引入层次型 AAA 的移动 IPv6 安全认证和注册协议

王尚平[1],邹永杰[1,2],邹又姣[1],冉占军[1]

(1. 西安理工大学 密码理论与网络安全研究室,陕西 西安 710054;
2. 西京学院,陕西 西安 710123)

摘 要:针对移动 IPv6 和 AAA 的融合问题,从移动 IPv6 的切换性能和安全性方面考虑,通过优化 AAA 引入一种层次型 AAA 模型,提出了一种移动 IPv6 的安全认证和注册协议。协议通过层次化管理,大大减轻了移动 IPv6 节点的切换开销,经过分析,协议在保证传统安全要求的同时,也证明了其比 IETF 提出的方案具有更优秀的切换性能。

关键词:移动 IPv6;认证;注册;层次型 AAA

中图分类号:TN918.91;TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)08-0158-03

A Mobile IPv6 Security Authentication and Registration Protocol by Introducing a Hierarchical AAA

WANG Shang-ping[1], ZOU Yong-jie[1,2], ZOU You-jiao[1], RAN Zhan-jun[1]

(1. Lab. of Cryptography and Network Security, Xi'an Univ. of Tech., Xi'an 710054, China;
2. Xijing College, Xi'an 710123, China)

Abstract: In allusion to fuse mobile IPv6 and AAA, in this paper, consider the handoff performance and security of mobile IPv6, and propose a hierarchical AAA model in order to optimize AAA. An authentication and registration protocol for the mobile IPv6 is proposed. Via the hierarchical management, the handoff cost of the protocol is reduced greatly, by analyzing the protocol, it assures the traditional security, at the same time, it has better handoff performance than the scheme which is proposed by IETF.

Key words: mobile IPv6; authentication; registration; hierarchical AAA

0 引 言

IPv6 是解决现有的 IPv4 协议缺陷而提出的下一代互联网协议,下一代互联网的最大特点之一就是移动性。在移动网络中,使用一定的网络资源就必须支付相当的费用,为此,IETF 下成立一个专门机构,即 AAA 工作小组。AAA 代表认证(authentication)、授权(authorization)和计费(accounting),当移动节点(MN, Mobile Node)使用相关网络资源时就必须向 AAA 服务器提交请求服务的相关信息,经过 AAA 服务器认证后授权 MN 一定权限,并在 MN 使用服务时计费,因此 MN 使用移动资源需要结合 AAA 模型。目前,IETF 关于 AAA 方面的标准还在修改和完善之中,其提出的框架在安全和效率方面也缺乏考虑[1]。

当 MN 漫游到外部链路时需要向家乡链路注册自己当前的 IP 地址,如果 MN 频繁移动,MN 就会频繁向家乡链路注册当前的 IP 地址,这样频繁的切换影响 MN 的网络性能。为此,研究者提出了层次型的移动 IPv6 方案,该方案能帮助 MN 实现快速切换,免除了因频繁切换而降低网络性能,提高了 MN 的效率。

文中引入了层次型 AAA 模型,其具有与 HMIPv6 类似的功能,能帮助 MN 在频繁移动中降低和减少认证和注册时间。在综合考虑 MN 的安全和性能的情况下,提出了一种移动 IPv6 节点的认证和注册协议。

1 相关工作

1.1 MIPv6 及 HMIPv6 介绍

MIPv6 是 IPv6 互联网的一个 IP 层移动协议,其设计思想是,移动主机不论是在固定还是移动的情况下,不需要更改任何设置就能保持原有的通信。在 MIPv6 中,一个 MN 拥有两个 IP 地址[2]:一个是永久性的家乡地址(home address, HoA);另一个是临时的

收稿日期:2006-10-10

基金项目:国家自然科学基金资助项目(60273089);陕西省教育厅专项科学研究计划资助项目(06JK213);陕西省自然科学基础研究计划资助项目(2005F02)

