doi:10.3969/j.issn.1000-436x.2013.06.023

基于动态邻接信任模型的安全路由算法研究

韩挺[1,2]，罗守山[1,2,3]，辛阳[1,2]，杨义先[1,2]，程工[4]，吴潇[4]

（1. 北京邮电大学 信息安全中心，北京 100876；2. 灾备技术国家工程实验室，北京 100876；
3. 北京安码科技有限公司，北京 100876；4.国家计算机网络应急技术处理协调中心，北京 100029）

摘 要：对现有路由节点信任相关问题进行了研究，综合路由节点的状态和行为因素提出了一种路由节点动态邻接信任模型。在此模型基础上提出了一种基于动态邻接信任熵的安全路由算法，并在现有 OSPF 路由协议中对该路由算法进行了验证。仿真结果表明提出的动态邻接信任模型能够准确地反映路由节点状态改变和恶意攻击，具有良好的动态响应能力，提出的安全路由算法能有效地保证路由节点的行为及状态可信并且具有良好的抗攻击性能。

关键词：路由节点信任；动态邻接信任；安全路由算法；OSPF 协议

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)06-0191-10

Study on security routing algorithm based on dynamic adjacent trust

HAN Ting[1,2], LUO Shou-shan[1,2,3], XIN Yang[1,2], YANG Yi-xian[1,2], CHENG Gong[4], WU Xiao[4]

(1. Information Security Center Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing 100876, China;
3. Beijing Safe-Code Technology Co.,Ltd. , Beijing 100876, China;
4. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China)

Abstract: By studying the related issues of the router node trust, a dynamic adjacent credibility- trust model which integrates factors of state and behavior of the router node was proposed. On the basis of dynamic adjacent credibility-trust model, a security routing algorithm based on dynamic adjacent trust entropy was also proposed, which was validated in the OSPF protocol. The simulation results show that dynamic adjacent credibility-trust model can accurately reflect the state altering and malicious attack of the router node and has better dynamic response ability. In addition, the security routing algorithm can effectively guarantee the behavior and state trust of the router node with highly attack resistant properties.

Key words: router node trust; dynamic adjacent trust; security routing algorithm; OSPF protocol

1 引言

现阶段针对网络路由节点的攻击越来越普遍且后果严重，路由节点面临被劫持、冒用、恶意攻击等风险。目前针对网络中路由节点安全的解决方案较为常见的是采用数字签名等基于密码学的安全加固方式。关于利用数字签名技术保护路由信息目前国内外已有相关研究，Murphy S 等人[1,2]提出对 OSPF 协议链路信息进行签名保护的方法；李道丰[3]等利用可净化签名技术提出一种新的开放式 OSPF 路由协议安全保护机制；Kent S[4]等提出采用公钥加密机制对 BGP 的通信进行授权；Sanzgiri K[5]等提出基于按需路由协议 AODV 的安全路由协议 ARAN，采用公钥机制对 REP 进行签名。上述方案主要解决了路由节点的身份认证和身份可信问题，能够抵御外部节点的虚假路由或篡改路由攻击，但基于密码学的安全手段无法防止路由网络内部具有合法身份的路由节点或被劫持节点发起的恶意

收稿日期：2012-08-06；修回日期：2012-11-02
基金项目：国家自然科学基金资助项目（61121061, 61161140320）；国家科技支撑计划基金资助项目（2012BAH38B02）
Foundation Items: The National Natural Science Foundation of China (61121061, 61161140320); The National Key Technology R&D Program(2012BAH38B02)

攻击行为。

目前国内外学者对基于信任评估方法的路由节点信任安全解决方案进行了相关研究。Peng[6]提出的信任评估方案通过 Bayes 方法评估节点行为，从而获得节点的主观信任；SUN[7] 、喻利[8]等提出了基于改进 Bayes 理论的信任度计算方法，并在移动自组织网络路由协议中进行了验证；许智君[9]等提出了一种信任路由协议，该协议中各路由节点监听邻居节点的数据分组转发行为，据此评价其信任度；王丽娜[10]等提出的模型是对路由实体之间的交互行为进行分析，评估路由实体的接入所带来的网络安全风险及网络增益。以上路由节点信任算法模型均是将路由节点的行为作为判定路由节点信任信息的依据，其给出的评价粒度较粗，且仅基于路由行为的信任评价方式，对路由节点自身状态发生异常但仍表现正常行为的情景未进行考虑，如状态异常的路由节点仍能表现出正常的行为，仅以路由节点的行为来评价其可信程度，不够合理全面，未真实反映路由节点的信任度，不能对恶意节点发起的攻击进行及时有效的评价。路由安全信任现有方案的总结如表 1 所示。

表 1　　路由节点安全已有方案总结

方案	优点	缺点
数字签名解决方案[1~5]	能够抵御各种外部节点的虚假路由或篡改路由攻击	无法防止路由网络内部有合法身份的路由节点或被劫持节点发起的恶意攻击行为
现有路由信任评估解决方案[6~10]	通过对路由节点的交互行为的分析，衡量路由节点的信任度，保证路由节点的行为可信	评价粒度较粗，且仅基于路由行为的信任评价方式对路由节点自身状态发生异常但仍表现正常行为的情景未进行考虑

针对现有路由安全信任方案中的不足，为了更好地体现路由节点的动态信任，提高路由节点选路的可信度，本文首先提出一种动态邻接信任模型，该动态信任模型从路由节点的状态和行为入手，将路由节点的信任度分为状态信任和行为信任；采用多属性决策理论对路由节点的状态信任进行度量并采用 Bayes 模型对路由节点的行为信任进行度量；最终通过灰色关联理论对状态信任和行为信任进行整合得出路由节点的动态邻接信任值。本文在动态邻接信任模型的基础上，提出了一种新的基于邻接信任熵的安全路由算法。该路由算法使用信任采集模型采集路由节点的动态邻接信任值，减小信任采集对已有网络的影响，同时在路由选路时参考动态邻接信任值，从而选择可信度较高的路径。基于邻接信任熵的安全路由算法可以减少状态异常节点和恶意攻击节点给网络带来的破坏，具有良好的动态响应能力，保证了路由网络中路由节点的状态和行为可信。

