移动 IPv6 早期 BU 中基于信息流模式的授权方案*)

游 红 吴中福 曹海鑫 于兴斌 刘建华
(重庆大学计算机学院 重庆 400044)

摘 要 与移动 IPv6 返回路由可达过程中地址测试相关的延迟对延迟敏感的应用造成了负面影响。EBU(早期绑定更新)通过在测试阶段使用新的转交地址缓解了这个问题。我们提出并分析了一种基于信息流模式的机制,这种机制防止了利用 EBU 进行放大洪水攻击,并使攻击者放弃使用其它类型洪水攻击的企图。

关键词 移动 IPv6,EBU(早期 BU),RRP(返回路由可达过程),信息流模式,BILL

Tarrfic-pattern Mode Based Authoration Shceme for Early Binding Update in Mobile IPv6

YOU Hong WU Zhong-Fu CAO Hai-Xin YU Xing-Bin LIU Jian-Hua
(Department of Computer Science, Chongqing University, Chonqing 400044)

Abstract The latency associated with test in Mobile IPv6's Return Routability Procedure can have an adverse impact on delay-sensitive applications. Early Binding Updates mitigate this issue by already using a new care-of address in parallel with testing it. We propose and analyze a traffic-patten-based mechanism that prevents misuse of Early Binding Updates for amplified flooding attacks and discourages such misuse for other types of flooding attacks.

Keywords Mobile IPv6, EBU(Early Binding Updates), RRP(Return Routability Procedure), Traffic-pattern, BILL

1 前言

大量移动设备(移动电话,PDA,笔记本等)的用户希望在移动过程中保持 Internet 接入和连续通信,移动 IP 就是在原来 IP 协议的基础上为了支持节点移动而提出的解决方案。Internet 业务飞速发展,只能用 IPv6 才能彻底解决 IPv4 存在的种种问题:地址空间耗尽、路由器爆炸、移动性支持不够、网络安全考虑太少、服务质量差等。移动主机通过无线链路接入到网络,开放的环境更容易遭受被动窃听、重放攻击和其他主动攻击,解决好移动安全性问题对于移动 IPv6 技术的推广与发展具有极大的实用意义。

2 移动 IPv6 及其安全现状简介

移动 IPv6 中有 3 个主要的功能实体:(1)移动节点 MN(Mobile Node):能够在不同链路上切换的节点。(2)通信对端 CN(Correspondent Node):与 MN 通信的对端节点,可以是固定或移动的节点。(3)家乡代理 HA(Home Agent):MN 家乡链路上的一台路由器,当 MN 不在家乡链路上时,HA 把目的地为 MN 的 IP 包通过隧道发送给 MN,并接收 MN 通过反向隧道发送过来的数据包,再转发给 CN。

目前,移动 IPv6 安全问题已经成为制约其推广应用的关键因素,该领域的研究进展甚微,几乎是空白,很少有可靠的安全协议和方案出现,当前 IETF(Internet 工程任务组)指出现行移动 IPv6 继承 IPv6 的 IPsec 存在着很大的安全漏洞,要彻底解决移动 IPv6 的安全问题,应重新设计一套安全机制。安全问题一直是制约移动 IPv6 发展的一大难题,虽然安全问题难以突破,但的确是亟待解决的瓶颈问题,只有在保证安全的基础上,才能得到更大的发展。

IETF 的安全专家最近宣布 IPsec 不能胜任保护"BU"工作,原因之一是 IPsec 需要一套公共密钥系统来运作,但该系统尚未实施;另一个原因是 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 协议的设备诸如手机、PDA 等的计算能力都很弱,而且能耗也需要考虑,因此要求进行大量计算的安全机制不太适合这些设备。安全专家对这一漏洞的发现,意味着 IETF 将不得不开发新的方法来识别使用 IPv6 地址漫游的设备,这将使移动 IPv6 的实现推迟,而移动 IPv6 的最初构想距今已有 10 年。

