第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 安全技术 •

文章编号：1000—3428(2011)24—0132—04 文献标识码：A 中图分类号：TP309

基于双线性对的卫星网络密钥协商协议

矫文成，吴 杨，潘艳辉，李 华，郑天明

(军械工程学院计算机工程系，石家庄 050003)

摘 要：提出一种基于双线性对的卫星网络密钥协商协议，分析卫星网络的特点，给出协议实现过程。对协议的安全性分析表明，该协议不存在密钥托管问题，能抵御主动攻击，会话密钥协商满足不可控性。对协议的性能分析表明，该协议能提高会话密钥协商效率，满足实际的卫星网络密钥协商需求。

关键词：卫星网络；双线性对；离散对数问题；密钥协商；主动攻击

Key Agreement Protocol in Satellite Network Based on Bilinear Pairings

JIAO Wen-cheng, WU Yang, PAN Yan-hui, LI Hua, ZHENG Tian-ming

(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

【Abstract】 This paper proposes a key agreement protocol in satellite network based on bilinear pairings. It analyzes the characteristics of the satellite network and gives the implementation procedure of the protocol. Security analysis demonstrates that the key agreement protocol can resist active and passive attacks without key trusteeship problem and the key generating process is uncontrolled. Performance analysis demonstrates that the protocol can increase the efficiency of the session key agreement, it is more satisfied with needs of key generation in real satellite network.

【Key words】 satellite network; bilinear pairings; discrete logarithm problem; key agreement; active attack

DOI: 10.3969/j.issn.1000-3428.2011.24.044

1 概述

卫星网络与传统地面网络存在较大差异，鉴于卫星网络资源有限、网络结构及通信数据的机密性等特点，安全卫星网络密钥协商机制较传统地面网络具有更高的要求，其面临着单点失效问题、安全性与效率的平衡等问题。

为解决密钥协商机制中存在的单点失效问题，文献[1]提出了基于分布式 CA(Certificate Authority)的密钥管理模型，并将其运用到了 Ad Hoc 网络中。为提高密钥协商过程的安全性与效率，文献[2]使用双线性对技术和门限共享机制，实现了基于身份的 Ad Hoc 网络的密钥管理方案。文献[3]结合 Ad Hoc 网络与卫星网络的相似性，将基于分布式 CA 的密钥管理方案引入空间网络密钥管理，但协议仍需要依靠证书实现认证。为解决卫星网络密钥管理过程中的证书维护难题，文献[4]提出了基于身份的空间网络会话密钥协商方案。在此基础上，文献[5]提出了分布式网络中基于 IDPKC 的私钥更新方案，文献[6]在上述基础上提出了基于身份的空间网络私钥管理方案，其方案需预先在卫星网络指定满足门限值要求的卫星节点，负责分发密钥协商过程中的相关密钥分量信息，大大加重了被选卫星节点的负担，其方案复杂度也相对较高。文献[7]提出了具有较低复杂度的基于无证书密码学的可认证三方密钥协商协议，但其并不适用于卫星网络点对点通信。

在文献[7]的基础上，本文提出了基于双线性对的卫星网络密钥协商协议。该密钥协商协议在具有同等安全特性的同时，复杂度更低，能满足实际卫星网络密钥协商需求。

2 相关知识

利用椭圆曲线上的 Weil 对和 Tate 对构造基于双线性对的密码系统是目前一致采用的有效方法。下面对双线性映射对及其性质进行介绍。设 G_1 和 G_2 分别为循环加法群和乘法群，G_1 和 G_2 阶数为素数 q。定义 e: $G_1\times G_1\to G_2$ 为一个双线性映射，且满足：