2　动态邻接信任模型分析与设计

信任关系是一种建立在自身知识和经验基础上的判断，是一种实体与实体之间的主观行为，是基于观察所得到的经验总结[11]。信任包括直接信任、间接信任和经过不同计算方法得到的节点总体信任。直接信任是指在给定的上下文中，评估主体根据所观察的直接接触信息的历史记录而形成的对另外一个实体的信任评估；间接信任是评估主体根据推荐者所提供的信任进行相关处理，最终给出的对实体的信任评估；节点总体信任是评估主体对直接信任和推荐信任进行相关组合形成的信任评估[12]。

直接信任可以保证信息的可靠传递，而间接信任由于作为推荐者的中间节点可能修改或篡改信息而出现恶意推荐（合谋攻击），因此本文采用邻接方式来获得路由节点的直接信任信息，避免间接信任对信任评价带来的不利影响。本文提出的动态邻接信任（DAC-trust, dynamic adjacent credibility trust）模型包含动态状态信任值(DSC，dynamic state credibility)的计算方案设计、动态行为信任值 (DBC, dynamic behavior credibility)计算方案设计以及动态邻接信任值（DAC, dynamic adjacent credibility）计算方案设计。

定义 1 （动态邻接信任值）动态邻接信任值是指评价主体以直接信任的方式（邻接采集）获取到的路由节点的动态信任信息，动态邻接信任值分为动态状态信任值和动态行为信任值。

定义 2 （动态状态信任值）动态状态信任值是指评价主体以直接信任的方式通过对路由节点状态信息进行信任评价而获取到的动态信任信息。

定义 3 （动态行为信任值）动态行为信任值是指评价主体以直接信任的方式通过对路由节点行为信息进行信任评价而获取到的动态信任信息。

2.1　动态状态信任值计算方案设计

采用多属性决策理论[13,14]对路由节点的动态状态信任值进行评价计算。根据多属性决策理论，

将对路由节点状态的 n 维属性做出的评价 e（evaluation）的可能值的集记为 $E=e_1\times e_2\times\cdots e_n$，即 E 为各分属性的笛卡尔积，称 E 为多属性偏好集。其属性值为 $E=[e_1\times e_2\times\cdots\times e_n]^{\mathrm{T}}$，其中，$e_i$（$i$=1,2,⋯,$n$），简记为 E，e_i 为各属性的信任评价值。各属性的权重向量定义为 $W=\{w_1,w_2,\cdots,w_n\}$，其中，$0\leqslant w_i\leqslant 1(i=1,2,\cdots,n)$且$\sum_{i=1}^{n}w_i=1$。定义 E 上的效用函数为 $Y(E)$，属性 e_i 的效用函数为 $y_i(e_i)$，且 $0\leqslant y_i(e_i)\leqslant 1(i=1,2,\cdots,n)$。

本文在衡量路由节点可信度时，采取风险厌恶的态度，且根据路由节点状态属性的重要程度将各属性进行排序。假设选取的路由节点状态的各属性相互独立，则有

$$Y(E)=\sum_{i=1}^{n}w_i y_i(e_i) \tag{1}$$

为了在对状态可信度进行衡量中体现对风险的厌恶，本文采用幂函数来表示所有维度的效用函数，其计算公式为

$$y_i(e_i)=g_i e_i^{\varepsilon_i} \tag{2}$$

其中，g_i 为常数，且 $g_i>0$，$0\leqslant e_i\leqslant 1(i=1,2,\cdots,n)$，$\varepsilon_i$ 为常数且 $0\leqslant\varepsilon_i\leqslant 1(i=1,2,\cdots,n)$。由式（1）和式（2）得出

$$Y(E)=\sum_{i=1}^{n}w_i g_i e_i^{\varepsilon_i} \tag{3}$$

本文中路由节点状态主要考虑以下 4 个维度：实时流量（throughput）、响应时间（response time）、网络时延（delay）以及安全系数（security），即 $E=e_t\times e_r\times e_d\times e_s$。其中，实时流量为某时间段内停留在路由器节点内的数据分组数量，由通过路由节点的入口处流量(进入路由器的流量)到出口处流量(流出路由器的流量)来决定；响应时间与该路由节点的等待队列长度和该节点的处理速度有关，等待队列越长则响应越慢，处理速度越快响应越快；网络延时反映该节点与相邻节点间链路的带宽等通信质量问题；安全系数是指对路由节点的安全加固措施以及路由器本身所采取的安全配置。此外假设路由节点为稳妥型，即设 $g_i=1$，$\varepsilon_i=1/2(i=t,r,d,s)$。设每次信任信息采集的初始时间为 t_1，结束时间为 t_2，则第 k 次信任采集的时间为$\triangle t_k=t_2-t_1$。

动态状态信任的计算由评价的效用函数 $Y(E)$ 按照路由节点的状态属性加权平均而来,考虑了评价的效用性，对某一路由节点的第 N 次动态状态信任计算公式为

$$DSC=f_{dsc}(N) \tag{4}$$

其中，当 N=0 时，$f_{dsc}(N)$=0；当 $N\geqslant 1$ 时 $f_{dsc}(N)$的计算公式为

$$f_{dsc}(N)=w_t\left(\frac{\sum_{k=1}^{N}\triangle t_k\times e_t^{\varepsilon_i}}{\sum_{k=1}^{N}\triangle t_k}\right)^{\frac{1}{2}}+w_r\left(\frac{\sum_{k=1}^{N}\triangle t_k\times e_r^{\varepsilon_i}}{\sum_{k=1}^{N}\triangle t_k}\right)^{\frac{1}{2}}+$$
$$w_d\left(\frac{\sum_{k=1}^{N}\triangle t_k\times e_d^{\varepsilon_i}}{\sum_{k=1}^{N}\triangle t_k}\right)^{\frac{1}{2}}+w_s\left(\frac{\sum_{k=1}^{N}e_s^{\varepsilon_i}}{N}\right)^{\frac{1}{2}} \tag{5}$$

式（4）和式（5）中，DSC 的计算由评价的效用函数 $Y(E)$按照路由节点状态各个维度的相应属性加权平均而来，既考虑了评价的效用性, 又考虑了每次状态变化对信任评价的影响。

