MIPv6 协议的切换算法的发展及其安全性研究*)

黄松华[1] 孙玉星[2] 黄 皓[1] 谢 立[1]
(南京大学计算机科学与技术系 计算机软件新技术国家重点实验室 南京 210093)[1]
(南京审计学院信息科学学院 南京 211815)[2]

摘 要 移动节点切换安全是移动 IPv6 网络今后研究中最基本的问题之一。切换安全对于保障移动 IPv6 网络的完整性、可用性,推动其实际应用具有重要意义。本文在全面地阐述了切换算法的发展历程的基础上,对切换过程的网络威胁、安全性需求及现状进行了总结,然后分别对当前的代表性切换算法提供的保护机制进行安全性分析,指出了这些算法相对于安全性需求存在的不足,最后进一步分析和总结了研究现状中存在的问题、需要研究的内容和切换安全性研究的发展趋势。

关键词 移动 IPv6,切换算法,网络威胁,安全性需求

Development of Handover Algorithm in MIPv6 and Research on its Security

HUANG Song-hua[1] SUN Yu-xing[1,2] HUANG Hao[1] XIE Li[1]
(State Key Laboratory for Novel Software Technology, Department of Computer Science and Technology, Nanjing University, Nanjing 210093, China)[1]
(School of Information Science, Nanjing Audit University, Nanjing 210031, China)[2]

Abstract The handover security of mobile mode is one of the fundamental problems in MIPv6 research for the future. It is of great significance to safeguarding the integrity, availability of MIPv6 network and then impelling its practical application. On the ground of making a full-scale introduction to the development of the handover algorithm, this paper, firstly, summarizes the network threats, requirements for security and related status quo. And secondly, this paper analyzes respectively the security mechanisms of the current representative algorithms and points out the defects against the requirements. Finally, existing problems, open issues and research trends are analyzed and summarized.

Keywords Mobile IPv6, Handover algorithm, Network threats, Requirements for security

自上世纪末以来,尤其最近几年,有线 Internet 技术和无线移动通信技术都取得了飞速的发展,并且两个技术不断融合,加上 IP 网络和便携式终端日益进入千家万户,使得随时随地接入 Internet 的全 IP 的组网方式成为网络发展的必然趋势,支持多元化无缝宽带接入的下一代移动 Internet 呼之欲出。

作为解决下一代移动 Internet 的多元化无缝宽带接入首选方案,IETF 于 2004 年推出的 MIPv6(Mobile IPv6)协议[1,2]继承了设计思想简洁、运行高效、应用丰富的 IP 技术而成为未来全 IP 有线无线网络一体化融合的基础框架协议,在异构网络下提供统一的实时移动服务方面具有广泛的应用前景,因而也引起了许多学术与标准化组织的极大关注,包括 ITU-T,3GPP,3GPP2,IEEE802 等组织都相继开始制定移动 IP 及其相关技术在蜂窝、MPLS、IEEE802.1x 等网络中的应用技术标准。

MIPv6 协议是为了支持节点在 IPv6 网络中移动时连接的连续性而提出的解决方案。作为 IPv6 网络的四个内建的基本扩展之一[3],它具有地址自动配置、邻居发现,甚至是黑洞检测、IPsec 等解决移动性问题的新特性,然而,其终端所必需的无线链路、移动时和网络节点的认证机制和基本 IPv6 网络及其功能扩展之间的互操作等都引入了许多未知的安全性问题[4]。

下面首先简单介绍 MIPv6 协议的相关概念及其切换算法的发展,然后介绍 MIPv6 协议切换时面临安全性需求和研究现状,第 3 部分对 HMIPv6,FMIPv6 等代表性切换算法的安全性进行了详细分析,第 4 部分全面地分析归纳当前研究中存在的问题和下一步需要研究的内容,最后给出总结和发展趋势。

1 MIPv6 协议的相关概念及其切换算法的发展

MIP 协议的设计目标是使移动节点(Mobile Node,MN)无论处在家乡网络还是位于异地链路,其它通信节点(Correspondent Node,CN)都可以通过 MN 的家乡地址(Home of Address,HoA)或转交地址(Care of Address,CoA)和移动中的 MN 进行不被中断的通信,并保证一定 QoS 和安全性[5],而发展中的 MIPv6 协议正是基于该设计目标,即利用 IPv6 协议解决移动性的新特性,在 MN 移动到外地链路的过程中,使用尽可能少的管理消息和人工干预、尽可能小的消息来实现对节点移动性的支持,以一定的服务质量保持 MN 当前连接的可用性、保密性和完整性。

在基于无线接入的 MIPv6 网络中,面对带宽有限,而带宽需求却日益增长情况,基站服务半径愈来愈小,切换愈加频

*)本文研究得到国家自然科学基金项目(NO:60303023)资助。黄松华 博士研究生,研究领域为网络移动、网络安全;孙玉星 讲师,博士研究生,研究领域为移动 IP、网络 QoS;黄 皓 教授,博士生导师,研究领域为计算机安全与网络安全;谢 立 教授,博士生导师,研究领域为信息安全、分布并行计算。

繁，切换算法的性能和安全性对 MIPv6 服务质量的影响也愈加深远[6]。

标准 MIPv6 采用的基本切换算法（Basic MIPv6，BMIPv6）在利用 IPv6 协议的邻居发现、黑洞检测、地址自动配置等许多新机制的基础上，能和任何链路层技术相结合，解决了 MIPv4 的三角路由问题[1]。然而，根据文献[1]，BMIPv6 的切换历经的链路层切换、路由器发现（移动检测）、转交地址获取与重复地址检测、绑定更新（Binding Update，BU）过程都会导致延时[1,7,8]，而频繁的切换使得在利用 MIPv6 部署多媒体实时业务时，面临着如何减少切换时所产生的延时、抖动、丢包以优化 MN 切换性能的挑战，所以切换算法的改进一直没离开快速[1]、平滑[2] 这两个无缝切换的思路，而改进思路的实现主要针对在微观层面的移动，包括以下几个方面：