(1)双线性：对任意 $a, b\in Z_p$，$P, Q\in G_1$，有 $e(aP, bQ)=e(P, Q)^{ab}$ 成立。

(2)非退化性：存在 $P\in G_1$，满足 $e(P, P)\neq 1$。

(3)可计算性：若 $P, Q\in G_1$，则可以在多项式时间内有效计算出 $e(P, Q)$。

本文提出的基于双线性对的卫星网络密钥协商协议安全性，依赖以下难题：

定义 1 若 G_1, G_2 是阶同为素数 q 的循环群，且有双线型映射 e: $G_1\times G_1\to G_2$，P 为 G_1 的生成元，则在$<G_1, G_2, e>$上的 BDH(Bilinear Difie-Hellman)问题是：给定 $a, b, c\in Z_P$，由$<P, aP, bP, cP>$计算 $e(P, P)^{abc}$。

定义 2 设 G_1, G_2 是阶为素数 q 的循环群，且有双线性映射 e: $G_1\times G_1\to G_2$，G_1 的生成元为 P，则$<G_1, G_2, e>$上的 DBDH (Decisional Bilinear Difie-Hellman)问题可描述为：由任意 $a, b, c\in Z_P$，由$<P, aP, bP, cP>$和 $h\in G_2$ 判断 $h=e(P, P)^{abc}$ 是否成立。

3 卫星网络密钥管理特点

卫星网络与传统地面网络存在诸多差异，其优点主要有：通信距离远，且费用与通信距离无关；信息覆盖面积大，

作者简介：矫文成(1970－)，男，副教授，主研方向：信息安全，软件工程；吴 杨，硕士研究生；潘艳辉、李 华，博士；郑天明，硕士研究生

收稿日期：2011-07-04 **E-mail：**baiyanwy@163.com

可进行多址通信；通信频带宽、传输量大，适用于多种业务数据传输；卫星通信具有良好的机动性。

卫星网络的上述突出优点有效补充了其他通信手段的不足。同传统地面网络相比，卫星网络仍存在的问题有：

(1)卫星星载资源有限，包括计算能力、电力供应、信息存储容量等。

(2)受轨道高度及节点计算速度影响，卫星网络空间链路时延较大，受复杂的空间电磁环境影响，信号误码率较高。

(3)伴随卫星节点的运动，网络拓扑结构处于不断变化状态中。

(4)地理条件及国界等限制因素，使地面控制中心对卫星节点的管理难度较大。

(5)卫星网络采用广播方式传输信号，信息易被窃听。

现有卫星网络密钥管理主要分为：集中式与分布式密钥管理。对于集中式密钥管理模式，密钥协商和分配主要由密钥生成及分发中心完成，面临严重的单点失效问题。为解决单点失效问题，文献[1]提出了基于分布式 CA 的密钥管理模型。典型的卫星网络分布式密钥管理网络模型如图 1 所示。

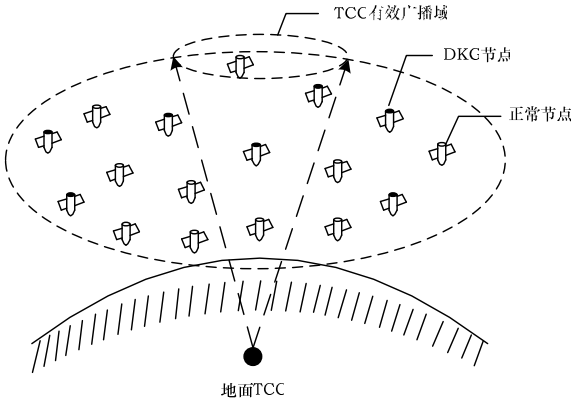

图 1　分布式卫星网络密钥协商网络模型

如图 1 所示，当卫星网络密钥协商采用分布式管理模式时，地面控制中心 TCC(Telluric Control Center)将选择满足门限值需求的 DKG(Distributed Key Generator)节点为密钥协商过程提供密钥分量，此举加重了 DKG 节点的负担。随着门限值的提高，密钥协商过程的计算及通信开销也将急剧增加，密钥协商效率也大大降低。结合现有密钥协商技术与卫星网络的特点，卫星网络密钥协商的主要难点及需求为：

(1)卫星网络卫星节点信息存储空间及计算能力有限，对卫星网络密钥协商协议的计算复杂度提出了很高的要求。因此，卫星网络密钥协商协议应使用较小的存储空间并具有较低的计算复杂度。

