

异构网络中高效切换认证算法研究 *

刘二刚, 黄开枝, 金 梁

(国家数字交换系统工程技术研究中心, 郑州 450002)

摘 要: 提出了一种异构网络高效切换认证算法, 包括目标切换网络的软预测机制和基于上下文传递的融合认证机制。该算法在集中式认证机制的基础上进行改进, 先通过层次邻居图法来快速确定目标切换网络, 然后协商、传递会话密钥和信任材料等相关上下文信息, 尽可能减少移动终端与家乡网络的认证交互, 提高了切换重认证的效率。

关键词: 异构网络; 融合认证; 上下文; 软预测机制

中图分类号: TP393. 03

文献标志码: A

文章编号: 1001-3695(2009)07-2698-03

doi:10.3969/j.issn.1001-3695.2009.07.084

Research on efficient algorithm of handoff and authentication in heterogeneous networks

LIU Er-gang, HUANG Kai-zhi, JIN Liang

(National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: This paper proposed an efficient algorithm of handoff and authentication in the heterogeneous networks, which contained two parts: soft prediction mechanism of target network for handoff and integrated authentication technique based on context transfer algorithm. Improved the algorithm based on centralized authentication method. The soft prediction mechanism could predict the target network quickly, so the integrated authentication technique could generate and transfer the security credentials and session key efficiently. Because of the mechanism, it could reduce the number for intercourse between mobile terminal and home networks. So, the method could decrease the latency for re-authentication.

Key words: heterogeneous networks; integrated authentication; context; soft prediction mechanism

目前,受带宽和覆盖范围的限制,单一一种无线网络难以满足用户所有的通信需求,因此多种无线通信网络在很长一段时间内将会并存。为了得到普适和高效的网络服务,异构无线网络的无缝融合显得尤为重要。国内外一些院校和研究机构正在对 3G/WLAN/WiMAX 的异构互连进行研究^[1]。

移动终端(MT)接入访问网络时,必须要相互认证后才能安全通信。大部分融合网络的认证方法均采用访问网络与家乡网络协作认证的方式,称为集中式认证机制(图 1)。每次认证时,访问网络都必须与家乡网络进行认证消息交互,这会带来巨大的消息开销和时间延迟,使切换性能下降,严重时可导致用户服务中断。

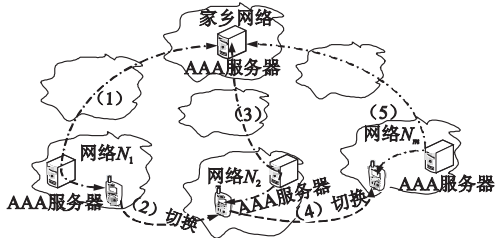


图1 集中式认证机制

为解决此问题,国内外提出了一些解决方案,主要包括:基于消息捎带的策略,在认证消息中捎带移动注册消息以减小认

证延时;基于二层暗示的策略,利用二层触发信号,在移动节点移动到新子网前,就开始认证和预切换处理;基于移动 IP 增强协议的策略,将接入认证与移动 IP 的增强方案结合以提高认证切换性能^[2]。但以上方法只考虑了如何结合认证和切换过程,忽略了认证框架下所采用的具体认证方法和移动切换中的安全问题,特别是认证安全和数据传输安全。

本文针对异构网络的特点,提出了一种融合网络的高效切换认证算法——基于集中式认证的融合改进认证算法。它充分结合异构网切换和认证的具体协议,一方面运用基于层次邻居图的软预测机制来提前确定目标切换网络;另一方面用上下文传递的方法传送相关认证信息,为重认证提供信任材料支撑,而不必每次都与家乡网络进行交互。如果当前网络传递给下一网络的信任材料,由于链路中断或是超过缓存时效丢失时,根据需要通过与家乡网络交互获得。这样,用户在异构网络间移动时,就可以减少切换认证延时,用户身份和传输消息的安全性也可得到增强。

1 基于软预测的快速切换设计

要做到异构网络间的无缝快速切换,就必须先要了解各邻居网络间的拓扑结构,还需要 MT 与网络协同工作,建立终端与网络、网络与网络间的安全关联^[3]。在不同的网络环境下,

收稿日期: 2008-11-03; 修回日期: 2008-12-10 基金项目: 国家“863”计划资助项目(2007AA01Z434)

