶意节点存在的情况下的性能对比,从中可以看出,在没有恶意节点存在的情况下,DSR 协议在分组达到率和吞度量两项指标上表现最好,TARP 协议次之.这是因为在基于属性相似度的路由模型中,如果邻居节点具有与上游发送节点较低的属性相似度时,会使得邻居节点丢弃其从上游发送节点接收到的数据包,从而导致了较低的分组到达率和吞度量.TARP 协议由于设定了信任阈值会导致部分节点无法发现到达目的节点的有效路由,所以其分组达到率和吞度量

低于 DSR 协议.在抖动和平均延迟两方面,改进后的 DSR 协议最好,原始 DSR 协议次之.这是因为原始 DSR 协议中的路由发现过程需泛洪广播发送路由请求分组,相邻节点路由请求消息可能发生传播冲突并可能产生重复广播,因此从源节点启动路由发现过程到接收到路由回复需要较长的时间,而改进后的 DSR 协议只需根据本地的信任度表进行路由决策即可.TARP 协议中路由请求包的长度被增加,而且节点需较长的时间匹配属性,因此导致了最差的抖动和平均延迟两项指标.

图 3 比较了原始 DSR 协议、TARP 协议和改进后的 DSR 协议当存在 20% 黑洞攻击节点情况下各自的性能,从中可以看出,改进后的 DSR 协议的各项网络性能指标均明显优于原始 DSR 协议,即便是分组到达率和吞吐量两项指标也要好于原始 DSR 协议,说明基于属性相似度的主观信任路由模型能够通过信任度的调整有效地避开恶意节点,选择更加可靠的路径转发数据包,具有较强的抵抗恶意节点破坏的能力.虽然改进的 DSR 协议会主动丢弃属性相似度低的数据包,但 TARP 协议由于设置了信任阈值,会导致无法发现到达目的节点的路由,因此二者具有相近的分组到达率和吞吐量两项指标,但 TARP 协议在抖动和平均延迟两项指标上依然没有好转.

图 4 给出了发起黑洞攻击节点比例对网络性能的影响,可以看出,逐渐增多的恶意节点比例会导致分组到达率和吞吐量指标恶化,而抖动和平均延迟两项指标却反直觉地好转.这是因为计算抖动和平均延迟两项指标时,被恶意节点丢弃的数据包并被不计数,恶意节点在网络中扮演着"黑洞"的角色,只接收和作为源节点主动发包,但不转发包,相当于节点总数变小,使得有效计数包经过的平均跳数减小,导致抖动和平均延迟两项指标呈现反直觉现象.但是,在计算分组到达率和吞吐量指标时,恶意节点也会像普通节点一样接收目的节点是自己的数据包,这种数据包会同样被计数,但需恶意节点转发的数据包却被全部丢弃,从而较高的恶意节点比例导致了较低的分组到达率和吞吐量.