• MN 在本地网络的移动尽量不影响到外地网络，以减小 BU 信令数量和切换时间。这方面切换延时的减少最早可以追溯到 Perkins 和 Johnson 提出的基于路由器辅助的 MIPv6 平滑切换算法，即 MN 送 BU 去它的前一个接入路由器（Previous AR，PAR），由 PAR 作为临时 HA 把数据流引向新的 CoA（New CoA，NCoA）[9]。类似地，Y. Wang 等在 1997 年提出了在 HA 和 MN 的 AR 之间架设路由代理来加快切换过程的方案[10]。这两个方法减少了切换时的 BU 的时间和对外地网络的影响，然而，前一方案运行一段时间后产生的层层代理嵌套会带来更大的延时，而路由代理的引入增加了 MIPv6 部署的成本，但也成为层次 MIPv6（Hierarchical MIPv6，HMIPv6）切换思想的前奏。2000 年，C. Castelluccia 提出了 HMIPv6 的切换思想，区分域内和域间移动，域内移动只需向一个成为移动锚点（Mobility Anchor Point，MAP）的路由器注册，域间移动采用原来的 BMIPv6 切换方案[11]。其后，HMIPv6 历经了一些改进，包括 S. -H. Hwang 等提出的结合 MN 移动模型的 HMIPv6[12] 和 I. Vhldi 等提出的结合多播技术的 HMIPv6[13]。前者保存一个移动模型，即 MN 在当前网络的平均停留时间，根据定义的阈值时间，MN 可以使用一个本地 CoA（Local CoA，LCoA）而不是一个区域 CoA（Regional CoA，RCoA），以优化切换性能，而后者从新的 AR 接收报文可以和 BU 的注册过程同时进行，这要求 MN 能获知切换的即将到来，并需要其他网络资源的支持，包括老的 MAP 建立的多播组、可能的新 AR 缓存去 MN 的包等。HMIPv6 的思想在 2005 年由 IETF 制定成为标准[14]。

• 利用链路层提供的信息，以缩短移动检测和 CoA 配置延时、减少丢包为目的，从另一个角度向快速、平滑切换迈进。2002 年，Koodli R 提出了 FMIPv6（Fast MIPv6），即当 MN 检测到新的链路时尽可能早地发送和接收数据包[18]。为了利用 IPv6 中的流标签减少切换需要改变的路径长度，M. Sulander. 第一次提出了 FFHMIPv6（Flow-based Fast Handover for Mobile IPv6）思想，并由 Miska Wander 等真正完整提出利用 IPv6 中流标签可以识别每一个通信流，并以尽量利用原有的路径为原则重定向到一个新的位置，减少由于路径改变导致的切换延时[15]。随后，Youngjune Gwon 等和 Yong Chu Eu 等分别提出了基于链路 Link up 机制的 EFWD-FMIPv6 方案和基于多播的 FMIPv6，前者加速 MN 的移动检测和新的接入路由器（New AR，NAR）的发现，节省了获取 NCoA 的时间，并使 MN 直接控制重定向 PAR 到 NAR 双向隧道的建立[19]，而后者为了减少丢包和缩短切换的数据流中断时间，在切换过程中，MN 会邀请 NAR 加入其多播组，多播路由器会给每一个加入该多播组的 AR 发送 MN 的通信数据[27]。由于 FMIPv6 在配置 MN 的 CoA 时，其重复地址检测过程（尤其在连接到 NAR 后）和 MN 在新链路实现三层可连接后向 HA 和 CN 的 BU 会消耗大量的时间，Ruidong Li 等提出了 EFMIPv6，为每一个 AR 维护一个可用 CoA 列表，为移动到该领域的 MN 产生 CoA，同时，到 HA 和 CN 的 BU 在 PAR 知道 MN 的 NCoA 后就开始[20]。2005 年，IETF 经详细讨论后，制定了 FMIPv6 的标准[7]，同年，HeeYoung Jung，Hesham Soliman 等提出了结合 HMIPv6 和 FMIPv6 两者优点 F-HMIPv6 的草案[16]，A. K. M. Mahtab Hossain 等结合 HMIPv6 和 FFHMIPv6 的思想，提出了 XMAP-HMIPv6[17]。FMIPv6 的其它改进大多都是结合具体的链路层提供的服务来优化性能。Norbert Jordan 等提出了基于链路层触发、网络层并行切换，以缩短网络层移动检测过程的 WLAN 支持方案；Byungjoo Park 等提出了基于增强型 AP 进行移动检测、快速配置 CoA 的 WLAN 改进方案[21,22]。Sasan Adibi 等提出了 QoS 支持的 M-MANET（MPLS MIPv6 Ad-Hoc Network）快速切换集成方案[23]。Minsik Shim 等针对 WiBro，提出了整合二、三层切换的 FMIPv6 方案[24]。Yoon Young An 等提出了利用 IEEE802.21 的 MIH 服务提供的二层信息加快 MIPv6 切换过程的方案，即增加 FMIPv6 执行主动预测方式的可能性[25]。其中 IETF 对基于 WLAN 的 FMIPv6 提出了 RFC 标准[26]。

• 基于多播和基于对 MN 进行修改等其它方向的改进。利用多播主要目的是为了在切换过程中保持 CN 和 MN 的连接，保证平滑切换，其原理是所有和一个特定 MN 保持连接的 CN 预定一个多播组，MN 的切换通过这个多播组通知 CN，然而，这个多播组增加了网络的额外开销[28]。另一个方向对网络元素的修改较小，但要求 MN 的额外资源和预先对即将来临的切换的检测。包括 K. Ome 等提出 MN 增加缓存功能以减小切换的影响，即在切换强制 CN 停止发包前，MN 缓存 TCP ACK，等切换完成后，把缓存的 TCP ACK 送给 CN，CN 继续传送和 L. Pawnapongpibul 等提出的一种新的切换机制和一种 MIP 注册的加强机制，即修改周期性的路由广告信息，使之只有在有必要切换时发布[29]，而 MN 保存一个路由广告的 Cache 以帮助决定是否发生了切换[30]。目前这些发展方向已经融入 HMIPv6 或 FMIPv6，作为单独的发展方向逐渐被学术圈和工业界淡忘[31]。

总之，在 MIPv6 切换过程中，进行合理、有效的切换成为降低网络负担的一个重要途径，而设计一种的延迟低、抖动小、丢包少的高可靠性切换算法依旧是提高网络实时移动服务质量和安全的一个研究热点。

2 MIPv6 切换算法安全性分析

从 MIPv6 切换算法的发展可以看出，其研究主要以性能优化为主线，而且经过众多研究者的努力，MIPv6 切换性能在近年来有了很大的改善，而对切换算法安全保障方面的关注与 MIPv6 协议安全改善方面的研究都有所欠缺。