作者简介:王尚平(1963-),男,陕西扶风人,教授,硕士研究生导师,研究方向为密码理论与网络安全。

转交地址(Care－of address, CoA)。当 MN 在家乡链路时,工作原理如固定节点一样,使用的是 HoA 地址。当 MN 离开家乡链路进入一个外部链路时,通过 IPv6 地址自动配置协议,MN 获取一个临时的 CoA 地址。此时,通信对端(CN, Correspond Node)与 MN 通信,由 CN 发给 MN 的数据包首先路由到 MN 的家乡地址上,MN 的家乡代理(home agent, HA) 通过代理机制截获这条消息,再将其转发到 MN 的 CoA 上,因此,当 MN 在外部链路时需要绑定 HoA 和 CoA 地址,发送绑定更新请求给 HA 告诉其当前的 CoA。

MN 在外部链路频繁移动和切换时需要不断地向 HA 发送绑定更新请求,这样影响了网络性能,为实现 MN 的快速切换,研究者提出了 HMIPv6 方案,该方案引入了一个新的实体称为移动锚点(MAP, Mobility Anchor Point),它可以是 HMIPv6 网络中的任何层次的路由器,充当了 MN 的本地 HA 的功能。MN 在 MAP 域内获得两个 CoA 地址,即区域转交地址(RCoA, Regional Care－of Address)和链路转交地址(LCoA, Linked Care－of Address),MN 使用 RCoA 作为当前 CoA,当 MN 在域内移动时不改变 RCoA,只改变 LCoA,MAP 收到 MN 的消息时转发到 MN 的当前地址 LCoA 上。MAP 的使用可以限制移动 IPv6 同本地域以外的节点的信令交互,它支持快速移动 IP 切换,帮助移动主机实现无缝移动,节约了向家乡进行登记所需的开销。

1.2　AAA 及层次型 AAA 介绍

MN 在接入网络时,尤其是移动到外地链路时,需要对其身份进行认证[3],并确认它可以使用的网络资源。而 MIPv6 本身没有提供对 MN 身份认证以及授权,更没有对记录资源使用状况等问题进行考虑。而这些对于移动互联网络的正常运营,尤其对于网络服务提供商来说,是不可或缺的基础设施,AAA 实现网络认证、授权、计费功能[4]。对于移动环境下,AAA 机制需要 MN 所属的家乡网络的参与,因为 MN 的信息是保存在它的家乡服务器的。同时如果是在不同的服务提供商之间的移动,服务提供商之间对于资源提供、费用分摊等问题需要协商。当一个 MN 移动到外部网络请求使用相关网络资源时向外地 AAA 服务器(AAAF)提交自己的网络访问标识符(NAI, network access identify),AAAF 没有 MN 相关的信息,将请求提交给 MN 的家乡 AAA 服务器(AAAH)来进行认证,AAAH 进行认证后再将一个经过认证的消息返回给 AAAF。

层次型 AAA 的功能类似 HMIPv6,它在一个区域内增加了一个根 AAA 服务器(记为 RAAA),除了 RAAA 和最底层的 AAA 服务器外,每个 AAA 服务器有上级和下级 AAA 服务器,这些服务器管理自己域内的所有 AAA 服务器,当 MN 请求服务时,相关信息首先传给 AAAF,再由 AAAF 逐层向上级传给 RAAA,最后由 RAAA 逐层向下级传给 AAAH,增加层次型 AAA 的优点是,当 MN 在外部链路从一个外地 AAA 服务器域内漫游到另一个外地 AAA 服务器内时(都在同一个上级 AAA 管理域内),MN 不需要向另一个外地 AAA 服务器请求认证,只需要上级 AAA 将相关信息提交给另一个外地 AAA 服务器即可,这样减少了 MN 的认证时间,优化了网路性能。

2　新的协议

2.1　协议主要目标

本方案主要目的是在 MN 移动到一个外地链路后,能够安全注册其新的转交地址,并保证其敏感信息的安全传输。同时,MN 还需要进行相应的认证和注册以后才能访问所需的资源,保证计费的准确性。综合考虑 MN 的安全、效率以及移动设备的计算和能耗局限性等问题,具体目标[5]如下:

