基于优化 GDH 协商的高效安全群组密钥管理方案*

王智文[1,2], 李绍滋[1**], 苏松志[1], 刘美珍[3], 蔡启先[2]
(1. 厦门大学 智能科学与技术系, 福建 厦门 361005; 2. 广西工学院 计算机工程系, 广西 柳州 545006; 3. 广西工学院 图书馆, 广西 柳州 545006)

摘要: 针对 GDH(group diffie-hellman)方案中节点可能成为系统的瓶颈以及计算复杂度、通信代价和存储复杂度远高于某些集中式方案等缺陷, 提出并实现了一种基于优化 GDH 协商的高效安全的动态群组密钥管理方案, 并对其安全性进行了证明。通过对计算量和通信量进行分析比较表明, 优化 GDH 协商协议具有很大的优势, 并且能够快速产生或更新组密钥, 具有很强的实用性。
关键词: 组密钥协商; GDH; 优化 GDH; 动态子群; 群组通信
中图分类号: TP393 文献标识码: A 文章编号: 1005-0086(2010)04-0584-04

High efficient and secure group key management scheme based on optimized GDH

WANG Zhi-wen[1,2], LI Shao-zi[1**], SU Song-zhi[1], LIU Mei-zhen[3], CAI Qi-xian[2]
(1. Cognitive Science Department of Xiamen University, Xiamen 361005, China; 2. Department of Computer Engineering, Guangxi University of Technology, Liuzhou 545006, China; 3. Library of Guangxi University of Technology, Liuzhou 545006, China)

Abstract: There are some defects in GDH(group diffie-hellman) scheme, such as the node that may become the bottleneck of the system, and the computational complexity, cost of communications and storage complexity that are much higher than some centralized group key management program. An efficient and secure dynamic group key management scheme based on optimized GDH is proposed and implemented and its security is proven. The optimized GDH consensus agreement has great advantage than GDH by comparing and analysing the volume of calculating and traffic. At the same time, the optimized GDH consensus agreement can quickly produce and update group key, and it owns highly practicability.
Key words: group key agreemen; GDH; optimized GDH; dynamic subgroup; group communication

1 引 言

在光纤通信环境下, 随着基于群组通信的网络业务的大量涌现, 在一个群体里用多播技术广播信息正逐渐成为广泛使用的方法。然而, 群组通信还有很多安全问题有待解决, 其中密钥管理作为基本的安全手段之一受到了众多关注。已有的群组密钥管理方案可以分为集中式管理方法和分布式管理方法两大类[1]。前者群组用户的认证和管理都是由服务器完成的, 因此服务器极有可能成为整个系统的瓶颈。而后者虽然有较好的可扩展性和容侵能力, 但已有方案的性能都不够理想[2]。例如, 在 TGDH(tree-based group diffie-hellman)方案中, Sponsor 节点可能成为系统的缺陷[3], 而且其计算和存储复杂度远远高于某些集中式方案, 如 KEY GRAPH[4]。本文提出了一种基于优化 GDH 协商的高效安全的动态群组密钥管理方案, 并对其安全性进行了证明, 结果表明, 提出的方案具有多方密钥协商和密钥独立性等特征。通过性能分析可以看出, 该方案对应的密钥管理协议能十分有效地减少群组通信的计算量、存储量和通信量。

2 组密钥协商方案简介

通常的群组密钥协商方案, 一般都是针对普通的、静态的群组。基于 GDH 协议的协商群组密钥管理方案, 是通过利用原来大群的密钥信息来实现子群的建立和对子群的管理。

2.1 有代表性的组密钥协商方案

组密钥协商是一群组之间实现安全通信的协议。它是基于分布式管理的思想, 它具有 3 大特点[5]: 1) 群组的密钥一般是由全体成员一起提供, 由个人密钥素材演算出来的公共值来生成; 2) 群组中成员的生成密钥素材不会对外泄露; 3) 群组中

①收稿日期: 2009-08-08 修订日期: 2009-10-11
* 基金项目: 国家自然科学基金资助项目(60873179); 广西教育厅科研资助项目(200707LX196)
** E-mail: szlig@xmu.edu.cn

