

# 无线异构网络的关键安全技术

## Key Technologies of Wireless Heterogeneous Networks Security

中图分类号:TN929.5 文献标识码:A 文章编号:1009-6868 (2008) 03-0032-06

**摘要:**异构网络的融合及协同工作在下一代公众移动网络中将是一个很普遍的问题,无线异构网络融合技术作为改善公众移动网络的覆盖和容量以及提供无处不在的通信能力、接入Internet的能力和无处不在的移动计算能力的有效手段,已引起广泛的关注,有着良好的应用前景。构建无线异构网络的安全防护体系,研究新型的安全模型、关键安全技术和方法,是无线异构网络发展过程中所必须关注的重要问题。无线异构网络中的关键安全技术包括安全路由协议、接入认证技术、入侵检测技术、节点间协作通信等。

**关键词:**无线异构网络;安全体系;关键安全技术;节点协作通信

**Abstract:** Convergence and collaboration of heterogeneous networks in the next generation public mobile networks will be a subject of universal significance. Convergence of heterogeneous networks, as an effective approach to improve the coverage and capacity of public mobile network, to enable communication services, to provide Internet access and to enable mobile computing from anywhere, has drawn widespread attention for its good perspective in application. Construction of security system for wireless heterogeneous networks and development of new security models, key security techniques and approaches are critical and mandatory in heterogeneous networks development. Key technology of wireless heterogeneous networks security covers security routing protocol, access authentication, intrusion detection system, cooperative communication between nodes, etc.

**Key words:** wireless heterogeneous network; security system; critical security technology; cooperative communication between nodes

吴蒙/WU Meng

季丽娜/JI Li-na

王堃/WANG Kun

(南京邮电大学,江苏 南京210003)

(Nanjing University of Posts &amp;

Telecommunications, Nanjing 210003, China)

网络,信息安全问题同样是无线异构网络发展过程中所必须关注的一个重要问题。异构网络融合了各自网络的优点,也必然会将相应缺点带进融合网络中。异构网络除存在原有各自网络所固有的安全需求外,还将面临一系列新的安全问题,如网间安全、安全协议的无缝衔接、以及提供多样化的新业务带来的新的安全需求等。构建高柔性免受攻击的无线异构网络安全防护的新型模型、关键安全技术和方法,是无线异构网络发展过程中所必须关注的一个重要问题。

虽然传统的GSM网络、无线局域网(WLAN)以及Ad hoc网络的安全已获得了极大的关注,并在实践中得到应用,然而异构网络安全问题的研究目前则刚刚起步。本文将在下一代公众移动网络环境下,研究无线异构网络中的安全路由协议、接入认证技术、入侵检测技术、加解密技术、节点间协作通信等安全技术等,以提高无线异构网络的安全保障能力。

### 1 Ad hoc网络的安全解决方案

众所周知,由于Ad hoc网络本身固有的特性,如开放性介质、动态拓扑、分布式合作以及有限的能量等,无论是合法的网络用户还是恶意的入侵节点都可以接入无线信道,因而

在过去的十几年里,全球移动通信发展迅速,蜂窝移动用户数量迅猛增长,除了单一的话音业务外,数据业务也获得了极大的增长。然而,无线网络(包括蜂窝网络)仍必须不断地提供无处不在的通信能力,以满足人们不断增长的通信以及接入Internet的需求。

异构网络融合是个崭新的概念——尽可能将各种类型的网络融合起来,在一个通用的网络平台上提

供多种业务,一直是人们追求的目标。4G网络的一个主要特征就是能够提供多种不同无线接入技术之间的互操作,无线局域网(WLAN)和3G网络的融合、Ad hoc网络与蜂窝网络的融合都是无线异构网络融合的重要模式。网络融合技术可极大地提升蜂窝网络的性能,在支持传统业务的同时也为引入新的服务创造了条件,成为支持异构互连和协同应用的新一代无线移动网络的热点技术。无线异构网络融合近年来受到了业界的高度重视和研究<sup>[1-6]</sup>。

如同所有的通信网络和计算机

**基金项目:**江苏省自然科学基金项目(BK2007236)、江苏省六大人才高峰基金项目(SJ207001)

32

中兴通讯技术

2008年6月 第14卷第3期 Jun. 2008 Vol.14 No.3

使其很容易遭受到各种攻击,安全形势也较一般无线网络严峻的多。目前关于Ad hoc网络的安全问题已有很多相关阐述<sup>[7-11]</sup>。Ad hoc网络中的攻击主要可分为两种类型,即被动型攻击和主动型攻击。

