综述:关于IPv6安全性问题的研究*)

陆 音 石 进 黄 皓 谢 立
(南京大学计算机软件新技术国家重点实验室 南京 210093)
(南京大学计算机科学与技术系 南京 210093)

摘 要 提供强有力的网络安全保障是实现IPv6成功应用的关键。本文在对IPv6新特性进行分析的基础之上,从多个角度考察和归纳了IPv6在安全方面所引入的若干新问题,介绍了其对应的安全机制及其研究进展,并尝试从整体上评估IPv6对将来网络安全状况的影响。

关键词 IPv6,网络安全,安全威胁,安全措施

A Survey on Security Issues in IPv6

LU Yin SHI Jin HUANG Hao XIE Li
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract To ensure the network security is the key to achieve successful applications of IPv6. In this paper, many new secure issues introduced by IPv6 are examined and summarized from a lot of aspects, based on the analysis of IPv6's novel features. The corresponding mechanisms of security and their working progress are discussed. We also evaluate the influence of IPv6 on the network security status in future at the end of the paper.

Keywords IPv6, Network security, Secure threat, Secure measure

1 引言

IPv4协议[1]是目前因特网互连技术领域公认的标准,在其应用和技术得到不断推广和深化的同时,也使得因特网从一个最初的研究性网络逐步扩展成为了一个拥有数百万节点的全球性综合性网络。随着IPv4互联网规模的不断增长及其应用范围的不断拓宽,它在地址数量、移动性、服务质量及安全性等方面所具有的设计局限性也越来越明显。为此,因特网工程任务组IETF提出了新一代因特网互连协议——IPv6[2]。

提供比IPv4协议更为有力的网络安全保障是IPv6技术进一步发展和成功应用的关键所在。全新IPv6协议的提出一方面有助于我们在下一代网际互连协议中实现更多的安全特性,另一方面,它在其他诸多方面所引入的新特性也将对当前的网络安全状况产生不容忽略的深远影响。

本文在对IPv6技术进行综合分析的基础之上,考察和归纳了IPv6在安全方面所引入的若干新问题及其相应的安全技术,以期对目前IPv6安全性问题的研究有所帮助。文章的第2部分简单回顾了IPv4所存在的问题以及IPv6的技术特点;第3部分对IPv6中安全性问题较为集中的8个方面进行了分析和总结,并分别论述了其各自的研究进展;最后给出了当前IPv6安全性研究现状的总结。

2 IPv4及IPv6技术概况

2.1 IPv4的问题

地址资源耗竭、安全问题严重以及业务性支持欠缺是IPv4所面临的三大难题,同时也是引入IPv6协议的主要推动力。

IPv4地址空间耗竭问题始于20世纪90年代企业网的迅猛发展,究其原因,主要在于IPv4效率低下、地址浪费严重的分级网络编址机制及其设计初期对发展规模预期的不足。人们提出了NAT[3]地址转换机制,期望以地址分配复用的方式部分缓解编址空间耗竭的压力。然而,随着互联网接入技术及其应用的发展,xDLS宽带接入、GRPS/3G数据移动业务和P2P/网格计算模式等要求主机能够长期在线的应用需求越来越强烈,这使得IPv4地址不足的问题不断恶化,其寻址与路由机制的可扩展性也已趋近极限。

网际互连是IPv4初期设计解决的主要问题。限于当时较小的网络部署规模和有限的应用方式,IPv4协议的安全性需求曾一度被忽略。时至今日,尽管人们先后提出了多种辅助安全机制,IPv4本身依然是一个缺乏内在安全保障的协议架构。IPv4寻址、路由和配置维护等多方面基础安全机制的缺失严重制约了电子商务、电子政务等诸多新兴应用的发展,同时由于其网络配置、维护及管理的复杂性,令当前IPv4互联网应用所面临的攻击威胁进一步加重。

此外,IPv4对业务性的支持严重欠缺。IPv4简单的路由、配置方式缺乏灵活性,不能实现可靠、高效的移动服务,它为早期低速网络互连所设计的传输控制机制也已不再适应目前高达10G乃至TByte量级的高性能网络环境。同时,IPv4中还缺乏有效的服务控制措施,无法为新兴媒体应用提供流

*)本文研究得到国家"863"计划项目(NO:2003AA142010)资助。陆 音 博士研究生,研究方向:信息与网络安全,系统安全;石 进 博士研究生,研究方向:安全操作系统与网络安全;黄 皓 教授,博士生导师,研究方向:计算机网络安全,分布式系统;谢 立 教授,博士生导师,研究方向:信息与网络安全,安全操作系统,分布式操作系统。

量、延迟、抖动等必需的服务质量保障。

2.2 IPv6 中引入的改进

从地址空间、高性能、安全性、业务性支持、配置和维护等5个角度考虑，IPv6主要针对如下几个方面进行了改进及增强：

1. 支持单地址长度高达128bit的网络寻址架构，并定义了全局聚合单播地址、本地链路地址、多播/选播地址、v6-v4兼容地址和测试地址等一系列地址类型；

2. 传输控制及路由交换性能的提高。简化报头及扩展选项定义，约束报文检视和分片机制，采用可聚合的层级化寻址、路由方式，从而更加适合交换式的高速网络环境；

3. 以标准建议形式强制性要求IPSec[4]的支持，其中包括了一个支持多种密钥加密方式的密钥交换-管理协议框架IKE，用以实现鉴别首部机制(AH)[5]和安全负载封装机制(ESP)[6]；

4. 明确定义了移动IP场合的主机注册、代理转接和优化路由机制[7]，任一IPv6移动主机在漫游的同时均能保持其原有的IPv6地址，实现与接入方式无关的端对端无缝通信；

5. 提供了流标签、服务优先级和路由策略等多种服务质量保障能力，实现了对分层编码、资源预留等实时网络控制的支持，具备综合集成的差异化数据服务提供能力；

6. 采用基于IP的邻居发现协议[8]替代链路层的ARP协议和部分ICMP功能，提供网络自动配置功能，以增强网络维护管理机制的健壮性，提高配置管理的效率。

3 IPv6所引入的安全性相关问题及对应机制分析

IPv6所引入的诸多新特性将从多个方面对IPv6网络的安全性产生直接或者是间接的影响。在下文中，我们将从8个方面来对其安全问题和各自的研究进展进行考察和归纳。

3.1 网络编址机制

网络寻址空间的大小对于目前的网络安全分析技术将产生直接的影响。IPv4相对较小的地址空间为网络攻击前期的拓扑检测、主机扫描以及攻击对象分析提供了便利，同时，IPv4网络下的蠕虫或者是木马病毒也多利用网络扫描的方式实现自身复制和传播。IPv6高达128bit的单地址长度将明显地有助于改善这种状况，然而，其所带来的安全性影响并不一定都是积极的，一方面，它使得流量窃听成为了IPv6环境下攻击者进行安全分析的主要方式，另一方面，庞大的地址空间也可能使得IDS、漏洞扫描、恶意主机检测等安全机制的实施变得更加困难。

