MANET 与 Internet 互联的自适应网关发现策略研究*)

徐 瑞 陈华胜 李伟华
(西北工业大学计算机学院 西安 710072)

摘 要 网关发现是 MANET 和 Internet 互联的关键技术。自适应网关发现策略是在混合网关发现策略的基础上对 TTL(hops)等参数动态调整以适应 MANET 的动态拓扑和不同网络环境的一种网关发现策略。本文指出自适应网关发现策略的关键问题是如何找到主动方法和被动方法之间的理想操作点。文章系统地介绍了目前自适应网关发现策略的研究进展,第一次给出了自适应网关发现策略的分类方法,最后结合该领域的研究现状指出自适应网关发现策略的一个发展方向,即在对 TTL 和 advertisement interval 等因素进行综合考虑的同时进一步控制 Reactive Zone 的范围。

关键词 移动自组网,Internet 互联,自适应网关发现

Survey of Adaptive Gateway Discovery Schemes for Connecting of MANET and Internet

XU Rui CHEN Hua-sheng LI Wei-hua
(Department of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract The gateway discovery scheme is a key problem of interconnection between MANET and Internet. Adaptive gateway discovery is based on hybrid gateway discovery, and according to dynamically adjusting TTL and other factors, adaptive schemes can fit dynamic nature and different scenarios of MANET. This paper indicates the key problem of adaptive gateway discovery schemes, which is how to select the optimal operating point between proactive and reactive strategies. The paper firstly presents a classification method after introducing recent representative adaptive schemes. Then different methods which these schemes used are compared and analyzed, including their commonness and characteristics. Finally, the future research issue in this area is pointed out.

Keywords Mobile Ad Hoc networks, Internet connectivity, Adaptive gateway discovery

1 引言

近年来,移动 Ad Hoc 网络(MANET)与 Internet 互联的问题逐渐成为了研究的热点。为了实现两者的互联,需要在 Ad Hoc 网络与 Internet 之间设置一种特殊的网关,它既能支持 Internet 网络的层次性路由机制,也能支持 Ad Hoc 网络中特定的路由机制,并且能够实现不同类型网络中节点间的通信。也就是说,这种网关是一个能够区别两网并能够中继分组的特殊节点,它是 Ad Hoc 网络与 Internet 互联的桥梁。网关发现[1,18]是 MANET 与 Internet 连接的一个关键技术。目前研究者们提出了一些网关发现策略,大致可分为主动网关发现方法、被动网关发现方法和混合网关发现方法。采用主动网关发现方法[2-4]就是网关周期性地全网广播网关通告消息;采用被动网关发现方法[5,6]的网关在有 Internet 接入需求的移动节点向网关发送网关请求消息时发送网关通告消息;混合网关发现方法是在主动与被动方法的基础上进行了一定程度的折中。

文献[7-9]采用了混合网关发现方法,方法使用固定的 TTL(time-to-live,即跳数值)限定网关广播网关通告消息的范围,在此范围之内采用主动方法,范围之外采用被动网关发现方法。对于不同的网络场景应选取不同的 TTL,不存在一个在任何场景和网络环境下都普遍适用的跳数值。同时,MANET 本身具有的动态性也导致了它与 Internet 的连接需求在不断改变。因此,研究者们设计了各种自适应网关发现策略,它们能够根据网络环境、节点移动性的不同而自适应地调整,从而最终达到平衡负载、优化网关发现策略的目的。

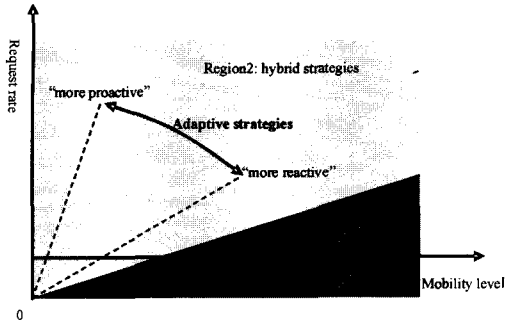
本文所做的工作是:1)指出自适应网关发现策略的关键问题;2)指出各个策略的特性与共性,给出了对目前各种自适应网关发现策略完整的分类方法;3)结合当前的研究现状指出自适应网关发现策略的发展方向。

