无线自组网中有效的证密钥协商方案

李小青 李 晖 马建峰
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要 在Diffie-Hellman密钥交换算法和基于身份的密码体制基础上,提出一种适用于无线自组网的认证密钥协商方案。该方案利用分布的多项式秘密共享的思想,实现PKG分布化和网络中节点公私钥的生成。通过随机数认证和基于身份的签名以及DH密钥协商算法实现认证密钥协商。该方案IBE与DH算法相结合,具有基于身份的密码体制低存储量和通信量的优点,同时认证密钥协商后的通信均可采用对称密码算法来有效降低计算量,节省网络资源。理论分析证明本方案是安全的。

关键词 密码学,密钥协商,IBE,Diffie-Hellman密钥交换,秘密共享
中图法分类号 TP309 **文献标识码** A

Efficient Authenticated Key Agreement Protocol in MANET

LI Xiao-qing LI Hui MA Jian-feng
(Ministry of Education Key Laboratory of Computer Network and Information Security, Xidian University, Xi'an 710071, China)

Abstract Based on IBE and Diffie-Hellman key agreement arithmetic, an efficient authenticated key agreement protocol for MANET was proposed. The PKG distribution and the created public/private key of nodes without using the trust third part were achieved by used distributed polynomial secret sharing scheme. The authenticated key agreement was carried out by IBS and DH key agreement arithmetic. The protocol was combined with IBE and DH, it had the advantage of low storage and traffic of IBE, as well as the communication after key agreement could adopt symmetry cryptographic algorithm which could availability lower computation and save resource of the MANET. The protocol was proved secure in theory.

Keywords Cryptography, Key agreement, IBE, Diffie-Hellman key agreement, Secret sharing

无线自组网是一种由移动节点组成的临时性自治系统。作为一种无线移动网络,无线自组网和传统的移动网络有着许多不同,其中一个主要的区别是无线自组网不依赖于任何固定的网络设施,而通过移动节点间的相互协作来进行网络互联。网络的这种特点使得无线自组网的安全问题尤为突出。由无线自组网的特点决定通信节点间共享的密钥应该能够动态生成而不依赖任何固定的第三方,在确保密钥安全和通信双方的相互认证的同时具有较小的计算量、存储量和通信量。

1 引言

密钥交换最早由Diffie和Hellman[1]在1976年提出,但这种方法却无法有效抵挡中间人的攻击。由Bellare[2]提出的第一个基于口令的认证密钥交换协议可以实现身份认证。用户通常事先共享一个口令,用来在通信中进行彼此身份认证,并协商一个短期会话密钥。基于口令的密钥交换协议需要满足协议运行过程中不泄漏关于口令的安全准则。如何有效地抵抗攻击者对口令进行猜测攻击成为设计这类协议的目标之一。基于口令认证的DH密钥协商机制可以利用口令提供有效的认证,如文献[3]中提出的DH-EKE,以及文献[4]中的PAK协议。

1984年,Shamir[5]提出了基于身份的密码系统。用户的公钥可以通过某个公开算法直接从其身份信息得到,而私钥从PKG(Private Key Generator)获得。与基于公钥基础设施PKI(Public Key Infrastructure)体制相比,基于身份的体制不存在颁发公钥证书所带来的存储和管理开销的问题,能有效地减少传统公钥体制下管理证书的开销。2001年,Boneh和Franklin[6]利用椭圆曲线上的双线性对,提出一个真正意义上的基于身份的高效加密方案IBE(Identity-Based Encryption)。此后,许多基于身份的密钥协商方案被提出,文献[7,8]相继给出了基于IBE的两方和三方可认证密钥协商方案。

2003年,Khalili和Katz在文献[9]中首先提出一个用于无线自组网的基于身份的密钥管理方案。该方案的基本思想是由一组选定的节点共同承担私钥产生中心(KGC)的职责,它们根据(t,n)门限方案获得系统主密钥的一个份额,联合为节点产生私钥。此方案的最大缺点是承担KGC职责的节点固定,它们不能随意离开网络,由于其身份的特殊性可能成为

