
陈 瑜

移动IP嵌入Linux方法及其安全问题解决方案

陈 瑜 刘 礼 王凤至

摘 要 作者在系统分析移动IP机理的基础上，详述了移动IP在Linux上的具体实现方法，提出了移动IP安全问题的解决方法，最后介绍了移动IPV6的一些新特性。

关键词 移动IP 家乡代理 外地代理 移动节点 转交地址 家乡地址

Mobile IP Within the Linux and its Solution to Secure Problem

Chen Yu Liu Li Wang Fengzhi

Abstract The writer describles the mechanisms of mobile IP and its secure problem. It details the impelemention of mobile IP within the Linux kernel. At last, the paper also present some new characters of mobile IPV6.

Kewyords mobile IP, home agent, foreign agent, mobile node, nome address

1 引言

随着经济全球化和信息技术的迅猛发展，移动计算正变得无所不在。通过移动技术，可以实现移动办公和远程管理，从而使人们的工作更加高效和灵活。在它的支持下，管理者可以从世界任何一个角落操纵公司的运作；市场人员可以随时向总 部报告业务的进展情况。移动计算正在改变着人们的工作和生活。

作为移动计算核心技术之一的移动IP技术，由于其巨大的市场潜力和商业价值，正为众多厂商所关注，成为学术及技术领域的研究热点。移动IP技术不仅利用各种路由技术提供随时随地的连通性，在安全性方面，它还使用了多种算法，设计了强大的加密和认证体系来解决因特网上越来越被人们所关注的“黑客”问题，就这些方面来说，移动IP可以说集中了当前因特网的各种先进技术。

然而，先进的技术必须与卓越的平台相结合才能发挥其应有的作用。Linux这个正在崛起的类Unix操作系统，由于它在因特网及安全方面的卓越表现，正在被越来越多的厂商和用户所认可和接受。因此，将移动IP技术嵌入到Linux内核中去，并对移动IP的一些安全问题提出解决办法，乃是一件十分有意义的工作。

2 移动IP的特点及体系结构

移动IP在全球因特网上提供移动功能的方案，具有可扩展性、可靠性和安全性等性能，并且与其它的移动方案相比较，移动IP的最显著特点就是能够使移动节点在切换链路时仍可保持正在进行的通信。移动IP提出了一种崭新的路由机制，利用这种路由机制使移动节点以一个不变的IP地址连接到任何链路上，这样，与移动节点通信的任何用户都不会遭受找不到移动节点或者是频繁更换对方IP地址的痛苦和麻烦了。

陈 瑜 北方交通大学 在读硕士研究生生 100044 北京市
刘 礼 北方交通大学 在读硕士研究生生 100044 北京市
王凤至 北方交通大学 副教授 100044 北京市

2.1 移动IP功能的实现

移动IP定义了三种必须在移动协议中实现的功能是：

(1)移动节点：一些在因特网上信息从一条链路转到另一条链路，而仍然保持所有正在进行的通信的节点，叫移动节点。

每次移动节点与别人通信所用的地址叫做移动节点的家乡地址。

(2)家乡代理：有一个端口与移动节点家乡链路相连的路由器，叫家乡代理。

移动节点切换到一条新的链路时，它总会把它的当前位置的地址通知家乡代理，这个地址称为移动节点的转交地址。家乡代理广播对移动节点家乡地址的网络前缀的可达性，从而"吸引"那些送往移动节点家乡地址的IP包。

家乡代理解析送往移动节点的家乡地址的包，并将这些包通过隧道技术传送到移动节点。

(3)外地代理：一个端口与移动节点外地链路相连的路由器，叫外地代理。

外地代理有时向移动节点提供自己在该链路上的IP地址称为移动节点的转交地址。

外地代理帮助移动节点把移动节点的转交地址通知给家乡代理。

外地代理有时拆封已被移动节点家乡代理封装在隧道中的包，然后再将它发送给移动节点。

外地代理一般都是作为移动节点在外地链路上的缺省路由器。

2.2 移动IP的控制机制

(1)家乡代理和外地代理都是通过周期地组播或广播一个称为代理广播的消息来宣告它们的代理身份，广播的消息中包括它们的网络地址。

(2)移动节点收到这些代理广播消息后，检查其中内容以确定自己是连在家乡链路还是外地链路上。当它连在家乡链路时，就可以像固定节点一样的工作。

(3)连在外地链路上的移动节点需要一个转交地址。转交地址有两种，外地代理转交地址和配置转交地址，外地代理转交地址可以从外地代理的广播消息中找到，配置转交地址则是通过DHCP或PPP的IPCP或手工来配置。

