# 一种适合于分级 Ad Hoc 网络的实时风险评估安全策略

于 尧,郭 磊,王兴伟,李平平
(东北大学信息科学与工程学院,辽宁沈阳 110004)

**摘 要:** 为提高分级 Ad Hoc 网络面临入侵行为时的路由性能,提出一种基于风险评估的入侵响应决策模型.该模型通过自组织神经元映射手段将攻击行为聚类,实时量化攻击节点的风险程度,以评估当前攻击对网络的威胁程度,并结合节点状态等辅助信息预测攻击持续程度和规模,对攻击节点采取相应的决策响应措施.仿真结果表明,该方法能够实时量化网络面临的威胁,及时、有效地遏制或减轻路由攻击对网络的危害.

**关键词:** 分级 Ad Hoc 网络; 风险评估; 动态决策; 聚类分析
**中图分类号:** TN915.08 **文献标识码:** A **文章编号:** 0372-2112 (2011) 01-0108-06

# A Real-Time Risk Evaluation Security Strategy in Hierarchical Ad Hoc Networks

YU Yao, GUO Lei, WANG Xing-wei, LI Ping-ping
(*School of Information Science and Engineering , Northeastern University , Shenyang , Liaoning* 110004, *China*)

**Abstract:** In this paper, an intrusion response decision-making model based on the risk evaluation is proposed to improve the routing performance in hierarchical Ad Hoc networks. In this model, the attack behaviors were in clustering analyzing according to self-organizing map, and the risk degree was calculated in real time and quantity, in order to evaluate the threaten extent of the current attack. Combined with the related information such as the node statue, we could forecast the sustainable extent and scale of the attack, and thereby adopt the relevant decision-making to the attack node. Simulation results show that, the model proposed in this paper can real-time quantize the intimidation that hierarchical Ad Hoc networks meet, and alleviate and even contain the network harm caused by the routing attacks.

**Key words:** hierarchical Ad Hoc networks; risk evaluation; dynamic decision-making; clustering analyze

## 1 引言

移动 Ad Hoc 网络具有组网灵活、展开迅速、分布控制等诸多优点[1],随着其应用范围的不断扩大,采用分级结构可以获得更好的性能[2].但是,新的网络特性使其安全形势严峻,如何减少攻击给网络带来的损失具有重要的现实意义[3~5],也成为网络安全研究的热点之一.

风险评估系统通过对网络威胁、脆弱点以及由此带来的风险大小进行定性或定量的评估,能够为网络系统应对复杂网络环境下各种突发网络攻击事件提供更准确的决策依据[6~8],从而保障网络将风险控制在其可承受的范围内,提高网络的可用性.目前,关于网络中通信实体评估的研究比较多,其中实时量化的风险评估机制具有直观和动态的优点[9],但是其结构相对复杂,该方面研究尚处于探索阶段,现有评估方法大致可分为基于概率论和基于模糊理论两类,其中前者着重解决"大样本不确定性"问题[10],后者则适用于"认知不确定性"问题[11,12].由于移动 Ad Hoc 网络的节点动态和随机等特点,以及攻击节点的隐蔽性,很难满足概率论方法中对体现统计规律的事件数量的要求,这势必会影响到该方法的评估效果.而模糊理论通过经验认知获得表达规律,可以有效地解决移动 Ad Hoc 网络事件样本偏少或者不全的问题,但其过多依赖先验认知也会对评估带来一些影响,具有一定的局限性.