目前Ad hoc网络的安全防护主要有二类技术:一是先验式防护方式:阻止网络受到攻击。涉及技术主要包括鉴权、加密算法和密钥分发。二是反应式防护方式:检测恶意节点或入侵者,从而排除或阻止入侵者进入网络。这方面的技术主要包括入侵检测技术(监测体系结构、信息采集、以及对于攻击采取的适当响应)。文献[12]和文献[13]描述了在没有认证中心的情况下Ad hoc群密钥分发技术,其中文献[12]还研究了密钥建立的有效性。然而这二种密钥分发方案仅仅只适用节点之间彼此可以直接通信的小规模的Ad hoc网络。还有由网络中多个节点共同协作完成认证中心(CA)功能的分布式认证的门限密码方案,该方案改善了网络的鲁棒性,因为它排除了一个或少量节点的捕获而摧毁整个网络的密钥管理的可能性。文献[14]研究了一种非集中式的密钥分配方案,假设每个移动节点在它的近邻有一个可信赖的节点群,二个节点通过合并它们各自的节点群的相关信息进行公钥交换,这就大大提高了获得的密钥的可信度。然而,该种方案仍然有可能发生密钥分配失败,特别是对于大规模的Ad hoc网络。

在Ad hoc网络中,路由安全问题是个重要的问题。在目前已提出的安全路由方案中,如果采用先验式防护方案,可使用数字签名来认证消息中信息不变的部分,使用Hash链加密跳数信息,以防止中间恶意节点增加虚假的路由信息<sup>[15]</sup>,或者把IP地址与媒体接入控制(MAC)地址捆绑起来,在链路层进行认证以增加安全性<sup>[16]</sup>。采用反应式方案,则可使用入侵检测法。每个节点都有自己的入侵检测系

统以监视该节点的周围情况,与此同时,相邻节点间可相互交换入侵信息。当然,一个成功的入侵检测系统是非常复杂的,而且还取决于相邻节点的彼此信任程度。看门狗方案也可以保护分组数据在转发过程中不被丢弃、篡改、或插入错误的路由信息<sup>[17]</sup>。另外,如何增强AODV、DSR等路由协议的安全性也正被研究<sup>[18-19]</sup>。总之,Ad hoc网络安全性差完全由于其自身的无中心结构,分布式安全机制可以改善Ad hoc网络的安全性,然而,增加的网络开销和决策时间、不精确的安全判断仍然困扰着Ad hoc网络。

## 2 异构网络的安全解决方案

### 2.1 安全体系结构

对于异构网络的安全性来说,现阶段对异构网络安全性的研究一方面是针对GSM/GPRS和WLAN融合网络,另一方面是针对3G(特别是UMTS)和WLAN的融合网络。如文献[20]在GSM/GPRS和WLAN融合支持移动用户的结构中,把WLAN作为3G的接入网络并直接与3G网络的组成部分(如蜂窝运营中心)相连。这两个网络都是集中控制式的,可以方便地共享相同的资源,如计费、信令和传输等,解决安全管理问题。然而,这个安全措施没有考虑双模(GSM/GPRS和WLAN)终端问题。文献[21]将3G和WLAN相融合为企业提供Internet漫游解决方案,在合适的地方安放许多服务器和网关,来提供安全方面的管理。还可以采用虚拟专用网(VPN)的结构,为企业与3G、公共WLAN和专用WLAN之间的安全连接。3GPP TS 23.234描述了3G和WLAN的互联结构,增加了如分组数据网关和WLAN接入网关的互联成分<sup>[22]</sup>。3GPP TS 33.234在此基础上对3G和WLAN融合网络的安全做出了规定,其安全结构基于现有的UMTS AKA方式<sup>[23]</sup>。

在Ad hoc和蜂窝融合网络安全性研究方面,文献[24]提出了利用蜂窝

网的“带外信令”和蜂窝网的中央管理机制来提高Ad hoc的网络管理和控制,从而提高Ad hoc网络的路由和安全性能。但该安全方案只针对Ad hoc网络,没有考虑蜂窝网络和网间的安全问题。

因此,构建一个完善的无线异构网络的安全体系,一般应遵循下列3个基本原则:(1)无线异构网络协议结构符合开放系统互联(OSI)协议体系,因而其安全问题应从每个层次入手,完善的安全系统应该是层层安全的。(2)各个无线接入子网提供了MAC层的安全解决方案,整个安全体系应以此为基础,构建统一的安全框架,实现安全协议的无缝连接。(3)构建的安全体系应该符合无线异构网络的业务特点、技术特点和发展趋势,实现安全解决方案的无缝过渡。

