

文章编号:1001-9081(2005)12-2768-02

基于角色授权的 Ad Hoc 网群密钥分配算法

徐光伟^{1,2}, 霍佳震¹, 徐光远³, 曹奇英²

(1. 同济大学 经济与管理学院, 上海 210097; 2. 东华大学 计算机系, 上海 200051;

3. 湖南科技大学 信息学院, 湖南 湘潭 411201)

(gwxu@dhhu.edu.cn)

摘 要:针对现有群密钥分配方案中存在的抗授权侵犯能力弱的问题,提出一种基于角色授权的群密钥分配方案,通过为群成员引入角色授权的接入约束,提高了抗授权侵犯的能力,减少了群在授权侵犯下的安全威胁范围。通过与其他群密钥分配方案的比较,显示该方案具有安全性和可用性。

关键词:角色授权;Ad Hoc 网;群密钥分配;授权侵犯

中图分类号:TP309;393.08 **文献标识码:**A

Group key distributed algorithm based on role authorization in Ad Hoc network

XU Guang-we^{1,2}, HUO Jia-zhen¹, XU Guang-yuan³, Cao Qi-ying²

(1. School of Economics and Management, Tongji University, Shanghai 200092, China;

2. Department of Computer Science and Technology, Donghua University, Shanghai 200051, China;

3. School of Information Engineering, Hunan University of Science and Technology, Xiangtan Hunan 411201, China)

Abstract: Ability of resisting authorization assault is weak for existed group key distributed scheme. A group key distributed algorithm based on role authorization was proposed. The algorithm improves ability of resist and depresses threat of security on authorization assault by importing role authorization restricted in access control for group. Comparing with the other alike schemes, the proposed scheme is secure and useable.

Key words: role authorization; Ad Hoc network; group key distributed; authorization assault

0 引言

随着 Ad Hoc 网的扩展应用,其中的安全问题正成为一个重要的研究热点^[1-2],尤其是针对安全敏感性的应用方面。由移动主机构成的多跳和无中心接入的自组系统的 Ad Hoc 网络,其网络自主性、动态变化的拓扑结构、带宽限制和变化的链路容量、节点受限于设备条件、多跳通信、分布式控制、有限的物理安全、网络的可扩展性不强、单向无线信道的存在和生存时间短等方面的特性,决定了网络中节点在组织群通信时,传统的有线网络环境中的加密、认证、访问控制、权限管理和防火墙等都不再适用。

支持群安全通信的基本方法是所有群成员共享一个不为非群成员知晓的秘密群密钥,然后对群密钥的产生和分发进行分配管理。现有的群通信安全机制中,根据密钥生成与管理方式的差异可分为两大类^[3]:集中式密钥管理和分散式密钥管理。其中集中式密钥管理由一个主控体(群管理员)产生密钥并分发给每一个群成员,适合于有群领导者的群结构。而分散式密钥管理没有固定的群管理员,由所有群成员共同建立群密钥。

本文在现有群密钥分配方案的基础上,引入角色授权约束,提出一种基于角色授权约束的群密钥分配算法(Group Key Distributed Algorithm based on Role Authorization, GKDARA),提高了抗授权侵犯的能力,减少了群组在授权侵犯下的安全威胁范围。

1 群密钥分配算法分析

在现有的两大类群密钥分配方案中,分散式群密钥管理因其所具有的群成员同等地位,适合于分散的、没有领导的群结构,这种管理方式较适合 Ad Hoc 网络的成员特征,但考虑到集中式密钥管理中有群领导者,可以构件密钥生成树结构,便于群成员之间协调,因此有必要以分散式群密钥管理为主,辅助以集中式群密钥管理方案来综合分析。

