基于分层身份的电子政务网格认证模型研究*)

于代荣[1,2] 杨 扬[1] 马炳先[2] 熊曾刚[1] 曾 明[1]
(北京科技大学信息工程学院 北京 100083)[1] (济南大学信息科学与工程学院 济南 250022)[2]

摘 要 在网格环境中,PKI公钥管理方式对GSI认证效率产生一定的制约,而基于IBC的认证机制轻量、高效,密钥管理较为简便,改进了TLS握手协议,在此基础上提出一种适用于电子政务网格的基于HIBC的认证模型HIAM(Hierarchical ID-based Authentication Model),该模型克服了基于PKI的证书认证机制效率方面的缺点,通过与GSI的结合,重用GSI提供的安全服务,同时便于部署。

关键词 GSI(Grid Security Infrastructure),HIBC(Hierarchical ID-based cryptography),IBC(ID-based cryptography),认证模型,电子政务网格

Research on Hierarchical ID-based E-government Grid Authentication Model

YU Dai-rong[1,2] YANG Yang[1] MA Bing-xian[2] XIONG Zeng-gang[1] ZENG Ming[1]
(School of Information Engineering ,University of Science and Technology Beijing,Beijing 100083,China)[1]
(School of Information and Science Engineering,Jinan University,Jinan 250022,China)[2]

Abstract In grid environment, the authentication efficiency of GSI is restricted by the key management methods of PKI. IBC-based authentication mechanism is lightweight, efficient and of more convenient key management. Therefore, this paper improved TLS handshake protocol and proposed a model named HIAM (Hierarchical ID-based Authentication Model) based on HIBC. HIAM overcame the efficiency drawback of PKI-based authentication mechanism, combined with security service of GSI, and was feasible to deploy.

Keywords GSI (Grid Security Infrastructure), HIBC (Hierarchical ID-based cryptography), IBC (ID-based cryptography), Authentication model, e-government gird

1 引言

网格是"在动态变化的、多机构的虚拟组织间共享资源和协同解决问题"[1],其目标是实现资源的全面共享。通过构建电子政务网格,政府可以充分利用现有各部门资源,极大地减少重复投资,实现网络虚拟环境下的资源共享和协同工作。网格中动态的、可扩展的分布式虚拟组织和动态的、跨组织的资源共享与协作,对系统和资源的有效控制提出了新的安全挑战。

认证与授权是电子政务网格安全中的首要环节。网格资源的分布性以及网格用户请求的动态性和频发性,决定了网格认证应满足以下要求[2]:跨信任域互认证,单点登录,委托等。GSI[2]基于PKI,是Globus Tookit(简称GT)中解决网格安全问题的集成解决方案,但PKI系统的建设和维护成本高,同时导致证书链处理和证书传递的沉重开销。通过IBC[4,5]/HIBC[6]实现身份认证是一种新型认证机制,它的特点是私钥由密钥生成中心产生,以用户的ID为用户的公钥,无需证书绑定公钥和身份,也不需要专门的目录来存放证书;认证机制简单、高效,大大减轻了密钥管理的负担,并可避免证书链处理和证书传递的开销。沈昌祥院士认为,IBC的密钥集中式管理模式适用于从属关系确定的信任体系[3]。参与电子政务网格的主体大多与机关事务处理相关,其上下级关系明确,角色确定,信息流向有序,应用边界清晰,因而IBC与电子政务网格有着天然的亲和性。把基于IBC的认证机制应用在电子政务网格认证之中,将大大提高认证效率。

2 GSI安全认证存在的问题

GSI是GT的安全组件,在当前网格部署中占主导地位。GSI基于PKI,通过TLS协议实现网格通信主体之间的认证和消息保护,使用代理和委托机制实现了网格计算环境中的安全单点登录,包括跨多个资源和地点的身份互认证、信任委托和信任转移等。用户如果没有创建代理,就不能提交作业,也不能传输数据。认证过程中,通讯双方同时协商一个会话密钥,通过这个会话密钥建立安全信道。互认证成功后,用户将通过代理进行委托授权以提交作业;GSI使用一个映射文件将实体的全局身份映射为本地帐号,网格用户的作业转由这个本地帐号根据自己的权限处理。