2 自适应网关发现策略的关键问题

图 1 给出了采用自适应策略的范围,横坐标表示节点的移动性因素,纵坐标表示负载(节点发送网关请求消息的概率,简记为请求率)。当节点的移动性较低时,节点所存储的路由信息过时的可能性较低,网关只需要以相对低的频率广播其通告消息,这样就可避免移动节点频繁地被动发现网关。因此,在节点的移动性较低时,宜采用主动式网关发现方法;当节点的移动性较高时,宜采用被动网关发现方法。此外,当请求率较高时,宜采用主动网关发现方法;反之,宜采用被动网关发现方法。而当节点的移动性远远高于请求率时,宜采用完全被动方法。总之,当请求率增加或移动性减小时,自适应策略更趋近于主动方法;反之,则更趋近于被动方法。

从以上分析中,不难看出自适应网关发现策略的关键问题是如何找到主动方法和被动方法之间的理想操作点。如果将采用主动式网关发现方法的范围,即网关广播网关通告消

*)国家部委基金。徐 瑞 博士研究生,主要研究方向为高性能网络技术、多媒体通信技术;陈华胜 博士研究生,主要研究方向为多媒体通信技术;李伟华 教授,博导,主要研究方向为多媒体通信技术、决策支持技术。



（高移动性宜采用被动策略；高请求率宜采用主动策略）

图 1　自适应策略的范围

息的范围记作“Proactive Zone”，将在“Proactive Zone”范围之外的采用被动式网关发现方法的范围记作“Reactive Zone”，那么上述寻找主动与被动网关发现方法之间的理想操作点问题就进一步归结为：如何确定“Proactive Zone”的范围并且使这一范围能够根据移动 Ad Hoc 网络环境的改变而动态调整。大多数自适应策略都采用 TTL(hops)限定“Proactive Zone”的范围，TTL 的值越大，策略的主动性就越高。TTL=0，表示完全被动方法；TTL=NETWORK_DIAMETER，表示完全主动方法。理想的自适应策略应该使大多数有 Internet 接入需求的节点能够收到网关广播的网关通告消息而建立到网关的路由，只有极少数节点通过发送网关请求消息并接收网关单播回复的通告消息建立与网关的连接。

3　自适应网关发现策略的相关工作

到目前为止，研究者们已经提出了一些 MANET 与 Internet 互联的自适应网关发现策略[10-17]：文献[10]较早地提出了一个根据 Ad Hoc 网络的拓扑结构改变而自适应的网关发现策略。网关通告只发送给移动的节点。但是节点的活动探测机制依靠的是源路由协议，这在一定程度上限制了网关发现策略的应用性和可扩展性。为了获得和主动网关发现方法近似的 PDR(数据包发送率)，文献[11]采用 TTL = h_{max}(最大跳数值)作为网关广播下一次网关通告消息的范围，以使网关获得最大的源节点(source)覆盖率。然而，当大部分源节点都在网关附近，只有极个别源节点离网关较远的情况下，如果仍采用大跳数值，就会引入大量不必要的开销。同文献[11]一样，文献[17]的策略也是使网关获得最大的源节点覆盖率，网关根据被动接收、解析源节点发送的 RREQ-I，以了解源节点数量及 MANET 规模，自适应调整 TTL。为了解决文献[11]中存在的上述问题，文献[17]中规定当 80%的源节点离网关距离大于 5 跳时，选择 TTL= h_{max}作为网关广播下一次网关通告消息的范围；当 80%的源节点离网关距离小于 3 跳时，放弃本次网关通告，采用被动网关发现方法找可用网关。显而易见，文献[17]中的规定并不适用于所有的网络环境，因此不能从本质上解决文献[11]存在的问题。造成文献[11]这一问题发生的根本原因是没有考虑最大源节点覆盖率的开销。因此，文献[12]提出了一个基于“Maximal Benefit Coverage”的策略，解决了文献[11]中的问题。文献[13]提出了一个负载自适应的网关发现策略。文献[14]除了动态调整 TTL 之外，考虑到节点移动性因素，还对发送网关通告的时间间隔进行了动态调整。文献[15]在动态调整 TTL 的基础上采用中间节点来获取有用的本地信息，来进一步减少控制开销。文献[16]提出了一个动态调整网关广播网关通告消息频率结合可控消息泛洪算法的自适应策略。与扩大的环搜索算法相比，文献[16]提出的消息泛洪算法能够更有效地控制被动网关发现方法的开销。下一节将重点介绍目前研究者提出的各种典型的自适应网关发现策略[12-16]。