文献[4]中提出了基于单向函数树(One-way Function Tree, OFT)的一种集中式群密钥管理方案。在以单向函数树组成的二元树中,其群密钥为树的根,并且自叶节点到根“向上”使用单向函数生成的,其中每个节点 x 关联着两个密钥:节点密钥 k_x 和盲节点密钥 $k'_x = g(k_x)$,每个内节点 p 的节点密钥 k_p 由它的两个儿子 x, y 的节点密钥 k_x, k_y 生成,即 $k_p = f(g(k_x), g(k_y))$ 。文献[5]中,对基于 Diffie-Hellman 算法的群密钥协商进行了改进,提出具有可证明安全性的分散式密钥协商协议套:CLIQUE。文献[6]为解决安全敏感环境下,节点易攻击而导致网络崩溃以及信道干扰造成较大传输延时等问题,提出异步的分布式密钥管理策略(Secure Distributed Online Certification Authority, COCA),以加密机制如数字签名来保护路由信息和数据交换,每个节点都有一个公用/私有密钥对,所需的密钥管理服务由 $t+1$ 个节点(网络中有 n 个节点)来完成,其假设条件为:网络中尽管没有任何一个单独的节点是值得信任的,但认为一个节点的集合是可信任的。

收稿日期:2005-06-29;修订日期:2005-08-25 基金项目:教育部重点项目资助(104086)

作者简介:徐光伟(1969-),男,江西吉水人,讲师,博士,主要研究方向:计算机网络通信及安全、电子商务及物流管理; 霍佳震(1962-),男,安徽芜湖人,教授,博士生导师,主要研究方向:管理信息系统与企业物流系统的决策支持; 徐光远(1962-),男,江西吉水人,高级工程师,主要研究方向:计算机网络通信及安全; 曹奇英(1960-),男,浙江宁波人,教授,博士生导师,主要研究方向:计算机网络和普适计算。

上述群密钥分配方案中,都是以节点的充分信任为基础的,而未考虑恶意主机伪装所带来的危害。此时的恶意主机加入群后,将会获取与其他群成员同等的地位,可轻而易举的窃取所有信息并对群成员之间的通信进行干扰,或通过破坏群成员的稳定性影响群密钥的动态更新^[7]。因此,有必要对 Ad Hoc 网络的群成员,采取最小权益策略、最小泄露策略和多级安全策略的原则来进行访问控制,通过引入角色授权访问控制(Role-Based Access Control, RBAC)^[8]约束,限制群成员在群系统中获取信息和权利的范围,按照权限和流向对其进行安全等级的划分实现接入控制,抗击来自授权侵犯的安全威胁。

基于角色授权的群密钥分配算法的基本思想是:每个群成员的加密密钥和身份签名通过单向函数形成节点密钥,然后由树型结构的叶子反算到根部的根节点密钥,成为群密钥。

2 基于角色授权的群密钥分配算法分析

基本假设:在群组通信中,一个主体成为群成员的标记是拥有群成员身份签名和相应的一个初始密钥。令 K 是群成员所有可能的密钥集合, $K = \{k_i | i \in N\}$, k_i 表示每个群成员的一个密钥,且 k_i 均匀分布并相互独立,即群成员之间的密钥是不能互相推测。令 R 为群管理员根据授权限制所划分的角色集合 $R = \{r_i | i \in N\}$, R_i 表示群成员的访问权限和身份签名。

定义 1 通用群密钥分配算法^[7] (大小任意、动态变化的群组,但不包含安全性要求)

设用户空间 K 上的一个群密钥分配方案定义为三元组 (K, σ, F) , $F = \{f_i | i \in N\}$ 是函数簇,满足下面条件:(1) $\sigma(X): K \rightarrow M$, 表示群成员集 $X = (x_1, x_2, \dots, x_n)$ 用于计算群密钥公开的函数,称为广播消息产生函数,其中的 M 表示广播消息;(2) $f_i: U \times M \rightarrow M$, 是相应的群成员用于计算群密钥的函数,满足对任意 $i \in N$, 有 $f_i(X, \sigma(X)) = k_x$, $k_x \in M$ 称为 X 的群密钥。

定义 2 安全性群密钥分配算法^[7]

设 (U, σ, F) 是用户空间 U 上的一个群密钥分配方案,由定义 1 导出三元组 $(X, \sigma(X), f_n)$ 和 $k_x \in K$ 使得 $f(X, \sigma(X)) = k_x$, 称 $(X, \sigma(X), f_n)$ 为 (U, σ, F) 在 X 的一个分配实例,记作 $DI_{(U, \sigma, F)}(X) = (X, \sigma(X), f_n)$ 。如果满足对 $\forall A \subset U$, 当 A 与 X 统计独立时,有 $H(K | \sigma(X)A) = H(K)$, 那么称 $(X, \sigma(X), f_n)$ 是安全的密钥分配。