1 Fast handover，以缩短切换时延为目标，不特别强调减少丢包的数量的切换方案。

2 Smooth handover，以减少丢包为基本目标，不特别强调缩短包转发的额外时延的切换方案。

2.1 安全性需求

为了保证 MIPv6 切换过程中，MN 能得到和本地链路一样的安全，IETF 的文档提出了切换算法相应的安全性需求和指导意见[32]：

(0)强制 BU 的身份验证，即使用现存的任何安全关联(Security Association，SA)保护 MN 与 HA 之间和 MN 与 CN 之间 BU，以减少节点附近或路径上(on-axis)的攻击威胁；

(1)BU 兼顾可扩展性，但不能依赖于尚未健全的全局 PKI；

(2)对于其他非路径上的(off-axis)实现分流或重定向远程攻击的难度与正确猜测一个大的随机数相似；

(3)可以只利用预先配置的 SA(比如 HA 和 MN 之间)来保护 MN 和 CN 间的 BU；

(4)在使用路由优化时可以保持 MN 的匿名性，包括支持的临时地址机制[33]的 MN，可用临时地址作为其 HoA 或转交地址，但当 MN 使用不同的临时地址时，它必须使用不同的可见标识；

(5)在使用 IPsec 作为解决方案时，不能对 IPsec 安全策略库选择符集合提出额外要求；

(6)保证 HA 向 MN 发送的路由器通告的安全；

(7)优化实体间(HA，MN，CN)信息交换的数量和字节数，这对无线链路尤为重要；

(8)CN 可以拒绝 MN 发送的 BU，此时 MN 发送前应该执行退避算法；

(9)任何方法都必须考虑移动环境中实体(尤其是 MN 和 CN)的可扩展性和计算能力，以及产生密钥相关的开销。

然而，由于 MN 在移动过程中和 HA，CN 一般都处于不同的网络管理域，加上移动终端所处的无线环境的开放性、传输的不稳定性和终端设备处理能力的局限性，MIPv6 协议的切换过程给 MN，CN，HA 或家乡网络带来了许多新的威胁[1,2]，这些威胁包括：

· MN 与所处外地链路的不可信任引起的威胁：①假冒 MN 的默认路由器，发送新的路由器通告以掩盖真实的路由器通告，使 MN 切换到新的接入节点；②向 PAR 发送 BU，设置 H 位，使其成为临时 HA，并建立 MN 不正确的绑定机记录，重定向 MN 的数据流，造成拒绝服务攻击[3]。

· MN 与 HA 的不可信任引起的威胁：①发送家乡代理发现信息，可以得到所有家乡代理路由器列表，暴露家乡网络拓扑结构；②篡改 MN 发往 HA 的 BU，同时也可以冒充 HA 向 MN 返回绑定确认，以后 HA 发往 MN 的包被重定向到恶意节点，造成拒绝服务攻击[4]；③向 HA 发送虚假 BU，设置 MN 的生命周期为 0，使 HA 相信 MN 已经回到家乡网络而删除绑定缓存的记录，造成 MN 不可达；④利用虚假的 BU 包对 HA 进行泛洪攻击，阻碍正常节点在 HA 绑定缓存中建立绑定记录；⑤冒充 HA 截取 CN 发往 MN 的包，同时 MN 的地址隐私丢失，比如 CoA，而且可以通过该 CoA，发送大量的绑定确认，对 MN 发起泛洪攻击；⑥利用虚假的 BU，使许多 HA 确信其 MN 的 CoA 为一个受害者的 IP 地址，造成 HA 作为反射器的分布式拒绝服务攻击。

· MN 与 CN 的不可信任引起的威胁：①篡改 CN 的绑带缓存记录，即向 CN 发送 MN 使用新 CoA 的虚假 BU，CN 为 MN 更新绑带记录，以后发往 MN 的包被重定向到恶意节点，造成拒绝服务攻击；②使用虚假的 BU，删除 CN 缓存中的 MN 绑带更新记录，致使路由优化失效；③利用虚假的 BU 包对 CN 进行泛洪攻击，阻碍正常节点在 CN 绑定缓存中建立绑定记录；④冒充 CN 对 MN 发起绑带确认或别的泛洪攻击；④利用虚假的 BU，使许多 CN 确信其 MN 的 CoA 为一个受害者的 IP 地址，或在发给 CN 的包中使用虚假的 HoA 选项，CN 然后把包源地址替换成该选项中地址，造成 CN 作为反射器的分布式拒绝服务攻击。

针对以上所述的威胁，根据 IETF 的切换安全性需求，MIPv6 的切换算法应该具有以下能力：①MN 有能力确认并验证接入点的身份；MN 的 PAR 在成为 MN 的临时 HA 之前必须和 MN 建立 SA。②对家乡代理发现请求的 MN 进行身份验证；HA 在更新绑定缓存记录之前，必须对 BU 进行认证；要求 HA 截取其数据包并发送到 NCoA(New CoA)的 MN 必须和 HA 拥有强 SA。③只有在验证了 MN 对 BU 中 HoA 选项的 HoA 拥有创建绑定缓存记录的权利后，CN 才能更新其绑定缓存；CN 在处理任何 MN 的数据包以前都必须验证其拥有对 HoA 选项中 HoA 的使用权。④CN/HA 为 MN 的 BU 创建状态的前提是验证了 MN 的身份，而且 CN/HA 节点拥有快速拒绝虚假 BU 的能力；MN 有能力验证绑定确认是否可信任，并拥有快速虚假绑定确认(Binding Acknowledgement，BA)的能力。

2.2 安全性现状

仔细地分析一下目前主流 MIPv6 切换算法的安全机制和安全性具体需求，便会发觉 MIPv6 切换的安全现状并不能保证 MIPv6 在现存的网络威胁下的实际运用。而另一方面，由于近年来移动设备性能的发展和价格的迅速降低，MIPv6 的市场已经凸现，如何解决 MIPv6 切换算法的安全问题日益成为一个研究的热点。IETF 在 RFC3775，RFC3776 中定义了一些安全机制[1,2]，而 RFC4225 针对包括途中(On-Path)攻击在内的路由优化方面的威胁提出了一些解决方案[34]。其它安全性解决方案包括解决 MN 和 AR 相互认证的基于 LKE 的移动安全机制、基于 CGA 的 MN 认证机制和基于身份加密的双认证方案、解决 MN 和 CN 相互认证的基于 PAK 的 BU 方法，以及投入实用必须解决的 AAA 问题等[36-41,44]。

