MANET 与 Internet 互联中网关发现策略研究*)

徐 瑞 李伟华 李 由

(西北工业大学计算机学院 西安 710072)

摘 要 本文给出 MANET 和 Internet 互联的网关发现策略的分类方法,系统地描述了当前各种典型的网关发现策略,并比较和分析这些策略的优势与不足,最后结合该领域当前的研究现状,指出 MANET 和 Internet 互联的网关发现策略的发展方向。

关键词 移动自组网,Internet 互联,网关发现

Research of Gateway Discovery Schemes for Connecting of MANET and Internet

XU Rui LI Wei-hua LI You

(Department of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract This paper presents a class method of gateway discovery schemes for the Integrated Network of Internet and MANET, and introduces recent representative gateway discovery schemes of this Integrated Network. Then their advantages and disadvantages are compared. Finally, the future research issues in this area are pointed out.

Keywords Mobile Ad Hoc networks, Internet connectivity Gateway discovery

1 引言

移动自组网 MANET(mobile ad hoc networks) 是由一组带有无线收发装置的移动终端节点组成的多跳、临时性、无中心的自治网络。随着移动式计算的需求和便携式无线上网设备(如手提电脑、PDA 等)地不断增长,人们希望能够在任何时间、任何地点都能获得连续的、稳定的、优质的网络连接,因此 Ad Hoc 网络与 Internet 互联[1]的问题逐渐成为近年来研究的焦点。同时,随着 Internet 上实时多媒体业务的逐步展开,也促使人们考虑将 MANET 和基础设施的网络尤其是 Internet 网络互联,以拓展固定网络的无线应用空间。总之,只有将 MANET 和 Internet 网络互联起来,才能真正发挥 Ad Hoc 网络的潜能并最终实现全球网络的无缝隙化。

由于 Ad Hoc 网络与 Internet 采用的是不同的路由方式,要进行两者之间的无缝连接就需要在 Ad Hoc 网络与 Internet 之间存在一种特殊的网关,它既能够适应 Internet 网络的层次性路由机制,也能够使用 Ad Hoc 网络中特定的路由机制,并且能够实现不同网络中节点间的通信。也就是说,网关是一个能够区别两者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]是 MANET 与 Internet 连接的一个关键技术,也是近年来学者们研究的热点。本文将对网关发现问题进行深入的研究,给出关于 MANET 和 Internet 互联的网关发现策略的分类方法;在归纳和总结各种网关发现策略的基础上,对以上各种策略进行详细的比较和分析,指出各自的优势与不足;最后结合该领域当前的研究现状,指出 MANET 和 Internet 互联的网关发现策略的发展方向。

2 网关发现策略分类

目前,研究者们已提出了一些不同的移动 ad hoc 网络与 Internet 互联的网关发现策略。归纳起来可以将网关发现策略分成以下几类(如图 1 所示)。

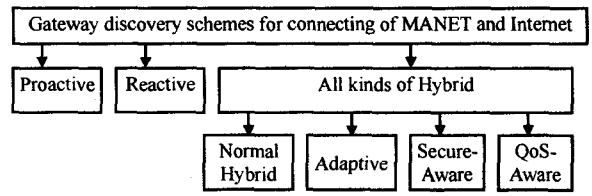

图 1 MANET 与 Internet 互联网关发现策略分类

3 网关发现策略详述

3.1 主动式网关发现

主动式网关发现[2-4]由网关自身发起。网关在 ADVERTISEMENT_INTERVAL 时间段内周期性地把网关通告消息(GWADVs)广播到所有的 MANET 节点,所有在网关传输范围内的移动节点都能够收到网关发送的 GWADVs 消息。在收到 GWADVs 消息之后,如果移动节点没有到此网关的路由,就在其路由表中为它创建路由项;反之,就更新到这个网关的路由项。之后,网关发送的通告消息就可以在其传输范围内的所有移动节点之间传输了。

主动网关发现主要都是利用移动 IP 的代理发现策略,Ad Hoc 网络通过外地代理(FAs)与 Internet 相连接。FA 基本上和 Internet 网关作用相同,它发送的代理通告可看作是 GWADV 消息。移动节点在收到代理通告之后,就能够知道全局的互联信息,如到 FA 的路由、FA 的 IP 地址、移动节点有可能和 Internet 进行互联的家乡地址,并将到网关的路由作为默认路由插入路由表。

