Diffie-Hellman 密钥交换技术综述

余海冰　潘泽宏
(广东轻工职业技术学院　广东　广州　510300)

摘要：本文主要介绍密钥交换技术的形成，理论及其应用。分析了 Diffie-Hellman 密钥交换协议以及其延伸产物动态多方 Diffie-Hellman 密钥交换协议。同时对此协议的性能作了比较详细的分析，最后给出他们的应用。

关键词：密钥交换；iffie-Hellman 协议；算法

Review of Diffie-Hellman key Exchange Technology Yu hai bing　Pan ze hong

Abstract: This paper mainly introduces the forming of Key exchange, theory and application. Analyze Diffie-Hellman key exchange Protocol and their extend trends many kinds of Diffie-Hellman key exchange Protocols. Make a more detailed analysis to the performance of these Protocols at the same time, provide their application finally.

Key word: Key exchange; Diffie-Hellman Protocol; Algorithm

一、Diffie-Hellman 协议介绍

第一个发表的公开密钥算法出现在 Diffie 和 Hellman 的论文“New Directions in Crytography”[1]中，这篇论文定义了公开密钥密码编码学，而这种算法就是通常被称为 Diffie-Hellman 密钥交换。Diffie-Hellman 密钥交换算法可以让 A、B 双方在一公用网络上传输敏感数据。传输的双方各持有一个公钥和私钥，双方共享一个会话密钥，并以此来传输敏感数据。这样，除了 A 和 B 之外的其他人都无法知道会话密钥，由此可知，敏感数据的安全性得以保证。下面是 Diffie-Hellman 协议算法的描述：

公开信息：素数 p,q,q|p-1,g 为 q 在 Z^*_p 中的阶。

步骤一：发起方 P_i，接到输入(P_i,P_j,s)，随机选择 $x \xleftarrow{R} Z_q$，并发送信息(P_i,s,$\alpha=g^x$)到 P_j。

步骤二：接收方 P_j 收到(P_i,s,α),随机选择 $y \xleftarrow{R} Z_q$，并发送信息(P_j,s,$\beta=g^y$)到 P_i，删去 y，输出会话 s 的会话密钥 $\gamma=\alpha^y$

步骤三：收到(Pj,s,β)，Pi 计算出 $\gamma'=\beta^x$,删去 x,同时输出会话 s 的会话密钥 γ'

然而此协议是在传输安全性可以保证的网络中使用，亦即攻击者只能按照发送方的原信息发送到目的地，而不能修改或增删任何信息。如果我们要在一个传输安全性不能保证的网络中使用，也就是攻击方可以监听所有传送的信息，并随意增加或删除甚至拒绝发送的信息。在此情况下，我们派生出签名的 Diffie-Hellman 协议。下面是签名的 Diffie-Hellman 协议算法的描述：

初始信息：素数 p, q, q|p-1,g 在 Z_p^* 中的阶为 q，每个成员拥有一个私有密钥以进行签名算法 SIG，他们都拥有其他成员的公开密钥以验证数字签名。

步骤一：发起方 P_i，接到输入(P_i,P_j,s),随机选择 $x \xleftarrow{R} Z_q$，并发送(P_i,s,$\alpha=g^x$)到 P_j。

步骤二：收到(Pi,s,α)，P_j 随机选择 $y \xleftarrow{R} Z_q$，并发送(P_j,s,$\beta=g^y$)到 P_j，并同时附上其数字签名(Pj,s,β,α,P_i)，同时计算出会话密钥 $\gamma=\alpha^y$，同时删除 y。

步骤三：P_i 收到(Pi,s,β)以及其签名，同时验证签名的正确性，包括成员，会话编号，以及其数值，如果验证成功，P_i 发送(Pi,s,SIG_i(P_i,s,α,β,P_j))并同时算出 $\gamma'=\beta^x$，删去 x,输出 γ 为会话编号 s 下的密钥。