(4)若外地链路上有一个可用的外地代理，移动节点就向它请求外地代理服务，然后移动节点向家乡代理注册自己的转交地址，为阻止拒绝服务攻击，注册消息要求进行认证。

(5)家乡代理或者是家乡链路的其他一些路由器广播对移动节点家乡地址的网络前缀的可达性，从而"吸引"发往移动节点家乡地址数据包。家乡代理截取这个包，并根据移动节点的转交地址，通过隧道将数据包传送给移动节点的转交地址处。

(6)在转交地址处——可能是外地代理或移动节点的一个端口，原始数据包被从隧道中提取出来送给移动节点。

(7)相反，由移动节点发出的数据包被直接选路到目的节点，无需隧道技术。对所有移动节点发出的数据包来说，外地代理完成路由器的功能。

3 移动IP嵌入Linux的方法

3.1 实现方法

移动IP支持的代理搜索并注册在Linux中，在程序中都是通过软状态来实现的。这些软状态中，除了空闲状态以外，其余的状态都是由定时器控制的。软状态的应用提高了系统的健壮性，实现细节如下：表中MN代表移动节点，HA代表家乡代理，FA代表外地代理。

3.1.1 代理搜索

在代理搜索中，移动节点有三种状态：空闲(idle)，代理请求(soliciation)和广播接收状态(advertisement receving)。图1说明了三种状态的相互转换。表1列出了各定时器的属性。表2用来解释各原语的作用。

表1 定时器属性

定时器	控制者	被记录的行为	到期后控制者的行为
T11	MN	代理请求有效期	重发代理请求消息
T12	MN	代理有效期	删除代理
T13	MN	注册请求有效期	重发注册请求消息
T14	MN	注册有效期	快到期时再次重发注册请求消息
T22	FA	广播间隔	发送代理广播
T32	HA	广播间隔	发送代理广播

表2 原语功能

原语	实体	功能
MIP_SOLICIT_REQ	MN	要求发送代理请求消息
MIP_SOLICIT_CNF	MN	发送了MIP_SOLICIT_REQ之后，收到广播后的应答
MIP_SOLICIT_IND	MN	没有发送MIP_SOLICIT_REQ，收到广播后的应答
MIP_DISSAPPEAR_IND	MN	宣布某一代理不再有效
MIP_REGISTER_REQ	MN	要求发送注册消息
MIP_REGISTER_CNF	MN	表明收到注册应答

原语MIP_SOLICIT_IND表明，核心栈已经收到一个代理广播消息，而MIP_SOLICIT_CNF则是对

前面发出的 MIP_SOLICIT_REQ 原语的一种应答，同时说明核心栈已经收到代理广播消息。

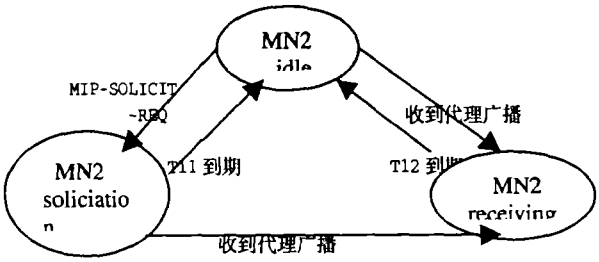

图 1 移动节点状态转换图

3.1.2 注册

在注册过程中移动节点上有四种状态：空闲(idle)，注册请求(registration request awaiting)，注册(registered)，注册再启动(registration reset awaiting)。就移动节点来说，只有当它在代理搜索中处于 MN2(advertisement receiving)状态时，这些状态才有可能出现。这时有人会问，什么时候移动节点才处于注册再启状态呢？就是当已有注册虽还未到期，移动节点却再次向家乡代理发出注册请求时所处的状态。