3.2 被动式网关发现

被动式网关发现方法是网关不主动广播网关通告信息。

*)国家部委基金(编号:9140A17050206HK03)。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;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。

当MANET中的节点有Internet要求而自己的路由表中又没有到网关的默认路由，或者当自己保存的网关信息需要更新的时候，就主动发起网关发现过程，即广播网关请求消息(GWSOLs)来找到可用网关[5,6]。大多数被动网关发现策略在Ad Hoc网络内部都采用Ad Hoc按需路由协议(如DSR和AODV)。网关请求(GWSOL)包含在MANET路由协议的路由请求(RREQ)消息中，当移动节点需要与Internet互联时，每一个移动节点都会创建一个RREQ_I请求消息到MANET的所有网关的IP组播地址(ALL_MANET_GW_MULTICAST)，中间节点收到此信息后仅仅是重新广播该信息，直到网关收到该请求信息后单播回复一个包含网关IP地址等信息的应答信息(RREP_I)给发起请求的节点。收到此应答信息后，节点就可以生成一个到网关的路由。

3.3 混合网关发现

混合网关发现方法[7-14]是主动和被动方式的综合。网关在一定(半径)范围内发送网关通告信息，即采用主动方式；在此范围之外的节点若要与Internet通信，则采用被动方式。

3.3.1 一般混合网关发现方法

文献[7,8]用TTL(time-to-live)值将网关广播GWADV消息限制在网关周围n跳以内。在此范围之外的节点，如果有Internet接入要求，则自己发送网关请求报文来获取网关信息。文献[9]在网关可移动的最大跳数范围内网关发送GWADV消息，最大跳数值由ADVERTISEMENT_ZONE决定。超出这一范围的移动节点，若要获得网关信息，就广播一个RREQ_I消息到ALL_MANET_GW_MULTICAST地址，收到RREQ_I消息的中间节点继续广播之，直到网关收到RREQ_I消息后再向发起这次请求的移动节点回复一个RREP_I消息作为应答。

以上各种混合方案所限定的跳数值都是固定的，但是MANET本身具有的动态性导致它与Internet的连接需求在不断改变，因此不存在一个在任何的场景和网络环境下都普遍适用的跳数值，必须使这一跳数值能随着网络环境的动态改变而改变。因此，研究者们设计了各种自适应网关发现方法。

3.3.2 自适应网关发现

文献[14]给出了一个负载自适应的网关发现方法。网关(AG)周期性地广播带有负载信息的网关通告(AGA)消息，从AGA消息中可获得网络中节点的总数、与Internet互联的源节点数及网络的规模等信息。用式(1)计算初始的TTL值(proactive area的范围)：

$$\text{Proactive\_area}(\mathcal{R})=\left|\frac{A}{\sum_{i=1}^{N}2P}\right|\times 0.1 \tag{1}$$

其中R表示TTL值，A是网络的大小，一般定义为一个给定长、宽的长方形区域；N是网络中的移动节点数；P是数据包的大小。用式(2)计算负载load(ρ)：

$$\rho=(\lambda_1+\lambda_2+\cdots+\lambda_n)\times(k_1+k_2+\cdots+k_n)=\sum_{i=1,j=1}^{n}\lambda_i k_j \tag{2}$$

其中λ是每个时间间隔平均流量到达率，k是每个时间间隔平均的数据包长度，n是与这个网关连接的所有节点数量。ρ的单位为bytes/s。对于时间间隔也要进行动态调整，即在网络流量大及节点高速移动的情况下，时间间隔将变小。反之，时间间隔将变大。