(2)有限的卫星网络带宽，对卫星网络密钥协商过程中的节点信息交互次数提出了新的要求。因此，卫星网络密钥协商协议应具有较少的交互次数，以降低通信开销。

(3)面对复杂的空间环境及传输信息的机密性，卫星网络密钥协商协议必须具有较高的安全性，确保密钥及信息的安全性。

(4)动态变化的卫星网络结构，大大增加了密钥协商的难度。因此，卫星网络密钥协商协议应适应不断变化的卫星网络结构。

综上所述，在保证卫星网络密钥协商过程及相关信息安全性前提下，卫星网络密钥协商协议应具有较低的计算复杂度，尽量少的信息交互次数以降低通信开销，并能够自主适应卫星网络结构的动态变化。本文提的基于双线性对的卫星网络密钥协商协议，其卫星网络模型如图 2 所示。

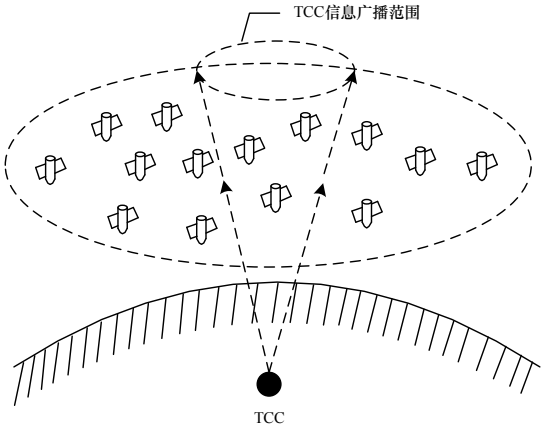

图 2　卫星网络密钥协商网络模型

如图 2 所示，所有卫星节点均具有同等地位，TCC 负责系统初始化及新卫星节点加入时的初始参数设置，TCC 为任一卫星节点被赋予唯一 ID 标志(其 MAC 值或 IP 地址)。

4　协议实现过程

4.1　系统初始化

系统初始化阶段，TCC 和所有卫星节点离线完成如下工作：

(1)选择阶为 q，生成元为 P 的循环加法群 G_1，循环乘法群 G_2。

(2)确定双线性映射 e: $G_1\times G_1\rightarrow G_2$。

(3)定义安全 Hash 函数：H_1: $\{0, 1\}^*\rightarrow G_1$ 将字符串映射为 G_1 上的点，H_2: $G_2\rightarrow\{0, 1\}^*$ 将循环乘法群 G_2 上的点映射为字符串。

(4)TCC 随机选取 $s\in Z_P^*$作为系统主密钥，计算系统公钥 $P_{\text{pub}}=sP\in G_1$。

(5)TCC 为任一卫星节点 A 指定唯一身份标志 ID_A，并计算其 $K_\text{A}=H_1(ID_\text{A})$，部分私钥 $K^{-1}{}_\text{A}=sK_\text{A}$。

(6)节点 A 随机选取 $x_\text{A}\in Z_P^*$作为其秘密参数。

(7)节点 A 计算其私钥 $S_\text{A}=x_\text{A}K^{-1}{}_\text{A}=x_\text{A}sK_\text{A}$，公钥 $P_\text{A}=x_\text{A}P$，短期密钥 $S'_\text{A}=K^{-1}{}_\text{A}+x_\text{A}K_\text{A}$。

(8)TCC 选择信息完整性验证函数 $MAC_K(m)$。

(9)TCC 设定节点秘密参数更新周期为 w。TCC 完成系统初始化后，公开如下参数：

$\{P, q, P_{\text{pub}}, G_1, G_2, e, H_1, H_2, g, MAC_K(m), w\}$

4.2　新节点加入

若有新节点 A 加入网络，TCC 为新加入节点 A 指定唯一标志 ID_A，并为其计算 K_A、$K^{-1}{}_\text{A}$。节点 A 选择秘密随机数 $x_\text{A}\in Z_P^*$作为其秘密参数，并计算其私钥 $S_\text{A}=x_\text{A}K^{-1}{}_\text{A}=x_\text{A}sK_\text{A}$，公钥 $P_\text{A}=x_\text{A}P$，短期密钥 $S'{}_\text{A}=K^{-1}{}_\text{A}+x_\text{A}K_\text{A}=(s+x_\text{A})K_\text{A}$。

