基于PBC的下一代移动网络接入安全

高天寒　郭　楠　索宝仲　等著

東北大學出版社
Northeastern University Press

基于PBC的下一代移动网络接入安全

高天寒　郭　楠　索宝仲　等著

东北大学出版社
·沈　阳·

图书在版编目（CIP）数据

基于 PBC 的下一代移动网络接入安全 / 高天寒等著. —沈阳：东北大学出版社，2014. 12

ISBN 978 - 7 - 5517 - 0846 - 3

Ⅰ. ①基… Ⅱ. ①高… Ⅲ. ①移动网—安全技术 Ⅳ. ①TN929. 5

中国版本图书馆 CIP 数据核字（2014）第 292927 号

出 版 者：东北大学出版社
地址：沈阳市和平区文化路 3 号巷 11 号
邮编：110819
电话：024 - 83687331（市场部）　83680267（社务室）
传真：024 - 83680180（市场部）　83680265（社务室）
E-mail：neuph@ neupress. com
http：//www. neupress. com
印 刷 者：沈阳航空发动机研究所印刷厂
发 行 者：东北大学出版社
幅面尺寸：170mm × 240mm
印　　张：8
字　　数：166 千字
出版时间：2014 年 12 月第 1 版
印刷时间：2014 年 12 月第 1 次印刷
责任编辑：孟　颖　　责任校对：子　敏
封面设计：刘江旸　　责任出版：唐敏志

ISBN 978 - 7 - 5517 - 0846 - 3　　定　　价：30. 00 元

前 言

随着互联网和移动通信技术的飞速发展，以移动 IPv6 为重要支撑的下一代移动网络已然开启，并不断改变着人们的生活方式，而安全性问题成为制约其快速发展和普及的主要瓶颈，主要体现在移动终端安全、接入与承载网络安全、应用安全和用户隐私保护等方面。在诸多安全因素中，接入安全是下一代移动网络安全的基础，如何实现移动节点与接入网络间的高效双向接入认证是当前的研究热点。

目前针对下一代移动网络接入安全的研究仍然依赖传统的 PKI 或 AAA 等安全架构，存在接入认证效率低、身份管理复杂、移动终端资源占用率高等问题。近年来，基于配对密码学（PBC）兴起，具有高安全性和低管理代价等优势，开始应用到移动网络安全等相关领域。以 PBC 为理论工具的下一代移动网络接入安全研究逐渐活跃，出现了一系列学术论文和博士、硕士学位论文，取得了可喜的研究成果，表现出显著的发展势头。但从已有的研究结果来看，基于 PBC 的下一代移动网络接入安全技术研究仍处于起步阶段，相关理论、机制、协议、系统等均存在不同程度的问题和缺陷，有待深入探索和改进。

本书旨在论述基于 PBC 的下一代移动网络接入安全背景、研究现状和解决方案，以作者及课题组多年的研究成果为重点，汇聚了国内外学者在相关领域的研究成果和贡献，对从事网络、通信、信息安全专业研究的高等院校教师、研究生和高年级本科生，以及从事下一代移动网络建设的技术人员具有一定的参考价值和指导作用。

本书分为六章，第一章介绍了以移动 IPv6 为核心的下一代移动网络发展现状及其面临的安全性威胁，分析了国内外针对下一代移动网络安全的研究现状；第二章阐述了 PBC 所涉及的数学知识及与 PBC

相关的典型数学难题和安全假设，并描述了几个典型的 PBC 机制；第三章主要介绍了几种典型的下一代移动网络支撑协议和几种主流的移动网络接入技术，着重指出接入安全的重要性和研究现状；第四章提出了一种基于证书和身份的 HMIPv6 网络认证机制；第五章构建了适用于 PMIPv6 的层次化网络架构，并以此为基础设计了一种基于 2-HIBS 的 PMIPv6 接入认证方案；第六章针对 WMN 匿名接入认证问题，提出了基于层次化代理的 WMN 接入认证方案。全书图文并茂，在全面分析现有研究成果的基础上，阐述了作者及课题组自主创新的研究成果和结论。

在此对本书的其他作者和课题组成员郭楠副教授、索宝仲硕士、王权琦硕士、韩志伟硕士、乔佩雨硕士、苗启迪硕士等给予的密切配合和支持表示感谢！

本书的出版得到了以下项目的资助：国家自然科学基金资助项目（61300196），国家科技重大专项（2013ZX03002006），中央高校基本科研业务费专项资金资助项目（N120417003，N120404010，N130817002）等，在此特别表示感谢！