2.2　动态行为信任值计算方案设计

路由节点动态行为信任值观测计算时使用 Bayes 模型。根据路由信任的本质，路由转发仅有成功与失败 2 种情况，因此路由节点能够成功完成路由的次数和失败的次数均可看作是一个随机变量，并服从概率近似为 p 的二项事件， 因此可利用二项事件后验概率分布服从 Beta 分布的特性推导动态邻接信任关系[15]，其计算公式为

$$DBC=\frac{s+1}{s+f+1}=\frac{s+1}{n+1} \tag{6}$$

其中，$n=s+f$，且 s 、f 分别表示事件成功次数和失败次数，此概率是对路由节点未来行为的期望值，可用以表示路由节点的行为信任值。

引入奖赏因子（RD）和惩罚因子（PN），为了体现信任建立难失去容易的特性，设惩罚因子大于奖赏因子。引入奖励因子和惩罚因子后的动态邻接信任值的计算公式为

$$DBC=\frac{s+1}{n+1}+RD(1+RAT)-PN(2-RAT) \tag{7}$$

其中，RAT 为节点整体历史行为良好率，其计算公式为

$$RAT=\frac{\text{节点历史良好行为数}}{\text{节点历史行为数}} \tag{8}$$

为了体现信任值的时间敏感特性，减少过去行为信息对当前信任值的影响，增加最近发生事件的权重，引入指数衰减因子(遗忘因子)来减少过去行

为的影响。引入指数衰减因子后的动态行为信任值计算公式为

$$DBC^{\text{new}} = DBC \times e^{-c\Delta t} \tag{9}$$

其中，c 为指数衰减系数。

以上所提到的参数可以按照具体应用的需要进行调整，表明了本文信任模型的灵活性。

2.3 动态邻接信任值计算方案设计

本文采用灰色关联理论[16~18]结合路由节点的动态状态信任、动态行为信任等信任信息，将由灰色关联理论计算得到的关联度作为路由节点的动态邻接信任值，反映一段时间内路由节点的信任值及其变化。

定义 4 （动态状态信任流）定义动态状态信任值流为序列 $DSC_s=(ds_s(1), ds_s(2),\cdots, ds_s(k),\cdots,ds_s(n))$，其中，$ds_s(k)$为时间节点 k 时路由节点的动态状态信任值。

定义 5 （动态行为信任流）定义动态行为信任值流为序列，其中，$DBC_s=(db_s(1),db_s(2),\cdots,db_s(k),\cdots, db_s(n))$，其中，$db_s(k)$为时间节点 k 是路由节点的动态行为信任值。

根据灰色关联理论，设邻接信任评估比较序列为 $dac_s=(dac_s(1), dac_s(2),\cdots, dac_s(k),\cdots, dac_s(n))$，其中，$dac_s(k)=min(ds_s(k), db_s(k))$。

设邻接信任评估的参考序列为 $dac_{s0}=(dac_{s0}(1), dac_{s0}(2),\cdots, dac_{s0}(k),\cdots, dac_{s0}(n))$，该序列为路由节点状态和行为的信任评价信息均为最优时的邻接信任评估比较序列。

根据灰色关联理论中灰色关联度的计算方法，动态邻接信任 DAC 的计算公式如式（10）和式（11）。

$$DAC = \frac{1}{n}\sum_{k=1}^{n} DAC(dac_s(k), dac_{s0}(k)) \tag{10}$$

$$DAC(dac_s(k), dac_{s0}(k)) = \frac{\text{minmin}\left|dac_s(k)-dac_{s0}(k)\right| + \tau\text{maxmax}\left|dac_s(k)-dac_{s0}(k)\right|}{\left|dac_s(k)-dac_{s0}(k)\right| + \tau\text{maxmax}\left|dac_s(k)-dac_{s0}(k)\right|} \tag{11}$$

其中，τ 称为分辨系数。当 $\tau \leqslant 0.5463$ 时，分辨力最好，通常取 $\tau = 0.5$。

定理 1 根据灰色关联理论[18]，动态邻接信任值 DAC 稳定的充分必要条件如下。

1) $0<(dac_s(k), dac_{s0}(k)) \leqslant 1, \forall k$; $1<DAC(dac_s(k), dac_{s0}(k)) < 0$; $DAC(dac_s(k), dac_{s0}(k))=1 <=> dac_s(k)= dac_{s0}(k)$。

2) 设 X 为灰关联因子集，$DAC(X,Y)= DAC(Y, X)<=> X=\{x,y,\}$。

3) $x_i, x_j \in X=\{x_k|k=0,1,2,\cdots,n\}$, $n \geqslant 2$。

$DAC(x_i, x_j) \neq DAC(x_j, x_i)$，且 n 为有限数，$n \in N$，N 为自然数集。

证明

必要性。

1) 若 $|dac_s(k)-dac_{s0}(k)|=$ minmin $|dac_s(k)-dac_{s0}(k)|$ 即 $dac_s(k)= dac_{s0}(k)$，则 $DAC(dac_s(k), dac_{s0}(k))=1$;

若 $|dac_s(k)-dac_{s0}(k)| \neq$ maxmax $|dac_s(k)-dac_{s0}(k)|$，则 $DAC(dac(k), dac_{s0}(k))=(\text{minmin}|dac_s(k)-dac_{s0}(k)|+\tau\text{maxmax}|dac_s(k)-dac_{s0}(k)|)/(1+\tau)\text{maxmax}|dac_s(k)-dac_{s0}(k)| < (\text{maxmax}|dac_s(k)-dac_{s0}(k)|+\tau\text{maxmax}|dac_s(k)-dac_{s0}(k)|)/(1+\tau)\text{maxmax}|dac_s(k)-dac_{s0}(k)|=1$，易知 $(\text{minmin}|dac_s(k)-dac_{s0}(k)|+\tau\text{maxmax}|dac_s(k)-dac_{s0}(k)|)/(1+\tau)\text{maxmax}|dac_s(k)-dac_{s0}(k)|>0$；

由上可知 $1 < DAC(dac_s(k), dac_{s0}(k)) < 0$

2) 若 $X=\{x,y\}$，则有 $|x(k)-y(k)|=|y(k)-x(k)|$，$\text{maxmax}|x_0(k)-x(k)|=\max|x_0(k)-x(k)|$，因此 $DAC(X,Y)=DAC(Y, X)$

