WMNs中基于节点可信度的机会路由改进算法

印新棋 吴 军 莫伟伟 白光伟

(南京工业大学计算机科学与技术学院 南京 211816)

摘 要 机会路由提高了WMNs的可靠性和吞吐量,但同时由于节点候选集中存在恶意节点,导致网络性能下降。对于如何及时识别、隔离网络中的恶意节点的问题,建立了一种节点可信度评估模型。基于贝叶斯网络算法,考虑到非恶意因素带来的网络异常行为,引入不确定交互因子,改进了直接信任的评估方法,利用熵为信任值的计算和更新分配权重。引入反映节点真实参与度的行为积极因子并结合信任值得出节点的可信度,对可信度处于待定状态的节点进行未来可信度的预测,以甄别潜在的恶意节点。最后将该模型应用于机会路由ExOR中,提出了一种基于节点可信度的机会路由算法BTOR。实验结果表明,该算法可以有效检测恶意节点,在各项性能指标上比原路由算法更具优势。

关键词 WMNs,机会路由,节点可信度,行为积极因子,可信度预测

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.08.027

Improved Opportunistic Routing Algorithm Based on Node Trustworthiness for WMNs

YIN Xin-qi WU Jun MO Wei-wei BAI Guang-wei

(College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China)

Abstract Opportunistic routing improves the reliability and throughput of WMNs, at the same time, the network performance degrades due to the existence of malicious nodes in candidate set. In order to solve the problem that how to timely identify and isolate malicious nodes, a node trustworthiness evaluation model was proposed. Based on Bayesian Networks Algorithm, considering the abnormal behavior caused by non-invasive factors, the uncertainty interaction factor is introduced to improve the estimate method of direct trust, and entropy is used to assign weights for calculation and update of trust value. The trustworthiness of the node is obtained by combining the trust value and the positive factor of behavior which is introduced to reflect the real participation of nodes, and the future trustworthiness for those nodes whose trustworthiness is uncertain is predicted to identify potential malicious nodes. Finally, the model was applied to ExOR and an opportunistic routing algorithm based on trustworthiness BTOR was proposed. The experimental results show that the algorithm can effectively detect the malicious nodes, and has advantages than original routing algorithms in performances.

Keywords WMNs, Opportunistic routing, Node trustworthiness, Behavior positive factor, Trustworthiness prediction

1 引言

无线Mesh网络(Wireless Mesh Network,WMNs)由Ad hoc网络发展而来,具有自配置、自治愈、高带宽、结构灵活等优点[1],然而网络本身的开放性和结构的灵活导致的不稳定性给无线Mesh网络路由节点的安全性以及网络的可靠性带来了威胁[2]。但是鉴于无线信道具有广播特性这一独特性质,机会路由(Opportunistic Routing)[3]的设计利用了无线信道的广播特性,很大程度地提高了无线网络的传输可靠性和端到端的吞吐量。但无线Mesh网络中存在的路由安全问题仍然没有得到解决,过去主要采用非对称密码机制来解决这一类问题,但是这种方法不能解决路由内部具有合法身份的节点发起的恶意攻击行为,例如恶意节点伪造信息加入机会路由候选转发节点集。因此,解决机会路由内部的安全问题已变得至关重要。目前,解决路由内部安全问题的一个行之有效的方法是对路由节点进行信任评估,建立信任模型,以有效识别恶意节点,增强网络的安全性和鲁棒性。

本文第2节介绍了相关工作;第3节详细阐述了建立的节点可信度评估模型的计算方案;第4节介绍了加入可信度模型的机会路由算法BTOR;第5节给出了实验仿真,并分析了实验结果;最后总结全文。

2 相关工作

2.1 机会路由

对机会路由的研究工作主要从以下3个方面进行:1)候选转发节点集的选择;2)候选转发集中各个节点优先级的确

到稿日期:2016-10-17 返修日期:2017-01-17 本文受国家自然科学基金项目(60673185,61073197)资助。

印新棋(1992-),男,硕士生,主要研究方向为机会路由、网络安全,E-mail:18795877698@163.com;吴 军(1962-),男,硕士,高级工程师,硕士生导师,CCF会员,主要研究方向为网络安全、可信计算、信息系统安全等;莫伟伟(1991-),男,硕士生,主要研究方向为可信计算、机会路由;白光伟(1961-),男,博士,教授,博士生导师,CCF高级会员,主要研究方向为无线传感网络等。