任何成员均不能事先确定群组密钥。目前有代表性的比较流行的群组密钥协商及分配方法有: CKD(centralized key distribution)协议动态选取组成员充当中心密钥管理器, 然后利用 Diffie-Hellman 协议建立中心密钥管理器和各成员间的两两通信密钥, 再利用这个通信密钥分发组密钥; GDH 协议将两方的 diffie-hellman 协议扩展到多方, 各成员利用这个协议协商建立组密钥; TGDH 协议将二叉树结构和 diffie-hellman 协议结合起来, 各成员协商建立组密钥; STR(steer, et al.)协议是 TGDH 的一种特例, 它采用一种非平衡的二叉树结构; BD(burmester-desmedt)协议是 GDH 协议的一种变体[6-8]。

2.2　GDH 组密钥协商方案

GDH 协议产生的组密钥是由全体成员共同参与协商出来的。GDH 协议创建新组的组密钥协商机制如图 1 所示。

设 P 和 g 分别是一个大素数, 且 $g/(p-1)$、G 是 Z_p^* 上的循

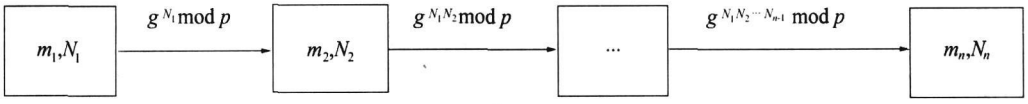

图 1　GDH 组密钥协商机制

Fig. 1　GDH key consultative mechanism for group

环子群且阶为 q, g 是 G 上的一个本原元, 并假设有 n 个成员 $\{m_1, m_2, m_3, \cdots, m_{n-1}, m_n\}$ 参加组密钥协商, $N_i \in Z_p$ 是由通信实体 m_i 产生的一随机数。可以通过以下步骤来进行组密钥协商:

1) 按照某种优先级定义要使用的大素数 p 以及底数 g, 并把 p 和 g 广播发送到每个组员 m_i;

2) 成员 m_1 产生自己的密钥素材 N_1, 然后计算出公共值 $g^{N_1} \bmod p$, 并将计算值发送给下一成员 m_2;

3) m_2 首先产生自己的密钥素材 N_2, 然后计算出公共值 $(g^{N_1} \bmod p)^{N_2} \bmod p = g^{N_1 N_2} \bmod p$, 并将计算值发送给下一成员 m_3, 依次将计算值按下标顺序逐次往下传送, 最后汇总到成员 m_n 处最后得到群密钥 $K_n = g^{N_1 N_2 \cdots N_n} \bmod p$;

4) 成员 m_n 得到群密钥 $K_n = g^{N_1 N_2 \cdots N_n} \bmod p$ 后, 直接广播给所有成员;

5) 成员 m_1 收到群密钥 $K_n = g^{N_1 N_2 \cdots N_n} \bmod p$ 后, 计算出公共值 $(g^{N_1 N_2 \cdots N_n} \bmod p)^{1/N_1} = g^{N_2 \cdots N_n} \bmod p$, 成员 $m_2 \cdots m_{n-1}$ 分别计算出公共值 $g^{N_1 N_3 \cdots N_n} \bmod p \cdots g^{N_1 N_2 \cdots N_{n-2} N_n} \bmod p$。然后把这些公共值发给成员 m_n;

6) 成员 m_n 根据收到所有成员的公共值来计算 $g^{\frac{N_1 N_2 \cdots N_n}{x}} \bmod p$, 其中 $x \in \{N_1, N_2, \cdots N_n\}$, 并广播这些公共值;

7) 每个成员根据公共值计算出群密钥 K_n, 如 m_1 计算群密钥通过 $(g^{N_2 \cdots N_n} \bmod p)^{N_1} \bmod p = g^{N_1 N_2 \cdots N_n} \bmod p$ 来计算 K_n。

GDH 协议在处理添加新组员或者删除组员时, 通常采取重新协商的做法。从上面协议执行过程可以看出, GDH 协议有如下特点: 1) 每个组员都对最终的密钥产生结果有影响, 也就是说最终密钥是以所有成员的密钥素材为基础计算出来的; 2) 每个密钥素材都是成员自己的私钥, 协商中传递的公共值是由密钥素材演算出来的, 但是第三方不能够根据这些公共值计算出任何其他成员的密钥素材, 也就是说每个成员的密钥素材始终是对其他成员保密的; 3) 当组成员发生变化时, 为了得到前向和后向安全性, 必须重新建立组密钥。因此当群组中成员有变动时, 运算量和通信量是相当大的[9,10]。