定义 3 带角色授权的群密钥分配算法

设 $R = \{r_i | i \in N\}$ 为所有角色的集合, $P = \{p_i | i \in N\}$ 为所有访问许可权的集合。从用户集合到角色集合的多对多映射 $UA \subseteq U \times R$ 表示用户被赋予的角色,从许可集合到角色集合的多对多映射 $PA \subseteq P \times R$ 表示角色被赋予的许可。对群密钥生成函数 $F = \{f_i | i \in N\}$ 加入限制条件 $f_i(X, P, R, \sigma(X \times P \times R)) = k_x$, $k_x \in M$, 使 RBAC 成员 X 间的访问通过对访问权力赋予角色来进行约束。

3 基于角色授权的群密钥分配算法设计

假设每一个群成员已建立了一个只与群管理员共享的密钥,群成员的所有可能密钥的集合设为 U (用户空间)。选择具

有较好安全性和较快速度的消息认证码函数(MAC 函数)作为单向函数^[4], 设 f 是 MAC 函数, $f(k, m)$ 表示在密钥 k 控制下 m 的 MAC, 群密钥的分配算法如下:

(1) 群成员的密钥生成算法

节点申请入群时,向群管理员提供自己的访问密钥 K_i 和角色 r_i 申请,群管理员经过身份认证后给该申请者发放相应的访问许可授权 p_i , 由单向函数 $f_i(k_i \times r_i \times p_i, \sigma(k_i \times r_i \times p_i)) = kx_i$ 算出成为群成员后的密钥 kx_i (图 1)。

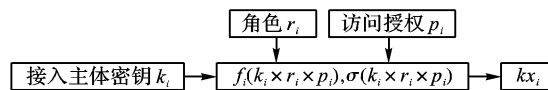


图 1 群成员的密钥生成算法流程

(2) 群密钥的生成算法

群密钥分配方案的算法结构采用多元树形成的分层结构^[4]的密钥分配树的形式建立(图 2)。树中的根节点代表群管理员,叶节点代表群成员,每个群成员关联着一个群成员密钥 $kx_i \in U$ 。通过密钥生成函数 $f(K, \sigma(K)) = k_F$, $K = (k_A, k_B, k_C)$ 算出上一层的群成员 x_F 的密钥 k_F , 最后由密钥生成函数 $f(K, \sigma(K)) = k_Z$, $K = (k_F, k_G, \dots)$ 算出根节点密钥 k_Z , 其中的 $\sigma(I)$ 为类似于文献[6]中用作数字签名的公用密钥。

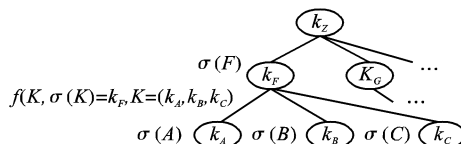


图 2 群密钥分配方案的算法结构

(3) 群密钥的分配策略

群密钥采用生成树算法形成后,采用类似 PKI 的管理结构,设立一些分层的管理代理(K_F, K_G)来满足分布式应用环境中的分散管理,并且这种代理只负责传递群密钥,而由群管理员用公钥对群密钥进签字,所有群成员可用群密钥(群管理员公钥)进行保密通信和群成员资格认证。

表 1 GKDARA 与其他群密钥分配方案的比较

| | GKDARA | OFT ^[4] | CLIQUEs ^[5] | COCA ^[6] |
|-------------|--------|--------------------|------------------------|---------------------|
| 密钥算法 | 单向函数 | 单向函数 | 公钥密码 | 公/私密码算法 |
| 运算速度 | 快 | 快 | 慢 | 快 |
| 每个群成员保存的密钥数 | 2 | $\log_2 m$ | 1 | 2 |
| 需要中心控制主体 | 需要 | 需要 | 不需要 | 不需要 |
| 适用环境 | 集中或分散 | 高度集中 | 分散 | 分散 |
| 抗授权侵犯能力 | 强 | 弱 | 弱 | 较强 |