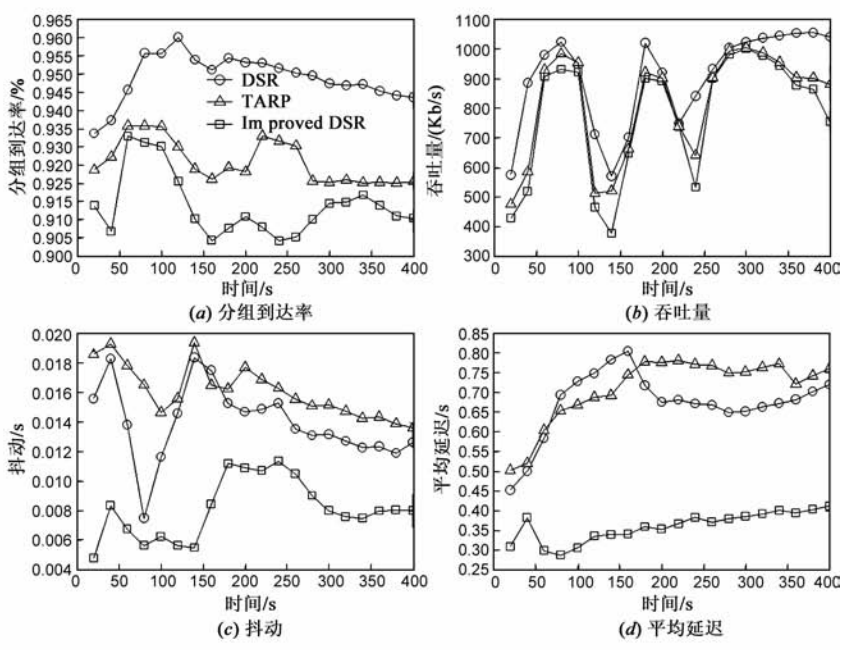

图2　原始DSR协议、TARP协议和改进后DSR协议在没有恶意节点的情况下的性能对比, 参数为R=250m,S=5m/s,N=20

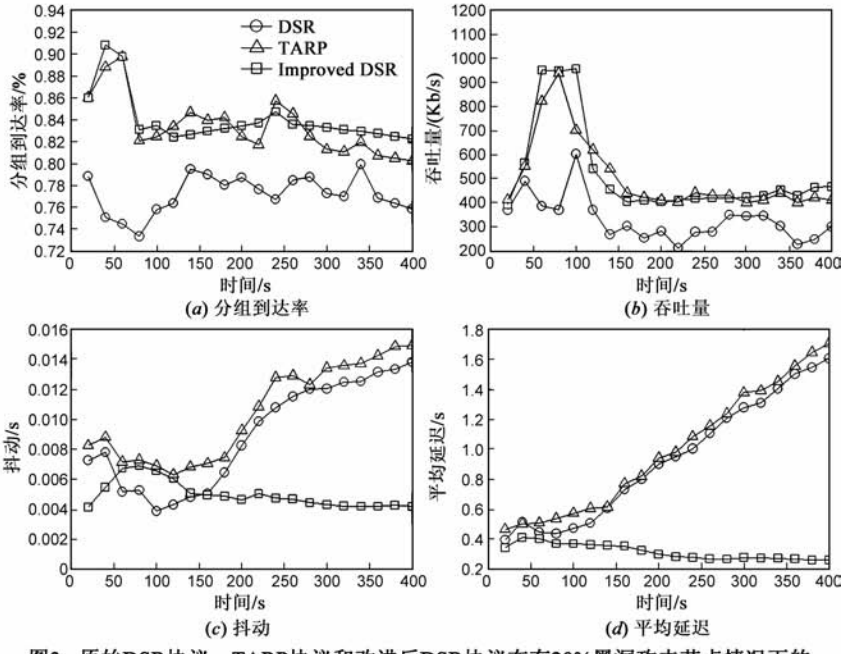

图3　原始DSR协议、TARP协议和改进后DSR协议在有20%黑洞攻击节点情况下的性能对比, 参数为R=250m, S=5m/s, N=20

5.2　行为改变攻击

一个恶意节点能够在转包与丢包行为间持续变化,从而达到破坏网络且不被发现的目的.本文假定攻击者在 t_{on}时间内正常转发包,在 t_{off}时间内丢包.不失一般性,t_{on}和 t_{off}均被设置等于采样间隔时间 20s,发起行为改变攻击的恶意节点数目固定在 20%.图 5 给出了原始 DSR 协议、TARP 协议和改进后的 DSR 协议在该攻击下的性能比较.类似于图3中的结论,改进后的

DSR 协议比原始 DSR 协议具有更强的抵御行为改变攻击的能力,同时,与 TARP协议具有近似的分组到达率和吞吐量两项指标,但在抖动和延迟两项指标上均优于 TARP 协议.所有曲线均展示出与行为转变间隔相一致的波动周期,但改进后的 DSR 协议和 TARP 协议对这种行为交替反应得更缓和.

5.3 诽谤攻击

在基于推荐的信任系统中,信任性可以通过直接观察和间接观察建立.直接观察是一种主观行为,类似于本文中的转发行为识别,间接观察(即:推荐)源于第三方报告.但是,这种信任性常常受困于诽谤和共谋攻击.诽谤者发送虚假的推荐报告去诋毁其他正常节点的信任性,而且,若干个恶意节点可以共同发起共谋攻击而达到成功攻击的目的.这些攻击将降低甚至摧毁一个分布式网络的性能.为评估本文方案和基于推荐信任性方案的健壮性,本文随机设定一些节点为诽谤节点,他们会发送虚假推荐说节点 A 有降低的信任级别.本文采用的基于推荐的信任系统的详情可以在文献[19]中找到.图 6 展现了不同诽谤者数目下节点 B 对节点 A 的信任级别的评估结果.从中可以看出,随着诽谤者比例的升高,基于推荐的信任系统对被攻击对象信任级别的评估结果急剧偏离,但基于相似性的信任系统工作正常,并不受诽谤攻击的影响,图中基于相似性的信任系统的评估值与实际值的微小误差是由于在转发行为识别中的误判引发的.