为了能够使网关广播GWADV消息的范围(proactive area)随网络负载的变化而动态改变，引入两个阈值：θ_{max}(max threshold)和θ_{min}(min threshold)，$\theta_{max}>\theta_{min}$。如果$\rho>\theta_{max}$，那么proactive area的值就加1；反之，如果$\rho<\theta_{min}$，那么proactive area的值就减1。θ_{max}和θ_{min}分别为$\rho+\rho\cdot\xi$和$\rho+\rho\cdot-\xi$)，$\xi=\left|\frac{\rho-\nabla\rho}{\rho}\right|$，其中$\rho$为当前负载，$\nabla\rho$是过去的负载。换言之，如果$\mathcal{R}$(now)表示当前的proactive area，下一个时间间隔的proactive area就变成$\mathcal{R}$(now+Γ) $=\mathcal{R}$(now)或$\mathcal{R}$(now+Γ) $=\mathcal{R}$(now)$\pm$1。

图2给出了TTL值的动态改变过程。如图2所示，在proactive area的x跳以内的移动节点接收从网关周期性发送的AGA消息。在此范围之外的移动节点广播网关请求消息(AGRQ)，在proactive area之内的与某个网关相连的移动节点或是回复给发起请求的节点AGRP消息，或继续中继AGRQ消息到其它网关。当网关收到AGRQ消息后，网关发送带有网关前缀和其它相关信息的AGRP消息到发起这次请求的移动节点。

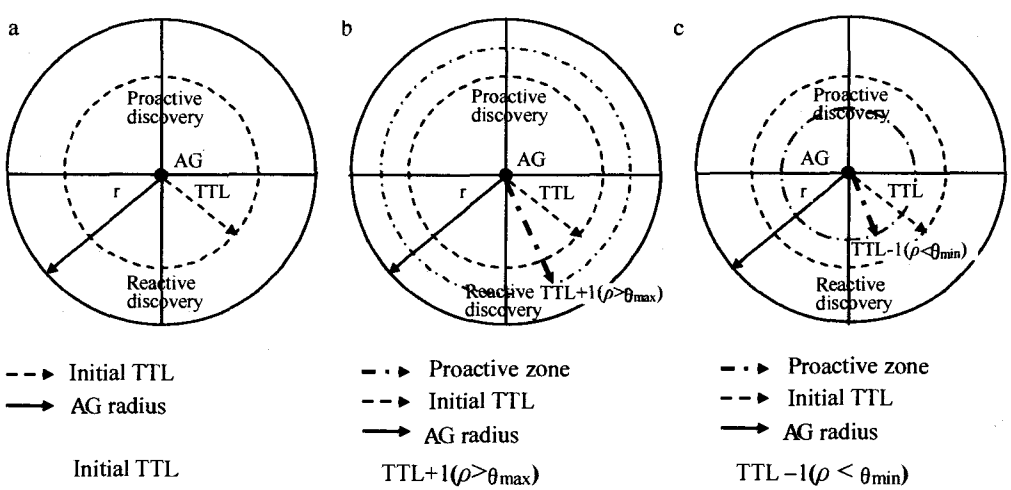

图2 TTL的动态改变过程

3.3.3 安全网关发现

3.1-3.4小节中各种不同的网关发现方法都假定网络环境是可信赖的，没有考虑网络环境中存在的各种不安全因素：那些未被授权的访问可能会妨碍Internet的连接；在MA-

NET 中广播消息也会增加潜在的不安全性；同时，通信的物理介质本身也是不安全的。总之，对网络互联的攻击是由那些恶意节点通过修改、丢弃或生成与移动 IP 相关的信息（如广播通告、注册请求或应答消息等）造成的。因此，为了保证 Internet 与 MANET 互联需要考虑安全性因素。

文献[10]设计了一个安全网关发现协议（SDP）。采用 ISMANET[11] 协议作为安全发现协议。ISMANT 用基于身份的签密（signcryption）方案来发现网关。移动节点首先用其公钥和私钥（PK_{AMN}，SK_{AMN}）注册到家乡网关（HIG，即家乡代理），然后寻找到外地网关（FIG，即外地代理）的路径。当移动节点找到到外地网关的最优路径时，注册到这个外地网关。安全网关发现过程如图 3 所示，其中各符号的定义见表 1。