作者简介: 刘二刚(1983-),男,河南平顶山人,硕士研究生,主要研究方向为第三代移动通信及网络安全(leg413@tom.com);黄开枝(1973-),女,副教授,硕导,主要研究方向为第三代移动通信及异构无线网络的安全;金梁(1969-),男,教授,博导,主要研究方向为第三代移动通信及阵列信号处理。

还要尽快确定符合用户需求的目标网络。

基于以上考虑,本章提出了基于层次邻居图的目标网络软预测机制。在此机制中,通过邻居图法的应用,认证服务器可以根据用户需求和网络环境,预测出潜在的最佳目标网络,为高效重认证提供保障,以达到快速切换的目的。

1) 邻居图(neighbor graph) 它是一种动态分布式的数据结构,用于抽象出网络接入点之间的切换关系。邻居图的生成是基于对网络中切换情况的持续观测,能适应用户不断移动的模式。随着用户移动习惯的改变,邻居图能增加新的边或删除旧的边来更好地反映当前的切换关系。邻居图的另一个优势是能够精确识别出潜在的最佳目标网络,从而减小新旧接入点间上下文传递引发的二层切换延时^[4]。当用户移动频繁时,此方法的效果会更明显。在 WiMAX 网络切换中,采用邻居图法,可以减少 99% 的重认证时间,还可减小移动终端 84% 的探路延时。

2) 层次邻居图(hierarchical neighbor graph, HNG) 邻居图不但可以用来抽象网络内的切换关系,也适用于描述同构或异构网间环境,网络普适化的邻居图被称为层次邻居图。

图 2 为 3G/WLAN/WiMAX 互连场景下的一个两级融合网络邻居图。假设基本节点 N_i 为 WLAN、WiMAX 的接入点或 3G 中的基站, P_i 为第 i 个网络的 AAA 认证服务器,则 N_i 之间组成了第一层邻居图 NG, P_i 之间组成了第二层邻居图 NGA。

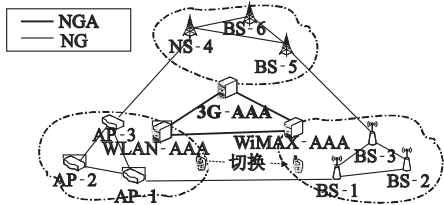


图2 融合网络邻居图

由于高层节点的用户是下层用户的集合,高层节点必须要熟知下层节点的网络拓扑结构^[5]。在图 2 中,WLAN 有两个邻居 3G 和 WiMAX,接入点 AP-2 只有网内而没有网间邻居,AP-1 和 AP-3 均有一个网间邻居。如果 AP-2 下的 MT 选择目标网络,就无须考虑其他两个网络,因为此网络环境下它要先切换到 AP-1 或 AP-3。因此,WLAN-AAA 应该对有网间邻居的 AP 进行优先缓存,而不是 WLAN 中的所有 AP。例如,当 AP-3 中的 MT 要切换时,WLAN-AAA 应该先考虑 3G 网络,而 AP-2 中的移动台则无须如此。这样,通过让 AAA 服务器了解邻居网络拓扑结构,层次邻居图就可不断升级完善,也可更好地预测 MT 要切换的目标网络。

在宽带无线网络环境中,用基于层次邻居图的目标网络软预测机制,可以得到较高的链路反馈和较少的信号开销,从而快速准确地选择用户切换的目标网络,并且在状态转移过程中,传递当前网络的用户认证信息(包括 NID 等认证信息的上下文),为随后的网络重认证提供支撑。这样,异构网间的切换延时和链路开销可大幅减小,网络带宽资源也可得到充分利用。

2 高效认证机制及相关算法

在现有认证框架中,用户的认证信息存放在其家乡网络,当用户接入外地网络时,重认证过程必须依赖与家乡网络的交互信息。当用户远离家乡网络时,访问网络与家乡网络之间交互带来的传输延时就成为移动切换的性能瓶颈^[6]。为解决

决此问题,本章在基于软预测快速切换的基础上,设计了一种高效融合式认证机制,即用户要切换时,当前网络利用上下文传递方式,将信任材料传递到目标网络,为随后的重认证提供支撑;如果由于链路中断或超过缓存时效丢失了这些信任材料,才需要与家乡网络交互。

