计算机科学2002Vol.29№.11

Ad-Hoc 网络中的密钥建立协议*)

Key Establishment Protocols in Ad-Hoc Networks

郎文华　周明天

(电子科技大学计算机科学与工程学院　成都610054)

Abstract　In Ad-hoc networks, key establishment protocol is mainly contributory, Diffie-Hellman based key agreement protocol. In this paper, Several typical protocols are analysed and evaluated, and then, their suitability is discussed from the point of view of Ad-Hoc networks.

Keywords　Ad-Hoc network, Key agreement, DH key exchange

Ad-Hoc 网络作为一种新兴的无线网络,与传统的无线网络相比缺少固定基础设施的支持(比如基站或移动交换中心),节点直接依靠无线链路进行通信并维持网络的连接。由于 Ad-Hoc 网络的建立灵活便捷,因此在军事、商业上有着广泛的应用前景,比如:战场上的作战单位之间的通信,数字电子设备之间的联网以及虚拟会议(教室)等等。Ad-Hoc 网络的安全性问题也随之成为一个研究热点,文[1,2]对此作了讨论。

本文将针对 Ad-Hoc 网络中的安全通信,结合 Ad-Hoc 网络的自身特点,对已有的密钥建立协议进行分析讨论。

1. 密钥建立协议的安全性考虑

在 Ad-Hoc 网络中,密钥建立协议应满足如下要求[3,4]:①完全向前保密(Perfect Forward Secrecy);②抗已知密钥攻击;③密钥认证;④密钥确认及密钥完整性。

传统的加密方法可以实现上述要求,但由于 Ad-Hoc 网络自身的限制[4,6],因而不能直接用于密钥建立协议。构成 Ad-Hoc 网络的节点往往是小的便携式设备,其计算能力差,因此要求协议的轮数和运算量要尽量少;网络节点动态变化,而且连接并不可靠,因此理想的协议不应事先假设网络的拓扑结构;缺少固定基础设施的支持,也就缺少可信的第三方,网络中各节点是对等的,因此指定一个节点来生成、分配密钥也是不现实而且不安全的。

2. 密钥建立协议

密钥建立协议可分为两大类[5]:密钥协商协议(key agreement protocol)和基于可信第三方的密钥分配协议(key distribution protocol)。在 Ad-Hoc 网络中,假设可信第三方来计算、分配密钥是不实际的,另外,用于密钥生成的节点也易于遭受攻击而造成整个网络通信的不安全,因此密钥分配协议不适合于 Ad-Hoc 网络的应用。本文主要讨论密钥协商协议,即多个节点协商产生一个共同的密钥。

已有的密钥协商协议大多基于 DH(Diffie-Hellman)密钥交换[7],其安全性:关于 DH 问题、DHD 及 DL 问题的复杂性研究可参看文[8]。

本文中用到的符号定义如下:

n:参与密钥协商的成员数;

i,j:成员序号($i,j\in[1,n]$);

M_i:第 i 个成员;

G:Z_p^* 的循环子群,阶为 q,其中 p,q 为素数;

q:G 的阶;

φ:$G\rightarrow Z_q$;

α:G 的生成元;

x_i:$x_i\in_R Z_q^*$($\in_R Z_q^*$ 表示从 Z_q^* 中随机选择);

k_n:n 个成员的共享密钥。

根据文[9,10],本文采用的效率参数如下:

消息(message)数、DH 交换数(或交换数)、同步轮(synchronous round)数(仅在协议需广播功能时才采用)、简单轮(simple round)数以及幂运算数。

2.1　Ingemarsson(ING)协议

ING 协议[11]是最早的密钥协商协议。协议要求 n 个成员组成一个逻辑环,同步启动。在每一给定轮次,M_i 将收到的中间值取 x_i 次幂,然后传递给下一成员,$n-1$ 轮后得到 $k_n=\alpha^{x_1x_2\cdots x_n}$。如图1。

第 k 轮(k∈[1,n−1]):

$$M_i \xrightarrow{\alpha^{\Pi(x_j)j\in[(i-1)\bmod n,i]}} M_{(i+1)\bmod n}$$

图1　ING 协议

ING 协议不需要成员具有广播能力,其效率参数如下:

消息数:$n(n-1)$;交换数:$n(n-1)$;简单轮数:$n-1$;M_i 的幂运算数:n;总的幂运算数为:n^2。

2.2　Burmester/Desmedt(BD)协议

BD 协议[12]是一个效率很高的协议,仅需3轮就可完成。

1. 每个成员 M_i 选择 x_i:$x_i\in_R Z_q^*$,然后广播 $z_i=\alpha^{x_i}$;

2. 每个成员 M_i 计算并广播 $t_i=(z_{i+1}/z_{i-1})^{x_i}$;

3. 每个成员 M_i 计算共享密钥 $k_n=z_{i-1}^{nx_i}\cdot t_i^{n-1}\cdot t_{i+1}^{n-2}\cdots t_{i-2} \bmod p$,即 $k_n=\alpha^{x_1x_2+x_2x_3+\cdots+x_nx_1}$。

BD 协议要求每个成员都具有广播能力,其效率参数如下:

消息数:$2n$;交换数:$2n$;同步轮数:2;简单轮数:$2n$;M_i 的幂运算数:$n+1$;总的幂运算数为:$n(n+1)$。

2.3　GDH 协议

Steiner 等[9]提出了 GDH(Generic Diffie Hellman)系列

*)本文的工作得到四川省重点实验室基金和电子科大—卫士通联合实验室基金的资助。郎文华　博士生,主要研究方向为网络与信息系统安全。周明天　教授,博士导师,主要研究方向为网络与信息系统安全、计算机网络、并行分布处理等。

协议，包括 GDH. 1、GDH. 2和 GDH. 3。其中，GDH. 1效率低，不适用。下面介绍 GDH. 2和 GDH. 3。

图2为 GDH. 2协议，协议分两个阶段，最后得到 $k_n=\alpha^{x_1x_2\cdots x_n}$。

1. 第 i 轮($i\in[1,n-1]$)：

$$M_i \xrightarrow{\{\alpha^{\frac{x_1x_2\cdots x_i}{x_j}}\mid j\in[1,i]\},\alpha^{x_1x_2\cdots x_i}} M_{i+1}$$

2. 第 n 轮：

$$M_n(\text{广播}) \xrightarrow{\{\alpha^{\frac{x_1x_2\cdots x_n}{x_j}}\mid j\in[1,n-1]\}} M_i, i\in[1,n-1]$$

图2 GDH. 2协议

图3为 GDH. 3协议，协议分4阶段完成，最后得到 $k_n=\alpha^{x_1x_2\cdots x_n}$。

1. 第 i 轮($i\in[1,n-2]$)：

$$M_i \xrightarrow{\alpha^{x_1x_2\cdots x_i}} M_{i+1}$$

2. 第 n−1轮：

$$M_{n-1}(\text{广播}) \xrightarrow{\alpha^{x_1x_2\cdots x_{n-1}}} M_i, (i\neq n-1)$$

3. 第 n 轮：

$$M_i \xrightarrow{\alpha^{x_1x_2\cdots x_{n-1}/x_i}} M_n$$

4. 第 n+1轮：

$$M_n(\text{广播}) \xrightarrow{\{\alpha^{x_1x_2\cdots x_n/x_i}\mid i\in[1,n)\}} M_i, i\in[1,n)$$

图3 GDH. 3协议

GDH. 2和 GDH. 3的效率参数见下表：

	GDH. 2	GDH. 3
消息数	n	$2n-1$
交换数	n	$2n-1$
同步轮数	n	$n+1$
简单轮数	n	$n+1$
M_i 的幂运算数	$i+1(i<n)$；$n(i=n)$	$4(i<n-1)$；$2(i=n-1)$；$n(i=n)$
总的幂运算数	$n(n+3)/2-1$	$5n-6$

基本的 GDH 协议没有带认证功能，因此不能加以实际应用。文[3] 提出了带密码认证的 GDH. 3协议，该协议在第 n 轮中引入了盲因子，用 $\alpha^{(x_1x_2\cdots x_{n-1}/x_i)\cdot x_i}$ 代替 $\alpha^{x_1x_2\cdots x_{n-1}/x_i}$，增强了密码的抗字典攻击能力。