步骤四：收到(P_i,s,sig),P_j 验证 P_i 的数字签名和其包含的值，如果验证成功，则输出 γ 为会话编号 s 下的密钥。

二、多方密钥交换的各种算法比较

在两方 Diffie-Hellman 协议的基础上，后来出现了不少群组密钥交换协议(Group Key Distribution Protocol)，GKDP。

术语定义：

n	参加密钥交换协议的成员人数
i,j,k	组内成员的下标，从 1 到 n
M_i	第 i 个组内成员
q	群的阶
g	指数式的底数
Ni	M_i 随机产生的指数
S,T	{1,…,n}的子集
π(S)	S 集合中所有元素的积
K_n	n 个成员共享的密钥

(一)、Group Key Distribution GDH 1.0：

1.包含两个阶段，向上阶段和向下阶段：

(1)、向上阶段　其主要任务是收集所有组内成员的信息，每个 Mi 的任务是将 $g^{N_1 \cdots N_{i-1}}$ 升幂为 $g^{N_1 \cdots N_{i-1}N_i}$，从而加入自己的信息，$M_i$ 向 M_{i+1} 传递 i 个中间值。最后，M_n 收到向上的信息，可以计算出会话密钥，$g^{N_1 \cdots N_{n-1}N_n}$。

(2)、向下阶段　从 M_n 开始向下流，每个 M_i 先计算出会话密钥 K_n，提供下一方 M_{i-1} i-1 个中间值，中间值在下降阶段不断减少。

2.GDH 1.0 的优点在于不需要额外的通讯开销，例如不需要广播和同步，其缺点就是需要太多轮才能完成密钥交换。

(二)、Group Key Distribution GDH 2.0：

GDH 2.0 其实是 GDH 1.0 的改进版，其通讯的轮数大大减少了。它同样包含了两个阶段，向上阶段和广播阶段。向上阶段，收集每个成员的信息，每个 M_i 的任务是计算出 i 个中间值和一个包含 i 个指数的重要值，其中有(i-1)次指数运算。M_n 收到最后一个向上流，然后首先计算出密钥值。进入广播阶段，M_n 计算出最后一轮的中间值。很明显，GDH 2.0 减少了通讯的轮数。

(三)、Group Key Distribution GDH 3.0

1.GDH 3.0 是设计用于最小化每个成员的计算次数。它包含四个阶段：

阶段 1：向上阶段：收集每个成员的基本信息。

阶段 2：广播阶段：M_{n-1} 到所有成员的信息，获得所有秘密指数的乘积，然后把它广播到各个成员。

阶段 3：回应阶段：M_i ($i \neq n$)根据其私有指数计算出密钥，并把结果返回给 M_n。

阶段 4：广播阶段：M_n 收到所有的输入，然后把每个都升幂自己的指数。最后把 n-1 个结果广播到其余 n-1 个成员。

2.下面分析一下 GDH 3.0 的优点：

(1)、信息包大小为常数。

(2)、每个成员进行的指数运算次数都一样，(除了 M_n 要 n 次)并且都不多。

(四)、ING 协议　此密钥交换协议需要一个各成员同步开始，各成员在逻辑上是一个环。一开始，每成员都将以其随机数为指数的幂发送给环的下一个成员。接着每一轮，每个成员都将上轮收到的中间值升幂，指数为其私有的指数。n-1 轮后，每个成员都可以计算出会话密钥。

(五)、BD 算法：

1.BD 算法分两个阶段。

(1)、每个成员 M_i 随机产生指数 N_i，并计算出 $Z_i=g^{N_i}$，并广播到其余每个成员。

(2)、Mi 收到 Z_{i-1} 和 Z_{i+1}，计算出 $X_i=(Z_{i+1}/Z_{i-1})^{N_i}$，并把这个指广播出去。

(3)、这时候，M_i 可以计算出会话密钥 $K_n=Z_{i-1}^{nN_i} * X_i^{n-1} * X_{i+1}^{n-2} \cdots * X_{i-2} \bmod p$。会话密钥就是 $K_n=g^{N_1N_2+N_2N_3+\cdots+N_nN_1}$。

(六)、下面看看各协议的对比：

	GDH 1.0	GDH 2.0	GDH 3.0	ING	BD
通讯轮数	2(n-1)	n	n+1	n-1	2
信息数	2(n-1)	n	2n-1	n(n-1)	2n
合计信息大小	n(n-1)	((n+3)n)/2-3	3(n-1)	n(n-1)	2n