图 2 是注册过程的状态转换图。由于一个移动节点可以有多重注册，因此 MN(id)中的 id 是注册号即具体与那个代理注册。

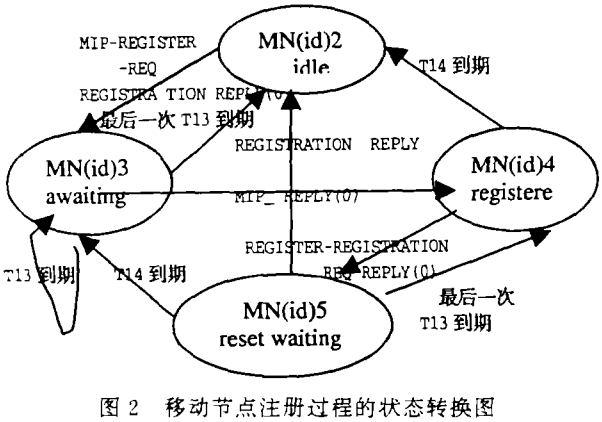

图 2 移动节点注册过程的状态转换图

定时器 T13 是记录移动节点的注册请求时间，系统规定了节点的注册请求重发次数，当还未到这个极限时，注册请求时间的到期，会引发注册请求消息的重发，而最后一次到期，节点则回到原状态。若到期前是注册请求状态，节点回到空闲状态；若到期前为注册再启状态，节点将回到注册状态(原来的注册还未到期的情况下)，移动节点以前的注册仍然有效，只有新的注册成功了，才会将旧的覆盖掉；若原来的注册已经到期，节点将回到空闲状态。

T14 是记录移动节点的注册有效期。T14 到期时，现存的绑定就不再有效了。在注册状态，过期后会回到空闲状态；若是注册再启状态，移动节点将回到注册请求状态，因为新的注册请求还仍在进行中。

REGOSTRATION REPLY 表示节点收到代理发出的注册成功的消息，REGISTRATION REPLY(0)则表示注册失败的消息。

用户程序可能会要求一个很长的注册有效期，但是家乡代理一般却只能授予一个不太长的有效期，这种情况下，当 T14 到期时，核心栈会自动再次发送注册请求消息，请求余下的还未满足的有效期。最后当这个长的有效期全部被满足时，注册才会被删除。

3.2 核心栈表和无线接口表

在移动节点的核心栈中，有一个代理表和注册表。所有可以用的代理都在代理表中。因此一旦一个代理表消失了(即过期了)，移动节点马上能注册一个新的转交地址，注册表则记录着所有的移动绑定。此外，还有一个无线接口表，这是为将来移动路由器备用的。

移动节点的代理表中应包括：代理表中的下一项，代理表中的前一项，定时器 T12，外地代理广播送往的地址，从广播消息中获得的路由器地址，从广播消息中获得的转交地址，代理有效期，代理忙不忙等信息。

移动节点注册表中包括：注册表中下一项，注册表中前一项，无线接口表首址，定时器 T13，定时器 T14，用户程序的进程号，在栈中的注册号，用户程序所用的套接字，指向代理缓冲的指针，用户程序要求的生存期，用户程序要求的生存期的备份，被代理授予的生存期，家乡代理地址，注册状态，是否保留以前的注册，对于 T13 到期的重发次数等信息。

3.3 用户接口

移动 IP 核心栈位于 IP 栈和 UDP/ICMP 模块之间。可以通过发送用户原语来控制核心栈，而核心栈则把核心原语放入套接字中以响应用户用 ioctl()这个 Unix 家族中的系统调用来向核心栈发送原语；同样，核心栈也是通过 iotcl()把原语排入套接字的队列中。若用户程序想要收听核心栈的消息时，调用 revfrom()即可。