IPv6引入了本地链路地址、全局聚合单播地址、IPv4兼容地址和随机生成地址等若干种新的地址类型及编址机制。其中，本地链路地址[9]无需DHCP/自动配置协议等外部机制干预即可自动根据网络接口标识符(如MAC地址)生成，实现不可路由的本地链路级端对端通信。尽管它提供了极大的配置便利，但与此同时也引入了额外的安全风险：移动恶意主机可以随时接入本地链路并实现对相邻主机或网关的攻击及非法访问，因此，有必要在IPv6本地链路地址应用当中引入相应的链路访问控制机制，依照“基本特权”原则对接入链路主机的通信能力加以约束，限制其只能访问最基本的网络服务。

全局聚合单播地址[10]则主要用以实现可在互联网全网范围内路由的任意点对点通信。为了提高路由表空间聚合效率和路由机制性能，它采用了层级式的子网分级编址机制，整个地址格式分为网络地址前缀和主机标识符两个部分，其中的主机标识符以基于链路层接口令牌(如MAC地址)创建的64位EUI-64形式加以描述，这意味着IPv6中规模最小的子网亦可容纳多达2^{64}个可用地址，类似IPv4中的扫描威胁已被极大削弱。但是，这种采用接口令牌和当前网络前缀导出主机地址的方式也简化了主机身份识别的过程，有可能泄漏用户身份，导致严重的隐私性问题。事实上，采用接口令牌方式创建接口标志符的方式部分削弱了IPv6庞大的地址空间带来的攻击抵制作用，比如，以太网MAC地址一般根据网络接口设备厂家来进行划分和分配，攻击者可以通过链路层流量窃听等多种方式来收集和分析子网中所采用的接口卡生产厂家的相关信息，或者进行有针对性的尝试，以达到迅速缩小地址搜索空间的目的，从而极大提高网络扫描速率。

针对上述问题，IPv6专门引入了随机地址生成机制[11]，以随机方式生成地址中的主机标识，并装配成为一个随机地址供主机临时使用。这种方式可以有效地抵制主机身份泄漏及小范围地址空间扫描尝试，但也同样给现有的网络安全管理机制带来了一系列新的负面影响[12]，例如，针对以随机生成地址为源地址的主机发起的攻击难以监控和追踪，其所发起的DoS攻击则更加难以进行有效防范。此外，随机地址对于整个网络安全策略的定义、实施和管理也提出了更高的要求。由于IPv6不再强调以单一IP地址的方式来标识主机，一个主机网络接口能够被赋予多个IP地址，而这些地址有可能同时具备可在因特网上路由的网络前缀，这种多宿主的网络地址配置方式和随机地址一样，在实现高度配置灵活性的同时，均要求网络安全策略中主机标识定义及其约束粒度能够与之相适应，从而在IPv6相对复杂的编址、配置方式下实现完备的整体安全策略和有效的访问控制机制。

3.2 报文格式定义

为适应当前高速网络环境，减少报文传输、处理所导致的带宽、延迟损耗和路由设备计算资源损耗，IPv6采纳了基本报头与可选的扩展报头相结合的分组格式，基本头格式简练，并且具有相对固定的长度，而扩展头则以选项链表的形式替代了IPv4下单一且长度不定的IP头选项字段，以提供良好的协议扩展性。出于中继处理效率及路由机制简洁性、高效性方面的考虑，IPv6标准建议中更进一步地规定：某些扩展头只能交由目的主机查看并处理，如分片扩展头、路由选择扩展头和部分类型的信宿选项报头等，源站和目标站之间的路由节点均不应当查看这些扩展数据，中间节点对这些主机扩展头的处理和解释是没有定义的。这项建议引起了广泛的争议，因为它事实上有可能与潜在的安全需求相抵触，譬如，信源和信宿之间的防火墙等边界访问控制节点将不得不对主机处理类型的扩展头数据进行严格检验，以保证流量的合法性；此外，IPv6建议规定只有主机才允许进行报文分片或重组操作，而防火墙、IDS等中间节点则完全有可能出于全面检查的缘故需要对报文分段进行先期组装和验证，这些安全机制所涉及的实现行为在目前的IPv6建议当中依然没有得到明确定义。

在通用扩展头选项类型当中，路由选择扩展头[13]的引入对IPv6网络安全性的影响最为显著。为提供与IPv4中ICMP源路由机制类似的设定路由能力，实现相应的路由排错及检测措施，任一IPv6主机均必须支持路由扩展头的处理，而这意味着任一IPv6主机均可具备报文转发的能力。这种源路由选择机制令攻击者有可能旁路边界访问控制机制的约

束实施针对 IPv6 内网的数据反射攻击和分布式 DoS 攻击，并且回避 ICMP iTrace[14] 等报文跟踪反馈机制，增加攻击源头追踪的难度；另一方面，路由选择扩展头设计的灵活性使得其成为了负载均衡等多种 IPv6 流量工程应用中重要的技术基础，同时它也是移动 IPv6 中实现上层协议针对三角路由优化过程透明性的关键机制，一旦网络中存在着流量工程及 IP 移动性支持的需要时，就必须提供路由扩展头处理支持，这使得我们不可能采取类似 IPv4 下限制 ICMP 的方式在网络边界上对其进行简单的封堵和屏蔽。上述问题再次表明，IPv4 下简单的网络边界控制方式在复杂的 IPv6 应用环境之下已不再适用，需要引入安全粒度更细、配置更为灵活的访问控制机制与之相适应，方可在保障 IPv6 网络安全性的同时满足其高性能、多业务的应用需求。

3.3 IPSec 与 VPN

以标准建议方式内建 IPSec 因特网安全互连协议的支持，尝试以协议透明的方式提供网络层流量鉴别、验证及加密功能，实现地址配置、寻址路由、服务提供及移动性支持等各方面的安全性提高，是 IPv6 安全性增强的一个显著特征。IPSec 包括了一个开放式的密钥交换及管理协议框架 IKE[15]，同时以插件形式兼容多种加解密算法，具有良好的协议开放性和扩展性，目前已被广泛地应用于组建虚拟专用网(VPN)等领域。然而，尽管它的引入为 IPv4/IPv6 提供了可靠的安全传输保障，在应用实践的过程中，IPSec 也暴露出了灵活性不够、互操作性较差、实现标准化欠缺等一系列缺陷。

作为一种“重量级”的网络安全机制，IPSec 的部署和实施需要网络边界、路由系统等外部环境的参与，这使得 IPSec 的通用性受到了一定的限制，其根源在于分布式网络自治环境下密钥部署及管理机制的复杂性和不灵活性，这一缺陷在强调任意端对端通信模式的 IPv6 网络环境中尤为突出。它给 IPSec 的配置和管理造成了较大的负面影响，同时也使得许多安全性要求较高的典型网络应用更为倾向于选择自定义的网络安全机制来实现安全增强，而不是盲目地信任外界网络环境；事实上，考虑到 IPv4 网络安全保障缺乏的历史性原因，许多基于 IPv4 发展起来的网络应用已经具备了自己的安全增强机制，如传输层的 SSL/TLS[16] 协议、应用层的 SSH/HTTPS/DNS-Sec[17] 等，这些自定义的安全机制在部署、配置和应用方面往往较 IPSec 更具针对性，因而也更加灵活、简便。此外，IPSec 的 API 应用开发接口仍然没有实现标准化。上述现状均阻碍了 IPSec 的进一步普及和应用。