由于作者水平有限，时间仓促，书中不妥之处在所难免，恳请读者批评指正。

作　者

2014 年 10 月于沈阳

目 录

1 引 言

1.1 下一代移动网络发展现状

近年来，计算机网络的快速发展极大地改变了人们的生活方式，但随着移动智能终端的激增、互联网客户规模的不断扩大和新业务的不断涌现，人们对网络也提出了更高的要求。移动互联网在产业巨头引领的终端软件、硬件与服务垂直一体化整合发展的背景下，规模得到快速扩张，技术、终端、应用等加速融合，特别是丰富的 APP 带来水平化模式的重要创新。移动网络关键要素仍在不断耦合升级，在智能终端及软硬件技术交替演进当中，随着宽带无线接入技术的飞速发展，人们迫切希望能够随时随地乃至在移动过程中方便接入网络，下一代移动网络已然开启。

在移动网络、云计算、物联网等技术快速崛起的背景下，IP 作为下一代互联网中的承载技术，大量的网络终端设备以及系统设备都支持 IP 协议，而且未来核心网向全 IP 网络演进，这些都要求有足够的 IP 地址。同时以 IP 协议为基础的物联网发展也对 IP 地址的数量提出了极高的要求。用户规模的不断扩大加大了对 IP 地址的需求。可以看到，下一代互联网迫切要求足够多的 IP 地址，世界主要国家相继出台国家战略部署 IPv6 协议。近 20 年来，移动网络获得了极大的重视和快速的发展，移动用户的数量呈现指数级增长，包括 3G，4G 在内的接入手段不断丰富和普及，移动网络和下一代互联网的结合——下一代移动网络势在必行[1]。

下一代移动通信系统将更加开放，致力于无缝融合多种无线通信技术与网络结构，包括 3G、B3G、无线广域网(WWAN)、无线城域网(WIMAX)、无线局域网(WLAN)、无线个人局域网(WPAN)以及无线车载网(WVAN)等。下一代异构无线网络是在现有各种网络充分发展的基础上，通过 IPv6 技术实现全 IP 的网络融合。移动终端整体上对 IPv6 的支持较弱，要求操作系统和硬件(主要是基带芯片)等配合。目前，主流操作系统包括 Android、IOS、Windows Phone 等，都能够提供不同的版本以支持 IPv6，但是当前在售的商用手机其操作系统往往都经过不同程度的裁剪，大多数都关闭了 IPv6 功能。就手机芯片而言，主

流厂商(包括 MTK、Marvell、高通等)量产的芯片尚不支持 IPv6 功能，但从其研发路线图上可以清晰看到支持 IPv6 功能的趋势。现阶段，大多数移动终端能够通过 WiFi 方式接入 IPv6 网络[2]。

移动 IPv6 技术不仅利用 IPv6 提供的巨大地址空间，同时增强了切换能力，还加入内嵌的安全机制，为接入网络的各种设备提供安全服务保证。2004 年 6 月，IETF 提出了移动 IPv6 的第一个协议标准——RFC3775。移动 IPv6 协议被视为下一代移动网络中的基础性协议。

移动 IPv6 的关键技术包括移动安全、服务质量和移动切换。移动切换是移动 IPv6 研究的热点，为此 IETF 成立了专门的工作组来解决移动 IPv6 的切换问题。2007 年 4 月，NETLMM(Network-based Localized Mobility Management)工作组发表了第一个 PMIPv6 草案，并在 2008 年 6 月正式发布了基于网络的移动性管理协议标准 RFC5213。另外，NETLMM 工作组研究和定义了移动终端在接入网中移动时如何降低移动终端复杂性到最小的协议，网络只是简单参与路由更新，而实际的触发和决策由终端完成。这样将全局移动性管理和区域移动性管理分开处理，进而设计模块化的移动性管理方案[3]。