4.3　节点秘密参数更新

任意节点 A 秘密参数更新时刻到达时，节点 A 随机选取新的 $x_\text{A}\in Z_P^*$作为其秘密参数；同时，节点 A 计算其新私钥 $S_\text{A}=x_\text{A}K^{-1}{}_\text{A}=x_\text{A}sK_\text{A}$，新公钥 $P_\text{A}=x_\text{A}P$，新短期密钥 $S'{}_\text{A}=K^{-1}{}_\text{A}+x_\text{A}K_\text{A}$。

4.4　节点会话密钥协商

系统初始化完成后，任意节点 A 与 B 间会话密钥 SK_{AB} 协商过程如图 3 所示。

本文提出的基于双线性对的卫星节点 A、B 间会话密钥

协商过程如下：

(1)节点 A 任意选择 $a \in Z_P^*$，计算 $T_A=aK_A$。

(2)节点 A 发送信息$\{ID_A, T_A, P_A\}$到节点 B。

(3)B 收到$\{ID_A, T_A, P_A\}$后，任意选择 $b \in Z_P^*$，并计算 $T_B=bK_B$、$SK_B=e(S'_B, P)^b+e(T_A, P_{pub}+P_A)$，由信息完整性验证函数计算得到信息：$MAC_{SKB}(ID_B, T_B, P_B)$、$MAC_{SKB}(ID_A, T_A, P_A)$，并发送$\{ID_B, T_B, P_B, MAC_{SKB}(ID_B, T_B, P_B)\}$到 A。

(4)节点 A 收到节点 B 的信息$\{ID_B, T_B, P_B, MAC_{SKB}(ID_B, T_B, P_B)\}$后，计算：$SK_A=e(S'_A, P)^a+e(T_B, P_{pub}+P_B)$、$MAC_{SKA}(ID_B, T_B, P_B)$、$MAC_{SKA}(ID_A, T_A, P_A)$，并验证等式(1)是否成立。若成立，则发送$\{ID_A, \mathrm{MAC}_{SKA}(ID_A, T_A, P_A)\}$；若等式(1)不成立，则信息完整性已被破坏，节点 A 重新发起会话密钥协商：

$$MAC_{SKA}(ID_B, T_B, P_B)=MAC_{SKB}(ID_B, T_B, P_B) \quad (1)$$

(5)节点 B 收到$\{ID_A, MAC_{SKA}(ID_A, T_A, P_A)\}$后验证等式(2)是否成立。若等式(2)不成立，则节点 A、B 重新进行会话密钥协商；若等式(2)成立，则节点 A、B 会话密钥协商成功。

$$MAC_{SKA}(ID_A, T_A, P_A)=MAC_{SKB}(ID_A, T_A, P_A) \quad (2)$$

结论：节点 A 验证式(1)、B 验证式(2)成立后，节点 A、B 计算获得会话密钥 $SK_{AB}=H_2(SK_A)=H_2(SK_B)$。证明 $SK_{AB}=H_2(SK_A)=H_2(SK_B)$等式成立过程如下：

证明：

$$SK_A=e(S'_A, P)^a+e(T_B, P_{pub}+P_B)=e((s+x_A)K_A, P)^a+e(bK_B, (s+x_B)P)=e(K_A, P)^{a(s+xA)}+e(K_B, P)^{b(s+xB)} \quad (3)$$

$$SK_B=e(S'_B, P)^b+e(T_A, P_{pub}+P_A)=e((s+x_B)K_B, P)^b+e(aK_A, (s+x_A)P)=e(K_B, P)^{b(s+xB)}+e(K_A, P)^{a(s+xA)} \quad (4)$$