难以实现与现有网络机制、安全机制之间良好的互操作性是目前 IPv6 下 IPSec-VPN 应用所面临的主要困难。任何在分组传输、路由的过程中端节点 IP 地址或端口发生改变的网络机制均与目前的 IPSec 协议存在着一定的兼容性问题，在运用了这些转换机制的网络环境中的主机将无法直接使用 IPSec 所提供的安全服务[18]。而 IPSec 协议中首部鉴别(AH)、安全负载封装(ESP)等安全机制端对端特性的存在则是造成其兼容性问题的根本原因。以 NAT 网络地址转换机制为例，NAT 对出/入站数据报报头中的地址、端口及 CRC 校验信息的修改将直接导致 AH 机制的失败，而在使用了 ESP 方式的 IPSec 部署环境下，所有真实数据报报头均已被加密，令 NAT 因不能检视并转换其内容而无法进行内/外网之间的双向地址转换，因而无法实现 NAT 与 IPSec 的互操作。针对上述问题，IETF IPSec 网络工作组专门提出了一个兼容协议方案——NAT-T[19]，尝试以 UDP 方式对 ESP 流量进行封装，并结合 IKE 中新增的 NAT 穿越协商机制实现 NAT 两端 VPN 主机的互连。

由于在 IPv6 中，其庞大的地址空间为主机之间直接进行端对端的 IPSec 通信提供了便利，NAT 网络地址转换机制存在的必要性已被削弱。然而值得注意的是，即便如此，IPv6 中依然存在着针对 IP 报头进行数据、格式转换的显著需求。为实现纯 IPv4 与纯 IPv6 网络之间的互连通信，IETF IPv6 工作组引入了具备 IPv4/IPv6 协议翻译功能的 NAT-PT 机制[20, 21]，以实现二者主机之间双向的透明访问。而这一协议翻译机制本身便是一个针对 IP 报文进行报头数据及格式转换的过程，和 NAT 一样，目前的 IPSec 与 NAT-PT 机制之间也存在着严重的互操作性困难，因而无法实现诸如纯 IPv4 VPN 与 IPv6 VPN 网络之间的无缝互访等一系列非常有实践价值的安全应用。另一方面，如何可靠、便捷地实现 IPSec 在移动 IPv6 场景下的有效应用，也是其面临的兼容性问题之一。该问题已经受到了广泛的关注，IETF 网络工作组正在致力于实现在 Mobile IPv6 中引入 IPSec 机制以实现移动主机与家乡代理通信过程中的信令保护[7, 22]，S. Sugimoto 等人在文[23]中给出了关于 Mobile IPv6 与 IPSec 之间互操作性的详细论述，在 Francis Dupont 等人撰写的文[24]中对移动 IP 场合下 IKE 协议的友好性也进行了相应的探讨和研究，文[25]还针对如何实现三角路由及路由优化场合之下移动主机与通信对端之间的 IPSec 安全互连的问题给出了一个初步的解决办法。至目前为止，IPSec 与 Mobile IPv6 之间的互操作性问题仍然没有得到圆满解决。

除上述与 IPv6 网络机制之间的不兼容问题之外，与 IPv4 场合相类似的，IPSec 还无法与防火墙、IDS 等常用的安全机制实现配合与协同，IPSec 对报头信息及内容的加密有可能妨碍边界访问控制机制的安全检查，并且逃避入侵监控机制对恶意内容的检测。由上述分析可知，尽管 IPSec 的安全作用在 IPv6 当中得到了空前的重视，但是由于目前其应用的弊端和适用范围的局限性，它并无法解决所有的安全问题，其在 IPv6 网络环境下的实际应用效果仍有待进一步的考察和研究。

3.4 Anycast/Multicast 的安全性

IPv4 链路层通信大多采用 CDMA/CD 的多址复用方式，这一事实使得信道广播成为了 IPv4 协议环境下最重要的一种业务发现及群组通信机制。然而实践证明，过度使用的广播机制也给 IPv4 网络的性能造成了较大的负面影响，同时还为恶意用户提供了一种简单、高效的目标发现及攻击手段，如被用来进行本地网络扫描、实施高强度、大范围的服务拒绝攻击等。随着分组交换技术的迅猛发展，链路广播早已不再是以太网中最基本的通信手段，为适应当前纯交换式的高性能网络环境，并且尽可能地限制和减少广播风暴对网络性能及其安全的影响，在经过仔细地权衡和取舍之后，IETF 在 IPv6 中全面取消了对报文广播方式的支持[2, 9]，同时专门提出了基于 IPv6 的选播(Anycast)[26] 及多播(Multicast)[27] 两种通信方式以替代原 IPv4 中的广播机制。

IPv6 中的组播机制与 IPv4 基本类似，它在 IPv6 网络当中也面临着诸如服务窃取、服务器哄骗及 DoS 攻击等与 IPv4 环境下相似的安全威胁，因而也同样存在着引入相应的组内容加密及组访问控制等安全机制的需要。IPv4 下多播机制的安全性问题早已引起了人们的注意，至目前为止，学术界在 IPv4 安全组播领域已经做了大量的研究工作，并提出了一系

列针对安全多播的组加密传输机制[28]、组密钥管理机制[29,30]和组成员访问控制机制[31,32]。随着组播应用及IPv6技术的逐渐普及,这些研究成果可望在IPv6领域得到更为深入的发掘和研究,并在实用环境中得到更进一步的验证。

选播机制是一种IPv6中新引入的网络机制,它通过将多台服务器组合成为一个选播集群来复制单一服务器的业务响应功能,请求业务的主机能够与网络拓扑距离"最近"的任一选播服务器建立起网络连接以实现同等的服务功能,在提供高效业务发现机制的同时实现有效的冗余和负载均衡,以保证较短的接入延迟以及较高的服务质量。作为一项IPv6环境下建议普遍采用的基本服务方式,选播机制的引入带来了一系列新的安全问题[33]。首先,在Anycast当中选播服务器通过发出业务提供声明的方式来加入或退出选播组,选播组需要对其声明加以身份鉴别管理及其合法性验证,以避免恶意主机提供哄骗服务并导致流量误导或服务拒绝;其次,用户在收到任一选播服务器的业务回复信息之后,在正式与之通信之前,必须验证当前回复的服务器是否经过了认证和授权,并检查回复信息是否新鲜,防止恶意服务器实施哄骗及数据重放攻击;除此之外,还有必要针对组内成员之间、组成员与用户之间的Anycast的传输控制信息以及Anycast群组与路由系统之间的交互信息实施加密保护,以杜绝服务窃取、关键服务器信息泄漏及网络入侵分析等安全事件的发生。选播与多播机制在对组成员管理响应时间、成员合法性和可用性、组成员报告之间的关系以及组策略管理方式等诸多方面均存在着不同的安全要求。