可采用中心控制式和分布代理相结合的管理体系,设置安全代理,对分布式网络在接入认证、密钥分发与更新、保障路由安全、入侵检测等方面进行集中控制。

### 2.2 安全路由协议

路由安全在整个异构网络的安全中占有首要地位。在异构网络中,路由协议既要发现移动节点,又要能够发现基站。现有的路由协议大多仅关注于选路及其策略,只有少部分考虑安全问题。

在联合蜂窝接入网系统中(UCAN)<sup>[25]</sup>,涉及的安全主要局限在数据转发路径上合法中间节点的鉴定问题。当路由请求消息从信宿发向基站时,在其中就引入单一的含密码的消息鉴定代码(MAC)。MAC鉴定了转发路径,基站就会精确地跟踪每个代理和转发节点的数据流编号,而每个用户都有一个基站所给的密码。UCAN着重于阻止个人主机删除合法主机,或者使未认可的主机有转播功能。它有效地防止了自私节点,但是当有碰撞发生时,防御力就会减少了。另外,文献[26]提出一种用于对付任意恶意

攻击的新路由算法。该方法主要在于保护路由机制和路由数据,开发融合网络信任模型,以及提出安全性能分析体制。该路由算法的核心机制是为每个主机选择一条到基站吞吐量最高的路径。每个主机周期性的探测邻居节点的当前吞吐量,选择探测周期内的吞吐量最高值。其目标是识别融合网络中恶意节点的攻击类型,提供有效检测,避免恶意节点。

一般而言,对安全路由协议的研究起码要包括两个部分:基站和移动终端间的路由安全和任意两个移动终端间的路由(Ad hoc网络路由)安全。而由于异构网络的路由协议主要来源于Ad hoc网络路由协议的扩展,从而对异构网络路由协议安全性的研究将主要延伸于Ad hoc网络路由协议的安全性研究。鉴于此,可以将现有的一些Ad hoc安全路由研究植入到异构网络的安全路由研究中。简单的防欺骗的基于信誉的系统SPRITE<sup>[27]</sup>就是一个很好的研究入口。SPRITE本身需要一个独立于Ad hoc网络之外的固定系统——信誉结算服务(CCS)系统,用于维持节点信誉的平衡,激励中间节点转发数据的积极性。不过,要实现SPRITE系统需要CCS获悉两个节点之间的完整路由信息。而这一点,在异构网络中,由于有基站等固定基础设施的存在,因而实现起来就相对简单了。

当然,异构网络路由协议的安全性要建立在节点得到服务提供商支持的认证,这就要完善基站等固定基础设施的安全体系和密码技术,以使得节点能接入到异构网络,获得异构网络的认证。

### 2.3 接入认证技术

现有的大多数认证体系如Kerberos及X.509等普遍是针对一般的集中式网络环境提出的,因其要求有集中式认证机构如证书发放中心或CA。而对于无固定基础设施支持的分布式移动Ad hoc网络,网络拓扑结

构不断地动态变化着,其认证问题只有采用分布式认证方式。对于异构网络,蜂窝基站的引入则可以在充分发挥Ad hoc自身优势的同时克服其固有缺陷。可以根据集中式网络和分布式网络各自的特点,建立异构网络的接入认证系统。文献[28]讨论了WLAN中的节点接入3G的安全认证问题。它构建3G-WLAN信任模型来严格维持3G-WLAN融合网络中所有组成成分之间的信任关系,以加强接入认证过程,保护3G网络免遭伪造的接入认证请求。

从Ad hoc和蜂窝融合网络3种系统模式来看,以蜂窝技术为主Ad hoc为辅的融合网络系统模式,其接入认证的重点就是如何让合法的Ad hoc网络用户安全地接入到蜂窝网络中;以Ad hoc为主蜂窝技术为辅的融合网络系统模式,其接入认证的重点则是如何在Ad hoc内部实现安全以及蜂窝网管理Ad hoc网络时如何安全的传输控制信息。而事实上,这种模式下甚至可以直接采用蜂窝网中一样的接入认证过程,如CAMA。Ad hoc和蜂窝融合的第三种模式——混合模式,则更需要对每个用户的身份信息等进行更加严格的认证。异构网络用户的身份信息认证又包括Ad hoc网络与有基站等固定基础设施的集中式网络之间的认证和任意两种集中式网络之间的认证。