1. FIG→broadcast: IGAM ‖ ID_{FIG} ‖ Sig_{FIG}{H(IGAM ‖ ID_{FIG} ‖ t_{FIG})}
2. AMNs→AMNx: IGRQ ‖ ID_{AMNs} ‖ t ‖ Sig_{AMNs}{H(IGRQ ‖ ID_{AMNs} ‖ t)}
3. AMNs→FLG: IGRQ ‖ ID_{AMNs} ‖ ID_{AMNx} ‖ t ‖ t_x ‖ Sig_{AMNs}{H(IGRQ ‖ ID_{AMNs} ‖ t)}
4. FIG→AMNx: IGRP ‖ ID_{FIG} ‖ t ‖ t_{FIG} ‖ Sig_{FIG}{H(IGRP ‖ ID_{FIG} ‖ t ‖ t_{FIG})}
5. AMNx→AMNs: IGRP ‖ ID_{FIG} ‖ ID_{AMNx} ‖ t ‖ t_{FIG} ‖ t_{AMNx} ‖ Sig_{FIG}{H(IGRP ‖ ID_{FIG} ‖ t ‖ t_{FIG})}

图 3　安全网关发现过程

表 1　安全网关发现中各符号的定义表

Symbol	Definition	Symbol	Definition
IDx	Identification of node X	$H(m)$	One-way hash function
SK^*	System master key	SKx, PKx	Private key and public key of X
t	Secure token	K	Shared secret key
$e(P, Q)$	Bilinear map based on the Well	P, P_{pub}	Generator, Master secret key-P

网关周期性地广播网关通告（IGAMs）消息：$\langle IGAM \| ID_{FIG} \| Sig_{FIG}\{H(IGAM \| ID_{FIG} \| t_{FIG})\}\rangle$，包括 FIG 的地址、消息序列号、CoA（家乡地址）及其验证信息。其中，t_{FIG} 是 FIG 的安全令牌。签名 Sig 定义如下：Sig＝Signcrypt（security parameters，private key，message）。采用 TTL 使网关广播 IGAM 消息的范围限制在 n 跳以内。采用负载自适应的网关发现方法（LAID[12]）来动态调整这一范围（proactive area）。在 proactive area 这一范围内，即 x 跳之内的移动节点接收网关通告消息 IGAM。如果移动节点在 x 跳以外，则向网关发送请求消息（IGRQs）。移动节点 S 选择任意数 r 并用公式 $k=\hat{e}(P, Ppub)^r$ 计算 IGRQ 消息的来源。S 发送的 IGRQ 消息、安全令牌及创建的所有值都要被签名。当中间节点 X 收到 IGRQ 后，首先检查源节点的签名，然后 X 用公式 $k'=\hat{e}(P, SK_{AMNS})*\hat{e}(Ppub, PK_{AMNS})^r$ 计算消息的来源，同时用 $t=H(ID_{AMNS} \| SK^*)$ 来检查发送节点的有效性。签名的验证定义如下：valid＝Unsigncrypt（Sig，public key，security parameters，message）。Valid 是一个二进制值，当其为 0 时表示签名无效，为 1 时表示签名有效。如果验证通过，S 和 X 之间是可信赖的。验证之后，中间节点 X 用上文同样的方法计算 X 的安全令牌（t_{AMNX}），然后 X 继续向下一节点广播 IGRQ 消息。当 FIG 收到 IGRQ 消息后，它先验证签名并计算 t 和中间节点 X 的安全令牌。如果验证通过，FIG 就将回复应答消息，否则丢弃 IGRQ 消息。当移动节点 S 收到带有验证信息的 IGRP 消息时，不仅要检验回复给 FIG 的验证信息，还要验证 FIG 的签名。如果对数字签名和安全令牌的验证顺利通过，到 FIG 的安全路由就建立起来了。

3.3.4　考虑 QoS 的网关发现

以上所有的网关发现方法都只考虑了“尽力而为”（best-effort）型服务，对实时的多媒体应用却没有考虑。为了在 MANET 和 Internet 互联的混网中能够传送实时媒体流，文献[13]提出了一个保障一定服务质量 QoS（这里的服务质量指的是端到端延时）的网关发现方法，仍然采用 AODV 路由协议以及移动 IPV6 技术对 MANET 和 Internet 进行互联。