定;3)不同节点之间为避免重复发送数据包的高效协调机制的研究。文献[4]回顾了近年来一些重要的机会路由协议,并对这些协议进行了分类和性能对比。机会路由的概念最初由MIT的Biswas等人提出[3],他们介绍了经典的机会路由协议ExOR,ExOR使用期望传输次数ETX作为路由测度,比较数据包发送节点及其邻居节点到目的节点的ETX值,若邻居节点的ETX值小于发送节点,则进入候选转发集,并依据ETX设置优先级。路由测度的选择多种多样,有的机会路由使用网络拓扑和地理信息作为路由测度,例如DPOR[5],DPOR结合邻居节点的地理信息和链路质量来选择候选转发节点集并确定节点优先级。文献[6]对机会路由进行建模和分析,提出一个马尔科夫链模型作为通用机会路由模型,能被用于任何的网络拓扑结构和任意的候选集选择算法。文献[7]提出了一种计算候选集节点数量的算法D-MACE,通过源节点与目的节点的距离确定每个源节点的候选转发集的数量,但不涉及具体的转发测度。文献[8]提出了一种新的机会路由协议JOKER,在候选节点集选择算法和节点协调转发阶段都做了新的创新,结合链路的投递率和候选节点到目的节点之间的距离作为新的路由测度,在接收到包的候选节点集中采用ack机制和定时机制来完成协调转发的工作。文献[9]把网络编码策略使用到机会路由中,有效减少了网络中重复分组的传递次数,很大程度地提高了分组投递率,进而提高了吞吐量。

2.2 信任模型

国内外研究人员基于信任模型对路由的研究情况如下。文献[10]回顾了一些最新的无线通信中的信任管理系统,并对使用的方法进行了分类和工作机制的阐述。文献[11]提出了一种基于模糊理论的分布式信任管理系统,利用模糊理论计算节点的信任值,但模糊理论的应用可能会导致信息的丢失。文献[12]提出了一种多维信任模型RMTM,根据节点的攻击情况将节点的攻击证据划分为多个维度,但是该模型较复杂,可操作性不强。文献[13]把基于主观逻辑思想的观点(opinion)作为节点间信任关系的信任模型并延伸到经典的AODV路由协议中,提出了TAODV路由协议,虽然TAODV路由协议在检测恶意节点方面能起到不错的效果,但其主观性较强,会对检测结果产生一定的不利影响。文献[14]首次将信任模型应用到机会路由中,信任值的计算基于直接交互的直接信任度和信任相似的推荐信任度,但是在直接信任度的计算中较多参数的取值依赖于专家经验,这会对信任模型的客观性造成一定影响。文献[15]基于贝叶斯理论进行信任评估,根据节点信任值服从Beta分布的性质计算信任值,但是该方法未考虑到失败交互中可能存在非恶意因素(如网络本身的不稳定)带来的数据包的丢失引起的网络异常行为。文献[16]也将信任模型结合到机会路由中,利用一种新的看门狗机制检测节点信息,将节点的链路投递率、节点的地理信息以及节点信任值整合作为路由测度,在优化候选集的同时势必会带来更多的网络开销,而且信任值的计算没有考虑推荐信息,这会影响信任值的完整性和准确性。

针对上述问题,本文在对信任模型进行研究的基础上提出一种节点可信度评估模型,考虑到非入侵因素,即网络自身的异常带来的误检率对行为信任值计算的影响,通过将交互行为分成成功交互、失败交互以及不确定交互,对信任值的计算进行改进,并通过熵给各个信任值分配权重,弥补了主观赋予权重的不足,并结合反映节点真实参与度、防止自私行为的行为积极因子得到节点可信度,且对可信度进行区间划分,对可信度处于不确定区间的节点进行未来可信度的预测,以识别出潜在的恶意节点;最后将该模型结合到机会路由ExOR中,提出了一种基于节点可信度的机会路由算法BTOR(Trustworthiness-Based Opportunistic Routing)。需要说明的是,本文的研究基于相对稳定的骨干网Mesh结构中的路由节点。

3 节点可信度评估模型

本文提出的节点可信度不仅包含了节点的信任值 T_{ij},还考虑了节点的真实参与度,引入行为积极因子 PF_{ij},结合节点信任值和行为积极因子得到节点可信度 TW_{ij}。

3.1 节点信任值评估

路由节点信任值 T_{ij} 是评估节点对被评估节点的信任程度的量化,信任值包括直接信任 T_{ij}^{d} 和推荐信任 T_{ij}^{ind}。

3.1.1 直接信任评估方法

定义1(直接信任值) 直接信任值是指节点 i 与邻居节点 j 在时间周期内根据直接交互行为信息所计算出的直接信任水平。

路由节点的信誉服从Beta分布[17],即:

$$rep_{ij} \sim Beta(\alpha+1,\beta+1)$$

其中,α_{ij} 和 β_{ij} 分别表示节点 i 与节点 j 在过去一个周期时间内交互的成功次数和失败次数,节点 i 对节点 j 的直接信任 T_{ij}^{d} 可以用信誉分布的统计期望表示:

$$T_{ij}^{d}=E(Beta(\alpha,\beta))=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \tag{1}$$