到稿日期:2010-04-22 返修日期:2010-09-29 本文受国家自然科学基金(60772136,60633020),863国家高技术研究发展计划(2007AA01Z429)资助。

李小青(1981—),女,博士生,讲师,主要研究方向为网络安全、安全路由协议研究等,E-mail:xqli@mail.xidian.edu.cn;李 晖(1968—),男,博士,博士生导师,主要研究方向为信息与网络安全等;马建峰(1963—),男,博士,博士生导师,主要研究方向为信息安全与网络安全等。

网络的瓶颈。

鉴于以上考虑，本文提出一种基于身份的无线自组网身份认证密钥协商方案。该方案具有基于身份的密码体制的优点，同时利用分布的多项式秘密共享的思想，实现 PKG 分布化和网络中节点公私钥的生成，并且在节点公钥中加入生存时间利于节点撤销，完成密钥管理；采用随机数认证和基于身份的签名实现节点间的相互认证，Diffie-Hellman 密钥交换算法完成无线自组网的安全密钥协商。与一般密码协商方案相比，本方案简单可行，在满足无线自组网中密钥安全的同时，利用基于身份密码体制的优点和会话密钥建立通信后，采用对称密码体制使得系统结构简化，节省网络资源。本文同时证明了方案的安全性。

本文第 1 节介绍本方案基于的基本数学问题和几种密码算法：IBE、秘密共享方案和 Diffie-Hellman 密钥交换算法；第 2 节将详细描述本方案；第 3 节对本协议的性能进行分析；最后是结束语。

2 背景知识

2.1 双线性对和相关困难问题

基于身份加密算法 IBE 的安全性建立在 CDH(Computational Diffie-Hellman)困难问题的一个变形之上，称为 BDH(Bilinear Diffie-Hellman)问题。IBE 的核心是使用了超奇异椭圆曲线上的一个双线性映射(Weil pairing)。

2.1.1 双线性对

令 G_1 和 G_2 是两个 q 阶循环群，G_1 是加法群，G_2 是乘法群。一个双线性对 e 就是一个从 $G_1 \times G_2$ 到 G_2 的双线性映射，并满足以下性质：

(1)双线性性：设 $P,Q\in G_1$，$a,b\in Z_q$，有 $e(aP,bQ)=e(P,Q)^{ab}$；

(2)非退化性：对每一个 $P\in G_1^*$，总存在 $Q\in G_1$，使得 $e(P,Q)\neq 1$；

(3)可计算性：给定 $P,Q\in G_1$，存在一个有效的算法用以计算 $e(P,Q)$。

当 q 为素数时，G_1 中任意一个元素 P 都是生成元，根据非退化性和双线性性，$e(P,P)$ 也是 G_2 的生成元。

2.1.2 相关困难问题

(1)计算 Diffie-Hellman 问题(CDH)：给定 P,aP,bP，计算 abP。

(2)双线性 Diffie-Hellman 问题(BDH)：给定 P,aP,bP,cP，计算 $e(P,P)^{abc}$。

2.2 基于身份的加密算法

Boneh-Franklin 基于双线性对的 IBE 算法主要由 Setup，Extract，Encrypt，Decrypt 4 个算法组成，分别完成系统参数建立、密钥提取、加密和解密功能。

(1)Setup：PKG 生成阶为 q 的群 G_1、G_2 和一个可有效计算的双线性对 $e:G_1\times G_1\rightarrow G_2$，$G_1$ 的生成元 P 和两个用于密码的 Hash 函数 $H_1:\{0,1\}^*\rightarrow G_1$ 和 $H_2:G_2\rightarrow\{0,1\}^k$(IBE 方案的信息空间是 $\{0,1\}^k$，即一个 k 比特的字符串集合)。PKG 随机地选择一个 $s\in Z_q$ 并秘密地保存它的值。它的公钥 $P_{pub}=sP$，系统公共参数为 (G_1,G_2,e,P,sP,H_1,H_2)，并且包括 PKG 向其用户公布私钥的“时间表”

