运用Kerberos方法构建移动IP的绑定更新安全*)

田凤斌[1] 吴中福[1] 文俊浩[2]

(重庆大学计算机学院 重庆400044)[1] (重庆大学软件学院 重庆400044)[2]

摘 要 绑定更新(Binding Update)是移动IPv6里面移动节点用于向家乡代理和通信对端告知自己当前位置而传输的信息。然而,移动IPv6里面的绑定更新在安全协议方面还需要做进一步的研究和改进。本文提出了一种基于Kerberos的认证框架来构建绑定更新的安全。指出了该框架较移动IPv6的RRP(Return Routability Procedure)的优越性。

关键词 移动IP,Kerberos,绑定更新,RRP,安全,攻击

Secure Binding Update of Mobile IP with Kerberos

TIAN Feng-Bin[1] WU Zhong-Fu[1] WEN Jun-Hao[2]

(College of Computer Science,Chongqing University,Chongqing 400044)[1]

(College of Software Engineering,Chongqing University,Chongqing 400044)[2]

Abstract Binding Update is the message transferred by Mobile Node to notice Home Agent and correspondent node about its current location. However,Binding Update in Mobile IPv6 needs to be further researched and improved in terms of security protocol. This paper presents a Kerberos framework to construct the security of Binding Update,and points out the advantages over the mobile IPv6 RRP.

Keywords Mobile IP,Kerberos,Binding update,RRP,Security,Attack

1 引言

移动IP技术的提出解决了通过采用特定主机路由和修改IP地址的方法所带来的缺陷。当一个移动节点MN(Mobile Node)从家乡链路进入外地链路时,它发出请求到家乡链路,请求家乡链路的某一个路由器充当它的家乡代理HA(Home Agent)。从通信对端CN(Correspondent Node)发往移动节点家乡地址的数据包被家乡代理截获,经过家乡代理封装再发往移动节点。移动节点解封该数据包,得到通信对端的相关信息,返回时直接将信息发给通信对端,这就是"三角路由"。

"三角路由"问题的存在,使得MN与CN之间的通信极大地依赖家乡链路和边界路由器,并且加剧了边界路由器和家乡链路的负载。针对"三角路由"的问题,人们提出了路由优化的模式,移动节点向通信对端发送绑定更新,在通信对端的缓存里面建立了移动节点的家乡地址和转交地址的对应关系,这样,MN与CN的通信就不再依赖家乡代理和家乡链路,从而大大提高了网络的健壮性。

然而,无论是MN发送给HA还是CN的绑定更新,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。一方面,对通信对端而言,如果恶意节点伪装成合法的移动节点发送绑定更新给它,而通信对端又相信了由恶意节点发送过来的绑定更新,则通信对端和合法移动节点之间的通信就被中断了,通信对端也就无法确定合法移动节点现在所处的位置。对家乡代理而言,如果绑定更新不是来自合法的移动节点,则在隧道模式下的所有发送给合法移动节点的数据包都被路由到其他节点而无法到达合法的移动节点。要安全地提高网络性能并充分利用带宽,移动节点必须对绑定更新进行安全保护,防止恶意节点对其进行破坏(篡改或者其他恶意行为),以便让通信对端和家乡代理获得移动节点的真正位置。

就目前来看,移动IP绑定更新技术还没有完全成熟,尤其是在安全协议方面还需要很大的改进。安全协议的改进,关系到移动IP技术的最终走向。现阶段基本上是采用Diffie-Hellman和传统的RSA公钥来保护绑定更新。采用Diffie-Hellman加密协议使得移动节点和通信对端以及家乡代理之间的通信特别容易受到中间人(man in the middle)的攻击[1],从而造成通信中断。RSA公钥算法广泛应用于包括移动IPv6在内的网络安全,而它所采用的密钥长度为1024Bit,这极大地消耗了网络带宽,增加了计算负荷,也不是一个理想的方案。有鉴于此,我们采用Kerberos密钥方案来保护绑定更新信息,使其不致受到恶意节点的伪造和DoS(Denial of Service)攻击。

2 几种安全方案的比较

2.1 Diffie-Hellman算法

Diffie-Hellman算法是由Whitfield Diffie和Martin Hellman于1976年创立的。其原理是由通信双方建立一个共享的安全密钥,用于二者之间的通信。基本步骤如下:

1. A,B两个人在有限的循环组G里面达成一个协议,在该循环组G里有一个生成器g。

2. A随机产生一个自然数a,并将g^a发送给B。

3. 同理,B也随机产生一个自然数b,也将g^b发送给

*)该论文受重庆大学研究生创新基金"MIPL环境下切换延迟性能分析"项目的资助。田凤斌 硕士研究生,研究方向:计算机网络、移动IP。吴中福 教授,博士生导师,主要研究方向:计算机网络、计算机安全。文俊浩 副教授,博士研究生,主要研究方向为数据挖掘、软件工程、计算机网络。

A。

4. A 计算$(g^{b})^{a}$，B 也计算$(g^{a})^{b}$。

5. $K=(g^{a})^{b}=(g^{b})^{a}$。

这样产生的 K 就是 A 和 B 共同产生的共享密钥。双方运用这个共享密钥在不安全的通信媒介上来加密彼此通信所传输的内容。然而该协议很容易受到中间人攻击，处于 A，B 通信路径之间的攻击者能够阅读和修改在 A，B 两者之间传输的信息[2]，对移动 IP 而言，由通信双方所产生的密钥并不能完全鉴定发送者和接受者的身份[1]，所以，由 Diffie-Hellman 构建移动节点绑定更新安全不认为是一个很好的方法。

2.2 RSA 算法

RSA 算法以该算法的三个发明者 Ron Rivest，Adi Shamir 和 Leonard Adleman 命名。它广泛应用于数据加密和数字签名。RSA 原理可以简述如下：

1. 找出三个数，p，q，r，其中 p，q 是两个相异的质数，r 是与$(p-1)(q-1)$ 互质的数，p，q，r 这三个数便是私钥。

2. 找出 m，使得 $rm \equiv 1 \bmod (p-1)(q-1)$。这个 m 一定存在，因为 r 与 $(p-1)(q-1)$ 互质，用辗转相除法就可以得到，紧接着计算 $n=pq$。m，n 这两个数便是公钥。

3. 得到公钥和私钥后，开始编码。其过程如下：若资料为 a，将其看成是一个大整数，假设 $a<n$，如果 $a\geqslant n$ 的话，就将 a 表成 s 进位（$s\leqslant n$，通常取 $s=2^{t}$），这样之后，则每一位数均小於 n，然后分段编码。之后计算 $b\equiv a^{m} \bmod n$，$(0\leqslant b<n)$，则 b 就是编码后的资料。

4. 编码之后就是解码。计算 $c\equiv b^{r} \bmod pq$ $(0\leqslant c<pq)$，c 就是解码后的内容，运用费马小定理[3]，很容易就能证明 $c=a$。

如果将 RSA 算法运用于移动 IP 环境中，虽然 RSA 的安全性已经得到了密码界的认可，但速度一直是制约 RSA 算法广泛应用的桎梏，与对称密码算法相比，在速度上至少慢几个数量级，此外，从上面的理论我们知道，RSA 产生密钥也很麻烦，需要消耗大量的资源，在移动 IP 环境中，移动节点和通信对端在交换数据之前至少要交换6次控制信息（HoTI，HoT，CoTI，CoT，BU，BA），如果再花费更多的资源在密钥计算上，肯定是不能忍受的，移动 IP 环境中对速度的要求也决定了 RSA 算法不太适合。

2.3 Kerberos 算法

2.3.1 Kerberos 概述　Kerberos 是由 MIT 在 Needham 和 Schroeder 研究的基础上开发出来的一个针对网络安全的协议。以古希腊守卫地狱入口门的一条有三个头的狗命名。旨在通过认证，清算和审计三个方面来建立一个完善的安全机制，但后两者目前还未完成。它通过使用一个强密码，使客户端能够在一个不安全的网络上向同域内的服务器证明自己的身份。在客户端和应用服务器向 Kerberos 服务器证明了各自的身份后，运用一个会话密钥来对传送的数据加密，从而保证了数据的完整性和机密性。

传统的基于口令的认证系统在开放的网络中存在很大的弊端，恶意节点很容易能够截获用户口令（如运用 sniffer 等工具），然后冒充合法用户登录系统。Kerberos 是基于密码的口令认证，它提供了一种在开放的网络上确认主体（principal）身份的方式。