3) 若 $X=\{x_k|k=0,1,2,\cdots,n\}$，$n \geqslant 2$，则有

$\text{maxmax}|x_a(k)-x_j(k)| \neq \text{maxmax}|x_b(k)-x_j(k)|$ 则 $DAC(x_i, x_j) \neq DAC(x_j, x_i)$。

充分性。

记 k 时刻 $|dac_s(k)-dac_{s0}(k)|$ 为 $\Delta(k)$，则各时刻的最小绝对差和最大绝对差分别为 $\Delta_{\min}=\text{min}-\text{min}|dac_s(k)-dac_{s0}(k)|$；$\Delta_{\max}=\text{maxmax}|dac_s(k)-dac_{s0}(k)|$。

$dac_s(k)$、$dac_{s0}(k)$两因素曲线在 k 时的相对差值即灰色关联系数可用式(12)来表示。

$$DAC\left(dac_s(k), dac_{s0}(k)\right) = \frac{(\Delta_{\min} + \tau\Delta_{\max})}{(\Delta(k) + \tau\Delta_{\max})} \tag{12}$$

灰色关联系数具有一定的分散性，因此用其平均值作为集中化处理的一种方法。所以节点的动态邻接信任值 DAC 的计算公式如式(10)。

证毕。

由定理 1 可以推导出动态邻接信任值的性质 1。

性质 1 当路由节点状态及行为信任评价信息越接近其最优值时，路由节点的动态邻接信任值越高，即 $|dac_s(k)-dac_{s0}(k)|$ 越小，DAC 越大。

根据定理 1 和性质 1 可知，动态邻接信任值可以正确地反映节点的状态和行为信任评价信息。

2.4　DAC-Trust 仿真分析

采用 Opnet 仿真软件构建路由交换网络，对 DAC-Trust 模型进行仿真实验，并从两方面分析动态信任模型：1) 模型准确性分析，验证所提出的信任模型与算法是否能够准确地反应路由节点的行为与状态变化；2) 动态响应能力分析，动态的信任评估模型应该具有良好的动态响应能力，以刻画实体信任演化程度。

1) 准确性分析

实验场景设计：在开放的路由交换网络中对 3 个路由节点进行信任评价，其中，节点 1 处于正常状态且行为表现正常（仅存在小概率的路由转发失败行为）；节点 2 处于紧急状态且存在较多异常行为（存在一定概率的路由转发失败行为）；节点 3 由紧急状态转移至危险状态且产生攻击行为（进行恶意攻击，存在较大概率的路由转发失败行为）。

DAC-Trust 模型的准确性分析仿真结果如图 1 所示。三角形标记代表节点 1，在初期存在一定小概率的路由转发行为导致信任值略低于 0.8，当路由行为稳定后，其信任值稳定在 0.8 以上的较高水平。正方形标记代表节点 2，由于其处于紧急状态所以信任值一直低于 0.7，当其产生一定概率的路由转发失败行为后，其信任值下降到 0.6 以下。圆形标记代表节点 3，初期从紧急状态转移至危险状态，其信任值从 0.7 下降至 0.6 左右，当其产生较大概率的路由转发失败行为后，其信任值下降至 0.2 左右。综上所述，动态邻接信任模型能够准确地反应路由节点行为和状态变化对信任带来的影响。

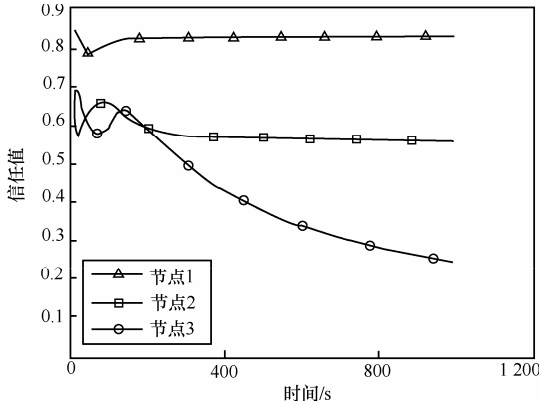


图 1　DAC-Trust 模型的准确性分析仿真结果

2) 动态响应能力分析

实验场景设计：基于以上的实验环境，本文的 DAC-Trust 模型和采用 Bayes 模型动态信任计算模型进行比较，即采用 2 种信任模型计算同一路由节点的信任值。假定路由节点是从正常状态和正常行为开始，而后随着状态的恶化（如其安全性遭到破坏导致状态恶化），最后处于危险状态表现出恶意行为的过程。

DAC-Trust 动态响应能力分析仿真结果如图 2 所示。正方形标记为采用 Bayes 动态信任模型的计算结果，三角形标记为采用 DAC-Trust 模型的计算结果。当路由节点状态出现恶化时（150s 左右），由于 Bayes 信任模型未考虑路由节点状态信息其计算得到的信任值暂时仍保持较高水平（0.8），直到其表现出恶意行为之后其计算得到的信任值才开始下降。DAC-Trust 考虑了路由节点状态信息，因此，当状态恶化之后 DAC-Trust 及时作出响应其计算得到的信任值会随之下降。综上所述，DAC-Trust 模型在信任计算动态响应方面优于 Bayes 信任模型。若突发事件发生，DAC-Trust 模型能比 Bayes 信任模型更快做出响应。

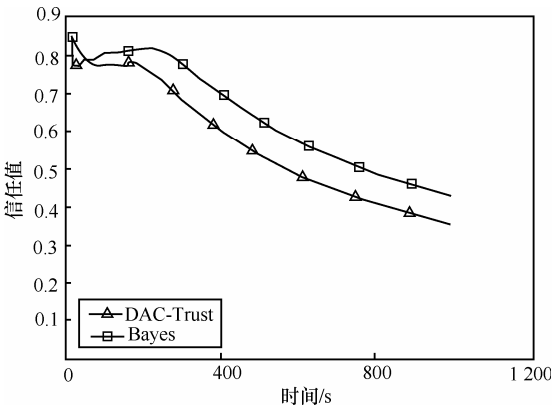


图 2　DAC-Trust 模型与 Bayes 模型动态响应能力比较

3　基于动态邻接信任熵的可信路由算法研究

3.1　CCM 平台设计

本文设计了信任采集平台（CCM, credibility collect monitors）对动态邻接信任信息进行采集。CCM 的引入保证了动态邻接信任信息的可靠获取和传递，其结构如图 3 所示。