GSI认证过程中的证书链验证和证书传递需要相当大的开销。以网格环境中用户U提交作业的一个简单场景为例,U将作业委托给gatekeeper(简称GK);在作业执行前,GK和资源R要使用TLS握手协议进行相互认证,GK必须向R传递证书链包含的所有证书,包括U的证书、U的代理证书、GK的证书、GK委托给R的代理证书(包含U的代理私钥签名)等4个证书,并且资源R必须查询每个证书状态和有效

*)基金项目:国家自然科学基金重大研究计划重点项目(No. 90412012),国家自然科学基金面上项目(No. 60673160),济南大学博士科研启动基金(No. B0626)。于代荣 讲师,博士研究生,研究方向为计算机网络和网格安全;杨 扬 教授,博士生导师,研究方向为计算机网络和图像处理。

性并验证证书链。同样资源 R 也必须向 GK 发送自己的证书，以实现互认证。而通常网格环境中一个大作业往往需要很多资源层层委托，协作完成，因而实际的证书处理开销要大得多，导致 GSI 认证结构的滞重、低效。

可见，PKI 的公钥和证书管理技术是形成制约 GSI 认证效率制约的瓶颈所在。此外，PKI 的证书分发以及密钥管理的其他方面也都带来不小的负担。因此，需要研究新的理论和方法解决问题。

3 分层的基于身份的加密和签名

基于分层身份的加密和签名体制(HIBC)[6]是对 IBC 的一种扩展，在 IBC/HIBC 中，公钥直接由用户身份信息充当，因此不存在公钥的管理和认证问题，也就没有了密钥产生、分发和 CA 管理等问题，这大大减少了系统的代价和复杂度。相比 PKI，IBC/HIBC 在密钥管理与认证等诸多方面有着明显的优势。而 HIBC 方案减轻了 PKG 的负担，同时增强了安全性。

文献[6]提出 HIBC 方案中，公钥可以是任意的一个字符串，在其基于分层身份的签名中，身份 ID 利用向量来表示，一个 j 元向量代表一个第 j 层的用户，而系统的主密钥看作是位于第 0 层用户的私钥。签名协议由 4 个算法组成，即系统初始化、密钥产生、签名和验证算法。

(1)系统初始化算法：输入安全参数 k 和系统分层层数(深度)l，输出整个系统的公开参数以及系统主密钥 sk；

(2)密钥生成算法：给定第 j 层用户身份 $ID=(ID_1,\cdots,ID_j)$和第 $j-1$ 层用户 $ID'=(ID_1,\cdots,ID_{j-1})$的私钥 $d_{ID'}$；输出用户 ID 的私钥 d_{ID}；

(3)签名算法：给定明文 M 和接收者的身份信息 ID 以及私钥 d_{ID}，产生相应的签名；

(4)验证算法：给定签名和用户身份，如果它是一个有效签名，输出 1，否则输出 0。

HIBC 的用户密钥生成示意如图 1 所示。密钥生成算法中，通过引入一个私密变量 s，其中每一层中 ID 对应的私钥可以由上一层父节点生成，而非父结点其任意祖先节点均无法生成。即某节点只能计算出其直接子节点的私钥，而所有其他子孙节点的私钥无法计算得出来，或者说是计算困难的。