考虑到Anycast的上述问题,并结合多播安全机制的研究当中所取得的经验,人们对IPv6下的选播组安全管理机制进行了初步的探讨。Paul Judge等人在文[34]中提出了一种同时面向多播及选播的组访问控制系统架构Gothic,并且从成员管理、策略管理和密钥管理三个方面详细地论述了其组成员授权、组策略管理及组访问控制敏感的组密钥管理等三个核心子系统的设计与实现;C. Castelluccia等人所著的文[35]中则给出了另外一种名为G-CGA的选播组成员鉴别方案,将选播地址拥有者公钥的散列值作为组成员身份标志是G-CGA的基本思想;除此之外,文[36]中还在多播MLD协议改进的基础之上实现了一种安全组播侦听发现协议SALD,以提供选播组成员管理功能。可以预见到,选播机制作为一种最为基本的IPv6网络机制,其安全性问题将随着IPv6应用的普及而越来越受到人们的重视。

3.5 自动地址配置、邻居发现协议

为减少因地址结构的复杂性所带来的手工配置错误,简化址配置过程并实现节点的零配置,IPv6专门引入了自动地址配置机制[37]。它由本地链路地址配置、网络参数获取两个步骤组成,主机首先根据接口链路EUI-64标志创建一个临时的本地链路地址,再使用其进行路由器发现,获取访问网络所需的前缀、网关、DNS等配置信息并生成正式网络地址。由于在地址配置阶段IPv6主机的网络接口还不具备合法的网络地址,因此,接入主机与所有邻接主机与本地链路路由器之间的交互极大地依赖于链路级组播方式来实现重复地址检测、路由器请求/应答/广播等功能。因此,自动地址配置机制的安全性首先取决于链路级组播的安全性[11],需要引入相应的本地链路主机、路由设备多播组访问控制机制,方可对链路报文哄骗攻击进行有效的抵制,保障自动接入过程不会因为受到恶意主机及路由设备的干扰而瘫痪。除此之外,如何利用身份鉴别和状态维护机制实现选择性的主机自动接入也是其需要考虑的安全问题之一。

邻居发现协议(NDP)[8]在自动地址配置过程中发挥着重要作用,并被用以实现链路地址解析、DOA检测、路由器及网络前缀发现、邻居可达性检测和流量重定向等链路机制。基于IP的协议结构则是其最大的特点。由于NDP在IPv6下取代了绝大多数IPv4下对等的链路层ARP及部分ICMP功能,直接关系到整个网络的可用性,因此其协议安全性非常关键。攻击者可以通过伪造虚假的重复地址检测和节点不可达信息发起DoS攻击,甚至发送虚假的路由器响应及重定向报文来误导网络流量,从而达到其它恶意目的。哄骗报文攻击是其所面临的主要安全威胁这一事实决定了报文身份的可鉴别性是NDP协议的主要安全需求[38]。在NDP协议的标准建议中曾经提议采用IPSec AH方式来达到这一目的,然而这种做法在实际应用当中并不可行,因为其所潜在的手工密钥部署及管理需求与自动地址配置机制所追求的零配置这一根本目标是相违背的。针对上述问题,IETF网络工作组进一步提出了安全邻居发现协议SEND[39],通过在NDP协议报文中捎带主机公钥及其RSA签名的方式来提供报文鉴别及完整性保护功能,利用CGA密钥地址生成技术来确保公钥与IP地址主机标识部分之间的匹配关系以防止公钥-地址哄骗,并引入了专门的授权委托发现机制辅助接入主机在配置未完成的场合下获取证书链信息,完成邻接路由器及主机的身份验证,此外,为了抵制重放攻击,SEND还定义了时间戳、现时值等一系列全新的NDP协议选项。值得指出的是,SEND本身并没有提供NDP协议数据机密性的保护,也没有实现相应的链路层安全机制以保证链路层地址与IP层地址之间可信绑定关系,这有可能导致关键配置信息泄漏及其针对链路层的哄骗攻击;同时,由于SEND中较多地采用了证书验证、数字签名等加解密运算,庞大的计算量使得其协议本身非常容易受到有针对性的DoS攻击的影响。这些安全问题依然有待于进一步研究。

3.6 移动IP支持的安全性

移动性支持(MIPv6)是IPv6所强调的一项新功能,主要用来实现与IP上层协议及应用无关的主机移动性服务。它包含了移动主机(MN)、家乡代理(HA)、对端节点(CN)等一系列通信实体,同时涉及实体与路由、定址、重编号及传输通信等多种网络机制间的互操作,协议架构的复杂性使得移动IPv6的安全性问题尤为突出。

至少达到与IPv4主机一致的安全性是移动IPv6安全技术研究的基本目标。随着人们近几年来对移动场合下安全威胁模型及其安全需求理解的逐步深入,MIPv6安全技术的研究已成为学术界关注的热点。概括而言,目前MIPv6安全性问题的研究主要针对如下4个方面:

1. MN与HA之间的绑定更新(BU)过程[7]。当MN在移动过程中改变当前的外网地址CoA时,它必须以绑定更新信令形式通知HA,以便HA完成后继的流量转发工作。BU过程本身并不提供鉴别功能和完整性保护,因而很容易遭致地址哄骗等安全攻击的威胁,令整个IPv6移动机制失效,同时由于BU信令交互过程均采用明文,该过程也有可能造成MN网络位置和HA地址等隐私及敏感信息泄漏。绑定更新鉴别机制的缺乏是IPv6移动性支持所面临的最严重的安全问题,为此,IETF网络工作组专门在移动IPv6的标准化建议[22]中定义了相应的保护机制,通过在MN、HA间的BU交

互过程中以 IPSec ESP 封装信令载荷的方式来实现其控制信息的可鉴别性、完整性和机密性，同时引入了若干随机现时选项措施来防范信令重放攻击和中继攻击。

2. MN 与 CN 之间的绑定更新过程[25]及路由优化(RO)机制[40]。为了将移动中 MN 的 CoA 地址通知给 CN 节点，MN 与 CN 之间也存在着与 MN、HA 之间类似的绑定更新过程；除此之外，移动 IPv6 还在 MN 与 CN 之间引入了专门的路由优化机制，以提高 MN、CN 之间通过 HA 转发的三角路由效率，实现 MN 与 CN 的直接通信。控制信令的可鉴别性和完整性是实现其二者交互性安全的前提和关键[41]。然而与 MN/HA 之间的 BU 过程不同的是，CN 对端的任意性及其节点密钥部署的难题使得采用 IPSec ESP 对其信令过程进行保护的方式在 MN 与 CN 交互场合下完全无法适用。