说明:表中 m 表示群成员数

4 GKDARA 的安全性和可用性

GKDARA 算法是以单向函数为安全条件的,这种函数的安全强度在文献[4]中已有论述,而本算法是在原有保证密钥安全的基础上,通过增加对密钥权限的限制来增强系统的抗破坏能力,这种抗破坏能力的主要表现有以下几个方面:1)对抗被动攻击,即使某个成员的密钥被破译或盗用,授权侵犯者所拿到的群密钥因是公钥,当用私钥解密得到明文时,也只是被角色授权限制的那部分信息;2)对抗主动攻击,授权侵犯者所能篡改的信息也仅仅是被角色授权的那部分,而对于群组中其他角色的数据没有影响,因此缩小了安全威胁的范围,提升了整个系统的安全性。

(下转第 2779 页)

0.864315 0.904599 0.472427 0.853969 0.762322 0.353557
 0.733695 0.745354 0.826991 0.773888 0.141575 0.905118
 0.985931 0.282205 0.426557 0.0703757 0.136357 0.683187
 0.153233 0.973174 0.82168 0.780938 0.817347 0.630177
 0.903073 0.470168 0.155553 0.503922 0.847468 0.405591
 0.0748619 0.62508 0.338481 0.225562 0.191015 0.367504
 0.808039 }。

训练纯 BP 网络时,采用三层网络结构,输入层的神经元个数为 4,隐含层的神经元个数为 7,输出层的神经元个数为 1。学习速率 $\eta = 0.3$,权值和阈值通过随机函数来初始化。

训练 GA-BP 网络时,采用三层网络结构,输入层的神经元个数为 4,隐含层的神经元个数为 7,输出层的神经元个数为 1。学习速率 $\eta = 0.3$,通过 GA 算法训练过的最优个体来初始化权值和阈值。两种网络训练的结果如表 3 所示。

表 3 训练效果比较

| 训练次数 | 纯 BP 网络的收敛精度 | GA-BP 网络的收敛精度 |
|------|--------------|---------------|
| 500 | 0.067768776 | 0.005568797 |
| 1000 | 0.009885647 | 0.004569888 |
| 2000 | 0.007886523 | 0.003641287 |
| 3000 | 0.006998745 | 0.002756899 |
| 4000 | 0.006333389 | 0.002011345 |
| 4826 | 0.006003488 | 0.001999916 |

由表 3 的数据可以看出,对于相同的训练次数,GA-BP 网络比纯 BP 网络的收敛精度要高,收敛速度相对比较快。在纯 BP 网络训练 6764 次后,网络的曲线变化趋于平缓,收敛精度几乎不再变化,经过训练,纯 BP 网络的收敛精度为 0.005。GA-BP 网络训练 4826 次后,网络曲线趋于平缓,经训练,GA-BP 网络的收敛精度为 0.001。GA-BP 网络较纯 BP 网络,明显提高了收敛精度。其中 GA-BP 网络循环次数比较少,也就是说它的收敛速度是相对比较快的。最后,用 100 个检验样本来检验该网络,也得到了比较理想的结果。两种网络的收敛曲线如图 4 所示。

由网络曲线图可以明显看出,相同的训练参数和训练次数下,GA-BP 网络在收敛速度和收敛精度上都比纯 BP 网络

好。由此可以看出,GA-BP 网络加快了网络训练的速度,提高了收敛精度。

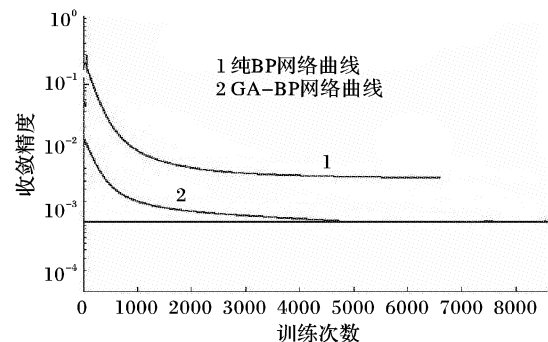


图 4 纯 BP 网络与 GA-BP 网络的收敛曲线比较

4 结语

通过以上研究可以看出,将 GA 与 BP 算法有机的融合,可以有效地弥补 BP 网络在网络结构、权值和阈值选择上的随机性缺陷,充分利用了 GA 的全局搜索能力和 BP 网络的局部搜索能力,从而增强了网络的智能搜索能力。当然基于 GA 的神经网络技术还有待继续研究学习,不断的完善和发展,使 GA-BP 网络更加成熟。

