IPv6链路本地地址安全技术研究

孙文歌，魏振方，江俊斌
（中国卫星海上测控部远望六号测量船，江苏 江阴 214431）

摘 要：IPv6协议虽然在某些方面增强了安全性，但同时也引入了新的安全风险，因此网络安全威胁在IPv6时代依旧存在。通过从IPv6地址、报文格式和相关协议等方面分析了IPv6可能带来的安全新问题，分析IPv6报文结构和IPv6链路本地地址的结构。结合物联网的应用范围和特点，研究了ND协议的应用原理和ND协议的无状态地址技术在物联网中的应用过程。根据物联网中存在安全隐患的特点，从链路本地地址结构出发，提出了基于“贝特反转”的IPv6链路本地地址安全技术。

关键词：IPv6；链路本地地址；邻居发现协议；物联网
中图分类号 TP393.08 **文献标识码**：A **文章编号**：1673-629X(2011)10-0237-04

Study of Link-Local Address Security in IPv6

SUN Wen-ge, WEI Zhen-fang, JIANG Jun-bin
(China Satellite Maritime Tracking and Controlling Department, Jiangyin 214431, China)

Abstract: Although in some aspects of IPv6, enhanced security, but it also introduces new security risks, so the network security threats still exist in the IPv6 era. From the IPv6 address, message formats and related protocols and other aspects of the IPv6 security may bring new problems, aimed at overcoming the analysis of IPv6 date packet and link-local address, based on the domain and way of the Internet of things, analyze and research on the Internet of things features of neighbor discovery protocol and the unspecified address automatic identification. As result view, "the bit inverse proportion" was presented based on the security requirement of the Internet of things and IPv6 date packet.

Key words: IPv6; link-local address; neighbor discovery protocol; Internet of things

0 引 言

Internet规模的快速扩大，特别是近十年来，Internet爆炸式增长使其走进了千家万户，人们的日常生活已经离不开它。同时Internet上的节点不再单纯是计算机，还将包括PDA、移动电话、各种各样的终端甚至包括冰箱、电视等家用电器，这些设备都需要分配IP地址。截止现在IPv4则只剩下不到6%的IP地址没有被分配，IPv6作为新的力量走上了前台，从20世纪90年代起，从理论界到用户，从设备厂商到IP服务提供商，都逐渐清晰地听到IPv6作为新的力量走上历史舞台的脚步声。

IPv6以其巨大的地址空间，世界上每个人可以拥有约5.7×10^{28}个IPv6地址来满足未来物流网与因特网的需要，其中IPv6链路本地地址作为IPv6单播地址的一种，在IPv6邻居节点之间的通信协议中广泛使用，尤其在ND协议与动态路由协议中作用十分重要，因此，IPv6链路本地地址在网络安全中地位也十分特殊。

1 IPv6链路本地地址结构分析

IPv6(Internet Protocol version 6，互联网版本协议6)，是IETF(Internet Engineering Task Force，互联网工程任务组)设计的一套规范，是IPv4的升级版本，其IP地址长度为128位，IPv6链路本地地址作为IPv6地址的一种单播地址，其长度同样也是128位。IPv4地址有单播、组播、广播几种类型，与IPv4地址分类方法相似的是，IPv6地址也有不同的类型，包括单播(Unicast)、组播(Multicast)、任播(Anycast)地址，IPv6的单播地址根据其作用范围的不同可以分为特殊地址(::/128，::1/128)、全球单播(2000::/3)、全球唯一本地(FC00::/7)、兼容地址(0:0:0:0:0:0::/96，0:0:0:0:0:FFFF::/96)，此外，属于单播地址的还有IPv4内嵌地址、NSAP等，链路本地地址就是IPv6单播地址的一种[1]。

收稿日期：2011-02-26；**修回日期**：2011-05-06
基金项目：海军装备科研项目(HJ-505-2009-23)
作者简介：孙文歌(1982-)，男，硕士研究生，从事航天远洋测控通信网络技术研究；江俊斌，工程师，从事航天远洋测控卫星技术通信研究。