现有的风险机制大多将研究重心放在风险评估基

收稿日期:2009-09-05;修回日期:2009-10-13
基金项目:中央高校基本科研业务费专项资金(No.N100304009,No.N090504003,N090504006);国家自然科学基金(No.61070162,No.71071028,No.60802023,No.70931001);高等学校博士学科点专项科研基金(No.20100042110025,No.20070145017);霍英东教育基金会青年教师基金(No.121065)

础理论支撑方面,对面向 Ad Hoc 网络的风险评估研究较少.在分级 Ad Hoc 网络中,节点根据某种成簇规则被划分为若干个簇,并按照其角色各司其责,这种结构特点和网络需求对风险评估机制的研究提出了新的挑战.首先,Ad Hoc 网络节点移动特性对风险评估的实时性要求较高;其次,Ad Hoc 网络具有节点合作的本质,相比于节点地位平等的平面网络,分级网络相对复杂的组织结构使节点间的关联性更强,因此在评估风险时需要考虑到以簇为单位的节点的表现;再次,由于不同角色节点在分级网络中的功能和职责不同,因此应有针对性地提出多种响应策略以适应分级网络的结构需求;另外,随着系统规模的扩大,分级 Ad Hoc 网络的评估管理也将变得非常复杂.

为提高分级 Ad Hoc 网络面临攻击时的路由性能,本文提出一种基于风险评估的入侵响应决策模型.该模型将入侵检测系统的告警作为输入,提取被攻击节点的性能指标,预测攻击节点的潜在威胁能力,实时量化攻击节点给网络带来的风险程度,并将其作为决策响应的主要依据,结合节点角色和网络环境等辅助信息,对攻击节点采取相应的处理措施,从而及时、有效地遏制或减轻路由攻击对网络的危害.仿真结果表明,该风险评估模型能够实时、准确地评估攻击节点的风险程度,其决策响应策略有效地提高了网络的安全性能.

## 2　基于风险评估的入侵响应决策模型

在分级 Ad Hoc 网络中,节点按照工作职责被划分为簇首、网关和簇成员.其中,簇首是簇结构的控制核心,网关是簇间通信的桥梁,这两类节点构成骨干网络,一旦出现问题,将直接导致簇结构性能下降,甚至造成全网瘫痪,因此在簇建立及维护的过程中应有针对性地加强对节点的安全监管.

为降低分级 Ad Hoc 网络在面临入侵行为时的性能损失,通过分析分级结构网络中节点的攻击特性,本文建立了一种实时风险评估安全模型,以适应分级 Ad Hoc 网络的安全需求.在该评估机制中,风险是指节点的攻击行为对网络造成的实际损失以及潜在的破坏程度,并将该值作为决策的重要依据.通过风险值量化风险的大小,节点的风险值越高,说明其安全程度越低,对周围节点的威胁程度越强.当入侵检测系统发现可疑路由攻击事件后,依据攻击样本属性的相似程度对样本进行聚类,分析簇结构中节点的性能变化趋势,实时计算统计可疑节点的风险值,以评估当前攻击对网络所造成的威胁程度,并结合节点状态等辅助信息预测攻击持续程度和规模,进而追踪可疑节点的安全状况,并将此作为决策的主要依据,针对不同的攻击节点采取不同的响应措施,以维护网络的通信质量,降低系统损失.

### 2.1　攻击样本聚类

自组织映射(self-organizing map,SOM)算法[13]是一种无监督自学习的聚类方法,通过模拟生物神经系统,自组织地将任意输入模式进行最佳匹配.借助 SOM 构建路由攻击样本聚类分析系统,摆脱了评判过程中的随机性以及参评专家主观上的不确定性等问题.由 SOM 构成的前向网络包括输入层和竞争层两层神经元,其结构如图 1 所示.