针对上述问题，人们提出了两种类型的解决方案，一类是以 CGA[42]技术为代表的基于网络地址结构的安全鉴别机制，CN 以及 MN 的 CoA 地址主机标识部分将由自身公钥哈希导出，并且在交互的信令中捎带各自的公钥和报文签名，从而实现地址及其拥有者身份的绑定，提供无需密钥基础设施支持的分组鉴别和完整性保障功能。类似机制还包括 CAM[43]和 SUCV[44]等，这些鉴别机制的主要缺陷在于，由于使用了高计算强度的校验、签名运算，其性能及可用性很容易受到 DoS 攻击的影响。除上述方法以外，还存在着另外一类基于路由机制的 MN-CN 鉴别方式，IETF 网络工作组所提出的返回可路由性检测机制 RR[7]是其中最为典型的一种，如图 1 所示，在 MN 发起一次 BU 过程之后，CN 将返回给 MN K0 和 K1 两个密钥，其中 K0 使用家乡地址(HoA)由经 HA 转发，而 K1 则直接发送给 MN 的 CoA 地址，所有 MN 发送给 CN 的信息均将以这两个密钥进行摘要签名，从而实现 CN 对 MN HoA 和 CoA 两个地址的可达性验证，并保证其 BU 数据内容的真实性和完整性。此外，为防止针对 RR 机制中 CN 节点的资源耗竭攻击，文[45]还在 RR 协议改进的基础之上进一步提出了一种无状态的可达性验证机制，同时引入了路径均衡的思想来抵制某些报文反射及流量放大攻击的威胁。无法有效防止与 CN 节点处于同一本地链路的恶意主机攻击[46]是 RR 机制目前存在的主要问题，因为此时的恶意主机完全可以同时捕获 CN 节点所发出的两个密钥，进而冒充合法的 MN 对 CN 实施哄骗；另外，无法避免多余的鉴别操作[25]给 CN 节点带来的 DoS 威胁也是基于路由的鉴别机制所具有的缺陷之一。

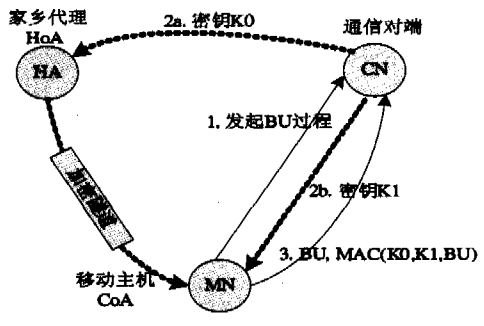

图 1　返回路由可达性检测机制

3. MN 与 HA 之间的前缀发现传播机制(MPP)[7]和动态家乡代理发现机制(DHAAD)[7]。对家乡网络环境进行重新配置将有可能导致 MN 的 HoA 地址失效，在这种情况下 MN 需要立即向 HA 发出家乡网络地址前缀发现请求，以获取新的 HoA 并重新建立绑定关系；为保障该 MPP 过程的安全性，移动 IPv6 的标准化建议中提出了一种基于 IPSec 的解决思路，重复利用 MN、HA 之间在 BU 过程中所建立起的 IPSec ESP 信道来完成 MPP 报文的可信交互。另一方面，与上述 MPP 过程类似的，在家乡代理 HA 失效的情况下，MN 将自动发起一个 DHAAD 过程，向家乡代理选播组发送 HA 发现请求，并根据选播组返回的信息重新设置自身的 HA 服务器。在 DHAAD 过程中，HA 选播组首先需要对其请求进行鉴别操作，确保发起请求的 MN 合法并尽可能削弱虚假请求对家乡代理组的服务拒绝威胁；其次，在 MN 收到了 DHAAD 回复之后，它必须有能力鉴别其来源以防止遭受哄骗；最后，我们还必须保证 DHAAD 回复的机密性和完整性，避免其中关键的 HA 地址列表信息被窃取或篡改。DHAAD 的上述安全需求[47]在目前的移动 IPv6 标准建议中暂时还没有得到充分地考虑。在文[48]中其作者对 DHAAD 的安全保障机制进行了初步的探讨，并给出了 DHAAD via IPSec、DHAAD 请求鉴别和 DHAAD 回复鉴别等三种解决方案，同时还对其各自的优缺点进行了详细的分析和比较。

4. MN 与外网之间的移动检测机制(MD)[7]。实时地检测外界网络环境并进行相应的网络层切换是 MIPv6 引入移动检测机制 MD 的主要目的，在当前采用的 MIPv6 标准化建议中，MN 节点通过优化调度的方式重复发送并监听邻居发现报文来对外网链路路由器进行双向可达性测试，在路由器不可达的情况下，MN 将立即发起新的网络前缀配置请求和地址冲突检测过程，以获取全新的 CoA 并更新与 HA、CN 的绑定关系。就目前所定义的 MD 实现机制而言，其安全需求和可采用的安全增强机制基本与自动地址配置过程类似[49]，上文已有详述，此处不再赘述。

3.7　IPv4/IPv6 并存过渡机制的安全性

出于建设成本、设备改造及服务应用迁徙数量等多方面制约因素，使得我们无法实现 IPv4 网络面向 IPv6 升级和改造的一步性到位。因此，必然存在着一个长期性的 IPv4/IPv6 并存过渡时期。而这一过渡时期的存在，不仅要求我们引入相应的 IPv4-IPv6 兼容互操作技术与之相适应，最大限度地利用和保护 IPv4 下已有的网络服务资源；另一方面，其混合异构的网络环境也势必引发一系列新的安全问题，这些安全问题一部分直接来源于过渡机制方法本身，而另一部分则间接来源于与外界网络环境的交互。

IPv4-IPv6 兼容的并存过渡机制主要分为双协议栈[50]、协议隧道[51]和协议转换[20,21]三种类型。在双协议栈方式中，每一网络节点均配置了 IPv4/IPv6 两套协议栈，两者独立处理各自对应的协议过程以实现 IPv4/IPv6 混合组网。双协议栈的部署为网络新增节点提供了一种 IPv4/IPv6 兼容互访的便捷机制，但是它有可能导致网络安全策略管理及其策略定义机制的混淆。IPv4/IPv6 混合网络中的 HTTP、DNS 等网络服务将以不同的协议方式同时存在，这种并存的局面有可能使得双栈主机用户错误地相信并访问本不可信的服务，从而导致一定的安全威胁。双协议栈应用方式下的网络环境对网络安全策略定义、实施的粒度，及其维护和管理均提出了更高的要求，这需要我们引入相应的混合网络安全策略管理机制来与之相适应。

协议隧道是另外一种常用的 6-4 并存过渡机制，它将 IPv6 报文作为载荷承载于 IPv4 协议之上实现 IPv6 孤岛之间的互连，其典型技术包括 GRE/手动隧道、6-4 兼容自动隧道、