(2)Extract：Bob 将身份 $ID\in\{0,1\}^*$ 发送给 PKG，PKG 计算 Bob 的私钥 $S_{ID}=sQ_{ID}=sH_1(ID)$。

(3)Encrypt：为了对消息 $M\in\{0,1\}^*$ 加密，Alice 使用随即生成的 $r\in Z_q$，计算密文：$C=[U,V]=[rP,M\oplus H_2(g^r)]$，这里，$g=\hat{e}(sP,Q_{ID})\in G_2$。

(4)Decrypt：为了解密 $C=[U,V]$，Bob 计算 $V\oplus H_2(e(U,S_{ID}))$，它与 M 相等的。

在假定 BDH 问题是困难的前提下，IBE 加密算法在应对选择明文攻击时是可证明安全的(在随机预言模型中)。

2.3 秘密共享

Shamir 等人[10]最早在 1979 年提出秘密共享的概念，并给出 (t,n) 门限秘密共享体制。它是将秘密 S 分割成若干个份额在一组参与者 $A=\{A_1,A_2,\cdots,A_n\}$ 中进行分配，使得每一个参与者得到关于该秘密的一个份额。只有 A 中的任一子集 T，$|T|\geqslant t$ 可以重构 S；A 中的任一子集 T，$|T|<t$ 都不能重构 S，甚至得不到关于秘密 S 的任何有用信息。

Shamir 提出利用有限域 $GF(p)$ 上的 $t-1$ 次多项式 $h(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1} \bmod p$，来构造秘密共享的 (t,n) 门限体制。其中，所选的随机素数 p 要大于最大可能的秘密数 s 和参与者总数 n，并且公开；$s=h(0)=a_0$，而 $\{a_1,\cdots,a_{t-1}\}$ 为选用的随机系数，这些都需保密，在生成 n 个秘密份额之后即可销毁。通过计算多项式 $h(x)$ 对 n 个不同 x_i 的取值就可给出每个共享者的秘密份额 $s_i=h(x_i) \bmod p$，$i=1,\cdots,n$。由于任意 t 个点都可唯一地确定相应的 $t-1$ 次多项式，因此秘密 s 可以从 t 个秘密份额重构。给定任意 t 个秘密份额 $s_{i_1},s_{i_2},\cdots,s_{i_t}$，由 Lagrange 内插法重构的多项式为 $h(x)=\sum_{r=1}^{t}s_{i_r}\prod_{j\neq r,j=1}^{t}\frac{x-x_{i_j}}{x_{i_r}-x_{i_j}} \bmod p$。

2.4 Diffie-Hellman 密钥交换算法

Diffie-Hellman 密钥交换算法的安全性基于有限域上计算离散对数的困难性。节点 A 和节点 B 协商一个大素数 n 和 g，g 是模 n 的本原元，这两个整数不必是秘密的，故 A 和 B 可以通过不安全的途径协商它们。协议描述如下：

(1)A 选择一个大随机整数 x，并计算 $X=g^x \bmod n$，将 X 发给 B。

(2)B 选择一个大随机整数 y，并计算 $Y=g^y \bmod n$，将 Y 发给 A。

(3)A 计算会话密钥 $k=Y^x \bmod n$。

(4)B 计算会话密钥 $k'=X^y \bmod n$。

显然，A 和 B 是独立计算会话密钥的，且 $k=k'=g^{xy} \bmod n$。网络中的窃听者若截获 X 和 Y，而且知道 n 和 g，除非能计算出离散对数，恢复 x 和 y，否则无法计算出会话密钥 k。但是 Diffie-Hellman 密钥交换算法的最大缺点是不能防止中间人攻击。