3　对 GDH 协议的优化及成员变动时组密钥协商分析

由于 GDH 协议在群组中成员有变动时, 运算量和通信量都很大, 要减少运算量和通信量就必须对 GDH 进行相应的优化。

3.1　对 GDH 协议方案的优化

针对 GDH 协议方案中, 如果攻击方在前两步中同时截获了质数 p、底数 g 以及 m_i 密钥 g^{N_i}, 那么攻击方进行简单的运算就可以计算出 N_i 的值。这样一来 m_i 就不存在秘密可言, m_i 能够计算出来的任何值攻击方都能够计算出来, 包括最终的组密钥 K_n; 并且当群组中成员有变动时, 存在运算量和通信量很大等方面的不足。经过分析 GDH 协议组密钥协商过程, 提出经过统筹优化的 GDH 协议方案。该方案能够大大地减少新建群组和群组中成员有变动时的运算量和通信量。具体实现步骤如下:

1) 按照某种优先级定义要使用的大素数 p 以及底数 g, 并把 p 和 g 广播发送给全体成员;

2) 成员 m_1 产生自己的密钥素材 N_1, 然后计算出公共值 $g^{N_1} \bmod p$, 并将计算值广播给其他成员;

3) m_2 首先产生自己的密钥素材 N_2, 然后计算出公共值 $g^{N_1 N_2} \bmod p$, 并将计算值连同 $g^{N_1} \bmod p$ 和 $g^{N_2} \bmod p$ 一起封装成一数据包广播发给所有成员, 后续成员依次将计算值与封装值再封装成一数据包广播发给所有成员;

4) 在 m_n 广播了 n 个公共值和随机数 r 后, 包括 m_n 在内的每个成员结合自己的密钥素材就可以计算出最终的组密钥 $K_n = g^{rN_1 N_2 \cdots N_n} \bmod p$。

3.2　成员增加

此方案支持动态成员事件, 当群组成员发生变动时, 组密钥必须改变。在组成员添加新成员的情况下, 可执行下面算法的步骤:

1) m_n 重新生成自己的密钥素材 g^{N_n}, 计算 $n+1$ 个公共值并产生一个随机数 r, 并把它们发送给新成员。

2) 新成员生成自己的密钥素材 $g^{N_{m+1}} \bmod p$, 计算公共值 $g^{\frac{r N_1 N_2 \cdots N_n N_{n+1}}{x}} \bmod p$, 其中 $x \in \{N_1, N_2, \cdots N'_n, N_{n+1}\}$, 并广播给所有成员。

3) 根据现有的信息, 所有成员都能够计算出新的组密钥 $g^{r N_1 N_2 \cdots N'_n N_{n+1}} \bmod p$。

3.3 成员删除

假设成员 m_i 要退出, 可执行下面算法的步骤:

1) m_n 重新生成自己的密钥素材 $g^{N'_n}$, 重新计算成员 m_{i+1} 广播出来的公共值 $g^{\frac{r N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N'_n}{x}} \bmod p$, 其中 $x \in \{N_1, N_2, \cdots N_{i-1}, N_{i+1}, \cdots N'_n\}$, 并把它广播给余下的所有成员。

2) 根据现有的信息, 除 m_i 之外的所有成员都能够计算出新的组密钥 $g^{r N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N'_n N_{n+1}} \bmod p$。

3.4 计算和通信代价分析

衡量一个组密钥协商协议的性能主要有计算量和通信量 2 个因素。本文提出的方案与 GDH 协议方案在建立新群和群中成员变动时的计算量和通信量比较见表 1 和图 2。

表 1　优化 GDH 和 GDH 的计算和通信代价对比表

Tab. 1　Cost comparison of calculation and communication by using optimized GDH and GDH

Method	Cost of calculation and communication of establishing new group by N members		Cost of calculation and communication of deleting a members of group		Cost of calculation and communication of adding a members of group	
GDH	n^2		$n^2 - n$	$(n-1)^2$	$(n-1)(n-2)$	$(n+1)^2$	$n(n+1)$
Optimized GDH	$\frac{n(n+3)}{2} - 1$	n	$2n-3$	1	$3n+1$	2