虽然目前在基于 IPv6 的下一代移动网络理论与技术方面取得了重大进展，但是仍然存在诸多问题，体现在以下几方面[4]。

(1) 现有固定互联网络拓扑结构的理论与协议不能完全满足新型移动网络的要求

移动网络对路由理论与协议在适应变化性、健壮性、可靠性、服务质量等方面提出了更高的要求，将会承载数据、语音、视频等多种业务，这是传统路由理论与协议所不能胜任的。

(2) 目前移动网络理论和协议主要是针对移动终端的，对移动子网的支持不足

虽然 IETF 提出了支持子网移动的 NEMO 协议——RFC3943，但只是给出了基本框架和概念，没有对细节内容展开讨论。现有的各种移动 IP 技术大部分都是基于终端的移动性方案，难以满足未来异构无线网络多样性与移动性管理技术的需求，并且基于终端的移动性管理协议均定义移动终端发起切换，没有网络侧的任何实体支持智能切换决策，从而导致协议的更新时延较长、传送命令负荷较大和位置保密性差等。目前已经提出了一些改进方案，如快速移动 IPv6(FMIPv6)和层次型移动 IPv6(HMIPv6)等，这些协议的作用是尽量减少移动终端在切换过程中的时延和丢包率，但是相关改进需要移动终端参与移动性管理，并且增加了移动终端协议栈的复杂度。

(3) 互联网应用的发展要求开展移动网络多播理论和算法研究

近年来，随着网络技术的发展，特别是网络应用的层出不穷，例如可视化

IP 电话会议、网络音/视频广播、多媒体远程教育、移动用户的 IP 接入和转发等，一对多和多对多的通信方式显得越来越重要，而 IP 多播正是实现这种通信方式的基础，意味着在未来 IP 多播会有巨大的市场端求。寻求和产生新的移动多播理论、协议与技术将是一个新的研究领域。而目前固定网络的多播理论与协议显然无法满足这些新变化所带来的需求。

（4）下一代移动网络仍然面临诸多安全隐患

随着无线网络与互联网的不断融合，移动通信网络环境变得越来越复杂，网络实体间的信任关系、有线链路的安全、安全业务及安全体系等都需要重新考虑。在移动通信的发展过程中，第一代模拟移动通信因其安全保密性差而被放弃。而以 GSM 为代表的第二代移动通信系统，由于其频谱利用率高、用户容量大、安全保密性好而成为主流的国际标准。第三代移动通信系统(3G)打破了传统意义上通信网络与互联网之间的物理隔膜，极大地提升了无线接入能力，实现了多种应用服务，但也对网络安全提出了挑战，意味着通信系统将同时面对互联网及移动通信空中接口的安全威胁。

1.2 下一代移动网络安全现状

美国政府于 2004 年正式提出下一代移动网络概念，与传统移动网络比有两个明显的优势，即更加安全可信和拥有更加方便快捷的接入方式。

在下一代移动网络中，一方面存在与传统移动网络相似的安全威胁，比如移动终端设备的安全漏洞、蠕虫病毒等恶意代码、利用手机发起的 DDoS 攻击、利用手机短信/彩信配合 WEB 服务进行钓鱼欺诈、垃圾短信、隐私信息窃取、非法定位、恶意扣费等。另一方面还存在诸多针对下一代移动网络协议的安全威胁，如在 IPv6 协议中广泛使用的 ND 协议的认证漏洞，可能被恶意用户所利用，进行多种方式的网络攻击[5]。根据国外黑客组织所进行的“War Driving”竞赛结果，当前的移动网络，以 WLAN 为例，大概平均每年都有 25% ~30% 的网络接入存在隐患，经常主动或被动地受到信息监听、窃取、DoS 攻击等威胁。因此移动网络安全理论的研究已经成为国际各个组织和机构关注的热点之一[6]。

总结起来，下一代移动网络的安全威胁主要体现在以下几个方面。

（1）移动终端安全

移动网络终端通常指的是手机、PAD、上网本、车载设备以及便携式计算机等设备。移动网络终端受到其计算能力、接入速率以及电力供应等因素的限制，比传统互联网终端更加脆弱，而且与传统的互联网终端相比，移动网络终端将会拥有更多的应用程序、更多的下载安装、更长的联网时间，而且会受到移动终端操作系统安全漏洞的影响，会面临更多安全威胁[7]。下一代互联网主

要是基于 IPv6 协议拓展的，由于 IPv6 协议本身具有设计上的缺陷，下一代移动网络终端很容易受到相关威胁。

（2）接入与承载网络安全

移动网络可以分为两部分，即接入网络和 IP 承载网络。在下一代移动网络中需要考虑设备和环境安全、接入服务安全以及信息自身安全等方面。设备和环境安全主要指路由器、交换机等网络设备自身的安全；接入服务安全主要指如何利用接入认证手段保证合法用户可以正常享受服务，而不受到恶意用户的干扰、冒用以及破坏。信息自身安全主要包括信息的安全传播、IP 承载网传递信息时需提供必要的隔离和保密措施以及接入网络所涉及的用户注册安全。