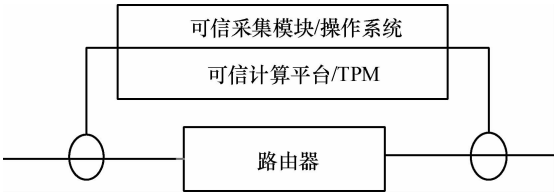


图 3　CCM 结构

CCM 采用可信计算平台模块保证 CCM 自身平台的完整性和安全性。CCM 利用信任信息采集评估模块来采集和计算路由节点的信任信息。

考虑到 CCM 对网络的影响，CCM 采用监听/采集部署方式。监听/采集方式是指 CCM 通过监听动作和采集动作获得路由节点的相关可信信息。一个 CCM 可以同时监测几个路由节点。这种部署方式的优点是只需要几个 CCM 就可以监视整个路由网络，同时 CCM 之间可以通过专有网络来交互信息，不给现有网络添加多余的负担。图 4 为 CCM 的部署方式。

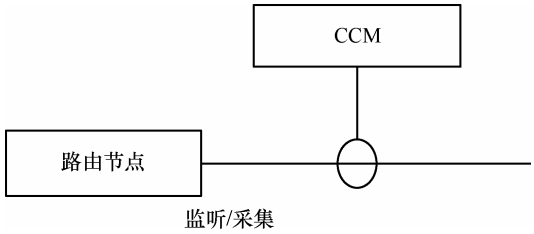


图 4 CCM 的部署方式

CCM 进行信任值采集的过程如下。

1) CCM 部署。采用监听/采集方式部署 CCM。在路由网络中部署若干个 CCM 监视所有路由节点。

2) CCM 信任信息采集。CCM 通过监听动作获得并计算动态状态信任值。CCM 通过采集动作获得动态行为信任值。

3) CCM 信任整合。将采集到的动态状态信任值和动态行为信任值通过计算整合为路由节点的动态邻接信任值。

4) CCM 之间信任信息交互。每个 CCM 采用可靠泛洪的方式将其采集到的路由节点的动态邻接信任值在 CCM 专有网络中洪泛给其他 CCM。通过信任信息交互，每个 CCM 都能获得到整个网络中所有路由节点的动态邻接信任值。

5) CCM 与路由节点之间信任信息交互。当 CCM 获得整个网络中所有路由节点的邻接信任值后，将这些邻接信任值的信息发送给其监视的路由节点，从而使每个路由节点都能获得整个网络中其他路由节点的邻接信任值。

3.2 动态邻接信任熵

为了评估出指定路由节点和目的路由节点之间的可信度最高的路线，本文引入动态邻接信任熵（DACE, dynamic adjacent credibility entropy）。

定义 6 (动态邻接信任熵)假设路由节点 a 到路由节点 b 存在 n 条可达路径，记为集合 $route(a \to b)$，中间节点集合为 $C=\{c_i,i=1,\ 2,3,\cdots\}$。对于其中任意一条路径 $r_\alpha=a\to c_1\to c_2\to c_3\to\cdots\to c_m\to b$，定义在 t 时刻时路径 r_α 的动态邻接信任熵为 $DACE$，其计算公式为

$$DACE_{r_\alpha}=\sum_{c_j\in C}DACE(c_j)^{-1}\cdot\ln DACE(c_j)^{-1} \quad (13)$$

由文献[10]可知，一条链路的 $DACE$ 越小，该条链路的总体信任程度越高，信任分布越均匀，同时跳数也越小。

3.3 基于动态邻接信任熵的安全路由算法设计

基于动态邻接信任熵的安全路由算法（DACERA dynamic adjacent credibility entropy security routing algorithm）是一个包含局部最优解的贪心迭代过程。本文采用 Dijkstra 算法来实现该贪心迭代过程并定义函数 $CalDACE()$来计算 2 点之间链路的动态邻接信任熵。由于 DACERA 是基于 Dijkstra 算法且 $CalDACE()$ 函数只增加了一个常量因子，所以 DACERA 的计算复杂度与 Dijkstra 算法相同为 $O(|E|+|R|\log|R|)$。

以下给出以路由节点 r_1 为源节点的 DEACRA 的具体形式化描述，其流程如图 5 所示。

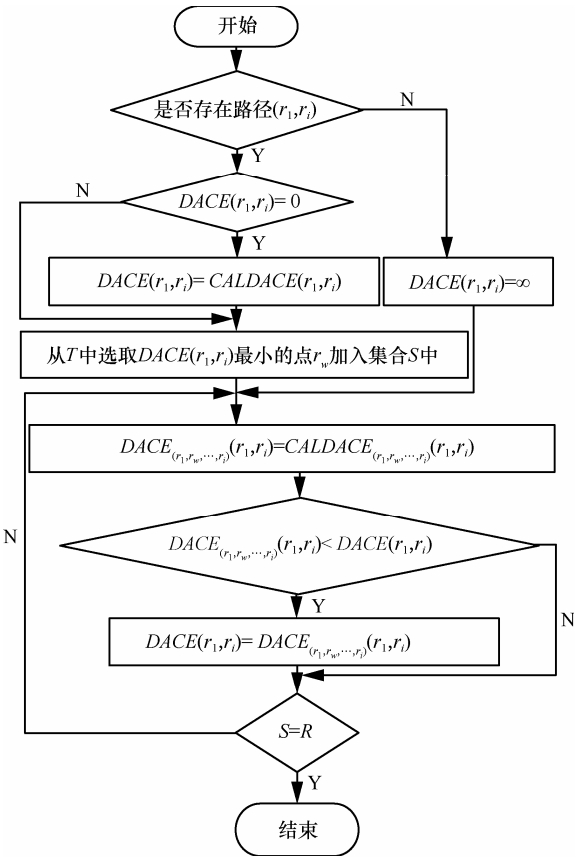


图 5 DACERA 算法流程

1) 初始时设全部路由节点的集合为 R，令集合 $S=\{r_1\}$,$T=$\{除了 r_1 以外的其他节点\}。

2) 若存在路径(r_1,r_i)且尚无权值则利用函数 $CalDACE()$计算 $DACE(r_1,r_i)$，将该路径的权值设为 $DACE(r_1,r_i)$；若不存在路径(r_1,r_i)将该路径权值设为∞。