3.1.2 直接信任计算方案的改进

实际上,α_{ij} 和 β_{ij} 并不能准确地反映出真正的节点交互行为,因为基于Beta分布的直接信任值评估模型忽略了在失败交互中存在非恶意交互行为的情况,例如由于链路的丢失特性带来的数据包的丢失,这些网络本身的因素会带来较大的误检率。为解决该问题,本文将节点 i 与节点 j 之间的交互分为成功交互、失败交互和不确定交互,引入不确定交互因子 U_{ij},改进了直接信任值的计算方案,U_{ij} 表示节点交互中由于非恶意因素导致交互失败的概率,依据D-S证据理论[18]给出了不确定交互因子的量化表示,并且在引入不确定交互因子后,计算了节点间成功交互的概率 S_{ij} 和节点间由于恶意因素导致失败交互的概率 F_{ij},计算公式如下:

$$S_{ij}=\frac{\alpha_{ij}}{\alpha_{ij}+\beta_{ij}}\times(1-U_{ij}) \tag{2}$$

$$F_{ij}=\frac{\beta_{ij}}{\alpha_{ij}+\beta_{ij}}\times(1-U_{ij}) \tag{3}$$

$$U_{ij}=\frac{12\times\alpha_{ij}\times\beta_{ij}}{(\alpha_{ij}+\beta_{ij})^2\times(1+\alpha_{ij}+\beta_{ij})} \tag{4}$$

其中,$S_{ij}+F_{ij}+U_{ij}=1$,因此直接信任值可以修改为:

$$T_{ij}^{d}=S_{ij}+\theta\times U_{ij} \tag{5}$$

其中,θ 是不确定交互中实际成功交互的占比,θ 值随应用场景变化而变化,θ 初始化为0.5。

3.1.3　推荐信任评估方法

定义 2(推荐信任值)　推荐信任值是指节点 i 与 j 共有的邻居节点集 $N(k)$ 所推荐的直接信任值，通过综合公共节点的推荐信息，能够更可靠、真实、准确地反映出推荐的信任水平。

推荐信任值 T_{ij}^{ind} 的计算公式为：

$$T_{ij}^{ind}=\frac{\sum_{k\in N(k)} T_{ik}^{d}\times T_{kj}^{d}}{\sum_{k\in N(k)} T_{ik}^{d}} \tag{6}$$

3.1.4　综合信任值的计算

定义 3(综合信任值)　将节点之间的直接信任值和推荐信任值进行有机融合而得到的信任值就是综合信任值。

为避免主观分配权重的局限性，增强信任模型的自适应性。本文使用信息熵来进行权值分配，信息熵反映了多个评价指标对于待评价事务的影响程度，即各指标在评价过程中提供有效信息的多寡程度，因此可以使用信息熵来度量各指标信息的有效程度并据此分别确定其相应的权重，综合信任值的计算公式如下：

$$T_{ij}=\omega_{ij}^{d}\times T_{ij}^{d}+\omega_{ij}^{ind}\times T_{ij}^{ind} \tag{7}$$

其中，ω_{ij}^{d} 和 ω_{ij}^{ind} 分别为直接信任值和推荐信任值的自适应权重，$H(T_{ij}^{d})$ 和 $H(T_{ij}^{ind})$ 分别为直接信任值和推荐信任值的信息熵[19]，计算公式如下：

$$H(T_{ij}^{d})=-T_{ij}^{d}\log_2 T_{ij}^{d}-(1-T_{ij}^{d})\log_2(1-T_{ij}^{d}) \tag{8}$$

$$H(T_{ij}^{ind})=-T_{ij}^{ind}\log_2 T_{ij}^{ind}-(1-T_{ij}^{ind})\log_2(1-T_{ij}^{ind}) \tag{9}$$

$$\omega_{ij}^{d}=\frac{1-\frac{H(T_{ij}^{d})}{\log_2 T_{ij}^{d}}}{[1-\frac{H(T_{ij}^{d})}{\log_2 T_{ij}^{d}}]+[1-\frac{H(T_{ij}^{ind})}{\log_2 T_{ij}^{ind}}]} \tag{10}$$

$$\omega_{ij}^{ind}=\frac{1-\frac{H(T_{ij}^{ind})}{\log_2 T_{ij}^{ind}}}{[1-\frac{H(T_{ij}^{d})}{\log_2 T_{ij}^{d}}]+[1-\frac{H(T_{ij}^{ind})}{\log_2 T_{ij}^{ind}}]} \tag{11}$$