对于复杂的异构网络安全性而言,传统意义上的接入认证只是第一道防线。对付那些已经混入网络的恶意节点,就要采取更严格的措施。建立基于基站的和节点声誉评价的鉴权认证机制或许是一个好的方法。因为蜂窝系统的末端接入网络是完全依赖于节点的广泛分布及协同工作而维护正常通信的,既要拒绝恶意节点的接入,又要确定合适的评价度,保证合法节点不因被恶意节点诬陷而被拒绝接入。这样可以最大限度的保证网络资源的可使用性。

在异构网络中,基站和各移动节

点可以共同担当声誉机制中心这类权威机构的角色,形成以基站为主,移动节点分布式评价为辅的方式。同时,还可以借鉴文献[29]中的方式:在节点接入网络时进行预认证,之后网络中的基站和其他移动节点对它的行为跟踪,使它的恶意行为对应一定的声誉值,重新对它进行鉴权认证。

### 2.4 入侵检测技术

异构网络与有线网络存在很大区别,针对有线网络开发的入侵检测系统(IDS)很难直接适用于无线网络。传统的IDS大都依赖于对整个网络实时业务的监控和分析,而异构网络中移动环境部分能为入侵检测提供的信息只限于与无线通信范围内的直接通信活动有关的局部数据信息,IDS必须利用这些不完整的信息来完成入侵检测。其次,移动网络链路速度较慢、带宽有限、且节点依靠电池供应能量,这些特性使得它对通信的要求非常严格,无法采用那些为有线IDS定义的通信协议。第三,移动网络中高速变化的拓扑使得其正常与异常操作间没有明确的界限。发出错误信息的节点,可能是被俘节点,也可能是由于正在快速移动而暂时失去同步的节点,一般IDS很难识别出真正的入侵和系统的暂时性故障。因此,一个好的思路就是研究与异构网络特征相适应的可扩展性好的联合分级检测系统。

目前备受好评的主流入侵检测系统有两种:基于移动代理技术的分布式入侵检测系统<sup>[30]</sup>和Ad hoc网络分布式入侵检测系统<sup>[31]</sup>。前者的核心是移动代理模块。根据有限的移动代理在Ad hoc中的不同作用,按某种有效的方式将移动代理分配到不同的节点,执行不同的入侵检测任务。检测的最后结果由一个行动执行模块来付诸实施。由于移动代理数量的大大减少,该模型相对其他IDS具有较低的网络开销。

Ad hoc网络分布式入侵检测系统



要求网络中所有节点共同参与入侵检测与响应。每个节点配备有一个IDS代理,这些IDS代理运用了基于统计性异常的检测技术。当某一节点报告一个异常时,不同区域IDS代理互相合作,发起全局入侵检测和响应。在这个分布式入侵检测系统的基础上,文献[32]提出了一种基于簇的多层合作入侵检测系统。簇中任一节点(包括簇头、副簇头和网关节点)都独立运行各自的IDS模块,监控本地的活动,参与本地入侵检测。如果节点(包括副簇头和网关节点)检测到异常或可疑,但不能判定是否被攻击,则向簇头发出执行全局协作检测的请求。簇头接到请求后,通过查询所有节点的IDS状态来判定是否遭受攻击。这一基于簇的多层合作IDS可以被引用到异构网络中来。因为基站等有中央控制管理功能的节点可以有效得替代簇头,实现簇头能全局协作的功能。

在Ad hoc和蜂窝融合网络安全性能研究方面,CAMA结构对入侵检测进行了探讨。当检测到有入侵节点时,CAMA代理就通过基站向整个网络广播安全信息。入侵检测主要用于解决CAMA中节点故意向基站提供错误定位信息而引发的路由安全问题。当节点发现基站发来的路由表中的下一跳节点根本不存在时,就向基站发送路由错误报告。CAMA代理找出恶意节点并将它逐出网络。

另外,从入侵检测系统的检测方法角度考虑,人体免疫系统对异体的检测方法是异常检测和误用检测两种检测方法的结合。根据Forrest设计人体免疫系统(AIS)来进行数据检测,以及Kephart利用AIS进行病毒检测,可以尝试利用基于AIS的理论,借鉴基因选择来设计入侵检测模型。

## 2.5 异构无线网络的节点协作通信

如何确保节点通信的内容在Ad hoc网络中继节点的传输过程中的保密性,如何确保异构网络中安全性最

差的Ad hoc网络的安全,不受到恶意节点和自私节点的攻击,都是迫切需要解决的问题。因此需要设计一种激励策略既能防止恶意节点的攻击和激励自私节点参与协作,又能保证通信内容在传输过程中的保密性。