(1)保护 MN 的 NAI 信息和 CoA 的完整性,防止假冒攻击;

(2)保证 MN 的 NAI 信息和 CoA 消息传输的新鲜性,防止重放攻击;

(3)MN 身份认证,其中 MN 的身份从其 HoA 和 NAI 加以绑定来进行标识;

(4)AAAH 到 AAAF 之间传输的 MN 账户信息的机密性与完整性,防止窃听和假冒攻击;

(5)改进 MN 在 AAA 上的认证和注册效率。

2.2　协议说明

为了后面使用方便,定义如下的相关概念:

(1)REG:注册请求消息;

(2)REP:注册应答消息;

(3) $H_k(\cdots)$:带密钥的消息认证码 MAC 函数;

(4)DR:默认路由器,通常是 MN 在外部链路时接入的路由器;

(5)$\{\cdots\}K$:公钥加解密运算;

(6)N_X:实体 X 产生的随机数,用于消息的新鲜性保护;

(7)PK_X:实体 X 的公钥;

(8)R′AAA:离 AAAF 和 AAAH 最近的上级节点;

(9)SK_X:实体 X 的私钥;

(10)ACK_X:实体 X 返回的注册成功确认消息;

(11)$INFO_{MN}$:移动结点 MN 的详细账户信息。

2.3 协议过程

新方案的协议过程如下：

(1) MN → DR → AAAF → … → R′ AAA: REG, $H_{KMN-AAAH}$(REG), REG = {HoA, LCoA, RCoA, NAI, N_{MN}};

(2) R′ AAA → MAP: {BU_{MAP}} PK_{MAP}, BU_{MAP} = {HoA, LCoA, RCoA, NAI, N_{MN}, N_R};

(3) MAP → R′ AAA: {BU_{MAPACK}} PK_{RAAA}, BU_{MAPACK} = {HoA, LCoA, RCoA, NAI, N_{MN}, N_R, ACK_{MAP}};

(4) R′ AAA → … → AAAH: REG, {$H_{KMN-AAAH}$(REG), N_{RAAA}} SK_{AAAF};

(5) AAAH → HA: {REG} PK_{HA};

(6) HA → AAAH: {REP} PK_{AAAH}, REP = {HoA, LCoA, RCoA, N_{MN}, NAI, ACK_{HA}};

(7) AAAH → … → R′ AAA: REP, {$H_{KMN-AAAH}$(REP), $INFO_{MN}$, N_{AAAF}} SK_{AAAH};

(8) R′ AAA → … → AAAF: REP, $H_{KMN-AAAH}$(REP), $INFO_{MN}$;

(9) AAAF → DR → MN: REP, $H_{KMN-AAAH}$(REP)。

当 MN 收到 DR 发出的路由通告并获取 CoA 后，向 DR 提交注册请求消息 REG，消息中包含了 MN 的家乡地址 HoA，链路转交地址 LCoA，区域转交地址 RCoA，网络访问标识符 NAI 及一次性随机数 N_{MN}。DR 没有能力验证 MN 的身份和注册消息，随后将其转发给 AAAF。AAAF 收到 DR 转发的请求消息后，也没有能力执行 MN 的身份和注册消息，因此，AAAF 继续将 MN 的请求消息逐层转发给 R′AAA。

R′AAA 收到 AAAF 提交的消息后，解析其中内容，并把 HoA，LCoA ，RCoA 和 R′AAA 的一次性随机数 N_R 发给 MAP。

MAP 收到 RAAA 的消息后，进行确认，如果成功，返回一个确认消息。否则，返回一个请求失败的消息。

如果 R′AAA 收到 MAP 的确认消息后，立即给 AAAH 提交 MN 的注册请求消息 REG，同时将其一次性随机数 N_R 加入到 MAC 消息中，并用自己的私钥加密。

AAAH 在收到 R′AAA 的消息后，查看 REG 里面的注册消息，同时用 R′AAA 的公钥解密 MAC，得到 MAC 和 R′AAA 的一次性随机数 N_R，再用 MN 和自己的共享密钥 $K_{MN-AAAH}$验证 MAC。