HIBC 隶属公钥密码体系，其安全性依赖于密码学领域的两个著名难题，即计算离散对数问题和双线性 Diffie-Hellman 指数问题。

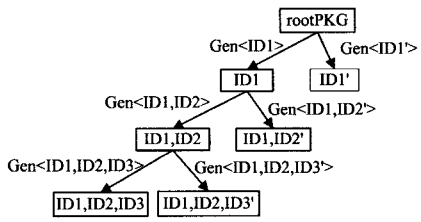

图 1 HIBC 的用户密钥生成示意图

4 对 TLS 握手协议的改进

一个 TLS[7]传输过程需要先握手，用公钥加密算法使服务器端和客户端相互验证，验证成功后产生一个会话密钥，随后使用这个会话密钥和对称密钥算法在通信中快速地加密、解密数据。在每次 TLS 会话中服务器都完成一次使用服务器专有密钥的操作和一次使用客户公开密钥的操作。握手协议流程如图 2 所示。由于网格环境中的实体要求互认证，所以图中未列出 TLS 握手协议中提供的无证书情形下的可选操作。

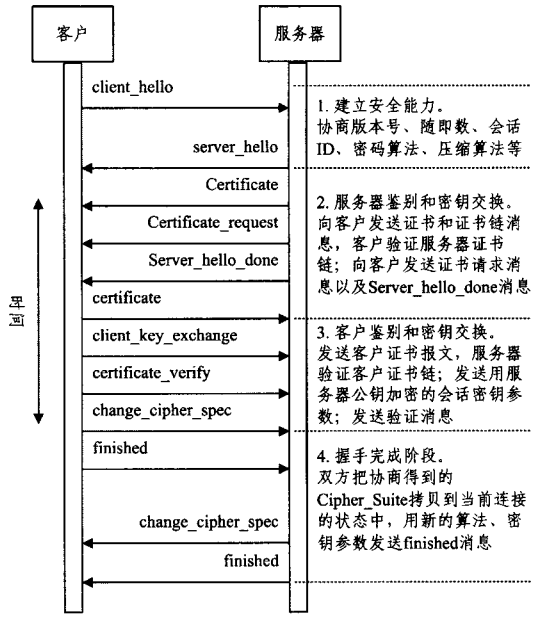

图 2 TLS 握手协议流程图

为了将 HIBC 的算法运用于 TLS 协议中，必须对 TLS 握手协议进行改进，使得改进的 TLS 协议支持 HIBC 算法。结合基于身份的加密和签名算法的特点，改进的方法具体如下：

(1) 在 TLS 中增加相应的加密套件：CipherSuite TLS_HIBC_WITH_3DES_CBC_SHA。该加密套件定义了使用 HIBC 和 HIBS 进行加密和认证，以及使用 3DES-CBC 的对称加密算法和 SHA 压缩算法。

(2) 使用身份标识代替证书公钥，相应地，有关证书的发送操作改为身份标识发送，如用户 U 可用其标识 u@163.com 作为公钥。

(3) 原握手协议的操作序列中有关公钥的验证操作取消。

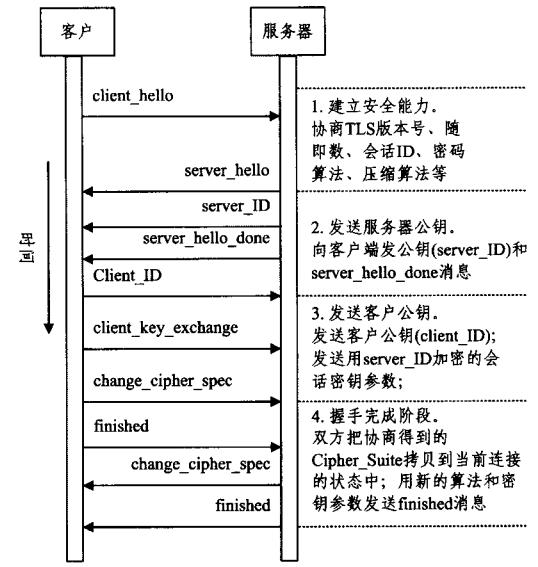

图 3 改进的 TLS 握手协议流程图

根据上述改进方法，得到改进的 TLS 握手协议工作流程，如图 3 所示。从对认证效率的提升看，改进的 TLS 握手

协议具有以下3方面的优点：

(1) 直接使用用户标识作为公钥，而无需验证公钥，从而避免了繁重的证书处理开销，这将大幅提高认证效率；

(2) 发送身份ID作为公钥进行认证而非发送证书，由于身份ID的大小比X.509证书要小得多，因而身份信息发送的开销大大减少；

(3)发送的消息数目由原来的12个减少到10个，从而交换的信息量有所减少，协议的复杂度降低。

因此，通过改进TLS握手协议，引入实体标识代替数字证书，能够更轻量、高效地完成认证过程与委托过程，同时建立起安全信道。

5 基于分层身份的电子政务网格认证模型(HIAM)