3.1.5　综合信任值的更新

综合信任值随时间周期 Δt 动态变化，综合信任值的更新取决于最近一个周期的综合信任值 T_{ij}^{new} 和历史信任值 T_{ij}^{old}。但是若给历史信任值较高的权值，则不能充分体现最近一个周期的信任值的变化；若给最近一个周期的信任值较高的权值，则有可能给一些恶意节点短期快速提升信任值的机会。因此使用熵进行权值分配，综合信任值的更新计算表达式为：

$$T_{ij}=\omega_{new}\times T_{ij}^{new}+\tau\times\omega_{old}\times T_{ij}^{old} \tag{12}$$

其中，τ 是时间衰减因子，信息熵和权重的计算公式如下：

$$H(T_{ij}^{new})=-T_{ij}^{new}\log_2 T_{ij}^{new}-(1-T_{ij}^{new})\log_2(1-T_{ij}^{new}) \tag{13}$$

$$H(T_{ij}^{old})=-T_{ij}^{old}\log_2 T_{ij}^{old}-(1-T_{ij}^{old})\log_2(1-T_{ij}^{old}) \tag{14}$$

$$\omega_{new}=\frac{1-\frac{H(T_{ij}^{new})}{\log_2 T_{ij}^{new}}}{[1-\frac{H(T_{ij}^{new})}{\log_2 T_{ij}^{new}}]+[1-\frac{H(T_{ij}^{old})}{\log_2 T_{ij}^{old}}]} \tag{15}$$

$$\omega_{old}=\frac{1-\frac{H(T_{ij}^{old})}{\log_2 T_{ij}^{old}}}{[1-\frac{H(T_{ij}^{new})}{\log_2 T_{ij}^{new}}]+[1-\frac{H(T_{ij}^{old})}{\log_2 T_{ij}^{old}}]} \tag{16}$$

3.2　节点行为积极因子

引入行为积极因子 PF_{ij} 不仅能够反映节点参与转发行为的积极性和真实参与度，而且能够有效遏制自私节点为自身利益只转发较小的数据包而丢弃较大数据包的问题，PF_{ij} 的计算公式如下：

$$PF_{ij}=\frac{t_{success}}{t_{success}+t_{fail}} \tag{17}$$

其中，$t_{success}$ 表示节点成功转发的包的总字节数，t_{fail} 表示未成功转发的包的总字节数，PF_{ij} 每周期更新一次。

3.3　节点可信度计算

节点可信度 TW_{ij} 反映的是节点行为的可信程度，主要由两部分组成：1)节点历史信任值；2)节点参与转发数据的行为积极程度，因此节点可信度的计算公式如下：

$$TW_{ij}=T_{ij}\times PF_{ij} \tag{18}$$

3.4　可信度的分类

根据计算得到的节点可信度的值，对可信度进行分类。

(1)若 $0\leqslant TW_{ij}<\gamma$，则表明节点很可能是恶意节点，其不能进入候选转发节点集。

(2)若 $\gamma\leqslant TW_{ij}<\delta$，则表明节点的可信度处于一般可信状态，是一种不确定的状态，很难根据这些节点的可信度判断其是否值得相信，其中包含潜在的恶意节点，因此设节点为“待定状态”。

(3)若 $\delta\leqslant TW_{ij}\leqslant 1$，则表明节点的可信度处于高可信状态，因为这些节点的可信度已经足够高并且为节约网络能耗，所以这些节点可以直接进入候选转发集。

其中，γ 为一般可信阈值，δ 为高可信阈值。在 NS2[20] 上进行模拟实验，设置区域大小为 1000m×1000m，节点个数为 100，恶意节点个数随机设置为 1～40 之间，每周期记录节点可信度。经过大量的实验表明，当节点可信度不低于 0.8 时，这些节点在未来的周期内几乎不会发生恶意攻击行为；而当节点可信度低于 0.5 时，这些节点会密集地表现出恶意攻击行为。因此，设置 γ 的取值范围为 $0.5\leqslant\gamma<\delta$，$\delta$ 的取值范围为 $0.8\leqslant\delta\leqslant 1$。对于可信度处于待定状态的节点，由于很难判断其历史可信度是否可信，它们有可能是潜在的恶意节点，因此科学地预测节点未来可信度是非常有必要的。本文使用一种路由节点行为预测算法对处于待定状态的节点进行未来行为可信度的预测，并结合当前行为可信度，最终判定待定状态的节点是否可以进入候选转发集。