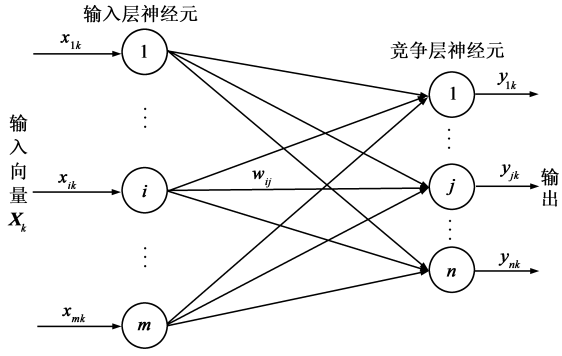


**图1　SOM网络结构图**

其中,$X_k=(x_{1k},x_{2k},\cdots,x_{mk})$为输入攻击特征向量的函数,$w_{ij}$为输入层神经元$i(i=1,2,\cdots m)$与竞争层神经元$j$ $(j=1,2,\cdots,n)$的连接权函数,$y_{jk}$为竞争层神经元$j$ 的输出向量,即输出攻击类别,处于同一类别中的向量具有特征相似性.在对攻击特征的描述中,分组转发率、控制开销、分组延迟、邻居节点数量、可疑节点身份等都可以作为特征向量.

设网络攻击样本集合为$\{X_1,\cdots,X_k,\cdots,X_p\}$$(1\leqslant k\leqslant p$ 且 $k,p\in N)$,则所有样本将按照某种标准属于设定的 $n$ 类输出模式之一,与该竞争神经元相连接的权函数包含本类模式的基本特征信息.其具体竞争学习步骤如下:

**步骤 1**　在满足 $\sum_{i=1}^{m}\sum_{j=1}^{n}w_{ij}=1$ 的条件下,赋予 $w_{ij}$ 随机初值.

**步骤 2**　按照某种确定的或随机的方式输入一个样本 $X_k$,计算输入层各神经元 $i$ 向竞争层各神经元$j$ 的加权输入激活值 $S_{jk}$,

$$S_{jk}=\sum_{i=1}^{m}w_{ij}x_{ik} \tag{1}$$

**步骤 3**　选取 $S_{jk}$中最大值所对应的神经元 $y_{jk}$为胜者,将其输出状态置为 1,其他竞争神经元的输出状态均置为 0,即

$$\begin{cases} y_{jk}=1 & ,(S_{jk}>S_{lk}) \\ y_{lk}=0 & ,\text{else} \end{cases} \tag{2}$$

如果出现 $S_{jk}=S_{ki}$ 的现象,则约定取 $j$ 值小的神经元为胜者.

**步骤 4** 设受到最大输入刺激的神经元 $j$ 在竞争中获胜,即 $j$ 满足

$$S_{jk}=\max_{j=1,2,\cdots,n}\{S_{jk}\} \tag{3}$$

建立 $j$ 的权矩阵 $W_j=(w_{1j},w_{2j},\cdots,w_{nj})$,式(3)可表示为

$$X_k\times W_j=\max_{j=1,2,\cdots,n}\{X_k\times W_j\} \tag{4}$$

等价于

$$|X_k-W_j|=\min_{j=1,2,\cdots,n}\{|X_k-W_j|\} \tag{5}$$

即具有权向量 $W_j$ 与输入向量 $X_k$ 最接近的竞争层神经元将获得竞争的胜利.

**步骤 5** 为使权值向量朝着趋近于输入向量的方向调整,与获胜神经元相连接的各权值按照式(6)进行修正,

$$w_{ij}'=w_{ij}+\Delta w_{ij} \tag{6}$$

其中,

$$\Delta w_{ij}=\eta\left(x_{ik}\Big/\sum_{i=1}^{n}x_{ik}-w_{ij}\right) \tag{7}$$

式(7)中 $\eta$ 为学习系数,表示连接权值的学习速率,一般 $0<\eta<1$.

**步骤 6** 选取样本集合$\{X_1,\cdots,X_k,\cdots X_p\}$中另一输入样本,返回步骤 3,直到 $p$ 个输入样本全部提供给网络.

**步骤 7** 返回步骤 2,对输入样本重复训练,直到满足训练 $t$ 次为止.网络训练次数一般取输入数据元素个数的 15~20 倍,经过 $t$ 次训练后,连接权的调整量都变得很小且分类结构不再变化.结束.

综上,从聚类的观点看,样本集被划分成了 $n$ 类,且每类样本在一定的距离测度上趋于最小,从而实现样本数据准确的无监督聚类.