3) 从 T 中选取一个权值最小的节点 r_w 加入 S。

4) 对 T 中节点的路径的权值进行修改：若加进 r_w 为中间节点，重新利用函数 $CalDACE()$计算 $DACE(r_1,r_i)$，若从 r_1 到 r_i 的 $DACE(r_1,r_i)$不包含 r_w 的 $DACE(r_1,r_i)$要小，则修改此路径的权值。

5) 重复上述步骤，直到 S 中包含所有节点，即 $S=T$ 为止。

3.4　DACERA 路由算法验证及仿真分析

为了验证 DACERA 路由算法，本文在现有的 OSPF 路由协议中引入了本算法。通过 OPNET 来仿真采用 DACERA 的 OSPF 路由协议，同时将采用 DACERA 的 OSPF 协议同基于数字签名的 OSPF 协议[1]以及同文献[6~8]中的采用 Bayes 理论的动态信任计算模型的 OSPF 协议进行比较。

1) 采用 DACERA 的 OSPF 协议同基于数字签名的 OSPF 协议仿真比较，其仿真参数如表 2 所示。

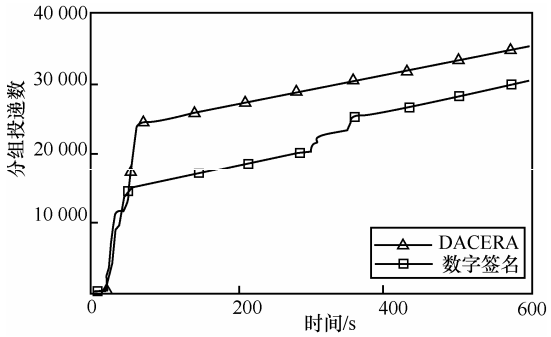
表 2　　仿真参数

仿真参数	数值
总节点数	10
存在恶意行为节点	0~5
仿真时间	600 s
仿真范围	500×500

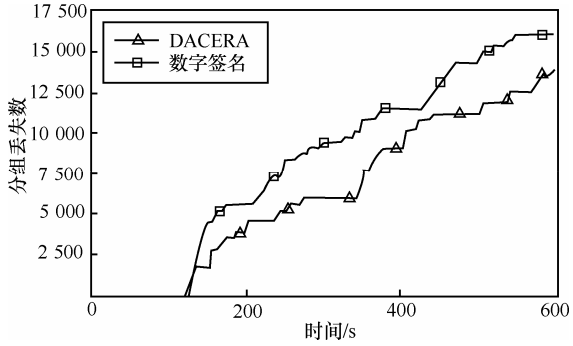
从仿真结果图 6(a)可以看出，随着被攻击的节点的增加，分组丢失行为也不断增多，采用 DACERA 的 OSPF 协议的分组投递数受到的影响明显低于数字签名 OSPF 协议，其分组投递数始终高于数字签名 OSPF 协议，这主要是由于采用 DACERA 的 OSPF 协议在路由选择时会选择可信度较高的路径，避免了实施恶意攻击的路由节点出现在路由路径上，减少了分组的丢弃，增加了整个网络运行的稳定性。

根据图 6(b)可以发现实施恶意攻击的节点随着时间增加导致分组丢失数逐渐增加，特别是第一个被恶意攻击的节点出现后，数字签名 OSPF 协议的分组丢失率明显增加。而采用 DACERA 的 OSPF 协议，将实施攻击的节点排除在路由路径之外，对实施恶意攻击的节点使用率减少，因此与数字签名 OSPF 协议相比，分组丢失数明显减少，具有更好的抵御恶意攻击的能力。

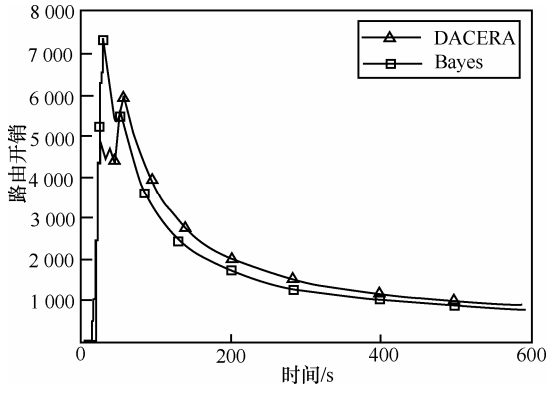
通过整个网络收集全局统计量平均值 OSPF 平均发送流量（bit/s）的仿真结果来分析路由的开销情况。从图 6(c)可知，采用 DACERA 的 OSPF 协议是收敛的。在 0~300 s 之间，整个网络中路由交换的数据量较大且变化较快；在 300 s 之后网络进入到收敛状态，所以仿真进行到 300 s 以后，数据通信量趋于零。从仿真结果可以看出，由于要进行可信信息的采集以及可信信息的评估，采用 DACERA



(a) 分组投递数



(b) 分组丢失数



(c) 路由开销

图 6　采用 DACERA 的 OSPF 协议同基于数字签名的 OSPF 协议仿真比较

的 OSPF 协议在大约 200 s 时开始收敛，采用数字签名的 OSPF 在大约 180 s 时开始收敛。由于路由节点需要通过报文与 CCM 之间交换可信度的信息，采用 DACERA 的 OSPF 协议的路由开销比数字签名 OSPF 协议略大。

综上所述，在存在攻击的情况下，采用 DACERA 的 OSPF 协议较采用数字签名的 OSPF 协议有更好的抗攻击性、更高的分组投递率以及更低的分组丢失率。

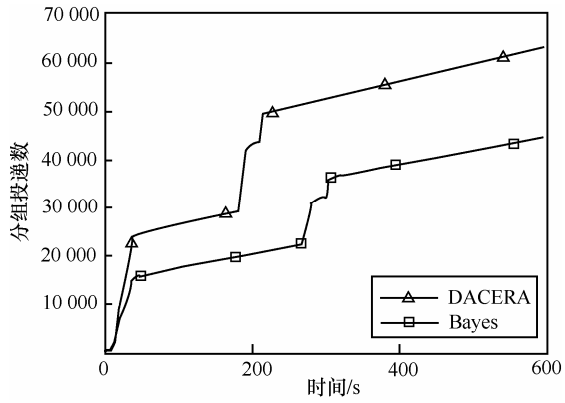
2) 采用 DACERA 的 OSPF 协议同采用 Bayes 理论的动态信任计算模型的 OSPF 协议仿真比较，其仿真参数如表 3 所示。