根据HIBC的概念，提出一种基于分层身份的电子政务网格认证模型HIAM，模型将GSI结构进行适当的修改，然后将HIBC与GSI相结合，从而即能重用GT中的GSI提供的安全服务，又利用了基于身份认证的轻量、高效的优势，而且提供了良好的扩展性。

5.1 HIAM在单信任域的认证及实现

在HIAM模型中，用网格身份权威GIA(Grid Identity Authority)代替基于PKI的GSI结构中的CA，GIA的作用相当于IBC中的PKG。用户需要在GIA注册，由GIA根据其ID为其生成私钥。为满足GSI中作业安全提交的要求，必须使用代理的方法，以实现网格服务间相互的认证和委托。

一个基本的HIAM结构包含了网格环境的层次化的多种实体如图4所示，其中GIA在0层，用户/资源在1层，用户代理/资源代理在2层。该模型中，各层实体的公钥为其身份标识，0层实体GIA为1层实体用户/资源分发长期私钥，1层实体为其代理产生短期私钥。下面通过一个场景来解释该模型的工作过程。

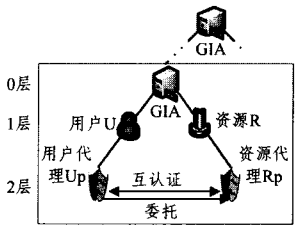

图4 HIAM工作原理

假设用户U要向资源R提交一个作业请求，为了简化过程，这里假定U可以直接和R进行安全通信，实际的过程是通过GK进行的。借助上述改进的TLS握手协议，其功能实现如下：

(1) 单点登录：用户U生成其代理的公钥/私钥对，通过该代理，在用户U的长期公钥/私钥对过期之前，U不必重复签名，而由其代理代其完成委托与授权过程，从而实现单点登录的功能。

(2) 授权：U通过其代理的基于身份的代理私钥签名作业请求后，将该签名的作业请求提交到R端，R端可以通过获得系统的IBC参数方便地验证该作业请求中的签名，并将U的身份标识映射到本地网格身份文件中，接着为该作业请求实例化一个网格服务，并向U返回一个端点引用。

(3) 相互认证和密钥协商：作业开始之前，U先完成与新创建的网格服务之间的相互认证，U必须确信他将作业提交到了一个合法的主机和帐户，而主机也必须检查U是否就是其所声称的身份。在GSI中，这个过程通过标准的TLS通信协议来完成，这里可用支持分层身份认证的改进的TLS握手协议完成握手过程，进行互认证，并建立起安全信道。

(4) 委托：由于U的代理在模型中处于第2层，他可通过其代理向R发送代理的身份公钥，把R看成U层次下的第3层实体，从而授权R代表U的代理执行作业，并可绑定U的授权策略。与(3)中过程相似，该过程可借助改进的TLS协议来完成。