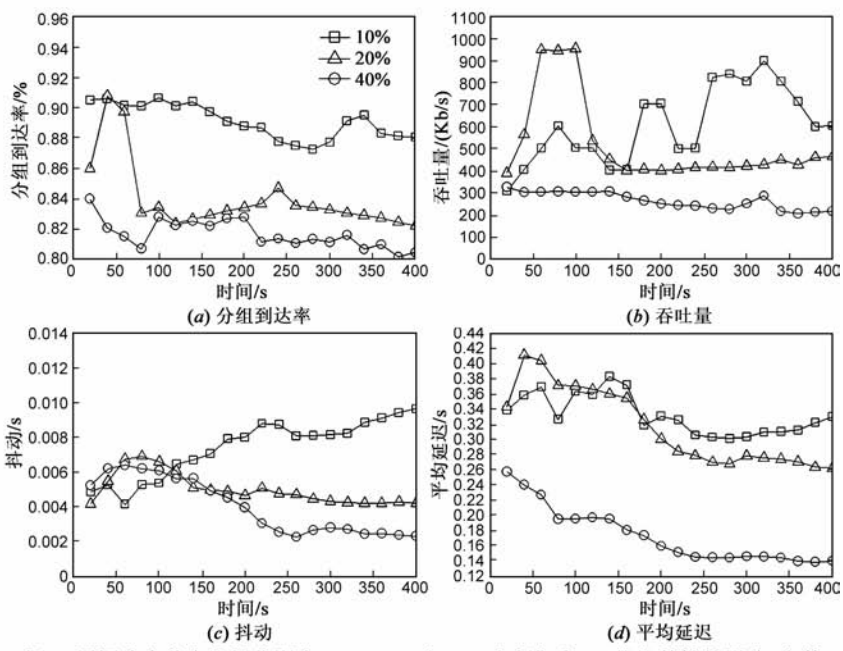

图4 黑洞攻击节点比例分别为10%、20%和40%对改进后DSR协议的性能影响,参数为R=250m, S=5m/s, N=20

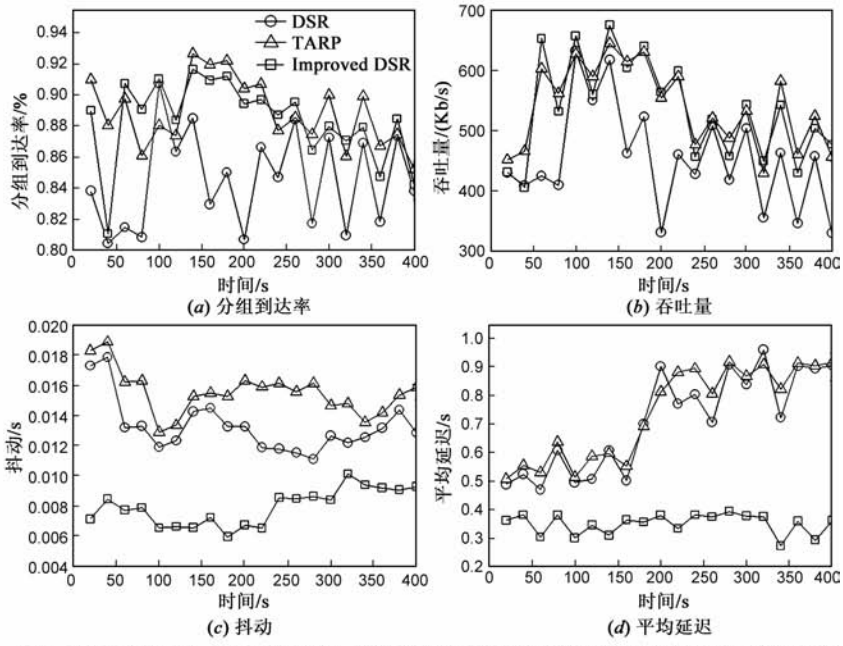

图5 原始DSR协议、TARP协议和改进后DSR协议在有20%行为改变攻击节点情况下的性能对比,参数为R=250m, S=5m/s, N=20

6 结论

在过去的几年中,很多关于移动自组网的应用研究都把信任路由作为基础,而信任传播是移动自组网中亟待解决的问题之一.本文引入属性相似度的概念,提出了一种新的信任传播模型,并定义了贴近实际情况的数据包转发规则.仿真结果表明该模型较传统的 DSR 协议和以往的信任路由协议能更好地抵御恶意节点的存在,具有较高的网络性能指标,在转发数据包时能有效地选择具有高可靠性的路由路径.

移动自组网较有线网络具有许多不同的特性,例如,易变的拓扑关系、移动的节点位置、有限的能量等,使得通常的有线网信任传播算法并不适用于移动自组网.本文提出的模型可使得具有相近特征的节点形成暂时的合作伙伴,能够更高效、更安全、更连通地协同工作.例如,瞬时速度和移动方向属性相近的节点可保证路由通道短时间内的可靠连通,减小易变的拓扑结构对数据包路由带来的影响;周围通信环境相同的节点更易于获得稳定的通信链路.