3.5　待定节点未来可信度的预测

本文使用了一种路由节点行为预测算法，该预测算法是在灰色预测模型的基础上通过节点历史可信度波动类型的交替规律进行可信度的预测，其优点有：在小样本状态下(样本数量不少于 4 个)即可实施预测，其无样本分布要求、不依赖专家经验，在样本数据值波动较大的情况下也能有较高的预测精度。

该算法定义了两种波动类型，即迁移波动和突发波动，设节点过去每个周期的可信度序列为：$TW(TW_{ij}(1),TW_{ij}(2),\cdots,TW_{ij}(n))$，其中，$TW_{ij}(m)$ 是第 m 周期的可信度，可信度级比

序列为$\sigma(\sigma_1,\sigma_2,\cdots,\sigma_{n-1})$，$\sigma$为节点相邻可信度比值集合，基于一个分组标准：$|TW_{ij}^{k+1}(1)/TW_{ij}^{k}(m)-\min(\sigma_i)|>\mu$，其中$\mu$的取值为：$\mu=\frac{1}{m}\sum_{i=1}^{m}|\sigma_i-\min(\sigma)|$且$1\leqslant i\leqslant m$。将节点历史可信度分成一个个组，用$TW_{ij}^{k}$来表示，其中$TW_{ij}^{k}$包含$m$个可信度，将$TW_{ij}^{k+1}(1)$称作相对于分组$TW_{ij}^{k}$的波动值，并且得到波动值序列$F(TW_{ij}^{1}(1),TW_{ij}^{2}(1),\cdots,TW_{ij}^{k}(1))$，然后对每个组进行波动类型的确定：计算波动值$TW_{ij}^{m}(1)$与$TW_{ij}^{m+1}(1)$之间的可信度的个数$Num$(包括$TW_{ij}^{m}(1)$)，由文献[21]可知，如果$Num\geqslant 3$，则$TW_{ij}^{m}$组属于迁移波动，否则$TW_{ij}^{m}$组属于突发波动。特别地，若可信度序列的最后一个数据$TW_{ij}(n)$是波动值，由于缺乏后继数据，因此需要对$TW_{ij}(n)$的波动类型进行预测。考虑到 Markov 模型可以根据状态之间的转移概率来推测未来的状态，利用分组波动类型的转移概率矩阵和前一个分组的波动类型来识别当前分组的波动类型。

根据当前周期节点可信度所属的波动类型进行下一周期可信度的预测：1)若当前可信度$TW_{ij}(n)$属于突发波动，则下一周期的可信度$TW_{ij}(n+1)$和$TW_{ij}(n)$存在较大差异，预测表达为$TW_{ij}(n+1)=GreyPred(Smooth(TW))$，其中灰色预测$GreyPred()$见灰色预测模型[22]，$Smooth(TW)$是一个平滑函数，用于防止序列中突然出现较大波动而影响预测结果，采用移动平均法：$TW_{ij}^{smth}(m)=\frac{1}{n-m+1}\sum_{k=m}^{n}TW_{ij}(k)$，且$m=1,2,\cdots m$；2)若当前可信度$TW_{ij}(n)$属于平滑波动或者是非波动值，则下一周期的可信度$TW_{ij}(n+1)$随着$TW_{ij}(n)$平稳变化，$TW_{ij}(n+1)$的表达式为$TW_{ij}(n+1)=TW_{ij}(n)\times PredSR(TW,F)$，其中$PredSR()$是平滑级比序列预测算法，算法的具体实现见文献[21]。

3.6 待定节点可信度的确定

综合当前可信度$TW_{ij}(n)$和预测可信度$TW_{ij}(n+1)$，使用信息熵给其分配权重，得到待定节点最终的可信度为：

$$TW_{ij}(final)=\omega_n\times TW_{ij}(n)+\omega_{n+1}\times TW_{ij}(n+1) \quad (19)$$

其中，ω_n和ω_{n+1}表示当前可信度和预测可信度的自适应权重，计算公式如下：

$$\omega_n=\frac{1-\frac{H(TW_{ij}(n))}{\log_2 TW_{ij}(n)}}{[1-\frac{H(TW_{ij}(n))}{\log_2 TW_{ij}(n)}]+[1-\frac{H(TW_{ij}(n+1))}{\log_2 TW_{ij}(n+1)}]} \quad (20)$$

$$\omega_{n+1}=\frac{1-\frac{H(TW_{ij}(n+1))}{\log_2 TW_{ij}(n+1)}}{[1-\frac{H(TW_{ij}(n))}{\log_2 TW_{ij}(n)}]+[1-\frac{H(TW_{ij}(n+1))}{\log_2 TW_{ij}(n+1)}]} \quad (21)$$