IETF 提出替代 IPSec 的定制密钥 PBK(Purpose Built Key),PBK 是一种轻量级认证协议,实现简单,但其安全性却没有 IPSec 好,比如还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。IPv6 的拥护者担心如果采用 PBK 机制而非更安全的 IP-Sec 机制,会削弱转向 IPv6 的动因。

PBK 生成一对临时的公共/私有密钥来确认一台漫游设备就是建立某个特定通信的设备。在每个移动 IPv6 会话开始前会生成一对新的密钥,会话结束密钥也会取消。这一对密钥只会由参与通信的设备使用,不会为第三方获得。由于密钥的经常变化,用户的匿名身份将会得到保护。

3 返回路由可达过程 RRP 及其面临的安全威胁

移动 IPv6 中采用了返回路由可达过程 RRP(Return Routability Procedure)来加强与 CNBU 的保护,在 MN 向 CN 发出 BU(绑定更新)之前,MN 与 CN 至少要交换 4 个控制信息(HoTI&HoT,CoTI&CoT),只有这 4 个控制信息成功交

*)本文受研究生创新基金支助,基金号:200504Y1A0110118 游 红 硕士研究生,研究方向:移动 IP,网络安全。吴中福 教授,博士生导师,主要研究方向:计算机网络教育、计算机网络安全。曹海鑫 研究方向:计算机网络、远程教育。于兴斌 硕士研究生,研究方向:移动 IP。刘建华 硕士研究生,研究方向:移动 IP,网络安全。

换之后，MN 才会向 CN 发出 BU，CN 也才会对 MN 发过来的 BU 进行处理。

但是，这种方案存在中间人攻击的威胁，无论是 MN 发送给 HA 还是 CN 的 BU，如果不采取一定的安全措施，就会诱发因此而带来的安全问题。这是因为：一方面，对 CN 而言，如果恶意节点伪装成合法的 MN 发送 BU 给它，而 CN 又相信了恶意节点发送来的 BU，则 CN 和合法 MN 之间的通信就反而中断了，CN 也无法确定合法 MN 现在所处的位置。对 HA 而言，如果 BU 不是来自合法的 MN，则在隧道模式下所有发送给合法 MN 的数据包都被路由到其他节点而无法到达合法的 MN。要保证提高网络性能的安全性并充分利用其带宽，MN 必须对 BU 进行安全保护，防止恶意节点对其进行破坏（篡改或者其他恶意行为），以便让 CN 和 HA 获得 MN 的真正位置。

图 1 是返回路由可达过程 MN 切换后同 CN 交换报文的基本信息。

MN 切换后同 CN 交换的报文	字节数	MN　　HA　　CN
(1)Home Test Init	56	|----------->|----------->|
(2)Home Test	64	|<-----------|<-----------|
(3)Care-of Test Init	56	|----------->|
(4)Care-of Test	64	|<-----------|
(5)Binding Update	72	|----------->|
(6)Binding Acknowledgement	64	|<-----------|

图 1　返回路由可达过程 RRP

4　早期绑定更新 EBU 简介[2]

当 MN 知道将改变其网络接入位置时，就发起预先家乡地址测试（HoTI&HoT）；如果 MN 无法预料切换，就应当定期重复家乡地址测试。当 MN 最终切换（handover）时，MN 就获得一个新转交地址 CoA，并向 CN 发送一条早期 BU 报文（Early Binding Update message）。预先家乡地址测试使 MN 能在该报文中证明其家乡地址 HoA。

MN 一发出 EBU 报文，就立即并发转交地址测试（与被测转交地址发送和接收数据的同时进行转交地址的测试）。然后 MN 就可以开始使用新的转交地址。当 CN 从 MN 接收到 EBU 报文，就开始使用 MN 的新转交地址。因此，MN 和 CN 都在并发转交地址测试阶段就已使用 MN 的新转交地址。