6over4、6to4、ISATAP、Teredo 等；隧道封装的方式将令边界防火墙和 IDS 等简单报文检测机制失效，攻击者可能以伪造隧道报文形式逃避入站源地址过滤并将其注入内网；此外，6to4[52]和 Teredo[53]等自动隧道机制在提供了配置便利的同时也带来了较大的安全风险[54,55]：自动隧道的终端节点必须允许对任意主机发送来的任一隧道报文进行解包操作，因而十分容易受到流量注入攻击的影响；为实现 IPv6 孤岛的互连，这些自动隧道机制还引入了主机、路由器等多种中继措施来配合其实施，而对这些中继服务提供者进行身份鉴别和授权往往是很困难的；另一方面，某些常用的 IPv4-IPv6 协议隧道机制本身打破了原有网络的安全假设，如 Teredo，它通过 UDP 方式在 IPv4 边界防火墙上“打孔”来提供穿越 NAT 的隧道功能，这一机制显然违反了 IPv4 NAT 地址转换方向性所隐含的安全假设，因而存在着严重的安全隐患。最后，与双栈方式一样，协议隧道方式同样面临着内外两层异构网络的安全策略管理的一致性问题。

NAT-PT 协议翻译方式是目前最具实践价值的 IPv4-IPv6 并存过渡机制，它们通过报文翻译、状态跟踪的方式实现 IPv4/IPv6 协议过程的相互转换，从而能够提供前两种兼容机制所不具备的纯 IPv6 与纯 IPv4 网络之间的透明交互能力。NAT-PT 网络地址及报头格式转换的分组处理方式决定了其无法使用 IPSec 的端对端安全特性来提高自身的安全性；由于在 NAT-PT 中，网络主机需要借助兼容网络地址前缀获取[20]和 DNS-ALG[56]等异构网络寻址机制来实现对信宿端节点的定址，而这些寻址机制本身并不具备防攻改及身份鉴别的功能，因此其工作过程对于伪造、修改报文攻击非常敏感；源地址哄骗攻击也是协议转换方式所面临的主要安全威胁之一，NAT-PT 不仅有可能被攻击者利用来发起针对主机的流量反射攻击和广播/多播攻击，作为异构网络互连的边界，其自身也非常容易成为性能的瓶颈，遭受直接的恶意哄骗攻击而导致转换地址资源及计算资源耗竭[57]。除此之外，如何保障协议转换前后内外网络安全策略一致性的问题在协议转换方式下也同样存在。

针对上述 NAT-PT 所存在的安全性问题，文[58]的作者建议统一采用 DNS-ALG 的方式来简化其安全保障机制，文[59]里给出了一种通过鉴别 DNS-ALG 返回的 DNS 信息来保护其完整性的简单方案，而文[60]则进一步提出采用 IPSec 来保护主机与 DNS-ALG 之间的交互过程；为了尽可能抵制和削弱地址哄骗所导致的地址转换资源耗竭及服务拒绝的影响，文[20]在传统 NAT-PT 协议改进的基础之上提出了一种基于地址、端口转换的协议转换机制 NAPT-PT；另外，文[61]的作者还给出了一个在主机与 NAT-PT 设备之间使用 IPSec 的解决方案，以实现对源站主机的鉴别及其相应的访问控制服务。

3.8 基于主机的分布式安全模型及策略

目前 IPv4 网络下通常采用基于网络的安全模型[11]，通过在网络边界上使用集中的单一安全设备从而达到网络防护的目的。然而，在 IPv6 网络环境之下这种方式已不再适用。这主要体现在：

1. IPv4 网络中通常存在着明显的网络边界，IPv4 地址数量短缺、内一外网络间需要进行地址转换是造成这一现象的主要原因之一。而在 IPv6 中，其庞大的地址空间和端对端特性使得全球 IPv6 互联网成为了一个逻辑上的整体，地址转换已不再需要；同时，在上述地址数量优势的基础上衍生出了移动 IP、P2P、网格计算等一系列全局性的新兴应用。强大的端对端特性和应用的新发展使得 IPv6 下网络边界的概念已变得日益模糊。

2. 边界控制的网络安全模型无法防止来自 IPv6 网络内部的安全威胁。如本文前几节所述，基于网络的安全模型无法解决 IPv6 中主机相关处理机制如路由选择/家乡地址选项等所涉及的安全问题，也无法针对多播/选播、自动配置和邻居发现等网内机制所面临的安全问题实施有效的防范。尽管我们依然可以沿用 IPv4 下的入侵检测等纵深防御措施与边界控制机制相结合的方式来提高 IPv6 网络的安全性，但这种方式并没有充分发挥 IPv6 所内建的安全能力，同时在与 IPv6 的互操作方面也存在着一定的局限性。

3. 基于网络的安全模型已无法适应 IPv6 环境下一系列新兴应用的发展。集中访问控制机制和网络边界的存在，不仅容易导致安全计算及网络性能瓶颈，而且人为地打破了 IPv6 天然的端对端安全特性，不利于 IPv6 下虚拟组织的建立，在无法适应用户及设备“游牧化”的同时也阻碍了基于 IPv6 的 Grid、P2P 等新兴计算模式的进一步应用与发展。

针对上述现状，为进一步适应 IPv6 的网络安全环境，IETF v6ops 工作组专门提出了一个基于主机的分布式安全模型[11,12]，其结构如图 2 所示。整个模型由策略描述语言、策略交换协议、策略实体三部分组成，其中的策略鉴别实体又分为两种类型，其分别是策略服务器和策略实施点；其基本思想为：以基于主机的策略描述语言集中定义安全策略，并通过策略交换协议将其分发至各主机，由各个主机来实施这些策略，在实施策略之前，各策略实体的身份必须得到相互鉴别和验证。基于主机的安全模型提供了一种独立于网络拓扑结构的策略实施方式，从而为 IPv6 端对端的网络应用模式提供了良好的适应性。通过针对不同类别的策略实体动态地指定不同的策略，由主机自身来作出相应的安全决策，在精化安全策略指定粒度的同时提高了攻击判定的准确性，使得来自网络内部的安全威胁也能得到防范。此外，这种集中定义、本地决策的策略实施方式也有利于高效的安全管理和信息收集、审计。

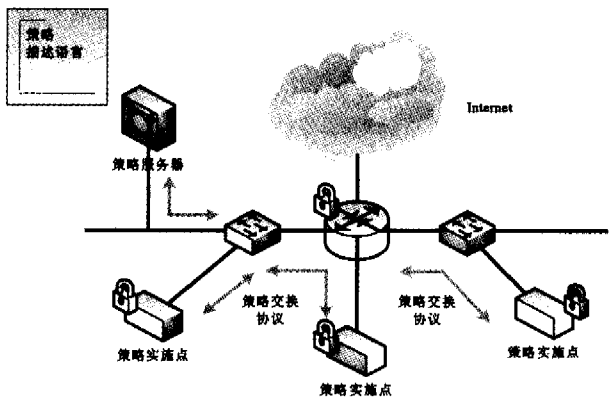

图 2 基于主机的分布式安全模型

然而很显然，这种动态的、分布式的安全模型较基于网络的安全模型而言引入了更多的复杂性。策略服务器成为了整个系统的瓶颈，在没有进行边界控制的情况下，单一策略服务器将直接暴露在攻击者的面前，为了保障其安全性和可用性势必需要引入其他复杂的保障机制，如分布式或者是冗余措施等。同时考虑到网内主机安全策略的受管性，还需要提供相应的节点策略执行监控、判别机制来确保其运行和维护与