2.3.2 Kerberos 工作过程　如图1所示，一个完整的 Kerberos 协议包含如下6个步骤[4]。

（1）用户（Client）第一次登录时，向认证服务器 AS（Authentication Server）发出一个要求使用某一特定应用服务器资源的请求，内容包括自己的名称，验证者（例如某一特定服务器）名称，Ticket 的使用期限，以及一个用来匹配请求和响应的随机数 Nonce。

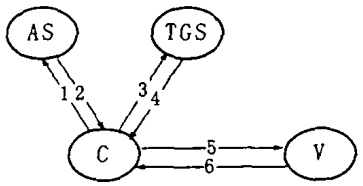

图1　Kerberos 工作过程示意图

（2）AS 收到用户的请求后对其进行响应，响应内容包括客户端和应用服务器进行通信所用的会话密钥（session key），制定的有效时间，请求时客户端所发送的随机数，验证者名称以及有关票据的其他方面的信息，这些内容均用用户在服务器上注册的私钥来加密，再附上包含相同内容的票据一起发送给客户端。

（3）经过1，2两个步骤之后，Client 获得了一个由 AS 发送给应用服务器的票据和会话密钥组成的身份证明。它可以通过该身份证明向应用服务器请求它所需要的资源。然而，为了解决用户每次和新的验证者进行认证时都要提交口令的弊端，Kerberos 使用了一个票据授予服务器 TGS（Ticket Granting Sever），它缓存票据和加密密钥，并使其在一个规定的时间段内有效。Kerberos 协议使用票据授予交换（ticket granting exchange）来允许用户使用这种短期并有效的身份证明来获得票据和加密密钥，而不用再重新输入口令。

（4）TGS 在步骤3之后，使用从票据授予交换中取得的会话密钥而不是用户口令来加密票据授予响应。

（5）用户向应用服务器 V 发出请求，请求它所需要的资源。应用服务器在收到应用请求后，通过解密票据，从中得到会话密钥，再用该密钥解密认证码。由于 Kerberos 使用的是对称密钥加密，如果应用服务器检验到加密和解密认证码使用的是相同的密钥，并且比较前后时间戳，如果在规定的范围内，则校验就会被通过，服务器就会向用户发送资源。

（6）如果用户要求和应用服务器相互认证的时候使用该步骤。

3 Kerberos 在移动 IP 环境中的具体应用与框架

在传统的移动 IPv6路由优化模式中，移动节点和家乡代理之间的通信通过 IPsec 来保护，而 MN 和 CN 的通信的安全是通过一种返回路由可达过程 RRP（Return Routability Procedure）来保证的。在 MN 向 CN 发出 BU（Banding Update）之前，MN 与 CN 至少要交换4个控制信息（HoTI&HoT，CoTI&CoT），只有这4个信息成功交换之后，MN 才会向 CN 发出 BU，CN 也才会对由 MN 发过来的 BU 进行处理。通过这四个信息的交换，CN 了解到通过 MN 的家乡地址和转交地址均能到达 MN[5]。

从上面的描述我们可以知道，在 MN 与 CN 传送数据（正式通信）之前，至少要交换6条控制信息。这大大增加了通信的冗余度和负荷。此外，移动 IPv6路由优化模式并不能解决中间人攻击问题[5]。基于此，笔者提出了一种用 Kerberos 的认证方法来替代移动 IPv6里面的返回路由可达过程和 IPsec 安全的思想。众所周知，Kerberos 是一种基于对称密钥的在开放网络实施认证的服务。将 Kerberos 应用于移动 IPv6环境不仅能够极大地减少通信的冗余度，还能解决中间人攻击的安全问题。下面是基于 Kerberos 的在移动 IPv6上的认证思想。

3.1 Kerberos 应用于移动 IPv6的框架构造

为简化起见，如图2所示，我们将 Kerberos 里面的认证服务器(AS)和票据授予服务器(TGS)统称为 KDC(Key Distribution Center)，因为 KDC 能够充当二者的功能[6]，此处我们特指 HA。而将用户称之为 Client，此处指定为 MN。而 CN 称之为验证者 Verifier。图2和图3的1、2、3、4序号相对应。