如果 AAAH 验证 MAC 成功，AAAH 把 MN 的注册请求消息 REG 经过 HA 的公钥加密发送给 HA。HA 用私钥打开 AAAH 发送的消息，得到 MN 的注册请求消息 REG。

MN 的注册请求消息成功后，HA 回复 MN，发送一个 REP 应答，REP 中包含了 HoA，LCoA，RCoA，NAI，ACK_{HA}。

AAAH 收到 MN 的应答后，得到 REP，AAAH 用自己与 MN 的共享密钥得到 REP 的消息验证代码 MAC，再把 MAC 和 RAAA 的一次性随机数 N_R 用私钥加密发送给 R′AAA。

R′AAA 收到 AAAH 的消息后，得到 REP，并用 AAAH 的公钥打开得到 R′AAA 的一次性随机数 N_R，验证成功。R′AAA 再把 REP，以及 $H_{KMN-AAAH}$(REP, N_{MN})发送给 AAAF。AAAF 收到 RAAAS 的消息后也确认了 MN 的身份。AAAF 再将 REP，以及 $H_{KMN-AAAH}$(REP, N_{MN})发送给 DR。DR 收到 AAAF 的消息后将其转发给 MN。MN 收到消息后，得到 REP，同时用与 AAAH 的共享密钥验证 MAC。验证成功即注册请求消息完成。

3 协议分析

3.1 协议安全性分析

(1) 实体间的身份认证。

在建立协议之前，相关的安全关联已经建立，如 DR 与 AAAF，AAAF 与 R′AAA，R′AAA 与 AAAH，AAAH 与 HA，它们之间的相互认证可以通过加解密运算来认证。当然 R′AAAS 与 MAP 的安全关联也要事先建立。MN 在离开家乡链路时与 AAAH 协商出共享密钥。

由于建立安全关联，MN 帐户信息在传递过程中始终处在安全的隧道中，其身份认证是 AAAF 借助 AAAH 来实现的。

(2)消息的完整性保护。

完整性保护的消息包括注册请求消息、注册应答消息和 MN 的详细账户信息。从 MN 到 AAAH 之间传输的注册请求消息通过 MN 与 AAAH 之间的共享密钥保护；从 AAAH 到 MN 之间传输的注册应答消息也通过 MN 与 AAAH 之间的共享密钥保护；AAAH 到 AAAF 之间传输的 MN 的详细账户信息通过 AAAH 公私钥加解密运算实现了保护。

(3)消息的新鲜性保证。

对消息的新鲜性采用了双重保护机制。整个传输过程中注册消息的新鲜性保护通过 MN 初始产生的随机数 N_{MN}实现，AAAF 到 AAAH 之间传输消息的新鲜性保护通过 R′AAA 产生的随机数 N_R 实现。

3.2 协议性能分析

本协议与 IETF 提出的方案相比较，因为增加了 AAA 服务器和 MAP 以及加解密运算，在这方面的

(下转第 172 页)

2.3 数据挖掘和数据分析

在 MS SQL Server2000 提供的 Analysis Manager 工具中,包含了两种用于数据挖掘 DM(Data Mining)的数学模型,即决策树模型和聚类分析模型,根据分析需求可选择不同模型。如本系统以创建的多维数据集为基础,建立了基于决策树的数据挖掘模型,以帮助决策者寻找数据间潜在的关联,发现被忽略的要素。

数据分析以 MS SQL Server2000 Analysis Services 的数据透视表服务,即 PivotTable Service 为接口,通过 Microsoft Excel 组件以及客户端应用程序和 ADO 对象模型连接到多维立方体,并进行数据分析,将数据呈现在用户面前。