2.1 融合式认证机制

融合式认证模型如图 3 所示,假设 $\{N_1, N_2, \dots, N_m\}$ 遍历所有的访问网络,它们之间的连接就是 MT 的移动路径。当 MT 从网络 N_i 切换到 N_{i+1} 时, N_i 称为先前网络, N_{i+1} 称为下一网络, MT 的家乡网络应该是与 N_1 认证进程相关的网络。



图3 融合式认证机制

邻近的两个网络应该保持可信关系,就是 N_{i+1} 相信 N_i 提供给 N_{i+1} 的正确信息,相信认证系统和 N_i 加密材料的机密性是安全的,并且两个可信网络间的安全通道是存在的。如果 N_i 的安全性被危及,随后网络的会话都可能被危及^[7]。此机制的一般认证过程分为以下几步:

- a) MT 和当前认证服务器交互材料,证明只有它们自己知道的秘密信息,典型的交换信息包括随机质询。确认后,产生新鲜、无重复并且秘密的材料(如会话密钥)。产生的会话密钥对除了 MT 和认证服务器外的每个实体来说都是随机的,其他人不能预测安全密钥。这样,就建立起了一个安全关联。
- b) 此外,MT 和认证服务器分享会话密钥,服务器需要传输哈希密钥给下一服务器,因此下一服务器和 MT 分享相同的密钥,而任何信息交互并不包含密钥。
- c) 当前服务器向下一服务器传递信任材料,或是由终端切换到下一网络时将信任材料携带过去。
- d) 若当前网络传递给下一网络的信任材料由于链路中断或超过缓存时效丢失,根据需要通过与家乡网络交互获得。
- e) 终端与切换后的网络之间,依靠本网的认证协议进行双向认证。

在此融合式认证架构中,下一网络依靠先前网络的安全关联与传递的信任材料,同 MT 进行双向认证,从而建立起安全通信链路,保证了切换认证的安全性和高效性。信任材料包含的信息是 MT 与认证服务器协商得来的,会根据下一网络的认证协议不同而有所差异。

2.2 安全上下文传递算法

在融合认证机制中,切换前后的网络间安全关联已经建立。不过各异构网络的信任材料和加密信息不尽相同,各网需要的认证信息必须要能自适应地进行传递。为解决此问题,提出了安全上下文传递算法,如图 4 所示。

- a) MT 在当前网络 N_i 中,利用第 1 章的快速切换算法选择最佳的目标访问网络 N_j 。
- b) 若网络 N_i 和 N_j 是同构同域网络,则无须重认证。
- c) 若不是同构同域网络,则 MT 与网络 N_i 的认证服务器交互各自的材料,协商会话密钥和相关信任材料。
- d) 当网络 N_i 主动向 N_j 传递会话密钥和相关信任材料时,

MT 可由网络 N_i 切换到 N_j , 或者 MT 先切换到 N_j , 再由 N_j 中认证服务器向 N_i 提出会话密钥和相关信任材料交付申请。

e) 当网络 N_j 成功获取上述信息后, 利用会话密钥对相关信任材料解密。

f) 如果由于链路中断或超过缓存时效丢失了上述信息时, 则 N_j 向 MT 家乡网络交互数据。

g) MT 和网络 N_j 进行双向认证。

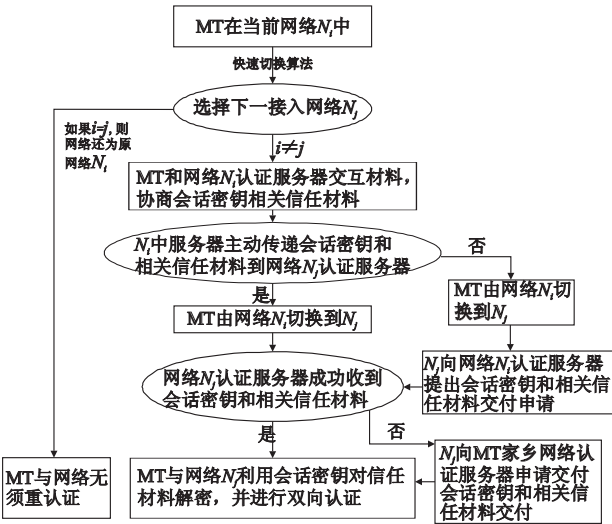


图4 安全上下文传递算法

由于异构网络使用不同的安全上下文信息, 如 3G 的 K、RAND、WLAN 的 MK、SessionID 和 WiMAX 的 PMK、AK、TEK 等。网内的用户要成功进行切换重认证, 也必须维护多套认证上下文信息, 这就会给系统造成很大负担, 还会影响到切换效率, 因此要在统一标志的基础上对异构网络上下文信息进行统一。定义了三个上下文传递消息, 即 CT-request、CT-response 和 CT-active。CT(context transfer)消息通用格式如表 1 所示。