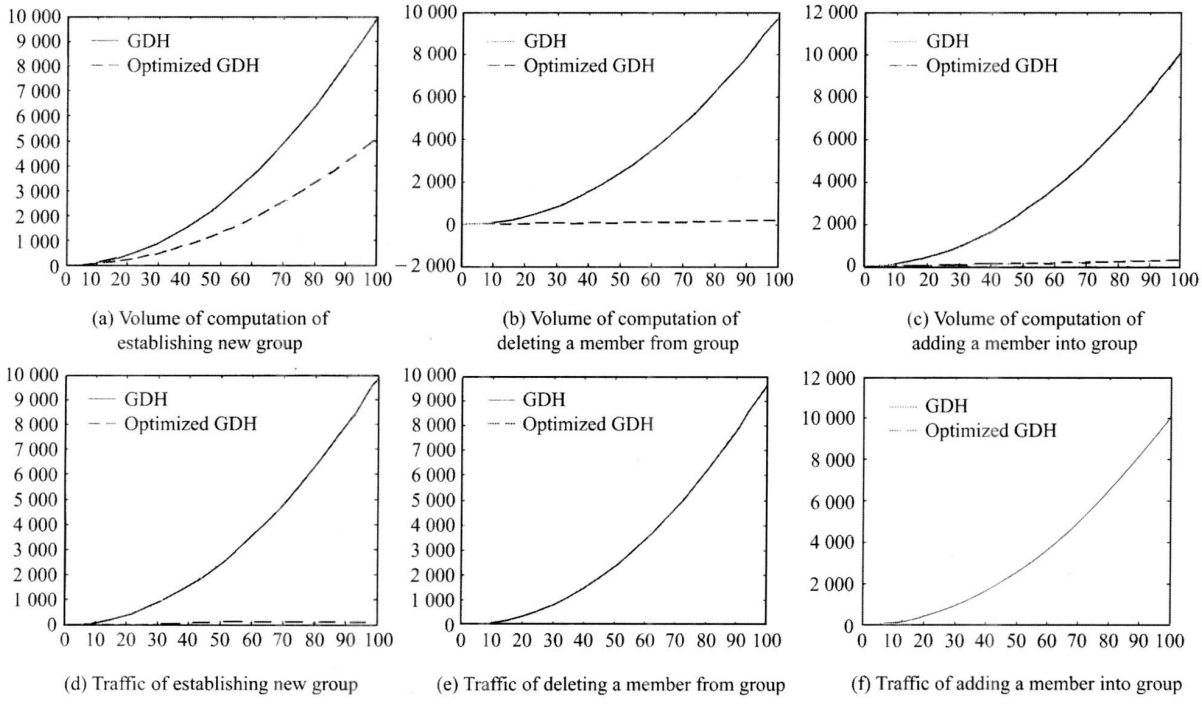

图 2　计算量和通信量比较图

Fig. 2　Comparison of the volume of computation and communication

从表 1 可以看出, 在建立新组时, 优化 GDH 协商协议的计算量比 GDH 协商协议减少了仅 1/2, 通信量减少到仅 1/n; 当成员发生变动时, 计算量和通信量减小得特别多。事实上, 这是因为在组成员变动时, 并没有重新协商组密钥, 而只是改变了一成员的密钥素材, 从而改变了最终密钥的值。而前向和后向安全性没有受到任何影响, 具体分析过程请见安全性分析。从图 2 可以看出, 当群组成员个数 $n \geqslant 10$ 时, 本文提出的优化 GDH 协商协议在计算量和通信量方面体现出明显的优越性。

表 2 是优化 GDH 协商协议方案和用其它典型方案在重新建立新群时的性能分析。从表可以看出, 在重新建立新群时, 优化 GDH 协商协议减少了大量的信息传输和密钥存储空间。

表 2　优化 GDH 和其它方案性能对比表

Tab. 2　Performance comparison of optimized GDH and other schemes

Method Performance	Optimized GDH	GDH	TGDH	CKD	BD
Establishing subgroup	Very fast	Slow	Slow	Fast	Slow
Stored key information of members	1	$o(n)$	$o(n)$	2	$o(\log n)$
The number of changed key after updating members of group	1	1	$o(\log n)$	1	$o(\log n)$
The amount of transmitted information while updating key	1	$o(n)$	$o(n)$	$o(n)$	$o(\log n)$