## 2.2 风险程度分析

在判断一个系统安全与否时,涉及的影响因素很多,通过模糊理论表征它们相互之间存在的复杂关系,可以有效地克服评价过程中人为因素对评判结果的影响.在本安全策略中,根据 SOM 竞争神经元的分类结果和性能参数之间的相互影响,通过模糊综合评判将样本按照其攻击程度划分级别,并结合节点所处的网络环境,评估节点的风险程度.

模糊综合评判的评价目标是 SOM 竞争神经元输出的各类别路由攻击样本,提取各类别中向量的平均值组成因素集,以第 $j$ 个类别为例,其因素集为 $U_j=|u_1,u_2,\cdots,u_m|$.

设定评语集合 $V=|v_1,v_2,\cdots,v_s|$ 中各元素分别代表目标因素所能选取的风险评语,根据攻击风险与因素的关系可以建立第 $j$ 个类别的隶属度矩阵为

$$R_{m\times s}=\begin{vmatrix} r_{11} & r_{12} & \cdots & r_{1s} \\ r_{21} & & & \\ \vdots & \ddots & & \vdots \\ r_{m1} & \cdots & & r_{ms} \end{vmatrix}$$

以分组转发率作为风险因素为例说明隶属函数的取值.分组转发率是指在应用层信宿节点成功接收的分组数与信源节点发送的分组数的比值,该值反应了网络处理、传输数据的能力.设 $s=4,0.5<\delta<1$,表 1 列出了随分组转发率 $u_1$ 变化的隶属函数.

**表 1 分组转发率的隶属函数**

| | $r_{11}$ | $r_{12}$ | $r_{13}$ | $r_{14}$ |
|---|---|---|---|---|
| $0\leqslant u_1<0.25$ | 0 | $0.5(1-\delta)$ | $0.5(1-\delta)$ | $\delta$ |
| $0.25\leqslant u_1<0.5$ | 0 | $0.5(1-\delta)$ | $\delta$ | $0.5(1-\delta)$ |
| $0.5\leqslant u_1<0.75$ | $0.5(1-\delta)$ | $\delta$ | $0.5(1-\delta)$ | 0 |
| $0.75\leqslant u_1\leqslant 1$ | $\delta$ | $0.5(1-\delta)$ | $0.5(1-\delta)$ | 0 |

按照信息论的理论,当评价对象在某个风险因素上的值相差较大时,熵值较大,说明该因素提供的有效信息量较大,其权重也应较大.本算法依据评价对象在各因素上的数值差异程度,即信息效用值来确定各因素的权重,并考虑 Ad Hoc 网络的应用需求,对各因素的权重进行微调.权值的具体计算方法如下:

(1)假设有 $p$ 个攻击样本,每个攻击样本含有 $m$ 个评价因素,构建判断矩阵 $U$ 为

$$U=(u_{ik})_{m\times p} \tag{8}$$

(2)对 $U$ 进行标准化处理,消除因素间不同单位的影响,如式(9)所示:

$$x_{ik}=\frac{u_{ik}-u_{ik\min}}{u_{ik\max}-u_{ik\min}} \tag{9}$$

其中,$u_{ik\max}$和 $u_{ik\min}$分别为同一评价因素下不同评价对象中的最大值和最小值.