套接字程序的编写不在此详述，重点放在移动IP上。

4 移动IP安全问题的解决方案

4.1 如何阻止拒绝服务攻击

拒绝服务攻击是指一个“黑客”假冒移动节点发送一个伪造的注册请求，把它自己的IP地址当作移动节点的转交地址。这样产生的后果是通信对端送出的所有数据包都会被移动节点的家乡代理通过隧道送给“黑客”，从而“黑客”能窃取每一个送给移动节点的数据包，并且移动节点再也得不到任何服务了。

对于这种攻击的解决办法是，在移动节点和它的家乡代理之间交互的注册信息都进行有效的认证，即每次交互的新的注册信息时，都要确认是否是真正的移动节点发出的信息，认证一下移动节点的身份的有效性。实现这种认证的方法是在移动节点产生的注册请求信息中，添加移动－家乡认证扩展，即身份验证域。这个认证域是由用加密算法Keyed MD5计算出的一串字节的消息摘要组成，而这个消息摘要一定是独一无二的，并且也绝对不会被“黑客”所推断出或猜出来。这一串字节由下列内容按次序组成：

(1)只有移动节点和它的家乡代理知道共享的秘密密钥；

(2)注册请求消息的定长部分；

(3)包括移动家乡认证扩展在内的所有扩展(即类型、长度和安全参数索引域)，但不包括认证域；

(4)接着又是移动节点和它的家乡代理知道的共享的秘密密钥。

这样计算出来的消息摘要使得“黑客”几乎不可能产生一个伪造的注册请求消息而又不被家乡代理识破，达到阻止拒绝服务攻击的目的。

4.2 如何阻止重发攻击

重发攻击是指一个“黑客”将一个有效的注册请求存起来，然后过了一段时间后，等移动节点到一条新的链路上时再重发这个消息，注册一个伪造的转交地址，从而假冒移动节点获得服务。为了防止这种重发攻击，移动节点为每个连续的注册消息的标识域产生一个唯一的值，这个值使得家乡代理可以知道下一个值应是多少，这样，“黑客”就无能为力了，因为它保存的注册消息会被家乡代理认为已经过时了。

移动IP可采取两种填写标识域的方法，一种是用时间标签，移动节点将它当前估计的日期和时间填写进标识域中。如果这种估计和家乡代理估计的时间不够接近，那么家乡代理会拒绝这个注册请求，并向移动节点提供一些信息来同步它的时钟，这样移动节点以后产生的标识域就会在家乡代理允许的误差范围内了。另一种方法是采用Nonces，在这种方法中，移动节点向家乡代理规定了移动节点发送下一个注册应答消息标识域的低半部分中必须放置的值，相似地，家乡代理向移动节点规定了在下一个注册请求消息标识域的高半部分中必须放置的值。如果有任一个节点接收到的注册消息的标识域与期望值不符，如果是家乡代理，就拒绝这条消息，而移动节点则不理会这条消息。拒绝机制使得移动节点可以和家乡代理同步，以防止它们保留有关下一个消息标识域过时的值。

4.3 移动IP包如何安全通过防火墙

有的防火墙会使移动节点发出的数据包被防火墙全部抛弃，因为它使用的源地址是它的家乡地址，而防火墙认为该地址应该位于移动节点的家乡链路上。

这种防火墙机制严重影响位于外地链路上的移动节点发出的数据包。注意，防火墙并不应该影响发往移动节点的数据包，因为隧道IP报头中的源地址(家乡代理地址)和目的地址(转交地址)在网络拓扑上都是正确的。

反向隧道可以解决防火墙给移动IP带来的问题。当移动节点注册时，可以申请反向隧道服务，将自己产生的数据包进行隧道封装后，再送到家乡代理。隧道封装工作可以由外地代理完成。隧道报头的IP源地址(转交地址)和目的地址(家乡代理地址)在拓扑结构上都是正确的，所以不会被防火墙丢弃掉。

(责任编辑：张树增 收稿日期：2000－05－10)