Steiner et al. 提出了带认证的 A-GDH. 2协议[5,13]，并证明了协议在主动攻击下的安全性。但 A-GDH. 2的认证只发生在 M_1 和其他成员之间，因此，Steiner 进一步提出了 SA-GDH. 2协议，该协议能提供任意成员之间的认证，提高了协议的安全性。

2.4 Hypercube(超立方体)协议

超立方体协议是 Becker，Wille[10]于1998年提出的，目的是获得协议所需的最少轮次。设 $n=2^d$，为 d 维超立方体的顶点，成员 M_i 由 d 维向量空间 $GF(2)^d$(基为 $\vec{b}_1,\vec{b}_2,\cdots,\vec{b}_d$)中的一个向量 $\vec{v}_i$ 唯一表示。协议描述如下：

·第1轮

1. $\vec{v}_i$ 选择 $x_i: x_i\in_R Z_q^*$；

2. $\vec{v}_i$ 与 $\vec{v}_j=\vec{v}_i+\vec{b}_1$进行 DH 交换(用各自的 x_i、x_j)；

·第 i 轮($1<i\leqslant d$)

$\vec{v}_i$ 与 $\vec{v}_j=\vec{v}_i+\vec{b}_i$ 进行 DH 交换(用第 $i-1$轮得到的 DH 值)；

超立方体协议不需要广播功能，其效率参数如下(设 $n=2^d$)：

消息数：$d\cdot 2^d$；交换数：$d\cdot 2^{d-1}$；简单轮数：d；M_i 的幂运算数：$2d$；总的幂运算数为：$d\cdot 2^{d+1}$。

Asokan 和 Ginzboorg[3]在超立方体协议的基础上加入了密码认证，而且还提出了具有容错功能的超立方体协议。当 $2^d<n<2^{d+1}$时，可以采用 Octopus 协议(见下节)，也可采用加入 $2^{d+1}-n$ 个虚拟成员的方式，文[3]详细分析比较了这两种方法。

2.5 Octopus 协议

Octopus 协议由 Becker，Wille[10]提出，目的是使完成协议所需的消息数最少。设 $2^d<n<2^{d+1}$，其中 2^d 个成员组成 d 维超立方体中心，其它 $n-2^d$ 个成员作为触角各自依附于中心的一个顶点。首先处于触角的成员与相应的中心成员作 DH 交换，然后中心成员用收集到的 DH 值执行超立方体协议，最后中心成员将结果值传给各自的触角。协议描述如图4：

设：$M_i(i\in[1,2^d])$为中心，I_{M_i} 为依附于 M_i 的触角成员，共 $n-2^d$ 个；

step1：1. $M_i(i\in[1,n])$选择 $x_i: x_i\in_R Z_q^*$；

2. 中心成员 $M_i(i\in[1,2^d])$，对每一个 $j\in I_{M_i}$，M_i 与 M_j 作 DH 交换，得 k_{ij}；

step2：中心成员 $M_i(i\in[1,2^d])$ 计算 $x_i'=K(I_{M_i})=\prod_{j\in I_{M_i}}\varphi(k_{ij})$，然后利用 x_i' 执行超立方体协议，得到 k_n；

step3：中心成员 $M_i(i\in[1,2^d])$ 计算 $k_j'=k_n^{k_{ij}^{-1}}$ 传给 $M_j(j\in I_{M_i})$，M_j 计算 $(k_j')^{k_{ij}}$ 便可得到 k_n。

图4 Octopus 协议

Octopus 协议的效率参数如下：

消息数：$3(n-2^d)+d\cdot 2^d$；

交换数：$2(n-2^d)-d\cdot 2^{d-1}$；

同步轮数：$d+2$；

简单轮数：

$$2\max\{|I_{M_i}|\}+d\approx 2\cdot\left[\frac{n-2^d}{2^d}\right]+d;$$

M_i 的幂运算数：

$|I_{M_i}|+2d+3(i\in[1,2^d])$；$3(i\in(2^d,n])$；

总的幂运算数为：$(2d-1)\cdot 2^d+4n$。

3. 分析比较

文[10]证明了在有广播功能和没有广播功能的情况下，完成密钥协商所需的各效率参数的下界值，如下表所示。本节将结合该表，对上述协议在 Ad-Hoc 网络中的效率、安全性进行分析比较。