4　自适应网关发现策略详述

4.1　基于“Maximal Benefit Coverage”(MBC)策略

MBC 策略[12]指的是网关广播的 GWADV(网关通告，Gateway Advertisement)消息能够最大程度地发送到源节点，即 proactive zone 的范围最大化。这样就可保证大量的有 Internet 接入需求的源节点能够收到 GWADV 消息而找到网关，仅有少量的不在这一范围内的源节点采取被动发现的扩大的环搜索来找到可用网关。

网关将通过选择广播网关通告消息的 TTL(跳数)使节省的开销最大。也就是说，网关如果选择 TTL=t，则泛洪 GWADV 消息到 t 跳的开销加上源节点在大于 t 跳的距离网关发现的开销最小。每一个网关用式(1)计算 GWADV 消息在 TTL=t 的 benefit：

$$\beta(t)=N\cdot\frac{S(t)}{t(t+3)} \tag{1}$$

其中，N (网络中的节点数)表示全网泛洪消息的代价；$S(t)$ 函数表示与网关距离小于或等于 t 跳的活动源节点数，可由路由表“Source TTL”得到。$t(t+3)/2$ 是距离这一网关在 t 跳范围以内的所有节点的个数，其中把 2 省略掉。即在距网关 t 跳范围以内的活动源节点数与所有节点数的比率乘以全网泛洪的代价 N，当这个比率为 1 时，代价最大为 N。

MBC 策略的目标就是要找到使 $\beta(t)$ 最大的 TTL 值 t。那么，下一个网关通告消息泛洪的跳数值 TTL 为：当 $t\in[1\cdots t_{max}]$时，$\beta(t)=\max_{1\leqslant x\leqslant t_{max}}\beta(x)$。其中 t_{max} 即离网关最远的源节点的 TTL 值。

MBC 策略通过最大化 $\beta(t)$可以最大程度地避免有 Internet 接入需求的源节点通过网络泛洪找可用网关而引起的大量开销。这里的源节点采用的泛洪机制指被动网关发现策略采取的扩大的环搜索方法。

4.2　Load Adaptive (LA)策略

LA 策略[13]用式(2)计算 Proactive Zone 的初始值：

$$\Pr\ oactive\_zone(\Psi)=r\cdot\frac{N}{N_{IG}\cdot N_i} \tag{2}$$

其中 Ψ 是用 TTL 表示的 Proactive Zone，$r=\frac{N}{N_i}$为给定半径，N 为网络中所有的节点数，N_i 为有 Internet 接入需求的节点数，N_{IG}表示 Internet 网关。在时间间隔(Δ_{t1}，Δ_{t2})内，Proactive Zone 根据网络流量而动态调整。

为了计算负载，假定流量到达率是 λ，每个时间间隔的平均流量持续期为 T，考虑在两次连续估算之间的周期性的时间间隔长度为 $\Delta_t\{>1\}$，在 Δ_t时间间隔内，连接网关的路径数为 $n(\Delta_t)$，共有 $\lambda_1\cdot T_1,\lambda_2\cdot T_2,\cdots,\lambda_n(\Delta_t)\cdot T_n(\Delta_t)$条到网关的路径。假定数据包的大小是独立的，在时间间隔(Δ_{t1}，Δ_{t2})内，负载由公式(3)计算：

$$\rho=\sum_{i=1}^{n(\Delta t)}\lambda_i\cdot\sum_{j=1}^{n(\Delta t)}T_j=\sum_{i=1,j=1}^{n(\Delta t_1,\Delta t_2)}\lambda_i\cdot T_j \tag{3}$$

为了避免不必要地对 Proactive Zone 的频繁调整，策略引入两个阈值：最大极限值 γ_{max}和最小极限值 γ_{min}，其中$\gamma_{max}>\gamma_{min}$。如果 $\rho>\gamma_{max}$，那么 *Proactive Zone* 的值就加 1；反之，如

果 $\rho < \gamma_{min}$，那么 *Proactive Zone* 的值就减 1。换言之，如果 $\Psi(now)$ 是当前的 *Proactive Zone*，那么下一个 *Proactive Zone* 将是 $\Psi(now+\Delta_t)=\Psi(now)$ 或 $\Psi(now+\Delta_t)=\Psi(now)\pm1$。$\gamma_{max}$ 和 γ_{min} 分别是 $\rho+\rho*0.05$ 和 $\rho+\rho^*(-0.05)$。图 2 给出了 TTL 值的动态改变过程。