当 CN 从 MN 接收到 EBU 报文时，根据家乡地址认证，就可以相信 MN 是在该报文中广播的家乡地址的合法所有者。既然在 EBU 报文中，没有转交地址认证，那么这时 CN 就不知道 MN 是否真在新转交地址。因而新转交地址是“半证实”的，而半证实转交地址的绑定寿命只有几秒。

当并发转交地址测试完成时，MN 就向 CN 发送一条标准的绑定更新（SBU）报文（Standard Binding Update message），该报文符合 RFC3775 中所定义的格式和语义[1]，对 MN 的家乡地址和新转交地址都加以认证。因此，当 CN 接收到 SBU 报文时，就可以相信 MN 使用的是正确的家乡地址而且 MN 真的在新转交地址。然后 CN 把新转交地址的状态从“半证实”更改为“已证实”，并将关联绑定的寿命更改为 MN 请求的和最大寿命 X_RR_BINDING_LIFETIME[1] 中较短的值。

因为在 EBU 报文中没有转交地址认证，所以当 MN 的转交地址半证实时，需要有其它保护，否则恶意节点就可以滥用 EBU 中使用半证实的转交地址来注册第三方的 IP 地址。CN 就会把攻击者的报文分组重定向到第三方。因此我们提出一种基于信息流的授权方案来提供当 MN 的转交地址“半证实”时所需要的保护，下一节将详细介绍基于信息流的授权思想。

图 2 是早期绑定更新过程。

MN 切换前同 CN 交换的报文	MN　　HA　　CN
(1)Home Test Init	|----------->|----------->|
(2)Home Test	|<-----------|<-----------|
MN 切换到另一个子网	
(3)Binding Update	|----------->|
(4)Early Binding Update	|----------->|
(5)Care-of Test Init	|----------->|
(6)Binding Acknowledgement	|<-----------|
(7)Early Binding Acknowledgement	|<-----------|
(8)Care-of Test	|<-----------|
(9)Binding Update	|----------->|
(10)Binding Acknowledgement	|<-----------|

图 2　早期绑定更新

5　基于信息流模式的授权方案

5.1　概念

INVESTMENT 是移动节点 MN 对带宽的投资。MN 通常付出两种 INVESTMENT：发送报文分组到通信对端 CN 的 INVESTMENT 和从 CN 接收报文分组的 INVESTMENT。

BILL 是 CN 用来确定它能发送到一个特定的 MN 的数据量的单位。MN 通过付出 INVESTMENT 获得 BILL。

已证实转交地址是 MN 已通过认证的 SBU 报文向 CN 注册的转交地址。半证实转交地址是 MN 已通过认证的 EBU 报文但是还不是通过认证的 SBU 报文向 CN 注册的转交地址。

5.2　基于信息流模式授权方案的分类

表 1 是不同分类情况下的 BILL 计算方法和报文分组的发送及接收情况：

CoA：MN的转交地址　　HoA：MN的家乡地址

MN-Sed：根据MN发送的报文分组来增加MN的BILL

MN-Rev：根据MN接收的报文分组来增加MN的BILL

表1　基于信息流模式授权方案的分类

		CoA已证实	CoA半证实
CN→MN	MN-Sed	发送到CoA，BILL不变	BILL>=size(P)：发送到CoA，BILL：=BILL−size(P) BILL<size(P)：发送到HoA，BILL：=0
	MN-Rev	发送到CoA，BILL：=BILL+size(P)	
MN→CN	MN-Sed	接收，BILL：=BILL+size(P)	
	MN-Rev	接收，BILL不变	

MN付出INVESTMENT，如带宽、处理能力和内存来向CN发送报文分组和从CN接收报文分组。CN可以为任何一类INVESTMENT支付BILL。在CN，可以通过测量从MN接收的报文分组为发送报文分组的INVESTMENT支付BILL。当MN的转交地址得到证实时，可以通过测量发送到MN的报文分组为接收报文分组支付BILL。两种模式各有其优缺点。