IPv6 的单播地址只能分配给一个节点上的接口，即寻址到该单播地址的数据报文最终会被发送到一个唯一的接口。一个主机接口上的 128 位 IPv6 单播地址一般可以看做成一个整体来代表这台主机。而当要表示这个主机上的接口所连接的网络时，将这个 128 位 IPv6 单播地址分成两部分来表示，如图 1 所示。

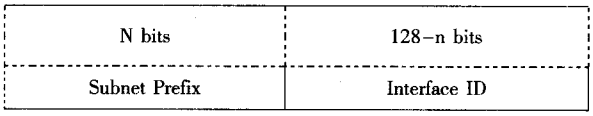

图 1 单播地址结构

其中各字段含义如下。

(1) Subnet Prefix：n 位子网前缀，表示接口所属的网络。

(2) Interface ID：接口标识，用以区分连接在一条链路上的不同接口。

IPv6 链路本地地址是一种特殊的单播地址，这种地址的应用范围受限，只能在连接的同一本地链路的节点之间使用，它有固定的格式，图 2 显示了链路本地地址的结构。

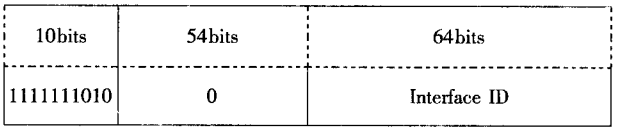

图 2 链路本地地址结构

从图 2 中可以看出，链路本地地址由一个特定的前缀和接口 ID 两部分组成。它使用了特定的链路本地前缀 FE80::/64(最高 10 位值为“1111111010”)，同时将接口 ID 添加在后面作为地址的低 64 位。这就是在 IPv6 链路本地地址的基本结构。

下面重点分析一下在 IPv6 链路本地地址邻居发现协议和动态路由协议数据报文中的实际应用。

2 IPv6 链路本地地址在邻居发现协议中的应用分析

链路本地地址在 IPv6 邻居节点之间的通信协议——邻居发现协议(Neighbor Discovery Protocol，简称“ND”协议)中广泛使用，特别是对连接在同一链路上的 IPv6 节点间，链路本地地址架起了它们之间通信的桥梁，因为节点的每个接口都配置有链路本地地址，ND 协议正是通过携带有链路本地地址的 IPv6 报文[2]，才实现了数据包的准确传输。链路本地地址具体是如何在 ND 协议中发挥其作用的呢？下面从 IPv6 报文的结构以及 ND 协议的原理入手详细分析其应用过程。

2.1 IPv6 报文的结构

ND 协议是 IPv6 的一个关键协议，它实现了 IPv4 中的一些协议功能，如 ARP、ICMP 路由器发现和 ICMP 重定向等，并对这些功能进行了改进，同时，作为 IPv6 的一个基础性协议，ND 协议还提供了其他许多非常重要的功能，如前缀发现、重复地址检测、无状态地址自动配置等，这些功能的实现离不开 ND 协议报文的交互，ND 协议定义了 5 种 ICMPv6 报文类型，包括 RS (Router Solicitation)、RA (Router Advertisement)、NS (Neighbor Solicitation)、NA (Neighbor Advertisement) 和 Redirect 报文，具体如表 1 所示。

表 1 ICMPv6 报文

ICMPv6 类型	Type=133	Type=134	Type=135	Type=136	Type=137
ICMPv6 报文名称	RS	RA	NS	NA	Redirect

其中 RS 是路由器请求报文，RA 是路由公告报文，NS 是邻居请求报文，NA 是邻居公告报文，Redirect 是重定向报文。NS/NA 报文主要用于地址解析，RS/RA 报文主要用于无状态地址自动配置，Redirect 报文用于路由重定向[3]。

在 IPv4 的地址解析中，ARP 报文直接封装在以太帧中，其以太网协议类型为 0x0806，代表 ARP 报文。ARP 被看做是工作在 2.5 层的协议。而 ND 协议本身基于 ICMPv6 实现，因此 ND 协议本是在三层上实现的。ND 协议本报文的以太网协议类型为 0x0806DD，即 IPv6 报文。IPv6 的下一个报头协议类型为 58，表示是 ICMPv6 报文，上述两者的对比如图 3 所示。