对于最终确定了可信度$TW_{ij}(final)$的节点，若其可信度不低于高可信阈值，则直接进入候选转发集，否则不能进入候选集。

4 BTOR 路由算法

本文将节点可信度评估模型结合到机会路由 ExOR 中，通过提出的可信度评估模型对恶意节点进行识别，将恶意节点隔离在候选节点集之外，帮助源节点确定安全可靠的候选转发集。BTOR 路由算法的基本思想为：首先根据各个节点到目的节点的 ETX 值进行初始化候选集的选择，如果邻居节点到目的节点的 ETX 值小于源节点到目的节点的 ETX 值，那么该邻居节点进入初始化候选集；然后利用本文提出的节点可信度评估模型计算初始化候选集中每个节点的可信度，在对可信度进行评估的基础上研究判断当前及潜在的恶意节点并获得最终的候选转发集，再利用 ETX 值对节点集中的节点进行优先级的分配；最后根据 ExOR 的协调转发机制进行数据包的转发。具体算法如算法 1 所示。

算法 1 基于节点可信度的机会路由算法(BTOR)

输入：发送节点到目的节点的 ETX(s,d)，发送节点的所有邻居节点到目的节点的 ETX(j,d)，式(2)－式(21)

输出：发送节点的下一跳候选转发集 CandSet(s,d)

```
Begin
1. CandSet(s,d)←Ø
2. If s==d then
3.    Return
4. End if
5. IniCandSet(s,d)←Ø
6. For all j∈NeighborSet(s) do
7.    If ETX(j,d)<ETX(s,d) then
8. IniCandSet(s,d)←IniCandSet(s,d)∪{j}
9.    End if
10. End for
11. For all j∈IniCandSet(s,d) do
      //计算信任值和行为积极因子
12.   Calculating T_sj^d, T_sj^ind, T_sj and PF_sj within Δt according to formula
      (5)－(7) and (17)
      //更新信任值
13.   Updating T_sj according to formula (12)
      //计算可信度
14. Calculating TW_sj using T_sj and PF_sj by formula (18)
      //对可信度进行区域划分
15.    If (0≤TW_sj<γ) then
16.       Node j can't enter the CandSet(s,d)
17.    Else If(δ≤TW_sj≤1) then
18.       CandSet(s,d)←CandSet(s,d)∪{j}
19.    Else
20.     Setting uncertainty--state for node j
21.     For all j∈uncertainty-state do
22.     Predict the next period TW_sj(n+1)by a routing node beha
        vior prediction algorithm
23.     Calculate the final TW_sj(final)by formula (19)
24.     If(TW_sj(final)≥δ) then
25.     CandSet(s,d)←CandSet(s,d)∪{j}
26.   Else
27.      Node j can't enter the CandSet(s,d)
28.    End for
29. End for
30. Sort CandSet(s,d) by ETX from j to d
31. Return CandSet(s,d)
End
```

5　仿真与分析

5.1　仿真实验参数设置

为了检验本文提出的可信度评估模型和 BTOR 路由算法的有效性，采用 NS2 进行仿真实验，仿真环境基于 MAC 层并使用 IEEE802.11b 的 DCF，仿真环境设置如下：100 个路由节点随机分布在 1000m×1000m 的区域内，随机设置 1～40 个恶意节点，恶意节点随机发起选择性转发攻击、黑洞攻击，并向其他节点提供虚假推荐信息。具体的参数如表 1 所列。

表 1　仿真参数

参数	值
网络拓扑区域	1000m×1000m
节点个数	100
节点传输半径	250m
恶意节点个数(含潜在恶意节点)	1～40
发送数据分组速率	50packet/s
低可信阈值 γ	0.5
高可信阈值 μ	0.8
可信度更新周期 Δt	5s
仿真时间	1000s
数据包大小	10～512byte
时间衰减因子 τ	0.8
初始化节点可信度	0.6

5.2　实验结果与分析

为了检验 BTOR 路由算法的性能，本文从节点可信度变化趋势、吞吐量、端到端的平均时延、数据包投递率等方面进行分析，并将本文算法与 ExOR，TAODV 路由算法进行性能对比。

5.2.1　节点可信度变化

图 1 示出了随着实验周期的增加，正常节点和恶意节点的可信度变化情况。正常节点的平均可信度在前 40 个周期内上升速度较快，随着周期的增加，上升趋势趋于平缓，可信度最终会无限趋近于 1；恶意节点却恰恰相反，一开始它们的平均可信度随着周期增长大幅度下降，大约在第 80 周期之后，下降趋势也逐渐趋于平缓，最后可信度会无限趋近于 0。图 1 表明本文所提出的可信度评估模型能够有效识别恶意节点。