当CN要发送报文分组给MN时，它首先检查MN转交地址的状态。如果转交地址是已证实的，转交地址近来已经被MN认证了，那么CN就可以相信MN真的在该转交地址。在这种情况下，CN正常地发送报文分组到MN的转交地址，而不涉及到MN的BILL。否则，如果MN的转交地址的状态是半证实的，CN就根据MN的BILL多少来确定报文分组的目的地：如果MN的BILL大于或等于要发送的报文分组的大小，那么CN就直接发送该报文分组到MN的转交地址，并根据报文分组的大小减少MN的BILL；而当MN的BILL小于要发送的报文分组的大小，那么CN就将报文分组发送到MN的家乡地址，在这种情况下，报文分组由MN的HA转发到MN。既然MN的家乡地址在EBU报文中已经得到认证，那么CN就可以认为MN是家乡地址的合法所有者[2]。因而，CN可以发送报文分组到MN的家乡地址而不必担心安全问题，而且在这种情况下，它也不需要减少MN的BILL。

我们认为与CN以正常方式进行通信的可信MN的自然付出INVESTMENT来发送报文分组给CN，也接收来自CN的报文分组。因此可信的MN因为正常的行为就自然获得了BILL，从而在BU阶段可以在半证实的转交地址接收报文分组。结果，MN不必知道CN启用了基于信息流的授权。

基于信息流的授权要求CN知道所有注册转交地址的状态，包括已证实和半证实的。转交地址状态决定MN是否需要为发送到转交地址的报文分组支付BILL。我们提出CN为每条绑定维护额外的长度位标志位。

5.3　指数老化

我们认为MN的BILL应该只代表MN最近付出的INVESTMENT。否则，MN就可能在非常长的时间内搜集BILL并在非常短的时间内消费该BILL。恶意节点可以通过相对慢的数据流积累大量BILL来对这种特性加以利用，并通过突然使用这些BILL，向任意受害者发送持续时间短、但数量大的数据。

我们提出了指数老化来逐渐减少MN的旧的BILL。使用指数老化后，当MN不使用BILL时，BILL就会减少，就不可能在很长时间内积累BILL并搜集无限量的BILL。这意味着指数老化能将发送到MN未证实转交地址的报文分组的比例限制到和最近发送到同一个MN证实的转交地址的报文分组相似。换句话说，指数老化能消费MN的BILL的报文分组的比例到和MN近来已经获得BILL的报文分组的比例相似。指数老化能限制发送到未证实转交地址的报文分组的比例的原因在于：无论MN的BILL增加还是减少，一个精确的老化函数都可以对BILL进行老化，并对MN的BILL改变后经过的时间进行调整。但是精确的老化函数非常复杂，因此我们提出了用TENTATIVE_BINDING_LIFETIME长度等间隔的"BILL计算间隔"(BILLing intervals)简单计算MN的BILL。MN在BILL计算间隔内所付出的INVESTMENT在MN旧BILL的BILL计算间隔结束时被指数老化后成为BILL。于是我们确保了新BILL在至少一个BILL计算间隔内不会老化。CN可以对其绑定缓存中所有条目的BILL计算间隔进行同步，因而一个时钟是足够的。

注意：TENTATIVE_BINDING_LIFETIME既定义了未证实转交地址的BILL计算间隔的长短，又定义了其绑定寿命的长短[2]。因为未证实转交地址的绑定寿命就是BU阶段MN的BILL健康时间的长短，所以让MN在这段时间搜集BILL而只老化该段时间以前的BILL是有意义的。

指数老化的替代方案是仅通过一个固定的上限来限制MN的BILL。限制肯定能防止MN搜集无限量的BILL。但是，限制不能防止MN在使用BILL前在很长时间内搜集BILL。限制也对MN和CN之间路径上的全部状况不敏感。低带宽连接的限制对高带宽连接肯定是不合适的，反之亦然。因此我们认为指数老化是一种比使用固定上限限制MN的BILL更合适的方法。