表 1 上下文传递通用消息格式

Byte0	Byte1	Byte2	Byte3
版本	命令	标志	
长度		数据	
数据...			

注: 版本为协议的版本号; 命令表示消息的功能; 标志为两字节标志域, 用于匹配 request 和 response 报文。对于所有发送的 request 报文, 该域的值是惟一的, 当发送 response 报文时, 该域的值与接收到的 request 报文保持一致, 标志域可以避免重复地请求和响应; 长度为长度域, 表示整个报文的长度, 包括从版本域到数据域的所有字节, 若接收报文超长, 则忽略长度域字节之外的所有数据, 若接收报文长度不够, 则被丢弃; 数据为数据域, 是可变长度域, 不同类型的报文对应的数据域不同。

CT-request 消息由切换后终端连接的认证服务器发送给切换前所连接的认证服务器, 请求将相关上下文信息传递给自己; CT-response 消息用来传输与认证协议相关的统一上下文信息。为了在新认证服务器上重新建立关于用户的认证信息, 就如同终端经过完整的认证过程一样。因此上下文中需包含 AAA 服务器在给终端授权时, 向终端发送的 Access-Accept 消息中的属性。数据为 AAA 协议中定义的属性列表消息 CT-active 由新认证服务器发送给原认证服务器, 通知终端已经切换到新网络, 并激活重建的相关信息。

统一上下文对新的通信链路来说应该是新鲜的, 从而无须认证协议, 以达到快速切换的目的。不过, 它需要网络间更强的可信关系。相反, 目的网络可能不相信先前的网络, 需要早先一些的会话, 上下文不会对目的网络造成安全威胁。基于此目的, 目的网络应持有有一个与终端的预共享密钥。本机制需要网络间折中的可信关系, 提供折中的性能收益。这样, 用户在异构网间移动过程中与家乡网络的数据交互大大减少, 降低了切换认证延时、用户及传输消息的安全性也可得到增强。

3 仿真与结果分析

下面讨论 3G-WiMAX 异构网络采用融合认证算法的情况, 并建立模型执行测试, 得出实验结果。

1) 建立模型 图 5 是用 OPNET Modeler 10.0 网络仿真工具建立的仿真模型, 3A 服务器模拟家乡网络、访问网络和 WiMAX 的认证服务器, 3G 基站由 UMTS 基站来模拟。其中, profile config 是图形配置模块; application config 是应用程序配置模块; task 是任务配置模块。MT 是 3G 移动终端, 模拟 3G 基站与 WiMAX 接入点之间的切换过程, 可以根据需要调整网络间的距离大小。

2) 方案执行 利用 3G-AKA 协议来仿真 3G 认证, 修改部分包括 AKA 的执行, 存储上下文的能力。AP 和 BS 运行 OPNET 上的认证者, 修改部分包括认证服务器传输上下文的能力、TLS 恢复能力和服务器端 AKA 状态机的性能。

对集中式认证, 执行 20 次切换, 每次将 3G-VLR/WiMAX AAA 和家乡认证服务器间的距离设置为 0~20 km; 3G-VLR 和 WiMAX AAA 之间距离设置为 2 km。对融合认证机制, 执行 3G 和 WiMAX 间的 20 次切换。通过测试认证延时, 计算平均延时来评估其性能, 利用 OPNET Modeler 可以对两种方法的优劣进行直观比较。