安全策略一致，当发现主机不符合指定安全策略或者是被蠕虫和木马等病毒操纵、感染时，该主机应当立即从可信节点集合中排除，而实现主机正常行为和异常行为的区分这一机制本身便是十分困难的。另外，如何实现移动主机在外部网络中的策略管理和仲裁，以及 PDA 等不经常在线设备的动态策略更新和实施监控，也是基于主机的分布式安全模型当中有待解决的问题之一。

结束语 目前，国内外针对 IPv6 安全性的研究整体上还处于安全需求定义、详细分析和初步实现阶段。IPv6 提供了一系列的全新机制，其中绝大多数的 RFC 标准化建议工作已经结束，发现、分析并且解决这些新特性对整个网络的安全所可能造成的负面影响，是目前关于 IPv6 安全性研究工作的一个重要来源。而尝试以现有安全机制实现对这些新特性的支持、针对现有特性自身安全机制进行相应的完善和扩充，或者是引入全新的特性以便更好地体现 IPv6 下的安全需求，则是目前提供 IPv6 安全性的三种主要途径。

通过上文的分析我们可以看出，尽管安全性保障是 IPv6 最为重要的设计出发点之一，出于兼容性的考虑，IPv6 并没有完全颠覆 IPv4 时代所采用的基本安全机制，而是采用逐步引入增强措施的方式来实现安全性的提高，这些安全增强机制的合理应用将会对 IPv6 下的网络安全状况产生积极影响。同时我们也可以预见到，在实现从 IPv4 向 IPv6 迁徙的过程中势必存在着一个两者长期并存的过渡时期，这一事实说明，针对 IPv4/IPv6 兼容过渡机制安全问题的研究也许将会成为当前 IPv6 安全性研究领域当中新的热点和关键。

随着 IPv6 技术的不断成熟和应用的逐渐推广，它对下一代互联网络安全方面的作用和影响必将逐步得以展现，出于目前人们对网络安全的重视及对新一代互连网络协议安全特性研究的审慎态度，从长远的观点来看，我们完全有理由相信 IPv6 将会给我们带来一个较之 IPv4 更为可靠、更为高效的网络安全解决方案。

参 考 文 献

1 Postel J. Internet Protocol. IETF RFC 791, Sep. 1981
2 Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. IETF RFC 2460, Dec. 1998
3 Kjeld B, Francis P. The IP Network Address Translator (NAT). IETF RFC 1631, May 1994
4 Kent S, Atkinson R. Security Architecture for the Internet Protocol. IETF RFC 2401, Nov. 1998
5 Kent S, Atkinson R. IP Authentication Header. IETF RFC 2402, Nov. 1998
6 Kent S, Atkinson R. IP Encapsulating Security Payload. IETF RFC 2406, Nov. 1998
7 Johnson D, Perkins C. Mobility Support in IPv6. IETF RFC 3775, Jun. 2004
8 Narten T, Nordmark E. Neighbor Discovery for IP Version 6 (IPv6). IETF RFC 2461, Dec. 1998
9 Hinden R, Deering S. IP Version 6 Addressing Architecture. IETF RFC 2373, Jul. 1998
10 Hinden R, O'dell M. An IPv6 Aggregatable Global Unicast Address Format. IETF RFC 2374, Jul. 1998
11 Vives A, Palet J. IPv6 Security Problem Statement. Internet-Draft draft-vives-v6ops-ipv6-security-ps-03, Feb. 2005
12 Palet J, Vives A. IPv6 Distributed Security Requirements. Internet-Draft draft-palet-v6ops-ipv6security-02, Feb. 2005
13 Savola P. Security of IPv6 Routing Header and Home Address Options. Internet-Draft draft-savola-ipv6-rh-ha-security-03, Dec. 2002
14 Bellovin S, Leech M. ICMP Traceback Messages. Internet-Draft draft-ietf-itrace-04, Feb. 2003
15 Harkins D, Carrel D. The Internet Key Exchange (IKE). IETF RFC 2409, Nov. 1998
16 Dierks T, Allen C. The TLS Protocol Version 1.0. IETF RFC 2246, Jan. 1999
17 Arends R, Austein R. DNS Security Introduction and Requirements. IETF RFC 4033, Jul. 2001
18 Aboba B, Dixon W. IPsec-Network Address Translation (NAT) Compatibility Requirements. IETF RFC 3715, Mar. 2004
19 Kivinen T, Swander B. Negotiation of NAT-Traversal in the IKE. IETF RFC 3947, Jan. 2005
20 Tsirtsis G, Srisuresh P. Network Address Translation - Protocol Translation (NAT-PT). IETF RFC 2766, Feb. 2000
21 Nordmark E. Stateless IP/ICMP Translation Algorithm (SIIT). IETF RFC 2765, Feb. 2000
22 Arkko J, Devarapalli J. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. IETF RFC 3776, Jun. 2004
23 Sugimoto S, Dupont F. PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE. Internet-Draft draft-sugimoto-mip6-pfkey-migrate-00, Feb. 2005
24 Dupont F, Haddad W. How to make IPsec more mobile IPv6 friendly. Internet-Draft draft-dupont-ipsec-mipv6-05, Feb. 2004
25 Dupont F, Combes J M. Using IPsec between Mobile and Correspondent IPv6 Nodes. Internet-Draft draft-dupont-mipv6-cn-ipsec-01, Jun. 2004
26 Johnson D, Deering S. Reserved IPv6 Subnet Anycast Addresses. IETF RFC 2526, Mar. 1999
27 Vida R, Costa L. Multicast Listener Discovery Version 2 (MLDv2) for IPv6. IETF RFC 3810, Jun. 2004
28 Mittra S. IOLUS: a framework for scaleable secure multicast. ACM Computer Communication, 1997, 27(3): 277～288
29 Hardjono T. Key establishment for IGMP authentication in IP multicast. In: Proc. of IEEE European Conf. on Universal Multiservice Networks (ECUMN), 2000
30 Harney H, Muckenhirn C. Group key management protocol (GKMP) architecture. IETF RFC 2094, Jun. 2002
31 刘璟. 大型动态多播群组的密钥管理和访问控制. 软件学报, 2002, 13(2): 291～297
32 Cainandal B. Internet Group Management Protocol. IETF RFC 3376, Oct. 2002
33 Dondeti L, Hardjono T. Security Requirements of IPv6 Anycast. Internet-Draft draft-dondeti-ipv6-anycast-security-00, Jun. 2001
34 Judge P. Gothic: A Group Access Control Architecture for Secure Multicast and Anycast. In: Proc. of IEEE INFOCOM, 2002
35 Aura T. Cryptographically Generated Addresses (CGA). Internet-Draft draft-ietf-send-cga-06, Apr. 2004
36 Wang Yue. Research on IP Anycast Secure Group Management. In: Proc. of Network Research Workshop, Advanced Network Conf. of 16th APAN Meetings, Korea, 2003
37 Thomson S, Narten T. IPv6 Stateless Address Autoconfiguration. IETF RFC 2462, Dec. 1998
38 Nikander P, Kempf J. IPv6 Neighbor Discovery (ND) Trust Models and Threats. IETF RFC 3756, May. 2004
39 Arkko J, Kempf J. SEcure Neighbor Discovery (SEND). IETF RFC 3971, Mar. 2005
40 Nikander P, Arkko J. Mobile IP version 6 Route Optimization Security Design Background. Internet-Draft draft-ietf-mip6-ro-sec-03, Jun. 2005
41 Arkko J. Issues in Protecting MIPv6 Binding Updates. Internet-Draft draft-arkko-mipv6-bu-security-01, Nov. 2001
42 Aura T. Cryptographically Generated Addresses (CGA). IETF RFC 3972, Mar. 2005
43 O'shea G. Child-proof Authentication for MIPv6 (CAM). ACM Computer Communications Review, Apr. 2001
44 Montenegro G. Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses. In: Proc. of Network and Distributed System Security Symposium, San Diego, Califoria, 2002