基于已有的安全方案和机制，我们可以得出以下结论：①MN 和外地链路的 AR 之间信任关系可以通过 LKE 协议中 LBSA(Local Binding SA)建立和维护，并和 PAR，NAR 进行基于身份加密的双认证。②在 MN 开始漫游并接入外地链路之前，MN 和 HA 之间有一个预先建立的 SA；使用 IPsec 安全关联保护 MN 与 CN 之间 BU 和 BA 的完整性和真实性；SA 的建立和维护由 IKE 协议完成[35]。③MN 和 CN 之间不存在预先建立的 SA；使用返回可路由(Return Routability，RR)过程保护 MN 和 CN 之间的 BU；在具有预共享密钥或 PKI 的支持的条件下，可以使用基于 PAK 的 BU 方法或使用 IPsec 机制保护 MN 和 CN 之间的所有通信。④HA 对 MN，MN 与 CN 之间的认证授权计费可以通过运营商的 Diameter 等 AAA 机制实现，而且然而不同管理域之间的 AAA 服务器之间的认证与安全通信仍是个问题。总之，目前的状

[3] 本文的拒绝服务攻击指由 MIPv6 选项引起的重定向攻击和反射攻击。

[4] 不加密的数据流还可以导致中间人攻击。

况是由于缺乏 PKI 的支持，在保证可扩展性的前提下，MN 和 CN 以及 AR 之间只能建立比较弱的信任关系，因此很容易受到重定向攻击、中间人攻击、拒绝服务攻击等的威胁。

3 MIPv6 代表性切换算法安全性分析

IPv6 移动性支持方面影响较大且具有代表性的切换算法包括 BMIPv6，HMIPv6，FMIPv6，FHMIPv6 和 FFHMIPv6[1,7,14-16]。根据第二部分的 IPv6 移动性支持安全需求和现状，针对各个具体算法涉及的网络元素之间通信，其安全性需求如表 1 所示。

表 1 代表性算法具体安全性需求

	BMIPv6	HMIPv6	FMIPv6	FHMIPv6	FFHMIPv6
(1)MN-HA	√	√	√	√	√
(2)MN-CN	√	√	√	√	√
(3)MN-AR	√	√	√	√	√
(4)PAR-NAR			√		
(5)MN-MAP		√		√	
(6)MAP-NAR				√	
(7)MN-CoR					√
(8)CoR-NAR					

• BMIPv6 解决 IPv6 最基本的移动性支持问题。由于 MN 需要和 HA，CN 绑定其当前位置，并保证对外地链路的威胁具有一定的免疫能力，BMIPv6 需要提供 MN 与 HA，MN 与 CN，MN 与 AR(包括 PAR 和 NAR)之间需要进行身份认证和通信保护。

• HMIPv6 区分域间的宏切换和域内的微切换，并在域间切换和域内切换时分别向一个被称为 MAP 的本地根 AR 注册和进行 BU，即在域内移动时把该 MAP 作为临时 HA，减少切换时 MN 向真实 HA 和 CN 发送 BU 消息的数量，缩短了切换的延时。与 BMIPv6 一样，HMIPv6 与底层的接入技术无关，是一种网络层的切换管理技术，但由于引入了 MAP，也引入了新的安全威胁，HMIPv6 在安全性方面需要扩展 MN 和 MAP 之间的双向认证、完整性保护和对重放攻击的保护，所以在 MAP 和 MN 之间建立强的 SA 非常重要。

• FMIPv6 允许 MN 在进入新的链路之前就完成 CoA 的配置，以在新的接入点处尽快恢复 IP 连接，即在 MN 完成 HA 和 CN 的注册前，通过在新的 AR 和旧的 AR 之间建立隧道，新的接入点就可以向 MN 传送 IP 数据包，使得在比较费时的移动 IP 注册前就可以恢复实时业务，而且当和链路层切换紧密结合时(比如利用 IEEE802.11 的 AP 信息)可以更大程度地缩短移动检测和 CoA(Care of Address)的配置过程引起的延时。由于 FMIPv6 需要在安全性相对薄弱的 MN 和 AR 之间引入一些扩展，产生的安全威胁也相应较多，包括假冒合法 MN 发送 FBU 导致的重定向或数据窃取、合法 MN 有意无意的重定向攻击等，所以在 MN 与 AR，PAR 与 NAR 之间需要进行身份认证和数据完整性保护。

• FHMIPv6 与 FMIPv6 的区别在于 MN 发送 FBU，请求快速切换的对象不是 PAR，而是 MAP，并且在切换完成之前需要建立 MAP 和 NAR 之间的临时隧道，所以需要保证 MN 与 MAP，MAP 与 NAR 之间的通信安全。

• FFHMIPv6 切换算法利用 IPv6 中流标签识别每一个通信流，并在切换过程中，MN 向 HA 发送 BU 时，邻接路由器(Cross-over Router，CoR[5])把通过 PAR 发往 MN 原 CoA 的数据重定向到 MN 的新 CoA，以尽量减少由于切换时数据流到 MN 的路径改变而带来的延时。FFHMIPv6 建议大部分的路由器填写控制流属性，维持数据流状态信息。数据流由 IPv6 流标签和数据包的源、目地址识别。在 MN 移动时，这些信息可以用来控制数据流向。与 BMIPv6 类似，对 FFMIPv6 最大的威胁还是存在于对 FFHBU 的处理过程，包括对发送 FFHBU 的 MN 的假冒、对 FFHBU 中流标签的篡改等，当然 CoR 还必须对 NAR 进行认证，所以 FFHMIPv6 需要在 MN 与 CoR，CoR 与 NAR 之间采取相应的安全机制。

下面主要根据表 1 中各个具体网络元素之间的通信安全需求对各个切换算法安全性和存在的不足进行分析。

(1)MN-HA

上述算法(2)-(5)均兼容 BMIPv6，即使用 IPsec 的 SA 来保护 MN 和 HA 之间 BU 和绑定确认的完整性和真实性，同时，MN 和 HA 支持非空(non-NULL)的负载认证算法以提供数据的原始鉴别、无连接的完整性和可选择的防重放保护。IPsec SA 支持 SA 的人工配置或使用 IKE 的自动密钥管理，使用 IKE 时，IPsec 的安全策略数据库(Security Policy Database，SPD)能精确地标识 IKE 第一阶段的证书，该证书用来授权建立 SA。IPsec 过程实现了 MN 和 HA 之间的双向认证、完整性保护和信道保密，有效防止了身份假冒、数据劫持、被动窃听和中间人攻击，并大大减轻了拒绝服务攻击的危害。