(3)根据传统信息熵概念,定义各评价因素的熵 $H_i$ 为

$$H_i=-\frac{1}{\ln p}\sum_{k=1}^{p}\frac{1+x_{ik}}{\sum_{k=1}^{p}(1+x_{ik})}\ln\frac{1+x_{ik}}{\sum_{k=1}^{p}(1+x_{ik})} \tag{10}$$

(4)计算各评价因素的熵权为

$$\omega_i=\frac{1-H_i}{m-\sum_{i=1}^{m}H_i} \tag{11}$$

(5)设对各风险因素的主观判定权值为 $\phi_i$,则得到因素 $i$ 的综合权值为

$$a_i=\frac{\omega_i\varphi_i}{\sum_{i=1}^{m}\omega_i\varphi_i} \tag{12}$$

从而得到权重矩阵为

$$A=|a_1,a_2,\cdots,a_m| \tag{13}$$

由此,可计算一个攻击类别的危险程度为

$$B = A \cdot R = \left| a_1, a_2, \cdots, a_m \right| \times \begin{vmatrix} r_{11} & r_{12} & \cdots & r_{1s} \\ r_{21} & & & \\ \vdots & & \ddots & \vdots \\ r_{m1} & & \cdots & r_{ms} \end{vmatrix} = \left| b_1, b_2, \cdots, b_s \right| \quad (14)$$

其中,$bi$ 代表评估结果隶属于第 $i$ 个风险级别的程度.

对模糊评估结果进行量化,可得攻击行为对网络造成的实际风险程度,即路由攻击的基本风险值 $r_{basic}$:

$$r_{basic} = 1 \cdot b_1 + 2 \cdot b_2 + \cdots + s \cdot b_s \quad (15)$$

为增强风险评估的准确性,还需考虑外界环境对攻击影响程度的潜在支持程度.其中节点度和相对移动性是评估节点物理性能的重要指标.本文以这两个指标为例进行说明.

节点度是指其一跳邻居节点的数目,分级结构网络中节点度越大说明簇结构覆盖密度越大.在分级 Ad Hoc 网络中,由于簇首负责为簇内其他节点提供路由及安全服务,若簇首出现故障,簇内其他节点的正常通信活动将难以进行.也就是说当簇首节点进行恶意攻击时,簇首节点的连接度越大,攻击所波及的范围越广,对网络所造成的危害也越大.

在分级 Ad Hoc 网络中,簇首节点频繁移动会导致簇内成员节点移进、移出簇的频率明显加大.移动性可以作为评估簇结构稳定性的重要指标,移动性越低说明节点间的相对位置变化越小.这里移动性指节点相对于其邻居节点的平均移动速度,即相对移动性.假设接收节点能够检测出接收的信号功率,根据弗里斯自由空间电波传播公式,通过从相邻节点接收的连续两个信号功率的比,就可知道此两节点间的相对移动速度.节点 $A$ 相对节点 $B$ 的移动性为 $M_{AB} = |10\lg(\frac{P_{new}}{P_{old}})|$,其中 $P_{new}$、$P_{old}$分别代表节点 $B$ 最近两次收到节点 $A$ 发送的分组功率大小.节点 $A$ 相对其周围所有邻居节点的移动性可表示为:$M_A = \frac{1}{n}\sum^{n} M_{AB}$,其中,$n$ 代表节点 $A$ 的邻居节点个数.

当簇首节点 $A$ 进行恶意攻击时,考虑其所处网络环境影响,计算综合风险值 $Risk$ 为

$$Risk = r_{basic} \times \left[1 + \frac{2}{\pi} \times \arctan(\frac{D_A}{D_m})\right] / \left[1 + \frac{2}{\pi} \times \arctan(\frac{M_A}{M_m})\right] \quad (16)$$

其中 $D_A$ 是节点 $A$ 的连接度,$D_m$ 和 $M_m$ 分别为最佳连接度和最佳移动性.借鉴文献[14],最佳连接度的计算考虑如下:若 $W_1$,$W_2$ 分别代表簇内、簇间的通信带宽,$N$ 代表节点个数,当 $N$ 足够大时,最佳簇个数 $M$ 表达为:$M = W_1\sqrt{N}/W_2$,则最佳连接度 $D_m$ 为:$D_m = N/M = W_2\sqrt{N}/W_1$.而最佳移动性的取值与网络的整体运行状态有关.

