

多服务器环境移动通信网身份认证方案设计

王崇霞¹, 高美真², 刘 倩³, 胡晓曦³

(1 长治学院 计算机系, 山西 长治 046010; 2 焦作师范高等专科学校 计算机与信息工程学院, 河南 焦作 454000;
北京科技大学 计算机与通信工程学院, 北京 100083)

摘 要: 基于双线性对和密钥协商机制, 与远程多服务器认证协议相结合, 提出一种自认证的多服务器环境远程用户身份认证方案, 建立移动通信网跨业务的统一身份认证机制, 实现可靠的双向认证和会话密钥协商, 提高业务使用的便捷性和用户身份信息的共享性。理论分析表明, 提议的方案可以抵御多种安全攻击, 通信复杂度更低, 适合移动通信网多服务器环境的用户需求。

关键词: 移动通信网; 身份认证; 多服务器环境; 自认证

中图分类号: TP391

文献标识码: A

文章编号: 1000—7180(2016)06—0152—05

Identity Authentication Scheme Design of Mobile Communication Network in Multi-server Environment

WANG Chong-xia¹, GAO Mei-zhen², LIU Qian³, HU Xiao-xi³

(1 Department of Computer Science, Changzhi University, Changzhi 046010, China;

2 School of Computer and Information Engineering, Jiaozuo Teachers College, Jiaozuo 454000, China;

3 School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: Based on bilinear pairings and secret key negotiation mechanism, combined with the remote multi-server authentication protocol, we propose a self- ∇ certified multi- ∇ server environment remote user authentication scheme, establish a unified identity authentication mechanism across the business for mobile communication networks, realize bidirection authentication and session key agreement, improve the convenience of business use and user identity information sharing. Theoretical analysis shows that our proposed scheme can resist a variety of attacks, suitable for mobile communication network multi- ∇ server environment user needs.

Key words: mobile communication network; identity authentication ; multi-server environment; self-certified

1 引言

移动通信以良好的灵活性和扩展性成为人们生活中不可或缺的一部分, 人们可以随时随地地将无线手持设备接入网络, 为我们日常生活带来了便利, 但其开放、移动和拓扑结构动态变化的特点, 使其安全问题成为移动通信网发展运行的关键, 而高效安全的身份认证协议是移动通信网发展的基础^[1]。

随着移动通信用户需求的广泛增加及无线网络

的快速发展, 移动业务种类越来越复杂繁多, 一些强大的在线移动服务提供商可以同时提供多种不同的服务, 如移动政务、移动学习、移动网络游戏、视频点播、电子邮件等等, 而不同的服务资源可能需要不同的服务器提供, 人们将此类网络环境称为多服务器环境^[2]。用户在使用移动通信网的不同服务时, 可能需要多次输入用户名和口令进行认证授权, 也就是说移动通信网业务的繁杂多样也要求用户必须维护其在移动通信网中的所有身份信息, 这会给用户带

来不便.随着移动通信系统的发展壮大,新业务层出不穷,移动通信网必须提供全网统一的安全认证机制,才能推动移动通信业务的普及进步.

学者们已提出了多种多服务器环境身份认证方案^[3-5],但都存在缺陷^[6].2008年,J. H. Lee, D. H. Lee提出一种安全高效的移动通信网多服务器环境认证协议^[7],存在不能自由添加服务器的缺陷^[6];文献^[8]提出基于双线性对的无线通信网身份认证方案,其存在不能实现双向认证和密钥协商的缺陷;2010年,K. H. Yeh, N. W. Lo提出一种新颖的多服务器环境远程用户认证方案^[11],但不能实现双向认证,且存在不可检测在线口令猜测攻击的缺陷^[12];2015年,文献^[12]提议的多服务器环境认证方案中,认证服务器必须参与用户认证并提供认证参数,随着网络应用和用户数量的增加,认证服务器将成为网络通信的瓶颈.本文基于双线性对和秘钥协商机制,与远程多服务器认证协议相结合,提出一种自认证的多服务器环境远程用户身份认证方案,实现移动通信网中跨业务的统一安全身份认证,提高了业务使用的便捷性和用户身份信息的可靠性.

2 相关的数学难题假设

定义1 椭圆曲线离散对数问题(discrete logarithm problem, DLP)^[13]:设 G 是 q 阶循环群, g 是 G 的生成元,对于元素 $P \in G$,为满足 $P = \alpha g$,求 $\alpha \in \mathbb{Z}_q^*$ 是困难的.