(2)MN-CN

上述各个切换算法均使用 RR 过程对向 CN 发送 BU 的 MN 进行身份认证。RR 过程利用同时在 MN-CN 和 MN-HA-CN 两条路径上交换节点密钥、随机数、cookies、令牌和加密函数来构建绑定管理密钥 Kbm，并使用该密钥和加密 Hash 算法来保护 MN 到 CNBU 的完整性和真实性。RR 过程使用序列号和 MAC 保护双方免受 BU 的重放攻击。RR 过程限制了 Internet 上对某一路径拥有访问权的潜在攻击者，避免了在 Internet 的任何地址伪造 BU，但该方法不能保证 MN 和 CN 之间的 BU 不受在 HA 到 CN 路径上的攻击者的威胁，这些威胁包括身份假冒、中间人攻击、重定向和反射等拒绝服务攻击等。

(3)MN-AR

MN 和 AR 之间的身份认证和通信保护也是各个切换算法都需要解决而未完全解决的问题。根据第 2 部分的分析，在 MN 和 AR 之间不存在安全关联的情况下，即使假设 AR 安全，也会导致重定向等拒绝服务攻击，这在 MN 发生切换时假冒默认路由器和利用 PAR 作为临时 HA 时威胁很大。关于这方面的问题，有研究者提出 MN 在接入 AR 时利用任何现存的包括 IKE 等 SA 协商机制和 AR 建立安全 SA，这样可以阻止上述第二种威胁，而且在 FMIPv6 中利用它为 FBU 服务，可以确保 PAR 收到的 FBU 来自拥有 PCoA 的合法 MN，即该机制应用于 RtSolPr 等邻居发现协议，使 PAR 能够确保数据包的源 IP 只能来自链路地址在 PAR 邻居缓存中已经存在的 MN，这样假冒的 MN 不能使用受害 MN 的 IP 对数据进行恶意重定向。该机制对于合法的 MN 有时有意或无意发送安全的 FBU，还是可能会导致重定向数据阻塞 NAR 的缓存。不过，由于对应于 NCoA 的 NAR 切换状态的生命周期有限，威胁的程度相对较小。基于上述机制，在假设 PAR 和 NAR 之间存在安全 SA 的条件下，NAR 可以丢弃 FMIPv6 中一个恶意 MN 发送的一个以已使用的合法 IP 作

[5] 从 PAR 和 NAR 到 HA，CN 的第一个公用的路由器。

为其 NCoA 的 FNA，阻止对数据的重定向攻击。然而，当一个恶意 MN 以 NAR 的一个可用 IP 作为其 NCoA 向其发送包含 FBU 的 FNA 时，NAR 必须为其维护状态，并向 MN 的 PAR 发送 MN 的 FBU，这样，即使 PAR 通过验证拒绝这个 FBU，这个过程可以导致对 NAR 的拒绝服务攻击。FHMIPv6，FFHMIPv6 中 MN-AR 的安全性与 FMIPv6 类似。

(4)PAR-NAR

在 FMIPv6 中，PAR 和 NAR 之间在 MN 切换时，需要通过交换 HI 和 Hack 信息确保 MN 配置的 NCoA 的可用性，并建立安全隧道。由于路由器相对稳定，属于 Internet 基础设施，这里假设 AR 安全，并在各个 AR 之间建立强 IPsec 的 SA，以保证 AR 之间的信任关系，防止恶意节点假冒 AR 通过发送 HI 请求消耗路由器资源，从而导致拒绝服务攻击。强 SA 也防止了数据劫持与重放、中间人攻击等威胁。

(5)MN-MAP

在 HMIPv6 和 FHMIPv6 中，通过使用 IKE 协议为 MN 和其 MAP 建立以 RCoA 作为 MN 身份的 SA，这和 MN 与 HA 建立 SA 以 MN 的 HoA 作为其身份一样。由于 RCoA 是临时的，并不和任何一个特定的节点绑定，MN 没有开始就去证明它拥有这个 RCoA，这和 MN 的 HoA 不一样。该 SA 保证 MAP 可以验证一个特定 RCoA 的 LBU(Local BU)来自为这个 RCoA 建立 SA 的同一个 MN，所以 MAP 没有必要知道 MN 的身份和 HoA。在 SA 建立后，HMIPv6 使用 IPsec 的传输模式保护 MN 到 MAP 的本地 BU。这些机制在一定程度上实现了 MN 和 MAP 的双向认证，保护域内切换时从 MN 到 MAP 的代理路由器通告请求消息和代理路由器通告消息，防止恶意主机发送合法 RCoA 的 LBU，但和 MN 与 CN，AR 的关系一样，对 MN 到 MAP 途中的中间人攻击以及由此导致的身份假冒、绑定篡改、拒绝服务攻击等攻击无能为力。虽然目前也有利用 HA 作为 MN 的 CA 以实现 MAP 和 MN 之间更强的认证，但 MAP 和不同域的 HA 之间信任关系的建立仍是一个问题[42]。

(6)MAP-NAR

和 FMIPv6 中 PAR-NAR 的关系一样，FHMIPv6 中 MAP-NAR 在假设路由器相对稳定安全，并在 AR 之间建立强 IPsec 的 SA 条件下，可以保证 MAP 与 NAR 之间的信任关系，防止拒绝服务攻击、数据劫持与重放、中间人攻击等威胁。

(7)MN-CoR

FFHMIPv6 中，FFHBU 的途中路由器使用 MN 的原 CoA 和流标签对 FFHBU 进行检查。在 FFHBU 到达 CoR 后，CoR 对发送 FFHBU 的 MN 身份进行验证。这里的 MN 的身份由 MN 的 PAR 对 MN 原 CoA 加密得到，相当于 PAR 对 MN 颁发的关于 MN 原 CoA 的证书。然而，这里存在 CoR 凭什么去信任 PAR 的问题，而且当攻击者在原 CoA 附近时还是可以假冒 MN 的身份，发动重定向、反射等拒绝服务攻击。注意，FFHMIPv6 对恶意路由器等不诚实的网络基础设施无能为力[43]。