考虑到簇首能够监测到簇中各节点的行为更新,因此在本安全策略中,由簇首集中管理和存储其所在簇的相关风险信息,以便于开展决策响应工作.

### 2.3　决策响应策略

在分级 Ad Hoc 网络中,簇首负责为簇内其他节点提供路由服务,若簇首出现故障,簇内其他节点的正常通信活动将难以进行;两个簇首之间通过网关交换路由信息,若网关出现故障,簇间通信活动将无法进行;簇成员依赖簇首和网关实现与外界的一切通信活动.显然,这三种节点的重要程度是不同的,对各角色攻击节点应采取不同的响应措施.

根据分级 Ad Hoc 网络中节点的重要程度分布,引入风险作为决策的主要依据,以节点角色设置风险区间,确定目标的风险状态,并选择相应的响应方案.针对风险较高的入侵行为,选择比较严厉的响应措施,反之则选择比较温和的响应措施.以簇首节点为例,将风险等级设为高和低两类.若攻击簇首处于低风险状态,说明其攻击程度较轻,考虑到该节点在簇结构中的重要地位,且无其他节点可直接替代,为避免簇重构给网络带来更大的影响,采用容忍策略,暂时保留其节点身份,并实时监测其性能变化.当簇首节点进行高风险攻击时,迅速隔离恶意节点,并进行簇重构和路由重构,以保障网络正常运行.对于隔离期满可以重新入网的节点,要对其行为进行限制,剥夺部分权限,只允许其参加一些安全级别要求较低的通信活动.对于可以明确地判断的攻击行为,产生一个报警信息通知邻居和网络中的节点,警惕该节点的行为,保障网络安全.此外,还可将响应机制与信誉系统相关联,将风险程度作用于节点信誉,对于风险程度较低的可疑节点,令其信誉降低较慢,进而通过节点信誉值评估其状态.以上这些策略可以使入侵响应系统对网络中各种异常活动具有一定的耐受力,从而降低系统对网络异常活动的过度敏感性,进而降低由误响应引发的路由性能损失.

## 3　性能仿真

本文使用网络仿真软件 NS-2 搭建网络仿真平台,对基于风险评估的决策响应机制的性能进行测试.该模型由 100 个节点构成,并在 1000m × 1000m 的区域中以最大移动速度 10m/s 做随机运动,仿真时间 1000s.

攻击者往往通过影响网络正常通信对路由进行攻击.对于攻击者的这个目的,分组转发率、路由控制开销和平均延迟是评价路由安全性能优劣的重要指标.因此,仿真中选取这三个指标为攻击特征因素.

为了考察风险评估安全策略,以簇首滥发 RREQ 报文攻击为例,在网络不同负载情况下对安全机制的性能进行仿真分析.滥发 RREQ 报文攻击是一种主要的资源消耗攻击形式,攻击者尝试创建一些到根本不存在的节点的路由,由于无法得到应答,这些频频发送的路由请求在网络中不断扩散,导致网络中大部分带宽被恶意占用,从而使得其他节点无法正常使用网络资源,由于拥塞造成丢弃报文的可能性明显增大.

图 2 描述了在面临高风险的恶意攻击时,网络的分组转发率和控制开销变化情况.从中可以看出,由于恶意节点频频发送的路由请求在网络中不断扩散,导致网络带宽被大量恶意占用,从而使得其它节点无法正常使用网络资源,导致网络分组转发率降低,大量的路由请求导致网络的路由开销增大.采用基于风险评估的安全机制后,根据其风险程度迅速采取相应措施,将恶意节点隔离出网络,维持网络的正常运行,使网络具有较高的分组转发率,路由开销维持在正常的水平.在决策响应的措施中,相对于受到攻击时急剧增加的路由开销,安全机制由于簇重构产生的控制开销显得微不足道.