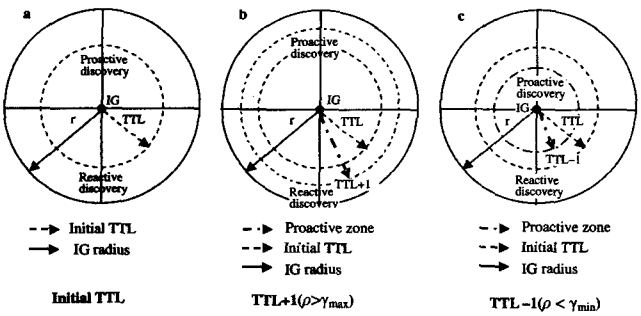


图 2　LA 策略中 TTL 的动态改变过程

4.3　动态改变 TTL 和 Interval(T&I)方案

T&I 方案[14]首先考虑网络中只有一个网关的情况：网关居于中心位置，所有具有 Internet 接入需求的节点围绕网关排好位置。到网关距离为 i 跳的节点数与那些到网关距离小于或等于 i 跳的节点数的比率用式(4)计算：

$$p_s(i)=(i^2-(i-1)^2)/i^2 \tag{4}$$

对于一个给定的 i，$P_s(i)$ 是固定的。

当网络中有多个网关时，按图 3 中的理想位置考虑：在阴影中的节点离最近的两个网关的距离是 i 跳且所有的节点都会选择一个最近的网关，如果两个网关到同一节点的距离相等，节点就任选一个网关。那么在阴影中的节点选择位于中心位置的网关的概率为 1/2。离网关 i 跳距离的节点数与那些距离网关小于或等于 i 跳的节点数的比率由式(5)计算：

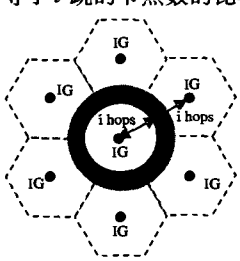


图 3　多个网关的理想分布

$$P_m(i)=\frac{\frac{1}{2}(i^2-(i-1)^2)}{(i-1)^2+\frac{1}{2}(i^2-(i-1)^2)} \tag{5}$$

在许多情况下，网关不会以这样的理想位置分布，所以这个概率值会在 $P_s(i)$ 与 $P_m(i)$ 之间分布，即

$$P_a(i)=(P_S(i)+P_m(i))/2 \tag{6}$$

这个值就是 TTL 的门限值。对于一个网关，假定有 Internet 接入需求的节点的最大跳数值是 H_{max}，离网关距离 x 跳的节点数是 $N(x)$，令

$$R(x)=N(x)/\sum_{j=1}^{x}N(j) \tag{7}$$

(分母表示距离网关 x 跳以内的所有节点数的总和)

通过比较 $R(H_{max})$ 和 $P_a(H_{max})$ 来确定 TTL 的值。如果 $R(H_{max})\geqslant P_a(H_{max})$，则当前的 TTL 值为 $H_{max}+1$；否则，$i=H_{max}$；执行 $i=i-1$ 直到 $R(i)\geqslant P_a(i)$ 或 $i=1$ 时，如果 $R(i)\geqslant P_a(i)$，则当前的 TTL 值为 $i+1$；否则，TTL$=i$。

T&I 策略除了对 TTL 值进行动态调整外，还考虑到节点的移动性问题：当节点的移动性高时，节点就会频繁进出当前网关的泛洪消息的范围，在这种情况下，网关就要缩小发送网关的通告时间间隔，这是为了给那些不断移进这一范围的节点以较新的网关通告消息从而缩小延时。反之，当节点的移动性低时，网络拓扑相对稳定，网关发送网关通告消息的时间间隔可以相应增大。T&I 策略采用在网关发送的两个相继网关通告之间向网关发送网关请求消息的节点数来表示节点的移动性，并从网关的角度给出了移动度的定义：移动度 MD 是在网关发送最后一个网关通告消息后发送网关请求消息的节点数与网关发送最后一个网关通告消息时通过这一网关与 Internet 通信的所有节点数的比值。如果 MD 的值大于门限值 β，网关将缩小发送网关通告的时间间隔；反之，网关将增大这一时间间隔。具体方法如文献[15]所述。

4.4　基于“Maximal Source Coverage”(MSC)策略

MSC 策略[15]中的最大源节点相关度[11]就是网关以到其所覆盖的源节点范围内最远的源节点的距离(hops)作为发送下一个网关通告消息的 TTL 值。对于每一个网关，用式(8)计算 $TTL=s$ 的概率(文中有实例，这里不再复述)：

$$P(TTL=s)=\sum_{i=1}^{s}\sum_{j=1}^{s}\cdots\sum_{k=1}^{s}p(i)\cdot p(j|i)\cdots p(k|i,j,\cdots),\quad i=s|j=s|\cdots|k=s \tag{8}$$