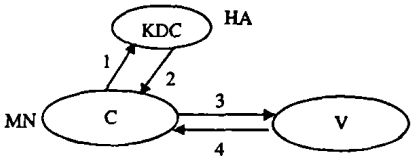

图2 Kerberos 简单示意图

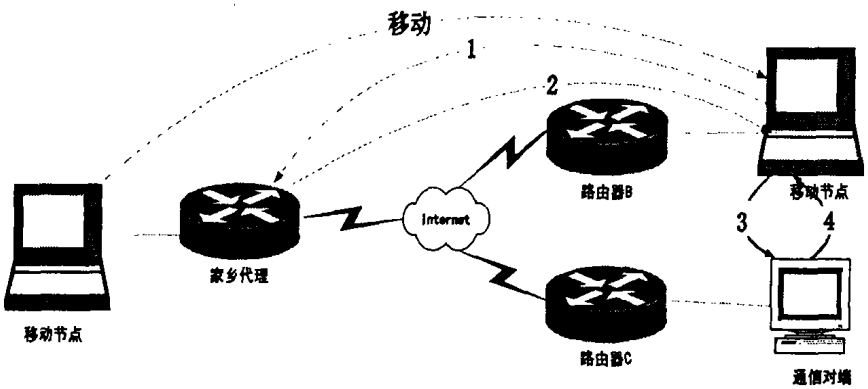

图3 Kerberos 在移动 IP 环境中示意图

通过上面的阐述，我们规定一个完整的 Kerberos 认证要经过如下几个步骤：

(1) 移动 IPv6环境中的每个实体(每个需要使用 Kerberos 的用户和资源)都有自己的秘密密钥，称为该实体的主密钥。该主密钥的获得是通过实体输入自己的名字和口令，然后运用 DES 算法而生成。所有用户的名字和相应的主密钥都存储在 KDC 的数据库里，所以，MN 和 CN 的主密钥都存储在 KDC 的数据库里。如图2中的1所示，移动节点(Client)向家乡代理(KDC)发出一个和 CN 通信的请求，访问 CN 里面的资源，同时附加发送自己的信息(网络地址，Nonce)。

(2) 家乡代理 HA(KDC)接收到来自 MN 的请求后，使用 MN 的主密钥加密访问家乡代理所需的证书(会话密钥 Kmn、cn 和 TGT，Nonce 等信息)，同时，也用 CN 的主密钥加密会话密钥 Kmn、cn 和 TGT，以及由 MN 发送给 HA 的诸如网络地址，Nonce 等其他信息。家乡代理将证书加密之后发送给 MN。因为 MN 不知道 CN 的主密钥，因而不能对由 CN 的主密钥加密的信息进行修改，有效地防止了 MN 对该信息的篡改，也防止了中间节点截获诸如 Nonce 信息。

(3) MN 在获得来自 HA(KDC)访问 CN 的门票后，一方面，它比较发送前后的 Nonce，如果相同，则证明该信息是可靠的，HA 也是可信任的。另一方面，它将由 CN 主密钥加密的信息发送给 CN。CN 运用自己的主密钥解密该门票，获得与 MN 通信的会话密钥 Kmn、cn，TGT，以及 MN 的网络地址，Nonce。

(4) CN 在解密 MN 发来的信息之后，获得与 MN 通信的会话密钥，然后运用该会话密钥加密诸如 Nonce 等信息。同时用随机生成器生成另外一个随机数 Nonce1，也用会话密钥加密该随机数传给 MN，如果 MN 能够用自己的会话密钥解密该信息，并且各自反馈回来的 Nonce、Nonce1通过解密后如果和先前的 Nonce、Nonce1一致，我们认为该信息是可信任的。

至此，MN 和 CN 通过了双方的信任。

3.2 域的运用

Kerberos 共有5个版本，前3个版本已经失去了使用价值，第4个版本和第5个版本各有优势，互相争夺市场份额。基于移动 IPv6的特性(使用 IPv6地址而不是 IPv4地址)，我们使用第5个版本，即 Kerberos V5。