3) 结果分析 图 6 描述当目标网络是 WiMAX 时, 采用集中式认证和融合式认证的延时情况。其中, 本地通信代表认证进程在本地所花费时间, 异构网间通信是 3G-VLR 与家乡认证服务器之间交互认证数据的通信时间。结果显示, 当访问网络与家乡网络之间的距离为 10 km 时, 融合式认证可以减少 EAP-TLS 延时 72.1%, 可见此认证机制的效率更高些。注意, 融合认证过程中上下文传递算法是不需要任何网间通信的, 上下文传递法的性能明显占优。由于原来每个 EAP-TLS 消息都必须与家乡 AAA 服务器进行交互, 使用融合认证机制后, 认证延时降低得就尤为明显。

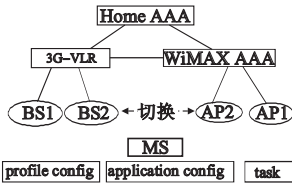


图5 测试模型

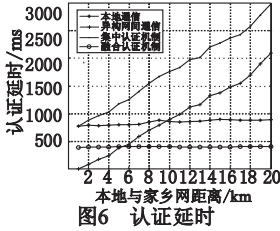


图6 认证延时

4 结束语

本文提出了异构网络高效融合认证机制, 通过基于层次邻居图的软预测机制达到快速切换的目的, 同时为随后的重认证提供相关信任材料。在此基础上, 设计了融合认证机制, 通过

表 2 各费用统计

业务 1 的 费用/元	业务 2 的 费用/元	业务 3 的 费用/元	接入费 用/元	总费 用/元	传统计费 费用/元
0.7213	1.8407	0.1454	0.06	2.7674	1.7970

由图 1 可见,由于 1 800 ~ 2400 s 之间发生拥塞,要收取高额 的拥塞费用,各业务费用和总费用曲线斜率增大,费用大幅 增加。因为高 QoS 业务的价格高,同时消耗的带宽资源又多,1 h 内业务 2 的费用最高,业务 1 次之,业务 3 最低。本计费方 法的总费用比传统计费方法的总费用要高,这主要是因为高 QoS 的业务收取了远高于平均价格水平的费用,且与传统计费 方法的总费用相当。由表 2 可见,高 QoS 业务费用是中等 QoS 业务费用的 2.552 倍,是低 QoS 业务费用的 12.660 倍,高 QoS 业务这一项费用就已经超过了传统计费方法的总费用。

图 2 给出了 1 h 内,业务 1 的各种费用比较,图 3 是横坐标 从 1 795 ~ 1 860 s 的局部放大图。表 3 是图 3 中 10 个点的各 种费用统计。

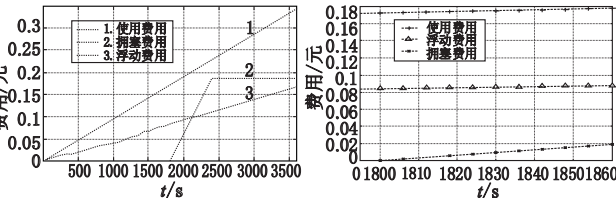


图2 业务1各种费用比较

图3 业务1各种费用的局部比较

表 3 业务 1 各种费用的局部数据统计

	1	2	3	4	5
C_u^{11}	0.172 2	0.172 8	0.173 4	0.174 0	0.174 5
C_f^{11}	0.084 5	0.084 5	0.085 1	0.085 7	0.085 7
C_c^{11}	0	0.001 6	0.003 7	0.005 9	0.007 4

	6	7	8	9	10
C_u^{11}	0.175 1	0.175 7	0.176 3	0.176 8	0.177 4
C_f^{11}	0.086 3	0.086 3	0.086 9	0.087 4	0.087 4
C_c^{11}	0.009 6	0.011 1	0.013 3	0.015 4	0.017 0

由图 2 所示,在 1 800 ~ 1 920 s 这段设定成网络拥塞的时间 中,拥塞费用快速增加,其他时间中拥塞费用为 0。由于拥 塞费用是以高价格定价的,收取高额费用,从图 2,3 中可见,拥 塞费用增加的幅度明显大于使用费用和浮动费用。由于仿真 流量是以标准值为中心的正态分布,而浮动费用只在实际流量 大于标准值时才收取,在一个大的时间范围内,浮动费用有近

似 50% 的时间保持不变,有近似 50% 的时间增加一个正值。 表 3 给出 10 个点的数据统计,可以看出这种 50% 的趋势。由 于使用价格不变,价格较低,只以流量为变量,使用费用呈现出 平缓连续增加的状态。