由式(3)、式(4)可知 $SK_A=SK_B$，因此，$SK_{AB}=H_2(SK_A)=H_2(SK_B)$得证，经信息完整性验证后节点 A、B 会话密钥 SK_{AB} 协商成功。

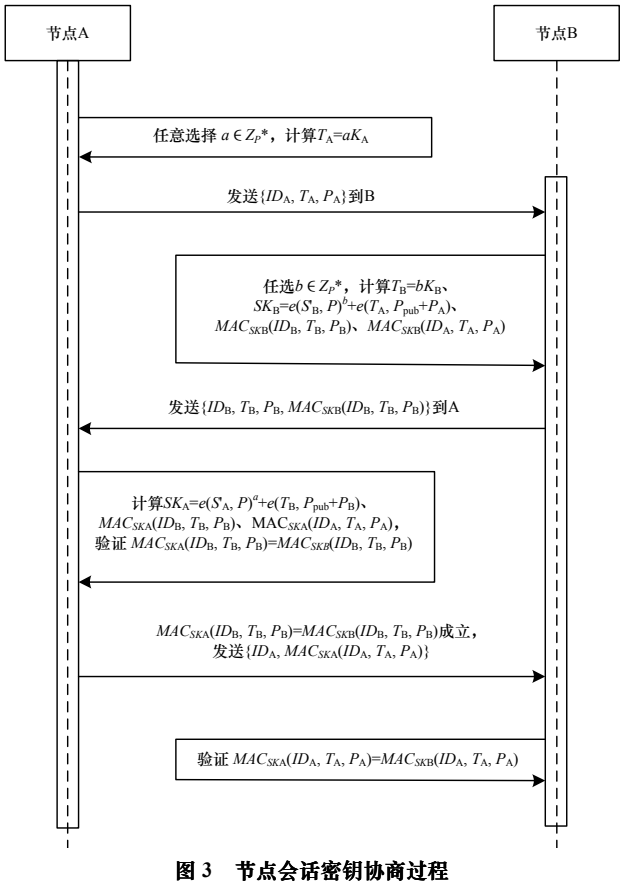

图 3 节点会话密钥协商过程

文献[7]为三方密钥协商协议，通过引入不同的密钥生成参数及参数交互过程，实现了适合于卫星网络的点对点密钥协商协议。为保证密钥协商过程安全，本文提出了节点秘密参数更新机制，定期对节点秘密参数进行更新，更加确保了节点间密钥协商的安全。

5 安全性及性能分析

5.1 安全性分析

本文提出的卫星网络密钥协商协议不存在密钥托管问题，其安全性基于椭圆曲线上离散对数问题的困难性，协议安全性证明如下：

定理 1 在密钥协商过程中，不存在节点私钥托管问题。

证明：系统初始化时，TCC 为卫星网络任一节点 A 指定唯一标志 ID_A，并使用其私钥 s 为节点 A 生成部分私钥 $K^{-1}{}_A=sH_1(ID_A)$，同时节点 A 随机选取 $x_A \in Z_P^*$作为其秘密参数，并生成其私钥 $S_A=x_AK^{-1}{}_A$，由于 x_A 为节点 A 随机选取的秘密参数，因此 TCC 无法获取节点 A 的 S_A，任意卫星节点在会话密钥协商过程中，不存在私钥托管问题。