	没有广播功能	有广播功能
消息数	$2n-2$	n
交换数	$2n-4,(n>4)$	n
简单轮数	$\lceil\log_2 n\rceil$	$\lceil\log_2 n\rceil$
同步轮数		1

ING 协议不需要广播功能，完成协议所需的消息数、交换数、轮数均远大于理论中的下界，而且每个成员要执行 n 次幂运算，使得协议效率很低；其次，成员必须组成环型拓扑，对 Ad-Hoc 网络来说难以实现。另外，协议的安全性差，因此 ING 协议并不适用。

BD 协议不但轮次少，而且运算量小(虽然 M_i 的幂运算次数为 $n+1$，但有 $n-2$次幂运算的指数是从2→$n-1$)，因此效率很高。但协议需要每个成员都具有广播功能，而且每轮能

同时接收 $n-1$ 条消息，这在 Ad-Hoc 网络中难以实现。BD 协议在某些环境，如广播 LANs 中具有实际用途。

GDH 系列协议中，GDH.1 效率低，没有实际用途。GDH.2/3需要 $M_n(M_{n-1}、M_n)$ 具有广播功能。其中，GDH.2的消息数和交换数达到理论中的下界，但轮数 n 却大于 $\lceil \log_2 n \rceil$，另外，M_i 的幂运算数随 i 的增大而增大，总的幂运算数为 $O(n^2)$，计算量较大；GDH.3 的消息数和交换数为 GDH.2的2倍，但计算量却小。因此 GDH.3适合于较大的情况。

就安全性来说，GDH 协议可抵抗被动攻击(基于 DDH 问题难的事实)，但不能抵抗主动攻击，而且广播消息的成员更易受到攻击。Steiner et.al. 提出了带部分认证的 A-GDH.2协议[5,13]，以及完全认证的 SA-GDH.2协议，并证明了协议在主动攻击下的安全性。另外，Asokan 和 Ginzboorg[3]引入盲因子，提出了带密码认证的 GDH.3协议，这些协议适用于一些特定的 Ad-Hoc 环境。

超立方体协议的轮数 $d=\lceil \log_2 n \rceil$ 达到理论中的下界，但消息数($n\log_2 n$)和交换数($(n\log_2 n)/2$)却大于最优值，总的幂运算数为 $O(n\log_2 n)$，优于 GDH.2。超立方体协议最大的缺点在于对网络拓扑结构的要求，这对动态的、连接不可靠的 Ad-Hoc 网络而言难以实现。但在某些成员数较少的 Ad-Hoc 环境中，Asokan 和 Ginzboorg[3]提出了具有容错功能、带密码认证的超立方体协议，既获得了较高的效率，又保证了协议的安全性。

基本的 Octopus 协议中心为4个节点($d=2$)，其交换数为 $2n-4$，在没有广播功能的情况下达到理论中的下界值，消息数 $3n-4$ 高于 $2n-2$，总的幂运算数为 $4n+12$。由于 Octopus 协议用超立方体作为中心，因此该协议与超立方体协议有相似的特点，轮数少，但难以维持网络的拓扑结构。

综上所述，以上协议均不能使每项效率参数都达到最优值。因此，上述协议只在一些特定的 Ad-Hoc 环境中才适用。

结束语 本文结合 Ad-Hoc 网络的特点，分析比较了各种密钥协商协议的效率性、安全性。它们有的需要节点具有广播能力，有的需要维持某种特定的拓扑结构，这些在 Ad-Hoc 网络中都很难实现，因此应根据实际的情况加以选择应用。而如何实现一个满足任意拓扑结构、高效的密钥协商协议仍然是一个公开的问题。

参考文献

1 Zhou Lidong, Haas Z J. Securing Ad-Hoc Networks. IEEE Network Magazine, 1999, 13(6)

2 Karpijoki V. Security in Ad-Hoc Networks. Tik-110.501, seminar on network secutity, Helsinki University of Technology Telecommunications Software and Multimedia Lab., Nov. 2000. Available at: http://citeseer.nj.nec.com/hietalahti01key.html