目前所提方案可粗略地分为两类,一类是基于信誉的(或基于检测的)策略,另一类是基于市场的(或基于计费的)策略。

在基于信誉的系统中,节点观察其他节点的行为并据此采取措施,或者奖励协作行为,或者惩罚不协作行为。节点可以使用“看门狗”来检测其他节点是否转发数据包,避免路由选择中的恶意行为;同时在源节点处使用“探路人”<sup>[31]</sup>选择最可靠的路由发送数据包。另一种叫做动态Ad Hoc网络的节点协作(CONFIDANT)<sup>[34]</sup>的信誉系统可以阻止拒绝服务的攻击。如果一个邻居节点不转发数据包,它就会被认为是不协作,其信誉就会在网络中广播。协作信誉系统(CORE)系统<sup>[35]</sup>提供3种不同的信誉量:主观信誉量,间接信誉量和功能信誉量。利用这3种信誉量的加权值来决定是否协作,同时避免了恶意节点的攻击。安全客观信誉激励(SORI)<sup>[36]</sup>策略的目标是拒绝转发的行为,使用类似看门狗的机制来监控,而信誉系统维持的信息是节点转发的数据包和发送的数据包数量的比率。

另一种激励协作的方法是基于市场的。在这种策略中,节点从它们转发的数据包那里获得报酬,反过来节点可以用这些报酬发送它们自己的数据。一种叫做Nuglets的虚拟货币作为单跳的单位费用来激励每次传输中的协作<sup>[37]</sup>,在文献[38]的策略中,节点转发数据后就会从发送者那里得到报酬,它们的策略需要在每个节点上安装一种防伪设备,如同在安全激励协议(SIP)<sup>[39]</sup>中,来确保费用准确地增加与扣除。SPRITE不需要防伪硬件,它利用一个安全协议来管理费用的交换。上面两种策略的共同特点就

是网络中每个节点转发数据包的定价相同。兼容激励拍卖策略(iPASS)<sup>[40]</sup>在路由器中运行“Vickery拍卖”来决定流量的带宽分配和价格。

安全问题是激励策略中最关键的问题。节点协作的安全性就是不仅要处理自私节点和恶意节点,还要阻止其他方面的攻击。拒绝转发只是不良行为中的一种类型,许多其他关于路由的攻击更值得关注,比如黑洞攻击、灰洞攻击、虫洞攻击等。因此激励策略需要额外的设备或机制来抵御攻击,这就增加了系统的复杂性和集中式服务。在SIP中,需要密钥建立设备,每个节点还需要安全模块;SORI要对传播的信誉评价进行基于Hash链的认证;SPRITE需要对每个数据包的RSA签名进行验证和储存;残余Ad Hoc网络(STUB Ad hoc)采用公钥加密技术;在协作计费策略网络(CASHnet)中,由于开放的环境,需要基于公钥的设施,这不需要直接密钥转换。数字签名的使用阻止了数据包的秘密篡改,并唯一地确认原始数据包和转发节点,因此无效的数据包(比如未付款的)就不会被转发,奖励也就能安全地分配。

如果没有外加的设备,激励策略往往易受攻击。在CONFIDANT中,由于没有机制验证收到的信息中不良行为的可靠性,恶意节点可以发送错误的信息来影响无恶意节点,易收到Sybil攻击。另外,对不良节点也没有救赎机制;iPASS的计费系统没有结合安全交易。最近的研究大多利用博弈论,考虑市场的概念,因为所有的网络功能都依靠参与者的贡献。节点不得不相互转发数据包来确保多跳通信,这样就没有必要设计协作机制,更重要的是考虑数据转发的均衡情况。

还有一些激励策略在没有外加设备的情况下考虑了安全问题。CORE使用本身的安全机制来抵御攻击:节点之间不会传播负面评价,这样节点不会恶意地降低另一个节点

的信誉。CORE的信誉系统允许MANET中的节点逐渐孤立自私节点。当邻居节点的信誉值降低到一个预先设定的门限值时,提供的服务就会中断。

### 3 结束语

事实上,异构多网融合在未来网络发展中是个很普遍的问题,其理论基础在不断奠定,应用在不断扩大。而且,无线与无线网络、无线与有线网络,都可以统一在下一代网络(NGN)的平台上。无线异构多网融合技术作为一种重要的未来无线移动网络的演化方式,有着广阔的应用前景和市场前景,有着巨大的经济效益和社会效益。