（3）应用安全

移动网络业务可以分为三类：第一类是传统互联网业务在移动网络上的复制；第二类是移动通信业务在移动网络上的移植；第三类是移动通信网络与互联网的相互结合，适配移动网络终端的创新业务。下一代移动网络应用安全主要指应用信息的安全，即与应用相关的信息的完整性、机密性和不可否认性等。此外，还需要对应用信息的内容提供必要的检查和过滤。

（4）用户隐私保护

在下一代移动网络中要格外注意对用户隐私的保护。一般来说，隐私是指个人、机构等实体不愿意被外部知晓的信息。比如，个人的行为模式、兴趣爱好、健康状况、公司的财务状况和用户信息等机密信息。随着下一代移动网络的不断发展，隐私保护已经越来越被重视。一方面在移动终端中存在许多未知安全风险的应用程序，极有可能泄漏用户或者机构的隐私信息；另一方面在下一代移动网络当中移动终端通过认证接入到移动网络当中，也有可能泄漏位置或者其他隐私信息。

综上，下一代移动网络是一个新生事物，是移动网络与下一代互联网相结合的产物，在下一代移动网络发展初期，完全有机会依据移动网络安全框架，通盘考虑安全需求与技术，使下一代移动网络乃至未来整个互联网都变得更加安全。可以预期，下一代移动网络安全研究将在很长一段时间成为信息安全研究的重点和热点。而在下一代移动网络安全研究中，接入认证是一个非常重要的方向，也是本书着重阐述的内容。

1.3 下一代移动网络安全国内外研究现状

目前，下一代移动网络的相关研究大多集中在 IETF 框架下，以工作组的形式进行标准的制定与优化。主要的研究组织包括：IETF Mobile IPv6 工作组、IETF Mobile IPv6 信令与切换工作组（MIPSHOP Working Group）、IETF 网络移动

性工作组(NEMO Working Group)、IETF 网络控制的局部移动性管理工作组(NETLMN Working Group)以及 IRTF Mobopts 等。

下一代移动网络当中的安全问题尤为重要，针对下一代移动网络所存在的安全威胁，国内外相关研究主要集中在以下几个方面。

(1) 移动终端安全

由于移动终端的特点，移动终端安全问题与传统的 PC 安全相比，存在一些区别。目前，恶意软件(如病毒、木马等)已对移动终端的安全构成重大威胁。移动终端的内存和芯片处理能力的不断增强给了恶意软件更多的生存空间；开放的操作系统和应用编程接口极大地方便了恶意软件的开发和植入；同时，移动用户日趋增加，为恶意软件的传播创造了环境。因此，如何进行恶意软件的检测和防护，是实现移动终端安全所亟需解决的问题。

在学术界，学者们在恶意软件的检测和防护方面做了很多研究工作，取得了不少研究成果。国外学者提出了一种行为检测框架，用以检测移动终端上的病毒、蠕虫、木马等恶意软件。该框架通过训练一个基于支持向量机(Support Vector Machines，SVM)的分类器来辨别恶意软件行为和正常应用程序行为。还有其他学者针对 Android 系统提出一种轻量级的应用程序安全验证方法[8]。通过对 Android 系统的安全分析，产生一些可以匹配恶意软件特征的规则，并应用这些规则在程序的安装阶段发现和清除恶意软件。此外，针对恶意软件的“能量耗尽”攻击，专家们提出一种基于能耗监控的检测方法，通过发现能耗异常来检测恶意软件。与此同时，一种基于移动终端间协作的病毒检测和预警系统也被人们所研究，这种方法从移动终端搜集通信行为信息，通过联合分析来检测单个终端或整个系统的异常行为。当检测到病毒存在时，给直接受威胁的移动终端发送警报。该系统采用基于代理的结构，对移动终端的处理负荷进行分流，并简化了移动终端之间的协作。还有针对恶意软件检测带来移动终端额外能耗的问题，从攻击监控范畴和恶意软件扫描频率考虑，提出了一种在安全与能耗之间折中的检测方法，只需消耗少量的额外能量，就能检测出绝大多数已知恶意软件的攻击。