网关在发送 GWADV 消息之前，首先检查实时数据流是否满足 QoS 要求，即每一个网关在最后的一个时间间隔 t 秒内检查它是否收到了 QoS_LOST 消息。QoS_LOST 消息是由有实时应用需求的目的节点（fixed node）发送给那些不能满足 QoS 要求的源节点的。发送实时媒体流的源节点的端到端延时，若超过了某一阈值（如 140ms），就不满足 QoS 要求。采用将时间戳（timestamp）或数据包生成的时间添加到 RTP 协议的 header 中的方法计算实时媒体流的端到端延时。如果网关没有收到 QoS_LOST 消息，就广播网关通告 GWADV；否则网关计算 $\alpha(t)=\frac{P}{F}$，其中 P 表示存在延时问题的发送实时数据的源节点的数量，F 表示用这个网关进行通信的所有源节点的数量。如果 $\alpha(t)>\gamma(0\leqslant\gamma\leqslant)$，网关不发送任何 GWADV 消息到 MANET。这是因为：在实时媒体流已经因为网络拥塞存在 QoS（延时）问题的情况下，如果网关再发送 GWADV 消息，就会进一步加重网络负载。如果 $\alpha(t)=\gamma$，网关继续发送 GWADV 消息。值 γ 广义上来说就是一个上限，这个上限值表示一个新的媒体流不能达到 QoS 要求的概率。因此，具有较低 γ 值的网关就能更好地满足媒体流的 QoS 要求。

用 TTL 值将网关广播 GWADV 消息的范围限定在距离网关 n 跳之内，在这一范围以外的移动节点若要与固定节点通信就发送网关请求消息，然后等待某个网关做出应答。收到网关的应答信息后，移动节点就可以生成一个到网关的路由。

4　比较和分析

上文按照网关发现策略的分类从不同角度讨论了一些典型的 MANET 与 Internet 互联的网关发现策略。主动式网关发现方法能够提供不错的互联性和低延时，但因为它采用周期性地全网广播网关通告消息而使方法的开销很大。被动式网关发现方法因为只在节点有互联需求时才发送网关请求消息，因而降低了路由开销，但却增加了延时。混合式策略是主动方法和被动方法的折中，它限定了网关广播网关通告消息的范围（proactive area），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。相比单纯的主动与被动方法，采用这种混合方法在路由开销较合理的范围内可以获得较好的互联性和较低的延时。但是，3.3.1 小节给出的混合方案中 proactive area 是固定的。当网络环境发生动态改变时，所限定的这一范围就有可能不再适用，这样就势必影响到整个方法的性能。3.3.2 小节给出了一个负载自适应的网关发现方法，它能够根据网络流量及网络中节点数动态调整 proactive area。仿真实验[14]结果表明，负载自适应的网关发现方法比混合方法的性能更优，且随着网络流量和规模的不断变化具有良好的可扩展性。

3.3.3 小节给出的基于安全考虑的网关发现方法可以对

（下转第 137 页）

4.4 实验 2

依据式(20)给定的的概率密度函数，随机生成 500 个真实模式。分别独立地对每一个真实模式进行 500 次 Monte-Carlo 仿真实验，每次实验观测 150s，即 30 次采样。通过全部位置联合估计的 RMSE 比较 ME-IMM 与集合 G 中各元素的性能，$G=\{\text{IMM}|\ M=\{m(1)=-w°/\text{s},\ m(2)=0°/\text{s},\ m(3)=w°/\text{s}\},\ w\in\{3:0.1:7\}$，$w$ 表示 M 中固定转率最大值。图 4 给出了 G 中各元素的全部位置联合估计的 RMSE，ME-IMM 的全部位置联合估计的 RMSE 为 126.63m。

结束语 本文分析了 IMM 算法在实际操作中存在的模型与真实模式之间可能存在差异及其可能可能造成的影响。通过使用模型误差这一概念将这种差异体现出来，提出了一种基于模型误差的交互式多模型算法。仿真结果表明，ME-IMM 比 IMM 更好地避免性能恶化，并且当真实模式保持不变时从全局角度考虑，ME-IMM 要优越于 IMM。

在本文中假设了 $e_k^{(i)}$ 与其它量无关。然而当真实模式保持不变时，$e_k^{(i)}$ 与 $e_t^{(i)}$，$t<k$ 是相关的。如何将这种关系更好地表示，以改进 IMM 性能，将是下一步可以研究的问题。