定义2 双线性映射^[11]:设 q 为大素数, G_1 是 q 阶加法循环群, G_2 是 q 阶乘法循环群,则双线性映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 满足:

- (1) 双线性: 设 $P_1, P_2, Q_1, Q_2, P, Q \in G_1, a, b \in \mathbb{Z}_q^*$ ($\mathbb{Z}_q^*$ 是 q 阶整数域),存在:

$$\begin{aligned} \hat{e}(P_1 + P_2, Q) &= \hat{e}(P_1, Q) \hat{e}(P_2, Q), \\ \hat{e}(P, Q_1 + Q_2) &= \hat{e}(P, Q_1) \hat{e}(P, Q_2), \\ e(aQ, bR) &= e(Q, bR)^a \\ &= e(aQ, R)^b \\ &= e(Q, R)^{ab}. \end{aligned}$$
- (2) 非退化性: 存在 $P, Q \in G_1$,使 $\hat{e}(P, Q) \neq 1$.
- (3) 可计算性: 存在有效算法计算 $\hat{e}(P, Q)$.

3 多服务器环境身份认证方案

3.1 多服务器环境总体结构

多服务器环境的移动通信网身份认证协议主要包含三部分.用户、认证服务器和多台提供服务的服务器.用户是服务申请方,服务器为用户提供多种不

同服务,认证服务器负责为系统中的用户和服务器建立注册认证账户和设定参数.提议的移动通信网络系统的总体结构如图1所示.

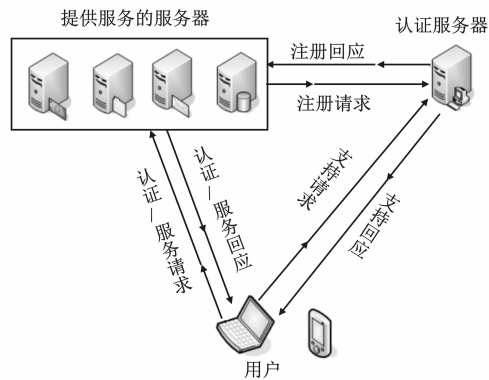


图1 多服务器环境移动通信网总体结构

系统建立: 设 G_1 为 q 阶(q 为大素数)的加法循环群, G_2 为 q 阶乘法循环群,且 $e: G_1 \times G_1 \rightarrow G_2$ 是双线性映射, p 是 G_1 的生成元,定义hash函数: $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_q^*, H_2: \{0,1\}^* \rightarrow G_1$. 令 $s_k \in \mathbb{Z}_q^*, s_k$ 为系统主密钥, $P_{pub} = s_k p$ 为系统公钥, S_i 为第 i 个提供服务的服务器标识,公布系统参数 $parameter = \{q, e, P_{pub}, p, H_1, H_2\}$.

本文提议的多服务器环境移动通信网身份认证协议包括:注册(服务器和用户)、登录认证、口令更新三个阶段.

3.2 服务器、用户注册

3.2.1 服务器注册

当服务器 S_i 申请成为系统一台提供服务的服务器时, S_i 首先在认证服务器RS注册.

(1) S_i 的注册名为 $ID_{S_i}, ID_{S_i} \in \{0,1\}^*$,产生随机数 $r_{S_i} \in \mathbb{Z}_q^* (r_{S_i} \neq 0,1)$,计算 $V_{S_i} = r_{S_i} \cdot H_2(ID_{S_i}), W_{S_i} = r_{S_i} \cdot p$,通过安全信道发送 (ID_{S_i}, V_{S_i}) 到RS.

(2) RS收到 S_i 的注册请求信息后,计算 $C_{S_i} = s_k \cdot H_2(ID_{S_i}), A_{S_i} = C_{S_i} + V_{S_i} = (s_k + r_{S_i}) \cdot H_2(ID_{S_i})$. 认证服务器RS在数据库中保存 S_i 的相关信息 $\{ID_{S_i}, A_{S_i}\}$,并通过安全信道发送 $\{ID_{RS}, C_{S_i}\}$ 到 S_i .

(3) S_i 收到信息后,计算 $p \cdot (C_{S_i} + V_{S_i}) = p \cdot A_{S_i} = (P_{pub} + W_{S_i}) \cdot H_2(ID_{S_i})$ 是否成立来验证RS的正确性,并保存 $\{ID_{S_i}, C_{S_i}, W_{S_i}, V_{S_i}\}$.