(2) 支撑网络安全

国外的许多标准化组织和论坛，包括 ITU-T(国际电信联盟)的第 13 工作组、IFTF 的 IP Telephony 工作组、信令传输工作组、媒体网关控制工作组、ETSI 的 Tiphon、ISC(国际软件联盟)、3GPP、3GPP2 论坛，ATM(异步传输模式)论坛等，都将下一代移动网络安全作为研究重点之一。国际标准由 IETF 的 IPng(IPv6)工作组组织开发，工作开始于 1992 年，到目前为止，已经有 53 项成为 RFC 文档，17 项成为互联网草案。其中安全类的标准有：互联网协议的安全性结构(RFC2401)、IP 认证包头(RFC2402)、IP 封装安全性载荷(ESP，

RFC2406)、采用 MD5 密钥的 IP 认证(RFC1828)、ESPDES-CBC(RFC1829)等[9]。

移动 IPv6 的安全问题是制约下一代移动网络发展的难题和瓶颈[10]，一直以来难以突破，但又亟待解决。目前世界上有很多组织及机构正在对移动 IPv6 进行研究，并且已有了一些在不同操作系统上开发出来的实验系统。例如 KAME project 实验系统，Windows 下的 Microsoft MIPv6 Project 实验系统，FreeBSD 下的 CMU Monarch project，Linux 下的 Lancaster MIPv6 工程，USAGI(universal playground)的 MIPLMIPv6 实验系统等。

在移动 IPv6 当中内嵌 IP 安全协议[11-13](IP Security Protocol，IPSec)及 RR(Return Routability)协议，以保护移动管理消息的安全成为解决移动 IPv6 安全的主要途径。但是在移动 IPv6 协议当中 IPSec 受到许多制约，需要更多的其他协议配合。RR 协议是用来给移动节点和通信伙伴提供安全认证的协议。首先，它保证移动节点可以从家乡地址和转交地址接收通信伙伴发来的信息。RR 协议不仅能够防范有权访问某一特定路径的潜在攻击者，还能有效地防止重放攻击。但是由于缺乏全局的信任框架支持，移动节点和通信伙伴之间无法实现安全的认证，实际上 RR 协议并没有提供身份认证服务，只提供了所谓的可达性服务，而且其提供的防止消息伪造服务也是比较脆弱的。另一方面，RR 协议同样给移动节点和通信伙伴之间的通信带来了较大的负荷，使得移动信息大大增加，这些都是必须考虑的问题。针对以上问题，有学者提出基于本地代理证书协议(Certificate Base on Home Agent，CBHA)。该协议通过引入本地代理的公钥证书和本地代理的签名，确保了移动节点与其本地地址和临时地址的有效身份绑定，从而增强了抗拒绝服务攻击、重放攻击和中间攻击的能力，提高了移动 IPv6 的安全性。而且在 CBHA 协议中，大大减少了在移动节点上的认证和加密计算，大部分计算都转移到本地代理上，有效地提高了移动节点的工作效率。当然，CBHA 协议是建立在本地代理的公钥证书基础之上的。通信节点可以预先建立一个常用家乡代理证书的队列，把使用次数最多的家乡代理证书放到队列的最前面，从而缓解通信节点获取证书的压力。

(3) 应用安全

移动终端的上层应用也存在不少安全问题，尤其是和传统个人计算机终端的应用程序配合所存在的安全隐患受到人们广泛关注和不断研究。

在众多移动上层应用安全威胁中，网络钓鱼攻击是一种典型的应用安全威胁。移动网络中的网络钓鱼是指攻击者利用一些移动终端的应用程序，配合具有欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信服务，骗取用户的

私人信息。由于网络钓鱼攻击危害大、欺骗性强，各式各样的网络钓鱼手段层出不穷。现已成立了一些反钓鱼的机构，国外比较著名的有 APWG 和 PhishTank，APWG 是目前国际规模较大的反钓鱼组织[14]。

国际反钓鱼工作小组(APWG)是一个自发的反钓鱼组织，该组织提供反钓鱼攻击的交流平台，向民众介绍网络钓鱼攻击的常识以及一些常用的反钓鱼方法，也可以向该组织报告可疑网站。APWG 致力于网络欺骗防御技术的研究，共享自己的反钓鱼技术成果，每个季度会发布一个报告，介绍网络钓鱼攻击的最新动态以及最新的网络钓鱼攻击防御方法。APWG 将一些大型的金融组织、执法机构、网络服务供应商等吸纳为自己的会员，一起对抗网络攻击，目前该组织是全球最大的防御网络钓鱼研究及网络钓鱼事件通报的组织。