5.4　CN发送报文分组情况

假设CN要发送报文分组给MN，且该MN的转交地址是已证实的。如果CN根据MN发送的报文分组为MN的INVESTMENT支付BILL，它就不必做任何与基于信息流授权相关的事。CN仅仅发送该报文分组到转交地址(A.1)而不改变MN的BILL。

(A)发送一个报文分组到已证实的转交地址(为发送报文分组支付BILL)

(A.1)send(PACKET,CARE_OF_ADDRESS)

如果CN根据它接收报文分组的INVESTMENT计算MN的BILL，它就按下面的算法进行。

(A′)发送一个报文分组到已证实的转交地址(为接收报文分组支付BILL)

(A′.1)BILL：=BILL+size(PACKET)

(A′.2)send(PACKET,CARE_OF_ADDRESS)

CN根据该报文分组的大小(字节数)来测量MN从CN接收报文分组的INVESTMENT(A′.1)。在一个BILL计算间隔内付出的INVESTMENT用一个变量进行累计该变量应当足够长以免发生翻转。CN在其绑定缓存中为每个条目维护该变量。在指数老化了任何旧BILL后，在步骤(D)中的BILL计算间隔结束时，根据INVESTMENT的值来计算新BILL。因此我们确保了至少一个BILL计算间隔内新BILL不会老化。在步骤(A′.2)中，报文分组被发送到MN的转交地址。

现在假设 CN 要发送一个报文分组给 MN 并且该 MN 的转交地址为半证实。在这种情况下，CN 根据下面的步骤确定该报文分组的目的地，而与该 CN 为 MN 发送还是接收报文分组的 INVESTMENT 支付 BILL 无关。

(B)发送报文分组到半证实的转交地址(根据发送或接收报文分组支付 BILL)

```
(B.1)If BILL >= size(PACKET)
       Then
(B.2)     BILL := BILL - size(PACKET)
(B.3)     send(PACKET,CARE_OF_ADDRESS)
(B.4)Else
(B.5)     BILL:=0
(B.6)     send(PACKET,HOME_ADDRESS)
     EndIf
```

CN 用变量 BILL 来保存 MN 的 BILL。该变量应当足够长以免发生翻转。CN 在其绑定缓存中为每个条目维护该变量。假设 BILL 大于或等于将发出的报文分组以字节计算的大小(B.1)，BILL 就减去该报文分组大小(B.2)，然后将该报文分组发送到 MN 的转交地址(B.3)。否则，当 BILL 小于将发出报文分组以字节计算的大小(B.4)，为了在报文分组大小不同时，在单独的 BU 阶段不在 MN 的家乡地址和当前的转交地址转换多次，任何剩余的 BILL 都被消除(B.5)。然后报文分组就发送到 MN 的家乡地址(B.6)。(注意：BILL 不能为负值)。

需要说明的是：当 MN 的转交地址为半证实时，CN 也能认为 MN 是所注册家乡地址的合法所有者，不需要考虑安全问题，就可发送报文分组到该家乡地址。这是因为 CN 近来已经从 MN 接收到了一条 EBU 报文，其中 MN 的家乡地址已经得到了认证[2]。但是，在 MN 和 CN 之间传送报文分组和经过 MN 的 HA 的报文分组的传播延迟差异可能对传输层协议和应用程序产生负面影响。这种影响的程度尚需进一步的研究。

可用 BILL 的量不影响 MN 发送到 CN 的报文分组的路由选取。即使转交地址为半证实并且 BILL 小于报文分组的大小，CN 也能安全地接受 MN 的转交地址发送的报文分组。原因是从 MN 发送到 CN 的报文分组不能发动除了直接洪水攻击或反射攻击之外的洪水攻击。这说明在发出了新转交地址的 EBU 报文后，MN 可立即从该转交地址发送报文分组给 CN。MN 不必知道 CN 使用了基于信息流的授权和它的 BILL 大小。