2.4 客户端的开发

C/S 模式下数据库应用系统的客户端软件开发工具有许多种,文中选择 PowerBuilder9.0 作为客户端应用程序的开发工具。在程序设计过程中,主要采用了 PB9.0 的基于视图的数据窗口技术。建立与 MS SQL Server2000 数据仓库相对应 ODBC 数据源,利用数据库描述文件可方便各个数据库连接之间的切换。PB 专门为这种操作提供了数据窗口对象,利用数据窗口与数据库通信既高效又方便。通过数据窗口,可以很方便地操作数据库,不但可以对每个数据库表进行检索、查询、插入、删除和更新,还可以为数据指定输入格式、输出格式和显示风格等等。另外,在数据窗口中,还可以添加各种对象。数据窗口既是数据库操作工具,又是界面的重要组成部分[7]。

3 结 论

面向高校后勤集团的财务与物流管理,利用现代的信息技术,将会计信息系统嵌入物流业务执行处理过程中,设计开发了基于 C/S 模式的业务事件驱动型财务与物流管理一体化的信息系统,使物流业务处理系统和会计信息系统相辅相成,构成了功能较为全面而灵活的管理信息系统,为高校后勤管理及决策提供了有效的系统支持。

参考文献:

[1] 江其玟.基于数据仓库的业务事件驱动型会计信息系统研究[J].审计与经济研究,2004(5):35-38.

[2] 陈 翔.会计信息系统的新发展——业务事件驱动[J].四川会计,2002(9):25-27.

[3] 黄梯云.管理信息系统[M].北京:高等教育出版社,2001.

[4] 蔡淑琴.物流信息系统[M].北京:中国物资出版社,2002.

[5] 陈文伟.决策支持系统及其开发[M].北京:清华大学出版社,2001.

[6] 康博创作室.数据仓库设计和使用指南[M].北京:清华大学出版社,2001.

[7] 朱爱民.Powerbuilder8.0 编程实用技术与案例[M].北京:清华大学出版社,2002.

(上接第 160 页)

开销要比以前大,但是本协议有优秀的切换性能,协议在开始运行阶段相对而言要慢一点,但是一旦协议运行后,其切换速度非常快,主要原因有以下几个方面:

(1)据法国 INRIA 公司的研究表明[1]:在通常的移动中,有 69% 的移动是在一个域内发生的。因此,针对 AAA 实体的分布,提出层次化的 AAA 架构,同时利用建立短期外地安全关联和上下文转移技术,提高了系统的性能。MN 离开 AAAF 域内进入另一个 AAAF 域内(在 R′AAA 域内)时不需要再向 HA 注册 CoA,只需 R′AAA 把 MN 相关信息提交给另一个 AAAF 即可,这样其切换速度大大增加。

(2)协议中虽然运用了加解密运算,但可以随其保密程度的高低,调整密钥强度,这样也可以提高协议的效率。研究表明:MN 移动越频繁,其优秀性能越能体现。

4 总 结

层次型移动 IPv6 能够帮助 MN 实行快速切换,同样,层次型 AAA 也能帮助 MN 实行快速注册。文中通过结合这两种方案提出一种移动 IPv6 的安全认证和注册协议,经过分析,在实体的身份认证、消息的完整性保护和消息的新鲜性上保证了传统安全性,在协议的切换性上保证了优秀的性能。

参考文献:

[1] 肖文曙,张玉军,李忠诚.移动 IPv6 网络的层次 AAA 方案研究[J].通信学报,2006,27(2):50-55.

[2] Perkins C. IP Mobility Support[EB/OL].1996-10.http://www.ietf.org/rfc/rfc2002.txt? number=2002.

[3] Farrel S, Vollbrecht J, Cahoun P, et al. AAA Authorization Requirements[EB/OL]. 2000 - 08. http://www.ietf.org/rfc/rfc2906.txt? number=2906.

[4] Glass S, Hiller T, Jacobs S, et al. Mobile IP Authentication, Authorization, and Accouting Requirements[EB/OL].2000-10.http://www.ietf.org/rfc/rfc2977.txt? number=2977.

[5] 刘东苏,王新梅.引入 AAA 模型的移动 IP 安全认证和注册协议[J].网络安全技术与应用,2006(4):91-92.