每成员发送信息	2 M_1和M_n为1	1	2 M_1和M_n为n	n-1	2
每成员收到信息	2 M_1和M_n为1	2 M_1和M_n为1	3 M_1和M_n为n	n-1	n+1
每成员进行的指数运算	i+1	i+1	4 M_1和M_n为n	n	n+1
指数运算合计	((n+3)n)/2-1	((n+3)n)/2-1	5n-6	n^2	n(n+1)
是否需要同步	否	否	否	是	是
是否DH密钥	是	是	是	是	是
是否对称	否	否	否	是	是

（七）、动态

多方Diffie-Hellman协议

1.上面介绍的协议都是基于群组成员都是静态的，成员不能动态加入或中途退出。

近年来出现了动态群组Diffie-Hellman协议。考虑到敏感数据共享或是小型会议时，要求一个群体都有责任保证数据传输的安全，因此他们需要共享一个密钥，并且多方能并行运行。动态群组Diffie-Hellman协议具有更广的应用性，也更加灵活和方便。首先：身份认证群组密钥交换协议需要达到哪些要求呢？必须是群组里面的成员才能计算出密钥，其他人不能。其次一个密钥必须和一个随机生成的01串不可区分。

2.群组动态Diffie-Hellman密钥交换协议具有以下特点：

（1）、群组的大小相对小，最大容量为100个成员。

（2）、不需要中心服务器。

（3）、各成员都具有相似的计算能力。

（4）、成员关系都是动态的，成员可以随时加入或离开广播群组。

三、Diffie-Hellman协议的应用

Whitfield Diffie和Martin Hellman在1976年发明了DH算法。现在已经广泛应用于很多安全传输协议中，例如安全套接字Secure Sockets Layer (SSL), Secure Shell (SSH), and Public Key Infrastructure (PKI)。

（一）、SSL中的Diffie Hellman算法 SSL协议是由Nescape公司在1995年开发公布的。其SSL v3.0版本已经成为了现在web服务器和web用户交互敏感数据资料的加密安全标准。IETF组织（The Internet Engineering Task Force）于1999年采纳了该协议，并更名为TLS（Transport Layer Security），并在RFC2246中定义。SSL/TLS由两部分组成。较低的一层是在TCP上运行的Record Protocol，主要负责对称加密以保证通讯是可靠的和保密的。上层则是握手协议（Handshake Protocal），负责成员身份认证和加密方法和密钥的协商。DH算法就是运行在这一层上。Wagner and Schneier专家指出[②]，DH算法是目前最好的密钥交换协议。

特别地，早期的系统，服务器和用户都是用明文来交换握手信息的。例如开始的Hello，然后协商加密解密的算法，密钥交换协议，压缩选项等等。而其中密钥交换协议就有DH算法。密钥交换过程是使用不对称加密（公钥）来保证交谈的双方都是他们所宣传的人。这是通过刚刚对每个会话计算出来的暂时密钥对来实现的。这次交换之后，密钥可以计算出来，双方可以按照协商好的加密方法用会话密钥来交谈了。

实际使用中，用户要求服务器认证服务器的身份。但是这时没有一个互联网上的公钥分布系统（PKI, Public Key Infrastructure）。这种一路的认证是通过把众所周知的CA（Certificate Authorities）的身份认证信息编码到浏览器中。

（二）、SSH中的Diffie Hellman SSH（Secure Shell）既是一个协议也是一个程序，用来在两个通讯的计算机之间加密信息。通常是telnet, ftp这些工具的取代品。这些一般的工具并没有加密传输的信息，所有的信息，包括帐号和密码都是通过明文来传输。SSH传输层协议在IETF草稿文档“SSH Transport Layer Protocol”中定义。连接的两方首先协商各个参数，例如加密和压缩的算法和某些随机参数。然后用与SSL/TLS类似的方法以DH算法算出共享秘密中间值。最后用一散列函数来生成加密的密钥。