(8)CoR-NAR

FFHMIPv6 中，CoR-NAR 之间的安全性与上述的(4)、(6)类似，依赖于固定路由器的安全以及之间预先建立的安全 SA 这个假设。

上述各切换算法一脉相承，都是为了实现节点的基本切换功能，进而实现分层切换、无缝切换，并保证一定的切换安全性，根据上面的分析，各切换算法存在的安全性问题见表 2。

表 2　代表性算法安全性问题

	BMIPv6	HMIPv6	FMIPv6	FHMIPv6	FFHMIPv6
身份假冒	MN-AR：弱	MN-AR：弱	MN-AR：弱	MN-MAP：弱	MN-AR：弱
被动窃听	MN-CN：中	MN-CN：中	MN-CN：中	MN-AR：弱	MN-CN：中
		MN-MAP：弱		MN-CN：中	MN-CoR：弱
拒绝服务攻击	MN-CN：中	MN-MAP：弱	MN-CN：中	MN-MAP：弱	MN-CN：中
中间人攻击		MN-CN：中		MN-CN：中	MN-CoR：弱

综上可以看出，由于强 IPsec SA 的保护，MIPv6 提供了 MN 到 HA 和 CN 的绑定更新、移动前缀发现的完整性、机密性等保护机制，在一定程度上缓解了拒绝服务攻击、中间人攻击等对 MIPv6 切换的威胁，目前问题是 MIPv6 的自举，尤其在部署大规模 MN 的时候，即如何为 MN 分配 HA 和 HoA 以及和 HA 的共享秘密。MN 到 CN 之间的安全性由于 RR 过程的保护，除了途中合作攻击威胁较大外，总体安全性较高。然而，由于 MN 和外地链路 AR 之间缺乏必要的认证，可以导致拒绝服务攻击等威胁，安全环节比较薄弱。最近 Hyun-Sun Kang 等提出了可以借鉴与其它 MIPv6 切换算法的关于 FHMIPv6 的一些保护机制[45]：利用 AAA 协议的家乡服务器和 MN 的共享秘密以及 AR，AAA 外地服务器、AAA 家乡服务器之间的信任关系来帮助 AR 和 MN 之间进行认证，并建立防止 MN 和 AR 相互欺骗共享秘密，以对 MN 和 AR 之间的路由器信息、本地 BU 加以保护。然而，不同提供商、不同域之间 AAA 服务器之间的信任关系的建立仍然是个问题，目前还不能依赖不太健全的 AAA 基础设施。基于此，本文建议 MN 和 AR 之间利用 IKE 协商建立临时 SA，以在切换时，缓减利用 PAR 和 MN 的相互无法验证进行身份假冒、拒绝服务等攻击带来的威胁。

4　研究中存在的问题和需要进一步研究的内容

上文总结了当前 MIPv6 切换研究中代表性算法的安全性，在介绍中也指出了其存在的缺陷，下面进一步将切换研究中存在的安全问题和需要进一步研究的内容概括为以下几点：

(1)域间设备的信任问题

由于域间设备之间不存在预设的共享秘密，MN 和 CN 以及外地网络的 AR 之间不能实现相互的强认证，这导致了上述的许多威胁，因此需要基于进一步研究部署方便、容易实现的 PKI，AAA，信任传递等安全认证机制。

(2)移动设备的自举问题[47]

MIPv6 切换要求 MN 知道 HA 的地址、MN 的 HoA 以及和 HA 建立 IPsec 安全关联所需的共享秘密。然而，MIPv6 切换算法没有定义任何 MN 自动获取这些信息的方法。这就意味着每一个网络管理员必须对 MN 和 HA 进行手工配置。然而，在真实的使用环境下，手工配置在 MN 使用数量增长时缺乏可扩展性，而自举的目的就是通过自举网络自动为 MN 提供这些配置信息。目前，自举的使用环境可根据 MN 网络接入认证授权者(Access Service Authorizer，ASA)和 MIPv6 服务认证授权者(Mobility Service Authorizer，MSA)之间的关系分为分布场景(split scenario)和集成场景(integrated scenario)。可研究的内容包括基于 AAA 协议、IKEv2 或 DHCP 的动态 HoA，HA 和预共享秘密配置等，需要解决的问题包括恶意网络提供假的 HA 和配置信息导致的数据窃取和拒绝服务攻击、恶意 MN 提供假的证书获得移

动服务授权、自举网络和 MN 的中间人攻击。

(3)移动设备的位置隐私保护不够

在 MN 从一个网络漫游到另一个网络时，MN 虽然可以利用和 HA 的隧道，通过 HA 和 CN 通信，屏蔽 MN 的当前位置，而且 MN-HA 的隧道可以通过加密保护位置隐私，但在实现路由优化后，CoA 向 CN 暴露了 MN 的位置，而且任何一个途中节点只要窃取 MN 的 BU 消息或绑定确认消息，甚至是 MN 和 CN 之间的数据包就可以了解到该 MN 发生了移动，因为这些消息中都包含了两个地址 CoA 和 HoA，所以在路由优化模式下如何向途中节点隐藏 HoA 和 CoA 关系，防止 MN 当前位置信息的泄漏是下一步要研究的内容。

(4)移动设备的处理能力不足

IPSec 的密钥管理要求终端具有很强的处理能力，而未来使用移动 IP 的设备诸如手机、PDA 计算能力都很弱，而且能源供应也有限，因此要求进行大量计算的安全机制不太适合这些设备。为此有人提出了一种称为定制密钥(PBK，purpose built key)的轻量级的安全保护协议。PBK 协议中，在每一个移动 IP 会话之前，通信双方产生一对新的密钥，这对密钥是临时的，只有通信双方能够使用，无需向第三方注册。当会话结束时，密钥失效。PBK 协议简单，但安全性没有 IPSec 好，如没有解决中间人攻击等问题，并且 PBK 实现的不是用户认证，而是设备认证。因此，基于 RSA 等构建适用于计算能力不平衡的网络设备之间的密钥管理机制是将来需要研究的内容。

(5)安全机制导致切换延时增加

支持安全实时服务的挑战之一是保证在切换时用最小的额外时延实现 MN 向 HA 和 CN 的注册，然而引入 IPsec，RR 过程等安全机制增加了大量切换延时，比如 RR 过程花费的时间至少是 MN 和 CN 之间数据来回的 1.5 倍，每一次切换执行 RR 过程对将来支持实时服务很不利[46]，所以，基于上下文转移(Context Transfer)等机制提供相同或更高安全等级的 MN 向 HA 和 CN 快速注册的方法依然是将来的研究内容。

由此看来，MIPv6 的切换安全性还存在许多问题，这些问题构成了 MIPv6 研究的丰富内容，这些研究内容之间有着极为密切的关系，它们是相互制约、相互促进、不可分割的整体。