在HIMA模型中，一个域内的作业提交和运行场景包括四个基本步骤，即基于身份的认证、委托、服务查找、运行服务程序。如图5所示。

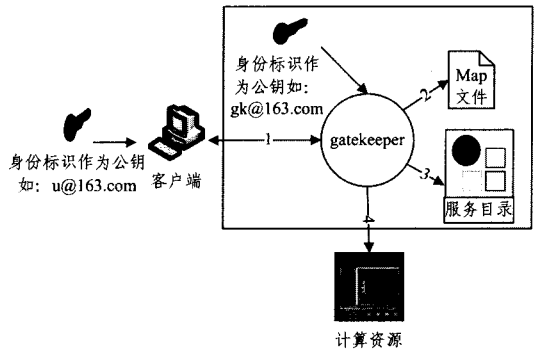

图5 HIMA域内作业的提交与运行场景

5.2 HIAM跨信任域认证及实现

在网格环境下双方主体如果都拥有基于身份的公钥，则可通过相互认证以确定彼此的身份，双方可采用改进的SSL协议作为互认证协议。而各个域的GIA可按图1的形式进行组织。下面通过构造一个网格作业提交场景，来说明HIAM的跨信任域认证方法及实现。假设存在三个信任域：域A、域B和域C，域A的用户U互认证的过程如图6所示。

由图6可知，认证过程为：

(1) 使用基于身份的公钥/私钥对，通过改进的TLS握手协议，用户U通过Gloobus客户端的GRAM与域A的GK完成互认证。

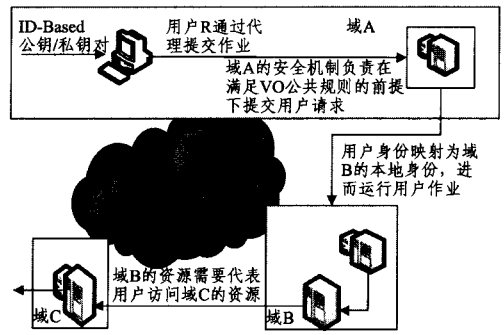

图6 HIAM跨域认证方法及实现

(2) GK检查gridmap文件，将用户身份映射为本地帐号；然后U通过其的代理对域A的GK的代理身份签名，完成委托过程。每次访问新的资源之前，域A的GK都出示该签名，以证明它是在代表U执行作业。

(3) 根据作业描述，域A的GK通过服务查找，确定可运

(下转第61页)

信源发送到信宿过程中因路由发现或路由维护等产生的路由数据包个数与传输的数据包个数之比，用以反映路由协议产生的负载。MODVWLS 和 AODV 协议的标准化路由负载如图 5,6 所示。从图中可看出，虽然 MODVWLS 协议需计算和存储路径上各链路的权重，增加了路由节点负载，但由于在路由请求和路由响应过程中都考虑了链路权值，且在路由发现过程同时进行了反向和正向路径选择，在一定程度上降低了协议的路由负载，从而使得 MODVWLS 协议的路由负载略优于 ADOV 协议。

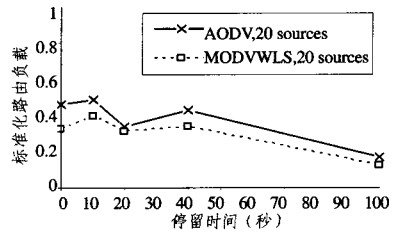

图 5　标准化路由负载对比(20 数据源)

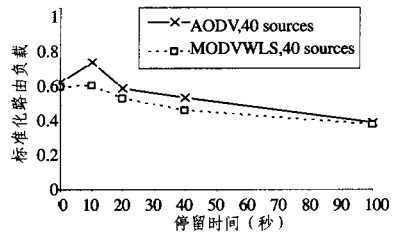

图 6　标准化路由负载对比(40 数据源)

结束语　MODVWLS 协议采用了反映链路和节点负载的累计路径权重作为路由评价标准，在权重相同的情况下，选择跳数较少的路径进行路由，同时采用节点过载报警机制，在一定程度上实现了网络负载动态均衡，提高了网络吞吐性能。实验结果表明，MODVWLS 协议在数据包转发率、端到端延迟和路由负载性能等方面都要优于广泛应用的 AODV 协议，并随着网络拓扑的动态变化，其性能变化也较为平稳。可见 MODVLS 协议能较好地适用于无线网状网。

虽然 MODVWLS 协议在一定程度上改进了 AODV 路由协议，但由于 802.11 MAC 采用分布式协调功能机制，我们仍不能充分地利用标准规定的理论带宽。因此，下一步工作重点研究如何将 MODVWLS 协议扩展到多个信道上，通过为每个无线路由节点设置至少两块网卡，并利用一定的策略将每块网卡分配到不同的信道上，以降低节点之间的冲突，从而进一步提高网络性能。