4 安全性分析

优化 GDH 方案协议的安全性是基于计算离散对数的困难性和门限方案的安全性[11, 12]。优化 GDH 协议不会泄露组密钥 K_n 或其他秘密参数。随机数 r 是包含在 $g^r \bmod p$ 的指数部分, 获取 r 相当于解决离散对数问题。只有系统管理者知道, 它的安全是由门限方案保证。因此, 攻击者获取 $g^{rN_1N_2\cdots N_n} \bmod p$ 是不可能的。一个已离开的成员, 用它原有的消息和服务器广播的消息是无法计算出组密钥 $g^{rN_1N_2\cdots N_n} \bmod p$ 的, 因为在它离开之后, 系统管理者重新拆分了它所在子组, 所以它所持有的那份消息也已经作废。几个离去的成员共谋也无法获得 $N_1N_2\cdots N_n$, 因为在初始化阶段和更新阶段选取的方程次数 $k-1$ 满足 $k > n_i (i \in \{1, 2, \cdots, n\})$ 且由 m_n 重新生成自己的密钥素材 g^{N_n} 和随机产生了随机数 r, 所以即使该子组成员全部离去并共谋, 也无法构成门限值 k, 从而计算出 $N_1N_2\cdots N_n$, 更不用说获得组密钥 $g^{rN_1N_2\cdots N_n} \bmod p$。这样, 保证了组密钥的前向和后向安全性。

5 结　论

提出了基于优化 GDH 协商的高效安全群组密钥管理方案, 采用改变一个成员的密钥素材和产生随机数 r, 从而改变了最终密钥的值, 且计算量和通信量都是很小的。与 GDH 协议相比, 在计算量和通信量方面具有很大的优势。与其他群组密钥协商管理方案相比, 该方案的性能存在明显的优越性。同时, 它是根据一般网络环境设计的, 能够快速产生或更新组密钥, 所以具有很强的实用性。

参考文献:

[1] Kyu Young Choi, Jung Yeon Hwang, Dong Hoon Lee. Efficient ID-based group key agreement with bilinear maps[J]. LNCS, 2004, **2947**: 130-144.

[2] Boneh D, Franklin M. Identity based encryption from the Weil pairing[J]. SIAM Journal of Computing, 2003, **32**(3): 586-615.

[3] WANG Wei, MA Jian-feng, YANG Shi-ping, et al. Secure and efficient group key management scheme in dynamic peer groups[J]. Journal of Jilin University(Engineering and Technology Edition)(吉林大学学报• 工学版), 2008, **38**(1): 131-136. (in Chinese)

[4] Kyung-Hyune Rhee, Young-Ho Park, Gene Tsudik. A group key management architecture for mobile ad-hoc wireless networks [J]. Journal of Information Science and Engineering, 2005, **21**(2): 415-428.

[5] ZHANG Zhan, LIU Guang-jie, WANG Jun-wen, et al. A novel qualtization-embedded steganographic algorithm based on Markov chain security[J]. Journal of Optoelectronics• Laser (光电子• 激光), 2009, **20**(7): 944-949. (in Chinese)

[6] WANG Zhi-wei, GU Da-wu. A Group Key Agreement Protocol Based on Tree and Threshold Idea[J]. Journal of Software, 2004, **15**(6): 924-927. (in Chinese)

[7] Xukai Zou, Byrav Ramamurthy. A block-free TGDH key agreement protocol for secure group communications[A]. IASTED International Conference on Parallel and Distributed Computing and Networks[C], 2004, ICPDCN 2004: 288-293.

[8] Kim Y, Perrig A, Tsudik G. Simple and fault-tolerant key agreement for dynamic collaborative groups[A]. 7th ACM Conference On Computer and Communications Security[C], 2000, CCCS 2000: 235-244.

[9] Wong C, Gouda M, Lam S. Secure group communications using key graphs[J]. IEEE ACM Transactions on Networking, 2000, **8**(1): 16-30.

[10] Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, et al. On the performance of group key agreement protocols[J]. ACM Transactions on Information and System Security, 2004, **7**(3): 457-488.

[11] Kumar K, Sumathy V, Begum J. Nafeesa efficient region-Based group key agreement protocol for ad hoc networks using elliptic curve cryptography[A]. 2009 IEEE International Advance Computing Conference[C], 2009, IACC 2009: 1052-1060.

[12] SUN Yun-feng, WANG Xiao-lei, WANG Ming-wei, et al. A phase-key type Fourier CGH digital watermarking method[J]. Journal of Optoelectronics• Laser(光电子• 激光), 2009, **20**(8): 1077-1081. (in Chinese)

作者简介:

王智文　(1969–), 男, 湖南邵阳人, 副教授, 博士研究生, 从事智能优化理论与网络安全的研究.