在移动 IP 环境中，我们引入 Kerberos 中域(Realm)的概念来实现 MN 与 CN 和 HA 通信时候的透明性。我们将大型网络分为多个域。每个域里面都有一个 KDC(HA)。为了保证网络的健壮性，我们引入备份 KDC 概念，如果一台 KDC 出现故障，备份 KDC 代替主 KDC 的功能。在 Kerberos V5中，允许经过多个域实现认证。然后通过在门票中加入“转移”域来解决中介域冒充别人身份的问题。当 MN 离开家乡链路到达了另一个域，它必须向该域中的 KDC(HA)注册，如果使用相同的口令，当在该域中口令被截获后它可以在其他域中从事破坏活动，为防止此类行为的发生，在 Kerberos V5中，口令到主密钥的转换过程中使用了域名。因而，使用相同口令会生成不同的主密钥。通过引入域的概念，用户输入口令转换成主密钥存储在 KDC 的数据库里一般比较安全。避免了用户每次通信时都要输入口令，从而间接地保证了对上层通信的透明性。

3.3 对安全的防范措施及冗余分析

首先，我们让 MN 携带自己的网络地址，与其他信息一起发送给 CN。一方面有效地防止了 MN 将门票和会话密钥转让给第三方；另一方面，通过网络地址的使用，可以防止第三方在网络上截获门票和认证值。可以设想，如果在门票中没有包含 MN 的网络地址，那么第三方只需要侦听到其门票和认证码，则在门票的生存时间之后再重新使用这些信息即可进行欺骗活动。

其次，在上面步骤1和步骤4中，我们通过使用 NONCE 字段不仅可以判断 HA 的真实性，而且可以通过该字段判断 MN 是否是要 CN 通信的真实节点。Nonce 是用来匹配请求与响应的字段，如果有中间节点截获，则类似于序号的 Nonce 就会变化。

最后，当 MN 发送信息给 HA 时，我们定义一个时间戳字段，并用 CN 的主密钥加密，当 CN 用自己的主密钥解密 MN 发送过来的门票之后，就能够看清时间戳，如果时间戳不在规定的期限之内，则 CN 认为该信息是不可靠的，于是抛弃该信息。防止了恶意节点对信息的篡改。

另外，我们还采用 DES 对称密钥加密方法来生成主密钥，与 RRP 相比较，采用了更短的密钥长度，也有利于减少系

统开销。

从文[4]我们知道，在一个 RRP 过程中，MN 和 CN 在交换 Payload 之前，至少要交换6条控制信息。而从图2和图3我们可知，MN 和 CN 在交换 Payload 之前，只需要交换4条控制信息。从冗余的角度来看，采用 Kerberos 方法减少了冗余通信，提高了系统通信的性能。

结论 综上所述，与文[4]中的 RRP 方法相比，采用 Kerberos 方法来构建 MN 与 CN 的通信安全，至少有以下优点：解决了第三方的攻击问题；减少了保护绑定更新所需交换的信息；减少了保护绑定更新所需的冗余通信；使用了较小的密钥长度达到了同样的保密效果。

未来的工作 该文提出的是一个用 Kerberos 保护 MN 与 CN 通信的 BU 的安全方案，下一步要通过编写代码实现 Kerberos。然后通过 MIPL(Mobile IPv6 for Linux)来实现，并进一步比较二者之间性能。验证 Kerberos 在移动 IPv6下的优越性。

参 考 文 献

1 Secure Mobile IPv6 Binding Updates with Identity-based Signature. Warodom Werapun, Apinetr Unakul, 2004

2 http://en.wikipedia.org/wiki/Diffie-Hellman

3 http://soft.Winzheng.com/infoView/Article_296.htm

4 Kerberos Authentication Protocol, Hanyil

5 Johnson D, Perkins C, Arkko J. Mibility Support in IPv6. RFC3775, June 2004

6 Kaufman C, Perlman R, Spciner M. Network Security Private Communication in a Public World Second Edition. ISBN 7-5053-9945-4

(上接第32页)