3 有效的身份认证密钥协商方案

基于身份的认证密钥协商方案总体上分两个阶段：系统初始化和会话密钥协商。其中系统初始化阶段设立系统主密钥和公共的参数，为系统中参与通信的所有节点生成相应的秘密信息；会话密钥协商阶段完成协商会话密钥，同时实现身份认证。

3.1 系统主密钥和节点私钥的产生

本方案系统初始化阶段采用 Shamir 提出的门限体制，利用分布的多项式秘密共享的思想，实现 PKG 分布化；通过

Lagrange 插值系数重构系统主密钥，利用 IBE，网络中各节点生成公私钥，并且在各节点公钥中加入生存时间，以利于节点撤销，实现密钥管理。

无线自组网包含 n 个节点，随着节点的加入和离开，网络节点数动态可变。选取阶为 q 生成元为 P 的群 G_1、G_2，双线性映射 $e:G_1\times G_1\rightarrow G_2$，两个用于密码的 Hash 函数 $H_1:\{0,1\}^*\rightarrow G_1$ 和 $H_2:G_2\rightarrow\{0,1\}^k$。选择有限域 $GF(p)$ 上的 $t-1$ 次多项式 $h(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1} \bmod p$ 构造秘密共享的 (t,n) 门限体制，主密钥 $s=h(0)$ 在所有 n 个节点中分布式共享，系统公钥 $P_{pub}=sP$ 公开的系统参数 (G_1,G_2,e,P,sP,H_1,H_2)。

当请求私钥时，身份为 ID 的节点秘密产生 x_i 并向邻节点广播私钥请求信息，通过多项式 $h(x)$ 得到秘密份额 s_i，当成功获得任意 t 个 (s_i,x_i) 时，节点通过 Lagrange 内插法重构多项式恢复出系统主密钥，并获得自己的私钥 $S_{ID}=sQ_{ID}=sH_1(ID)$，节点公钥 $Q_{ID}=H_1(ID)$。其中在节点公钥中包括公钥生存时间，以便实现密钥及时更新。

3.2 会话密钥协商

本方案采用基于身份的签名实现节点间的相互认证，通过 Diffie-Hellman 密钥交换算法实现密钥协商，利用基于有限域上计算离散对数的困难性保证会话密钥安全。假设节点 A 和节点 B 要建立会话密钥，它们知道彼此的公钥 $Q_A=H_1(ID_A)$ 和 $Q_B=H_1(ID_B)$。$S_A=sQ_A$ 和 $S_B=sQ_B$ 分别是两个节点的私钥，被秘密保存。密钥协商算法描述如图 1 所示。

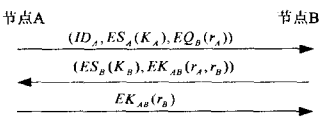

图 1 双向认证密钥协商

(1)节点 A 选取随机整数 r_1 和 r_A，计算密钥 $K_A=g^{r_1} \bmod n$，利用初始阶段产生的私钥对 K_A 签名，得到 $ES_A(K_A)$，同时用节点 B 的公钥加密随机数 r_A，发送消息 $(ID_A, ES_A(K_A), EQ_B(r_A))$ 给节点 B。

(2)节点 B 收到消息(1)后，通知节点 A 与它建立会话密码，用 Q_A 验证签名是否正确，同时用 S_B 解密得到 A 的随机数 r_A。节点 B 选取随机整数 r_2 和 r_B，计算密钥 $K_B=g^{r_2} \bmod n$，并发送 $(ES_B(K_B), EK_{AB}(r_A, r_B))$ 给 A。

(3)节点 A 收到消息(2)后，通过验证签名确定消息是否来自节点 B，同时得到 K_B，计算得到协商密钥 K_{AB} 后解密 r_A 和 r_B。比较 r_A 是否正确后，发送确认消息 $EK_{AB}(r_B)$ 给节点 B。