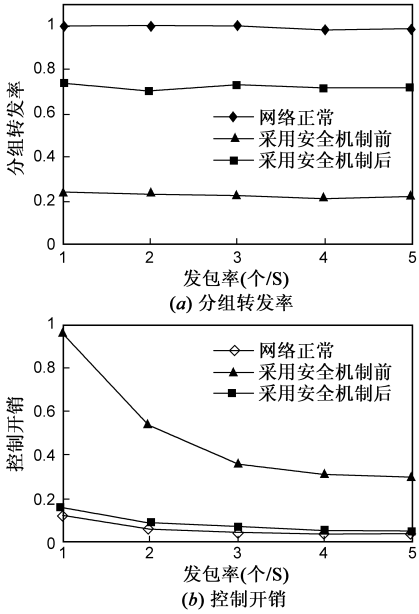


**图2 高风险攻击下路由性能比较**

图 3 描述了在面临低风险的恶意攻击时,网络的路由性能变化曲线.从中可以看出,采用直接隔离措施时,为维持网络正常工作,需要进行路由重构,分组转发率和控制开销有一定程度的损失;而采用风险评估的响应机制后,由于系统检测到攻击节点威胁程度较弱,且节点在网络中处于关键位置,故采取相对温和的响应措施,容忍该恶意节点的同时加强对该节点的实时监测力度,限制其某些异常行为,使网络仍能保持较高的分组转发率,监测带来的少量控制开销也是值得的.

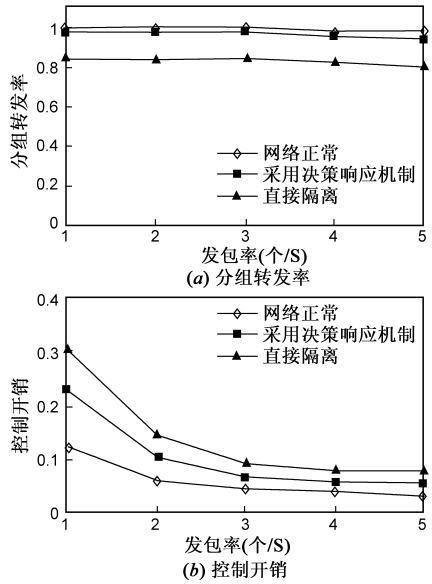


**图3 低风险攻击下路由性能比较**

## 4 结论

本文结合分级 Ad Hoc 网络的结构特点,提出一种基于风险评估的安全入侵响应模型.该模型从当前入侵对网络产生的客观影响出发,结合节点的攻击强度、角色特点、环境因素等多方面因素评估一个攻击节点对网络的威胁程度.通过计算攻击节点对网络造成的影响,将攻击样本进行分类,并根据网络对性能参数的重要性级别明确攻击样本的基本风险程度,再结合攻击节点所处的分级 Ad Hoc 网络环境,评估其潜在的威胁程度,得到最终的风险值.利用风险评估,可以更清晰地了解网络的安全态势,以便于开展高效的决策响应工作,维护网络的通信质量,降低系统损失.仿真结果表明,该风险评估模型能够实时、准确地评估攻击节点的风险程度,及时、有效地遏制或减轻路由攻击对网络的危害.

**参考文献:**

[1] Alexander Zemlianov, Gustavo de Veciana. Capacity of Ad Hoc wireless networks with infrastructure support [J]. IEEE Journal on Selected Areas in Communications, 2005, 23(3): 657 – 667.

[2] Satu Elisa Schaeffer, Stefano Marinoni, Mikko S, Pekka Nikander. Dynamic local clustering for hierarchical Ad Hoc networks [A]. Proceedings of SECON '06[C]. Virginia: IEEE press, 2006, 667 – 672.

[3] Meng-Yen Hsieh, Yueh-Min Huang, Han-Chieh Chao. Adaptive security design with malicious node detection in cluster-based sensor networks [J]. Computer Communications, 2007, 30(11 – 12): 2385 – 2400.