与此同时,信息安全问题同样是无线异构网络发展过程中所必须关注的一个重要问题。随着网络应用范围的不断扩大和接入方式的多样化,各种攻击手段与日俱增,安全性在异构网络的各个关键技术问题上起着至关重要的作用,如异构网络的路由、认证、计费、节点协作、入侵检测等各个方面都存在安全的脆弱性。目前国内外对无线异构网络的安全性研究尚为起步阶段,针对安全性某一个方面或问题开展了相关的研究工作,取得了一些初步的研究成果。但由于异构网络的极其复杂性,需要解决的安全问题还相当多。

因此开展无线异构网络信息安全技术的研究,从整体上、系统地研究异构无线网络的互连融合所涉及的安全关键技术和管理工作,研究保证融合网络安全的个性和共性问题,显得尤为重要。要通过对安全机制和协议的广泛研制与应用,积极建立新型主动安全防护系统,以真正达到可信、可控、可用这一信息安全的最终目标。

### 4 参考文献

- [1] Inoue m, Mahmud k, Murakami h, et al. Novel out-of band signaling for seamless internetworking between heterogeneous

networks[J]. IEEE Wireless Communications, 2004, 11(2):56-63.

- [2] Lin y d, Hsu y c. Multihop cellular: A new architecture for wireless communication[C]// Proceedings of the Conference on Computer Communications (Infocom' 00): Vol 3, Mar 26-30, 2000, Tel Aviv, Israel. Piscataway, NJ, USA: IEEE, 2000: 1273-1282.

- [3] Aggelou g n. An integrated platform for ad hoc GSM cellular communications[M]// Ilyas m. Handbook of Ad Hoc Wireless Networks. Boca Raton, FL, USA: CRC Press, 2002.

- [4] Zhao Dongmei, Todo t d. Real-time traffic support in relayed wireless access networks using IEEE 802.11[J]. IEEE Wireless Communications, 2004, 11(2):32-39.

- [5] Wei Hungyu, Gitlin r d. Two-hop-relay architecture for next-generation WWAN/WLAN integration[J]. IEEE Wireless Communications, 2004, 11(2):24-30.

- [6] McNair j, Fang Zhu. Vertical handoffs in fourth-generation multinet environments [J]. IEEE Wireless Communications, 2004, 11(3):8-15.

- [7] Karpjokiv. Security in ad hoc network[EB/OL]. <http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers>.

- [8] Luo Haiyun, Zerfos p, Kong Jiejun. Self-securing ad hoc wireless networks[C]// Proceedings of the Seventh International Symposium on Computers and Communications (ISCC' 02), Jul 1-4, 2002, Taormina, Italy. Piscataway, NJ, USA: IEEE 2002:567-574.

- [9] Papadimitratos p, Haas z j. Secure routing for mobile ad hoc networks[C]// Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS' 02), Jan 27-31, 2002, San Antonio, TX, USA. 2002:27-31.

- [10] Deng Hongmei, Li Wei, Agrawal d p. Routing security in wireless ad hoc networks[J]. IEEE Communication Magazine, 2002, 40(10): 70-75.

- [11] Aura t, Maki s. Towards a survivable security architecture for ad hoc networks [EB/OL]. <http://research.microsoft.com/users/tuomaura/Publications/aura-mak-protocols 01.pdf>.

- [12] Asokan n, Ginzboorg p. Key agreement in ad-hoc network[J]. Computer Communications, 2000, 23(17):1627-1637.

- [13] Hietalahti m. Key establishment in ad-hoc network[EB/OL]. [http://www.camars.kaist.ac.kr/hyoon/courses/cs710\\_2002\\_fall/2002cas/security/papers](http://www.camars.kaist.ac.kr/hyoon/courses/cs710_2002_fall/2002cas/security/papers).

- [14] Hubaux j p, Buttyan l, Capkun s. The quest for security in mobile ad hoc network[C]// Proceedings of 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing in MOBIHOC' 01, Oct 4-5, 2001, Long Beach, CA, USA. New York, NY, USA: ACM, 2001:146-155.

- [15] Zapata m g, Asokan n. Securing ad hoc routing protocols[C]// Proceedings of ACM Workshop on Wireless Security (WiSe' 02), Sep 28, 2002, Atlanta, GA, USA. New York, NY, USA: ACM, 2002:1-10.

- [16] Binkley j, Trost w. Authenticated ad hoc routing at link layer for mobile systems[J]. Wireless Networks, 2001, 7(2):139-145.