结束语 本文综述了 MIPv6 切换算法的发展及其安全性研究现状，并对代表性切换算法的安全性和当前存在的问题进行了分析。目前的 MIPv6 切换算法形成了 HMIPv6 和 FMIPv6 两大主流，并在改进和融合的基础上不断提高其性能，以实现对实时服务的支持，然而，在其安全性方面，各主流代表性切换算法及其研究现状都仍然存在许多问题，包括域间设备的信任问题、移动设备的自举问题、移动设备的位置隐私保护等。总之，MIPv6 切换算法已经取得了初步的研究成果，但是大多数的算法还没有考虑实际应用的诸多安全性方面的困难，还有许多问题需要进一步研究，特别是需要探索在移动设备计算能力、域间的信任基础设施等实际应用背景下对切换安全性的具体需求和解决方案。

参 考 文 献

[1] Johnson D, Perkins C, Arkko J. Mobility support in IPv6. IETF RFC 3775, June 2004

[2] Arkko J, Devarpalli V, Dupont F. Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents. IETF RFC 3776, June 2004

[3] Andersen F-U, Caviglione L. Survey of IPv6 functional interoperability for mobile Internet // IEEE 2nd International Conference on Mobile Technology, Applications and Systems. Berlin, Germany, 2005

[4] Lee J-H, Chung T-M. Performance Evaluation of Dual Authentication Scheme in Mobile IPv6 Networks // IEEE International Conference on Systems and Networks Communications. Tahiti, French, 2006

[5] Panoutsopoulos I C, Kotsopoulos S. Handover and new call admission policy optimization for G3G system. ACM Wireless Network, 2002(8): 381-389

[6] Alexe E, Mark I B. Modeling and Analysis of Fast handoff algorithms for Microcellular Networks // IEEE/ACM International Conference on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems. Fort Worth, USA, 2002

[7] Koodli R. Fast Handovers for Mobile IPv6. IETF RFC 4068, 2005

[8] An Y-Y, Yae B H, Lee K-W, et al. Woo Young Jung. Reduction of Handover Latency Using MIH Services in MIPv6 // IEEE international conference on advanced information networking and applications. Vienna, Austria, 2006

[9] Perkins C, Johnson D. Mobility support in IPv6 // 2nd Annual International Conference on Mobile Computing and Networking. New York, USA, 1996

[10] Wang Y, Chen W, Ho J S M. Performance Analysis of Mobile IP Extended with Routing Agents. Technical Report, 9-CSE-13. Southern Methodist University, 1997

[11] Castelluccia C. HMIPv6: A Hierarchical Mobile IPv6 Proposal. ACM Mobile Computing and Communications Review, 2000 (1): 48-59

[12] Hwang S-H, Fe B-K, Han Y-H, et al. An Adaptive Hierarchical mobile IPv6 with route optimization // 57th IEEE Semiannual Vehicular Technology Conference. Jeju, Korea, 2003

[13] Vhldi I, Ali B M, Habaebi H, et al. Routing Scheme for Macro Mobility Handover in Hierarchical Mobile IPv6 Network // 4th National Conference on Telecommunication Technology. Selangor, Malaysia, 2003

[14] Soliman H, Castelluccia C, Malki K E, et al. Hierarchical Mobile IPv6 Mobility Management. IETF RFC 4140, Aug. 2005

[15] Sulander M, Hamalainen T, Viinikainen A, et al. Flow Based Fast Handover Method for Mobile IPv6 Network // IEEE 59th Semiannual Vehicular Technology Conference. Los Angeles, USA, 2004

[16] Young J H, Soliman H, et al. Fast Handover for Hierarchical MIPv6 (F-HMIPv6). IETF Internet draft: draft-jung-mipshop-fhmipv6-00, Apr. 2005

[17] Hossain A K M M, Kanchanasut K. A Handover Management Scheme for Mobile IPv6 Networks // 14th International Conference on Computer Communications and Networks. San Diego, USA, 2005

[18] Koodli R. Fast Handovers for Mobile IPv6. IETF Internet Draft: draft-ietf-mobileip-fast-mipv6-05, Sep. 2002

[19] Gwon Y, Yegin A. Enhanced Forwarding from the Previous Care-of Address(EFWD) for Fast Handovers in Mobile IPv6 // IEEE Wireless Communication and Networking Conference. Atlanta, USA, 2004

[20] Li R, Li J. An Enhanced Fast Handover Scheme for Mobile IPv6 // ACM International Wireless Communications and Mobile Computing Conference. Vancouver, Canada, 2006

[21] Jordan N, Poropatich A, Fleck R. Link Layer Support for Fast Mobile IPv6 Handover in Wireless LAN based Networks // 13th IEEE Workshop on Local and Metropolitan Area Networks. Mill Valley, USA, 2004

[22] Park B, Latchman H A. Fast Handover Scheme Based on Enhanced Access Point (EAP) for Mobile IPv6 // IEEE International Conference on Advanced Communication Technology. Phoenix Park, Korea, 2006

(下转第 83 页)

ings of the First Asia International Conference on Modelling & Simulation. Washington, DC: IEEE Computer Society, 2007: 198-199

[4] Intanagonwiwat C, Govindan R, Estrin D, et al. Directed diffusion for wireless sensor networking. IEEE/ACM Trans. on Networking, 2003, 11(1): 2-16

[5] Braginsky D, Estrin D. Rumor routing algorithm for sensor networks // Proc. of the 1st Workshop on Sensor Networks and Applications. Atlanta: ACM Press, 2002: 22-31

[6] Sadagopan N, Krishnamachari B, Helmy A. Active query forwardingin sensor networks. Elsevier Ad Hoc Networks Journal, 2005, 3(1): 91-113

[7] Helmy A. CAPTURE: location-free contact-assisted power-efficient query resolution for sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review, 2004, 8(1): 27-47

[8] Haas Z J, Pearlman M R. The Performance of Query Control Schemes for the Zone Routing Protocol. IEEE/ACM Transactions on Networking, 2001, 9(4): 427-438

[9] Helmy A. Mobility-assisted Resolution of Queries in Large-scale Mobile Sensor Networks (MARQ). Computer Networks Journal -Elsevier Science, 2003, 43(4): 437-458

[10] Watts D J, Strogatz S H. Collective dynamics of 'small-world' networks. Nature, 1998, 393: 440-442