3.2.2 用户注册

(1) 当用户 U_i 申请成为系统成员时, U_i 输入用户名 ID_{U_i} 和口令 $PW_{U_i}, ID_{U_i} \in \{0,1\}^*$,计算 $P_{U_i} = H_1(PW_{U_i}), W_{U_i} = P_{U_i} \cdot p, V_{U_i} = P_{U_i} \cdot H_2(ID_{U_i})$,

U_i 通过安全信道发送信息 $\{ID_{U_i}, V_{U_i}\}$ 到 RS.

(2) RS 收到请求信息后, 计算 $C_{U_i} = s_k \cdot H_2(ID_{U_i})$, $A_{U_i} = C_{U_i} + V_{U_i}$, 确定 U_i 在 RS 的注册时间 T_{U_i} , 在数据库中保存 U_i 的相关信息 $\{ID_{U_i}, A_{U_i}, T_{U_i}\}$, 为用户 U_i 颁发包含 $\{ID_{U_i}, V_{U_i}, C_{U_i}, T_{U_i}\}$ 的智能卡, 并通过安全信道发送给 U_i .

(3) U_i 收到智能卡后, 计算 $p \cdot (C_{U_i} + V_{U_i}) = p \cdot A_{U_i} = (P_{pub} + W_{U_i}) \cdot H_2(ID_{U_i})$ 是否成立来验证智能卡的正确性.

3.3 登录认证

(1) 用户 U_i 登录, 并申请服务器 S_i 的服务

U_i 输入用户名 ID_{U_i} 和口令 PW_{U_i} , 计算 $V_{U_i}' = H_1(PW_{U_i}) \cdot H_2(ID_{U_i})$, 并与智能卡中保存的 V_{U_i} 比较, 错误则退出, 否则 U_i 登录成功. U_i 申请服务器 S_i 的服务, U_i 产生随机数 $r_i \in \mathbb{Z}_q^*$, 计算 $D_i = r_i \cdot H_2(ID_{U_i})$, $R_i = e(r_i \cdot C_{U_i}, H_2(ID_{U_i}))$, 发送信息 $\{ID_{U_i}, D_i, R_i\}$ 到 S_i .

(2) S_i 认证 U_i

S_i 验证 $R_i' = e(D_i, C_{S_i}) = R_i$ 是否成立, 成立则确定用户 U_i 为合法移动通信网用户. S_i 产生随机数 $r_j \in \mathbb{Z}_q^*$, 计算 $D_j = r_j \cdot H_2(ID_{U_i})$, $T_j = r_j \cdot D_i$, S_i 计算 $B_i = e(C_{S_i}, H_2(ID_{U_i}))e(V_{S_i}, P)$, 发送 $\{ID_{S_i}, D_j, B_i, W_{S_i}\}$ 到用户 U_i .

(3) U_i 认证 S_i

U_i 接到 S_i 发来的信息后, 验证 $B_i' = e(H_2(ID_{S_i}), W_{S_i} + C_{U_i}) = B_i$ 是否成立, 成立, 则确定服务器 S_i 的正确性. 计算 $T_i = r_i \cdot D_j = T_j = r_i \cdot r_j \cdot H_2(ID_{U_i})$ 为 S_i 与 U_i 通信的协商密钥.

3.4 口令更新

当用户 U_i 申请更改口令或其 T_{U_i} 到达有效期, U_i 需要更新口令.

(1) U_i 输入用户名 ID_{U_i} 和口令 PW_{U_i} , 计算 $V_{U_i}' = H_1(PW_{U_i}) \cdot H_2(ID_{U_i})$, 判断 V_{U_i}' 与智能卡中保存的 V_{U_i} 是否相等, 如果不相等则终止操作; 否则, U_i 产生随机数 $r_n \in \mathbb{Z}_q^*$, 计算 $N_i = r_n \cdot p$, $D_{U_i} = V_{U_i}' \oplus r_n \cdot P_{pub}$, 发送 $\{ID_{U_i}, D_{U_i}, N_i\}$ 到 RS 申请更改口令.

(2) RS 收到信息后, 在数据库中查找用户 ID_{U_i} 的相关信息, 计算 $V_{U_i}' = D_{U_i} \oplus s_k \cdot N_i$, $C_{U_i} = s_k \cdot H_2(ID_{U_i})$, $A_{U_i}' = C_{U_i} + V_{U_i}'$, 比较 $A_{U_i}' = A_{U_i}$ 是否成立, 成立则确定用户 U_i 的合法身份. RS 计算 $X_{RS} = H_1(V_{U_i}' \parallel s_k \cdot N_i)$, 发送 $\{ID_{RS}, X_{RS}\}$ 到 U_i .