用式(9)计算平均 TTL 值：

$$s_{avg}=\sum_{I=1}^{\bar{N}-1}i\cdot p(\mathrm{TTL}=i) \tag{9}$$

网关发送下一个网关通告消息的 TTL 值就是 s_{avg}。

与 4.1－4.3 小节中的自适应策略不同的是，MSC 策略不但用 s_{avg} 限制了 Proactive Zone 的范围，而且为了控制被动网关发现方法产生的大量开销，规定了网关请求消息只在 Proactive Zone 之外发送，它们在整个 Reactive Zone 中广播。网关应答消息由位于 Proactive Zone 的边缘节点回复，而不是由某个网关回复。

4.5　Adaptive Frequency & Spiral Flooding (AF&SF)策略

AF&SF[16]策略通过指数退避算法(Exponential Bakeoff Algorithm)动态调整频率 f，通过螺旋式泛洪算法(spiral flooding algorithm)控制被动网关发现方法的开销。

定义 *Cost* 为整个网络流量，它包括主动式网关发现和被动式网关发现的开销，f 是网关广播通告消息的频率。令网络中每一个网关发出的一个通告的开销为单位开销，由主动网关发现方法引入的每一次请求(指有 Internet 接入需求的源节点发送的请求消息)的平均开销是 f。$P(f)$ 是 f 的单调递减函数，表示存储一条过时路由的可能性。令 $c_{controlled}$ 表示一个约束泛洪机制的开销，那么对每一次请求，由被动网关发现引起的平均开销是 $P(f)\cdot c_{controlled}$。$c_{controlled}$ 是一个常量，由约束泛洪算法给出，它定义为每一个有请求的移动节点为了找到至少一个网关所广播的平均消息数，$c_{controlled}<1$。那么，对于每一次请求，在时间 t 的总开销由式(10)得到：

$$C=f+p(f)c_{controlled} \tag{10}$$

AF&SF 策略通过动态改变频率 f 来找 Proactive 方法和 Reactive 方法的最佳操作点。将时间分成时隙，每一时隙内有 N 次请求。将主动广播通告消息的频率设置成每一次请求 $c_{controlled}$，网关计算移动节点发起被动网关发现的次数，用 $N_{discovery}$ 表示，$\frac{N_{discovery}}{N}$ 表示路径过时的可能性 $P(f)$，则(由式(10)得到)每一次请求的总开销为 $C=f+\frac{N_{discovery}}{N}c_{controlled}$。

在这 N 次请求之后，算法进入到两个无限循环中，分别记作 loop-down 和 loop-up。

在 loop-down 循环中，算法试图减少频率 f。通过乘以常量 β，且 $\beta<1$ 来使 f 减少。网关计算移动节点完成被动网关发现的次数，然后再次计算总开销，如果开销减少，算法将仍在此循环中执行并且继续减少频率 f，否则算法执行 loop-up 循环。在 loop-up 循环中，算法试图增加频率 f（通过乘以 $1/\beta$，且 $\beta<1$ 增加 f。如果开销减少，算法将仍在此循环中执行并且继续增加频率 f，直到开销不再减少；当开销增大，算法再次执行 loop-down 循环。可见，最佳的 f，即网关发送网关通告消息的最佳频率应该是 $f\cdot\beta<f<f/\beta,(\beta<1)$。

可控的消息泛洪算法原理如下：源节点分布于二维空间的四个象限中，以源节点自身为起始点（如图 4 所示），在 round1 中，S_1 向网络中的其他节点发广播消息，包括一个标志为 round1 的标志位、源节点的物理位置和表明其跳数 TTL 等信息。如果在第一象限的某一节点 I_1 收到这一消息，I_1 检查消息中的 TTL 值是否大于从 S_1 到 I_1 的最短路径。如果是，I_1 将继续广播这一消息。如果节点 I_2 在两个象限边界上，当收到 S_1 发的广播消息，如果这是最短路径，I_2 在路由表中存储这一路径，且不再广播这一消息。如果在 round1 之后，S_1 没有找到可用网关，它将在第二象限发起 round2，其 TTL 值比第一次泛洪 round1 中的大。同理，只有那些在第二象限的节点才继续广播 S_1 发出的广播消息。如果在 round4 之后，S_1 仍然没有找到可用网关，那么就再次发起 round5，直到找到可用网关。算法假定每一个节点通过 GPS 得知其位置信息，且节点不知道其他节点的位置信息。为了泛洪的需要，节点只是临时存储源节点到它自身的最短路径，否则也会引入大量的不必要的开销。