表 3　　仿真参数

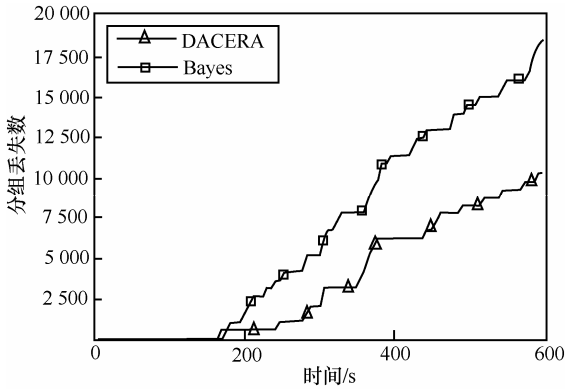
仿真参数	数值
总节点数	15
存在恶意行为节点	0~5
状态异常节点	0~5
仿真时间	600 s
仿真范围	500×500

从仿真结果图 7(a)可以看出，随着状态异常节点的增多，采用 DACERA 的 OSPF 协议的分组投递数受到的影响明显低于采用 Bayes 理论的 OSPF 协议，其分组投递数始终高于采用 Bayes 理论的 OSPF 协议，这主要是由于采用 DACERA 的 OSPF 协议在路由信任评价时采集节点的状态信息，避免了状态异常的路由节点出现在路由路径上，减少了分组的丢弃。在 180 s 时，当信任信息采集完成后，采用 DACERA 的 OSPF 协议的选路基本避开状态异常节点，分组投递数随之增加；而采用 Bayes 理论的 OSPF 协议直到状态异常节点出现异常行为后才能在选路时避开这些节点（240 s 左右）。因此与采用 Bayes 理论的 OSPF 协议相比，采用 DACERA 的 OSPF 协议在动态节点变化中具有更好的动态适应能力。

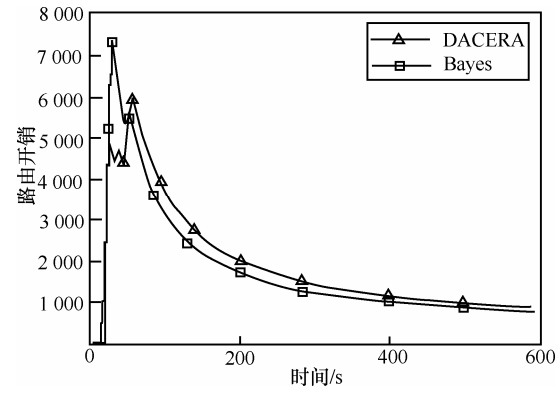
根据图 7(b)可以发现随着状态异常节点的增加导致 OSPF 网络中分组丢失数逐渐增加，但采用 DACERA 的 OSPF 协议通过 DACERA 基本将状态异常的节点排除在路由选路之外，对状态异常节点的使用率减少，与采用 Bayes 理论的 OSPF 协议相比，分组丢失数明显减少。因此与采用 Bayes 理论的 OSPF 协议相比，采用 DACERA 的 OSPF 协议能更细粒度地对路由信任进行评价，减少状态异常路由对网络的影响，提高网络的稳定性。



(a) 分组投递数



(b) 分组丢失数



(c) 路由开销

图 7　采用 DACERA 的 OSPF 协议同采用 Bayes 理论的动态信任计算模型的 OSPF 协议仿真比较

通过整个网络收集全局统计量平均值 OSPF 平均发送流量（bit/s）的仿真结果来分析路由的开销情况。从仿真结果图 7(c)可以看出，由于采用 DACERA 的 OSPF 协议同采用 Bayes 理论的 OSPF 协议均要进行可信信息的采集以及可信信息的评估，两者路由开销的差距细微即采用 DACERA 的 OSPF 协议

同采用 Bayes 理论的 OSPF 协议具有相近的路由性能。

综上所述，在存在异常状态节点的情况下，采用 DACERA 的 OSPF 协议较采用 Bayes 理论的 OSPF 有更好的动态适应能力、更细粒度的信任评价、更高的分组投递率、更低的分组丢失率以及更高的网络稳定性。

4　结束语

首先本文在深入研究了路由节点的状态信息及行为信息的基础上，设计了路由节点的动态状态信任值计算方案和动态行为信任值计算方案，最后通过引入灰色关联理论，提出了一种有别于传统信任模型的动态邻接信任模型。仿真结果表明该模型能够准确反映路由节点的状态和行为信任信息并具有更高的动态响应能力；其次本文在动态邻接信任模型的基础上提出了基于动态邻接信任熵的安全路由算法并在现有 OSPF 协议中对该算法进行了验证。仿真结果表明，该算法可以有效地评测节点的动态邻接信任值并且在路由选择时选择可信度较高的路径，有效抵御恶意行为和状态异常节点的攻击，具有更好的动态响应能力以及更细粒度的信任评估，有效地提升了网络的抗攻击性及稳定性。

参考文献：

[1] MURPHY S, BADGER M, WELLINGTON B. OSPF with digital signatures[EB/OL]. http://www.faqs.org/rfcs /rfc2154. html.

[2] MURPHY S, BADGER M. Digital signature protection of the OSPF routing protocol[A]. Proceedings of the Symposium on Network and Distributed System Sercurity[C]. Washington DC,USA,1996. 93-102.

[3] 李道丰, 杨义先, 谷利泽. 采用可净化签名的 OSPF 协议安全保护机制[J].北京邮电大学学报,2011,34(3):79-83.
LI D F, YANG Y X, GU L Z. Secure protection mechanism for OSPF protocol with sinitizable signature scheme[J]. Journal of Beijing University of Posts and Telecommunications, 2011, 34(3):79-83.