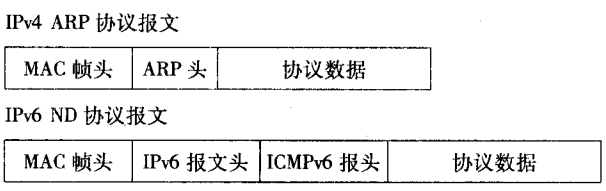

图 3 ARP 与 ND 协议报文封装

2.2 ND 协议的原理

ND 协议报文是三层协议报文，按照 tcp/ip 分层结构应用在网络层，链路本地地址主要应用在 ND 协议的无状态地址自动配置中，在未来的物联网英文名称为“The Internet of things”中 ND 协议的无状态地址自动配置将成为主流，因为物联网是通过射频识别(RFID)、红外感应器、全球定位系统信息传感设备，按约定的协议，把任何物体与互联网相连接，进行信息交换和通信，以实现对物体的智能化识别、定位、跟踪、监控和管理的一种网络，它本质上是互联网特征，即对需要联网的物一定要能够实现互联互通的互联网络；是识别与通信特征，即纳入物联网的“物”一定要具备自动识别与物物通信的功能；是智能化特征，即网络系统应具有自动化、自我反馈与智能控制的特点。因此其传输节点以“物”作为主体，要实现信息设备、家电和通信设备的智能互联，这些以“物”作为传输的节点需

要用 ND 协议的无状态地址自动配置来分配 IP 地址和链路本地地址,无状态地址自动配置涉及三种机制:路由器发现、DAD 检测(Duplicate Address Detection,重复地址检测)和前缀重新编址[4]。

路由器发现可以使节点获得链路上可用的路由前缀信息及路由信息,路由器发现是指主机怎样定位本地链路上的路由器和确定其配置信息的过程,主要包括以下 3 个方面的内容。

(1)路由器发现(Router Discovery):主机发现邻居路由器以及选择哪一个路由器作为默认网关的过程。

(2)前缀发现(Prefix Discovery):主机发现本地链路上的一组 IPv6 前缀列表。该列表用于主机地址自动配置和 on-link 判断。

(3)参数发现(Parameter Discovery):主机发现相关操作的过程,如链路最大传输单元(MTU)、报文的默认跳限制(Hop Limit)、地址配置方式等信息。

在路由器通告报文 RA 中承载着路由器的相关信息,ND 协议通过 RS 和 RA 的报文交互完成路由器发现、前缀发现和参数发现三大功能。

2.3　无状态地址自动配置过程

ND 协议的无状态地址自动配置包括两个阶段:链路本地地址的配置和全球单播的配置,在物联网中,智能家电海尔、海信在内的国内品牌推出的从智能冰箱到智能空调,再到智能洗衣机,可以通过 U-home 物联网家庭方案:其中,物联网冰箱不仅可以储存食物,而且可以通过与网络连接,实现了冰箱与冰箱里的食品、与超市的食品、与人类之间自由沟通;而物联网洗衣机具有自动识别洗涤剂品类、衣物质料、自来水水质及脏污程度、家庭水电费的管理、网上购物等功能,都需要链路本地地址的配置和单播地址的配置进行互联访问,当这些物联节点介入 Internet 时[5],节点首先会根据前缀 FE80::/64 和 EUI-64 接口标识符,为该接口生成一个链路本地地址,如果在后续 DAD 检测中如果发生地址冲突,则必须对该接口重新配置链路本地地址,否则该接口将不可用,并且一个链路本地地址的优先时间是无限和永不超时的。

具体配置步骤如图 4 所示。

(1)节点 Node A 在配置好链路本地地址后,发送 RS 报文,请求路由器前缀的信息。默认情况下,最多发送 3 个 RS 报文.