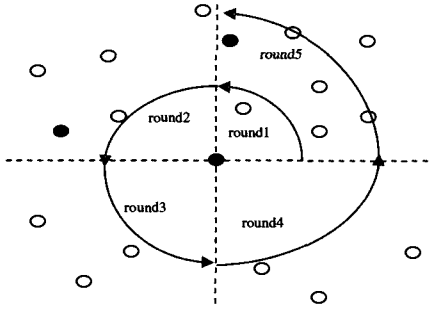


图 4　螺旋式泛洪算法

5　自适应网关发现策略分析

4.1—4.5 小节讨论了目前研究者们提出的最新的典型自适应网关发现策略，从中可以总结出目前自适应网关发现策略所采用的几种方法：方法(1)，通过动态改变 TTL 的值使网关广播网关通告消息的范围限制在 Proactive Zone 范围以内；在 Proactive Zone 范围以外，采用被动式网关发现方法，即有 Internet 接入需求的源节点通过一般的消息泛洪机制或通过扩大的环搜索算法找到可用网关。方法(2)，仍然通过动态改变 TTL 的值使网关广播网关通告消息的范围限制在 Proactive Zone 范围以内，采用中间节点获取有用的本地信息，进一步减少被动网关发现方法的开销。方法(3)，没有限制 Proactive Zone 的范围，采用可控的消息泛洪机制限制了 Reactive Zone 的范围。

4.1—4.3 小节中的 MBC 策略、AL 策略和 T&I 策略都属于方法(1)，通过动态调整 TTL 限制了 Proactive Zone 的范围，但是调整 TTL 的标准却不尽相同，MBC 策略根据有 Internet 接入需求的源节点数来调整 TTL 值；AL 策略用网络流量作为调整 TTL 的标准；T&I 策略则通过节点的分布作为调整依据。此外，T&I 策略还考虑到节点的移动性因素也会给自适应策略的性能带来一定影响，因此根据节点不同的移动度 MD，网关动态调整广播通告消息的时间间隔，但遗憾的是 T&I 策略并没有给出选取 MD 门限值 β 的方法。

然而，上述的 3 个自适应策略在 Proactive Zone 范围以外所采用的一般的消息泛洪机制或扩大的环搜索算法将会引入大量的开销，因此 4.4 小节的 MSC 策略（方法 2）对上述问题进行了改进：使网关请求消息只在 Proactive Zone 之外发送，它们在整个 Reactive Zone 中广播。网关应答消息由位于 Proactive Zone 的边缘节点回复，而不是由某个网关回复。

4.5 小节的 AF&SF 策略（方法 3）并未通过调整 TTL 来限制 Proactive Zone 的范围，而是限制了主动式网关发现方法中网关广播网关通告消息的频率，采用螺旋式泛洪算法限制了 Reactive Zone。对比扩大的环搜索算法，螺旋式泛洪算法可以大大减少被动网关发现方法消息泛洪的开销。

通过上述分析，本文给出对目前各种自适应网关发现策略的分类方法，如图 5 所示。

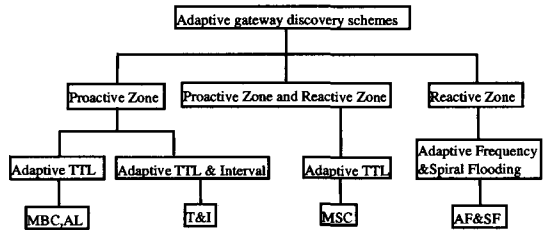


图 5　自适应网关发现策略的分类

结束语　自适应网关发现策略都是在混合网关发现策略的基础上发展而来的，其关键问题是如何找到采用主动方法和被动方法之间的最佳操作点。影响最佳操作点选取的关键因素包括：网关广播网关通告消息的范围（由 TTL 决定）以及网关广播通告消息的时间间隔（advertisement interval）或网关广播通告消息的频率（f 与 advertisement interval 互为倒数）。

目前的研究表明：在动态调整 Proactive Zone 范围的基础上控制源节点泛洪网关请求消息的范围（Reactive Zone）将进一步减少开销，因此自适应策略如何能够在对上述影响最佳操作点的关键因素进行综合考虑的同时还能进一步控制 Reactive Zone 的范围，这是自适应策略的一个发展方向，也是未来的研究重点。