[11] De Nardis L, Di Benedetto M-G. The Small World Routing: A methodological framework for driving the emerging topology of energy-constrained multi-hop wireless networks // IEEE Radio and Wireless Simposium. San Diego: IEEE Press, 2006: 599-602

[12] Sharma G, Mazumdar R. Hybrid sensor networks-A small world // Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing. Urbana-Champaign: ACM Press, 2005: 366-377

[13] Chitradurga R, Helmy A. Analysis of Wired Short Cuts in Wireless Sensor Networks // ACS/IEEE International Conference on Pervasive Services. Beirut: IEEE press, 2004: 39-48

[14] Helmy A. Small Worlds in Wireless Networks. IEEE Communications, 2003, 7(10): 490-492

[15] Breslau L, Estrin D, Fall K, et al. Advances in Network Simulation. IEEE Computer, 2000, 33(5): 59-67

[16] 郭龙江,李建中,李贵林. 无线传感器网络环境下时-空查询处理方法. 软件学报, 2006, 17(4): 794-805

[17] 谢磊,陈力军,陈道蓄,等. 无线传感器网络的查询处理机制研究综述. 计算机科学, 2006, 33(9): 45-49

[18] 赵志滨,于戈,李斌阳,等. 无线传感器网络中基于动态过滤器的多维 K-NN 查询优化算法. 软件学报, 2007, 18(5): 1186-1197

(上接第 53 页)

[23] Adibi S, Naserian M, Erfani S. A fast handover M-MANET with QoS support // IEEE Conference on Electrical and Computer Engineering. Saskatchewan, Canada, 2005

[24] Shim M, Kim H, Lee S. A Fast Handover Mechanism for IPv6 Based WiBro System // IEEE 8th International Conference on Advanced Communication Technology. Phoenix Park, Korea, 2006

[25] An Y, Yae B, Lee K, et al. Reduction of Handover Latency Using MIH Services in MIPv6 // IEEE International Conference on Advanced Information Networking and Applications. Vienna, Austria, 2006

[26] McCann P. Mobile IPv6 Fast Handovers for 802.11 Networks. IETF RFC 4260, Nov. 2005

[27] Eu Y C, et al. Multicast Based and Fast Handover Scheme in MobileIPv6Wireless Network // IEEE International Workshop on Antenna Technology: Small Antennas and Novel Meta-materials. Singapore, 2005

[28] Emst T, Castelluecia C, Lmh H-Y. Extending Mobile-IPv6 with Multicast to Support Mobile Networks in IPv6 // 1st European Conference on Universal Multi-service Networks. Colmar, France, 2000

[29] Ome K, Ikeda T, Inoue M, et al. Mobile Node Extension Employing Buffering Function to Improve Handoff Performance. 5th International Symposium on Wireless Personal Multimedia Communications. Singapore, 2002

[30] Pawnapongpibul L, Mapp F. A Client-based Handoff Mechanism for Mobile IPv6 Wireless Networks // 8th IEEE International Symposium on Computers and Communication. Antalya, Turkey, 2003

[31] Natalizio E, Scicchitano A, Marano S. Mobility Anchor Point Selection Based on User Mobility in HMIPv6 Integrated with Fast Handover Mechanism // IEEE Wireless Communications and Networking Conference. New Orleans, USA, 2005

[32] Nikander P, Harkins D. Threat Models introduced by Mobile IPv6and Requirements for Security in Mobile IPv6[S]. IETF Internet Draft: draft-ietf-mobileip-mipv6-scrty-reqts-02, Nov. 2001

[33] Narten T, Draves R. Privacy Extensions for Stateless Address Auto configuration in IPv6[S]. IETF RFC 3041, Jan. 2001

[34] Nikander P, Aura T, Arkko J, et al. Mobile IPv6 Route Optimization Security Design Background[S]. IETF RFC 4225, Dec. 2005

[35] Harkins D, Carrel D. The Internet key exchange (IKE)[S]. IETF RFC 2409, Nov. 1998

[36] Liu Changwen, Soliman H. Local key exchange for mobile IPv6 local binding security association // IEEE 59th Vehicular Technology Conference. Los Angeles, USA, 2004

[37] Ryu S, Mun Y. An Optimized Scheme for Mobile IPv6 Handover between Domains Based on AAA // IFIP International Conference on Embedded and Ubiquitous Computing. Seoul, Korea, 2006

[38] Lee J-H, Chung T-M. Performance Evaluation of Dual Authentication Scheme in Mobile IPv6 Networks // IEEE International Conference on Systems and Networks Communications. Tahiti, French, 2006

[39] Yoon H-S, Kim R-H, Hong S-B, et al. Heung-Youl Youm. PAK-based Binding Update Method for Mobile IPv6 route optimization // IEEE International Conference on Hybrid Information Technology. Cheju Island, Korea, 2006

[40] Le F, Patil B, Perkins C E, et al. Diameter mobile IPv6 application. Internet IETF Draft: draft-le-aaa-diameter-mobileipv6-04, Nov. 2004

[41] Wei Da, Liu Yanheng, Yu Xuegang, et al. Research of Mobile IPv6 Application Based On Diameter Protocol // International Multi-Symposiums on Computer and Computational Sciences. Hangzhou, China, 2006

[42] Choi J, Mun Y. Mechanism of Authenticating a MA Pin Hierarchical MIPv6 // 1st International Conference on Grid and Pervasive Computing. Taiwan, 2006

[43] Ghebregziabher T, Puttonen J, Hämäläinen T, et al. Security Analysis of Flow-based Fast Handover Method for Mobile IPv6 Networks // IEEE International Conference on Advanced Information Networking and Applications. Vienna, Austria, 2006

[44] Haddad W, Krishnan S. Combining Cryptographically Generated Address and Crypto-Based Identifiers to Secure HMIPv6. IETF Internet Draft: draft-haddad-mipshop-hmipv6-security-01, Oct. 2005

[45] Lee J K, Yi O, Yung M. Authenticated Fast Handover Scheme in the Hierarchical Mobile IPv6 // Springer 3rd International Workshop on Web Information Systems and Applications. Nanjing, China, 2006

[46] Kafle V, Kamioka E, Yamada S. Extended correspondent registration scheme for reducing handover delay in mobile IPv6 // 7th International Conference on Mobile Data Management, Nara, Japan 2006

[47] Patel A, Giaretta G. Problem Statement for Bootstrapping Mobile IPv6 (MIPv6). IETF RFC 4640, Sep. 2006