3 结束语

现有的计费方法,要么是基于区分业务类来保证 QoS,要 么是基于流量控制来保证 QoS,本文提出了一种结合两者的计 费方法。其中使用费用体现了区分业务定价的思想,不同的业 务,在单位带宽单位时间内收取的使用费用是不同的^[6,7];浮 动费用体现了动态 SLA 的思想,在网络资源有剩余时,可以充 分利用网络资源;拥塞费用体现了控制流量的思想,根据业务 拥塞的实际情况,区分制定拥塞价格,收取高费用,利用价格杠 杆规范用户使用资源的行为。多费用体系克服了静态计费方 法的不公平性,使得用户和 ISP 的效益均达到最大^[8]。

参考文献:

[1] 张登银, 王雪强. 下一代网络计费技术分析[J]. 电子工程师, 2004, 30(12): 55-58.

[2] DAVOYAN R, ALTMANN J. Real-time market model for pricing differentiated services[C]//Proc of the 4th International Conference on Networking and Services. 2008:134-140.

[3] MANAFFAR M, BAKHSHI H, PILEVARI M. A new dynamic pricing scheme with call admission control to reduce network congestion [C]//Proc of the 22nd International Conference on Advanced Information Networking and Applications - Workshops. 2008:347-352.

[4] NAN Jin, JORDAN S. On the feasibility of dynamic congestion-based pricing in differentiated services networks [J]. IEEE/ACM Trans on Networking, 2008, 16 (5): 1001-1014.

[5] 张登银, 王雪强. 基于服务级别和流量控制的网络计费[J]. 重庆邮电学院学报:自然科学版,2005,17(3): 328-331.

[6] WANG Xin, SCHULZRINNE H. Pricing network resources for adaptive applications[J]. IEEE/ACM Trans on Networking, 2006,14 (3): 506 - 519.

[7] 张登银, 卢栋梁, 王雪强. 基于数据包的下一代网络计费策略研究[J]. 电子与信息学报, 2006,28(12):2382-2385.

[8] ZACHARIADIS G, BARRIA J A. Income maximization using prices and QoS for a multi-class telecommunications system [J]. IEEE Communications Letters, 2007, 11(2): 222-224.

(上接第 2700 页)安全上下文传递算法达到高效重认证的目的, 它吸取了集中式认证机制的优点,减少了认证延时,提高了认 证效率和安全度。

不过各异构网络的认证机制和技术不尽相同,它们需要的 信任材料也不一样,因此还需要设计出一套自适应的信任材料 协商机制。此外,智能移动终端的设计也是一个重要的课题, 里面需要嵌入对各异构网络通用的模块,利用相关算法来实现 高效认证。本文的切换认证机制还有待进一步改进和完善,以 给用户带来更加安全快捷的服务。

参考文献:

[1] XU Fang-min, ZHANG Lu-yong. Interworking of WiMAX and 3GPP networks based on IMS [J]. IEEE Communications Magazine, 2007, 7(3):145-149.

[2] KIM C, KIM Y S, HUH E N, et al. Performance improvement in mobile IPv6 using AAA and fast handoff [C]//Proc of ICCSA 2004,

LNCS 3043. [S. l.]: Springer-Verlag, 2004: 738-745.

[3] ZHANG Liang, SETA N, MIYAJIMA H, et al. Fast authentication based on heuristic movement prediction for seamless handover in wireless access environment[C]// Proc of IEEE WCNC. 2007.

[4] SHIN M, MA J, A W. The design of efficient internetwork authentication for ubiquitous wireless communications, CS-TR- 4617 [R]. Maryland: University of Maryland, 2004.

[5] STEVENS-NAVARRO E, WONG VS W, LIN Yu-xia. A vertical handoff decision algorithm for heterogeneous wireless networks [C]// Proc of IEEE WCNC. 2007.

[6] TIAN Ye, ZHANG Yu-jun, ZHANG Han-wen, et al. Identity-based hierarchical access authentication in mobile IPv6 networks[C]// Proc of IEEE ICC. Istanbul, Turkey: [s. n.], 2006:11-15.

[7] CHEN Y T, STUDER A, PERRIG A. Combining TLS and TPMs to achieve device and user authentication for Wi-Fi and WiMAX citywide networks[C]// Proc of IEEE WCNC. 2008.