3 Asokan N, Ginzboorg P. Key agreement in ad hoc networks. Computer Communications, 2000, 23: 1627～1637

4 Hietalahti M. Key Establishment in Ad-Hoc Networks: [technical report of Helsinki University of Technology Lab. for Theoretical Computer Science]. 2001. Available at: http://citeseer.nj.nec.com/hietalahti01key.html

5 Ateniese G, Steiner M, Tsudik G. New Multiparty Authentication Services and Key Agreement Protocols. IEEE Journal of Selected Areas in Communications, 2000, 18(4)

6 Stajano F, Anderson R. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In: Proc. of the Seventh Intl. Workshop on Security Protocols, April 2000. Available at: http://citeseer.nj.nec.com/stajanoresurrecting.html

7 Diffie W, Hellman M E. New Directions in Cryptography. IEEE Transactions on Information Theory, 1976, IT-22(6): 644～654

8 Maurer U M, Wolf S. The Diffie-Hellman Protocol. supported by SNF, No. 20-42105.94, July 1999. Available at: http://citeseer.nj.nec.com/maurer99diffiehellman.html

9 Steiner M, Tsudik G, Waidner M. Diffie-Hellman Key Distribution Extended to Group Communication. 3rd ACM conf. on Computer and Communications Security, March 1996, New Delhi, India. Available at: http://citeseer.nj.nec.com/steiner96diffiehellman.html

10 Becker K, Wille U. Communication complexity of group key distribution. Fifth ACM Conference on Computer and Communications Security, Nov. 1998. Available at: http://www.zurich.ibm.com/security/publications/1998/BecWil98.ps.gz

11 Ingemarsson I, et al. A conference key distribution system. IEEE Transactions on Information Theory, 1982, 28(5): 714～720

12 Burmester M, Desmedt Y. A secure and efficient conference key distribution system. Advances in Cryptology. In: Proc. of EUROCRYPT'94, Springer-Verlag, 1995

13 Ateniese G, Steiner M, Tsudik G. Authenticated Group Key Agreement and Frinds. In: Proc. of the 5th ACM Conf. on Computer and Communication Security, Nov. 1998, San Francisco, CA. Available at: http://citeseer.nj.nec.com/ateniese98authenticated.html

(上接第156页)

3 Key Logic, Inc. Introduction to KeySAFE. Key Logic Document SEC009

4 Secure Computing Corporation. DTOS Lessons Learned Report. DTOS CDRL A008, June 1997

5 Loscocco P, Smalley S. Integrating Flexible Support for Security Policies into the Linux Operating, NSA Labs, Jan. 2001

6 中软安全增强 Linux. http://linux.cosix.com.cn

7 黎忠文，熊光泽. 安全(Safety)内核机制的研究与实现. 计算机科学，2001，28：87～90

8 King R. Safety kernel enforcement of software safety policies: [Doctor Thesis]. USA: University of Virginia, 1995

9 Graham G S, Denning P J. Protection - principles and practice. In: Proc. AFIPS 1972 SJCC, AFIPS Press, 1972, 40: 417～429

10 Bell D E, La Padula L J. Secure computer systems: Mathematical foundations and model: [Technical Report M74-244]. The MITRE Corporation, May 1973

11 O'Brien R C, Rogers C. Developing applications on LOCK. In: Proc. 14th National Computer Security Conf. Washington, DC, Oct. 1991. 147～156

12 Ferraiolo D F, Cugini J A, Kuhn D R. Role-Based Access Control (RBAC): Features and motivations. In: Proc. of the Eleventh Annual Computer Security Applications Conf. Dec. 1995

13 Clark D D, Wilson D R. A comparison of commercial and military computer security policies. In: IEEE Symposium on Security and Privacy, Oakland, CA, April 1987. 187～194

14 Sandhu R S. A lattice interpretation of the Chinese Wall policy. In: Proc. of the 15th NIST-NCSC National Computer Security Conf. Baltimore, MD, Oct. 1992. 221