- [17] Marti s, Giuli t, Lai k, et al. Mitigating routing misbehavior in mobile wireless networks[C]

// Proceedings of 6th Annual International Conference on Mobile Computing and Networking (MOBICOM' 00), Aug 6-11, 2000, Boston, MA, USA. New York, NY, USA: ACM, 2000: 255-265.

- [18] Buchegger s, Le Boudec j v. Performance analysis of the confident protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks) [C]// Proceedings of 6th Annual International Conference on Mobile Computing and Networking (MOBICOM' 00), Aug 6-11, 2000, Boston, MA, USA. New York, NY, USA: ACM, 2000: 226-236.

- [19] Wang Vweichao, YI Lu, Bhargava b k. On vulnerability and protection of ad hoc on-demand distance vector protocol[C]// Proceedings of International Conference on Telecommunication (ICT' 03): Vol 1, Feb23-Mar 1, 2003, Paris, France. Piscataway, NJ, USA: IEEE, 2003:375-382.

- [20] Ala-Laurila j, Mikkonen j, Rinnemaa j. Wireless LAN access network architecture for mobile operators[J]. IEEE Communications Magazine, 2001, 39(11): 82-89.

- [21] Luo h, Jiang z, Kim b j, et al. Integrating wireless LAN and cellular data for the enterprise[J]. IEEE Internet Computing, 2003, 7(2):25-33.

- [22] 3GPP TS 23.234 V6.1.0. 3GPP System to WLAN Interworking; System Description[S].

- [23] 3GPP TS 33.234 V1.0.1. 3G Security: Wireless Local Area Network (WLAN) Interworking Security[S].

- [24] Bhargava b, Wu Xiaoxin, LU Yi, et al. Integrating heterogeneous wireless technologies: A cellular aided mobile ad hoc network (CAMA) [J]. Mobile Networks and Applications, 2004, 9(4):393-408.

- [25] Luo H, Ramjee R, Sinha P, et al. UCAN: a unified cellular and ad hoc network architecture[C]// Proceedings of 9th Annual International Conference on Mobile Computing and Networking (MOBICOM' 03), Sep 14-19, 2003, San Diego, CA, USA. New York, NY, USA: ACM, 2003:353-367.

- [26] Carlbunar b, Ioannidis l, Nita-Rotaru c. JANUS: Towards robust and malicious resilient routing in hybrid wireless networks [C]// Proceedings of the ACM Workshop on Wireless Security (WiSe' 04), Oct 1, 2004, Philadelphia, PA, USA. New York, NY, USA: ACM, 2004: 11-20.

- [27] Durrresi A, Evans L, Paruchuri V, et al. Secure 3G user authentication in ad hoc serving networks[C]// Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES' 06), Apr 20-22, 2006, Vienna, Austria. Los Alamitos, CA, USA: IEEE Computer Society, 2006: 488-495.

- [28] Aboudagga n, Refaei m t, Eltoweissy m, et al. Authentication protocols for ad hoc networks: Taxonomy and research issues [C]// Proceedings of the 1st ACM international workshop on Quality of Service & security in wireless and mobile networks (Q2SWinet' 05), Oct 13, 2005, Quebec, Canada. New York, NY, USA: ACM, 2005: 96-104.

- [29] Kachirski o, Guha r. Intrusion detection using mobile agents in wireless ad hoc networks [C]// Proceedings of IEEE Workshop on

- Knowledge Media Networking (KMN'02), Jul 10-12, 2002, Kyoto, Japan. Piscataway, NJ, USA: IEEE, 2002: 153-158.
- [30] Zhang Y, Lee W, Huang Y A. Intrusion detection techniques for mobile wireless networks[J]. Wireless Networks, 2003, 9 (5): 545-556.
- [31] Gevaryahu r, Yaros b. Misuse Detection and Prevention in Ad-hoc Networks[EB/OL]. [http://www.seas.upenn.edu/~cse400/CSE400\\_2004\\_2005/18writeup.pdf](http://www.seas.upenn.edu/~cse400/CSE400_2004_2005/18writeup.pdf).
- [32] Marti s, Giuli t j, Lai k, et al. Mitigating routing misbehavior in mobile ad hoc networks[C]// Proceedings of 6th Annual International Conference on Mobile Computing and Networking (MOBICOM'00), Aug 6-11, 2000, Boston, MA, USA. New York, NY, USA: ACM, 2000: 255-265.
- [33] Buchegger s, Le Boudec j y. Performance analysis of the CONFIDANT protocol (Cooperation of nodes-fairness in dynamic ad-hoc networks) [C]// Proceedings of Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), Jun 09 - 11, 2002, Lausanne, Switzerland. 2002: 80-91.
- [34] Michiardi p, Molva r. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks[C] // Proceedings of IFIP Communication and Multimedia Security Conference (CMS'2002), Sep 26-27, 2002, Portoroz, Slovenia. 2002: 107-121.
- [35] He q, Wu d, Khosla p. SORI: a secure and objective reputation-based incentive scheme for ad hoc networks[C]//

Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'04): Vol 2, Mar 21-25, Atlanta, GA, USA. Piscataway, NJ, USA: IEEE, 2004: 825-830.