定理 2 卫星节点密钥协商过程，能够抵御主动攻击。

证明：攻击者通过伪造、重放、假冒等方式获得系统信息，本文提出的卫星网络密钥协商协议，能够抵御以下主动攻击：

(1)假冒攻击

在会话密钥协商过程中，假定节点 C 冒充节点 A 与节点 B 协商会话密钥，节点 C 伪造 a'、x'_A，并计算 $T'_A=a'K_A$、$P'_A=x'_AP$，发送消息$\{ID_A, T'_A, P'_A\}$给节点 B；节点 B 收到$\{ID_A, T'_A, P'_A\}$后，计算 $SK_B=e(S'_B, P)^b+e(T'_A, P_{pub}+P'_A)=e(K_B, P)^{b(s+xB)}+e(K_A, P)^{a'(s+x'A)}$、$MAC_{SKB}(ID_B, T_B, P_B)$，并发送应答消息$\{ID_B, T_B, P_B, MAC_{SKB}(ID_B, T_B, P_B)\}$给节点 C；节点 C 收到节点 B 的应答消息后，将试图计算 $SK_A=e(S'_A, P)^{a'}+e(T_B, P_{pub}+P_B)$，而 $S'_A=K^{-1}{}_A+x_AK_A$，由于节点 C 不具有 $K^{-1}{}_A$，因此节点 C 无法克隆 S'_A，即使节点 C 为 S'_A 指定随机值，其计算获得的 SK_A 也无法与 SK_B 保持一致，节点 C 冒充节点 A 与节点 B 的会话密钥协商也将失败，因此，本文提出的协议能够抵御卫星节点间会话密钥协商过长中的假冒攻击。

(2)重放攻击

假定正常卫星节点 A 与 B 会话密钥协商过程中，攻击者 C 截获节点 A 与 B 间的会话信息，并选择重放其中的信息，攻击者 C 即使得到相应回复，由于 C 不具有节点 A 或 B 的秘密信息，因此，仍然无法生成合法会话密钥。

(3)中间人攻击

若攻击者对卫星节点会话密钥协商过程的交互信息进行任何修改，式(1)、式(2)可以检测此类攻击。因此，本文提出的密钥协商方案，能够有效抵御中间人攻击。

定理 3 卫星节点密钥协商过程，能够抵御被动攻击。

证明：被动攻击方式中，攻击者通过窃听方式获取卫星节点间会话密钥协商过程中的会话信息，但攻击者不具有会话密钥协商双方的秘密信息，即使攻击者获得了会话密钥协商阶段的相关信息，依然无法计算获得卫星节点间的会话密钥。因此，本文提出的密钥协商方案，能够有效抵御密钥协商过程中的被动攻击。

定理 4 本文提出的密钥协商协议具有前向安全性。

证明：若卫星节点的长期秘密或私钥泄露，但在每次会话密钥协商过程中，卫星节点均随机选择一非零整数参与会话密钥生成。因此，即使卫星节点的长期秘密或私钥泄露，

攻击者仍无法重构先前协商的会话密钥，本文提出的密钥协商协议具有前向安全性。

定理 5 本文提出的密钥协商协议使协商的会话密钥具有不可控性。

证明：会话密钥协商过程中，参与双方均随机选取一非零整数参与会话密钥生成。随机整数的引入，使得参与会话密钥协商的任何一方都不能控制会话密钥生成参数。因此，本文提出的密钥协商协议使协商的会话密钥具有不可控性。

5.2 性能分析

本文提出的密钥协商协议实现过程，涉及的主要运算有：双线性对运算；字符串到 G_1 上点映射运算；G_2 上点到字符串映射运算；G_1 上数乘运算；G_1 上点加运算；Hash 函数运算。卫星节点会话密钥协商只需 3 轮信息交换即可完成会话密钥协商过程，较少的通信轮数不但提高了会话密钥的协商效率，同时也减少了对卫星网络带宽资源的占用。

文献[6]基于门限值的分布式密钥管理机制，需在空间卫星网络预先设置满足门限需求的若干节点，不足之处在于加重了被选节点的负担，对其管理也比较复杂，其计算及通信开销均高于本文的密钥协商协议。在系统初始化时，TCC 离线为所有卫星节点计算相关参数，系统建立后，卫星节点间的会话密钥协商过程可自主进行，不需要 TCC 参与，因此，本文的密钥协商协议更符合实际的空间卫星网络运行需求。

6 结束语

构建合理的卫星网络密钥协商协议，关键在于怎样平衡效率与安全需求。本文结合双线性对技术与椭圆曲线上离散对数问题的难解性，构建了无需密钥托管的卫星网络密钥协商协议。与现有卫星网络基于门限值的分布式密钥协商机制相比，在满足同等安全需求的条件下，本文构建的协议具有更高的执行效率。下一步将结合卫星网络的特点，设计开发相应的密钥协商协议仿真系统，进一步评估密钥管理方案的执行效率。

参考文献

[1] Zhou Lidong, Hass Z J. Securing Ad Hoc Networks[J]. IEEE Networks, 1999, 13(6): 24-30.