[4] KENT S, LYNN C, SEO K. Secure border gateway protocol (SBGP)[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592.

[5] SANZGIRI K, DAHILL B, LEVINE B N. A secure routing protocol for ad hoc networks[A]. Proeedings of the 10th IEEE International Conference on Network Protocols[C]. Paris, France, 2002.

[6] PENG S C, JIA W J. Voting-based clustering algorithm with subjective trust and stability in mobile ad-hoc networks[A]. Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous-Computing[C].Washington, DC, USA, 2008.3-9.

[7] SUN Y X, HUANG S H, CHEN L. Bayesian decision-making based recommendation trust revision model in ad hoc networks[J]. Journal of Software, 2009, 20(9): 2574- 2586.

[8] 喻莉,李静茹,刘祖浩. 基于自适应遗忘机制的半环信任模型[J].电子信息学报.2011, 33(1):175-179.
YU L, LI J R, LIU Z H.Semiring trust model based on adaptive forgetting scheme[J]. Journal of Electronics & Information Technology, 2011, 33(1):175-179.

[9] 许智君,胡琪一,张玉军.MANET 网络激励节点协作的信任评估路由协议[J].通信学报.2012, 33(7):27-35.
XU Z J, HU Q Y, ZHANG Y J. Trust evaluation routing protocol to enforce cooperation in mobile adhoc networks[J]. Journal on Communications, 2012, 33(7):27-35.

[10] 王丽娜,赵磊, 郭迟. 一种基于信任理论的路由安全接入与选路模型[J].武汉大学学报.2008, 10(10):999-1002.
WANG L N, ZHAO L, GUO C. A network connection and routing model based on trust theory[J]. Geomatics and Information Science of Wuhan University, 2008, 10(10):999-1002.

[11] 贺利坚, 黄厚宽, 张伟. 多 Agent 系统中信任和信誉系统研究综述[J].计算机研究与发展, 2008, 45(07) : 1151- 1160.
HE L J, HUANG H K, ZHANG W. A survey of trust and reputation systems in multi-agent systems[J]. Journal of Computer Research and Development, 2008,45(07): 1151- 1160.

[12] DUMA C, SHAHMEHRI N, CARONNI G. Dynamic trust metrics for peer-to-peer systems[A]. Proceedings of the 16th Intel Joint Workshop on Database and Expert Systems Applications[C]. Washington DC, USA, 2005. 776−781.

[13] 魏世孝, 周献中. 多属性决策理论方法及其在 C^3I 系统中的应用[M]. 北京: 国防工业出版社,1998.31-45.
WEI S X, ZHOU X Z. Multiple Attribute Decision Making Principle and Its Application In C3I System[M]. Beijing: National Defense Industry Press, 1998. 31−45.

[14] 甘早斌, 丁倩, 李开. 基于声誉的多维度信任计算算法[J].软件学报, 2011,22(10):2401−2411.
GAN Z B, DING Q, LI K. Reputation-based multi-dimensional trust algorithm[J]. Journal of Software, 2011,22(10):2401−2411.

[15] 洪亮, 洪帆, 彭冰. 一种基于邻居信任评估的虫洞防御机制[J] . 计算机科学, 2006 , 33 (8): 130-133.
HONG L, HONG F, PENG B.Defend against wormhole attack based on neighbor trust evaluation in MANET[J]. Computer Science, 2006, 33 (8): 130-133.

[16] 邓聚龙.灰色系统理论教程[M]. 武汉:华中理工大学出版社, 1990.128-134.
DENG J L. Grey System Theory Tutorial[M].Wuhan: Huazhong University Press, 1990.128-134.

[17] 徐兰芳, 胡怀飞 ,桑子夏. 基于灰色系统理论的信誉报告机制[J]. 软件学报, 2007, 18(7) : 1730- 1737.
XU L F, HU H F, SANG Z X. A prestige reporting mechanism based on gray system theory[J]. Journal of Software, 2007, 18(7) : 1730-1737.

[18] 徐兰芳, 张大圣, 徐凤鸣. 基于灰色系统理论的主观信任模型[J]. 小型微型计算机系统,2007,28(5):801-804.
XU L F, ZHANG D S, XU F M. Subjective trust model based on grey system theory[J]. Journal of Chinese Computer Systems, 2007, 28(5): 801-804.

作者简介：

韩挺（1984-），男，吉林四平人，北京邮电大学博士生，主要研究方向为计算机网络与信息安全。

杨义先（1961-），男，四川盐亭人，博士，北京邮电大学教授、博士生导师，主要研究方向为信息安全、网络安全、编码密码学、数字信号处理、神经网络等。

罗守山（1962-），男，安徽合肥人，北京邮电大学教授、博士生导师，主要研究方向为信息安全、密码学理论、安全多方计算等。

程工（1972-），男，北京人，国家计算机网络应急技术处理协调中心高级工程师，主要研究方向为互联网信息安全。

辛阳（1977-），男，山东烟台人，北京邮电大学副教授，主要研究方向为信息安全和密码学。

吴潇（1982-），男，湖南株洲人，国家计算机网络应急技术处理协调中心副高级工程师，主要研究方向为移动互联网信息管理、互联网信息安全。

（上接第 190 页）

[14] BELKACEMI H, MARCOS S, PAURA L. Robust subspace-based algorithm for joint angle/doppler estimation in non-Gaussian clutter[J]. Signal Processing, 2007, 87(4):1547-1558.

[15] 兰天, 邱天爽, 杨娇. 脉冲噪声环境下循环 ESPRIT 新方法[J]. 通信学报, 2010, 31(9):88-93.
LAN T, QIU T S, YANG J. New cyclic-ESPRIT algorithms in impulsive noise environment[J]. Journal on Communications, 2010, 31(9): 88-93.

作者简介：

刘洋（1981-），男，辽宁黑山人，博士，内蒙古大学副教授，主要研究方向为非平稳信号处理、通信信号处理等。

邱天爽（1954-），男，江苏海门人，博士，大连理工大学教授、博士生导师，主要研究方向为数字信号处理理论与应用、非平稳非高斯信号处理和生物医学信号处理等。

李景春（1966-），男，河北宁晋人，博士，国家无线电监测中心总工程师、教授级高工，主要研究方向为电磁兼容与无线电监测新技术等。