(3) U_i 收到信息后计算 $X_{RS}' = H_1(V_{U_i} \parallel r_n \cdot P_{pub})$, 验证 $X_{RS} = X_{RS}'$ 是否成立, 成立则产生新的

口令 PW_{new} , 计算 $P_{new} = H_1(PW_{new})$, $V_{new} = P_{new} \cdot H_2(ID_{U_i})$, $W_{new} = P_{new} \cdot P$, $D_{new} = V_{new} \oplus r_n \cdot P_{pub}$, $X_{U_i} = e(C_{U_i}, W_{new})$, 发送 $\{ID_{U_i}, D_{new}, X_{U_i}, N_i\}$ 到 RS.

(4) RS 收到请求信息后, 计算 $V_{new}' = D_{new} \oplus s_k \cdot N_i$, $X_{U_i}' = e(V_{new}', P_{pub})$, 判断 $X_{U_i}' = X_{U_i}$ 是否成立, 成立则计算 $A_{new} = C_{U_i} + V_{new}'$, 产生新的注册时间 T_{new} , 更新数据库中用户 U_i 的信息为 $\{ID_{U_i}, A_{new}, T_{new}\}$, 计算 $X_{new} = H_1(V_{new}' \parallel s_k \cdot N_i)$, 发送 $\{ID_{RS}, X_{new}, T_{new}\}$ 到 U_i .

(5) U_i 计算并验证 $X_{new}' = H_1(V_{new} \parallel r_n \cdot P_{pub}) = X_{new}$, 若正确, U_i 更新智能卡信息, 将 V_{U_i} 更新为 V_{new} , 将 T_{U_i} 更新为 T_{new} .

4 安全性分析

本文提议的认证方案的安全性主要从以下几方面考虑.

(1) 用户、服务器在认证服务器只需要注册一次.

提议的认证方案中, 用户和服务器必须在系统认证服务器注册成为系统成员, 并建立相应的注册信息. 注册后, 用户可以申请访问服务器, 服务器认证用户后提供服务, 用户一次注册就可以直接访问认证服务器管理的多个服务器, 不需要向每个服务器登记注册.

(2) 任意用户申请服务器认证 / 服务时, 不需要认证服务器的参与.

提议的认证方案中, 用户需要某个服务器提供服务时, 直接向相应服务器申请认证 / 服务, 认证申请过程中, 不需要认证服务器 RS 的参与, 也就是说用户与服务器的认证过程中, 不需要用户与认证服务器、服务器与认证服务器的多次认证通信, 减少了认证服务器的负担和认证中三方的交互通信. 尤其在用户认证申请频繁时, 认证服务器不会成为系统瓶颈.

(3) 任意服务器的加入 / 撤出并不影响多服务器环境移动通信网身份认证协议的正确执行.

提议的认证方案中, 服务器首先注册成为一台系统合法服务器, 认证服务器保留服务器注册信息 $\{ID_{S_i}, A_{S_i}\}$, 服务器保留信息 $\{ID_{S_i}, C_{S_i}, W_{S_i}, V_{S_i}\}$. 如果新服务器需要加入系统, 新服务器首先在认证服务器注册并产生相应信息, 系统添加相应服务; 若服务器撤出, 系统撤销服务并删除其保留信息, 用户在申请已撤出服务器提供服务时, 验证信息 $R_i' =$

$e(D_i, C_{S_i}) = R_i$ 不成立,无法提供服务.因此服务器的加入 / 撤出并不影响多服务器环境移动通信网身份认证协议的正确执行.

(4) 实现双向认证和密钥协商,安全性高

本文提议的认证方案是基于实体双向认证和协商密钥的基础上实现通信.当用户 U_i 申请任意服务器提供服务时,首先进行自我验证并登录系统,然后向服务器 S_i 提出服务申请,并产生随机数 $r_i \in \mathbb{Z}_q^*$. S_i 通过验证 $R_i' = e(D_i, C_{S_i}) = R_i$ 是否成立认证用户 U_i 的合法性, U_i 通过计算 $B_i = e(C_{S_i}, H_2(\text{ID}_{U_i}))e(V_{S_i}, P) = e(H_2(\text{ID}_{S_i}), W_{S_i} + C_{U_i}) = B_i'$ 是否成立验证服务器的正确性,验证通过后,根据双方产生的随机数 r_i, r_j , 产生协商密钥 $T_i = T_j = r_i \times r_j \times H_2(\text{ID}_{U_i})$. 用户每次申请认证 / 服务时,都需要生成随机数 r_i, r_j , 随机数不同,协商的密钥不同.所以本文提议的认证方案属于一次一密,安全性较高.