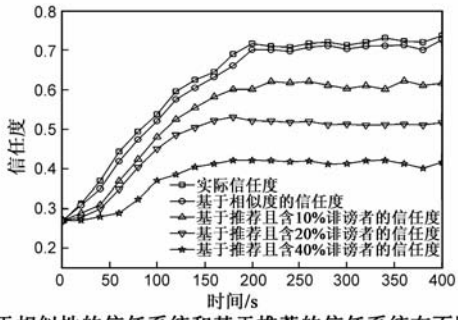

图6　基于相似性的信任系统和基于推荐的信任系统在不同诽谤者比例下的信任度评估结果,参数为R=250m, S=5m/s, N=20

参考文献

[1] Ramana K S, Chari A A, et al. Trust based security routing in mobile adhoc networks[J]. International Journal on Computer Science and Engineering, 2010, 2(2): 259 – 263.

[2] 王晓东,霍广城,等.移动自组网中基于部分网络编码的机会主义路由[J].电子学报,2010,38(8):1736 – 1740.
WANG X D, HUO G C, et al. An opportunistic routing for MANET based on partial network coding[J]. Acta Electronica Sinica, 2010, 38(8): 1736 – 1740. (in Chinese)

[3] 王国栋,王钢.MANET 中一种具有能量意识的无信标地理路由算法[J].电子学报,2010,38(7):1547 – 1551.
WANG G D, WANG G. An energy-aware and beaconless geographic routing for mobile ad hoc network[J]. Acta Electronica Sinica, 2010, 38(7): 1547 – 1551. (in Chinese)

[4] RAYA M, HUBAUX J-P. Securing vehicular ad hoc networks [J]. Journal of Computer Security, 2007, 15(1): 39 – 68.

[5] ADIBI S, AGNEW G B. Multilayer flavoured dynamic source routing in mobile ad-hoc networks[J]. IET Communications, 2008, 2(5): 690 – 707.

[6] JOHNSON D, MALTZ D. Mobile Computing[M]. Germany: Kluwer Academic Publishers, 1996. 153 – 181.

[7] IETF RFC 3561, Ad-hoc On-demand Distance Vector (AODV) Routing[S]. July 2003.

[8] Anantvalee T, Wu J. Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks[A]. IEEE International Conference on the Communications [C]. New York: IEEE Press, 2007. 3383 – 3388.

[9] Peng S C, Jia W J, et al. Voting-based clustering algorithm with subjective trust and stability in mobile ad-hoc networks[A]. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing[C]. Washington, DC: IEEE Computer Society, 2008. 3 – 9.

[10] Luo J, Liu X, et al. Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks [A]. IEEE Conference on Local Computer Networks [C]. Washington, DC: IEEE Computer Society, 2008. 305 – 311.

[11] Li J, Li R, et al. Future trust management framework for mobile ad hoc networks[J]. IEEE Communications Magazine, 2008, 46(4): 108 – 114.

[12] Pirzada A A, Datta A, et al, Incorporating trust and reputation in the DSR protocol for dependable routing [J]. Computer Communications, 2006, 29(15): 2806 – 2821.

[13] Chen T, Mehani O, et al. Trusted Routing for VANET[A]. International Conference on Intelligent Transport Systems Telecommunications[C]. Washington, DC: IEEE Press, 2009. 647 – 652.

[14] Yu M, Leung K K. A trustworthiness-based QoS routing protocol for wireless ad hoc networks[J]. IEEE Transactions on Wireless Communications, 2009, 8(4): 1888 – 1898.

[15] Abusalah L, Khokhar A, et al. Trust aware routing in mobile ad hoc networks[A]. Global Telecommunications Conference [C]. Washington, DC: IEEE Press, 2006.

[16] Choudhury S, Roy SD, et al. Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics[M]. Netherlands: Springer, 2008. 496 – 500.

[17] Luo J, Ni X, et al, A trust degree based access control in grid environments[J]. Information Science, 2009, 179(15): 2618 – 2628.

[18] Byrne D, Griffitt W, et al. Attraction and similarity of personality characteristics[J]. Journal of Personality and Social Psychology, 1967, 5(1): 82 – 90.

[19] MUNDINGER J, LE BOUDEC J-Y. Analysis of a reputation system for mobile ad-Hoc networks with liars[J]. Performance Evaluation, 2008, 65(3 – 4): 212 – 226.

作者简介

王　健　男,1981 年 3 月出生于黑龙江省加格达奇市.现为吉林大学计算机科学与技术学院讲师.在国内外发表学术论文 30 余篇.
E-mail: wangjian591@gmail.com

刘衍珩(通信作者)　男,1958 年 2 月出生于吉林省松原市.博士.现为吉林大学计算机科学与技术学院教授、博士生导师,从事移动网络、下一代网络、车联网的研究工作.
E-mail: yhliu@jlu.edu.cn

张　婧　女,1986 年 12 月出生于吉林省松原市.硕士研究生.主要研究方向为移动自组网.　E-mail: tiger-habit@163.com

刘雪莲　女,1984 年 12 月出生于吉林省长春市.硕士研究生.主要研究方向为信任管理.　E-mail: zuiaihonglou@gmail.com