参考文献:

- [1] 周明. 遗传算法原理及其应用[M]. 北京: 国防工业出版社, 2001.
- [2] 潘昊, 钟珞, 陈杰. BP 神经网络训练的函数变步长搜索调整法[J]. 湖北工学院学报, 1997, 12(2).
- [3] LEUNG FHF, LAM HK, LINGSH, *et al.* Tuning of the Structure and Parameters of a Neural Network Using an Improved Genetic Algorithm[J]. IEEE Transactions on Neural networks, 2003, 14(1): 79-88.
- [4] 刘勇, 康立山, 陈屏. 非数值并行算法——遗传算法[M]. 北京: 科学出版社, 2000.
- [5] 杨朋林, 贺新. 人工神经网络与遗传算法结合的研究[J]. 现代电子技术, 2002, (12).
- [6] XIN YAO. Evolving Artificial Neural Networks[J]. Proceedings of the IEEE, 1999, 87(9): 1423-1447.
- [7] -32, 2002.
- [3] LAKSHMINATH R, MUKHERJEE S, SAMA A. A dual encryption protocol for scalable secure multicasting[A]. Proceedings of the 4th IEEE Symposium on computers and communication[C]. Red Sea, Egypt, 1999. 2-8.
- [4] DINSMORE PT, BALENSON DM, HEYMAN M, *et al.* Policy-based security management for large dynamic groups: An overview of the DCCM project[A]. Proceedings of the DARPA Information Survivability conference & Exposition[C]. SC, USA, 2000. 64-73.
- [5] STEINER M, TSUDIK G, WAIDNER. CLIQUES: A new approach to group key agreement[A]. Proceedings of 18th IEEE International Conference on Distributed Computing Systems[C]. Amsterdam, Netherlands, 1998. 380-387.
- [6] ZHOU LD, SCHNEIDER FB, VAN RENESSE R. COCA: A Secure Distributed On-line Certification Authority[EB/OL]. <http://www.cs.cornell.edu/fbs/publications/cocaTOCS.pdf>, 2002.
- [7] 李先贤, 怀进鹏, 刘旭东. 群密钥分配的动态安全性及其方案[J]. 计算机学报, 2002, 25(4): 337-345.
- [8] SANDHU R. Issues in RBAC[A]. Proceedings of the ACM RBAC Workshop MD[C]. ACM Press, 1996. 21-24.

(上接第 2769 页)

GKDARA 算法是一种基于角色授权约束的群密钥分配方案,其群密钥的生成和使用与其他方案的比较可见表 1 所示,结果显示该算法具有速度快和抗授权侵犯能力强的优点,减少了群成员在授权侵犯下的群组的安全威胁,具有可用性。

5 结语

本文在原有群密钥分配方案的基础上,提出了基于角色授权的群密钥分配算法,通过在群密钥生成和分发中加入角色授权的约束控制,增强了群的抗授权侵犯能力,减少了群成员在授权侵犯下的群的安全威胁。由于 Ad Hoc 网络的诸多复杂不安全因素的存在,文中提出的方案还只是着眼于一个具体问题的研究,如何提出一整套能满足所有安全目标的方案仍将是今后研究的热点。

参考文献:

- [1] ZHOU LD, HASS ZJ. Securing Ad Hoc Networks[J]. IEEE Network, 1999, 13(6): 24-30.
- [2] DAHILL B, LEVINE B, BELDING-ROYER EM, *et al.* A Secure Routing Protocol for Ad Hoc Networks[R]. UMass Tech Report 02