(5) 认证服务器和服务器不需要保存任何用户的验证信息

提议的认证方案中,认证服务器 RS 和服务器 S_i 不需要维护和保存用户的任何验证信息,认证服务器 RS 只保存用户的身份信息 $\{\text{ID}_{U_i}, A_{U_i}, T_{U_i}\}$. 当一个合法用户申请服务器认证时,通过彼此拥有的系统参数实现相互验证,验证过程中不需要 RS 提供任何密钥或参数.

(6) 抵抗多种安全攻击

① 抵抗重放攻击

重放攻击是指重放远程用户发送给服务器的消息从而再次获得服务.在提议的认证方案中,用户申请服务器提供服务时,需要产生随机数 r_i ,并根据 r_i 产生参数 R_i 发送给服务器.基于定义 1 中的 DLP 困难性假设,攻击者 Aanony 获得随机数 r_i ,并重放消息是不可能的,所以提议方案可以抵抗重放攻击.

② 抵抗服务器欺骗攻击

假设攻击者 Aanony 伪装成一个合法的服务器 S_j 来欺骗用户 U_i . 因服务器是伪装的,用户发送的 $R_i = e(r_i \times C_{U_i}, H_2(\text{ID}_{S_i})) = R_i'$ 就无法验证通过,且伪装的服务器不可能拥有系统主密钥 s_k 和注册时产生的随机数 r_{S_i} ,则不可能计算合法的 C_{S_i}, V_{S_i} ,其计算的 $B_i = e(C_{S_i}, H_2(\text{ID}_{U_i}))e(V_{S_i}, P)$ 发送到用户后,用户 U_i 验证 $B_i' = e(H_2(\text{ID}_{S_i}), W_{S_i} + C_{U_i}) = B_i$ 不成功,则无法产生协商密钥,通信失败,伪装的服务器欺骗不成功.

③ 抵抗恶意用户和不可检测口令猜测攻击

提议的认证方案中,恶意用户即使可以获取到合法用户的身份 ID_{U_i} ,但其登录口令 PW_{U_i} 是经过 Hash 函数计算后传输,恶意用户无法获得,即使恶意用户通过不可检测口令猜测攻击获取到了合法用户口令 PW_{U_i} 和 V_{U_i} ,但由于不能获得系统主密钥 s_k ,所以不能计算 C_{U_i} ,其计算的 $R_i = e(r_i \times C_{U_i}, H_2(\text{ID}_{S_i})) = R_i'$ 在申请服务器 S_i 认证时不能成功.因此,提议方案可以抵抗恶意用户和不可检测口令猜测攻击.

5 性能分析

根据计算复杂性理论,移动通信网中远程用户身份认证协议的性能主要从通信量和计算量两方面衡量.通信量主要取决于交互轮数,交互轮数是远程认证过程中影响认证方案性能的最主要因素.计算量主要包括 Hash 运算、幂乘运算、加解密运算和对运算,为了方便协议评估,我们定义如下符号:

TG_e :运行双线性映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 的执行时间;

T_m :运行幂乘运算的时间;

T_{H_2} :Hash 函数 H_2 的执行时间;

T_E :运行加 / 解密算法的时间;

提议的认证方案与文献[8,10]进行比较,结果如表 1 所示.综合性能分析的各个方面,提议的认证方案与文献[8]相比,实现了双向认证和密钥协商,增加了认证安全性;与文献[10]比较,降低了通信量,减少了认证服务器的认证参与.所以提出的认证方案综合性能较好.

表 1 性能比较

方案	客户方				服务器				交互轮数
	TG_e	T_m	T_{H_2}	T_E	TG_e	T_m	T_{H_2}	T_E	
文献[8]	0	3	2	0	2	3	2	0	3
文献[10]	0	4	2	2	0	4	5	2	5
提出方案	2	1	2	0	2	2	2	0	3

6 结束语

随着移动通信服务的应用普及,移动通信网的业务种类越来越繁杂多样,不同的业务服务需要不同的服务器提供服务,而移动通信网用户身份与业务应用的紧密耦合致使同一用户需要在不同的应用中注册认证,给用户增加负担的同时也带来了潜在的安全隐患,统一安全的身份认证机制使保障多服务器环境移动通信网实现的基础.本文基于双线性对和密钥协商机制,提出一种自认证的多服务器环境远程用户身份认证方案,实现移动通信网中

跨业务的统一安全身份认证. 提议的方案中远程用户和服务器在认证服务器注册后, 用户即可独立申请服务器提供服务, 服务申请过程中不需要认证服务器参与. 理论分析证明, 提议的认证方案有较高的安全性, 可以抵抗各类攻击, 通信复杂度更低.