(4)节点 B 收到消息(3)后，确认节点 A 已收到自己发出的消息。此后节点 A 和节点 B 用协商好的会话密钥 K_{AB} 通信。

在节点 A 和节点 B 的密钥协商过程中，利用基 DH 密钥交换算法保证会话密钥安全，同时采用基于身份的签名对节点身份进行认证，以有效防止中间人攻击。本方案利用 IBE 的优点有效简化系统结构，节省网络资源。

3.3 新加入节点密钥份额产生

本方案允许节点动态加入。新节点请求加入网络时，发送私钥请求，由至少 t 个邻节点联合为其产生私钥。采用和初始阶段相同的方法生成私钥后，再从其它任意 t 个邻节点处安全地获取自己的主密钥份额，由此实现系统的完全分布式。

4 性能分析

在本方案中，利用 IBE 算法和分布的多项式秘密共享的思想，实现 PKG 分布化和网络中节点公私钥的生成。Shamir 的门限体制是完善的，同时要想从 IBE 算法产生的私钥 sP 或 $S_{ID}=sQ_{ID}$ 中计算出主密钥及各节点私钥是基于求解离散对数的困难性，由 DH 算法截获会话密钥也是困难的，因此保证了主密钥和各节点私钥的安全性。

采用随机数认证和基于身份的签名实现节点间的相互认证，在密码建立过程中，用 Diffie-Hellman 密钥交换算法得到对称会话密钥，由于随机数临时选取，一个节点被攻击后，也不会影响其他节点的密钥安全和网络安全，从而保证了网络的可用性。方案结构简单，密钥协商后的通信过程都采用此对称密钥算法实现，降低了网络的计算量，同时 IBE 算法能有效降低协议的存储量和通信量。本方案简单可行，在满足无线自组网中密钥的安全要求的同时也能有效简化系统结构，节省网络资源。

结束语 本文提出一种基于身份的无线自组网身份认证密钥协商方案。方案在实现秘密共享的同时，采用随机数认证和基于身份的签名实现节点间的相互认证，利用 Diffie-Hellman 密钥交换算法实现无线自组网的安全密钥协商。与一般密码协商方案相比，本方案结构简单，在满足密钥安全的同时利用基于身份密码体制的优点和对称会话密钥进行通信，可有效简化系统结构，节省网络资源，能适应无线自组网拓扑动态变化且网络资源紧张等特点，实现安全有效的通信。

参 考 文 献

[1] Diffie W, Hellman M E. New Directions in Cryptography[J]. IEEE Trans. on Information Theory, 1976, IT-22: 644-654

[2] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks[C]// Advances in Cryptology-EUROCRYPT 2000. Lecture Notes in Computer Science, vol. 1807. Springer-Verlag, 2000: 139-155

[3] Bellovin, Merrit. Encrypted key exchange: password-based protocols secure against dictionary attacks [C]// Proceedings of the IEEE Symposium on Research in Security and Privacy. Oakland, IEEE Computer Society, 1992: 72-84

[4] Boyko V, Mackenzie P, Patel S. Provably secure password authenticated key exchange using Diffie-Hellman [C] // Proceedings of Advances in Cryptology-Eurocrypt 2000. LNCS, 2000: 156-171

[5] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Crypto'84. Berlin: Springer-Verlag, 1984: 47-53

[6] Boneh D, Franklin M. Identity based encryption from the weil pairing[C]// Proc. of Crypto'01. Berlin: Springer-Verlag, 2001: 213-229

[7] Al-Riyami S S, Paterson K G. Tripartite Authenticated Key Agreement Protocols from Pairings [EB/OL]. http:/ /eprint. iacr. org/2002/035/, 2002: 07-21

[8] Smart N P. An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairing [J]. Electronics Letters, 2002, 38(13): 630-632

[9] Khalili A, Katz J, Arbaugh W A. Toward secure key distribution in truly Ad-Hoc networks[C]// Proceedings of The Symposium on Applications and the Internet Workshops. Los Alamitos: IEEE Computer Society Press, 2003: 342-346

[10] Shamir A. How to share a secret [J]. ACM Communications, 1979, 22(11): 612-613