中国反钓鱼网站联盟(APAC)由国内银行证券机构、电子商务网站、域名注册管理机构、域名注册服务机构、专家学者共同组成，是国内唯一为解决钓鱼网站问题而成立的协调组织。该组织旨在建立反钓鱼网站协调机制，推动反钓鱼网站综合力量体系的建立，增进相关企业在反钓鱼网站工作方面的合作与交流，共享反钓鱼网站方面的相关信息，组织成员单位共同预防、发现和治理钓鱼攻击，它和 PhishTank 类似，接收用户的举报，由技术人员对举报的网站进行验证，如果确认为网络钓鱼攻击，则通过网络监管机构关停相应的钓鱼页面。

另外，为了减少用户因网络钓鱼攻击而造成损失，提出了一些反钓鱼的方法[15]，目前防御网络钓鱼攻击的方法主要分为教育引导和技术防范两大类。教育引导的方法是通过向用户普及防御网络钓鱼攻击的常识来减少钓鱼的可能性，例如不随便点击陌生人发送的链接、手动输入网址等。技术防范是指通过利用反钓鱼技术，在技术层面上对钓鱼攻击进行检测，目前可以将技术防范方法分成三类：服务器端防御方法、客户端防御方法和预防性的防御方法。

(4) 隐私保护

在下一代移动网络当中，对隐私保护的研究变得更加深入。这是由于现代社会中，“人”与“手机”等移动终端的关系越来越密切，许多涉及隐私的重要信息都保存在随身携带的移动终端中，对于移动网络中隐私保护的研究是当前热点之一。

当前主要的隐私保护技术有基于策略的隐私保护和利用噪声的隐私保护。其中，策略保护机制最早由 Marc Langheinrich 提出，现已经成为主动模式中用户参与控制的主要方式。定位服务(Location Based Services，LBS)发布服务隐私策略，对其所需位置信息的采集、使用、保存进行承诺。用户和 LBS 之间通过各自隐私策略代理(Privacy Policy Proxy)进行策略的比对，若比对成功，则 LBS 获得用户位置信息的采集和使用授权[16]。常见的策略设计方案可以分为乐观策略方案、悲观策略方案和动态策略方案三种。基于数据隐藏的研究方法也是目

前的一个主流，其核心思想是采用 K-匿名（K-anonymity）方法对用户的地理位置或者身份信息进行相应的泛化。将用户的位置信息由具体的点变换为一个区域，或者隐藏用户的某些身份信息，使得用户无法从周边的人群中进行分离。即当且仅当一个用户不能从 $K-1$ 个其他用户中分离出来的时候，称该用户匿名度为 K。

另外，针对移动网络中匿名用户的认证和授权问题，Konidala 提出了一个基于能力的隐私保护方案[17]，实现用户与服务提供商或智能设备的匿名交互。Chau 提出了一种利用多服务器组成的混合网络隐私架构模型，让每个服务器接收一组输入消息，然后以混合方式输出为一组消息，从而使恶意用户或者攻击者不能推断出输入消息和输出消息之间的对应关系，从而保护了用户的隐私信息不被泄露。

总之，在下一代移动网络当中，需要越来越频繁的接入认证，如何在接入认证过程中保证用户的隐私不被侵犯，是今后研究的重点之一。

1.4 本章小结

本章重点阐述了以移动 IPv6 为核心的下一代移动网络发展现状及其面临的安全性威胁，包括：移动终端安全、接入与承载网络安全、应用安全和用户隐私保护等。分析了国内外针对下一代移动网络安全的研究现状，得出接入安全研究的必要性。

参考文献

[1] 黄明超. 下一代互联网 IPv6 技术的研究[D]. 南京：南京邮电大学，2013.
[2] 孙召刚. 下一代互联网通信协议的技术研究与应用[D]. 济南：山东大学，2008.
[3] 王媚. 移动 IPv6 切换技术研究[D]. 西安：西安电子科技大学，2012.
[4] 林闯，雷蕾. 下一代互联网体系结构研究[J]. 计算机学报，2007，30(5).
[5] 康祥青. 基于移动 IPv6 的安全保障关键技术研究[D]. 北京：北京邮电大学，2011.
[6] 刘欣然. 网络攻击分类技术综述[J]. 通信学报，2004(7).
[7] 魏亮. 移动互联网和下一代互联网安全研究是当务之急[J]. 世界电信，2009(10).
[8] 罗军舟，吴文甲，杨明. 移动互联网：终端、网络与服务[J]. 计算机学报，