参考文献:

- [1] 王崇霞, 高美真, 刘倩, 等. 异构云匿名身份认证方案设计[J]. 微电子学与计算机, 2014, 31(7): 37-40.
- [2] 张晓敏. 基于二次剩余的多服务器环境下的身份认证协议[J]. 计算机安全, 2012(8): 15-20.
- [3] 万涛, 廖维川, 马建峰. 面向多服务器架构的认证协议分析与改进[J]. 西安电子科技大学学报, 2013, 40(6): 174-180.
- [4] C H Huang, J S Chou, Y Chen. Improved multi-server authentication protocol[J]. International journal of Security and Communication Networks, 2012, 5(3): 331 - 341.
- [5] X Li, Y Xiong, J Ma, et al. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards[J]. Journal of Network and Computer Applications, 2012, 35(2): 763 - 769.
- [6] J S, Chou Y I, Chen, C H Huang, et al. Comments on four multi-server authentication protocols using smart card[EB/OL]. [2016-04-20]. <http://eprint.iacr.org/2012/406.pdf>.

- [7] J H Lee, D H Lee. Efficient and secure remote authenticated key agreement scheme for multi-server using mobile equipment[C]// Proceedings of International Conference on Consumer Electronics, Las Vegas, NV: IEEE, 2008: 1-2.
- [8] Y M Tseng, T Y Wu, J D Wu. A pairing-based user authentication scheme for wireless clients with smart card[J]. Informatics, 2008, 19(2): 285-302.
- [9] K H Yeh, N W Lo. A novel remote user authentication scheme for multi-server environment without using smart cards [J]. International Journal of Innovative Computing Information and Control, 2010, 6(8): 3467-3478.
- [10] 舒剑. 高效的基于口令多服务器认证方案[J]. 计算机应用研究, 2015, 33(8): 2444-2446.
- [11] 张华, 温巧燕, 金正平. 可证明安全算法与协议[M]. 北京: 科学出版社, 2012.

作者简介:

王崇霞(1970-), 女, 副教授. 研究方向为密码学与网络安全. E-mail: cxwang2000@sina.com.

高美真(1970-), 女, 副教授. 研究方向为计算机网络与图像处理.

刘倩(1987-), 博士研究生. 研究方向为智能网络及网络安全.

胡晓曦(1988-), 博士研究生. 研究方向为云计算、空间网络等.

(上接第 151 页)

- [2] Pawlak Z. Rudiments of rough sets[J]. Information Sciences, 2007, 177(1): 3-27.
- [3] 陈志奎, 吕爱玲, 张清辰. 基于属性重要性的不完备数据填充算法[J]. 微电子学与计算机, 2013, 30(7): 167-172.
- [4] 王超, 罗可. 不完备信息系统中基于限制容差关系的属性约简方法[J]. 计算机应用, 2011, 31(12): 3236-3239.
- [5] Kryszkiewicz M. Rough set approach to incomplete information system. Information Sciences[J]. 1998, 112(1-4): 39-49.
- [6] Leung Y, Li D. Maximal consistent block technique for rule acquisition in incomplete information systems [J]. Information Sciences, 2003, 153(1): 85-106.
- [7] Leung Y, Wu W, Zhang W. Knowledge acquisition in

incomplete information systems: A rough set approach [J]. European Journal of Operational Research, 2006, 168(1): 164-180.

- [8] 关晓蔷, 钱宇华. 基于不完备信息系统的决策树生成算法[J]. 计算机科学, 2012, 39(1): 156-158.
- [9] Qian Y, Liang J, Li D, et al. Approximation reduction in inconsistent incomplete decision tables [J]. Knowledge-Based Systems, 2010, 23(5): 427-433.
- [10] 鄂旭, 邵良杉, 周津, 等. 一种新的不完备信息系统属性约简算法[J]. 重庆邮电大学学报(自然科学版), 2010, 22(5): 648-651.

作者简介:

黄治国 男, (1978-), 博士, 讲师. 研究方向为数据挖掘、智能计. E-mail: huangzg2020@139.com.