(2)路由器收到 RS 报文后,发送单播 RA 报文,携带着用于无状态地址自动配置的前缀信息,同时路由器也会周期性地发送组播 RA 报文。

(3)Node A 收到 RS 报文后,根据前缀信息和配置信息生成一个临时的全球单播地址。同时 Node A 启动 DAD 检测,发送 NS 报文验证临时地址的唯一性,此时该地址处于临时状态。

(4)链路上的其他节点收到 DAD 检测的 NS 报文后,如果没有用户使用该地址根据,则丢失报文;否则,产生应答 NS 的 NA 报文。

(5)Node A 如果没有收到 DAD 检测的 NA 报文,说明地址是全局唯一的,则用该临时地址初始化接口,此时地址进入有效状态。

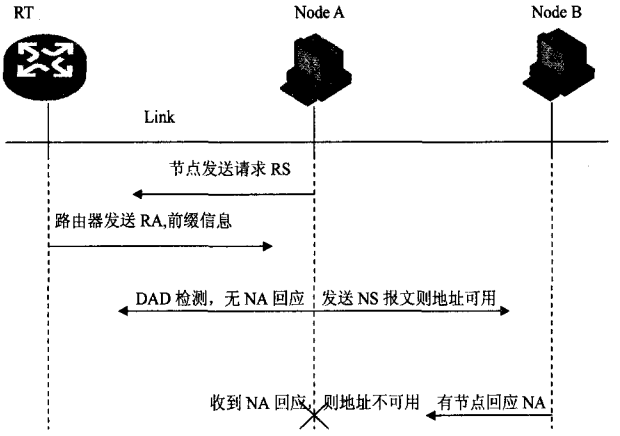

图 4　无状态地址配置过程

无状态地址自动配置实现了对物联网节点的智能化识别、定位、跟踪、监控、管理和互联访问[6],其中链路本地地址发挥了关键作用,没有链路本地地址也就无法传输 IPv6 协议报文,无法实现智能化联通,可以说链路本地地址是物联网节点的智能互联的基础,正是这些关键性的作用,链路本地地址将成为物联网安全防范的重点[7,8]。

3　基于“贝特反转”的 IPv6 链路本地地址安全技术

随着科技的飞速发展,人们已经越来越接近这个“智能时代”;然而,人们却发现在实现这一切之前依然有很多问题是无法回避的,首先就是“安全”——人们已经生活在一个由网络主宰的世界[9],几乎没有什么“隐私”可言,一旦未来自己的个人物品也“物联”了,那更是会被周围的物质所“左右”! 而随着技术的进步,物品植入的芯片越来越复杂,对周围的感知能力越来越强大。完全可以利用“物联网”对你和你的家庭发动最可怕、最恐怖的攻击——你家中的每一件物品都可能因为他的指令变成致命的武器,那些过去只能在科幻片中看到的犯罪情节可能在现实中被还原! 而这已不再只是梦想,在物联网时代“一切皆有可能”。于是,回到出发点,“安全”将是物联网时代最稀松平常也是最惊心动魄的关键词[10,11];在安全没有得到保障的情况下,首选应该是“勿联网”而非“物联网”。

IPv6 链路本地地址是否安全,是“物联网”是否安

全的基本出发点，当一个物联网节点启动时，节点的接口会配置链路本地地址，上文提到一个链路本地地址的优先时间是无限和永不超时的，若第三方获得了物联网节点的链路本地地址，就容易对该节点非法互联，从而导致非法控制。因此安全的重点是防止非法获得真实的物联网节点的链路本地地址，链路本地地址有固定的格式，图 2 显示了链路本地地址的结构。

从图 2 中可以看出链路本地地址有固定的前缀 FE80::/64，低 64 bits 是 IEEE 定义的一种扩展标识符，是接口 ID，链路本地地址的接口 ID 由 MAC 地址映射而来，MAC 地址是 48 位的，EUI-64 定义在 MAC 地址中间位置插入十六进制数 FFFE（11111111 11111110）。为了确保这个从 MAC 地址得到的接口标识符是唯一的，还要将 U/L 位（从高位开始的第七位）设置为“1”。最后得到的这组数就作为链路本地地址的 Interface ID，通过链路层地址，在以太网中就是 MAC 地址，而生成接口 ID，保证了接口的唯一性，也保证了链路本地地址的唯一性。但是，这种透明方式，缺乏安全性，从安全考虑，可以从 MAC 地址入手把 MAC 地址进行变换，变换 MAC 地址的前提是必须确保接口 ID 的唯一性，也即保证本地链路地址的唯一性，如图 5 所示。