参 考 文 献

[1] Woo A, Tong T, Culler D. Taming the underlying challenges of reliable multi-ho Prouting in sensor networks[J]// SenSys. 2003

[2] Awerbuch B, Holmer D, Rubens H. High throughput route selection in multi-rate ad hoc wireless networks[J]. Technical report. Johns Hopkins University, 2003

[3] Hu Y-C, Johnson D B. Design and demonstration of live audio and video over multi-ho Pwireless networks[J]// MILCOM. 2002

[4] Draves R, Padhye J, Zill B. Routing in Multi-Radio, Multi-HoP Wireless Mesh Networks[J]// ACM Annual Int'l. Conf. Mobile Comp. and Net. (MOBICOM). 2004:114-128

[5] Raniwala A, Chiueh T. Archietcture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network[J]. IEEE Magazine, 2005

[6] Tao Xiaojing, Kunz T, Falconer D. Traffic Balancing in Wireless MESH Networks[C]// International Conference on Wireless Networks, Communications and Mobile Computing. 2005

[7] Cali F, Conti M, Gregori E. IEEE 802.11 Wireless LAN-Capacity Analysis and Protocol Enhancement[C]. IEEE Magazine, 1998

[8] Wu Haitao, Cheng Shiduan, Peng Yong. IEEE 802.11 Distributed Coordination Function (DCF) Analysis and Enhancement [C]. IEEE Magazine, 2002

[9] Lu ke, Berndt K. A Quick Guide to AODV Routing[M]. Wireless Communications Technologies Group, 2004

[10] Jones E. Basic 802.11 Statistics[J]. Evan Jones' Scratch Pad, 2004

(上接第 57 页)

行 U 的作业的资源，比如找到域 B 的某资源适合运行 U 的作业；在运行作业之前，域 A 的 GK 需要和域 B 的主机进行互认证，其过程与步骤(1)、(2)相同。

(4) 运行服务程序，完成作业。作业完成后，域 A 的 GK 会将结果返回给 U。

(5) 通常，作业运行过程中可能需要访问新的资源，如域 B 的运行程序需访问域 C 的资源，这需要进一步进行委托，其过程同前。

通过改进 GSI 中的 TLS 握手协议，避免了证书处理的繁重开销。提出的 HIAM 模型集成了 GSI 和 HIBC 两者的优势，克服了传统的 PKI 证书体制下认证环节繁琐、效率较低的弊端，又使得方案便于部署。相比传统的 PKI 认证方案，这种方案更轻量、更高效。

结束语　本文在改进 TLS 握手协议的基础上，提出了基于分层身份的 HIAM 模型，并应用在电子政务网格中。由于 IBC 与电子政务网格的天然亲和性，HIAM 模型在现实电子政务网格部署中有良好的应用前景。目前该方案存在的不足是密钥第三方托管问题，还需要进一步研究解决。

参 考 文 献

[1] Foster I, Kesselman C, Tuecke S. The anatomy of the grid: enabling scalable virtual organizations[J]. International Journal on Supercomputer Applications, 2001, 15(3): 200-222

[2] Foster I, Kesselman C, Tsudik G, et al. A Security Architecture for Computational Grids[C]// Proceedings of the 5th ACM Conference on Computer and Communications Security. 1998: 83-92

[3] 沈昌祥. 网络信任与公钥认证[J]. 电子商务, 2006(3): 58-64

[4] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of the Cryptology-Crypto' 84. 1984: 47-53

[5] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C]// Proceedings of the Cryptology-Crypto 2001. 2001: 213-229

[6] Gentry C, Silverberg A. Hierarchical ID-based cryptography[C] // Proceedings of Asiacrypt 2002. LNCS 2501. Berlin: Springer-Verlag, 2002: 548-566

[7] Dierks T, Allen C. The TLS Protocol Version 1.0 [S]. RFC 2246, January 1999