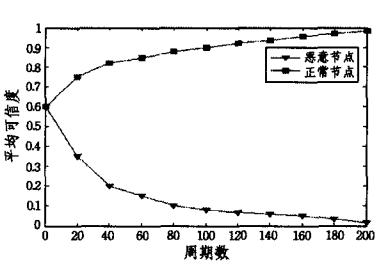

图 1　节点可信度随周期的变化情况

5.2.2　吞吐量

图 2 示出了随着恶意节点的增加 3 种路由算法的吞吐量对比情况。因为恶意节点的黑洞攻击、选择转发攻击致使丢包率上升，大量数据包的丢失使得 3 种路由算法的吞吐量都在下降，而在一开始没有恶意节点时由于机会路由可以大幅提升网络吞吐量，因此 BTOR 和 ExOR 的吞吐量均比 TAODV 大；但随着恶意节点的增多，由于 ExOR 路由算法没有恶意节点检测机制，因此它的吞吐量下降得最快，而本文提出的 BTOR 路由算法较其他路由算法可以更有效地检测恶意节点，将恶意节点从候选转发节点集中剔除，选择更安全的节点来降低丢包率，因此它能减小恶意节点对网络吞吐量的影响。TAODV 路由算法拥有对恶意攻击的防范措施，但效果不是明显。

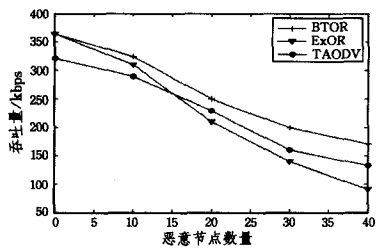

图 2　吞吐量随恶意节点增加的变化情况

5.2.3　端到端的平均时延

图 3 示出了在恶意节点不断增多的情况下，3 种路由算法的端到端平均时延的对比。在恶意节点不断增多的情况下，3 种路由算法的端到端平均时延都在不断增加。由于 BTOR 路由算法增加了对节点可信度的计算、判断以及更新，因此需要额外计算消耗。虽然 TAODV 路由算法也判别恶意攻击，但是 TAODV 的计算没有 BTOR 的计算那么复杂，因此其额外的消耗比 BTOR 少。而 ExOR 路由算法不计算可信度，但是它缺少对恶意攻击的防范能力，随着恶意节点的增多，其通信过程会遭受严重影响，恶意节点会丢弃源节点发送的包，由于频繁丢包，上层的网络协议需要不断地等待通信节点建立连接和数据包重传，因此时延增大。

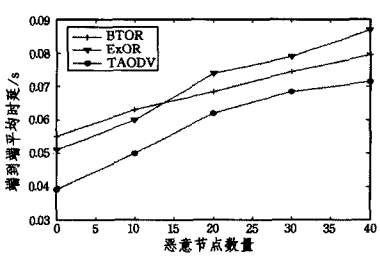

图 3　端到端平均时延随恶意节点增加的变化情况

5.2.4　数据包投递率

图 4 表明，随着恶意节点的增多，总体上 3 种路由算法的数据包投递率均在不同程度地下降。在不存在恶意节点时，3 种路由算法的数据包投递率稳定在 0.9 左右，这是由于存在非恶意因素即网络自身原因带来的丢包等情况会影响数据包投递率。从图中可以看到，随着恶意节点数量的增加，ExOR 路由算法的数据包投递率大幅度下降，在恶意节点个数增加到 40 时，ExOR 路由算法的数据包投递率降到 0.2 左右，但是 BTOR 路由算法的数据包投递率却未大幅度下降，因为它可以识别恶意节点并将其隔离出候选集。TAODV 虽然也能识别恶意节点，但效果不明显，随着恶意节点增多，其数据包投递率的下降幅度也增大。

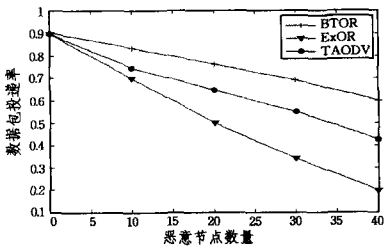

图 4 数据包投递率随恶意节点增加的变化情况

结束语 本文建立了一个可信度评估模型并将其应用在机会路由 ExOR 中，提出了一种基于节点可信度的机会路由改进算法 BTOR。该算法不仅通过利用机会路由提高了无线 Mesh 网络的可靠性和吞吐量，而且有效解决了无线 Mesh 网络中存在的当前以及潜在恶意节点的识别、隔离问题。可信度的建立不仅考虑了节点的信任值，而且考虑了节点行为的积极程度，更加全面地体现节点的可信程度；并对节点可信度进行划分，对可信度处于不确定状态的节点进行未来可信度的预测，以便识别潜在恶意节点。实验结果表明，该算法可以有效识别恶意节点，在恶劣环境下其性能较原来路由协议更具优势。

参 考 文 献

[1] AKYILDIZ I F, WANG X. A survey on wireless mesh networks [J]. IEEE Communications Magazine, 2005, 43(9): 23-30.