EPGMCC 协议的吞吐量比 PGMCC 提高了将近40%((354－254)/254)。

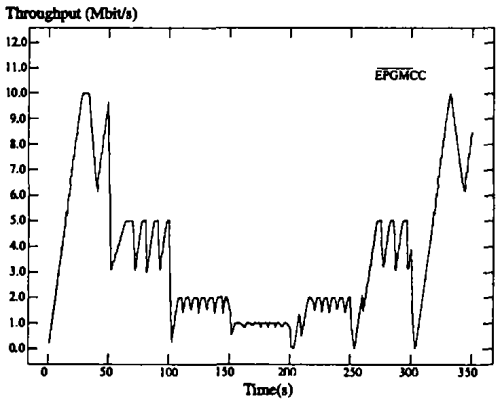

图4 EPGMCC 的灵敏性

从仿真结果可知，在有线网络环境中，EPGMCC 协议保持对传统组播拥塞控制协议的友好性；同时，在无线网络环境中，EPGMCC 有效地提高了传统协议的吞吐量。当无线链路上的随机丢失率为1%时，EPGMCC 协议的吞吐量比传统的 PGMCC 提高了将近40%。

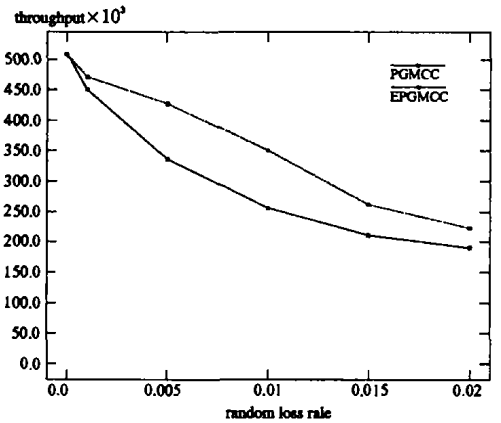

图5 EPGMCC 与 PGMCC 的吞吐量比较

结论 为了解决传统的组播拥塞控制协议在无线接入网络中的性能下降问题，本文提出了一种新的组播拥塞控制协议 EPGMCC。该协议通过在组播组的发送端和接收端对网络的拥塞状态进行估计，并以此为依据辨别分组的丢失原因，对于因网络拥塞发生的分组丢失和因无线链路传输错误发生的分组随机丢失区别对待，从而有效地提高了组播拥塞控制协议在无线网络中的性能。仿真结果表明，在有线网络环境中，EPGMCC 协议实现了良好的 TCP 友好性；在无线网络环境中，EPGMCC 协议能较准确地辨别出分组的随机丢失，从而有效地提高了组播拥塞控制协议的性能。当无线链路上的随机丢失率为1%时，EPGMCC 协议的吞吐量比传统的 PGMCC 提高了将近40%。

在本文提出的组播拥塞控制协议中，如何有效地辨别分组的丢失原因并采取适当的处理措施是提高组播组性能的关键。我们将在以后的工作中进行更深入的研究。

参 考 文 献

1 Rizzo L. PGMCC: A TCP-friendly Single-Rate Multicast Congestion Control Scheme. ACM SIGCOMM '00, Aug. 2000

2 Widmer J, Handley M. Extending Equation-Based Congestion Control to Multicast Applications. ACM SIGCOMM'01, San Diego, Aug. 2001

3 Fu C P, Liew S C. TCP Veno: TCP Enhancement for Transmission Over Wireless Access Networks. IEEE Journal of Selected Areas in Communications, Feb. 2003

4 Fu C P. TCP Veno: End-to-end Congestion Control over Heterogeneous Networrks: [Ph. D dissertation]. July, 2001. http://www.broadband.ie.cuhk.edu.hk

5 Ayanoglu E, Paul S, LaPorta T F, et al. AIRMAIL: A link-layer protocol for wireless networks. ACM ACM/Baltzer Wireless Networks J, 1995(1): 47～60

6 Balakrishnan H, Seshan S, Katz R H. Improving reliable transport and handoff performance in cellular wireless networks. ACM Wireless Networks, 1995(1)

7 Mankin A, Romanow A, Bradner S, Paxson V. IETF criteria for evaluating reliable multicast transport and application protocols. RFC2357, June 1998

8 Padhye J, Firoiu V, Towsley D, Kurose J. Modeling TCP Throughput: A Simple Model and its Empirical Validation. In: Proc ACM SIGCOMM, 1998

9 苏晓丽，郑明春，李锦涛，孟强. 一种基于速率的组播拥塞控制算法及其性能分析. 电子学报，Feb. 2004. 330～334

10 VINT Project. Network Simulator version 2(ns-2). http://www.isi.edu/nsnam/ns