(下转第 21 页)

由图2和图3易知，系统1：$\sum_1=(N_1,M_{10})$和系统2：$\sum_2=(N_2,M_{20})$都是有界的、活的。又因为$\sum_1$和$\sum_2$的共享Ⅱ型子网合成满足定理3.2的条件，所以由定理3.2得，合成网系统$\sum=(N,M_0)$是有界的、活的。

结束语 本文讨论了Petri网的共享子网合成性质继承关系及其在系统设计中的应用，其主要贡献在于：针对柔性制造系统的设计和分析问题，提出了经由Petri网共享子网构成共享子网合成网的解决方案；提出了共享子网合成网保持有界性、活性的充分条件，按这些条件对有界的、活的Petri网两两进行共享子网合成，可得到有界的、活的共享子网合成网。实施Petri网的共享子网合成，可以实现合成网系统的资源共享和同步操作，解决系统的调度优化问题。文中通过对两个柔性制造系统的共享子网合成分析，进一步展示了该方法的实际价值。下一步要研究的工作是给出更为广泛的条件，来研究Petri网共享子网合成的其它性质（如公平性等）的保持问题。

参 考 文 献

1 Bednarczyk M A, Bernardinello L, et al. Modular system development with pullbacks [J]. In: Proc. the 24th International Conference on Application and Theory of Petri Nets. Eindhoven, The Netherlands, 2003. 140～160

2 Morin R. Decompositions of asynchronous systems [J]. In: Proc. CONCUR'98, LNCS 1466, 1998. 549～564

3 Badouel E, Darondeau P H. The synthesis of Petri nets from path-automatic specifications. Information and Computation, 2004, 193: 117～135

4 Juhás G, Lorenz R, et al. Synthesis of Controlled with Modules of Signal Nets. In: Proc. the 25th International Conference on Application and Theory of Petri Nets. Bologna, Italy, 2004. 238～257

5 Chao D Y. Petri net synthesis and synchronization using knitting technique. Journal of Information Science and Engineering, 1999, 15: 543～568

6 Mäkelä M. Model checking safety properties in modular high-level nets [J]. In: Proc. the 24th International Conference on Application and Theory of Petri Nets. Eindhoven, The Netherlands, 2003. 201～219

7 van Hee K, Sidorova N, et al. Soundness and separability of workflow nets in the stepwise refinement [J]. In: Proc. the 24th International Conference on Application and Theory of Petri Nets. Eindhoven, The Netherlands, 2003. 337～356

8 Bernardinello L, Ferigato C, et al. Towards modular synthesis of EN systems [J]. In: Caillaud B, et al. eds. Synthesis and Control of Discrete Event Systems, Kluwer Academic Publishers, 2002. 102～113

9 Souissi Y. On liveness preservation by composition of nets via a set of places [J]. I: Rozenberg G. ed. LNCS 483, New York: Springer-Verlag, 1990. 457～470

10 Murata T. Petri nets: properties, analysis, and applications. Proc. IEEE, 1989, 77(4): 541～580

11 Peterson J L. Petri net theorey and the modeling of systems. Englewood Cliffs. New York: Prentice-Hall, Inc, 1981

12 Resig W. Petri nets. EATCE Monographs on Theoretical Computer Science. Vol. 4, New York: Spring-Verlag, 1985

（上接第11页）

45 Aura T. Mobile IPv6 Security. In: Proc. of Security Protocols, 10th International Workshop, Cambridge, UK, 2002

46 Kempf J. Mobile IPv6 Security. Wireless Personal Communication, 2004, 29: 389～414

47 Mankin A, Patil B. Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6. Internet-Draft draft-ietf-mobileip-mipv6-scrty-reqts-02, Nov. 2001

48 Sun Q, Mu L. Security Issues in Dynamic Home Agent Address Discovery. Internet-Draft draft-sun-mipv6-dhaadsecurity-00, Nov. 2004

49 Nikander P, Harkins D. Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6. Internet-Draft draft-team-mobileip-mipv6-sec-reqts-00, Jul. 2001

50 Bound J. Dual Stack IPv6 Dominant Transition Mechanism (DSTM). Internet-Draft draft-bound-dstm-exp-02, Feb. 2005

51 Savola P. A View on IPv6 Transition Architecture. Internet-Draft draft-savola-v6ops-transarch-03, Jan. 2004

52 Carpenter B, Moore K. Connection of IPv6 Domains via IPv4 Clouds. IETF RFC 3056, Feb. 2001

53 Huitema C. Teredo: Tunneling IPv6 over UDP through NATs. Internet-Draft draft-huitema-v6ops-teredo-05, Apr. 2005

54 Davies E, Krishnan S. IPv6 Transition/Co-existence Security Considerations. Internet-Draft draft-savola-v6ops-security-overview-03, Oct. 2004

55 Savola P, Patel C. Security Considerations for 6to4. IETF RFC 3964, Dec. 2004

56 Srisuresh P, Tsirtsis G. DNS extensions to Network Address Translators (DNS_ALG). IETF RFC 2694, Sep. 1999

57 Okazaki S, Desai A. NAT-PT Security Considerations. Internet-Draft draft-okazaki-v6ops-natpt-security-00, Jun. 2003

58 Park S D. Scalable mNAT-PT Solution. Internet-Draft draft-park-scalable-multi-natpt-0, May 2003

59 Eastlake D. Domain Name Security Extensions. IETF RFC 2535, Mar. 1999

60 Durand A. Issues with NAT-PT DNS ALG in RFC2766. Internet-Draft draft-durand-v6ops-natpt-dns-alg-issues-00, Jan. 2003

61 Van Der Pol R. Issues when translating between IPv4 and IPv6. Internet-Draft draft-vanderpol-v6ops-translation-issues-00, Jan. 2003