[2] ESLAMI M, KARIMI O, KHODADADI T. A survey on wireless mesh networks: Architecture, specifications and challenges [C] // Control and System Graduate Research Colloquium. IEEE. Shah Alam, Malaysia, 2014: 219-222.

[3] BISWAS S, MORRIS R. Opportunistic routing in multi-hop wireless networks[J]. ACM Special Interest Group on Data Communication, 2004, 34(1): 69-74.

[4] BOUKERCHE A, DAREHSHOORZADEH A. Opportunistic Routing in Wireless Networks: Models, Algorithms, and Classifications[J]. ACM Computing Surveys, 2015, 47(2): 1-36.

[5] DAREHSHOORZADEH A, CERDA-ALABERNL. Distance-progress based opportunistic routing for wireless mesh networks [C]// 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, Shanghai, China, 2012: 179-184.

[6] DAREHSHOORZADEH A, SANCHEZMI, Boukerche A. Modeling and Analysis of Opportunistic Routing in Multi-hop Wireless Networks[C]// International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems. Pairs, France, 2014: 337-344.

[7] DAREHSHOORZADEH A, ALMULLA M, BOUKERCHE A, et al. On the number of candidates in opportunistic routing for multi-hop wireless networks[C] // ACM International Symposium on Mobility Management and Wireless Access. Barccelona, Spain, 2013: 9-16.

[8] SANCHEZ-IBORRA R, CANO M D. JOKER: A Novel Opportunistic Routing Protocol[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(5): 1690-1703.

[9] WANG W, CHEN X, LU M, et al. Code pruning in opportunistic routing through bidirectional coding traffic comparison [J]. Wireless Communications & Mobile Computing, 2016, 16(3): 279-299.

[10] YU H, SHEN Z, MIAO C, et al. A Survey of Trust and Reputation Management Systems in Wireless Communications[J]. Proceedings of the IEEE, 2010, 98(10): 1755-1772.

[11] JADIDOLESLAMY H, AREF M R, BAHRAMGIRI H. A fuzzy fully distributed trust management system in wireless sensor networks[J]. International Journal of Electronics and Communications, 2016, 70(1): 40-49.

[12] 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. (in Chinese)
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.

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

[14] BO W, HUANG C, LI L, et al. Trust-based minimum cost opportunistic routing for Ad hoc networks[J]. Journal of Systems & Software, 2011, 84(12): 2107-2122.

[15] THORAT S A, KULKARNI P J. Opportunistic Routing in Presence of Selfish Nodes for MANET[J]. Wireless Personal Communications, 2015, 82(2): 689-708.

[16] SALEHI M, BOUKERCHE A, DAREHSHOORZADEH A, et al. Towards a novel trust-based opportunistic routing protocol for wireless networks[J]. Wireless Networks, 2016, 22(3): 927-943.

[17] BALZANO L, SRIVASTAVA M. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks, 2008, 4(3): 1-15.

[18] LI N, DAS S K. A trust-based framework for data forwarding in opportunistic networks[J]. Ad Hoc Networks, 2013, 11(4): 1497-1509.

[19] ZHOU Z P, SHAO N N. A Improved trust evaluation model based on Bayesian for WSNs[J]. Chinese Journal of Sensors and Actuators, 2016, 29(6): 927-933. (in Chinese)
周治平，邵楠楠. 基于贝叶斯的改进 WSNs 信任评估模型[J]. 传感技术学报，2016，29(6)：927-933.

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

[21] XIA N, LI W, LUO J Z, et al. A Routing Node Behavior Prediction Algorithm based on Fluctuation type identification[J]. Chinese Journal of Computers, 2014, 37(2): 326-334. (in Chinese)
夏怒，李伟，罗军舟，等. 一种基于波动类型识别的路由节点行为预测算法[J]. 计算机学报，2014，37(2)：326-334.

[22] SHI B, LIU S F, DANG Y G, et al. Recursive solution to unbiased grey model and its optimization[J]. Systems Engineering Theory & Practice, 2011, 31(8): 1532-1538. (in Chinese)
石斌，刘思峰，党耀国，等. 无偏灰色预测模型递推解法及其优化[J]. 系统工程理论与实践，2011，31(8)：1532-1538.