[2] 吴　平, 王保云, 徐开勇. 基于身份的 Ad Hoc 网络密钥管理方案[J]. 计算机工程, 2008, 34(24): 143-145.

[3] 杨德明, 慕德俊, 许　钟. Ad Hoc 空间网络密钥管理与认证方案[J]. 通信学报, 2006, 27(8): 104-107.

[4] 彭长艳, 沈亚敏, 王　剑, 等. 基于身份的空间网络安全研究[J]. 飞行器测控学报, 2008, 27(3): 56-62.

[5] 李　伟, 罗长远, 初　晓. 分布式网络中基于 IDPKC 的私钥更新方案[J]. 计算机应用, 2009, 29(7): 1825-1827.

[6] 李　伟. 空间信息网络密钥管理研究[D]. 郑州: 解放军信息工程大学, 2009.

[7] 陈家琪, 冯　俊, 郝　妍. 基于无证书密码学的可认证三方密钥协商协议[J]. 计算机应用研究, 2010, 27(5): 1902-1904.

编辑　顾姣健

(上接第 131 页)

特点。MCBAC 与 RBAC 的对比分析如表 2 所示。

表 2　MCBAC 与 RBAC 的对比分析

指标	RBAC	MCBAC
授权管理	一次授权，无限访问	有限授权，自动回收
主体可信评估	无	多维评估
环境敏感性	无	有
安全性	一般	强

5 结束语

在分布式网络环境下，应用系统能够提供访问服务并实现信息共享，但非法用户的接入可能会对系统造成潜在的威胁，对分布式系统资源实现有效的访问控制是目前系统安全领域研究热点之一。本文提出一种适合于分布式系统的访问控制模型 MCBAC，它扩展了传统 RBAC 的功能，具有较好的灵活性和安全性，可以很好地适用动态多变的开放的分布式系统。下一步工作是进一步完善 MCBAC 模型实现过程，运用访问控制策略和访问控制请求/响应描述语言(XACML)对本模型进行形式化的描述，并进行安全策略分析。

参考文献

[1] Park J, Sandhu S. Towards Usage Control Models: Beyond Traditional Access Control[C]//Proc. of the 7th ACM Symp. on Access Control Models and Technologies. Monterey, USA: [s. n.], 2002.

[2] 王东安, 张方舟, 南　凯, 等. 网格计算中基于信任度的访问控制研究[J]. 计算机应用研究, 2006, 23(6): 49-51.

[3] Chakraborty S, Ray I. Trust BAC Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems[C]// Proc. of the 11th ACM Symp. on Access Control Models and Technologies. New York, USA: ACM Press, 2006.

[4] Sandhu R S. Peer-to-Peer Access Control Architecture Using Trusted Computing Technology[C]//Proc. of the 10th ACM Symp. on Access Control Models and Technologies. Stockholm, Sweden: [s. n.], 2005.

[5] 李晓峰, 冯登国, 陈朝武, 等. 基于属性的访问控制模型[J]. 通信学报, 2008, 29(4): 90-98.

[6] Bertino E, Catania B. GEO-RBAC: A Spatially Aware RBAC[C]// Proc. of the 10th ACM Symp. on Access Control Models and Technologies. New York, USA: ACM Press, 2005.

[7] 黄　恺, 李　斓, 李建华. 分布式环境下行为感知的信任管理[J]. 计算机工程, 2011, 37(1): 139-141.

[8] 田立勤, 林　闯. 可信网络中一种基于行为信任预测的博弈控制机制[J]. 计算机学报, 2007, 30(11): 1930-1938.

编辑　陈　文