参 考 文 献

[1] Biom H A P, Bar-Shalom Y. The interacting multiple model algorithm for systems with Markovian switching coefficients [J]. IEEE trans on Automatic Control, 1988,33(8): 780-783

[2] LI X R, Bar-Shalom Y. Performance prediction of the interacting multiple model algorithm [J]. IEEE trans on Aerospace and Electronic Systems,1993, 39(3): 775-771

[3] LI X R, Jilkov V P. Survey of maneuvering target tracking. part V: multiple-model methods [J]. IEEE trans on Aerospace and Electronic Systems, 2005,43(4):1255-1321

[4] LI X R,Zhao Zhan Lue, LI Xiao Bal. General model-set design methods for mulitple-model approach [J]. IEEE trans on Automatic control, 2005, 50(9): 1260-1276

[5] Zhao Zhan Lue, LI X R. The behavior of model probability in multiple model algorithms[c] //Proc. 2005 Int Conf on Informational Fusion. 2005:331-336

[6] LI X R. A survey of maneuvering target tracking. part I dynamic models[J]. IEEE trans on Aerospace and Electronic Systems, 2003, 39(4): 1333-1364

[7] Kirubarajan T, Bar-Shalom Y. Kalman filter versus imm estimator: when do we need the latter[J]. IEEE trans on Aerospace and electronic systems, 2003, 39(4): 1452-1457

(上接第 101 页)

抗恶意节点的攻击及提供一定的容错能力，可用于有安全需求的应用中。由于这一方法也可以对 proactive area 进行动态调整，因而方法的可扩展性较好。但因为要进行安全认证，却引入了一些开销。为了能够在 MANET 和 Internet 互联的混网中传送实时媒体流，3.3.4 小节给出了一个实时的网关发现方法。对于 VoIP 这种实时媒体流，仿真试验表明[13]考虑 QoS 的网关发现方法在端到端延时、分组传送率、路由开销等方面均优于一般的混合方法。但是这一方法因为采用固定的 proactive area 而影响到整个方案的可扩展性。各种网关发现策略特点见表 2。

表 2 网关发现策略特点比较表

schemes	connectivity	latency	overheads	scalability	proactive-area(TTL value)
Proactive	best	lowest	highest	—	—
Reactive	worst	highest	lowest	—	—
Hybrid	middle	middle	middle	—	fixed
Adaptive	better	lower	lower	good	dynamic
Secure-Aware	better	lower	low	good	dynamic
QoS-Aware	better	lowest	low	not good	fixed

结束语 本文给出了移动 Ad Hoc 网络和 Internet 互联的网关发现策略的分类方法，系统地描述了当前各种典型的网关发现方法。从上述分析可以看出：单纯采用主动式或被动式的方法要么牺牲路由开销，要么牺牲延时，因此研究者们采用主动与被动的混合策略在一定程度上进行了折中。对于所有的混合策略，确定网关周期性广播网关通告消息的范围(proactive area)是关键问题。

尽管对 MANET 和 Internet 互联的网关发现策略的研究得到了很大进展，还有一些问题有待于进一步研究：如何更合理地选取 proactive area，使网关发现方法具有更好的稳定性和可扩展性。如何更好地提供 QoS 保证，是网关发现策略所面临的挑战和发展方向。

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 HocNetworks//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] Park B, Shin C. Securing Internet Gateway Discovery Protocol in Ubiquitous Wireless Internet Access Networks//Proceedings of IFIP International Conference on Embedded & Ubiquitous Computing (EUC'2006). Seoul, Korea, August 2006

[11] Park B, Lee W. ISMANET: A Secure Routing Protocol Using Identity-based Signcryption Scheme for Mobile Ad-hoc Networks. IEICE Transaction on Communications, 2005,E88-B(6)

[12] 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 (ICOIN) 2006. January 2006

[13] Domingo M C. Integration of ad hoc networks with fixed networks using an adaptive gateway discovery protocol, Intelligent Environment,2006, 1:371-379

[14] Park B, Lee C. QoS-aware Internet access schemes for wireless mobile ad hoc networks. Elsevier Computer Communications (COMCOM), 2007,30(2): 369-384