参 考 文 献

[1] Xi J, Bettstetter C. Wireless Multi-hop Internet Access: Gateway Discovery, Routing and Addressing // Proceedings of the International Conference on Third Generation Wireless and Beyond (3Gwireless'02). San Francisco, USA, May 2002

[2] Jonsson U, Alriksson F, Larsson T, et al. MIPMANET-Mobile IP for Mobile Ad Hoc Networks // Proceedings of IEEE/ACM Workshop on Mobile and Ad Hoc Networking and Computing. Boston, MA USA, August 1999

[3] Sun Y, Belding-Royer E M, Perkins C E. Internet Connectivity for Ad Hoc Mobile Networks. International Journal of Wireless Information Networks, Special Issue on Mobile Ad Hoc Networks (MANETs): Standards, Research, Applications, 2002

[4] Jelger C, Noel T, Frey A. Gateway and Address Auto-configuration for IPv6 Ad Hoc Networks. IEFT Internet-Draft, draft-jelger-manet-gateway-autoconf-v6-02. txt, April 2004
[5] Broch J, Maltz D, Johnson D. Supporting Hierarchyand Heterogeneous Interfaces in Multi-hop Wireless Ad Hoc Networks // Workshop on Mobile Computing Held in Conjunction with the International Symposium on Parallel Architectures, Algorithms, and Networks. Perth, Australia, June 1999
[6] Wakikawa R, Malinen J T, Perkins C E, et al. Global Connectivity for IPv6 Mobile Ad Hoc Networks. Internet Engineering Task Force, Internet Draft (Work in Progress), Nov. 2002
[7] Ratanchandani P, Kravets R. A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks // Proceedings of IEEE Wireless Communications and Networking Conference (WCNC2003). New Orleans, USA, March 2003: 1522-1527
[8] Lee J, et al. Hybrid gateway advertisement scheme for connecting mobile ad hoc networks to the Internet // Proceedings of VTC 2003. Volume 1. April 2003: 191-195
[9] Shen Bin, Zou Li, Hu Zhong-Gong. Performance Comparison and Analysis of Three Gateway Discovery Protocols of Internet Connectivity for Ad Hoc Networks. Journal of Communication and Computer, 2006, 3: 53-58
[10] Lee J, Kim D, Choi Y, et al. Hybrid gateway advertisement scheme for connecting mobile ad hoc networks to the Internet // 57th IEEE Semiannual Vehicular Technology Conference (VTC2003). Jeju, South Korea, Apr. 2003
[11] Ruiz P M, Gomez-Skarmeta A F. Maximal source coverage adaptive gateway discovery for hybrid ad hoc networks // ADHOC-NOW 2004 (Lecture Notes in Comput. Sci. Vol. 3158). Vancouver, BC, Canada, July 2004
[12] Ruiz P M, Skarmeta A F G. Enhanced Internet Connectivity for Hybrid Ad hoc networks Through Adaptive Gateway Discovery // Proc. of the 29th Annual IEEE Conference on Local Computer Networks. 2004: 370-377
[13] Park B, Lee W, Lee C, et al. LAID: Load-Adaptive Internet Gateway Discovery for Ubiquitous Wireless Internet Access Networks // Proceedings of the International Conference on Information Networking 2006 (ICOIN 2006). Sendai, Japan, 2006: 349-358
[14] Zhang Kaijie, Xiang Yong, Shi Meilin. Adaptive Internet Gateway Discovery Scheme for Mobile Ad Hoc Networks // ChinaCom'06. Beijing, China, 2006, 10: 1-5
[15] Ros F J, Ruiz P M. Low Overhead and Scalable Proxied Adaptive Gateway Discovery for Mobile Ad Hoc Networks // IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS). Vancouver, BC, 2006: 226-235
[16] Jiang Hongbo, Jin Shudong. Design and analysis of adaptive strategies for locating internet-based servers in MANETs. Journal of Performance Evaluation of Elsevier, 2006: 464-479
[17] 沈斌, 石冰心, 李波. 基于自适应策略的移动自组网与 Internet 互联. 华中科技大学学报, 2006, 34(5): 5-8
[18] 胡中功, 邹莉, 沈斌. Mobile Ad Hoc Network 与 Internet 互联的技术研究. 武汉科技学院学报, 2005, 18(6): 65-69

(上接第 44 页)

服务请求，进行数据传输。实验选择 KDD Cup99 数据集[8]中代表性强的正常数据集 2000 个、攻击数据集 4000 个作为测试集。KDD Cup99 为 DARPA 产生的 7 周网络流量数据，包含大量的正常连接和各种攻击连接。为简化实验，通过网络检测来验证 gIDS 的入侵检测性能。