- [36] Buttyan l, Hubaux l p. Nuglets: a virtual currency to stimulate cooperation in self-organized ad hoc networks [R]. Technical Report DSC/2001/001, Lausanne: Swiss Federal Institute of Technology, 2001.
- [37] Buttyan l, Hubaux j p. Stimulating cooperation in self-organizing mobile ad hoc networks[J]. ACM/Kluwer Mobile Networks and Applications, 2003, 8(5): 579-592.
- [38] Zhang y c, Lou w j, Fang y g. SIP: a secure incentive protocol against selfishness in mobile ad hoc networks[C]// Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'04): Vol 3, Mar 21-25, 2004, Atlanta, GA, USA. Piscataway, NJ, USA: IEEE, 2004: 1679-1684.
- [39] Zhong s, Chen j, Yan y r. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks[C]// Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03): Vol 3, Mar 30-Apr 3, 2003, San Francisco, CA, USA. New York, NY, USA: IEEE, 2003: 1987-1997.
- [40] Chen k, Nahrsted t. iPass: an incentive compatible auction scheme to enable packet forwarding service in MANET[C] // Proceedings of 24th International Conference on Distributed Computing Systems (ICDCS'04), Mar 23-26, 2004,

Tokyo, Japan. Piscataway, NJ, USA: IEEE, 2004: 534-542.

收稿日期: 2008-03-21

## 作者简介



吴蒙, 南京邮电大学通信与信息工程学院教授、博导。主要研究方向为无线通信、信息安全, 已发表论文70余篇, 获国家发明专利2项。



季丽娜, 南京邮电大学通信与信息工程学院在读硕士研究生, 主要研究方向为无线通信和信息安全。



王堃, 南京邮电大学通信与信息工程学院在读博士研究生, 主要研究方向为无线通信和信息安全。

## 中兴通讯CDMA产品综合竞争力排名全球第二

全球领先电信市场调研咨询公司Yankee Group的CDMA专题报告《ZTE shines in CDMA Market》显示, 中兴通讯CDMA产品2007年综合竞争力排名第二位。Yankee Group报告预测, 2008年和2009年中兴通讯仍稳居第二, 并逐年逼近头名。在中国、印度、亚太新兴市场、非洲和东欧等地区, 中兴通讯CDMA产品的地区综合竞争力均拔得头筹。

CDMA综合竞争力包括七大指标: 价格、技术、现CDMA装机容量、产品集成能力、产品系列化、政府支持以及企业文化。在七大指标中, 中兴通讯表现最抢眼的分别是: 价格、技术、现CDMA装机容量和产品系列化, 四项均获最高分。技术领先也在意料之中, 领先的All-IP技术和EV-DO Rev. A技术的成熟实现, 创造并倡导了世界第一个基于CDMA的集群系统GoTa, 以及软基站SDR的率先推出等一系列技术创新, 都为中兴通讯的技术实力增色不少。

Yankee Group资深分析师王学军(XJ Wang)评价: “中兴通讯CDMA产品综合竞争力与日俱增, 源自其大量分布于中国、印度以及亚太新兴市场的CDMA装机容量, 以及对CDMA技术的长期的投资和坚持不懈”, “我们预计中兴通讯将继续强化其合作伙伴战略; 当前的行业态势也为中兴通讯创造了与北美老牌CDMA设备商合作的最佳时机。”

中兴通讯CDMA产品总经理李键介绍: “持续的技术创新、快速的客户需求反应以及低TCO的整体All-IP CDMA2000解决方案, 促成了中兴通讯连续两年创造了‘全球CDMA合同数量第一’和‘基站新增出货量全球第一’的佳绩”, 以及“秉承十多年来对CDMA产业的支持, 中兴通讯全力开发新产品和拓展全方位的服务, 争取更大规模地突破美日韩等高端CDMA市场。”

至今, 中兴通讯CDMA无线产品已经服务全球1.35亿用户; CDMA基站累计出货量高达74 000台。中兴通讯在中国CDMA市场份额高达34%, 稳居第一。