[4] Andre Konig, Matthias Hollick, Ralf Steinmetz. On the implications of adaptive transmission power for assisting MANET security[A]. Proceedings of ICDCS '09 [C]. Quebec: IEEE press, 2009, 537 – 544.

[5] S A Razak, S M Furnell, N L Clarke, P J Brooke. Friend-assisted intrusion detection and response mechanisms for mobile Ad Hoc networks [J]. Ad Hoc Networks, 2008, 6(7): 1151 – 1167.

[6] 江常青,张利,林家骏,吴世忠.一种基于系统安全性差距分析的风险评估尺度和方法[J].电子学报,2006,34(12A):2556 – 2559.
Jiang Chang-qing, Zhang Li, Lin Jia-jun, Wu Shi-zhong. A system security gap analysis based risk assessment metric and method [J]. Acta Electronica Sinica, 2006, 34(12A): 2556 – 2559. (in Chinese)

[7] 付才,洪亮,彭冰,韩兰胜,徐兰芳.移动自组网中非完全信息节点风险评估[J].计算机学报,2009,32(4):805 – 816.
Fu Cai, Hong Liang, Peng Bing, Han Lan-Sheng, Xu Lan-Fang. Incomplete information nodes risk assessment in mobile Ad Hoc networks [J]. Chinese Journal of Computers, 2009, 32(4): 805 – 816. (in Chinese)

[8] Jie Zeng, Jinquan Zeng. A dynamic immunity-based real-time network risk evaluation method[A]. Proceedings of ISBIM '08 [C]. Wuhan: IEEE press, 2008. 3 – 6.

[9] 李伟明,雷杰,董静,李之棠.一种优化的实时网络安全风险量化方法[J].计算机学报,2009,32(4):793 – 804.
Li Wei-ming, Lei Jie, Dong Jing, Li Zhi-tang. An optimized Method for real time network security quantification[J]. Chinese Journal of Computers, 2009, 32(4): 793 – 804. (in Chinese)

[10] Vasileios Karyotis, Symeon Papavassiliou. Risk-based attack strategies for mobile Ad Hoc networks under probabilistic attack modeling framework[J]. Computer Networks, 2007, 51(9): 2397 – 2410.

[11] Wenyuan Li, Jiaqi Zhou, Kaigui Xie, Xiaofu Xiong. Power system risk assessment using a hybrid method of fuzzy set and Monte Carlo simulation[J]. IEEE Transactions on Power Systems, 2008, 23(2): 336 – 343.

[12] Lei Wen, Zhaocai Xi. Supply chain risk evaluation based on fuzzy multi-criteria lattice-order decision-making [A]. Proceedings of ICAL'07[C]. Jinan, IEEE Press, 2007, 1442 – 1445.

[13] A. M. Kalteh, P. Hjorth, R. Berndtsson. Review of the self-organizing map (SOM) approach in water resources: Analysis, modelling and application [J]. Environmental Modelling & Software, 2008, 23(7): 835 – 845.

[14] Elizabeth M. Royer, P. Michael Melliar-Smith, Louise E. Moser. An analysis of the optimum node density for Ad Hoc mobile networks[A]. Proceeding of ICC'01[C]. Helsinki, IEEE Press, 2001. 857 – 861.

**作者简介:**

**于 尧** 女,1982 年 11 月生于辽宁省沈阳市,东北大学信息科学与工程学院博士研究生.主要研究方向为无线网络路由安全.
E-mail: yuyaosy@163.com

**郭 磊** 男,1980 年 4 月生于四川省眉山市,博士,现任东北大学信息科学与工程学院教授、博士生导师,主要研究方向为无线网状网、光网络生存性技术等.

**王兴伟** 男,1968 年 1 月出生于内蒙古包头市,博士,现任东北大学信息科学与工程学院教授、博士生导师,主要研究领域为下一代互联网、自组织网络和移动互联网等.