（三）、PKI下的Diffie-Hellman 公钥分布系统（Public Key Infrastructure, PKI）是指一个协议和服务的系统，在不对称加密环境中可以给公钥加密提供支持。可以同时提供身份认证和数字签名等服务。例如我用A在PKI的公钥加密一段信息，只有A才能看到，因为只有他才有私钥把密文转换为明文。同样，如果我用我的私钥加密或一段消息，或用散列函数加上签名，那么其他人可以用公钥看到此消息，并且确信此消息是由我发出的。因此PKI可以用来防止抵赖和保密。公钥加密中一个重大的问题就是保证你有其他人的一个正确的公钥。就是说，在没有加密之前，你担心别人会盗取或改变你要发送的信息。在加密出现之后，你担心的就是你的公钥会否被其他人改变。这是通过分层的CA来实现的。一个CA可以产生包含身份信息和公钥的数字证书。为保证这个证书是合法的，证书里面亦含有上级CA的数字签名。这时候，双方可以通过得到对方的公钥来交换数据。在此过程中，公钥不能改变是十分重要的，因此证书的一个加密的散列出现，而此密钥就是从Diffie-Hellman算法得出。

总之，Diffie-Hellman算法已经几乎渗透进入互联网上每个加密安全协议中，包括SSL,SSH,IPSec和PKI，而其他的安全协议又或多或少地依赖这些核心协议。科

参考文献

[1] Diffie W,Hellman M E. New directions in cryptography.IEEE Transactions on Information Theory,1976,22 (6):644~654.
[2] Yair Amir _ Yongdae Kim _ Cristina Nita-Rotaru _ Gene Tsudik, On the Performance of Group Key Agreement Protocols.
[3] Wagner,David and Bruce Schneier, Analysis of the SSL 3.0 Protocol, PDF document available from http://www.counterpane.com/ssl.html.
[4] Ylonen,T.,et al.,SSH Transport Layer Protocol,IETF IPSec Working Group,January 2001,http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-09.txt.
[5] 孔晖,郑志华,徐秋亮《几种典型的认证Diffei2Hellman型密码共识协议的分析与比较》计算机工程与应用2001,37(18):72—74.
[6] (USA) BRUCE SCHNEIER.应用密码学:协议、算法与C源程序(Applied Cryptography: Protocols,Algorithms and Source Cord in C) 北京机械工业出版社2000.
[7] 韦卫,王行刚《密钥交换理论与算法研究》通信学报1999.20(7):64—68.
[8] 李克洪著《实用密码学与计算机数据安全》吉林.东北学大学出版社1997.

作者简介：余海冰（1979、11），女，在职研究生，现在广东轻工职业技术学院任教。

潘泽宏（1980、10），男，广东轻工职业技术学院计算机系老师。

关注：① Diffie W,Hellman M E.New directions in cryptography.IEEE Transactions on Information Theory,1976,22 (6):644~654.

② Wagner, David and Bruce Schneier,Analysis of the SSL 3.0 Protocol,PDF document available from http://www.counterpane.com/ssl.html中指出.

（上接第67页）立即停止施工，采取相应的措施，确保使用安全。

(7)对施工升降机、物料提升机的采购、租赁及使用必须严格控制，防止不合格产品投入现场使用。

(8)在恶劣的气候（如雨雪天、大雾、六级以上强风）和环境不良的条件下，禁止从事高处或洞口作业。

根据博德（Frank Bird）现代事故因果连锁理论对事故的分析，我们将各种坠落事故的原因进行了比较全面的分析，并给出了一些防范措施，在广泛采纳以上对策和建议的基础上，深入开展安全标准化管理，认真执行现行的安全技术标准、规范和规程，高处坠落事故是完全可以减少和避免的。科

参考文献

[1] 孙连捷《安全生产事故案例分析》中国经济出版社/2004-04-01.
[2] 王赫《建筑工程质量事故分析》第二版，中国建筑工业出版社，1999年6月.
[3] 陈喜山，《系统安全工程学》中国建材工业出版社2006-1-1.

作者简介：赵雪梅，女，1979年8月出生，安徽淮南人，安徽理工大学2005级安全技术及工程专业硕士研究生。