5.5 CN 接收报文分组情况

假设 CN 从 MN 接收一个报文分组。如果 CN 根据 MN 发送报文分组给 CN 的 INVESTMENT 支付 BILL，CN 就执行下面的算法，而不管 MN 的转交地址证实与否。

(C)接收一个报文分组(根据接收报文分组计算 BILL)

```
(C.1)BILL := BILL + size(PACKET)
(C.2)deliver(PACKET)
```

CN 根据报文分组以字节数计算的大小来测量 MN 发送一个报文分组的 INVESTMENT(C.1)。在步骤(C.2)中，该报文分组被提交给应用程序。

如果 CN 根据接收报文分组为 MNINVESTMENT 支付 BILL，它就不必做与基于信息流授权相关的任何事。它仅将该报文分组提交给应用程序(C′.1)而不改变 MN 的 BILL：

(C′)接收一个报文分组(根据发送报文分组计算 BILL)

```
(C′.1)deliver(PACKET)
```

5.6 处理时钟标记

CN 可以同步其绑定缓存中所有条目的 BILL 计算间隔。因而标记 BILL 计算间隔结束的一个时钟是足够的。当时钟标记到达时，CN 根据下面的公式重新计算其绑定缓存中每个条目的 BILL。该公式与 CN 根据接收还是发送报文分组来计算 BILL 无关。与已证实和半证实转交地址的绑定没有区别。

(D)处理时钟标记(根据发送或接收报文分组计算 BILL)

```
(D.1)For Each Binding Do
(D.2) NEW_BILL := INVESTMENT_QUENCH_FACTOR * INVESTMENT
(D.3)BILL := BILL * BILL_AGING_FACTOR
      \ + NEW_BILL
(D.4)INVESTMENT := 0
     EndFor
```

结论 移动 IPv6EBU 已被提议作为移动 IPv6 的可选优化方案。EBU 使得 MN 在转交地址测试进行过程中使用新转交地址。为防止基于重定向洪水攻击滥用这种并发性，需要采取保护性措施。我们提出了一种基于信息流授权机制来防止滥用 EBU 进行放大的、基于重定向的洪水攻击。通过选取适当参数，基于信息流的授权可以阻止滥用 EBU 来进行非放大的、基于重定向的洪水攻击。

通过基于信息流的授权，CN 可以监控 MN 发送或接收报文分组的 BILL。CN 根据 MN 发送到 CN 或从 CN 接收的报文分组的大小确认所付出的 BILL。付出的 BILL 被转化成 BILL。在 BU 阶段，CN 发送到半证实的转交地址的每个报文分组都消耗 BILL。BILL 使恶意节点滥用 EBU 进行基于重定向的洪水攻击所付出的 BILL 比进行常规洪水攻击付出的 BILL 更多。这种特性会使恶意节点改变其滥用 EBU 的企图。

下一步研究方向：

(1)设计失效因子算法，为了更合理地计算 BILL，必须设计一种更科学的算法，要考虑的因素很多，与论文中提出的 BILL 计算间隔为基础的算法相比是相当复杂的。我们将从算法设计的角度入手，综合分析和考虑影响因素，从而提出一个安全和性能上取得较好平衡的算法。

(2)通过搭建 MIPL(Mobile IPv6 for Linux)实验床对已有的代码进行修改，增加论文中有关部分，并测试其性能和效果，通过对比，进行论证。

(3)考虑到报文分组丢失对 BILL 计算精确程度的影响，应重点研究信道条件的参数化问题，以提高该机制的可行性。

参 考 文 献

1 Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. RFC 3775

2 Vogt C, Bless R, Doll M, Kuefner T. Early Binding Updates for Mobile IPv6. draft-vogt-mip6-early-binding-updates-00 (work in progress), February 2004

3 Nikander P, Arkko J, Aura T, et al. Mobile IP version 6 Route Optimization Security Design Background. draft-ietf-mip6-ro-sec-00 (work in progress), April 2004

4 Hsieh R, Seneviratne A. Performance analysis on Hierarchical Mobile IPv6 with Fast-handoff over End-to-End TCP