图 1 显示了在网络流量及测试集不断变化过程中，gIDS 和 Snort 的 ROC 曲线情况。由图中可以看出，基于智能网格的 gIDS 比 Snort 具有更高的检测率及更低的误报率，这是因为 gIDS 各组件继承了 IABS 的智能和协作等特性，能自动适应复杂的网格环境，更好地应用网格强大的计算能力对入侵行为进行协作检测，并通过灵活地采用与入侵特征更匹配的采集、分析算法，提高了系统的入侵检测性能。

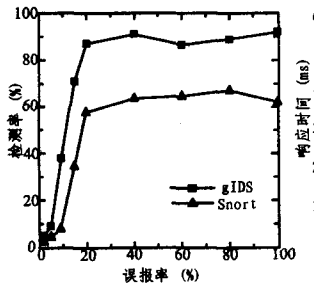


图 1 gIDS 和 Snort 的 ROC 曲线

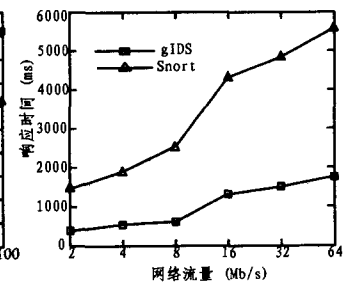


图 2 gIDS 和 Snort 的响应时间

图 2 中，网络流量在 2～64Mbps 范围变化时，首先采用 2000 个正常数据集、2000 个攻击数据集分别对 gIDS 和 Snort 进行攻击测试。当网络流量达到 8Mbps 时，再增加 2000 个攻击数据集继续进行攻击。图中显示出，gIDS 的响应时间明显小于 Snort，且随着网络流量的增加，gIDS 的响应时间变化更加平稳。当攻击变为更加复杂时，gIDS 的响应时间增幅较大，但因智能 Agent 的协调作用，使得之后 gIDS 的响应性能很快恢复平稳。而 Snort 由于攻击数据包的类型和数量突变，导致检测响应时间明显增加。结果表明，gIDS 能很好地适应网格平台特点，根据攻击的变化及时作出相应调整，将大量计算均衡地分布到各网格节点上，减轻了承担安全及管理任务的主机负担，提高了系统检测效率和灵活性。

结束语 网格环境的动态性、异构性和分布性等自身特点给基于网格的应用开发带来极大困难。本文结合智能 Agent 技术，提出并设计了基于 Agent 的智能网格模型 ICGM。ICGM 利用智能 Agent 的移动性和智能性等特性，很好地解决了上述问题。针对网格中安全问题的严峻性，设计了基于 ICGM 智能网格平台的入侵检测系统(gIDS)。gIDS 结合网格服务 API 和智能 Agent 开发，其代理组件继承了 IABS 的智能性和灵活性等特性。基于原型系统的实验表明，gIDS 在检测功能和效率方面体现出了很好的性能优势。下一步的工作重点包括平台健壮性和可靠性方面的研究，同时，智能 Agent 在自身安全性和智能性完善等方面仍存在诸多问题亟待研究。

参 考 文 献

[1] Tianfield H. Towards agent based grid resource management [C] // IEEE/ACM International on Cluster Computing and Grid (CC-Grid'05). Cardiff, UK, 2005: 9-12
[2] Casanova H, Dongarra J. NetSolve's network enabled server: examples and applications[C]. IEEE Computational Science & Engineering, 1998
[3] Kahn M, Cicalese CDT. The CoABS grid[C]. WRAC, 2002: 125-134
[4] Patel J, Teacy W T L, Jennings N R, et al. Agent-based virtual organisations for the grid[C] // Proc. 1st International Workshop on Smart Grid Technologies. 2005
[5] Overeinder B J, Wijngaards N J E, van Steen M, et al. Multi-Agent support for Internet-scale grid management[C] // Proceedings of the AISB'02 Symposium on AI and Grid Computing. April, 2002: 18-22
[6] Foster I. A globus toolkit primer[Z]. www.globus.org/primer, 2005
[7] Kruegel C, Toth T, Kirda E. Sparta-a mobile agent based intrusion detection system[C]. Network Security 2001, Leuven, Belgium, 2001
[8] The UCI KDD Archie. KDD99 Cup Datase[DB/OL]. http://kdd.ics.uci.edu/databases/kddcup99.html, 1999