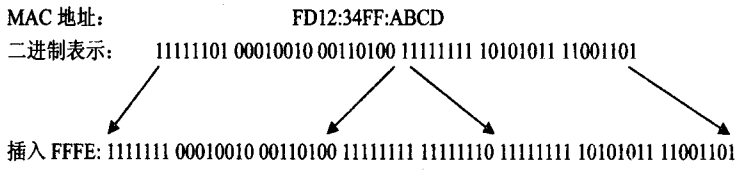

图 5 接口 ID 的生成过程

MAC 地址 FF12:34FF:ABCD 生成的接口 ID 为：FF12:34FF:FEFF:ABCD，为了进一步增强 MAC 地址的安全性，从而增强链路本地地址的安全，增强物联网中无状态地址分配的安全性，可以对 MAC 地址进行“贝特反转”变换，可以把 MAC 地址 FF12:34FF:ABCD 变换为 00000010 11101101 11001011 00000000 01010100 00110010 即 02ED:CB00:9832，生成的新接口 ID 为 02ED:CBFF:FE00:9832，可见通过“贝特反转”变换，在一定程度上增加了 MAC 地址的隐蔽性，增强了链路本地地址的安全性。由于没有对原 MAC 地址的二进制排列次序进行更改，因此没有破坏接口 ID 的唯一性，从而确保了链路本地地址的有效性，避免了物联网节点在无状态地址自动配置过程中进行 DAD 检测时发生地址冲突。

IPv6 链路本地地址的“贝特反转”法，在不改变接口 ID 的唯一性的前提下，对 MAC 地址进行了加工，增强 MAC 地址的隐蔽性。作为物联网安全技术的一种方法，它只能从接口地址层面增强了安全性，还不能完全防范第三方的网络攻击，在未来的物联网中应用中，将存在很多安全威胁，还需为物联网开发出更多的安全技术。

4 结束语

IPv6 作为下一代互联网应用协议，为未来物联网技术的广泛应用提供了充足的地址空间。在众多 IPv6 协议中，ND 协议是一个关键的协议，特别是在物联网节点的地址自动配置中，发挥了十分重用的作用。物联网安全技术是未来互联网安全技术的焦点，文中所提出的链路本地地址安全技术，是针对物联网内部接口访问互联地址的一种安全策略，只能起到抛砖引玉的作用，为了不使“物联网”变成“勿联网”[12]，还需要从多方面、多角度考虑，去防范各种网络攻击，只有这样，才使人们在未来只需要去享受“物联网”带来的便捷，而不需要为个人的安危担忧。

参考文献：

[1] 许精明. 下一代互联网关键技术的分析与研究[J]. 计算机技术与发展，2009，19(11)：115-116.
[2] 刘化君. 网络编程与计算机技术[M]. 北京：机械工业出版社，2009.
[3] 张东亮. IPv6 技术[M]. 北京：清华大学出版社，2010.
[4] 王立超. 推动 IPv4/IPv6 过渡策略分析. 计算机技术与发展，2010，20(8)：115-116.
[5] Hinden R, Deering S. IPv6 Multicast AddressAssignments [S]. RFC 2375, IETF, 1998.
[6] Li Qing, Shima Keiichi. IPv6 详解：高级协议实现[M]. 北京：人民邮电出版社，2009.
[7] Lim JaeDeok, Kim YoungKi. Protection, Algorithm against security holes of IPv6 routing header[C]//IEEE ICA0T2006. [s. l.]:[s. n.], 2006.
[8] Vida R, Costa L. Multicast Listener DiscoveryVersion 2 (MLDv2) for IPv6[S]. RFC 3810, IETF, 2004.
[9] Conta A, Deering S. Research & Development Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) [S]. RFC 4443, IETF, 2006.
[10] Aura T. Cryptographically Generated Addresses (CGA) [S]. RFC 3972, IETF, 2005.
[11] Gont F. ICMP attacks against TCP[R]. Workin Progress, IETF, 2005.
[12] Droms R, Bound J, Volz B, et al. Dynamic HostConfiguration Protocol for IPv6 (DHCPv6)[S]. RFC 3315, IETF, 2003.